IMPLEMENTACIÓN DE SERVICIOS DE ANONIMATO PORTABLE BASADO EN UN SBC DE BAJO COSTO

FABRICIO ESPINOZA GELIZ & MARÍA ALEJANDRA ZÚÑIGA.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA.

FACULTAD DE INGENIERÍA.

INGENIERÍA INFORMÁTICA.

POPAYÁN

2019

IMPLEMENTAR UN SERVICIO DE ANONIMATO PORTABLE BASADO EN UN SBC DE BAJO COSTO

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniería Informática

FABRIZIO ESPINOZA GELIZ & MARÍA ALEJANDRA ZÚÑIGA.

Director:
Msc. SILER AMADOR DONADO

Co-Director:
Msc. KATERINE MARCELES VILLALBA

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA.
FACULTAD DE INGENIERÍA.
INGENIERÍA INFORMÁTICA.
POPAYÁN
2019

TABLA DE CONTENIDO

LISTA DE TABLAS 7
LISTADO DE IMÁGENES 8
LISTADO DE GRÁFICAS 9
ABSTRACT 10
RESUMEN 11
ACRÓNIMOS 12
1. INTRODUCCIÓN 13
CAPITULO I 15
2. PLANTEAMIENTO DEL PROBLEMA. 15
3. JUSTIFICACIÓN 16
4. OBJETIVOS. 17
4.1. Objetivo general. 17
4.2. Objetivos específicos. 17
CAPITULO II 18
5. MARCO TEÓRICO 18
5.1. Revisión bibliográfica 18
5.1.1. Revisión de literaturas sobre el servicio de anonimato 18
5.1.1.1. Bases de datos y términos de búsqueda 18
5.1.1.2. Proceso de selección 18
5.1.2. Criterios de selección 19
5.1.3. Criterios de evaluación de calidad 20
5.1.4. Estudio de evaluación de calidad 21
5.1.5. Análisis de resultados 23
5.1.6. Amenazas a la validez 25
5.2. Antecedentes 26
5.3. Marco conceptual 33
5.3.1. Dispositivos SBC 33
5.3.2. Ventajas y desventajas de SBC 33
5.3.3. Proxy 33
5.3.4. Criptografía 34
5.3.5. Técnicas de criptografía 34
5.3.6. ¿Qué es un servicio? 35
5.3.7. Tipos de servicios 36
5.3.7.1. Información que se puede enviar por e-mail 36
5.3.8. VPN 36
5.3.9. ISO 3166 37
5.4. Marco legal 37
5.4.1. Ley 1273 de 2009 38

5.4.2. Ley 1581 de 2012 38
5.4.3. Decreto 1377 de 2013 39
CAPITULO III 40
6. METODOLOGÍA 40
7. FASE 1: Establecer un análisis comparativo entre los diferentes servicios de anonimato para determinar el más adecuado 40
7.1. Recolección de información de los distintos servicios de anonimato: 40
7.1.1. Indicadores de selección 41
7.2. Analizar los diferentes tipos de servicios de anonimato que se utilizan 44
8. FASE 2: Categorizar por medio de un análisis comparativo el SBC adecuado, para la implementación del servicio de anonimato portable. 47
8.1. Recolección de información de un SBC de bajo costo. 47
8.2. Selección de SBC de bajo costo que se utilizará en el proyecto 60
9. FASE 3: Proponer la arquitectura para un servicio de anonimato portable basado en un SBC 60
9.1.1.1. Instalación de la arquitectura diseñada en el SBC para la navegación 61
9.1.1.2. Instalación de la arquitectura diseñada en el SBC para la llamada Voip 63
9.2. Realizar pruebas de servicio anónimo bajo SBC 63
9.2.1. Pruebas del servicio navegación anónima 64
9.2.2. Instalación del sistema operativo raspbian 64
9.2.3. Instalación de VPN Raspberry pi 3 Model B+ 66
8.1.1.1. Instalación de host-Point Raspberry pi 3 Model B+ 71
9.2.4. Resultados Raspberry pi 3 model B + en la navegación 75
9.2.5. Pruebas del servicio de llamada VoIP 76
9.2.6. Instalación del SO 79
9.2.7. Configuraciones Iniciales 80
9.2.8. Actualizaciones 83
9.2.9. Instalación de paquetes 83
9.2.10. Instalación de Asterisk 83
9.2.11. Creación de usuarios y extensiones 86
9.2.12. Configuración PROXYCHAINS 89
9.3. Documentación de resultados de las pruebas realizadas 90
9.3.1. Pruebas de rendimiento del dispositivo 90
CAPITULO IV 94
10. CONCLUSIONES Y TRABAJOS FUTUROS 94
10.1. Conclusiones 94
11. REFERENCIAS 96

LISTA DE TABLAS

Tabla 1 Resultados arrojados por las fuentes bibliográficas. 21
Tabla 2 Resultados de cada estudio primario con respecto a los criterios de evaluación de calidad..... 23
Tabla 3 Actividades diarias online de navegación 42
Tabla 4 Características de los dispositivos SBC's. 52
Tabla 5 Aportes característicos de los SBC's..... 57
Tabla 6 Información con de los datos normalizados. 59
Tabla 7 Dispositivos SBC's que se adecuan más a nuestro proyecto..... 60

LISTADO DE IMÁGENES

Imagen 1 Diagrama de burbujas de los estudios y escenario por año. 24
Imagen 2 Diagrama de burbuja de los escenarios y tipo de investigación. 24
Imagen 3 Diagrama de burbuja de los escenarios y tipo de contribución. 25
Imagen 4 Estadística de pérdidas de información durante la navegación desde dispositivos móviles. . 45
Imagen 5 Características de antena Wi-fi. 61
Imagen 6 Diseño de la infraestructura de red. 62
Imagen 7 Diseño de la infraestructura de red 63
Imagen 8 Selección del sistema operativo. 64
Imagen 9 Descarga del sistema operativo. 65
Imagen 10 Configuración de Putty. 66
Imagen 11 Instalación del VPN 67
Imagen 12 Configuración de llaves y clientes. 68
Imagen 13. Asignación de IP por DNS 71
Imagen 14 Estadísticas del uso de dispositivos a temprana edad 78
Imagen 15 Hipervínculo que descarga el SO 80
Imagen 16 Aplicación utilizada para instalar el SO 80
Imagen 17 Menú de configuración de Raspberry 81
Imagen 18 Selección de conexión a internet (Mediante Wi-fi) 81
Imagen 19 Nombre de la red que se conectara 81
Imagen 20 Menú de configuración de Raspberry 82
Imagen 21 Configuración del continente 82
Imagen 22 Configuración del país 82
Imagen 23 Zona horaria 82
Imagen 24 Verificación de los archivos en la carpeta 84
Imagen 25 Menú de configuración y selección de extensiones de Asterisk 85
Imagen 26 Selección de las extensiones 85
Imagen 27 Creación de usuarios 86
Imagen 28 Configuración para la comunicación entre usuarios 87
Imagen 29 Registro de llamada en la consola de Asterisk 88

LISTADO DE GRÁFICAS

Gráfica 1 Estadística de frecuencia de uso de internet 46
Gráfica 2 Numero de cambios de IP Raspberry pi 3 Model B+ 75
Gráfica 3 Estadística de amenazas móviles 79
Gráfica 4 Resultado de prueba hardware Raspberry pi 3 modelo b+ 91
Gráfica 5 Resultado de prueba hardware Raspberry pi 2 92

ABSTRACT

This document details the investigation and implementation of portable anonymity services based on low-cost SBC, such as navigation and VoIP calling. To carry out this task, three very limited phases are carried out, one dependent on the other. As a first phase, a complete recognition of the different types of existing anonymity services and those most used by the community in general is carried out, thus reaching the choice of the most appropriate service. In this process, the development of the SIP protocol for IP telephony is also realized in parallel. This is called "Information collection to establish a comparative analysis between the different anonymity services to determine the most appropriate one." The second phase was to conduct a detailed investigation against SBC technology, covering equipment, cost, operating models, characteristics of the devices and associated applications (operating systems and projects made with SBC devices).

Phase three refers to the application of capabilities, focusing all efforts on developing the concept of portable anonymity service without losing the properties of the implementation of security and constant IP change when navigating in the cloud or performing a VoIP call this is how the concept of Security and types of services is studied. There is also a development of the model that is needed for this implementation, ending with a practical development that allowed the creation of an anonymity service through the previous study on the capabilities of the SBC equipment, which meets certain standards to be marketed to the user. Together with the integrated study from the system design to its application with the user.

RESUMEN

El presente documento, detalla la investigación e implementación de servicios de anonimato portable basado en SBC de bajo costo, como lo es la navegación y llamada VoIP. Para llevar a cabo esta tarea se realizan tres fases muy delimitadas una dependiente de la otra. Como primera fase se realiza un reconocimiento completo de los diferentes tipos de servicios de anonimato existentes y los más usados por la comunidad en general llegando así a la elección del servicio más adecuado. En este proceso también se da cuenta en forma paralela del desarrollo del protocolo SIP para la telefonía IP. Esto se denomina "Recolección de información para establecer un análisis comparativo entre los diferentes servicios de anonimato para determinar el más adecuado". La segunda fase fue realizar una detallada investigación frente a la tecnología SBC, abarcando equipamiento, costo, modelos de funcionamiento, características de los dispositivos y aplicaciones asociadas (sistemas operativos y proyectos hechos con dispositivos SBC).

La fase tres se refiere a la aplicación de las capacidades, centrando todos los esfuerzos en desarrollar el concepto de servicio anonimato portable sin perder las propiedades que presenta la implementación de seguridad y cambio de IP constante a la hora de navegar en la nube o realizar una llamada VoIP. Es así como se estudia el concepto de Seguridad y tipos de servicios. Se realiza también un desarrollo del modelo que se necesita para esta implementación finalizando con un desarrollo práctico que permitió crear un servicio de anonimato a través del estudio previo sobre las capacidades de los equipos SBC, que cumple con ciertos estándares para ser comercializado al usuario. Junto con el estudio integrado desde el diseño del sistema hasta su aplicación con el usuario.

ACRÓNIMOS

CAC: Call Admission Control

CDR: Call Detail Record

GSM: Groupe Special Mobile

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IMS: IP Multimedia Subsystems

IP: Internet Protocol

ITSP: Internet Telephony Service Providers

LAN: Local Area Network

PBX: Private Branch Exchange

SBC: Single Board Computer

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

VoIP: Voice over IP

WAN: Wide Area Network

XML: Extensible Markup Language

1. INTRODUCCIÓN

La seguridad informática en la actualidad es un área que toma cada vez más fuerza, debido al alto nivel de ciberataques y robos de datos personales que existen en el mundo de la Internet, a diario los hackers buscan obtener información importante, lo cual afecta a una gran cantidad de personas que navegan de manera insegura en la red.

En este proyecto se pretende minimizar el riesgo de la información que viaja en las redes de comunicaciones, la cual puede estar expuesta a las diferentes amenazas que trae consigo el internet y por ende permitirle al usuario establecer comunicaciones seguras al momento de realizar una petición a través de la red por medio de la utilización de un dispositivo de bajo costo portable.

A continuación, el desarrollo del proyecto se encuentra distribuido en 4 capítulos, organizados de la siguiente manera: En el capítulo I se encuentra el planteamiento del problema donde se evidencian las consecuencias por las cuales este proyecto se lleva a cabo dejando claro las debilidades que tienen tanto las medianas y pequeñas organizaciones como las personas del común que hagan uso de una red WI-FI pública y como se ve involucrada la seguridad informática en los últimos años y la importancia de la misma, con base en lo anterior se construirá una herramienta capaz de administrar dos servicios de seguridad empleando la tecnología SBC para brindar anonimato de bajo costo y se resalta en la justificación y los objetivos del proyecto. En el capítulo II se lleva a cabo una revisión bibliográfica para la recolección de información necesaria para la ejecución del proyecto; además de la elaboración del marco teórico que encierra aspectos relacionados con las definiciones conceptuales esenciales, unificando fortalezas amenazas y debilidades de trabajos similares que den solución a la problemática planteada con el fin de mejorar cada uno para la implementación de este proyecto, un marco legal donde se tienen en cuenta las leyes bajo las cuales se rige la seguridad informática el anonimato y la elaboración de este trabajo. En el capítulo III se encuentra la metodología con la cual se desarrolla la elaboración del proyecto la cual está ejecutada por 3 fases la primera donde se realiza un análisis comparativo de los diferentes servicios de anonimato para la selección del más adecuado, en la segunda fase se detalla el estudio de SBC para implementar los servicios anteriormente seleccionados para continuar con la fase 3 de implementación con el SBC seleccionado

y los servicios adecuados se mide rendimiento y resultados de las pruebas realizadas. Finalmente se presentan unas conclusiones y trabajos futuros que enmarcan toda la reflexión del trabajo realizado.

CAPITULO I

2. PLANTEAMIENTO DEL PROBLEMA.

Desde el año 2010 hasta la actualidad se ha identificado un índice bastante alto de inseguridad en la red, como por ejemplo el 65% de las personas han sido afectadas por un cibercrimen, el 21% de los negocios colombianos han sido víctimas de ciberataques y unos 133 usuarios empresariales son infectados al mes por códigos maliciosos que se encuentran a la hora de entrar al mundo de la red, (Ciberseguridad, 2018) entre muchas otras estadísticas que establecen las amenazas latentes que se está expuesto a la hora de navegar por la nube.

Es importante destacar que aún en el año 2019 se siguen viendo noticias sobre datos sustraídos a particulares y a grandes compañías, donde a través del uso de software malicioso han obtenido fotos comprometedoras accedidas desde sus dispositivos móviles, dado que los ciberdelincuentes cada vez más fijan su atención en los dispositivos de mayor uso. De este modo se evidencia la necesidad de implementar seguridad, prevención, y sobre todo la concienciación de las personas para que naveguen siempre de manera segura y así tengan la confianza de no dejar rastros e información que los pueda exponer frente a una amenaza.

No obstante en la actualidad se han evidenciado Puntos de acceso Wi-Fi públicos, tales como cafeterías, universidades, parques, hoteles entre otros, los cuales corren el riesgo de que su tráfico de datos se encuentre expuesto a diferentes amenazas, debido a que en estos sitios se utiliza por lo general una red Wi-Fi pública con requisitos mínimos de seguridad, donde su tráfico de red podría ser capturado fácilmente por otros usuarios que accedan a ésta; por lo que se encuentra una problemática bastante considerable al momento de conectarse a internet, dando como resultado la siguiente pregunta de investigación ¿CÓMO SE PODRÍA GARANTIZAR EL SERVICIO DE ANONIMATO DE MANERA PORTABLE BASADO EN UN SBC DE BAJO COSTO?

3. JUSTIFICACIÓN

Este proyecto de investigación surge de la necesidad de una respuesta a la problemática planteada anteriormente, y es allí donde es aplicable la misión de garantizar la privacidad, confidencialidad e integridad a la hora de utilizar un servicio de internet, dado que al ejecutar este tipo de actividades a través de los ordenadores y dispositivos móviles se dejan una serie de rastros compuestos por cookies, cache, historial y hasta la ubicación geográfica de la IP del usuario, las cuales son pistas que permiten obtener información sensible acerca de hábitos de navegación y datos personales.

Hasta hace un tiempo, aquellas personas preocupadas por su privacidad o que utilizan ordenadores compartidos con frecuencia en hoteles, lugares de trabajo, centros educativos, parques, etc. Deben hacer una limpieza manual de todos los posibles rastros que se dejan a la hora de navegar en una red de internet; por ende, a pesar de hacer uso de navegadores incógnitos no evita el dejar una pista visible a todos los hackers y/o crackers que se encuentran en el internet en busca de esta información. Con la implementación de este proyecto se pretende hacer uso de los recursos computacionales que ofrecen los SBC, utilizando una arquitectura adecuada e implementando un servicio anónimo portable que certifique la privacidad, confidencialidad e integridad de la información al momento de estar de cara al internet por medio de diferentes tipos de dispositivos y por ende minimizar la cantidad de rastros digitales que se dejan al ejecutar un servicio.

4. OBJETIVOS.

4.1. Objetivo general.

Implementar dos servicios de anonimato portable basado en un SBC de bajo costo

4.2. Objetivos específicos.

- Establecer un análisis comparativo entre los diferentes servicios de anonimato para determinar los más adecuados.
- Categorizar por medio de un análisis comparativo el SBC adecuado, para la implementación de los servicios de anonimato portable.
- Proponer la arquitectura para los servicios de anonimato portable basado en un SBC.

CAPITULO II

5. MARCO TEÓRICO

El presente marco teórico hace referencia a trabajos realizados previamente que están relacionados con la temática del proyecto y se mencionan algunos de los conceptos que son fundamentales para el conocimiento del proyecto.

5.1. Revisión bibliográfica

Se realizó una revisión de la literatura sobre un conjunto de bases de datos bibliográficas, con el fin de obtener artículos en inglés y español dentro de un intervalo de tiempo entre el año 2008 y 2019 que estén relacionados con la navegación web anónima en internet mediante el cambio de IP.

5.1.1. Revisión de literaturas sobre el servicio de anonimato

5.1.1.1. Bases de datos y términos de búsqueda

Para realizar esta investigación, se seleccionaron bases de datos que tuvieran las siguientes características: un motor de bases de datos bibliográficas basado en la web, un motor de bases de datos bibliográficas capaz de realizar búsquedas filtrando por palabras claves y que contenga artículos relacionados con el área de seguridad durante la navegación. Dado a lo anterior, se realizó una revisión bibliográfica sobre los siguientes motores de bases de datos bibliográficas:

Google Scholar

IEEE Xplore Digital Library.

Sciencedirect

Google

La lista de palabras clave usadas para encontrar una respuesta a la pregunta de investigación propuesta en el capítulo 1 son: “tor”, “browsing anonymous”, “information vulnerability”, “single board computer”, “methodology”, “p2p”, “privacy”, “encryption”, “raspberry”, “proxy”, “navigation private”, “vpn”, “private network”, “proxyHam”, “Voip”, “GSM”, “security”.

5.1.1.2. Proceso de selección

El proceso de selección está dividido en 5 fases.

A) **Búsqueda en las bases de datos.** Se listan las fuentes bibliográficas que se consideren necesarias, se construyen las cadenas de búsqueda con palabras clave y sus respectivos sinónimos, posteriormente se adaptan las cadenas a cada motor de búsqueda de las fuentes bibliográficas.

B) **Eliminar estudios repetidos**. Al realizar la búsqueda de estudios los resultados pueden ser redundantes, por tal motivo se eliminan dichos estudios y son almacenados en un gestor de referencias bibliográficas.

C) **Selección de estudios primarios.** A partir de los artículos encontrados se aplicaron los criterios de inclusión y exclusión los cuales son mencionados en la sección "Criterios de selección" para poder extraer los artículos primarios. Posteriormente cada estudio primario es almacenado.

D) **Selección final.** Una vez almacenado cada estudio primario, se procede a realizar una lectura completa de cada estudio.

E) **Evaluación de calidad.** Con base en los criterios de calidad que serán nombrados en la sección Criterios de evaluación de calidad, los estudios primarios son evaluados y clasificados con el fin de garantizar la evaluación apropiada de los estudios primarios.

5.1.2. Criterios de selección

Una de las actividades esenciales durante la fase de planeación de esta investigación, es la definición de los criterios de inclusión y los criterios de exclusión. El objetivo de dichos criterios es ayudar a los investigadores, en el momento de seleccionar los artículos apropiados, y se emplea para reducir la cantidad de trabajos que serán analizados.

Para la selección de estudios relevantes, el criterio de inclusión se basó en un análisis del título, resumen y palabras claves de los artículos obtenidos en la búsqueda, esto con el fin de determinar si están relacionados con la navegación anónima, si el artículo menciona el uso de algún VPN, arquitecturas, metodología o procesos que nos permita una navegación segura en internet.

5.1.3. Criterios de evaluación de calidad

El objetivo de los criterios de evaluación de calidad es asegurar una apropiada evaluación de cada estudio que fue considerado primario. Los criterios de evaluación establecidos son:

- **CEC 1**. ¿El artículo o documento presenta algún tipo de contribución: metodología, herramienta, enfoque, estrategia para la navegación segura?
- **CEC 2**. ¿El estudio presenta algún método de investigación basado en el análisis y descripción como: estudio empírico, estudio experimental, pruebas de concepto, teórica o caso de estudio?
- **CEC 3**. ¿El estudio menciona y aplica el tipo de contribución planteado?
- **CEC 4.** ¿El estudio realiza un análisis de los resultados obtenidos?

Para cada uno de los criterios de evaluación de calidad, se aplicó la siguiente valoración: B (Bueno) = 1, In (Intermedio) = 0.5, N (no) = 0. De esta manera, el resultado total para la evaluación de cada estudio (CEC1 + CEC2 + CEC3 + CEC4) puede resultar de la siguiente manera: 0, 0.5 y 1 (incompleto) 1,5 y 2 (regular), 2,5 (bueno), 3 (muy bueno) y 3,5 y 4 (excelente).

Para evaluar cada estudio primario, se establecieron reglas a cada criterio de evaluación, esto con el fin de complementar la parte cualitativa a la valoración:

- **CEC 1.**

B, el estudio propone el uso o una nueva metodología, técnica o herramienta.

In, la contribución está presente pero no se describe claramente.

N, la contribución no puede ser identificada o no está establecida.

- **CEC 2.**

B, el estudio menciona que ha aplicado explícitamente algún método de investigación.

In, el estudio presenta información relevante pero no especifica el método de investigación.

N, el método de investigación no puede ser identificado o no está descrito.

- **CEC 3.**

B, el estudio presenta de forma detallada el tipo de contribución que ha sido llevado a cabo.

In, el tipo de contribución llevado a cabo es representado de forma breve.

N, el estudio no describe claramente el tipo de contribución llevado a cabo.

- **CEC 4.**

B, el estudio presenta un análisis detallado que explique los resultados obtenidos.

In, los resultados son explicados brevemente.

N, los resultados no pueden ser identificados o no están descritos.

5.1.4. Estudio de evaluación de calidad

Inicialmente se identificaron 55 estudios en los motores de bases de datos bibliográficas, estos de ahora en adelante se consideran como encontrados. Al eliminar los estudios redundantes, 42 estudios fueron considerados como no repetidos. Con el criterio de inclusión, 27 estudios fueron considerados como relevantes, mediante la lectura del título, resumen y palabras claves. Los 17 estudios fueron leídos y con el criterio de exclusión, se obtuvieron 17 primarios, como se observa en la siguiente tabla (tabla 1).

BASES DE DATOS Y OTROS	**ESTUDIOS**			
	ENCONTRADOS	NO REPETIDOS	RELEVANTES	PRIMARIOS
Google Scholar	6	4	1	0
IEEE Xplore Digital Library	20	14	11	6
Sciencedirect	4	4	2	2
Google	24	19	13	9
TOTAL	**54**	**41**	**27**	**17**

Tabla 1 Resultados arrojados por las fuentes bibliográficas.

Fuente: Propia.

A continuación, la tabla 2 muestra el resultado total de los estudios primarios luego de aplicar la evaluación de calidad. Cada estudio es enumerado por la columna ID, los nombres de los estudios primarios son presentados en la columna Nombre del estudio con su respectivo año de publicación en la columna Año de la publicación. Las columnas compuestas por CEC (Criterio de Evaluación de Calidad) corresponden a la valoración obtenida de los criterios de evaluación. Las columnas Cuantitativo y Cualitativo, muestra el resultado final de cada criterio.

ID	NOMBRE DEL ESTUDIO	AÑO DE LA PUBLICACIÓN	CEC				CALIDAD	
			1	2	3	4	Cuantitativo	Cualitativo
1	Raspberry pi – Vpn server einrichten (anleitung)	2017	B	B	In	B	3,5	MB
2	Instalación FreePbx en Raspberry PI 3	2014	B	In	B	B	3,5	MB
3	Cambiar IP en Linux por medio de la consola (bash shell)	2013	In	In	B	In	2,5	B
4	Prográmate un "SIMPA" telefónico con una Raspberry Pi y Asterisk	2015	B	In	B	B	3,5	MB
5	The Pi-Point Raspberry Pi Wireless Access Point	2017	B	B	B	B	4	E
6	Raspberry Pi VPN Server: Build Your Own Virtual Private Network	2019	B	B	B	B	4	E
7	MuxComp - A New Architecture to Improve VoIP Bandwidth Utilization	2009	In	In	B	B	3,0	MB
8	Attacking Anonymous Web Browsing at Local Area Networks Through Browsing Dynamics	2011	B	B	In	B	3,5	MB
9	Instalar Asterisk 11.2 certificado en Raspberry pi Model B con Raspbian	2013	In	B	B	B	3,5	MB
10	Arquitectura de Asterisk PBX - VoIP	2014	In	In	N	In	1,5	R

ID	NOMBRE DEL ESTUDIO	AÑO DE LA PUBLICACIÓN	CEC				CALIDAD	
			1	2	3	4	Cuantitativo	Cualitativo
11	**Modeling of packets loss in VoIP Networks and measurement of speech quality**	2008	N	In	B	B	2,5	B
12	**Asterisk server performance under stress test**	2017	In	In	In	B	2,5	B
13	**Secure VoIP architecture based on honeypot technology**	2014	In	B	B	B	3,5	MB
14	**Authentication threats in PSTN-VoIP architecture using multi-service gateways**	2012	In	In	In	B	2,5	B
15	**A mobile VoIP architecture over LTE & WLAN networks**	2010	In	In	B	B	3,0	MB
16	**Chapter 3 - VoIP virtual private networks (VPNs)**	2015	B	In	B	B	3,5	MB
17	**VoIP Security**	2013	In	B	B	In	3,0	MB
Leyenda: B: bueno; In: intermedio; N: no; CEC: Criterio de evaluación de calidad; E: excelente; MB: muy bueno; B: bueno; R: regular; I: incompleto.								

Tabla 2 Resultados de cada estudio primario con respecto a los criterios de evaluación de calidad

Fuente: Propia.

5.1.5. Análisis de resultados

Para realizar la definición de algunos aspectos en el proceso de la revisión de la literatura se tomó en cuenta las palabras claves, los conceptos y el contexto de la investigación para una comprensión más detallada de cada estudio seleccionado, donde cada actividad proporciona la identificación de los siguientes aspectos: (i) escenarios de destino: Arquitectura, Procesos y Metodología; (ii) tipo de investigación: estudio empírico, investigación aplicada, investigación teórica e investigación cualitativa; (iii)

tipo de contribución: metodología, herramienta, enfoque, método. Esta clasificación se puede ver en las imágenes 1, 2 y 3.

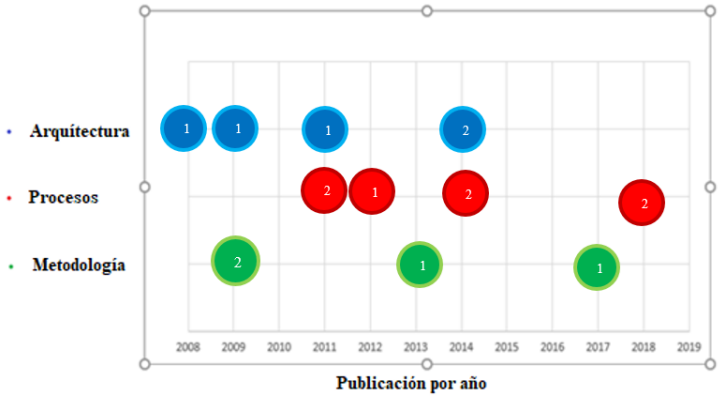


Imagen 1 Diagrama de burbujas de los estudios y escenario por año.

Fuente: Adaptado de **(Alexander Mampotes, 2019)**

Esta sección presenta una evaluación cuantitativa con respecto a los contextos donde se podrá llevar a cabo el proyecto de investigación. La imagen 1 muestra un gráfico de burbujas con la distribución de los escenarios en relación con el año de publicación. Los estudios se agrupan por años, por lo que es posible visualizar arquitecturas, procesos, metodologías similares y recientes a la idea principal del proyecto además de conceptos fundamentales que aportan desarrollo para tener una mayor seguridad de la información y de la comunicación. Se puede observar en la imagen 1 que en la actualidad hay un índice amplio de enfoque de procesos de seguridad que aportaron antecedentes significativos para la documentación del proyecto, en cuanto a la inclusión de diseños y estructuras segura para la implementación del anonimato.

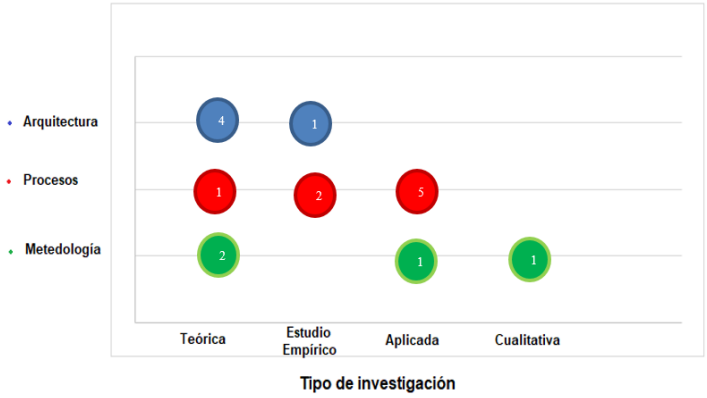


Imagen 2 Diagrama de burbuja de los escenarios y tipo de investigación.

Fuente: Adaptado de **(Alexander Mampotes, 2019)**

La imagen 2 muestra la relación entre el escenario de destino y el tipo de investigación. La mayoría de los estudios primarios seleccionados se analizaron y caracterizaron como investigaciones teóricas. Este resultado apunta a que normalmente los trabajos de investigación se aplican a un área específica, buscando obtener el mejor resultado a través de una causa-efecto y no son estrategias generales que se pueden aplicar a cualquier contexto.

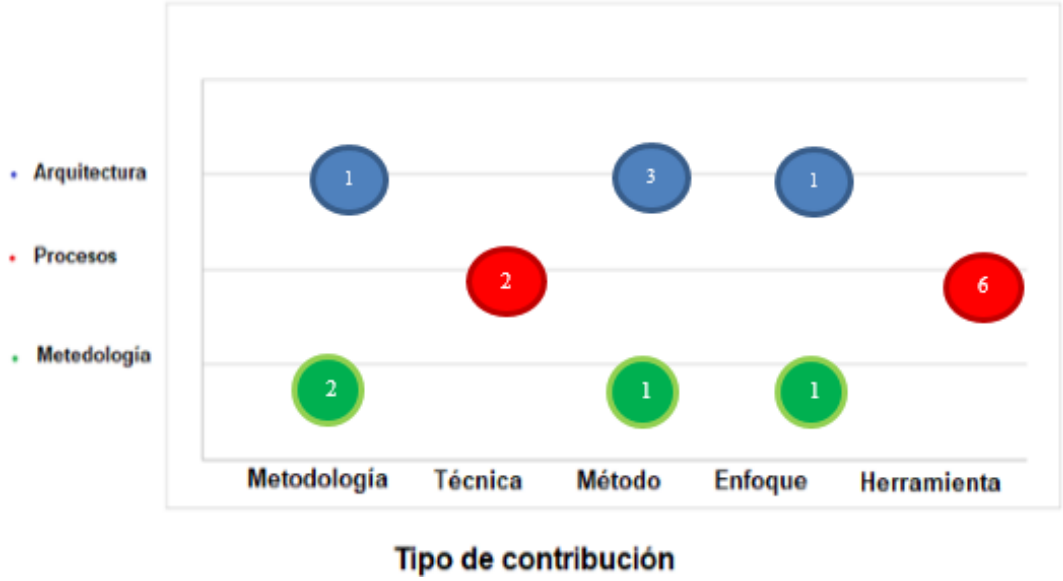


Imagen 3 Diagrama de burbuja de los escenarios y tipo de contribución.

Fuente: Adaptado de **(Alexander Mampotes, 2019)**

Mientras tanto en la imagen 3 muestra la relación entre el escenario y el tipo de contribución. Por lo tanto, se puede apreciar que la mayoría de los estudios aportaron procesos significativos para la implementación y ejecución exitosa del proyecto en cuanto a la selección de los dispositivos y servicios más óptimos a seleccionar para una ejecución adecuada y enfocada a alcanzar el eje central del proyecto.

5.1.6. Amenazas a la validez

Las principales amenazas identificadas que pueden comprometer la validez de los estudios primarios durante el proceso de selección son:

A) **Sesgo de publicación:** se refiere a la posibilidad de que algunos artículos no se seleccionen porque el proceso de búsqueda no arrojó los resultados deseados o

porque la investigación se realizó sobre temas que no encajan en las conferencias, ponencias, revistas y artículos.

B) **Sesgo de selección de estudios primarios**: no se puede garantizar que todos los estudios primarios seleccionados fueron los ideales durante el proceso de búsqueda y evaluación. En este sentido, los criterios de calidad establecidos, así como la asignación de puntajes apuntan a mitigar esta amenaza.

C) Falta de familiaridad con otros campos: se definieron tres cadenas de búsqueda basadas en el conocimiento y experiencia de los autores, pero no se puede evitar por completo que algunos términos definidos en las cadenas de búsqueda tengan sinónimos que no se hayan identificado. Para minimizar esta amenaza se adaptó y se refino cada cadena a las bases de datos bibliográficas hasta que se encontraran los mejores resultados.

D) **Sesgo de selección de los estudios relevantes:** para la selección de artículos relevantes se pudo haber descartado algunos estudios, debido a que el análisis se basó en el título, resumen y palabras claves de los artículos obtenidos en la búsqueda, obviando el material o método del artículo.

5.2. Antecedentes

A continuación, se citan los proyectos ubicados en el ámbito de la seguridad de la información y el anonimato de los cuales fueron referentes para la realización del proyecto.

a) TOR (Anonimo, Tor, s.f.)La red Tor es un grupo de computadoras operadas de forma voluntaria que permite a las personas mejorar su privacidad y seguridad en internet. En lugar de establecer una conexión directa la red Tor se conecta a través de una serie de máquinas intermediarias, lo que permite compartir información en redes públicas sin comprometer tu privacidad. Tor son las siglas en inglés para “The Onion Router”, algo así como “El Enrutador de Cebolla”. Esta forma de navegación aporta a esta investigación una amplia imagen de lo que se quiere lograr con el cambio de IP en diferentes ocasiones mientras se navega por la red, además de la importancia de la navegación anónima y todos los beneficios que se pueden tener al hacerlo de esta manera.

b) NUESTRAS 10 PRINCIPALES VPN (Anonimo, Las mejores VPN , 2019) una VPN o red privada virtual puede enlazar dos o más tipos de dispositivos de forma segura por internet y es un método que garantiza más seguridad y privacidad a la hora de navegar por la internet, conectando al usuario a un servidor localizado en un país diferente al que se encuentre en el momento. El uso de VPN resulta muy útil al momento de conectar uno de los dispositivos y hacer uso del internet en puntos WI-FI públicos como hoteles cafeterías parques etc. Este proporciona un aporte significativo al aplicarlo en la investigación y ejecución de este proyecto puesto que en este artículo se encuentran opciones como las 10 mejores VPN por lo que al hacer uso de ellas permitió desarrollar y garantizar así la eficiencia del objetivo principal, el cual se basa en un servicio de anonimato entre ellos el de la navegación.

c) SERVIDOR VPN RASPBERRY PI CREE SU PROPIA RED PRIVADA VIRTUAL (Gus, 2019) El uso de dispositivos SBC como lo es la Raspberry Pi aporta para la seguridad un menor costo monetario referente al costo industrial de esta tiene en el área laboral aportando en gran medida capacidad para distintos tipos de configuraciones incluida las de la VPN, la cual permite permanecer en línea 24/7 sin consumir una gran cantidad de energía. Sumado a eso es lo suficientemente pequeño y potente como para manejar algunas conexiones a la vez, lo que lo hace ideal para uso privado en el hogar. Esta información aporto a la investigación información necesaria para la óptima selección del dispositivo requerido para la implementación de los servicios de anonimato portable y de bajo costo.

d) PROXYHAM, (Gurierrez, 2015) Es un proyecto basado en la protección de datos a la hora de navegar en una red. Ben Caudill es el creador de este nuevo dispositivo en forma de antena que ayuda a localizar la ubicación de una conexión no segura, este proyecto nos aporta una técnica bastante interesante a la idea que se tiene con la propuesta de investigación pues basados en este trabajo se entrará a mejorar y aumentar la capacidad de la navegación segura en un tráfico de red. Esta información aporto en gran medida conceptos y arquitecturas para tener en cuenta en la implementación de un servicio de navegación anónima, debido a que su objetivo es similar al objetivo general propuesto para este proyecto, el cual es el cambio constante de la IP para una navegación segura.

e) ¡CÓMO SER ANÓNIMO EN WI-FI A MÁS DE 2! ¡5 MILLAS DE DISTANCIA USANDO RASPBERRY PI! (Ninja, 2015) Es un proyecto basado en mantener el anonimato y la seguridad en línea, Próxima funciona, combinado con una suscripción paga para un servicio VPN; además de utilizar dos o más ProxyHam para la seguridad de su red, y el enrutamiento a través de un conmutador de cortafuegos. Mediante el uso del Wi-Fi de "Larga Distancia", así como una conexión de radio de 900 MHz entre el dispositivo y su computadora designada. Ben su creador apunta a tener este dispositivo para transmitir una señal inalámbrica hasta 2.5 millas de distancia de su dirección física. Este proyecto aporta una técnica bastante interesante a la idea que se ha planteado pues basados en esta investigación se pretende mejorar y aumentar la capacidad de la navegación segura.

f) MONTAR UN SERVIDOR CASERO CON RASPBERRY PI (PARTE 3): (Wong, 2013) En este artículo se encuentran los distintos pasos con los que utilizando un sistema operativo raspbian e instalando un servidor DHCP se puede cambiar la IP para que la navegación sea segura; por lo que haciendo uso de la lista de comandos que brinda este artículo y también investigando otros posibles servidores es posible establecer, cuál es la mejor técnica que se pueda implementar sobre un SBC de bajo costo para brindar una navegación 100% segura y conocer de igual manera las posibilidades y alcances que pueda brindar el proyecto frente a la seguridad que debe haber a la hora debe navegar en una red anónimamente.

g) RASPBERRY PI AS A TOR ROUTER AND WEB FILTER (Anonimo, Raspberry Pi Geek, 2013) Este artículo brinda los pasos para instalar en el Raspberry Pi, un proxy como Tor que encaminará todas las conexiones a Internet desde su red doméstica a través de red anónima Tor. Tomando como referencia éste y realizando los distintos pasos que se encuentran en él se obtienen diferentes resultados que aportarían al proyecto conocimiento acerca de cuál puede brindar mejor resultado a nuestro objetivo general.

h) THE PI-POINT RASPBERRY PI WIRELESS ACCESS POINT (Anonimo, Pi Point, 2016) Configuración de una Raspberry Pi como punto de acceso inalámbrico, en este artículo se muestra la Configuración de una Raspberry Pi como punto de acceso inalámbrico. Haciendo uso de los pasos que brinda este artículo y también investigando

otros métodos es posible establecer cuál es la mejor técnica que se puede implementar sobre un SBC de bajo costo en este caso un RASPBERRY-PI para establecer una adecuada instalación y conocer de igual manera las posibilidades y alcances que pueda brindar nuestro proyecto frente a la eficiencia y eficacia que debe haber a la hora de la ejecución del proyecto.

i) CRIPTOANÁLISIS DEL ALGORITMO RSA DE AL MENOS 330 BITS CON DISPOSITIVOS DE BAJO COSTO SBC (Jimenez, 2017) Este articulo habla de cómo actualmente los dispositivos Single Board Computer (SBC), han sido utilizados en muchas ramas de la ciencia, pero no específicamente en el campo del criptoanálisis, y tomando como relevancia componentes como el hardware y el software para realizar distribuciones y llevar a cabo la técnica de criptoanálisis, dado a lo anterior éste artículo busca demostrar ¿Qué tan eficiente en tiempo resulta una técnica de criptoanálisis sobre un SBC que resulte adecuado para quebrantar llaves del algoritmo RSA de al menos 330 bits?, dando como aporte la respuesta a esta pregunta y bajo el análisis de los componentes de hardware y software adecuados para la utilización de SBC de bajo costo se puede destacar según sus cualidades, cual es más apropiado para brindar eficiencia en la elaboración y ejecución de una navegación anónima portable.

j) ASTERISK EN UNA RASPBERRY PI CON RASPBX (Man, 2019) Uno de los múltiples usos que se le puede dar a un Raspberry pi es montar una pequeña central telefónica para uso doméstico o negocio que es basada en Raspbian, la cual es una distribución de Linux en la cual se pueden instalar Asterisk, FreePbx, entre otras, tener un pequeña central telefonía IP diferentes beneficios como la posibilidad de usar nuestro teléfono móvil para hacer y recibir llamadas. Este aporto al proyecto las características y utilidades de la instalación de Asterisk como central para el servicio anónimo de llamadas VoIP.

k) ASTERISK SERVER PERFORMANCE UNDER STREES (Debajyoti Pal, 2017) Los servicios de telefonía VoIP ha ganado una gran popularidad en la actualidad, sin embargo la seguridad y calidad de servicio (QoS) son dos factores que afectan gravemente su rendimiento. Los servidores de protocolo de inicio de sesión (SIP) deben tener suficientes configuraciones de hardware, así como deberían ser correctamente configurado para obtener una buena calidad de voz.

l) SECURE VOIP ARCHITECTURE BASED ON HONEYPOT TECHNOLOGY (Sepideh Poyan Raad, 2014) VoIP está llegando rápidamente al mercado después del establecimiento del Protocolo de Inicio de Sesión como el estándar de facto protocolo de señalización en Internet y multimedia IP Subsistemas (IMS). Básicamente, protocolo de inicio de sesión (SIP) permite dos partes comunicarse entre sí, las principales ventajas de VoIP son la flexibilidad y el bajo costo. Debido a estos beneficios, VoIP obtuvo un rápido crecimiento tanto en el mercado empresarial como en el de consumo.

m) INSTALACION DE FREEPBX EN RASPBERRY PI 3 (Informatico Barcelona, 2014) Esta es una guía de la instalación de FreePbx en un Raspberry Pi 3, en la cual permitirá al cliente realizar llamadas simultaneas desde diferentes extensiones, trasferir la llamada entre extensiones, retener llamadas y por últimos enviar la llamada al buzón de voz.

n) INSTALAR ASTERISK 11.2 CERTIFICADO EN RASPBERRY PI MODEL B CON RASPBIAN (Admin, 2013) Siguiendo los pasos de esta guía se aprenderá a instalar Asterisk en un Raspberry Pi con la última versión de Raspbian, desde el cual una vez instalado permitirá realizar llamadas, enviar mensajes a buzón de voz entre otras cosas.

o) AUTHENTICATION THREATS IN PSTN-VOIP ARCHITECTURE USING MULTI-SERVICE GATEWAYS (Patrik Gallo, 2012) Este artículo propone acerca de las llamadas en internet, las cuales en la última década aumentó su importancia siendo cada vez más confiable y robusta, sin embargo a medida que esta crece los problemas de seguridad se hicieron más notorios. El objetivo de este artículo es proporcionar una descripción general de arquitecturas, así como requisitos de autenticación necesarios para que las llamadas obtengan mejor seguridad.

p) VOIP VIRTUAL PRIVATE NETWORKS (VPNs) (Regis J., 2014) Este artículo habla sobre el uso de VPNs y técnicas de encriptación como posibles medios para brindar seguridad al VoIP. Además, también se discutirá lo que la codificación de datos aportará al rendimiento general y el uso de la infraestructura de clave pública desde una perspectiva general junto al uso de protocolos 802.1X para proporcionar seguridad en la red.

q) VOIP SECURITY (Harsh Kupwade Patil. Dan Wing, 2013) Este artículo habla sobre la importancia de la seguridad en la telefonía VoIP, debido a que en los últimos años se ha utilizado mucho, porque ofrece a sus usuarios ventajas como desvíos de llamadas a larga distancia, comercio electrónico, atención al cliente en línea entre otros. Debido a este creciente uso del VoIP, la seguridad de dichas redes ha ganado mayor prioridad, lo cual en este artículo se revisarán algunos ataques en VoIP y sus correspondientes soluciones.

5.2.1. Aporte de los antecedentes al proyecto

Los antecedentes anteriormente descritos generaron en gran medida un amplio aporte al proyecto, debido a los diferentes análisis que se realizaron frente a los distintos servicios de anonimato, a los dispositivos SBC más adecuados, su manejo y utilidad a la hora de implementarlos en la navegación y llamada previniendo de alguna manera el robo o pérdida de información debido al inadecuado uso que se le da a la misma, y ayudando en gran medida a prever en la ejecución y pruebas de este proyecto posibles errores o fallos que no se conocían antes de realizar la amplia investigación de proyectos y herramientas similares a este.

Todo esto bajo la investigación exhaustiva de las cualidades y características que se encuentran en los diferentes SBC, los cuales cumplen con los principales requisitos para la elaboración e implementación eficiente de los objetivos principales del proyecto.

Dentro de las capacidades a desarrollar sobre el proyecto, existe una fuerte tendencia a los conceptos genéricos de seguridad, integración, escalabilidad y portabilidad. En estos puntos fuertemente aplicados en las actuales tecnologías, pero aún con un gran campo de aplicación y evolución en tecnologías renovadas, como es el caso de este proyecto enfocado en la seguridad en navegación y llamadas VoIP.

5.2.1.1. Seguridad

La seguridad en internet son todas aquellas precauciones que se deben tomar para proteger todos los elementos que hacen parte de la red como infraestructura e información, la más afectada por delincuentes cibernéticos.

El aporte de este proyecto en cuanto a la seguridad informática es encargarse de crear métodos, procedimientos y dispositivos que logren identificar y minimizar

vulnerabilidades en los dispositivos que permiten el transporte de la información a la hora navegar por una red de internet.

5.2.1.2. Integración

Concepto base en el desarrollo de cualquier tecnología que sea sustentable en el tiempo y en el actual periodo tecnológico de desarrollo, todo sistema actual apunta a ello. El significado de la integración es principalmente la capacidad de un sistema de ser evolutivo, flexible, vigente, compatible con su entorno presente y futuro de trabajo. Aplicar el concepto de integración es vital en sistemas de telefonía y navegación por el simple hecho de su trayectoria y tiempo en el caso de la telefonía, por ejemplo: que es una tecnología usada por más de cuatro décadas y por tanto se producen fuertes dependencias frente a las actuales tecnologías. El entender el concepto de integración ayuda a la compresión la cantidad de soluciones que conlleva la navegación y telefonía anónima y segura en beneficio a la disminución de perdida de información y forma de comunicación actual.

5.2.1.3. Escalabilidad

A partir de la integración, consecuentemente se derivan muchos otros conceptos. La escalabilidad es un compromiso del sistema con el crecimiento del sistema implementado, esto apunta a la habilidad para extender el margen de servicios, manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande, sin perder calidad en los servicios ofrecidos pues este es un punto vital por ser dos servicios de uso diario y masivo.

5.2.1.4. Portabilidad

Con base a la definición de portabilidad relacionada al hardware, este proyecto aporta a los usuarios que lo utilicen la facilidad para transportar el dispositivo electrónico en este caso un SBC el cual en su mayoría aporta básicamente una relación al costo, al peso y las dimensiones del equipo un valor bajo en todas estas características con relación a otros dispositivos existentes que aporten seguridad.

5.2.1.5. Redundancia

Es un concepto bastante amplio que abarca prácticamente todas las capas de comunicaciones en redes. La referencia de este concepto apunta a la redundancia física, se habla entonces de respaldo, alta disponibilidad entre otros. Redundancia es una

estrategia que genera un factor conmutativo en el sistema, es decir, se refuerza el sistema con más de un método idéntico o distinto de comunicación al original diseñado en él. El concepto aplica en la telefonía IP en aspectos de seguridad y confiabilidad. Se toma entonces como un punto fuerte dentro del proyecto, al momento de pensar en un diseño de sistema de alta demanda y flexible.

5.3. Marco conceptual

En el presente marco conceptual se hace referencia a trabajos similares que han sido trabajados previamente que están relacionados con el tema de investigación y se mencionan además algunos conceptos que son fundamentales para el tratamiento de este proyecto.

5.3.1. Dispositivos SBC

Los SBC (Single Board Computer) como su nombre lo indica es un sistema computacional en una sola placa (Crespo, 2019) .Este contiene todos los componentes básicos de hardware para llevar a cabo tareas designadas a sistemas tradicionales de computo. Por lo que este trabajo busca analizar las características de estos dispositivos y aprovecharlas para implementar una arquitectura y/o configuración eficiente y un proxy anónimo portable que garantice la eficiencia y efectividad a la hora de navegar seguramente por un tráfico de red además de implementar distintos servicios que amplíen el anonimato al hacer uso y acceder a cualquiera de estos.

5.3.2. Ventajas y desventajas de SBC

No siempre el uso del SBC es la mejor forma de solucionar un problema, pero para la ejecución de este proyecto es lo ideal para hacer una configuración correcta, así mismo se debe tener routers que funcionen como se desea y que el protocolo que se utilice en todos los dispositivos sean 100% compatibles, pero esto por desgracia no siempre es posible y por ese motivo, debido a esto se inicia un estudio investigativo para desarrollar y llevar a cabo un excelente servicio de anonimato todos basados en un SBC de bajo costo adecuado y el más óptimo para cumplir con los objetivos propuestos.

5.3.3. Proxy

Un proxy es un ordenador intermedio que se usa en la comunicación de otros dos. La información (generalmente en Internet) va directamente entre un ordenador y otro. Mediante un proxy, la información va, primero, al ordenador intermedio (proxy), y éste

se lo envía al ordenador de destino, de manera que no existe conexión directa entre el primero y el último. (Certerus, 2019) . Los proxies son utilizados en la mayoría de los casos para realizar prácticas ilegales y estos sirven solo para ocultarnos, debido a esto surge la idea de este proyecto, el cual al desarrollar y crear un proxy que garantice el anonimato de las personas que naveguen a través del dispositivo que será configurado adecamente se evitará el robo de información y el dejar el verdadero rastro de nuestra dirección IP en la internet.

5.3.4. Criptografía

La palabra criptografía (Buba, 2016) es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. El verbo asociado es cifrar. La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para: Modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple y asegurarse de que el receptor pueda descifrarlos.

5.3.5. Técnicas de criptografía

Criptográfica de clave secreta o simétrica: Se caracteriza porque la clave de cifrado y descifrado es la misma. Cada par de usuarios debe tener una clave secreta compartida. Si en la comunicación intervienen más de un usuario es necesario muchas claves secretas distintas. Su método de cifrado es un Cifrado de flujo el proceso de cifrado y descifrado se realiza bit a bit del texto claro al texto cifrado y viceversa. Es decir, el emisor con una clave secreta y un algoritmo determinístico genera una secuencia binaria, cuyos elementos se suman con los correspondientes bits de texto claro, dando lugar a lo bits de texto cifrado; y esta secuencia es la que se envía a través del canal. El proceso contrario sucede cuando la secuencia es la que se envía a través del canal. El proceso contrario sucede con el receptor para descifrar. Y utiliza también un Cifrado de bloques: su funcionamiento es similar al cifrado de flujo, a diferencia que el cifrado y descifrado no se realiza elemento por elemento sino un bloque de bit por bloque de

bit. Las formas de gestionar los bloques de bits ya dependen del modo de cifrado (IBM®, 2014)

Sus algoritmos son: algoritmo determinístico (RKG), algoritmo DES o DEA (modificado del lucifer, algoritmo de cifrado en bloque de 64 bits de longitud y longitud de cave de 56 bits), Algoritmo IDEA también es un algoritmo de bloque donde el cifrado compuesto por bloques de 64 bits al igual que los datos en claro; sin embargo, la clave consta de una longitud de 128 bits. Su concepto es mezclar diferentes operaciones algebraicas. Sus métodos de cifrado son por lo general: ECB, CBC OFB y CFB estos describen el cifrado por bloques

CRIPTOGRAFÍA DE CLAVE PÚBLICA O ASIMÉTRICA: Utiliza dos llaves complementarias. La llave pública y la llave primaria. La clave pública puede ser conocida por todo el mundo, pero la clave privada solo debe ser conocida por su propietario. Lo que se cifra con una clave solo puede ser descifrado con otra clave utiliza funciones unidireccionales (va en una sola dirección y es muy complicado devolverlas), factorización, logaritmo discreto y mochila tramposa Está basada en la utilización de números primos muy grandes.

Sus algoritmos son: el Criptosistema RSA. (Se intenta romperlo a través de factorización de números primos pares) Algoritmo asimétrico ELGAMAL (Anonimo, IBM, 2014)

5.3.6. ¿Qué es un servicio?

Un servicio de TI (tecnología de información) es un conjunto de actividades que buscan responder a las necesidades de un cliente, en este proyecto el servicio que se busca brindar es el mantener el anonimato a la hora de navegar o realizar una llamada entre otros tipos de servicios existentes, todo esto por medio de un cambio de condición en los bienes informáticos, potenciando el valor de éstos y reduciendo el riesgo inherente que puede existir a la hora de navegar y estar expuestos al riesgo de robo de información o ataques informáticos que se puedan encontrar en el sistema. La tecnología permite hacer muchas cosas, pero en última instancia, el rendimiento es lo más importante, por lo cual se busca obtener el dispositivo y la configuración más adecuada para no incumplir con esta condición fundamental (Milenium, 2019).

5.3.7. Tipos de servicios

5.3.7.1. Información que se puede enviar por e-mail

Es importante destacar el buen uso de las cuentas creadas en este servicio de correo electrónico, dado que para garantizar la integridad y disponibilidad de los datos que se manejen a través de éste, se considera de gran importancia para las pequeñas y medianas empresas (Pymes), que se realice un procedimiento seguro atendiendo a la política de seguridad que tengan estas organizaciones y/o la Oficina de Tecnología e Informática. (DIAN, 2018) . Lo que aporta para el proyecto el servicio que puede ser usado por las medianas y pequeñas empresas para la transferencia de información vía email lo que puede exponer en gran medida la perdida de datos vulnerables sin contar con un nivel de seguridad, debido al alto costo del mismo.

5.3.7.2. Servicio de acceso a Internet

Para la Superintendencia y en general para la mayoría de funcionarios, el uso de Internet se ha convertido en una herramienta adicional en el desarrollo de sus actividades diarias y que sirven para el cumplimiento de sus funciones. (TIC, 2018)

5.3.7.3. Servicio de Intranet

Una intranet es un sitio Web interno y privado donde los usuarios pueden acceder ciertos servicios informáticos que no se pueden utilizar a través de Internet, permitiendo múltiples funcionalidades encaminadas a mejorar la eficiencia de búsqueda de información. También se considerada como una red informática privada, o web empresarial que utiliza normas y protocolos de Internet, para permitir a los miembros de una organización comunicarse y colaborar entre sí con mayor eficacia, aumentando de esta manera la productividad. (TIC, 2018) (Superintendencia de industria y comercio)

5.3.8. VPN

Una Virtual Private Network (VPN) en español: Red Privada Virtual (RPV), es una red privada y virtual como su nombre lo indica, por lo tanto, todo el tráfico que pasa por esa red está asegurado y protegido de ojos no deseados. Esto puede ser de mucha utilidad cuando se conectan a una red Wi-Fi pública. Un **VPN (***Virtual Private Network***)** permite crear una conexión segura a otra red a través del Internet. Cuando se conecta cualquier dispositivo a un VPN, este actúa como si estuviese en la misma

red que la que tiene el VPN y todo el tráfico de datos se envía de forma segura a través del VPN. (González, 2014)

5.3.9. ISO 3166

La ISO 3166 es un estándar internacional para los códigos de país y los códigos para sus subdivisiones. Ha sido publicada por la Organización Internacional de Normalización. El propósito de la norma ISO 3166 (ISO, 2013) es el establecimiento de códigos reconocidos de manera internacional para la representación de nombres de países, territorios o áreas de interés geográficos. La ISO 3166 no establece los nombres de los países, sólo los códigos que los representan. La ISO 3166 se ha convertido en uno de los estándares más conocidos y utilizados del mundo para la codificación de los nombres de países. La utilización de un código de letras y números para representar el nombre de un país puede ahorrar tiempo y energía.

Los códigos de los países que se encuentran en la norma ISO 3166-1 son usados por muchas empresas y gobiernos. Todas las empresas postales nacionales utilizan contenedores que llevan el código del país para poder identificarlo. En los pasaportes de lectura mecánica, los códigos ISO 3166-1 se utilizan para establecer la nacionalidad de la persona. El sistema de nombres de dominio de internet utiliza diferentes códigos para definir nombres de dominio de nivel como fr para Francia, au para Australia y br para Brasil. (DESTACADOS, 2016).

5.4. Marco legal

Este proyecto de investigación e implementación del mismo se encuentra enmarcado dentro del ámbito sistémico y de seguridad total, cuyos conceptos están involucrados dentro de un marco legal por la industria y los servicios. Es por esto que existen aspectos legales que deben tomarse en cuenta para no infringir las leyes nacionales, por lo que a continuación se hace referencia de todas las leyes que tienen relación con el tema de la “implementación de los servicios de anonimato portable basado en un SBC de bajo costo.

Para la base legal de este proyecto se tiene en cuenta los principios de la seguridad informática que sustenta la integridad donde se salvaguarda la exactitud y totalidad de la información y los métodos de procedimientos; la disponibilidad de los datos que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos

relacionados con la misma siempre que estos lo requieran; y por último la confidencialidad de los datos la cual está respaldada por la ley estatutaria 1581 del 2012, Habeas Data donde "En Colombia, la aplicación de esta Ley es obligatoria tanto para empresas como para personas naturales, lo cual las obliga a darle un tratamiento seguro y buen manejo a las bases de datos que éstas mantengan o tengan acceso (Auditing, 2017)

Entre otras leyes que se tienen en cuenta para el respaldo de la ejecución de este proyecto están:

5.4.1. Ley 1273 de 2009

"Por medio de la cual se modifica el **código penal,** se crea un nuevo bien jurídico tutelado – denominado "la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (González Cuervo, y otros, 1991)

Esta ley abarca distintos campos que se encuentran presentes en la temática de este proyecto la cual en su capítulo I "**de los atentados contra la confidencialidad, la integridad, y la disponibilidad de los datos y de los sistemas informáticos**" esta regula todas las acciones delictivas que se pueden presentar en cuanto al robo o acceso abusivo a la información personal o a un sistema informático. Con el objetivo principal de este proyecto se puede minimizar en gran cantidad este tipo de hechos delictivos en cuanto al robo de la información que esté disponible en la red cuando se navega puesto que de alguna manera los datos principales de rastreo como lo es en este caso la IP no será la real lo que hace menos vulnerables a las personas que naveguen de manera segura con este sistema y más complicado a los ciberdelincuentes rastrear y capturar dicha información.

5.4.2. Ley 1581 de 2012

Mediante esta ley se expidió el Régimen General de **protección de datos personales**, el cual de conformidad con su artículo 1, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos libertades y garantías constitucionales a que se refiere el **Artículo 15**

de la constitución política; así como el derecho a la información consagrado en el **Artículo 20** de la misma".

Que la ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia. (González Cuervo, y otros, 1991)

5.4.3. Decreto 1377 de 2013

Por el cual se reglamente parcialmente la ley 1581 de 2012, donde El PRESIDENTE DE LA REPUBLICA DE COLOMBIA en uso de sus atribuciones constitucionales u en particular las previstas en el numeral 11 del artículo 189 de la constitución política y en la ley 1581 de 2012 y considerando: que mediante la Ley 1581 de 2012 se expidió el régimen general de protección de datos personales, el cual, de conformidad con su **Artículo 1**°, tiene por objeto: "desarrollar el derecho constitucional que tienen todas a conocer actualizar y rectificar las informaciones que se hayan recogido de ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el **Artículo 15** de la constitución política; así como el derecho a la información consagrado en el **Artículo 20** de la misma.

CAPITULO III

6. METODOLOGÍA

La metodología por implementar en el proyecto planteado es denominada Estudio de caso de YIN (Martínez Carazo, 2006), la cual propone una manera de pensamiento de diseño de investigación aportando cinco componentes importantes y fundamentales para llevar a cabo la ejecución del mismo. Fases que por su criterio para la interpretación de los datos, las preguntas de investigación y las proposiciones teóricas servirán de punto de partida para la recolección de información, desde distintos niveles de análisis para los casos que se presenten y para el análisis posterior, debido a que tanto las preguntas de investigación, como las proposiciones teóricas contienen los constructos (conceptos, dimensiones, factores o variables) de los cuales es necesario obtener información y según esta plantear y establecer la posible solución a la problemática del proyecto y cumplir con los objetivos propuestos anteriormente. (Martínez Carazo, 2006)

Por lo anterior y siguiendo las pautas, la metodología que se estableció en este proyecto se dividió en tres fases como se describirán a continuación. Es de aclarar que cada fase depende de la realización de la fase anterior, buscando así el cumplimiento de los objetivos propuestos.

7. FASE 1: Establecer un análisis comparativo entre los diferentes servicios de anonimato para determinar el más adecuado.

7.1. Recolección de información de los distintos servicios de anonimato:

El presente análisis hace referencia a investigaciones realizadas previamente que están relacionados con la temática de la fase de recolección de información para la selección del servicio más adecuado a implementar en el proyecto y así mismo se mencionan algunos de los conceptos que son fundamentales para el conocimiento de los tipos de servicios.

Con este estudio se logró la recolección de información basada en investigaciones y artículos encontrados en libros y distintos motores de búsqueda que enriquecieron y facilitaron la elección del más adecuado servicio a implementar en este proyecto. Como primera etapa se tuvieron en cuenta unos criterios, los cuales se consideraron necesarios para el éxito de los objetivos principales, a continuación, se muestra dicha selección.

7.1.1. Indicadores de selección

Una de las actividades esenciales durante la fase de recolección y selección del servicio más adecuado en esta investigación, es la definición de los criterios de inclusión y los criterios de exclusión. El objetivo de dichos criterios es ayudar a sesgar la información que en realidad se necesita para lograr así la más acertada selección del servicio para la ejecución del proyecto, en el momento de seleccionar dicho servicio según esto se tuvieron en cuenta características de cada uno y el impacto que estos tienen en la sociedad. Con esto claro se obtuvo la siguiente información y final conclusión de selección:

La red posee una serie de servicios que, en mayor o menor medida, tienen que ver con las funciones de información, comunicación e interacción. Algunos de los servicios disponibles en Internet aparte de la Web, son el acceso remoto a otros ordenadores (a través de telnet o siguiendo el modelo cliente/servidor), la transferencia de ficheros (FTP), el correo electrónico (e-mail), los boletines electrónicos y grupos de noticias (USENET), las listas de distribución, los foros de debate y las conversaciones en línea (chats) y en la actualidad las llamadas VoIP.

Hoy en día existe una amplia gama de instrumentos y contextos para el acceso y la recuperación de documentos, la comunicación y la interacción en el internet es cotidianamente utilizado por todos sin ningún tipo de seguridad. Además, el acceso y la distribución de información ya no se limitan al texto en código ASCII, como en los primeros tiempos de Internet, sino que abarcan todas las morfologías de la información: texto, imagen, audio, vídeo, recursos audiovisuales, etc. En Internet también se puede escuchar la radio, ver la televisión, asistir a un concierto, visitar un museo o jugar a través de la red.

A continuación, se enuncian algunos de los tipos de servicios encontrados entre ellos están:

- Correo electrónico
- Grupos de Noticias (News, Boletines de noticias)
- Listas de distribución

- Foros web
- Transferencia de archivos FTP (File Transmision Protocol)
- Intercambio de archivo P2P
- Archie
- Chats o IRC (Internet Relay Chat), audio y videoconferencia, mensajería instantánea y llamadas telefónicas vía Internet (VoIP)
- Telnet
- Redes sociales o Social networking
- Wikis
- Sindicación de contenidos (RSS, Atom, XML)

Para la selección de los criterios se basó en el análisis detallado y soportado por los antecedentes encontrados del uso de los servicios, los más utilizados mencionados anteriormente, la seguridad que estos brindan y la cantidad de perdida de información que se puede tener al utilizar dicho servicio, esto con el fin de determinar el más adecuado y si están relacionados con los objetivos a aplicar en el proyecto. A partir del estudio que realizaron los autores Peter Lyman y Hal R. Varian de la School of Information Management and Systems de la Universidad de California, Berkeley, las actividades diarias realizadas en Internet son las siguientes (Hal, 2017)

ACTIVIDADES DIARIAS ONLINE		
ACTIVIDAD (NAVEGACION)	**% de aquellos con acceso a Internet**	**Fecha del dato**
Enviar correo	52	marzo-mayo 2017
Obtener noticias	32	marzo-mayo 2017
Usar un buscador para obtener información	29	ene-17
Navegar por la Web para divertirse	23	marzo-mayo 2017
Buscar información sobre algún hobby	21	marzo-mayo 2017
Hacer una búsqueda en Internet para responder a una cuestión específica	19	sep-18
Hacer algún tipo de comprobación para el trabajo	19	nov-18
Comprobar un producto o servicio antes de comprarlo	19	dic-18
Consultar el tiempo	17	marzo-mayo 2018
Enviar un mensaje instantáneo	14	marzo-mayo 2017

Tabla 3 Actividades diarias online de navegación

Fuente: Propia.

Fuente: http://www.hipertexto.info/documentos/serv_internet.htm

Con la Tabla anterior y las estadísticas dadas en la misma se obtuvo el peso de la utilización del servicio de navegación y el amplio uso que esta tiene en la sociedad.

Por ello se procedió a realizar el estudio detallado de la seguridad que existe en cuanto a la navegación en el momento de ser utilizado este servicio y los riesgos que esto puede traer para los usuarios al no tener algún tipo de prevención.

Para detallar la seguridad de este servicio se debe tener claro antes el concepto de la navegación, su funcionamiento, y cómo se transmite la información en Internet, dado que es una tela de araña que no parece tener fin, en la cual unas redes se conectan con otras. En Internet la información se transmite en pequeños trozos llamados “paquetes”; y para intercambiar esta información entre computadores es necesario desarrollar, regular la transmisión de estos paquetes, a este conjunto de normas se le denomina protocolo. Se podría definir el concepto protocolo como el “idioma” que le sirve a los sistemas de Internet para poder comprenderse entre ellos. Uno de los motores de búsqueda más utilizados para hacer uso del servicio de navegación es Google Chrome, Google Chrome es un navegador web desarrollado por Google y compilado con base en componentes de código abierto como el motor de renderizado WebKit y su estructura de desarrollo de aplicaciones (framework), disponible gratuitamente bajo condiciones de servicio específicas. Cuenta con más de 310 millones de usuarios, y dependiendo de la fuente de medición global, puede ser considerado el navegador más usado de Internet variando hasta el segundo puesto, algunas veces logrando la popularidad mundial en la primera posición. Su cuota de mercado se sitúa aproximadamente entre el 17% y 32% para finales de junio de 2018, con particular éxito en la mayoría de países de América Latina donde es el más popular. Actualmente el navegador está disponible para los sistemas operativos de escritorio Microsoft Windows, Mac OS X, Ubuntu, Debian, Fedora, openSUSE, Chrome OS, y en los sistemas operativos móviles Android15 y IOS. Sus características de seguridad incluyen protección integrada contra phishing y malware, cifrado de alta seguridad al navegar, y la capacidad de eliminar fácilmente datos privados, como, por ejemplo: cookies, caché y datos de inicios de sesión.

Lamentablemente son pasos de eliminación ignorados por la gran mayoría de personas a la hora de navegar desde cualquier equipo o Wi-Fi público lo que incrementa la pérdida y rastreo de localización e información personal.

"Según los datos de KSN, las soluciones de Kaspersky Lab neutralizaron 479 528 279 ataques lanzados desde recursos de Internet ubicados en 190 países del mundo y a la fecha se han registrado 79 209 775 direcciones URL únicas que provocaron reacciones del antivirus web. Se neutralizaron intentos de ejecución de programas maliciosos que roban dinero mediante el acceso a cuentas bancarias en los equipos de 288 000 usuarios" (Fedor Sinitsyn, 2017).

El análisis detallado de cada servicio concreto podrá abordarse apoyándose en el estudio de investigación anterior que se ha realizado sobre los servicios básicos más utilizados actualmente y los cuales tienen un nivel de seguridad bajo a la hora de ser manipulados, cuando se habla de los servicios anteriormente se ha ido tratando en general el concepto de servicios de anonimato sin entrar a describir las aplicaciones concretas (correo, transferencia de ficheros, navegación, servidores de información, llamadas, etc.) en esta fase del proyecto se lleva a cabo la recolección de toda la información necesaria para la selección adecuada del servicio en específico a tratar.

Para esto se tuvieron en cuenta criterios fundamentales de cada servicio dándole peso según su importancia obteniendo así un amplio listado del mismo como se muestra en la siguiente investigación realizada, donde se analizaron los diferentes tipos de servicios.

7.2. Analizar los diferentes tipos de servicios de anonimato que se utilizan

Para la conclusión y análisis de la selección del servicio más adecuado se tuvo en cuenta que las inversiones en tecnología para protección en seguridad informática cada día aumentan, y aun así, se presentan resultados como los que se muestran en la encuesta que se visualiza en la siguiente imagen obtenida del sitio web redeszone (Velasco, 2019); el cual menciona que a lo largo de 2017 la empresa kaspersky Labs descubrió alrededor de 66 millones de ataques informáticos contra Smartphone consistían en aplicaciones maliciosas que daban permisos de modificar y extraer información de las víctimas como datos personales o bancarios.

Posteriormente en el año 2018 la misma empresa anteriormente mencionada tuvo registros de 116.5 millones de ataques informáticos basados en software malicioso los cuales en su mayoría fueron los siguientes:

- Trojan-Dropper: Este malware malicioso se encarga de evadir la seguridad del sistema permitiendo instalar un troyano de manera remota.
- Troyanos bancarios: Este malware se utilizan junto con la aplicación anterior para robar datos bancarios de las víctimas.
- RiskTool: Esta aplicación maliciosa son diseñadas para causar daños en los dispositivos tanto a nivel de software como hardware.
- Adware: Esta aplicación maliciosa se encarga de saturar los dispositivos con anuncios y publicidad.

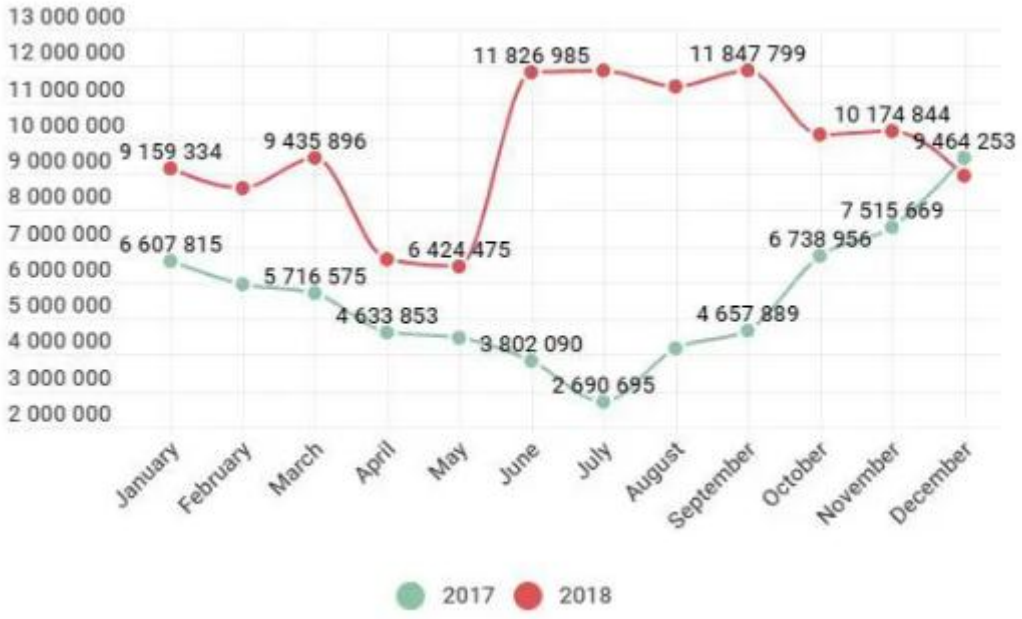


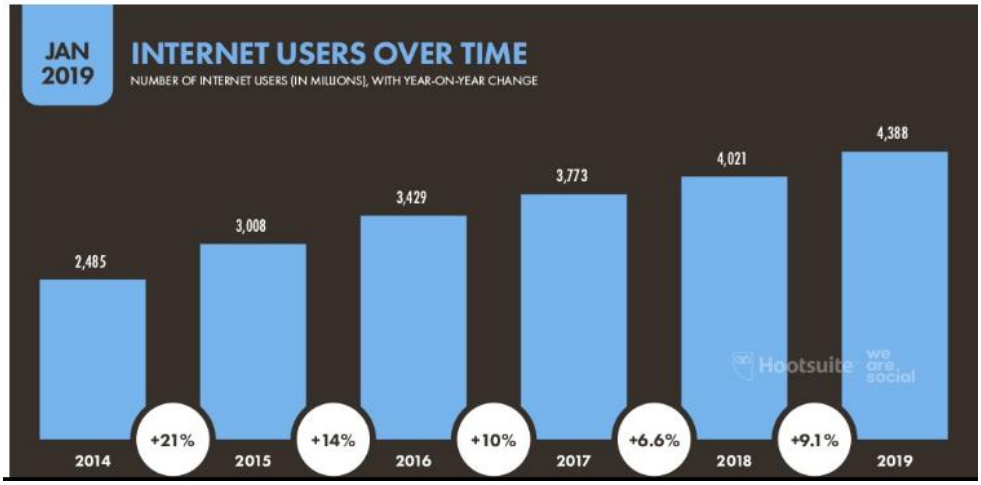
Imagen 4 Estadística de pérdidas de información durante la navegación desde dispositivos móviles. Fuente: https://www.redeszone.net/app/uploads/2019/03/Ataques-inform%C3%A1ticos-m%C3%B3viles-2018.jpg

Teniendo en cuenta la información anteriormente mencionada los riesgos que existen en los servicios que ofrece internet son muchos, por lo cual en el presente proyecto se implementó un servicio de navegación y llamada Voip anónima la cual ayudará a reducir estos ataques de terceros.

Para el análisis de los diferentes tipos de servicios y la selección del más apropiado a implementar y desarrollar en el proyecto se tuvieron en cuenta 3 indicadores los cuales

surgieron de la investigación anteriormente detallada de los riegos que pueden existir en los servicios que ofrece internet y la seguridad que cada uno maneja; además del riesgo que corren las personas y/o empresas que hacen uso de los mismos, este análisis dio como resultado que los servicios más apropiados a utilizar inicialmente son la **navegación** y la **llamada VoIP** por los siguientes valores obtenidos:

- **Frecuencia de uso:** las veces en que un usuario asiste al servicio es un indicador bastante importante por lo que obtuvo un 42% a partir del estudio previo además de las estadísticas presentadas a continuación de la frecuencia de uso de cada servicio por empresas y personas del común planteada en la estadística dadas por la cual muestran las amenazas de exposición a la red son relativas al tiempo en el que se esté usando el servicio conectado a internet (GALEANO, 2019) , como se muestra en la siguiente gráfica.



Gráfica 1 Estadística de frecuencia de uso de internet

Fuente: https://marketing4ecommerce.net/usuarios-internet-mundo/

- **Nivel seguridad:** Básicamente, se pueden agrupar las amenazas de las cuales se encuentran expuestas la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y Actos maliciosos o malintencionados; algunas de estas amenazas son: Espionaje, Virus informáticos o código malicioso, Robo de Información, Alteración de la Información, Divulgación de Información, Fraudes basados en el uso de computadores por lo que la seguridad pasa a ser un punto bastante importante para ofrecer al servicio

seleccionado un mejor nivel de seguridad por esto obtuvo un porcentaje del 22% obteniendo este valor de la información suministrada por la revista marketing4ecommerce (GALEANO, 2019) y según estadísticas de robo y pérdida de información en empresas y personas que no cuentan con un adecuado y preventivo manejo de la red.

8. FASE 2: Categorizar por medio de un análisis comparativo el SBC adecuado, para la implementación del servicio de anonimato portable.

8.1. Recolección de información de un SBC de bajo costo.

Las computadoras de una sola placa están diseñadas de manera diferente a las computadoras personales o de escritorio estándar, ya que son completamente independientes lo que es apropiado para la portabilidad que se requiere tener el proyecto. A menudo utilizan una amplia gama de microprocesadores y tienen una mayor densidad para los circuitos integrados utilizados. También están disponibles con una amplia gama de capacidades, aunque algunas son lentas y limitadas en comparación con las computadoras personales, ya que se utilizan para controlar procesos simples.

Existen muchas ventajas al usar computadoras de una sola placa. Sus características están bien integradas, debido a que casi todo es nativo de la máquina. A menudo se proporcionan ranuras para la interconexión, y hay configuraciones de ranura y placas posteriores disponibles. Los SBC se pueden producir fácilmente y se comercializan rápidamente en comparación con las computadoras personales o portátiles lo que aporta en gran medida el principal objetivo de brindar un dispositivo de calidad para la implementación de un servicio de anonimato que además de ser portable que es una de las principales características de estos dispositivos también cuente con un costo bajo en cuanto a su valor en el mercado. Los SBC Son dispositivos más livianos, compactos, más confiables y mucho más eficientes que las computadoras con múltiples placas.

El análisis comparativo de los diferentes SBC fue de gran importancia para la implementación de los dos servicios seleccionados en la fase 1 (Navegación Anónima, llamada). Esta investigación contó con datos e información que sirvieron para conocer y valorar las características indicadas con las cuales se determinó cual fue el dispositivo más adecuado para el proyecto y su futura elaboración.

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
1	**Orange Pi Plus 2E**	-	H3 Quad-core Cortex-A7 H.265/HEVC 4K	·Mali400MP2 GPU @600MHz	2GB DDR3 (shared with GPU)	Android, Ubuntu, Debian, Raspbian Image	DC input can supply power, but USB OTG input don't supply power	Aprox. 270.000 COP
2	**Rasperry Pi 2 Model B**	Broadcom BCM2835	Quad-Core Cortex A7 a 900MHZ	Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0	512 MB LPDDR SDRAM 400 MHz	GNU/LINUX, Windows 10	5V	Aprox. 121.629 COP
3	**Rasperry Pi 3**	Broadcom BCM2837	4× ARM Cortex-A53, 1.2GHz	Broadcom VideoCore IV 3D graphics core	1GB	Linux	5V	Aprox. 220.000 COP
4	**Raspberry Pi Model B**	Broadcom BCM2835	700 MHz ARM1176JZF-S core (ARM11 family)	·Supports OpenGL ES 2.0	256 MB (shared with GPU)	Debian GNU/Linux, Fedora, Arch Linux ARM	5V/2A	Aprox. 195.000 COP
5	**Mele A1000**	Allwinner A10	1GHz+ Cortex-A8	MALI400MP OpenGL ES 2.0	512MB DDR3	Android 2.3,ubuntu, Debian, puppy, android ics	5V	Aprox. 170.000 COP
6	**Rhombus-Tech A10 EOMA-68**	Allwinner A10	1.2ghz Cortex A8 ARM Core	MALI400MP OpenGL ES 2.0 GPU	1gb	-	6V	Aprox. 177.500 COP
7	**Gooseberry board**	A10	1 Ghz - 1.5 Ghz 1.2 Ghz highest stable	Mali 400 MHz	512MB	Android 2.3, ubuntu, Debian, puppy, android ics	7V	Aprox. 215.000 COP
8	**Pineriver H24/MiniX S**	A10	1.2GHz	Mali400	512MB	Android 2.3/4.0, Puppy Linux, Ubuntu		Aprox 80.720 COP
9	**Smallart UHOST**	Allwinner A10	1GHz Cortex-A8	Mali400	1 GB	android 4.0, Puppy Linux, Ubuntu	5V/1C	Aprox 140.100 COP
10	**A13-OLinuXino**	Allwinner A13	1GHz A13 Cortex A8	Mali400	512 MB	Linux	10V	Aprox 130.900 COP
11	**VIA APC**	VIA WonderMedia 8750	800 MHz ARM11	OpenGL ES 2.0	DDR3 512MB	Android 2.3	11V	Aprox 150.700 COP

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
12	**BeagleBoard Rev. C4**	TI OMAP3530	720 MHz ARM Cortex-A8	PowerVR SGX	256 MB	Android, Ubuntu, Fedora, ArchLinux, Gentoo	12V	Aprox 115.000 COP
N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
13	**BeagleBoard-xM**	TI DM3730	1 GHz Cortex-A8	PowerVR SGX	512 MB	Angstrom, Android, Ubuntu, Fedora, ArchLinux, Gentoo	13V	Aprox 160.700 COP
14	**BeagleBone**	TI AM3359 Sitara	500MHZ-USB Powered 720MHZ-DC Powered Cortex A8	SGX530	256MB DDR2 (128MB Optional)	Angstrom, Debian, Ubuntu, Fedora, ArchLinux, Gentoo, Sabayon	14V	Aprox 595.700 COP
15	**PandaBoard**	OMAP4430	1GHz Dual-core ARM Cortex-A9 MPCore	PowerVR SGX540	1GB DDR2	Ubuntu, Ångström, Android,Supported by Linaro	15V	Aprox 660.100 COP
16	**PandaBoard ES**	OMAP4460	1.2 GHz Dual-core ARM Cortex-A9 MPCore	PowerVR SGX540	1GB DDR2	Ubuntu, Ångström, Android,Supported by Linaro	16V	Aprox 440.450 COP
17	**Cotton Candy**	Samsung Exynos 4210	1.2 GHz dual-core ARM Cortex-A9	quad-core 200 MHz Mali-400 MP	1 GB	Android, Ubuntu	17V	Aprox 90.000 COP
18	**CuBox**	Marvell Armada 510 (88AP510)	800 MHz ARMv7	Vivante GC600	1 GB DDR3-800MHz	Ubuntu 10.04, Android 2.2, Linux kernel 2.6.x or later Android 2.2.x and later	5V/5A	Aprox 270.000 COP
19	**Hawkboard**	TI OMAP-L138	300-MHz ARM926EJ	-	128 MByte	Ubuntu, Fedora, Impactlinux	5V/1A	Aprox 430.000 COP
20	**IGEP v2**	Ti DM3730	ARM Cortex A8 1GHz	SGX530 @ 200 MHz	512 M	Android, Angstrom, Ubuntu	5V/3A	Aprox 530.000 COP
21	**IGEP COM Proton**	DM3730 (optional OMAP3530)	1GHZ ARM CORTEX A8 (720Mhz for OMAP3530)	SGX 530 (200Mhz) (110Mhz for OMAP3530)	512 MBytes	Android, Angstrom, Ubuntu	5V/3C	Aprox 540.100 COP

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
22	**IGEP COM Module**	DM3730 (optional OMAP3530) A	1GHZ ARM CORTEX A8 (720Mhz for OMAP3530)	SGX 530 (200Mhz) (110Mhz for OMAP3530)	512 MBytes	Android, Angstrom, Ubuntu, ..	5Vcc / 1.3A	Aprox 325.200 COP
N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
23	**Gumstix Overo series**	AM3703, DM3730, OMAP3503, OMAP3530	ARM Cortex-A8 Up to 1GHz	-	512MB or 256MB	Ubuntu, Android, ..	USB Powered	Aprox 555.450 COP
24	**Origen Board**	Exynos4210	1.2GHz Dual Core Cortex-A9	Mali400 MP4	DDR3 1GB	Android, Ubuntu, ..	USB Powered	Aprox 282.600 COP
25	**Nimbus**	Marvel Kirkwood 6281	1.2 GHz	-	512MB	Debian	5V	Aprox 380.900 COP
26	**Stratus**	Marvel Kirkwood 6281	1.2 GHz	-	512MB	Debian	5V 2A	Aprox 290.550 COP
27	**SheevaPlug dev kit (Basic)**	Marvel Kirkwood 6281	1.2 GHz ARM9E	-	512 MB	Ubuntu/Debian	AC 100 - 240VAC, 13W	Aprox 300.550 COP
28	**GuruPlug Standard**	Marvel Kirkwood 6281	1.2 GHz	-	512 MB	Ubuntu/Debian	100-240VAC, 5V/3.0A Max	Aprox 580.200 COP
29	**GuruPlug Display**	Marvell ARMADA 168	800MHz	-	512MB	Ubuntu/Debian	100-240VAC, 5V/3.0A Max	Aprox 429.200 COP
30	**DreamPlug**	Marvel Kirkwood 6281	1.2 GHz	-	512MB	Ubuntu/Debian	5V/3A	Aprox 715.900 COP
31	**D2Plug**	Marvell PXA510	800MHz	-	1GB	Ubuntu/Debian	100-240VAC, 5V/3.0A Max	Aprox 619.900 COP
32	**Trim-Slice series**	NVIDIA Tegra 2	1 GHz	-	1 GB DDR2-667	Android, Ubuntu, ..	12V DC (8V-16V tolerant)	Aprox 468.450 COP

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
33	**Snowball**	STEricsson Nova A9500	1GHz Dual Cortex A9	Mali 400	1GByte	Linaro (Ubuntu, Android)	DC IN +5V	Aprox 421.452 COP
34	**i.MX53 Quick Start Board**	Freescale i.MX535	1GHz	-	1GB of DDR3	Linaro (Ubuntu, Android)	5V, 2A	Aprox 370.950 COP
35	**Genesi Efika MX Smarttop**	Freescale i.MX515	ARM Cortex-A8 800MHz	-	512MB	Ubuntu	-	Aprox 400.600 COP
36	**FriendlyARM Mini 210s**	Samsung S5PV210	1 GHz Cortex-A8	PowerVR SGX540	512 MB	Linux-2.6.35, Android 2.3, 4.0, WindowsCE 6.0	5V	Aprox 550.000 COP
37	**Embest DevKit8600**	TI's Sitara AM3359	720MHz ARM Cortex-A8	SGX530	512MBytes	Linux 3.1.0, Android 2.3 and WinCE 7	12V	Aprox 280.600 COP
38	**Embest SBC8018**	TI AM1808	375MHz ARM926EJ-S	128MByte	128MByte	Linux2.6.33 and WinCE 6.0	5V	Aprox 290.100 COP
39	**Embest SBC8530**	TI DM3730	1GHz ARM Cortex-A8		512MByte	Linux2.6.32, Android 2.2 and WinCE 6.0	5V	Aprox 580.200 COP
40	**Embest DevKit8500D**	DM3730	8 1GHz ARM Cortex-A8	-	512MB	Linux2.6.32, Android 2.2 and WinCE 6.0.15	5V	Aprox 370.200 COP
41	**TechNexion Infernopack**	TI OMAP3530	600Mhz	POWERVR SGX 530	128 MB	Linux 2.6.x, Windows CE 6.0 BSP or Android	5VDC	Aprox 735.150 COP
42	**TechNexion Thunderpack**	TI OMAP3530	600Mhz	POWERVR SGX 530	256 MB	Linux 2.6.x, Windows CE 6.0 BSP or Android	5VDC	Aprox 1.100.500 COP
43	**VIA ARTiGO A1200 Fanless**	Chipset VIA VX900	1.0GHz x86 VIA Eden X2 L2 Cache 2MB	VIA Chrome 9	Up to 4GB DDR3	"ordinary" X86 OS	DC 12V	Aprox 980.000 COP
44	**VIA ARTiGO A1150**	Chipset VIA VX900H	1.0GHz VIA Eden X2	VIA Chrome 9	Up to 4GB DDR3	"ordinary" X86 OS	DC 12V	Aprox 223.000 COP

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
45	**DMP - eBox 3350MX**	-	1Ghz Vortex86MX (i586, no CMOV)	-	512MB	i586 compatible OS	5V/2A	Aprox 580.000 COP
46	**DMP - eBox 3310MX-AP**	-	933MHz Vortex86MX+	-	1GB DDR2	i586 compatible OS	8V/15V	Aprox 150.000 COP
47	**Udoo Basic Dual**	Freescale i.MX 6 ARM	Cortex-A9 Dual core 1GHz	Vivante GC 880 + Vivante GC 320	1GB DDR3	Linux/Android/Windows 10	6-15V	Aprox. 285.000 COP
48	**Udoo Dual**	Freescale i.MX 6 ARM	Cortex-A9 Dual core 1GHz	Vivante GC 880 + Vivante GC 320	1GB DDR3	Linux/Android/Windows 10	6-15V	Aprox. 340.000 COP
49	**Udoo**	Freescale i.MX 6 ARM	Cortex-A9 Dual core 1GHz	Vivante GC 2000 + Vivante GC 355 + Vivante GC 320	1GB DDR4	Linux/Android/Windows 11	6-15V	Aprox. 400.000 COP
50	**LattePanda**	Intel Cherry Trail Z8300	Intel Atom Quad Core 1.8GHz	Intel HD Graphics	2 GB DDR3L	Windows 10	5V/2A	Aprox. 350.000 COP

Tabla 4 Características de los dispositivos SBC's.

Fuente: Propia.

Las preguntas determinantes para elegir el SBC que se va a usar son:

- Frecuencia de CPU: ¿Cuál es la frecuencia de CPU del SBC?
- RAM: ¿Cuál es la cantidad de RAM del SBC?
- WI-FI: ¿El SBC permite conexión inalámbrica?
- SO: ¿Qué sistemas operativos libres soporta el SBC?
- Power source: ¿Cuál es la fuente de alimentación que necesita el dispositivo SBC para su funcionamiento?
- Costo del SBC: ¿Cuál es el precio del SBC?

Los indicadores que se tuvieron en cuenta para la realización de la tabla anterior fueron la Frecuencia de la CPU, RAM, Puerto USB, WI-FI, Sistema operativo, Power source, Precio del SBC, estos debido a que para la ejecución del proyecto se requiere de:

a) Para **la frecuencia de CPU**, se estableció un 10% del total de los indicadores, debido a que para la ejecución del servicio de navegación anónima se necesitará velocidad, para reducir tiempo como se justificó en el proyecto. Para ello la frecuencia será tomada en Megabytes.

b) **La RAM** representó un porcentaje de 5%, dado que la mayoría de los SBC cuentan con la RAM suficiente para cargar un sistema operativo. Este indicador se tomará en GB (Gigabyte) para ser evaluado.

c) **Los puertos USB** establecieron un porcentaje 15%, puesto que para la arquitectura establecida se necesitan de antenas adicionales para el cumplimiento del objetivo del proyecto, además que es posible utilizar periféricos como teclado y mouse para el manejo del SBC.

d) **El WI-FI** integrado determinó el 15% de los indicadores, porque es necesario hacer uso del servicio WI-FI para la conexión a internet y la realización de la navegación y la llamada.

e) **El precio del SBC** representó el 45%, dado a que se requiere un SBC de un precio bajo, en vista de que es enfoque importante en el proyecto.

f) **El sistema operativo** estableció el 5% de los indicadores, debido a que se va a utilizar una instalación basada en raspbian, además de ser de uso libre lo cual aporta una reducción de costos para uno de los indicadores de más peso el cual está representado en el precio total del proyecto.

g) **La Conexión por Ethernet** se estableció el 5% de los indicadores, porque es la conexión a internet es necesaria y una buena opción es a conexión por cableado Ethernet.

Según lo anteriormente planteado y como conclusión de los porcentajes obtenidos en cada indicador se procede a desarrollar es segundo ítem de la fase 2 realizando un análisis del SBC adecuado, para la implementación del servicio de anonimato portable.

METRICAS PARA LA SELECCIÓN DEL SBC DE BAJO COSTO QUE SE UTILIZARA EN EL PROYECTO

Una vez determinados los factores que se necesitan para formalizar una métrica de los 50 SBC’s encontrados en el mercado, para identificar el más adecuado se efectuó el respectivo cálculo para obtener una tabla normalizada selección para el SBC, todo lo

anterior se realizará de acuerdo a las fórmulas obtenidas por el libro Introducción a la minería de datos (Jimenez Anderson, 2017) .

Fórmula empleada para normalización de CPU, Costo, RAM, Puerto USB, Wi-fi, Ethernet y SO.

$$V' = \frac{V - min_A}{max_A - min_A} * (newmax_A - newmin_A) + \ newmin_A$$

Para ello se procedió a enumerar (transformar valores categóricos en numéricos) y normalizar la tabla de datos de los SBC´s, para lo cual se tomó una escala entre 1 y 5. Para los indicadores se aplicó la fórmula de normalización, con los siguientes valores de mínimo y máximo:

Frecuencia de CPU

- Valor máximo: 1,8GHz – En la escala de normalización corresponde a 5
- Valor mínimo: 0,3GHz - En la escala de normalización corresponde a 1

Costo del SBC

- Valor máximo: 1’100.500 COP – En la escala de normalización corresponde a 5
- Valor mínimo: 80.720 COP - En la escala de normalización corresponde a 1

RAM

- Valor máximo: 4 Gb – En la escala de normalización corresponde a 5
- Valor mínimo: 0,128 - En la escala de normalización corresponde a 1

Puerto USB

- **SI** posee puerto(s) USB en la escala de normalización corresponde a 5
- **NO** posee puerto(s) USB en la escala de normalización corresponde a 1

Wi-fi

- **SI** posee conexión a internet inalámbrica en la escala de normalización corresponde a 5
- **NO** posee conexión a internet inalámbrica en la escala de normalización corresponde a 1 **Ethernet**
- **SI** posee puerto para conexión a internet mediante cableado en la escala de normalización corresponde a 5

- **NO** posee puerto para conexión a internet mediante cableado en la escala de normalización corresponde a 1

Sistema Operativo.

- **SI** se puede instalar un sistema operativo que se adapte a lo que requerimos en la escala de normalización corresponde a 5
- **NO** se puede instalar un sistema operativo que se adapte a lo que requerimos en la escala de normalización corresponde a 1

Aplicando las métricas al listado de 50 SBC's encontrados se facilita la selección del SBC más adecuado para el proyecto.

NOMBRE DEL SBC	CPU	RAM	USB	ETHERNET	WI-FI	SO	PRECIO
Orange Pi Plus 2E	0.6 GHz	2GB	SI	SI	SI	SI	Aprox. 270.000 COP
Raspberry Pi 2 Model B	0.9 GHZ	0.512GB	SI	SI	SI	SI	Aprox. 121.629 COP
RaspBerry Pi 3	1.2 GHz	1GB	SI	SI	SI	SI	Aprox. 220.000 COP
Raspberry Pi Model B	0.7 GHz	0.256GB	SI	SI	SI	SI	Aprox. 195.000 COP
Mele A1000	1 GHz	0.512GB	SI	SI	SI	SI	Aprox. 170.000 COP
Rhombus-Tech A10 EOMA-68	1.2 GHz	1GB	SI	SI	SI	NO	Aprox. 177.500 COP
Gooseberry board	1.5GHz	0.512GB	SI	NO	SI	SI	Aprox. 215.000 COP
Pineriver H24/MiniX S	1.2 GHz	0.512GB	SI	NO	SI	SI	Aprox 80.720 COP
Smallart UHOST	1 GHz	1GB	SI	NO	SI	SI	Aprox 140.100 COP
VIA APC	0.8 GHz	0.512GB	SI	SI	NO	SI	Aprox 150.700 COP
BeagleBoard Rev. C4	0.72 GHz	0.256GB	SI	SI	NO	SI	Aprox 115.000 COP
BeagleBoard-xM	1 GHz	0.512GB	SI	SI	NO	SI	Aprox 160.700 COP
BeagleBone	0.72 GHz	0.256GB	SI	SI	NO	SI	Aprox 595.700 COP
PandaBoard	1 GHz	1GB	SI	SI	NO	SI	Aprox 660.100 COP
PandaBoard ES	1.2 GHz	1GB	SI	SI	NO	SI	Aprox 440.450 COP

NOMBRE DEL SBC	CPU	RAM	USB	ETHERNET	WI-FI	SO	PRECIO
Cotton Candy	1.2 GHz	1GB	SI	SI	SI	SI	Aprox 90.000 COP
CuBox	0.8 GHz	1GB	SI	SI	SI	SI	Aprox 270.000 COP
Hawkboard	0.3 GHz	0.128GB	SI	SI	NO	SI	Aprox 430.000 COP
IGEP v2	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 530.000 COP
IGEP COM Proton	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 540.100 COP
IGEP COM Module	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 325.200 COP
Gumstix Overo series	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 555.450 COP
Origen Board	1.2GHz	1GB	SI	SI	SI	SI	Aprox 282.600 COP
Nimbus	1.2 GHz	0.512GB	SI	SI	SI	SI	Aprox 380.900 COP
Stratus	1.2 GHz	0.512GB	SI	SI	SI	SI	Aprox 290.550 COP
SheevaPlug dev kit (Basic)	1.2 GHz	0.512GB	SI	SI	NO	SI	Aprox 300.550 COP
GuruPlug Standard	1.2 GHz	0.512GB	SI	NO	SI	SI	Aprox 580.200 COP
GuruPlug Display	0.8 GHz	0.512GB	SI	SI	NO	SI	Aprox 429.200 COP
DreamPlug	1.2 GHz	0.512GB	SI	SI	NO	SI	Aprox 715.900 COP
D2Plug	0.8 GHz	1GB	SI	SI	SI	SI	Aprox 619.900 COP
Trim-Slice series	1 GHz	1GB	SI	SI	NO	SI	Aprox 468.450 COP
Snowball	1 GHz	1GB	SI	SI	SI	SI	Aprox 421.452 COP
i.MX53 Quick Start Board	1 GHz	1GB	SI	SI	NO	SI	Aprox 370.950 COP
Genesi Efika MX Smarttop	0.8 GHz	0.512GB	SI	SI	NO	SI	Aprox 400.600 COP
FriendlyARM Mini 210s	1 GHz	0.512GB	SI	SI	NO	SI	Aprox 550.000 COP
Embest SBC8018	0.375GHz	0.128GB	SI	SI	SI	SI	Aprox 290.100 COP

NOMBRE DEL SBC	CPU	RAM	USB	ETHERNET	WI-FI	SO	PRECIO
Embest SBC8530	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 580.200 COP
Embest DevKit8500D	1 GHz	0.512GB	SI	SI	SI	SI	Aprox 370.200 COP
TechNexion Infernopack	0.6 GHz	0.128GB	SI	NO	SI	SI	Aprox 735.150 COP
TechNexion Thunderpack	0.6 GHz	0.256GB	SI	NO	SI	SI	Aprox 1.100.500 COP
VIA ARTiGO A1200 Fanless	1 GHz	4GB	SI	SI	NO	SI	Aprox 980.000 COP
VIA ARTiGO A1150	1 GHz	4GB	SI	SI	NO	SI	Aprox 223.000 COP
DMP - eBox 3350MX	1 GHz	0.512GB	SI	NO	NO	SI	Aprox 580.000 COP
DMP - eBox 3310MX-AP	0.93 GHz	1GB	SI	SI	SI	SI	Aprox 150.000 COP
Udoo Basic Dual	1 GHz	1 GB	SI	NO	NO	SI	Aprox. 285.000 COP
Udoo Dual	1 GHz	1GB	SI	SI	SI	SI	Aprox. 340.000 COP
Udoo	1 GHz	1GB	SI	SI	SI	SI	Aprox. 400.000 COP
LattePanda	1.8 GHz	2GB	SI	SI	SI	SI	Aprox. 350.000 COP

Tabla 5 Aportes característicos de los SBC's.

Fuente: Propia.

Una vez establecidos los componentes necesarios para efectuar una métrica se efectuó el respectico cálculo para obtener una tabla normalizada. De lo anterior realizado se obtuvieron los siguientes puntajes dentro de la tabla normalizada:

Fórmula empleada para normalización de CPU, Costo, RAM, Puerto USB, Wi-fi, Ethernet y SO.

$$V' = \frac{V - min_A}{max_A - min_A} * (newmax_A - newmin_A) + newmin_A$$

NOMBRE DEL SBC	CPU (10%)	RAM (5%)	USB (15%)	ETHERNET (5%)	WI-FI (15%)	OS (5%)	PRECIO (45%)	PUNTAJE (1 – 5)
Orange Pi Plus 2E	1,8	2,933	5	5	5	5	2,74	3,55965
Nimbus	3,4	1,4	5	5	5	5	1,17	2,9365
Genesi Efika MX Smarttop	2,33	1,4	5	5	1	5	2,25	2,7155
Raspberry Pi 2 Model B	2,12	1,9	5	5	5	5	2,35	3,3945
Mele A1000	2,87	1,4	5	5	5	5	1,35	2,9645
Rhombus-Tech A10 EOMA-68	3,4	1,9	5	5	5	1	1,37	2,8515
Gooseberry board	4,2	1,4	5	1	5	5	1,52	2,29
Pineriver H24/MiniX S	3,4	1,4	5	1	5	5	1	2,21
Smallart UHOST	2,87	1,9	5	1	5	5	1,23	2,182
A13-OLinuXino	2,87	1,4	5	1	5	5	1,19	2,157
VIA APC	2,33	1,4	5	5	1	5	1,27	1,703
BeagleBoard Rev. C4	2,12	1,13	5	5	1	5	1,13	1,6685
BeagleBoard-xM	2,87	1,4	5	5	1	5	1,31	1,757
BeagleBone	2,12	1,13	5	5	1	5	3	1,6685
PandaBoard	2,87	1,9	5	5	1	5	3,2	1,782
PandaBoard ES	3,4	1,9	5	5	1	5	2,4	1,835
Cotton Candy	3,4	1,9	5	5	5	5	1,03	2,435
CuBox	2,33	1,9	5	5	5	5	1,74	3,111
Hawkboard	1	1	5	5	1	5	2,37	2,6165
IGEP v2	2,2	1,4	5	5	5	5	2,76	3
IGEP COM Proton	2,2	1,4	5	5	5	5	2,8	2,357
IGEP COM Module	2,2	1,4	5	5	5	5	1,95	3,12
Origen Board	3,4	1,9	5	5	5	5	1,79	3,2405

NOMBRE DEL SBC	CPU (10%)	RAM (5%)	USB (15%)	ETHERNET (5%)	WI-FI (15%)	OS (5%)	PRECIO (45%)	PUNTAJE (1 – 5)
Raspberry Pi 2 Model B	2,12	1,9	5	5	5	5	2	3,207
Stratus	3,4	1,4	5	5	5	5	1,82	3,229
SheevaPlug dev kit (Basic)	3,4	1,4	5	5	1	5	1,86	2,647
GuruPlug Standard	3,4	1,4	5	1	5	5	1,95	3,0875
GuruPlug Display	2,33	1,4	5	5	1	5	2,36	2,765
DreamPlug	3,4	1,4	5	5	1	5	2,49	2,9305
D2Plug	2,33	1,9	5	5	5	5	2,11	3,2775
Trim-Slice series	2,87	1,9	5	5	1	5	2,52	2,916
Snowball	2,2	1,9	5	5	5	5	2,33	3,265
i.MX53 Quick Start Board	2,87	1,9	5	5	1	5	2,13	2,7405
RaspBerry Pi 3 Model B +	3,4	1,9	5	5	5	5	2,54	3,578
FriendlyARM Mini 210	2,87	1,4	5	5	1	5	2,84	3,035
Embest DevKit8600	2,12	1,4	5	5	5	5	1,78	3,083
Embest SBC8018	1,2	1	5	5	5	5	1,82	2,989
Embest SBC8530	2,87	1,4	5	5	5	5	2,95	3,3845
Embest DevKit8500D	2,87	1,4	5	5	5	5	2,13	3,3155
TechNexion Infernopack	1,8	1	5	1	5	5	2,56	3,182
TechNexion Thunderpack	1,8	1,13	5	1	5	5	3	3,3865
VIA ARTiGO A1200 Fanless	2,87	5	5	1	1	5	2,52	2,871
VIA ARTiGO A1150	2,87	5	5	5	1	5	1,55	2,6345
DMP - eBox 3350MX	2,87	1,4	5	1	1	5	2,95	2,8845
DMP - eBox 3310MX-AP	2,68	1,9	5	5	5	5	1,27	2,9345
Udoo Basic Dual	2,87	1,9	5	1	1	5	1,8	2,392
Udoo	2,87	1,9	5	1	5	5	2,25	3,3845
LattePanda	5	2,933	5	5	1	5	2,05	2,96915

Tabla 6 Información con de los datos normalizados.
Fuente: Propia.

Como se ve reflejado en la tabla anterior, se notan 4 SBC's con buenas características las cuales se adaptan mejor al proyecto, debido a las métricas planteadas anteriormente; no obstante, también se consideraron otros factores importantes además de las métricas planteadas, el cual fue la facilidad de adquirir un SBC y el soporte a estos dispositivos.

8.2. Selección de SBC de bajo costo que se utilizará en el proyecto

La selección del SBC más adecuado para el proyecto esta argumentada según los indicadores mencionados anteriormente y la información suministrada en la tabla anterior, la cual dio como resultado los siguientes dispositivos posibles para la ejecución del servicio de navegación anónima basada en un SBC de bajo costo portable.

N°	NOMBRE	SOC	CPU	GPU	RAM	OS	POWER SOURCE	PRECIO
1	**Orange Pi Plus 2E**	-	H3 Quad-core Cortex-A7 H.265/HEVC 4K	·Mali400MP2 GPU @600MHz	2GB DDR3 (shared with GPU)	Android, Ubuntu, Debian, Raspbian Image	DC input can supply power, but USB OTG input don't supply power	aprox. $282.000 COP
2	**Raspberry Pi 2 Model B**	Broadcom BCM2835	Quad-Core Cortex A7 a 900MHZ	Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0	512 MB LPDDR SDRAM 400 MHz	GNU/LINUX, Windows 10	5V	aprox. $130.900 COP
3	**Raspberry Pi 3 Model B +**	Broadcom BCM2837	4× ARM Cortex-A53, 1.2GHz	Broadcom VideoCore IV 3D graphics core	1GB	Debian GNU/Linux, Fedora, Arch Linux ARM	5V	aprox. $239.000 COP
4	**Raspberry Pi Model B**	Broadcom BCM2835	700 MHz ARM1176JZF-S core (ARM11 family)	·Supports OpenGL ES 2.0	256 MB (shared with GPU)	Debian GNU/Linux, Fedora, Arch Linux ARM	5V/2A	aprox. $210.000 COP

Tabla 7 Dispositivos SBC's que se adecuan más a nuestro proyecto.

Fuente: Propia.

En esta selección de SBC se obtuvo finalmente según los indicadores seleccionados y bajo pruebas que se realizaron previamente que el dispositivo más adecuado es el **Raspberry Pi 3 Model B+,** para el cumplimiento del objetivo de este proyecto.

9. FASE 3: Proponer la arquitectura para un servicio de anonimato portable basado en un SBC

Esta fase constituye una introducción a la elaboración de la Arquitectura de Software, para dos servicios de anonimato portables uno de ellos es el servicio de navegación y el otro las llamadas VoIP, esto con el propósito puntual de brindar una visión amplia del desarrollo y ejecución del proyecto para el cumplimiento del objetivo general del mismo, para luego establecer las respectivas pruebas en relación con la estrategia

arquitectónica del servicio, sus herramientas y los comandos necesarios para el cumplimiento de diseño.

9.1.1.1. Instalación de la arquitectura diseñada en el SBC para la navegación

Para el servicio de navegación se implementó una arquitectura que consta de dos antenas Wi-Fi las cuales están configuradas para recibir y emitir señales desde el Raspberry pi 3 Model B+ bajo protocolos DHCP, los cuales están especificados en la fase 3 de este proyecto. Además de esto se implementó una configuración de instalación de VPN en el dispositivo, la cual aporta junto a la navegación bajo TOR el cambio de IP a la hora de navegar por la red de internet, la cual es suministrada por una red W-FI pública. Unificando estos procesos por medio de la implementación del protocolo DHCP y el protocolo DNSMASQ se logra el objetivo general del proyecto, el cual bajo el servicio de navegación cambia de manera aleatoria por medio de la configuración y conexión del túnel al server de IP de la VPN el cambio de la IP local, este proceso y el flujo de datos de la arquitectura se ve reflejado en la imagen 4.

Para la arquitectura utilizada en la implementación del servicio de navegación se recurrió como se dice anteriormente al uso complementario de las antenas WI-FI, las cuales conectadas a través de los puertos USB, debido a que el dispositivo SBC seleccionado tiene una arquitectura ARM que para la implementación del servicio de navegación Raspberry PI 3 model B+ tiene una dificultad para emitir y recibir señal al mismo tiempo se hizo necesario la implementación de antenas WI-Fi configuradas para lograr así que la comunicación entre los dispositivos móviles y router se cumpliera y se diera con éxito la navegación anónima.

Imagen 5 Características de antena Wi-fi.

Fuente: https://images-na.ssl-images-amazon.com/images/I/71Glvyh7EiL._SY355_.jpg

Como se ve en la imagen 5 Las antenas WI-FI utilizadas cuentan con unas características básicas una de las pequeñas antenas la Deepow USB wifi de largo alcance receptor, wifi Inalámbrico 433/150Mbps 11ac banda dual 5.8Ghz/2.4GHz con antena 2dBi funciona muy bien en relación al precio que tiene, lo cual no afecta en el propósito de la implementación de un servicio de navegación anónima portable y de bajo costo además es de fácil instalación y sus características son las ilustradas obtenidas en (Amazon, 2019)

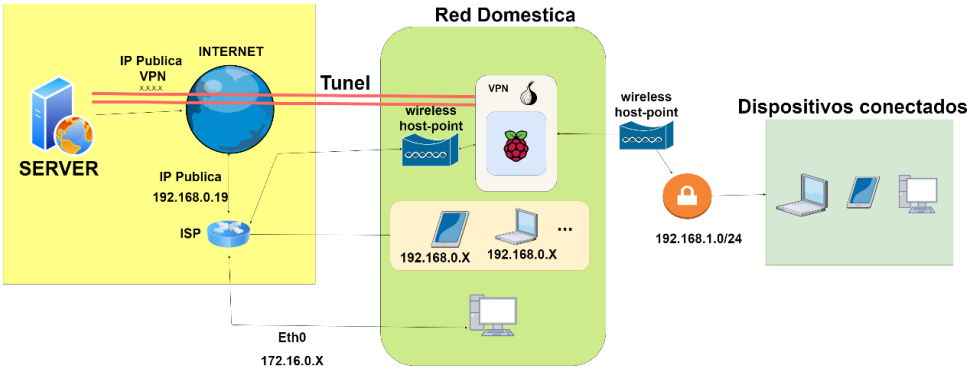


Imagen 6 Diseño de la infraestructura de red.

Fuente: Propia

En el escenario anterior, se puede visualizar el proceso de comunicación que existe desde un Server, el cual esta conecta a la VPN, también se encuentra el ISP (Proveedor de servicios de Internet) este ISP tiene la función de asignar IP locales a una red doméstica, esta red está compuesta a través de una conexión de Ethernet (Eth0) a un equipo de escritorio cuya IP es 172.16.0.X, también a dos dispositivos (dispositivo móvil celular, y portátil) conectados por Wi-Fi con IP 192.168.0.X donde por X se da a entender que depende del número de dispositivos conectados. Además de esto se encuentra un dispositivo SBC que para la implementación del servicio fue utilizado el Raspberry pi 3 Model B, cuyo dispositivo cuenta con una antena configurada bajo host-point que permite que el dispositivo SBC reciba la señal simbolizado en la imagen 7 como el wireless 01, el cual emite la señal al Raspberry y dentro de este, se encuentra una configuración unificada con el VPN y TOR que realiza el enmascaramiento de la IP pública que viene desde el flujo del ISP siguiendo con la red donde se encuentra un wireless 02 que es el encargado de continuar la conectividad ya anónima suministrada a 3 dispositivos que están conectados a la red y que están siendo emitidas por el wireless 02.

9.1.1.2. Instalación de la arquitectura diseñada en el SBC para la llamada Voip

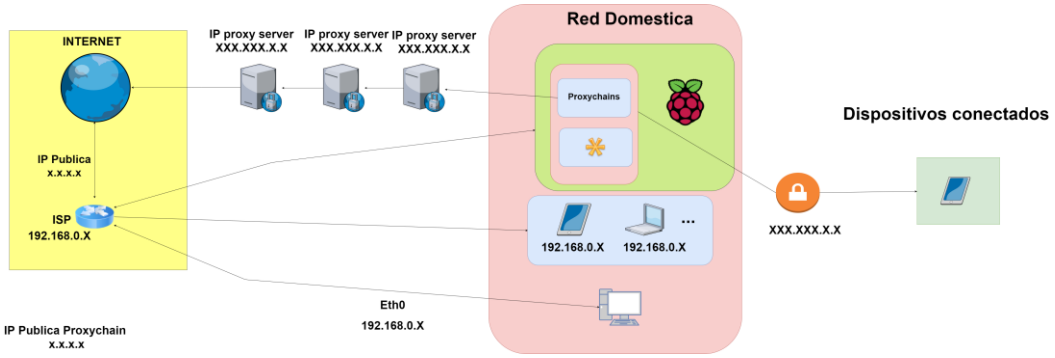


Imagen 7 Diseño de la infraestructura de red

Fuente: Propia

En la imagen anterior, se evidencia el proceso de comunicación que existe entre internet y el ISP, este a su vez funciona asignando IP locales a una red doméstica, esta red está compuesta por una conexión de Ethernet (Eth0) a un equipo de escritorio cuya IP es 192.168.0.X, también dos dispositivos (móvil celular, y portátil) conectados por Wi-Fi con IP 192.168.0.X donde por X se da a entender que depende del número de dispositivos conectados, además de esto se encuentra un dispositivo SBC que para la implementación del servicio de llamada, el cual fue utilizado el Raspberry pi 3 Model B+, en el cual se implementó una configuración de Asterisk , que permite crear un servidor en el cual se realizaran llamadas VoIP, también se configuró un Proxychain, el cual permitió realizar el proceso de enmascaramiento de la IP pública suministrada por el ISP mediante servidores proxies los cuales le brindan a los usuarios registrados en nuestro servidor de Asterisk poder realizar llamadas VoIP de forma anónima.

9.2. Realizar pruebas de servicio anónimo bajo SBC

Los ataques informáticos constituyen una de las amenazas más grandes que existen para las empresas actualmente, afectando por igual a individuos particulares, empresas e incluso estados y sociedades.

Debido a esto es que las medidas de seguridad informática se han convertido en prioritarias, especialmente para aquellas empresas o entidades que dependen casi al 100% de Internet para realizar sus operaciones. Es por esta razón que la implementación de las pruebas en los servicios que se encuentran principalmente

ligados a internet como lo es la Navegación y las llamadas VoIP. A continuación, se inicia la configuración y comandos a tener en cuenta para el cumplimiento del objetivo general del proyecto.

9.2.1. Pruebas del servicio navegación anónima

Inicialmente para la ejecución de pruebas cumplimiento y ejecución del servicio de anonimato portable basado en un SBC de bajo costo se creó una arquitectura que ayudo a la emisión y recepción de la señal WI-FI para el exitoso acceso de los usuarios al tráfico de red de una manera segura.

A continuación, se describe el paso a paso de la elaboración y configuración del sistema operativo raspbian y las antenas para el punto de acceso inalámbrico.

9.2.2. Instalación del sistema operativo raspbian

Como paso inicial se debe realizar la descarga del sistema operativo que se encuentra en la página: https://www.raspberrypi.org y en la sección de Descargas que se encuentra en este punto se puede seleccionar el raspbian pero en este caso se descarga noobs que es más sencillo y trae por defecto el sistema operativo raspbian que hasta el momento se adapta y es el más óptimo para la elaboración del proyecto y para el trabajo en el Raspberry pi 3

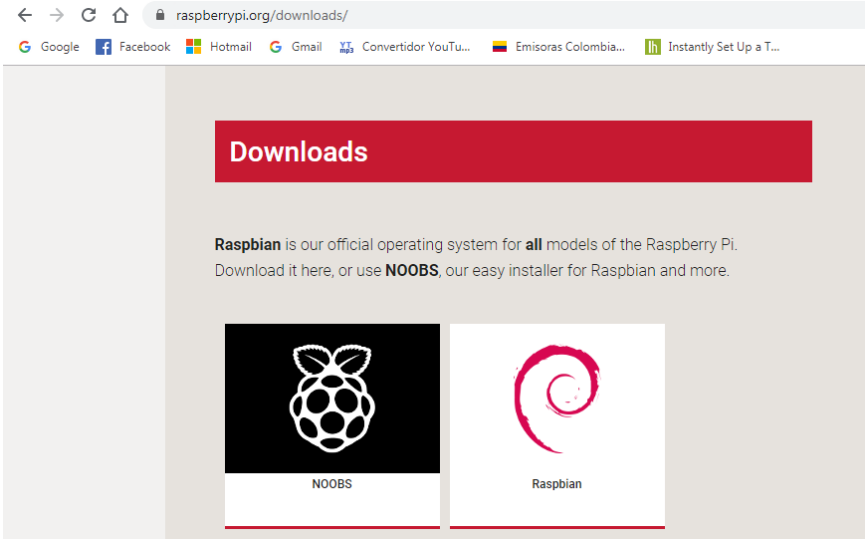


Imagen 8 Selección del sistema operativo.

Fuente: Propia.

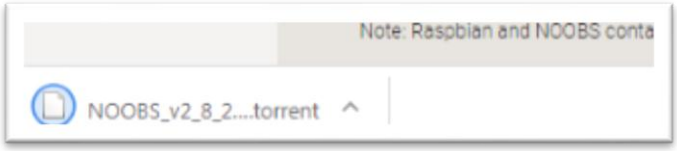


Imagen 9 Descarga del sistema operativo.

Fuente: Propia.

Después de descargar el archivo se descomprime y se realiza una imagen en la SD que será colocada en la Raspberry pi 3 modelo B +, se le inyecta corriente hasta el momento de al menos 1A y se verá el Noobs que fue copiado anteriormente y seguirá el proceso que dura entre 5 a 10 minutos de particiones y el resto de módulos que requiere para su ejecución y finalización de su instalación, de esta manera será instalado el sistema operativo en el SBC seleccionado para la ejecución del proyecto.

- Acceso al dispositivo

Para la configuración del hot-point como primer paso se debe Iniciar sesión en el Raspberry Pi 3 Model B+ por medio de diferentes herramientas que existen gratuitas en este caso se utilizó PuTTY el cual es un cliente SSH con licencia libre con esta herramienta se pudo acceder al Raspberry Pi 3 Model B+ desde el equipo pc para la manipulación e implementación de los comandos necesarios para el cumplimiento de los objetivos del proyecto. Este se realizó través de SSH. Si este proceso no se realiza a través de SSH, se debe asegurar de tener una conexión de red con acceso a Internet o una pantalla que permita mostrar la interfaz con la que cuenta el sistema operativo Raspbian ejecutado en el anterior paso.

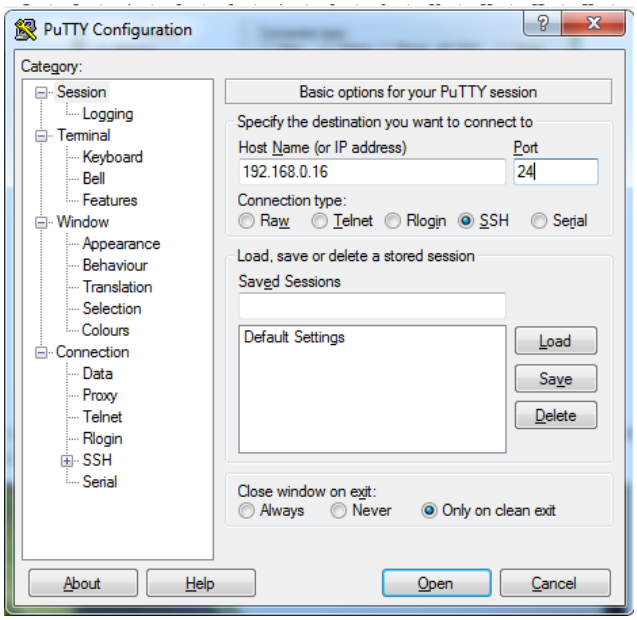


Imagen 10 Configuración de Putty.

Fuente: propia.

9.2.3. Instalación de VPN Raspberry pi 3 Model B+

Tras dados los conceptos básicos en el marco teórico acerca de que es una VPN sus ventajas y cuanto aporta para el cumplimiento de los objetivos principales de este proyecto se llevó a cabo la instalación de la misma bajo los comandos encontrados en página web (Guide, 2017). Los comandos aplicados para la implementación del servicio de navegación anónima sobre la Raspberry pi 3 Model B+ son:

Inicialmente la instalación de la VPN sobre el dispositivo SBC, este debe tener los terminales abiertos para corroborar que no existen actualizaciones pendientes por los paquetes instalados esto se realiza bajo los siguientes comandos:

- **sudo apt-get update**
- **sudo apt-get upgrade**

Continuando con el proceso de configuración se realizó la instalación correspondiente con la herramienta OpenVPN, el cual busca recibir la señal de internet que obtiene desde el ISP, para posteriormente realizar un encapsulamiento a la IP que de cara al internet logré tener un acceso al canal de red privada virtual (VPN), para esto se ingresó el comando, que se observa en la siguiente imagen: **sudo apt-get install openvpn**

```
pi@vpnserver ~ $ sudo apt-get install openvpn
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblzo2-2 libpkcs11-helper1
The following NEW packages will be installed:
  liblzo2-2 libpkcs11-helper1 openvpn
0 upgraded, 3 newly installed, 0 to remove and 1 not upgraded.
Need to get 586 kB of archives.
After this operation, 1,334 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://mirrordirector.raspbian.org/raspbian/ wheezy/main liblzo2-2 armhf 2.06-1+deb7u1 [56.0 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ wheezy/main libpkcs11-helper1 armhf 1.09-1 [46.1 kB]
Get:3 http://mirrordirector.raspbian.org/raspbian/ wheezy/main openvpn armhf 2.2.1-8+deb7u3 [484 kB]
Fetched 586 kB in 2s (285 kB/s)
Preconfiguring packages ...
Selecting previously unselected package liblzo2-2:armhf.
(Reading database ... 78734 files and directories currently installed.)
Unpacking liblzo2-2:armhf (from .../liblzo2-2_2.06-1+deb7u1_armhf.deb) ...
Selecting previously unselected package libpkcs11-helper1:armhf.
Unpacking libpkcs11-helper1:armhf (from .../libpkcs11-helper1_1.09-1_armhf.deb) ...
Selecting previously unselected package openvpn.
Unpacking openvpn (from .../openvpn_2.2.1-8+deb7u3_armhf.deb) ...
Processing triggers for man-db ...
Setting up liblzo2-2:armhf (2.06-1+deb7u1) ...
Setting up libpkcs11-helper1:armhf (1.09-1) ...
Setting up openvpn (2.2.1-8+deb7u3) ...
```

Imagen 11 Instalación del VPN

Fuente: Propia.

- GENERACIÓN DEL ARCHIVO DE CONFIGURACIÓN PARA EL SERVIDOR OpenVPN

En este paso se deben crear llaves para que el servidor y los clientes se reconozcan entre sí, de esta manera proceder con la configuración del servidor VPN a implementar.

Con el comando (**. /Clean-all**) se busca que en el disco seleccionado se eliminen todas las particiones liberando de esta manera memoria para el funcionamiento óptimo del dispositivo.

Para construir en la configuración de VPN es necesario establecer una PKI (clave pública) con el comando (**./build-ca OpenVPN**), el cual construirá el certificado y la clave para la autoridad de certificación llamando también el comando **openssl**. De la misma manera para la certificación del cliente se utiliza el comando (**./build-key-server server**) y se generarán los parámetros necesarios para el servidor openVPN con el comando **(./build-dh)** y se finaliza la configuración (**Exit)**.

```
pi@Rasp:~ $ cd /etc/openvpn/easy-rsa
pi@Rasp:/etc/openvpn/easy-rsa $ ./clean-all
Please source the vars script first (i.e. "source ./vars")
Make sure you have edited it to reflect your configuration.
pi@Rasp:/etc/openvpn/easy-rsa $ sourse vars
-bash: sourse: command not found
pi@Rasp:/etc/openvpn/easy-rsa $ ls
build-ca     build-key         build-key-server  clean-all      list-crl          openssl-1.0.0.cnf  revoke-full  whichopensslcnf
build-dh     build-key-pass    build-req         inherit-inter  openssl-0.9.6.cnf  openssl.cnf        sign-req
build-inter  build-key-pkcs12  build-req-pass    keys           openssl-0.9.8.cnf  pkitool            vars
```

Imagen 12 Configuración de llaves y clientes.

Fuente: Propia.

Se debe abrir el archivo de configuración OpenVPN por medio de: **Sudo nano /etc/openvpn/openvpn.conf**

Con el comando redirect-gateway def1 bypass-dhcp se les indica a los clientes que todo el tráfico se redirige a través del túnel de la VPN. Con los comandos:

- **push "redirect-gateway def1 bypass-dhcp"**, **push "redirect-gateway def1 bypass-dhcp"**, **push "dhcp-option DNS 217.237.150.188"**, **push "dhcp-options DNS 8.8.8.8", log-append /var/log/openvpn**

Los comandos anteriores son utilizados para nombrar los servidores DNS públicos, los cuales son los que utilizará la VPN.

Una vez configurado el servidor, se puede pasar a la configuración de los clientes de la VPN. Para ello se crea un fichero de configuración en el que se tiene que introducir los siguientes comandos: **client-to-client**, status /var/log/openvpn-status.log**, persist-tun,** user nobody, **group nogroup,** verb3**, comp-lzo.**

Por último, con la orden *client-to-client* se determinan que los clientes VPN no solo reconozcan al servidor, sino también a otros clientes VPN y con ***comp-lzo*** se habilita la compresión LZO (que también se ha de indicar en el archivo de configuración del cliente).

Se guardan los cambios con Ctrl+0 y se cierra el editor con Ctrl+X, para que la configuración del archivo quede ajustada con los cambios establecidos.

- CREACIÓN DE UN SCRIPT PARA ACCEDER A INTERNET CON UN CLIENTE

Para **acceder a la conexión a Internet de la red local propia a través del túnel VPN** se crea una redirección. Para ello se crea el fichero **/etc/init.d/rpivpn**:

- **Sudo nano /etc/init.d/rpivpn**

A continuación, se activa la redirección ip_forward escribiendo en el archivo un 1 de esta forma:

- **echo 'echo "1" > /proc/sys/net/ipv4/ip_forward' | sudo -s**

Ahora solo queda crear las órdenes necesarias que permitan a los clientes VPN acceder a la LAN y a Internet. Esto se logra con las siguientes líneas, implementadas desde el terminal del sistema operativo de las raspbian:

- **iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT**
- **iptables -t nat -F POSTROUTING**
- **iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE**

Luego, se guarda y se cierra el archivo de nuevo.

Para realizar la **asignación de los derechos correspondientes al script** e instalarlo como archivo Init, se debe implementar los siguientes comandos:

- **sudo chmod +x /etc/init.d/rpivpn**
- **sudo update-rc.d rpivpn defaults**

Se ejecuta el script y se reinicia el servidor OpenVPN, empleando los siguientes comandos:

- **sudo /etc/init.d/rpivpn**
- **sudo /etc/init.d/openvpn restart**

➢ Cierre de la configuración de los clientes

En el último paso se reúnen los certificados y las claves de cada cliente en un paquete propio. Para ello se requiere de nuevo derechos de supe usuario. Una vez asignados, se abre la carpeta /etc/openvpn/easy-rsa/keys/ y se deposita en ella el archivo de configuración de los clientes. Con el siguiente comando se abre el archivo del cliente.

Todos los clientes se configuran de la misma forma, lo único que hay que cambiar es el nombre del dispositivo:

- **sudo su**
- **cd /etc/openvpn/easy-rsa/keys**
- **nano laptop.ovpn**

En el archivo **openvpn** del cliente se añade los siguientes comandos, mediante editor nano:

- **dev tun**
- **client**
- **proto udp**
- **remote x.x.x.x 1194**
- **resolv-retry infinite**
- **nobind**
- **persist-key**
- **persist-tun**
- **ca ca.crt**
- **cert laptop.crt**
- **key laptop.key**
- **comp-lzo**
- **verb 3**

Con todo lo anterior, hay que ajustar este contenido. En la cuarta línea sustituimos ***x.x.x.x*** por **x.x.x.x** se entiende que la IP que se asigna desde el proveedor de servicio puede variar de acuerdo al escenario en el que se encuentre para el caso del proyecto se obtuvo una IP de red local 192.168.0.19 que al realizar la modificación ésta cambio **por la dirección IP del proveedor del DNS**, la cual para el escenario propio se dio la IP 192.168.0.16/24. Aunque también puedes incluir aquí una dirección IP pública estática si dispones de una; le sigue el puerto en el cual el servidor VPN ha de estar disponible, un ejemplo de ello se visualiza en la imagen siguiente luego que surge el cambio en el ajuste de direcciones.

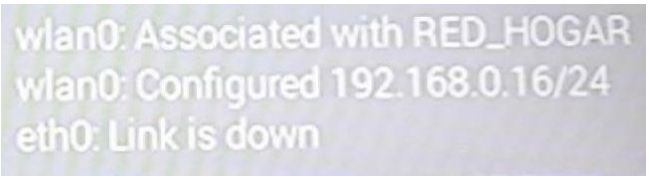


Imagen 13. Asignación de IP por DNS

Fuente: Propia.

Por último, comprime el archivo de configuración, junto con sus certificados y claves, en un archivo Zip. Esto con el fin de disminuir el espacio de RAM del dispositivo y su ejecución sea más óptima. En caso como no se ha realizado la instalación en el Raspberry Pi de un paquete de compresión, dicha acción se realiza a través del comando digitado en el terminal del sistema operativo:

- **apt-get install zip**

Para crear el archivo comprimido se emplea el comando que viene a continuación con cuidado de utilizar siempre el **nombre de cliente correcto** el cual fue utilizado a la hora de crear las PKI o llaves de los clientes del servicio este nombre debe ponerse en el área con las letras rojas de la línea del comando que se muestra a continuación:

- **zip /home/pi/raspberry_laptop.zip ca.crt laptop.crt laptop.key laptop.ovpn**

Hecho esto finalmente se configuran los derechos de los archivos con el siguiente comando y se finaliza con exit:

- **chown pi:pi /home/pi/raspberry_laptop.zip**
- **exit**

Este archivo comprimido se transfiere desde el Raspberry Pi al cliente con un programa SCP o SFTP y se configura el cliente en el dispositivo. Este estaría ahora ya preparado para acceder a la red local conectada con el cliente y a su conexión a Internet desde cualquier punto de acceso externo.

8.1.1.1.Instalación de host-Point Raspberry pi 3 Model B+

Para que el Raspberry Pi funcione como un punto de acceso este debe tener instalado un software de punto de acceso o Host-Point junto con el software del servidor DHCP

para proporcionar dispositivos de conexión con una dirección de red, mediante la utilización del siguiente comando.

- **sudo apt install dnsmasq hostapd**

Para establecer la dirección IP estática, se abre el archivo de configuración DHCPCD con el comando:

- **sudo nano /etc/dhcpcd.conf**

Se edita el archivo con los siguientes comandos:

- **interface wlan**
  static ip_adress=192.168.4.1/24
  nohook wpa_supplicant

Se reinicia el **dhcpcd con el siguiente comando:**

- **sudo systemctl restart dhcpcd**

➢ Configuración del servicio dhcp con un dnsmasq

El servidor DHCP es proporcionado por dnsmasq (Commons, 2008), este será el que proporcione el redireccionamiento de la señal, dando por medio de este protocolo la configuración dinámica del host para evitar a futuro que las dos antenas que se configuren choquen sus señales una entre sí. Este archivo de comandos trae consigo una gran cantidad de configuración que no es necesaria por lo que se deben ejecutar en el terminal del sistema operativo los comandos: **sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig** y **sudo nano /etc/dnsmasq.conf** para evitar así la información que no es necesaria configurar.

Con la siguiente información en el archivo de configuración se termina la configuración del protocolo dnsmasq y se procede guardar los cambios efectuados.

- **interface=wlan0 # Use the require wireless interface - usually wlan0 dhcp-range=192.168.4.2, 192.168.4.20,255.255.255.0,24h**

Se proporcionan direcciones IP entre 192.168.4.2 y 192.168.4.20, con un tiempo de conexión continua de 24 horas, lo cual se ve especificado en la línea anterior del

comando **dhcp-range**. Si está proporcionando servicios DHCP para otros dispositivos de red. Esto permitirá un tiempo de 24 horas donde la IP se estará cambiando dentro del rango dado por la VPN pasado este tiempo se seguirá navegando, pero no cambiando la IP de manera aleatoria si no que queda la última IP que fue asignada durante este tiempo de ejecución del servicio de navegación. Por ello se recomienda reiniciar el sistema para volver a obtener una asignación y rango diferente para otras 24 horas.

Se recarga el dnsmasq para usar la configuración actualizada con el siguiente comando:

- **sudo systemctl reload dnsmasq**

➢ Configuración del software del host-point

Se debe editar el archivo de configuración de hostapd ubicado en la dirección: /etc/hostapd/hostapd.config para agregar los parámetros para la red inalámbrica después de la instalación inicial este será un archivo nuevo / vació esto con el fin de que la información a suministrar sea la adecuada de acuerdo a las que se requieran según el escenario puesto que la IP puede variar según su proveedor. Para ejecutar esta acción se digita en el terminal del sistema operativo el comando **sudo nano /etc/hostapd/ hostapd.conf** para de esta forma acceder a las configuraciones necesarias para la correcta instalación.

Ahora se le indica al sistema donde encontrar este archivo de configuración mediante la siguiente línea de código:

- **sudo nano /etc/default/hostapd**

Encuentre la línea con #DAEMON_CONF, y reemplácela con el comando **DAEMON_CONF="/etc/hostapd/hostapd.conf"**

Ya estando dentro de la configuración general del hostapd se habilita con los siguientes comandos:

- **sudo systemctl unmask hostapd**
- **sudo systemctl enable hostapd**
- **sudo systemctl start hostapd**

- Añadir enrutamiento y mascarada

Edite /etc/sysctl.conf y desconecte esta línea, con el siguiente comando:

- **net.ipv4.ip_forward=1**

Agregue una mascarada para el tráfico saliente en eth0, mediante la aplicación del comando:

- **sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

Guarda la regla de iptables, en la siguiente ruta como se establece en el comando:

- **sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"**

Edite /etc/rc.local y agregue esto justo encima de "exit 0" para instalar estas reglas en el arranque, como se muestra en el siguiente comando:

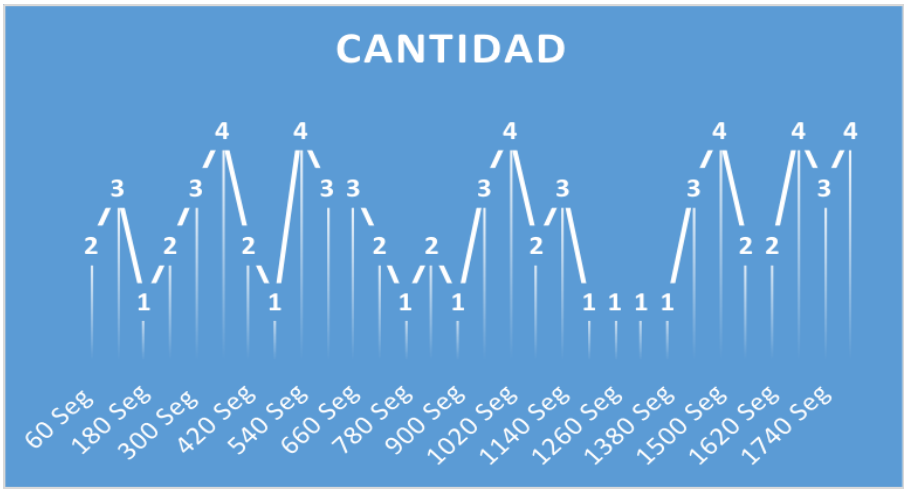
- **iptables-restore < /etc/iptables.ipv4.nat**

Usando un dispositivo inalámbrico, busque las redes. El SSID de red que especificó en la configuración de hostapd este debe estar presente, y permite así el acceso con la contraseña que se haya especificado.

Al estar habilitado el protocolo SSH en el punto de acceso de Raspberry Pi, es posible la administración remota que le permitirá controlar y modificar la IP del ISP, al cual se encuentre conectado teniendo en cuenta esto se ejecuta el comando: **ssh pi@192.168.4.1**

En este punto, la Raspberry Pi está actuando como un punto de acceso, y otros dispositivos pueden asociarse con él. Los dispositivos asociados pueden acceder al punto de acceso Raspberry Pi 3 Model B a través de la dirección IP para realizar operaciones como rsync, scpo ssh esto con el fin de permitir accesos instantáneos de las antenas configuradas por medio de un punto caliente (host-point) dando así por finalizada la unificación de las configuraciones de VPN y TOR por medio de DNS y protocolos de DHCP para que la IP suministrada al Raspberry Pi 3 Model B por el proveedor de servicios de internet llegue al usuario final con el enmascaramiento exitoso de esta IP inicial brindando así el anonimato a la hora de navegar.

9.2.4. Resultados Raspberry pi 3 model B + en la navegación



Gráfica 2 Numero de cambios de IP Raspberry pi 3 Model B+

Fuente: Propia.

En grafica anterior se puede evidenciar que como resultado de las pruebas se logró obtener dos cambios de IP en el primer minuto y en el segundo 180 una suma de 3 IP, lo cual muestra que la variación de éstas no es constante, debido a la disponibilidad aleatoria de las mismas. La prueba realizada en el SBC (Raspberry pi 3 model B) que fue el dispositivo seleccionado inicialmente se procedió a la ejecución e instalación de los comandos propuestos anteriormente para el cumplimiento del cambio de IP constante para el servicio de navegación anónima y segura en el cual después de la implementación de los mismos se logra finalizar con éxito y obteniendo los datos dados en la grafica 2 con la unificación del comando de la VPN y de TOR bajo los protocolos de DHCP y DNS, el cual logra además que las configuraciones adicionales para lograr la conectividad y el flujo de la señal de emisor y receptor desde el Raspberry cumpliendo este escenario de prueba se obtuvo un análisis de los resultados prometedor y disponible a la mejora pues no se tiene problema de rendimiento mientras se ejecuta el servicio de navegación además de que cuenta con capacidades de RAM y PROCESADOR óptimos para aumentar la capacidad de rendimiento.

El dispositivo mencionado da hasta el momento el mejor resultado puesto que cuenta con las características apropiadas para el cumplimiento del proyecto esta razón, dado por los indicadores y resultados obtenidos en las pruebas mostrando que el Raspberry

pi 3 Modelo B+ es el más adecuado para la ejecución del proyecto pues no genera problemas de instalación del sistema operativo ni la ejecución completa de los comandos planteados en la fase de escenario y pruebas.

9.2.5. Pruebas del servicio de llamada VoIP

Para la implementación del servicio anónimo de llamadas se utilizó en el dispositivo SBC seleccionado la instalación de Asterisk (Asterisk, 2019) puesto que esta es una plataforma telefónica de código abierto (GPL) que pretende revolucionar el mundo de las comunicaciones IP frente a las tradicionales soluciones de grandes corporaciones entre ellas Cisco que se caracteriza por su falta de transparencia hacia los usuarios, sus protocolos propietarios y cerrados, así como su elevado coste. Debido a esto se tiene la herramienta Asterisk como una plataforma convergente por cuanto que unifica muchos de los servicios que, tradicionalmente, se ofrecía por separado y/o sistemas no integrados.

Asterisk es una solución completamente software y corre bajo GNU/Linux. Esta configuración le confiere una robustez innata para desplegar servicios típicos de los sistemas tradicionales, pero aportando mucha más flexibilidad, control, creatividad y a muy bajo costo lo cual aporta en gran cantidad para el cumplimiento del objetivo general del proyecto aportando la posibilidad y facilidad de modificación ajuste y correcciones en implementación sin poner en riesgo su calidad y costo, además se une toda la potencia de interacción con cualquier tipo de lenguaje de programación para realizar funcionalidad que se desee. Todo se hace vía software y se hace de una manera que pueda inter-operar con otros sistemas o tecnologías de manera clara y cercana, todo esto se evidencia con la implementación del mismo bajo la prueba de llamadas anónimas realizadas para este proyecto.

Una alternativa que existe de Asterisk es Skype, que fue creado por dos jóvenes universitarios en el año 2003. (Microsoft, 2019) A diferencia de Asterisk, Skype hace uso de un protocolo privado que no está basado en un estándar, lo que a largo plazo se piensa que limitará a sus usuarios. A día de hoy Skype se puede emplear en multitud de plataformas y su uso se encuentra también ampliamente extendido.

Algunos de los beneficios que aportan en gran medida a la investigación del proyecto asociados al uso del Asterisk a las llamadas VoIP para mejorar la comunicación por voz de una entidad empresa u hogar, son:

- **Ahorrar dinero:** en una red telefónica como lo es GSM la relación del tiempo significa dinero. Como una llamada VoIP emplea internet como medio de transporte, el único coste que se puede llegar a tener es la factura mensual de internet la cual es un costo fijo sin importar la duración de la llamada realizada ni el lugar al que se esté direccionando la llamada. Hoy en día el servicio de internet puede encontrarse de manera gratuita en diferentes sectores, parques, restaurantes y hoteles entre otros.
- **Más de dos personas:** En una línea telefónica por lo general si no se cuenta con una tecnología de alta gama la llamada puede verse limitada a 2 dos personas en la comunicación, con llamadas como la VoIP se puede configurar una conferencia que permite a un grupo de personas comunicarse en tiempo real. VoIP comprime los paquetes durante la transmisión, algo que permite que se pueda transmitir una cantidad mayor de datos. Como resultado, se pueden establecer más llamadas a través de una única línea de acceso
- **Hardware y Software baratos:** Si un usuario de internet desea usar VoIP para comunicarse por voz, el único dispositivo adicional que este requiere es el Raspberry pi 3 Modelo B+ y su conexión a internet los cuales son accesibles para las empresas o personas que deseen una comunicación de voz.
- **Prestaciones abundantes, interesantes y útiles:** Usar VoIP también significa beneficiarse de sus prestaciones abundantes que pueden hacer la experiencia de emplear VoIP mucho más rica y sofisticada, tanto en el hogar como en una empresa. En general, se puede estar mejor equipado para la gestión de llamadas.

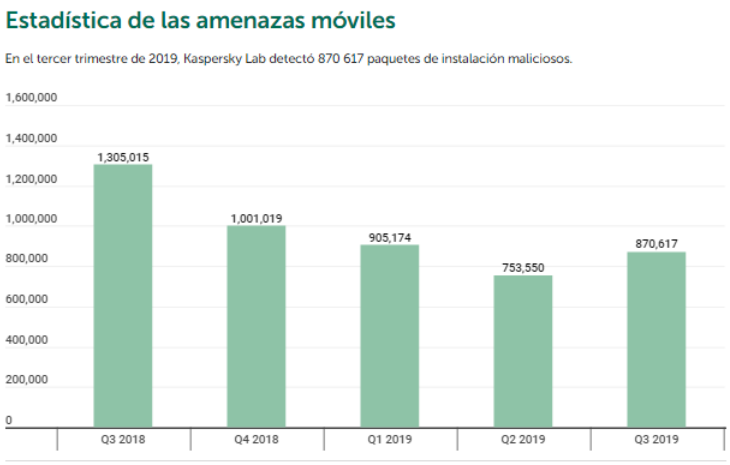
La utilización de las llamadas (VoIP) por medio de Asterisk cuenta con una desventaja que al estar conectado a una red de internet se está más expuesto al riesgo de robo de información más alta que la que puede generar las llamadas GSM según las estadísticas existen más perdidas de información de un móvil al momento de navegar que al realizar una llamada según el estudio hecho por LR república (Monterrosa, 2018), como se

muestra en la siguiente imagen donde a nivel nacional se evidencia que las personas tienen un promedio de uso de internet, el cual corresponde a una población de menores de edad en búsqueda de trabajos e interacción en redes sociales en un promedio de 3 horas diarias, por lo que muestra claramente que la mayoría de personas se encuentran conectados a los servicios que otorga la internet lo que trae como consecuencia una alta vulnerabilidad lo que hizo que se le diera relevancia a los servicios que cuenten con una conexión a internet, debido a su alto riesgo de pérdida o robo de información.

Imagen 14 Estadísticas del uso de dispositivos a temprana edad

Fuente: https://securelist.lat/it-threat-evolution-q3-2019-statistics/89858/

Estas estadísticas y estudios aportaron a la justificación de selección del servicio de llamadas VoIP a implementar en el proyecto dejando de lado por el momento la llamada GSM, debido a que los datos obtenidos arrojan señales de alertas más altas en cuanto a inseguridad en los servicios que se encuentran ligados a una conexión de internet. En la siguiente grafica se evidencian las estadísticas en cuanto a las amenazas que se ven expuestas en este tipo de servicios como lo es la llamada a través del VoIP (Victor Chebyshev, 2019).



Gráfica 3 Estadística de amenazas móviles

Fuente: https://securelist.lat/it-threat-evolution-q1-2017-statistics/85017/

Aplicando la investigación al proyecto por lo que se pudo concluir que el programa de software libre más adecuado a implementar es el llamado Asterisk, puesto que, el riesgo de vulnerabilidad es más alto cuando se está realizando una tarea bajo un servicio de internet como las llamadas VoIP. Por este motivo la elección de Asterisk fue elegida debido a que su implementación es de alguna manera más sencilla para el usuario que desee adquirirlo además de que es un área que requiere de una implementación de seguridad mayor, debido al alto riego que existe al contar con una conexión permanente a internet. Por ello a continuación se muestra la instalación y ejecución de la instalación de Asterisk y la configuración de su respectivo enmascaramiento de anonimato al momento de realizar una llamada VoIP en el dispositivo seleccionado.

9.2.6. Instalación del SO

Inicialmente se debe realizar la descarga del SO que se encuentra en la siguiente página: http://www.raspberry-asterisk.org y en la sesión de descargas se encuentra un hipervínculo donde se puede descargar raspbian

Torrent	raspbx-04-04-2018.zip.torrent
HTTP	raspbx-04-04-2018.zip
SHA-1	8f473d01935da0347fbafb7f71c649914934c5b6
Contents	Asterisk 13.20.0 & FreePBX 14.0.2.10

A 4GB card is required.

Imagen 15 Hipervínculo que descarga el SO

Fuente: Propia.

Luego de descargar el archivo se procede a descomprimirlo quedando un archivo .IMG, posteriormente se guarda la imagen en una tarjeta SD con capacidad de 32 GB, con la herramienta Win32DiskImager, la cual se puede descargar de la siguiente página https://sourceforge.net/projects/win32diskimager/. Después de descargar e instalar la herramienta se ejecuta y se elige la letra que corresponde a la tarjeta SD, luego se busca donde se tiene la imagen del SO y se presiona en el botón "Write".

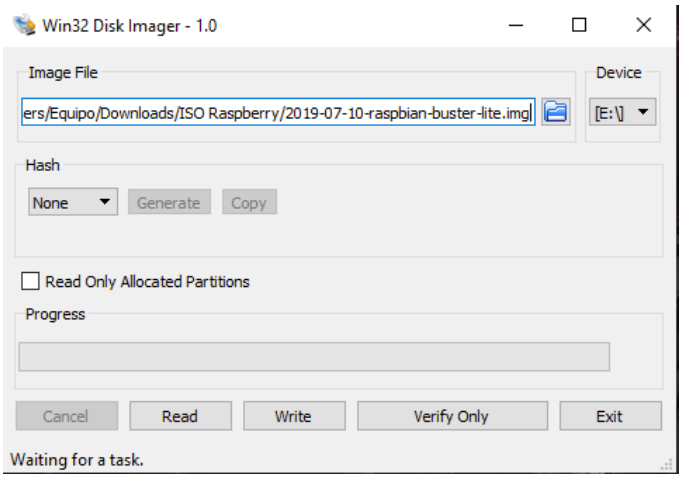


Imagen 16 Aplicación utilizada para instalar el SO

Fuente: Propia.

Una vez instalada la imagen en la tarjeta SD se extrae del PC y se procede a insertarla en el Raspberry.

9.2.7. Configuraciones Iniciales

Después de hacer la correcta instalación del sistema operativo se enciende el Raspberry con los periféricos necesarios para su correcto funcionamiento (Teclado y monitor).

Luego se debe ingresar el usuario y contraseña para acceder al menú donde se realizan todas las configuraciones que se requieren.

Para la configuración inicial se ingresa al menú de configuración de Raspberry con el comando **sudo raspi-config** y se selecciona la opción **Network Options:**

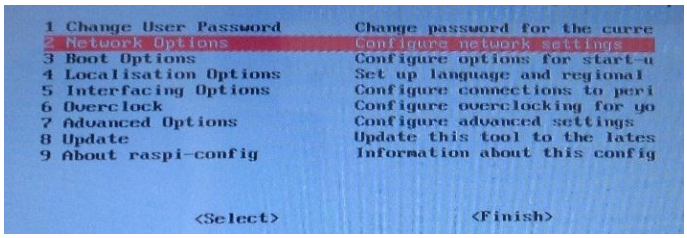


Imagen 17 Menú de configuración de Raspberry

Fuente: Propia.

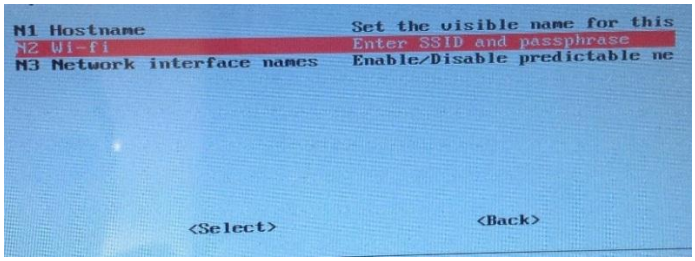


Imagen 18 Selección de conexión a internet (Mediante Wi-fi)

Fuente: Propia.

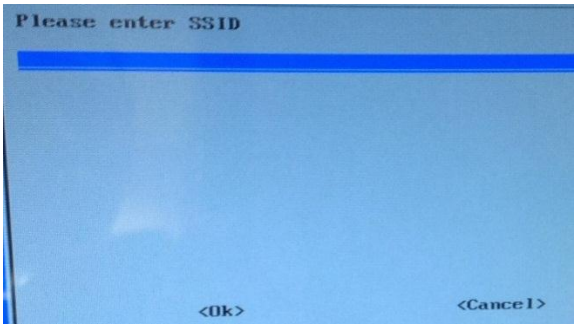


Imagen 19 Nombre de la red que se conectara

Fuente: Propia.

Luego se ingresa el comando “sudo raspi-config” donde se realizan dos configuraciones, una de ellas es la zona horaria la cual se realiza de la siguiente manera:

Luego se ingresa a la opción “Localisation Options” aquí se elige el continente en que se encuentre, posteriormente la ciudad capital del país de residencia y luego se da ok y confirmar esta información, en pantalla se muestran los datos de la zona horaria que se acaba de ingresar. A continuación, se muestran las imágenes de este paso.

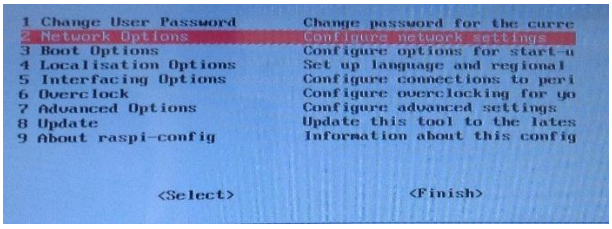


Imagen 20 Menú de configuración de Raspberry

Fuente: Propia.

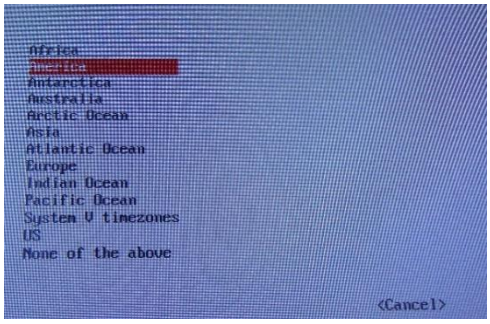


Imagen 21 Configuración del continente

Fuente: Propia.

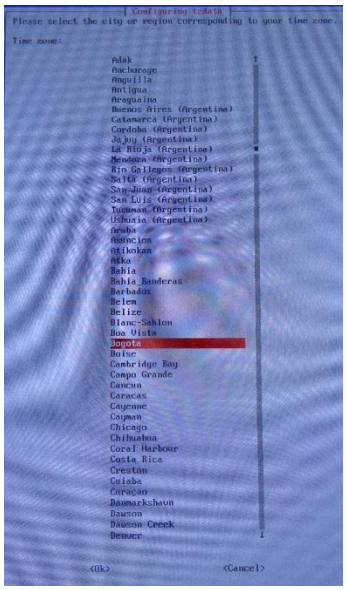


Imagen 22 Configuración del país

Fuente: Propia.

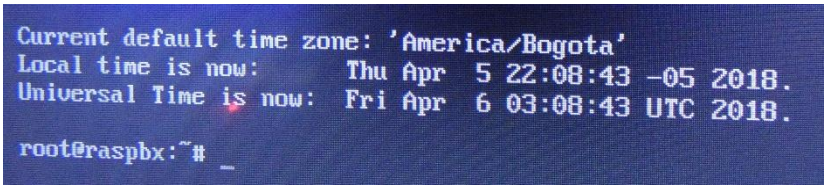


Imagen 23 Zona horaria

Fuente: Propia.

Una vez en la consola de comandos insertaremos el comando “Reboot” lo cual reiniciara todo el sistema para que nuestras configuraciones tomen efecto.

9.2.8. Actualizaciones

Ahora se procede a actualizar el sistema raspbian ingresando los siguientes comandos uno por uno los cuales nos descargaran todas las actualizaciones que se necesitan:

- **sudo apt-get update**
- **sudo apt-get upgrade**

9.2.9. Instalación de paquetes

Ahora se instalan una serie de paquetes y dependencias que se necesitan para la instalación de Asterisk, se ejecutan los siguientes comandos uno después del otro.

- sudo apt-get install libsqlite3-dev libncurses5-dev libxml2-dev libnewt-dev libssl-dev libiksemel-dev libgnutls28-dev libcurl4-openssl-dev libspandsp2 libspandsp-dev mysql-client libmariadbd18 libmariadbd-dev mariadb-server unixodbc-dev unixodbc libportaudio-dev libical-dev libneon27-dev libportaudio-dev libspeex-dev speex libvorbis-dev libsrtp0-dev iptables-persistent libsox2 libsox-dev
- sudo apt-get install libuuid1 uuid uuid-dev libjansson4 libjansson-dev subversion sendmail sox ngrep sendmail-bin

9.2.10. Instalación de Asterisk

Se debe acceder a la carpeta donde se instalará Asterisk ejecutando el siguiente comando:

- **cd /usr/src**

Luego de ingresar en esta carpeta se procede a la descarga de Asterisk con el siguiente comando:

- **sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz**

Ahora se procede a descomprimir el archive que se ha descargado con el sgt comando

- **sudo tar –xf asterisk-13-current.tar.gz**

Una vez que se descomprime se verifican los archivos que se tienen en la carpeta con el comando “ls” y se verán que se tienen 2 archivos, que en nuestro caso sería:

- “asterisk-13.29.1” será el archivo que se descomprimió para obtener el siguiente archivo
- “asterisk-13-current.tar.gz” será el archivo que se obtendrá

```
root@raspbx:/usr/src# sudo tar -xf asterisk-13-current.tar
root@raspbx:/usr/src# ls
asterisk-13.29.1  asterisk-13-current.tar.gz
root@raspbx:/usr/src# cd asterisk-13.29.1
```

Imagen 24 Verificación de los archivos en la carpeta

Fuente: Propia.

Ahora se proceden a ingresar a la carpeta del archivo que se ha descomprimido (puede variar la versión, pero el proceso es el mismo) con el comando:

- **cd asterisk-13.29.1/**

En la carpeta **asterisk-13.29.1** es donde se realizan las configuraciones e instalación del servidor Asterisk, luego se ejecuta el siguiente comando que configurará todo el archivo que se ha descargado para luego dar paso a descargar los servicios que v se van a necesitar en el servidor

- **sudo ./configure**

Luego se ejecutará un comando que mostrará un menú donde podrá escoger las extensiones que se van a necesitar:

- **sudo make menuselect**

Luego de abrir el menú seleccionar las siguientes opciones, guardamos y salimos

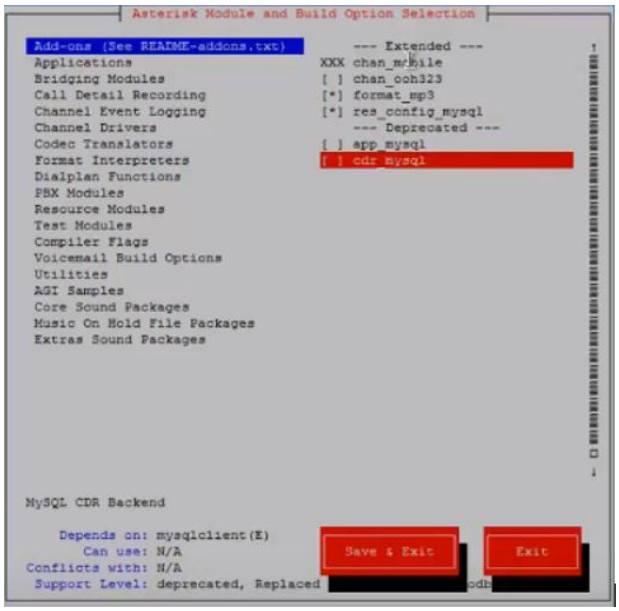


Imagen 25 Menú de configuración y selección de extensiones de Asterisk

Fuente: Propia.

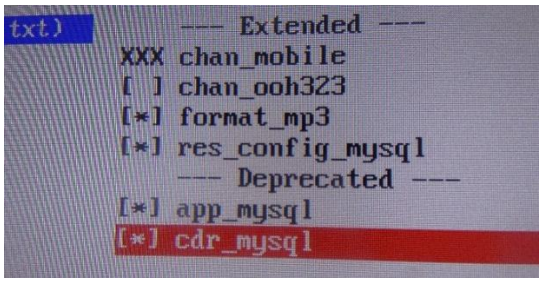


Imagen 26 Selección de las extensiones

Fuente: Autor.

Ahora con el siguiente comando hará que se descarguen las extensiones que se deben seleccionar:

- **sudo make**

Luego de finalizar la descarga de las extensiones se ejecuta un comando que instalará todo lo que se descargó:

- **sudo make install**

Luego ejecutar un comando que creará todos los archivos que se necesitan para configurar nuestra telefonía IP.

- **sudo make samples**

Posteriormente se ejecuta un comando que configurará automáticamente todos los archivos que se crearon anteriormente.

- **sudo make config**

Para finalizar la instalación de asterisk

Con el comando “cd” se regresa a la carpeta inicial y se ejecuta el siguiente comando para verificar que todo funcionó correctamente.

- **sudo /etc/init.d/asterisk start**

Lo que hace que empiece a funcionar el servidor, y con el siguiente comando detendremos el servicio:

- **sudo /etc/init.d/asterisk stop**

9.2.11. Creación de usuarios y extensiones

Se ingresa a la siguiente carpeta:

- **cd /etc/asterisk**

Luego se ingresa al siguiente archivo donde se crean los usuarios

- **sudo nano sip.conf**

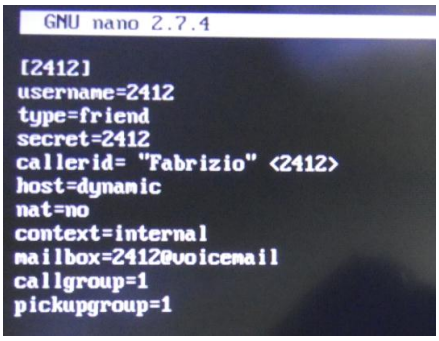


Imagen 27 Creación de usuarios

Fuente: Propia.

A continuación, se especifican la función de cada ítem utilizado en la creación de los usuarios:

- username – Como se identificará al usuario

- type - Tipo de cliente SIP. Existen 3 tipos: “peer”, “user” y “friend” en función de cómo se manejan las llamadas entrantes/salientes y cómo se identifica el usuario.
- secret - Contraseña que utiliza el cliente para autenticarse en el sistema.
- callerid - Define el indicador cuando no hay otra información disponible
- nat – indica si el dispositivo está detrás de una NAT
- host - Dirección IP o nombre del host que utiliza el cliente. Si está asignada de manera dinámica por DHCP, ' dynamic’.
- context - Contexto al que pertenece el cliente.

Después de crear el usuario se guarda presionando la combinación de teclas “Ctrl + O” después se confirma con “Enter” y luego se sale con “Ctrl + X”.

Después de lo anterior se procede a configurar un archivo, permitiendo la comunicación entre los usuarios, esto se hace con el siguiente comando:

- **sudo nano extensions.conf**

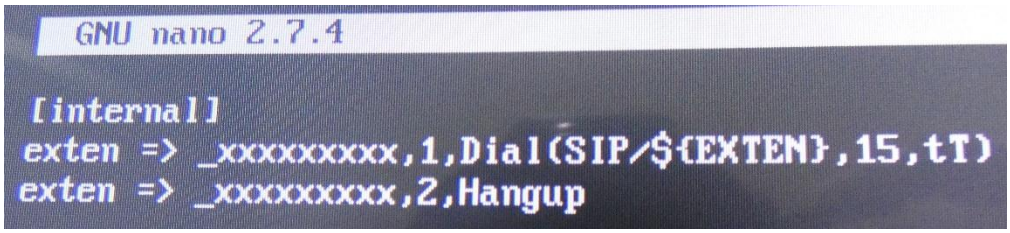


Imagen 28 Configuración para la comunicación entre usuarios

Fuente: Propia.

A continuación, se configurará la comunicación entre usuarios

- **exten** – indicamos que se trata de una extensión.
- **_xxxx** – significa que es la extensión que asterisk espera que se marque.
- **1 –** Numero de prioridad o de orden de ejecución, indica que se ejecuta primero y luego la siguiente prioridad hasta terminar todas.
- **Dial (SIP/${EXTEN}** – Es la aplicación dial y le pasamos como parámetro a quien debe marcar por protocolo SIP.
- **15, tT –** El numero indica el tiempo en que terminará la llamada si no contesta, “tT” hará que la finalice al no contestar.
- **Hangup –** Se encarga de finalizar la llamada.

Después de crear el usuario se procede a guardar con “Ctrl + O” después se confirma con “Enter” y luego salir con “Ctrl + X”.

Luego de creados los usuarios deseados, se levanta el servicio de Asterisk con el comando

- **sudo /init.d/asterisk start**

Posteriormente se ingresa a la consola de Asterisk con el comando:

- **sudo asterisk –rvvvvvvvvvvv**

Una vez dentro de la consola de Asterisk se debe ejecutar el comando “reload” para que todas las configuraciones que se realizaron tomen efecto.

Para visualizar los usuarios que se tienen registrados en Asterisk se puede ingresar con el siguiente comando:

- **sip show peers**

Posteriormente de la instalación de Asterisk se tiene un registro en consola de los usuarios que se encuentran en comunicación por medio de llamada VoIP como se ve en la siguiente imagen:

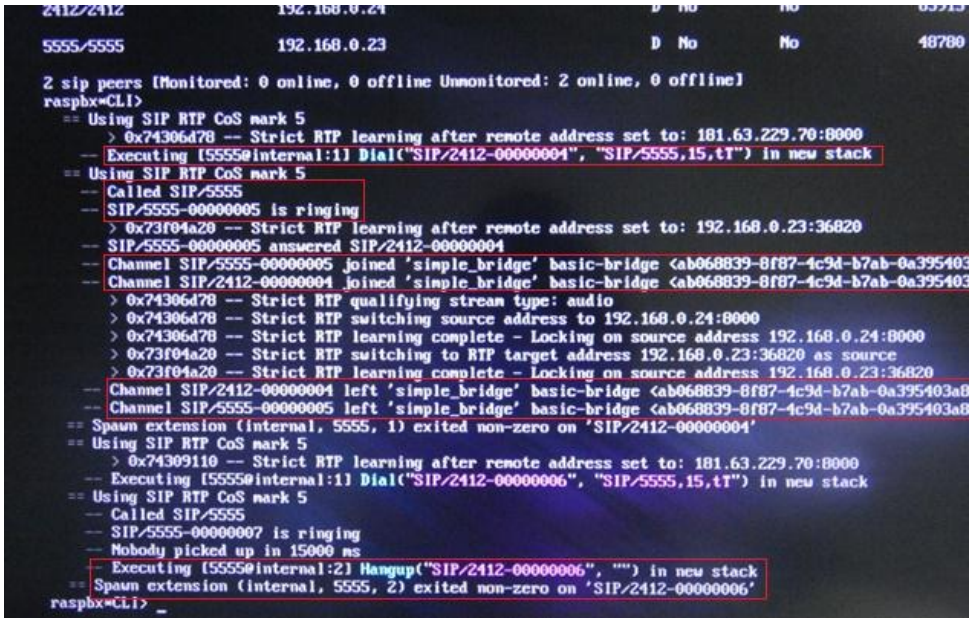


Imagen 29 Registro de llamada en la consola de Asterisk

Fuente: Autor.

En el primer segmento de arriba hacia abajo subrayado en rojo podemos observar que mediante las configuraciones que se realizaron en el “internet” (Imagen 32) en pasos anteriores, se ejecuta la primera línea de código, en la cual se puede observar que el usuario “2412” está realizando una llamada al usuario “5555” la cual está en espera para ser contestada como se observa en el segundo cuadro subrayado; en el tercer cuadro subrayado se puede observar que se realizó la llamada con éxito permitiéndoles ingresar a un canal a cada uno donde continuara la llamada; en el cuarto cuadro subrayado se observa que la llamada finaliza y ambos salen de los canales en los cuales estaban anteriormente; y seguidamente de lo anterior se ejecuta el comando del último cuadro subrayado el hará que finalice la llamada (en ocasiones no mostrara que se ejecuta algún comando en la consola, pero si funciona todo correctamente)

Con la ejecución de los anteriores comandos se da por finalizada la configuración e instalación de Asterisk y se procede a la configuración del PROXYCHAINS para enmascarar la IP original.

9.2.12. Configuración PROXYCHAINS

La configuración de PROCHAINS estuvieron basados en los otorgados por Linux GZ el cual permite realizar una correcta instalación del mismo (galicialinux, 2017) es por esto que se obtiene la implementación de los ajustes necesarios con los siguientes comandos:

En primera instancia para lograr el acceso al fichero de configuración **proxychains.conf.** El cual permite que el PROXYCHAINS busque dicho fichero de forma jerárquica a través de los siguientes directorios:

- ./proxychains.conf
- $(HOME)/.proxychains/proxychains.conf
- /etc/proxychains.conf

Teniendo en cuenta que el fichero cuenta con más opciones de configuración que se necesitan para la instalación del PROXYCHAINS se especifican a continuación cuales fueron las usadas para este proyecto, como lo es:

- chain_len: esta configuración permite ver el número de proxies que se utilizarán en el encadenamiento aleatorio (random_chain).
- proxy_dns: esta opción es para realizar consultas DNS a través del proxy y evitar una fuga de información.
- tcp_read_time_out: establece un valor de timeout o tiempo de salida para la respuesta de las conexiones.
- tcp_connect_time_out: establece un valor de timeout para el establecimiento de la conexión.
- socks4 127.0.0.1 9050: proxy que trae configurado proxychains por defecto.

Para utilizar proxychains se arranca con el servicio TOR mediante el comando **sudo service tor start** y se comprueba su estado (active) a través del comando sudo service TOR status:

Tal y como se ha comentado anteriormente, PROXYCHAINS por defecto tiene configurado un proxy de tipo socks4 en la dirección local 127.0.0.1 a través del puerto 9050:

Arrancando un navegador utilizando PROXYCHAINS mediante el comando **sudo proxychains <aplicación> <parámetros>** se observa cómo se realiza una petición, en este caso se utilizó el **proxy local 127.0.0.1** definidos en el fichero de configuración:

Con esta configuración se enmascara la IP original y se finaliza la instalación y configuración de la llamada VoIP.

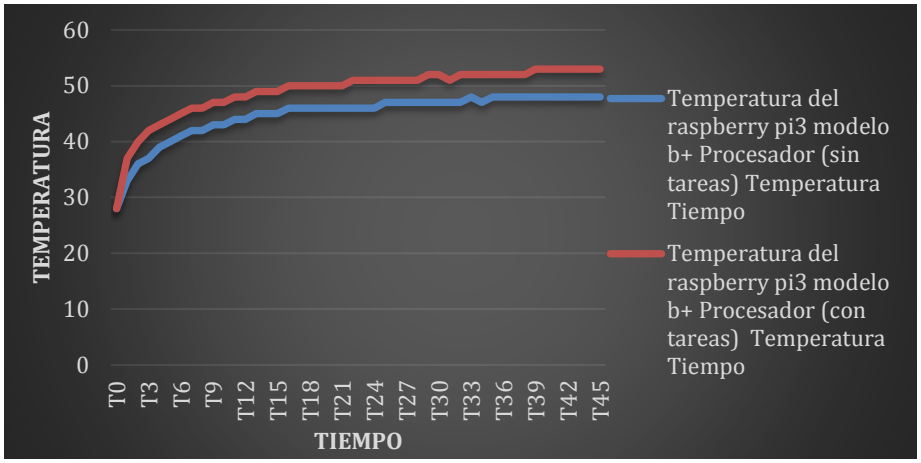
9.3. Documentación de resultados de las pruebas realizadas

9.3.1. Pruebas de rendimiento del dispositivo

9.3.1.1. Análisis de resultados

Para el análisis de los resultados anteriores se realizaron pruebas del comportamiento de los dispositivos en escenarios antes y después de la ejecución de los comandos implementados anteriormente. En las pruebas se obtuvieron datos de temperatura del Hardware y en el software donde se midió el rendimiento de la navegación y cuanto afectaba el cambio de IP constante mientras se ejecutaba el servicio.

Como resultado de estas pruebas en el dispositivo Raspberry pi 3 modelos B+ se obtuvieron los datos mostrados en las siguientes gráficas:



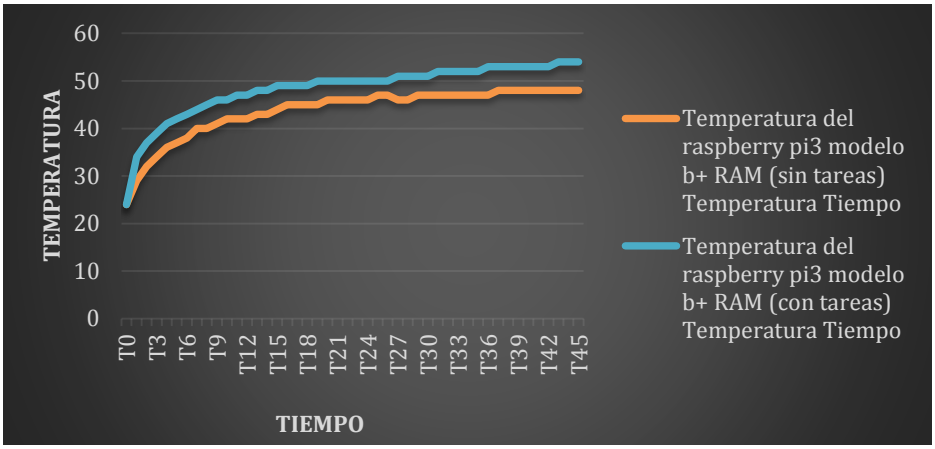
Gráfica 4 Resultado de prueba hardware Raspberry pi 3 modelo b+

Fuente: Propia.

En la gráfica anterior, se puede observar que la línea azul la cual es el resultado de la prueba de temperatura del procesador sin realizar tareas el SBC comenzó con una temperatura base de 28° C en el minuto 0, que a lo largo del tiempo comenzaba a subir hasta alcanzar una temperatura casi estable de 47°C que ocurrió en el minuto 25, después de este tiempo la temperatura oscilo entre 47°C y 48°C hasta el minuto 35 donde se pudo observar que la temperatura se estabilizo en 48°C donde, ya no se reducía ni aumentaba la temperatura pudiéndose estabilizar.

En cuanto a la línea roja es el resultado de la prueba de temperatura mientras en el SBC se realizaban tareas, en esta se puede observar que la temperatura partió de 28°C en el minuto 0, la cual tuvo un aumento de temperatura mayor, donde llego hasta los 53°C en el mismo tiempo que la prueba del SBC sin tareas, demostrando así que la estabilidad logra en una cantidad de tiempo aún mayor.

A continuación, se mostrará los niveles de temperatura de la RAM en el SBC Raspberry pi 3 modelo B+:



Gráfica 5 Resultado de prueba hardware Raspberry pi 2

Fuente: Propia.

En la gráfica anterior se observa que la línea naranja, la cual es el resultado de la prueba de temperatura de la RAM sin realizar tareas el SBC comenzó con una temperatura base de 24° C en el minuto 0, que a lo largo del tiempo comenzaba a subir hasta alcanzar una temperatura estable en el minuto 37 con 48°C.

En cuanto a la línea azul que es la temperatura del SBC mientras se realizaban tareas se obtuvo mayores niveles de calentamiento de la RAM, el dispositivo inició con una temperatura de 24°C, la cual mientras se realizaban tareas la temperatura aumento de forma más rápida llegando hasta una temperatura de 54°C en el mismo tiempo que cuando no se realizaba ninguna tarea y esta se predice que iría aumentando a lo largo del tiempo hasta alcanzar una temperatura estable

9.3.1.2. Resultados raspberry pi 2

En este dispositivo evaluando los indicadores planteados en la teoría y ejecutando los comandos necesarios para la implementación del servicio de navegación anónima en el mismo se evidencia que su capacidad de procesamiento no es óptima para la ejecución completa de los servicios necesarios para el cumplimiento del objetivo es por esta razón que se descarta la utilización de este dispositivo puesto que su funcionamiento se vuelve lento y no cumple con el cambio de IP constante evitando que el usuario navegue de manera fluida en la red.

En esta prueba no se obtuvieron resultados del tiempo y cantidad de cambios de IP puesto que no se pudo completar la instalación completa de todos los archivos y comandos planteados en la fase de escenarios y pruebas.

9.3.1.3. Resultados orange pi plus 2E

En la placa de Orange pi Plus 2E se obtuvo para estas pruebas comparativas que el dispositivo no cuenta con la compatibilidad de instalación del sistema operativo Raspbian si no de sistemas operativos como DEBIAN UBUNTO O LINUX, lo cual impidió para este caso la continuación de las fases de las pruebas dándonos como resultado que la investigación realizada frente a este dispositivo no es certera a pesar de estar soportada en diferentes motores de bases de datos e investigación amplia del mismo.

Por lo planteado anteriormente, no se pudo obtener para este dispositivo resultados que brindaran datos para sus análisis. Cabe destacar que para esta oportunidad y la elaboración de esta fase de prueba no se tuvieron en cuenta otro tipo de sistemas operativos para lograr así el análisis comparativo entre los 3 dispositivos y obtener de esta manera una comparación equitativa entre los SBC.

CAPITULO IV

10. CONCLUSIONES Y TRABAJOS FUTUROS

En esta fase final del trabajo de proyecto de grado se da a conocer conclusiones obtenidas por medio de las pruebas realizadas y los resultados generados a partir de las mismas, donde dichos resultados dan cumplimiento a los objetivos establecidos en la implementación de un servicio de anonimato portable basado en SBC de bajo costo.

10.1. Conclusiones

De acuerdo a las pruebas iniciales de configuración del software para la navegación anónima de VPN, instalación de TOR y la unificación de las configuraciones de dos antenas WI-FI conectadas por puertos USB para la emisión y recepción de señal desde el Raspberry Pi Model B, además de la implementación de protocolo DHCP junto con el protocolo DNSMASQ se dedujo que el diseño y las características del dispositivo SBC son significativas, puesto que influye en gran medida para el desempeño del software, eligiendo así según unos indicadores evaluados que arrojaron que las características que se ajustaban al objetivo del servicio de navegación fue la Raspberry pi 3 Model B, el cual se caracteriza por tener un procesador ARM Cortex A9, y la capacidad para la implementación del software requerido (sistema operativo raspbian) para la ejecución del debían correspondiente a la arquitectura tratada, al seleccionar los comandos adecuados para que no existiese ningún tipo de inconveniente que correspondan a una arquitectura de procesador *x86*, por ejemplo, al montar estas implementación en una Raspberry pi 2 no se logró realizar un funcionamiento correcto para la navegación anónima debido a su baja capacidad de procesamiento.

También se resalta los tiempos de cambio de IP que se obtuvieron, los cuales variaron de acuerdo a las IP que se encuentran disponibles en el momento de realizar una navegación lo que mostro un cambio de IP variado con respecto al tiempo.

Continuando con las conclusiones en la implementación del servicio de la llamada se determinó la elección para este servicio el dispositivo SBC Raspberry PI 3Model B+, donde la configuración estuvo basada en la instalación de Asterisk para obtener una central que permitiera la creación de usuarios, los cuales realizaran la comunicación vía llamada VoIP; además para el anonimato y enmascaramiento de la IP la

configuración de un PROXYCHAINS el cual por medio de una estructura de proxy permite el cambio constante de IP mientras se está efectuando la llamada la elección tanto del dispositivo como de los comandos a implementar fueron los correctos puesto en los resultados finales no interfirieron con el objetivo del proyecto, brindando un buen nivel de seguridad y anonimato sin sacrificar la portabilidad ni el bajo costo del servicio anónimo en este caso la llamada VoIP.

Finalmente, se responde de manera afirmativa la pregunta de investigación planteada en el problema la cual es: "¿cómo se podría garantizar el servicio de anonimato de manera portable basado en un SBC de bajo costo?" dando por hecho la factibilidad de ejecutar una implementación de dos servicios bajo ocultamiento y enmascaramiento de una IP publica suministrada por cualquier proveedor de servicios de internet mientras se está navegando o realizando una llamada VoIP por medio de un dispositivo SBC, permitiendo así aprovechar bondades como la de su precio reducido y la fácil portabilidad del dispositivo físico.

Se concluye así, que si se desea implementar un servicio de anonimato portable y de bajo costo se puede optimizar costo, tamaño y potencia con un dispositivo con las características del Raspberry Pi 3 Model B+. También si se desea optimizar mucho más el costo sin sacrificar potencia en el Software se puede tener en cuenta el uso de las Raspberry Pi 3 Model B, dado que también es posible llevar a cabo la implementación de los dos servicios sin ver afectado su rendimiento.

11. REFERENCIAS

(s.f.). Obtenido de http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

Admin. (25 de Noviembre de 2013). *VozToVoice*. Obtenido de https://www.voztovoice.org/?q=node/655

Alexander Mampotes, M. D. (18 de febrero de 2019). Sistema de gestion unificada de amnaza basada en sbc. Popayan, Trabajo de Tesis, Colombia.

Amazon. (2019). *Amazon.es*. Obtenido de https://oficina10.top/mejores-antenas-wifi-de-largo-alcance/

Anonimo. (2013). *Raspberry Pi Geek*. Obtenido de http://www.raspberry-pi-geek.com/Archive/2013/02/Raspberry-Pi-as-a-Tor-router-and-web-filter

Anonimo. (04 de ABRIL de 2014). *IBM*. Obtenido de https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm

Anonimo. (8 de Noviembre de 2016). *Pi Point*. Recuperado el 15 de 12 de 2019, de https://www.pi-point.co.uk/documentation/

Anonimo. (2019). *Las mejores VPN* . Obtenido de https://www.top10vpn.com/mejores-vpn/?v=2&bsid=c47se1kw129&gclid=EAIaIQobChMIhO3fga-H2QIViwOGCh3VYQMcEAAYASAAEgLjo_D_BwE

Anonimo. (s.f.). *Tor*. Obtenido de https://www.torproject.org/

Asterisk. (2019). *Asterisk Administrator Guide*. Recuperado el 05 de 2019, de https://www.asterisk.com/

Auditing, G. G. (20 de ABRIL de 2017). *blogs.eltiempo*. Obtenido de http://blogs.eltiempo.com/huella-forense/2017/04/20/abc-del-habeas-data-ley-1581-del-2012/

Buba, B. (2016). *Scrib*. Obtenido de https://es.scribd.com/doc/51337882/TECNICAS-CRIPTOGRAFICAS

Certerus. (2019). *Certerus.com*. Recuperado el 02 de 2019, de ¿Qué es un Proxy y para qué sirve?: https://mi.certerus.com/knowledgebase/124/iQue--es-un-Proxy-y-para-que-sirve-.html

Ciberseguridad, F. G. (17 de ENERO de 2018). *EL TIEMPO*. Obtenido de https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

COLOMBIA, C. P. (s.f.). Obtenido de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Commons, C. (15 de octubre de 2008). *recursos tic*. Obtenido de Servidor DNS sencillo en Linux con dnsmasq: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/638-servidor-dns-sencillo-en-linux-con-dnsmasq

Crespo, E. (2019). *Aprendiendo Arduino*. Recuperado el 02 de 2019, de ARCHIVO DE LA ETIQUETA: SBC: https://aprendiendoarduino.wordpress.com/tag/sbc/

Debajyoti Pal, T. T. (2017). *ieee xplore digital library*. Obtenido de https://ieeexplore.ieee.org/document/8359973

DESTACADOS, S. D. (16 de AGOSTO de 2016). *ISO TOOLS*. Obtenido de https://www.isotools.org/2016/08/16/la-iso-3166/

DIAN. (10 de OCTUBRE de 2018). *DIAN*. Obtenido de https://www.dian.gov.co/normatividad/Proyectosnormas/Proyecto%20Resoluci%C3%B3n%20000000%20de%2022-10-2018.pdf

Fedor Sinitsyn, D. P. (22 de Mayo de 2017). *securelist*. Obtenido de Desarrollo de las amenazas informáticas en el primer trimestre de 2017 Estadística: https://securelist.lat/it-threat-evolution-q1-2017-statistics/85017/

GALEANO, S. (31 de ENERO de 2019). *marketing4ecommerce*. Obtenido de El número de usuarios de Internet en el mundo crece un 9,1% y alcanza los 4.388 millones (2019): https://marketing4ecommerce.net/usuarios-internet-mundo/

galicialinux. (1 de febrero de 2017). *linux GZ*. Obtenido de Cómo configurar Proxychains correctamente: https://linuxgz.wordpress.com/2017/02/01/como-configurar-proxychains-correctamente/

González Cuervo, M., Henao Pérez, J. C., Calle Correa, M. V., Pinilla Pinilla, N., Mendoza Martelo, G. E., Palacio Palacio, J. I., . . . Vargas. (1991). *Constitución política Colombiana.* (https://www.ramajudicial.gov.co/documents/10228/1547471/CONSTITUCION-Interiores.pdf?fbclid=IwAR31CEMBbLqSe34PG6A6vRMm5u8MWiUB_6Og75hrdEbc89n1RdFimHIxcm8, Ed.) Bogota, colombia: Imprenta Nacional de Colombia. Obtenido de http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

González, G. (19 de Diciembre de 2014). *Blogthinkbig*. Obtenido de https://blogthinkbig.com/que-es-un-vpn

Guide, D. (07 de 08 de 2017). *Ionos*. Obtenido de Cómo crear un servidor VPN en un Raspberry Pi con OpenVPN: https://www.ionos.es/digitalguide/servidores/configuracion/crear-un-servidor-vpn-en-un-raspberry-pi/

Gurierrez, C. (02 de Julio de 2015). *FayerWayer*. Recuperado el 15 de 12 de 2019, de https://www.fayerwayer.com/2015/07/proxyham-es-una-antena-proxy-que-esconde-tu-ubicacion-ip-por-medio-de-una-conexion-de-radio/

Gus. (07 de marzo de 2019). *PiMyLifeUp*. Recuperado el 15 de 12 de 2019, de https://pimylifeup.com/raspberry-pi-vpn-server/

Hal, P. L. (17 de MAYO de 2017). *UC Berkeley school of information*. Obtenido de https://www.ischool.berkeley.edu/research/projects/how-much-info-2017/internet.htm

Harsh Kupwade Patil. Dan Wing, T. M. (24 de Mayo de 2013). *ScienceDirect.* Obtenido de https://www.sciencedirect.com/science/article/pii/B9780123943972000507

Höbel, V. (5 de Febrero de 2013). *Raspberry pi Geek*. Recuperado el 15 de 12 de 2019, de http:www.raspberry-pi-geek.com/Archive/2013/02/Raspberry-Pi-as-a-Tor-router-and-web-filter

IBM®. (25 de ABRIL de 2014). Obtenido de IBM Integration Bus, versión 9.0.0.2 Sistemas operativos: AIX, HP-Itanium, Linux, Solaris, Windows y z/OS: https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm

Informatico Barcelona. (2014). Obtenido de https://informaticobarcelona.wordpress.com/portfolio/instalacion-freepbx-en-raspberry-pi-3/

ISO. (15 de 11 de 2013). *ISO*. Recuperado el 02 de 2019, de Codes for the representation of names of countries and their subdivisions: https://www.iso.org/iso-3166-country-codes.html

Jimenez Anderson, D. P. (07 de 12 de 2017). CRIPTOANALISIS DEL ALGORITMO RSA CON LLAVES DE AL MENOS 340 BITS BASADOS EN SBC DE BAJO COSTO. *Proyecto de grado*. Popayan, Colombia: Institución Universitaria Colegia Mayor del Cauca.

Jimenez, D. P. (11 de Noviembre de 2017). *Criptoanalisis del algoritmo rsa con llaves de al menos 340 bits basados en sbc de bajo costo.* Popayan.

Man, A. (2019). *maneldeantonio.com*. Recuperado el 03 de 2019, de Asterisk en una Raspberry Pi con RasPBX: http://maneldeantonio.com/asterisk-raspberry

Martínez Carazo, P. C. (20 de JUNIO de 2006). El método de estudio de caso. (P. &. Gestión, Ed.) *Revista Pensamiento & Gestión*. Obtenido de Pensamiento & Gestión: https://www.redalyc.org/pdf/646/64602005.pdf

Microsoft. (02 de 2019). *SKYPE*. Recuperado el 2019, de ¿Que es skype?: https://www.skype.com/es/about/

Milenium. (2019). *Informatica Milenium*. Recuperado el 02 de 2019, de Servicios: https://www.informaticamilenium.com.mx/es/temas/cuales-son-los-servicios-it.html

Monterrosa, H. (4 de AGOSTO de 2018). *La republica*. Obtenido de internet economy: https://www.larepublica.co/internet-economy/los-ninos-y-jovenes-colombianos-usan-internet-tres-horas-y-media-al-dia-2756640

Ninja. (20 de Octubre de 2015). *Anonhq*. Recuperado el 15 de 12 de 2019, de https://anonhq.com/how-to-be-anonymous-on-wi-fi-over-2-5-miles-away-using-raspberry-pi/

Patrik Gallo, D. L. (14 de Septiembre de 2012). *Ieee Xplore Digital*. Obtenido de https://ieeexplore.ieee.org/document/6338494

Regis J., (. B. (21 de Noviembre de 2014). *ScienceDirect.* Obtenido de https://www.sciencedirect.com/science/article/pii/B9780124170391000036

Sepideh Poyan Raad, H. A. (9 de Septiembre de 2014). *Ieee Xplore Digital*. Obtenido de https://ieeexplore.ieee.org/document/7000824/authors#authors

TIC, G. (12 de JULIO de 2018). *TIC Portal*. Obtenido de ¿Qué supone la intranet para una empresa?: https://www.ticportal.es/glosario-tic/intranet

Velasco, R. (06 de MARZO de 2019). *Redeszone*. Obtenido de https://www.redeszone.net/2019/03/06/malware-movil-doble-2018/

Victor Chebyshev, F. S. (29 de Noviembre de 2019). *Securelist*. Obtenido de Desarrollo de las amenazas informáticas en el tercer trimestre de 2019. Estadísticas: https://securelist.lat/it-threat-evolution-q3-2019-statistics/89858/

Wong, F. (14 de Diciembre de 2013). *Eleva tu limite*. Recuperado el 15 de 12 de 2019, de https://elevatulimite.wordpress.com/2013/12/14/parte-3-montar-un-servidor-casero-con-raspberry-pi-primera-ejecucion-de-raspbian/