Arquitectura de comunicación anónima para un servicio de red basada en dispositivos SBC

Alejandro Jiménez Lagos

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Programa de Ingeniería de Sistemas
Popayán, noviembre de 2020

Arquitectura de comunicación anónima para un servicio de red basada en dispositivos SBC

Trabajo de grado presentado como requisito para obtener el título de Ingeniero de Sistemas

Alejandro Jiménez Lagos

Director: MSc. Siler Amador Donado

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Programa de Ingeniería de Sistemas
Popayán, noviembre de 2020

AGRADECIMIENTOS

Primeramente, quiero agradecer a Dios por permitirme llegar a esta etapa de mi vida. También a mi padre y a mi madre por su apoyo incondicional, su afecto y consejos que guiaron mis decisiones, además de ser mi ejemplo de vida y darme fuerzas en los tiempos de incertidumbre.

A mi director de trabajo de grado Siler Amador Donado brindarme su orientación y dirección para desarrollar este trabajo de investigación, asimismo por su contribución al proyecto con respecto a dispositivos hardware utilizados en la etapa de desarrollo, me siento honrado de haber contado con su guía y apoyo en este proyecto.

A todo el conglomerado de docentes del programa de ingeniería de sistemas de la universidad del cauca por trasmitir sus conocimientos y experiencias para mi crecimiento intelectual.

Alejandro Jiménez L.
Popayán - Cauca,
Agosto de 2020

RESUMEN

En el mundo existen diferentes tipos de redes electrónicas o informáticas que facilitan la comunicación entre usuarios y del mismo modo brindan diversos tipos de servicios a los que el usuario puede acceder, un ejemplo de esto es la red informática conocida como “internet” que permite al usuario acceder a servicios como correo electrónico, mensajería instantánea, transacciones bancarias, o compras en línea donde se requieren datos reales de la persona que utiliza estos servicios, como resultado las compañías que proporcionan estos servicios logran obtener un perfil de cada usuario con información que voluntaria e involuntariamente proporcionan los usuarios, parte de dicha información puede ser obtenida por entes externos o delincuentes informáticos, en definitiva sea por medios legales o ilegales dicha información puede usarse para cometer delitos informáticos o monitorear cada movimiento que el usuario realiza, por tal motivo se presenta la necesidad de un mecanismo que permita al usuario permanecer anónimo mientras mantiene la comunicación a través de la red. Teniendo en cuenta lo anterior se implementó un prototipo compuesto por un dispositivo SBC y software de anonimato que permite al usuario mantener anónima su identidad en cada área de la comunicación, para llegar a ello, primeramente, se realizaron estudios para determinar qué áreas de la comunicación proteger, cuál es el software adecuado para la arquitectura y que dispositivo usar para el prototipo hardware, adicionalmente se realizaron las correspondientes pruebas de rendimiento al prototipo, además de las pruebas de seguridad del proyecto OWASP IoT las cuales fueron diseñadas especialmente para estos dispositivos, en conclusión el prototipo desarrollado brinda anonimato al usuario navegando desde el sistema operativo configurado en el dispositivo y adicionalmente permite compartir ese anonimato por medio de una red WiFi para que los usuarios que se conecten puedan navegar de forma anónima.

ABSTRACT

In the world there are different types of electronic or computer networks that facilitate communication between users and in the same way provide various types of services that the user can access, an example of this is the computer network known as "internet" that allows users to user access services such as email, instant messaging, banking transactions, or online purchases where real data of the person who uses these services is required, as a result the companies that provide these services manage to obtain a profile of each user with information that is voluntary and involuntarily provided by users, part of said information may be obtained by external entities or computer criminals, ultimately, whether by legal or illegal means, said information can be used to commit computer crimes or monitor every movement that the user makes, for this reason it is presented the need for a mechanism that allows the user Aryan remains anonymous while communicating over the network. Taking into account the above, a prototype composed of an SBC device and anonymity software was implemented that allows the user to keep their identity anonymous in each area of communication, to achieve this, first, studies were carried out to determine which areas of communication protect ?, which is the appropriate software for the architecture and which device to use for the hardware prototype ?, additionally, the corresponding performance tests were carried out on the prototype, in addition to the security tests of the OWASP IoT project which were specially designed for these devices In conclusion, the prototype developed provides anonymity to the user browsing from the operating system configured on the device and additionally allows sharing that anonymity through a WiFi network so that users who connect can browse anonymously.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. Definición

El *anonimato* es la condición o cualidad de un individuo para ser desconocido en un entorno, esto presenta múltiples ventajas como la *libertad de expresión*, *libertad de movimiento*, brinda *seguridad al individuo* y *protege su información privada*. En el mundo existen diferentes campos en donde el anonimato se presenta como una herramienta principal para desempeñar una labor, por ejemplo, cuando un gobierno desea mantener en secreto sus operaciones, cuando un miembro de una organización quiere dar a conocer su opinión o simplemente cuando se requiere un resultado justo en una encuesta.

En el campo de la informática y telecomunicaciones una comunicación anónima tiene como objetivo *ocultar el nexo entre el emisor y el receptor de la comunicación*, esto incluye, el contenido del mensaje, la ruta de trasmisión de la comunicación y las identidades de los individuos, esto quiere decir que el contenido del mensaje se mantiene protegido contra entes externos que quieren acceder a su información y la información de su ruta de trasmisión, adicionalmente, ningún ente interno o externo puede conocer la verdadera identidad del individuo con quien mantiene la comunicación. el anonimato en las telecomunicaciones no solo ayuda a proteger la privacidad de las preferencias personales o expresar las opiniones de minorías, sino que también ayuda a combatir la vigilancia masiva por parte de entidades gubernamentales o grandes corporaciones que usan la información recolectada para su propio beneficio.

Desde otro punto de vista para mantener una comunicación anónima se debe contar con una arquitectura de comunicación que permita anonimizar cada componente de la comunicación, es decir que cada parte que compone la arquitectura debe tener como objetivo principal resguardar la comunicación. Finalmente, una arquitectura de comunicación es el diseño de una red de comunicaciones que contiene los componentes físicos y lógicos de la comunicación, su configuración, sus procedimientos y principios operacionales, así como el formato de los datos utilizados en su funcionamiento.

1.1.2. Pregunta de investigación

¿Cómo proteger la privacidad del canal de comunicación entre sus usuarios para evitar la fuga *de información sensible*[1] en un entorno de comunicaciones de red, basados en dispositivos SBC?

[1] **información sensible:** se refiere a información privada de un individuo, empresa o institución, como por ejemplo los datos personales, datos bancarios o contraseñas relacionadas con Internet o informática (correo electrónico, conexión a Internet, PC, smartphone, etc.) o cualquier otro dato

Lo que se pretende demostrar en este trabajo de grado es lo siguiente: Es factible diseñar e implementar un prototipo hardware y software que permita *anonimizar el canal de comunicación de un servicio de red*, usando dispositivos SBC de bajo costo.

1.1.3. Justificación

Vivir en el mundo interconectado de hoy trae consigo grandes ventajas y amenazas. Aparentemente la velocidad de las comunicaciones e intercambio de información ha abierto nuevos caminos para el desarrollo de nuevas tecnologías que pocos años atrás eran inimaginables. Sin embargo, junto con los beneficios que ofrece este nuevo mundo, se plantean nuevos desafíos significativos. *La misma tecnología que permite a las familias comunicarse en tiempo real atravesando continentes también permite la vigilancia y catalogación de los contenidos de esas conversaciones*. De igual forma la tecnología que permite a los usuarios en línea personalizar sus experiencias de compra de tal manera que le brinden exactamente lo que desea desde la comodidad de su hogar, *también permite a los centros de intercambio de datos elaborar un perfil de información muy detallado de cada usuario, información que actualmente los proveedores de servicios de internet venden a diferentes organizaciones y empresas las cuales la usan para mejorar sus estrategias de marketing e incrementar sus ganancias entre otros fines* [1]. Sumado a esto en el mundo *existen redes de espionaje las cuales se dedican a la interceptación de comunicaciones, algunos ejemplos de esto son* ***ENFOPOL*** *(del inglés Enforcement Police) la cual es administrada por la Unión Europea, otra denominada* ***MUSCULAR*** *que es administrada por el cuartel general de comunicaciones del gobierno británico y la agencia de seguridad nacional de Estados Unidos (****NSA****) que interceptaron los canales de comunicación entre los centros de datos de google, yahoo y hotmail para acceder a la información de los correos electrónicos de sus usuarios* [2].

Muchos de los sistemas usados actualmente para navegar en la red son susceptibles a intrusiones no autorizadas debido al bajo nivel de seguridad que protege el canal de comunicación, para mantener una comunicación anónima uno de los principales obstáculos es la fuga de información ya que si un sistema permite un fácil acceso a los datos de origen o destino de la comunicación se expone numerosa información privada del usuario como, por ejemplo, su ubicación geográfica, el tipo de comunicación utilizada, además de los datos de cada nodo por donde se trasmite la comunicación. Otro problema a tener en cuenta es el uso de protocolos inseguros o protocolos que no proporcionan protección a los componentes de una comunicación, un ejemplo de esto son los protocolos http y https usados para la navegación web, *un usuario al usar el protocolo http, el contenido de la consulta viaja a través de la red en forma de texto plano por lo que todo el contenido del mensaje queda expuesto*, por otro lado, al usar el protocolo https la información se trasmite cifrada, pero esto solo garantiza la privacidad del

privado. La información sensible incluye todos aquellos datos cuya divulgación puede perjudicar a la persona o entidad interesada, en caso de caer en manos equivocadas.

contenido por lo que *si un individuo realiza una captura de datos en la red obtendrá entre otras cosas la dirección ip de origen de la comunicación la cual puede usarse para conseguir información sensible como el tipo de dispositivo, la marca, el sistema operativo y los servicios que se están ejecutando*, al recopilar esta información un individuo capacitado puede lograr un acceso no autorizado al sistema o dispositivo de su víctima.

A medida que avanza el tiempo se desarrollan mejores herramientas de espionaje, se desarrolla nuevo malware y se descubren nuevas vulnerabilidades informáticas, por tales motivos surge la necesidad de proteger las comunicaciones que se realizan a través de la red y específicamente el *canal de la comunicación*, esta es solo una de las raíces que se logró identificar (**ver figura 1**) al construir completamente el árbol de problemas tomando como problema central ***"la facilidad de acceso a información privada de usuarios conectados a dispositivos electrónicos en la red"***, a continuación en la siguiente figura se muestran algunas causas (una raíz del árbol de problemas) que se identificaron como puntos críticos en el canal de la comunicación, los cuales al no ser controlados conllevan a tener un bajo nivel de seguridad en la comunicación dejando vulnerables a los usuarios involucrados en la comunicación y sus componentes o dispositivos.

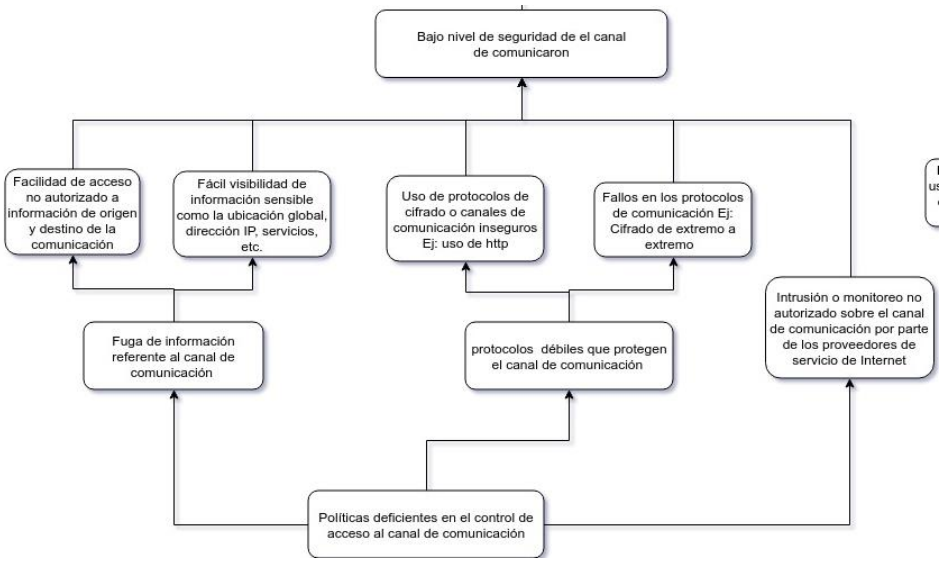


Figura 1. Árbol de problemas, canal de la comunicación.

Nota: el árbol de problemas se elaboró teniendo en cuenta cada una de las áreas que causan el problema central mencionado anteriormente, áreas como la parte física y de entorno, seguridad de la red, seguridad del sistema host o servidor, generación de backups y el manejo por parte del usuario, se deben tener en cuenta para garantizar la privacidad de la información. Después de realizar el análisis del árbol de problemas y elaborar el árbol de objetivos, además, un análisis comparativo con respecto a las referencias bibliográficas se catalogó el canal de comunicación como el área de mayor prioridad para afrontar el problema central.

En el ***anexo A*** se muestra el árbol de problemas completo con sus correspondientes causas y efectos.

Adicionalmente en el ***anexo B*** se muestra el correspondiente árbol de objetivos que permitió establecer el objetivo general planteado en este proyecto de investigación. Según la revisión de documentos presentada en la **sección 2.1** se tomaron los primeros 63 artículos (resultado de la primera iteración) y se marcó la relación entre el contenido de los artículos y los ítems del arboles de problemas para verificar el rumbo de la investigación y determinar claramente el enfoque u objetivos que se desean alcanzar con este proyecto, en el ***anexo C*** se muestra el árbol de problemas con sus correspondientes relaciones, a manera de explicación en el árbol se encuentra resaltado en color azul el camino desarrollado en el artículo desde su inicio (causas) hasta su final (efectos), el numero encerrado en un rombo corresponde al número del artículo.

Por otro lado, en la actualidad una tecnología que está en crecimiento es IoT o internet de la cosas la cual viene acompañada de los dispositivos SBC (single board computer) estos son dispositivos que poseen los componentes principales de una computadora corriente fusionados en una sola placa de circuito integrado cuyas principales características son sus dimensiones reducidas, son de bajo costo, además tienen una gran variedad de dispositivos en el mercado, a causa de esto, el uso de estos dispositivos ha aumentado en los últimos años, cada vez son más utilizados para trabajos de oficina, en la industria y en el hogar convirtiéndose en una excelente alternativa para trabajos de automatización, monitoreo y control de equipos entre otros, además, muchos de estos dispositivos SBC están construidos basados en la arquitectura ARM[2] que debido a su lógica simple de procesamiento de instrucciones mejora la velocidad y reduce el consumo de energía, de igual forma esta arquitectura permite el multiprocesamiento de datos haciendo que estos dispositivos sean compatibles entre sí creando la posibilidad de construir clusters o conjuntos que mejoran aún más el rendimiento y la velocidad de procesamiento.

debido a los motivos mencionados anteriormente se realizará la implementación de una arquitectura de comunicación segura que permita anonimizar un servicio de red, utilizando dispositivos SBC de bajo costo para crear un prototipo hardware accesible en términos monetarios.

1.2. OBJETIVOS

[2] **ARM:** sus siglas en ingles Acorn RISC Machine es una arquitectura desarrollada por la empresa Acorn Computers Ltd para usarse en computadoras personales que manejan un sistema de instrucciones simples lo que le permite ejecutar tareas con un mínimo consumo de energía.

1.2.1. Objetivo general

- Anonimizar[3] un servicio de red[4] entre usuarios conectados en un entorno de comunicaciones de red, basado en dispositivos SBC.

1.2.2. Objetivos específicos

- Diseñar la arquitectura[5] de comunicación que anonimice el servicio de red.
- Diseñar un diagrama de red[6] basada en dispositivos SBC que permita anonimizar el servicio de red.
- Implementar la arquitectura de comunicación propuesta en un ambiente controlado.
- Realizar pruebas de penetración e integridad a la arquitectura propuesta para validar la confiabilidad de la comunicación.

1.3. METODOLOGÍA

El proyecto se desarrollará siguiendo la metodología de investigación-acción para ingeniería de software que propone [3]. Esta metodología propone dos ciclos, uno es el ciclo de la investigación y el otro es el ciclo de la solución al problema. Dichos ciclos tienen un comportamiento iterativo e incremental, además, contienen procesos que ayudan a realizar el proyecto de investigación. A continuación, en la **Figura 2** es presentado de manera general la metodología de investigación a usar por medio de un diagrama de actividades.

[3] **Anonimizar**: expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad. [7]

[4] **Servicio de red:** es una tecnología que facilita las operaciones de red, normalmente lo proporciona un servidor, basado en protocolos de red que se ejecutan en la capa de aplicación del modelo OSI.

[5] **Arquitectura:** es un diseño para la especificación de los componentes software y hardware de una red además de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los formatos de los datos utilizados en su funcionamiento.

[6] **Diagrama de red:** es una representación visual de una red de computadoras o telecomunicaciones, muestra los componentes que conforman una red y cómo interactúan.

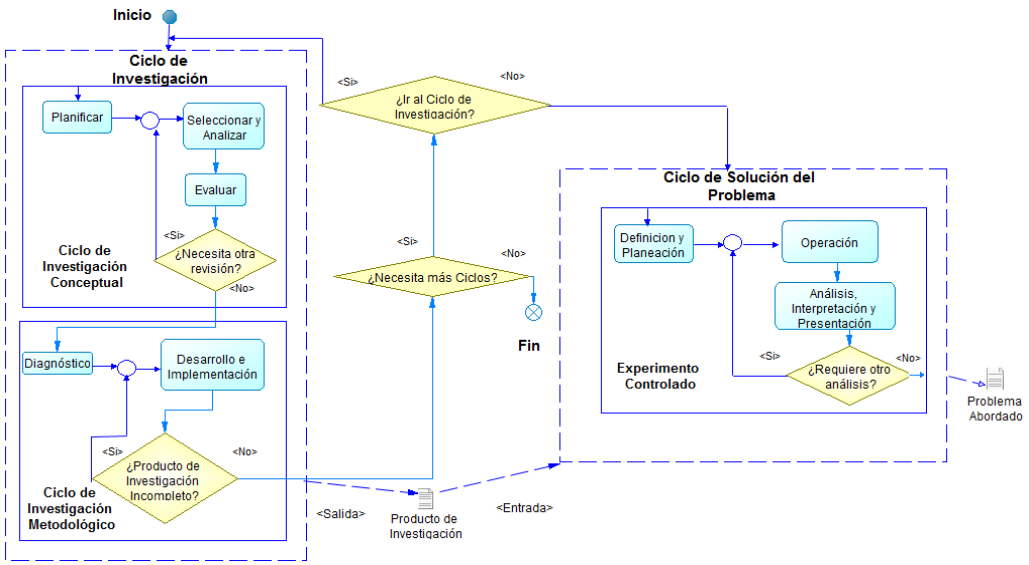


Figura 2. Diagrama de actividades de la metodología Investigación-Acción.

El ciclo de investigación está comprendido por dos ciclos adicionales que son: ciclo de investigación conceptual y ciclo de investigación metodológica. Además, dado que la metodología plantea tres procesos genéricos en cada ciclo para llevar a cabo una investigación (diagnóstico, acción y reflexión), se explicará en cada ciclo los procesos con nombres específicos y sus respectivas actividades, además, en este trabajo se incluye una etapa adicional relacionada con la Documentación, que se realizará en forma transversal a los ciclos mencionados y que tendrá por objetivo la generación de la monografía y la elaboración del artículo científico.

1.4. Ciclo de investigación

1.4.1. Ciclo de investigación conceptual

Planificar: Este proceso se enfoca en la planeación del alcance y los objetivos que van a ser abordados en la revisión de la literatura. Definir el alcance de la investigación por medio de una pregunta de investigación. Estructurar las cadenas de búsqueda con sinónimos y operadores lógicos para que puedan ser procesadas sobre un motor de base de datos bibliográficas basada en la web, como por ejemplo EBSCO. Por otra parte, se definen los criterios de inclusión y exclusión, para poder seleccionar los estudios obtenidos en: estudios primarios y estudios secundarios.

Seleccionar y analizar: Este proceso se enfoca en la recolección de estudios por medio de las cadenas de búsqueda planteadas anteriormente y en seleccionar los estudios primarios para la investigación. Para poder agrupar los resultados obtenidos, se aplican una serie de filtros para determinar qué estudios se consideran relevantes, los filtros son: eliminar estudios repetidos, aplicar los criterios tanto de inclusión como de exclusión. Analizar cada estudio considerado como primario para tener un punto de partida a la hora de realizar la propuesta que busca dar solución a la pregunta de investigación.

Evaluar: Este último proceso del ciclo de investigación conceptual está enfocado en garantizar que los estudios seleccionados hasta el momento sean acordes a la literatura. Debido a que la investigación será realizada por dos investigadores, se pretende realizar una reunión para resolver la discrepancia (si se presenta) en el análisis de los estudios y crear una lista final de los estudios que van a ser tomados. Evaluar los estudios mediante criterios de evaluación de la calidad, donde se aplican unos valores cuantitativos que indican si el estudio cumple con todos los criterios propuestos, por último, tabular los resultados respectivos de cada estudio.

1.4.2. Ciclo de investigación metodológico

Diagnóstico: Este proceso se enfoca en la recolección de información necesaria para poder llevar a cabo el desarrollo de la propuesta. Debido a que se utilizarán dispositivos SBC basados en arquitectura ARM, se procede a realizar una clasificación de dichos dispositivos, con el fin de obtener las características más importantes de cada uno, determinar si es factible su uso y finalmente realizar una cotización total de los componentes hardware y software necesarios para la construcción del prototipo. Adicionalmente se realiza una evaluación de los controles, herramientas y metodologías existentes que permiten una comunicación anónima entre usuarios conectados, dicha evaluación servirá para clasificar y seleccionar las tecnologías adecuadas para la implementación del prototipo.

Desarrollo e implementación: En este proceso se lleva a cabo el desarrollo de la solución que busca resolver la pregunta de investigación. Inicialmente se selecciona el servicio de red que se va a anonimizar, se procede con la elaboración del diagrama de red y la arquitectura de la comunicación teniendo en cuenta los componentes hardware y software clasificados anteriormente, por último, la construcción del prototipo usando el dispositivo SBC basado en arquitectura ARM seleccionado en el proceso anterior.

1.5. Ciclo de solución del problema

Se requiere un método que guíe la solución del problema mediante el uso del producto de investigación en una situación real. Este método permite el análisis del enfoque de investigación desarrollado a fin de determinar su validez. Para ello se basó en un experimento controlado, el cual consiste en evaluar las diferentes opciones disponibles para lograr un objetivo, que muestre cómo las actividades genéricas del ciclo de solución del problema (diagnóstico, acción y reflexión) se pueden cumplir a partir de las actividades descritas para estos métodos de investigación [3]. Las actividades se realizarán así:

Definición y planeación: en los capítulos 1 y 2 se define y planea el experimento. Esto incluye el personal y el ambiente, determinar las variables independientes (entradas) y las variables dependientes (salidas), escoger el tipo de diseño, preparar la instrumentación (herramientas) y evaluación de validez.

Operación: en los capítulos 3 y 4 se procede con tres pasos principales: preparación, ejecución y validación de datos. Se realizan pruebas funcionales y no funcionales al prototipo mediante una lista de chequeo que logren medir su rendimiento y funcionalidad.

Análisis, interpretación y presentación de datos recolectados: en el capítulo 5 se presentan las conclusiones resultantes de los anteriores capítulos, se presenta el análisis de cada objetivo del proyecto para determinar si fue posible verificar la propuesta planteada y una presentación de los posibles trabajos futuros para continuar con el proyecto [4].

1.6. ESTRUCTURA DEL TRABAJO DE GRADO

Se realizó la elaboración de los siguientes puntos: *Planteamiento del problema*, *pregunta de investigación*, *estado del arte*, *aportes*, *objetivos*, *cronograma* y *presupuesto* correspondientes al anteproyecto, se desarrolló de la siguiente forma.

Para formular el planteamiento del problema se elaboró el *árbol de problemas* especificado en el **Anexo A**, de esta forma se identificaron los problemas centrales a abordar en este proyecto además de la formulación de la *pregunta de investigación*, teniendo esto presente se continuó con la *revisión bibliográfica inicial* en la que *se encontraron 84 artículos* referentes al anonimato de los cuales *10 se clasificaron como primarios*, estos artículos primarios son los que se encuentran en el estado del arte y fueron la base para formular los aportes del proyecto. Partiendo del árbol de problemas *se elaboró el árbol de objetivos* que luego de realizarle un análisis surgió *el objetivo general y los cuatro objetivos específicos*, posteriormente se realizó *el cronograma* con cada una de sus actividades y su correspondiente etapa según la metodología utilizada [3], el tiempo de desarrollo de cada etapa es el siguiente: Diagnostico 12 semanas, desarrollo e implementación 20 semanas y evaluación del producto 4 semanas que en total suman 36 semanas (9 meses) como el tiempo límite para el desarrollo de este proyecto. *Se elaboró un presupuesto inicial* para la construcción del prototipo funcional de este proyecto con un valor estimado de $4’370.000 pesos colombianos, el cual se pretende minimizar para presentar un producto de bajo costo para los usuarios conservando un equilibrio entre precio y beneficios.

Capítulo I: *Introducción*. En este capítulo se presenta la problemática y la justificación que motivan la realización de este proyecto de investigación. Adicionalmente, se presentan los objetivos planteados y la estrategia utilizada para llevar a cabo el proyecto.

Capítulo II: *Revisión bibliográfica.* Se describe el *proceso de investigación* que se llevó a cabo para la revisión de la literatura relevante referente a la privacidad y anonimato de la comunicación en la red, presentando las actividades relacionadas de la revisión de la literatura, los criterios de selección y un análisis de los estudios con sus respectivos resultados, adicionalmente se realizaron estudios para

determinar las herramientas software y hardware adecuadas para el prototipo a desarrollar.

Capítulo III: *Diseño e implementación del prototipo hardware y software.* Inicialmente se realizó el diseño de la arquitectura de la comunicación anónima con su correspondiente diseño de red cumpliendo con los controles de seguridad, se continuo con la implementación y desarrollo del prototipo funcional configurando las herramientas seleccionadas en cada uno de los estudios realizados.

Capítulo IV: *Experimento controlado.* Se realizó un experimento controlado teniendo en cuenta cada uno de los componentes de la comunicación para determinar la seguridad y el anonimato del servicio, adicionalmente se realizó una evaluación para determinar si es viable el desarrollo del prototipo implementado.

Capítulo V: *Conclusiones y trabajos futuros*. Se presentan las conclusiones obtenidas a partir de la realización del trabajo de investigación y posibles trabajos futuros. Como complemento al trabajo presentado, se presentarán los siguientes artefactos: (i) monografía del trabajo de grado, (ii) anexos, (ii) artículo técnico y (iv) un disco compacto con todos los artefactos mencionados anteriormente en formato digital.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

La revisión bibliográfica se llevó a cabo tomando un conjunto de bases de datos bibliográficas gratuitas, con el fin, principalmente, de obtener artículos en el idioma inglés dentro de un intervalo de tiempo entre el año 2012 y 2019 relacionados con temas como son, la privacidad de la información, el anonimato en la red, la navegación anónima, tecnologías para el anonimato en internet y prototipos de navegación anónima usando dispositivos basados en arquitectura ARM.

2.1. REVISIÓN DE LA LITERATURA ACERCA DE LA PRIVACIDAD Y ANONIMATO DE LA INFORMACIÓN

2.1.1. Bases de datos y términos de búsqueda

Para la realización de esta investigación, se seleccionaron ciertas bases de datos que satisfacen una serie de características particulares: motor de bases de datos bibliográficas basado en la web, motor de base de datos de acceso gratuito, motor de bases de datos bibliográficas capaz de realizar búsquedas filtrando por palabras claves y que contengan artículos relacionados con el área de seguridad de la información, el motor de bases de datos asociado con la Universidad del Cauca. La revisión bibliográfica se llevó a cabo en las siguientes bases de datos bibliográficas:

- Springer, sobre el tema de ciencias de la computación (Computer Science).
- ScienceDirect, sobre el tema de ciencias de la computación (Computer Science).
- IEEE Xplore Digital Library.
- Microsoft Academic
- Google Scholar
- EBSCO
- Hindawi
- ACM Digital Library
- International journal of advanced research in computer Science

Cabe resaltar que el motor de Google Scholar y EBSCO recopilan muchos de los estudios que pueden ser encontrados en los demás motores de bases de datos bibliográficas (de ahora en adelante *fuentes bibliográficas*), la diferencia con respecto a EBSCO es la accesibilidad, ya que en este caso se obtuvo acceso por medio de la Universidad del Cauca.

Se utilizaron ciertas palabras claves para filtrar información y encontrar documentos que facilitaron el hallazgo de artículos relacionados con el tema objetivo de la investigación, dichas palabras claves fueron las siguientes: *"privacy", "anonymity", "anonymous", "anonymous browsing", "security", "anonymization", "anonymous information", "anonymous network", "network security", "privacy of information", "cyber security", "privacy in internet", "tor", "vpn", "proxy", "single board computer", "sbc", "arm", "anonymous IoT", "safe", "risk" "privacy issues", "anonymous call".*

Tomando la lista de palabras claves vistas anteriormente como punto de partida y haciendo combinaciones de conectores lógicos como *"AND"* y *"OR"*, se obtuvieron las siguientes cadenas de búsqueda.

Cadena de búsqueda	
1	**(((privacy of information) OR security of information) OR anonymity)**
2	**(((cyber-security) OR anonymous network) OR privacy in internet) AND anonymous)**
3	**((((anonymous browsing) OR tor) OR vpn) AND information)**
4	**(((((single board computer) OR ARM) AND anonymous) OR privacy) OR security)**
5	**(((((single board computer) OR ARM) AND tor) OR vpn) OR anonymous browsing)**

Tabla 1. Cadenas de búsqueda bibliográfica.

Primera cadena: Se encontraron estudios relacionados con las metodologías que pueden ser usadas para preservar la privacidad y el anonimato de la información.

Segunda cadena: Se encontraron resultados relacionados con ciberseguridad orientados a metodologías de protección de la información privada e investigaciones que presentan la seguridad informática como uno de los factores más importantes para los usuarios de internet.

Tercera cadena Se encontraron estudios y proyectos relacionados con las tecnologías de anonimato en la internet como la red tor, vpn, proxys y adicionalmente tecnologías implantadas con criptografía.

Cuarta cadena: se logró recolectar los proyectos e investigaciones realizadas con dispositivos SBC enfocados a la seguridad y privacidad de navegación en internet.

Quinta cadena: se recolectaron proyectos realizados con dispositivos SBC y ARM enfocados a la comunicación anónima y segura haciendo uso de tecnologías como tor, vpn, criptografía entre otros.

2.1.2. Proceso de selección

El proceso de selección está dividido en 6 fases como se muestra en la figura 3:

1. **Búsqueda en las bases de datos**: Se consideran las fuentes bibliográficas relevantes y a partir de éstas se procede a realizar y construir las cadenas de búsqueda con sus respectivas palabras claves.
2. **Eliminar estudios repetidos**. Al realizar la búsqueda de estudios los resultados pueden ser redundantes, por tal motivo se eliminan dichos estudios.
3. **Selección de estudios primarios**. A partir de los artículos encontrados se aplicaron los criterios de inclusión y exclusión (se lee el título, el resumen/abstract, introducción y conclusión si es necesario) los cuales son mencionados en la sección *"Criterios de selección"* para poder extraer los artículos primarios. Posteriormente cada estudio primario es almacenado.
4. **Selección final**. Una vez almacenado cada estudio primario, se procede a realizar una lectura completa de cada estudio.
5. **Eliminar inquietudes**. Si se presentan dudas e inquietudes una vez leídos los artículos, se acude a un experto en el tema para intentar resolver las diferencias, ésto con el fin de almacenar o de eliminar estudios que sean del interés deseado (fase 2.)
6. **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.

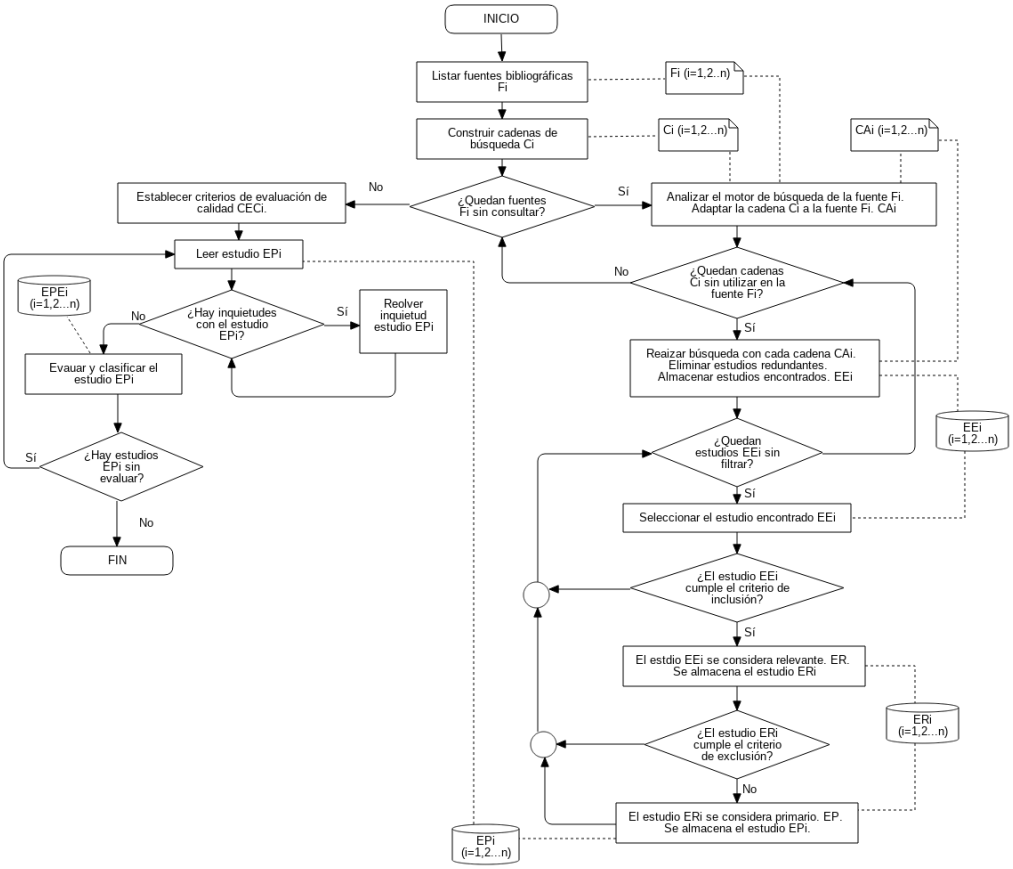


Figura 3. Proceso de selección para obtener estudios primarios [5].

2.2. 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, ésto con el fin de determinar si están relacionados con la privacidad, seguridad y el anonimato en el ámbito de la informática o lo digital, si el artículo menciona el uso de algún método, proceso, herramienta o metodología para mantener la privacidad de la comunicación o el anonimato, y artículos relacionados con el uso de estas tecnologías usando dispositivos basados en arquitectura ARM.

Para determinar qué estudios eran lo suficientemente importantes para considerarlos como estudios primarios, el ***criterio de exclusión*** fue el encargado de excluir artículos que tuvieran los siguientes aspectos: el estudio presenta una herramienta o metodología de anonimato pero no provee suficiente información acerca de su uso o de su aplicación, si el estudio está basado en versiones de una tecnología actualmente desactualizada o descontinuada, si el estudio no presenta

un tipo de evaluación para demostrar los resultados de la metodología aplicada, si el artículo no contempla aspectos como integridad, disponibilidad y accesibilidad de la información, finalmente si el estudio menciona el uso de dispositivos ARM, pero se centra más en lo teórico que en lo práctico.

2.3. 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 estudio presenta algún tipo de contribución: metodología, técnica, herramienta, enfoque, modelo, método, estrategia o framework?
- **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, aplicamos la siguiente valoración: S (sí) = 1, P (parcialmente) = 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**. S, el estudio propone el uso o una nueva metodología, framework, modelo, técnica o herramienta; P, la contribución está presente pero no se describe claramente; N, la contribución no puede ser identificada o no está establecida.
- **CEC 2.** S, el estudio menciona que ha aplicado explícitamente algún método de investigación; P, 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.** S, el estudio presenta de forma detallada el tipo de contribución que ha sido llevado a cabo; P, 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.** S, el estudio presenta un análisis detallado que explique los resultados obtenidos; P, los resultados son explicados brevemente; N, los resultados no pueden ser identificados o no están descritos.

2.4. Estudio de evaluación de calidad

Inicialmente se identificaron 137 estudios en los motores de bases de datos bibliográficas, estos de ahora en adelante se consideran como **encontrados**. Al eliminar los estudios redundantes, 117 estudios fueron considerados como **no repetidos**. Con el criterio de inclusión, 45 estudios fueron considerados como

relevantes, mediante la lectura del título, resumen y palabras claves. Los 45 estudios fueron leídos completamente y con el criterio de exclusión, se obtuvieron 17 **primarios** (tabla 2).

Bases de datos	Estudios			
	Encontrados	**No repetidos**	**Relevantes**	**Primarios**
ScienceDirect	13	10	5	3
IEEE	25	22	16	7
Microsoft Academic	8	5	0	0
Google Scholar	28	24	9	3
EBSCO	30	28	7	2
Hindawi	7	5	2	0
Springer	20	17	3	2
International journal in computer Science	6	6	3	0
Total	137	117	45	17

Tabla 2. Resultados arrojados por las fuentes bibliográficas.

A continuación, la tabla 4 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. Para asignar el valor cualitativo de la calidad se utilizó una escala Likert como se denota en la siguiente tabla.

Símbolo	Evaluación
E	Excelente
MB	Muy bueno
B	Bueno
R	Regular
I	Incompleto

Tabla 3. Escala Likert evaluación cualitativa.

Leyendas usadas: S=sí, N=no, P=parcialmente.

ID	Nombre del estudio	Año de publicación	CEC				Calidad	
			1	2	3	4	Cuantitativo	Cualitativo
1	Secure Portable Virtual Private Network with Rabbit Stream Cipher Algorithm	2018	S	P	P	S	3	Muy Bueno

2	Anonymous and analysable web browsing	2017	S	N	S	S	3	Muy Bueno
3	A combination of Raspberry Pi and SoftEther VPN for controlling research devices via the Internet.	2017	S	N	S	P	2.5	Bueno
4	Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance	2017	S	N	S	P	2.5	Bueno
5	Implementación Del Proyecto De Red Invisible Para El Aseguramiento De Privacidad Y Calidad En Las Comunicaciones	2017	S	P	P	N	2	Regular
6	Implementasi The Onion Router (Tor) Berbasis Virtual Private Network (VPN) pada Raspberry Pi	2017	S	P	P	S	3	Muy Bueno
7	SymBiosis: Anti-Censorship and Anonymous Web-Browsing Ecosystem	2016	S	N	P	S	2.5	Bueno
8	Secure and Anonymous Communication Technique: Formal Model and Its Prototype Implementation	2016	S	N	S	S	3	Muy Bueno
9	A TOR-based anonymous communication approach to secure smart home appliances	2015	S	P	P	S	3	Muy Bueno
10	A Service Protection mechanism Using VPN GW Hiding Techniques	2015	S	N	P	P	2	Regular

11	An efficient and secure anonymous mobility network authentication scheme	2014	S	N	P	S	2.5	Bueno
12	Internet Traffic Privacy Enhancement with Masking: Optimization and Tradeoffs	2014	S	N	P	S	2.5	Bueno
13	Study of cryptography-based cyberspace data security	2014	S	N	P	P	2	Regular
14	The Effectiveness of the Tor Anonymity Network	2014	S	N	P	S	2.5	Bueno
15	A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis	2014	S	N	S	P	2.5	Bueno
16	FreeRec: an anonymous and distributed personalization architecture	2013	S	N	S	S	3	Muy Bueno
17	Predicted Packet Padding for Anonymous Web Browsing Against Traffic Analysis Attacks	2012	S	N	S	S	3	Muy Bueno

Tabla 4. Resultados de cada estudio primario con respecto a los criterios de evaluación de calidad.

2.5. 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:

a) **Escenario de destino:** comunicación en la red, dispositivos ARM, software y aplicaciones.
b) **Tipo de investigación:** estudio empírico, estudio experimental, estudio teórico.
c) **Tipo de contribución:** arquitectura, técnica, herramienta, modelo, prototipo.

Esta sección presenta una evaluación cuantitativa con respecto a los estudios primarios luego de aplicar la evaluación de calidad, los resultados se muestran en

un diagrama de burbujas donde el tamaño de la burbuja indica la cantidad de estudios relacionados con respecto al escenario de destino, tipo de investigación y tipo de contribución.

Esta clasificación se puede ver en las siguientes **figuras 4, 5** y **6**.

La **figura 4** muestra el gráfico de burbujas de los escenarios de destino en relación con el año de publicación, por lo que es posible visualizar el progreso de estudios de la comunicación anónima en los últimos años, también se puede observar que el anonimato es un tema constante de investigación en las comunicaciones de red adicionalmente se puede notar como a medida que avanza el tiempo el anonimato va incursionando en los demás escenarios, en definitiva, el anonimato es un tema que se está implementando en cada escenario nuevo o existente en el mundo de la informática.

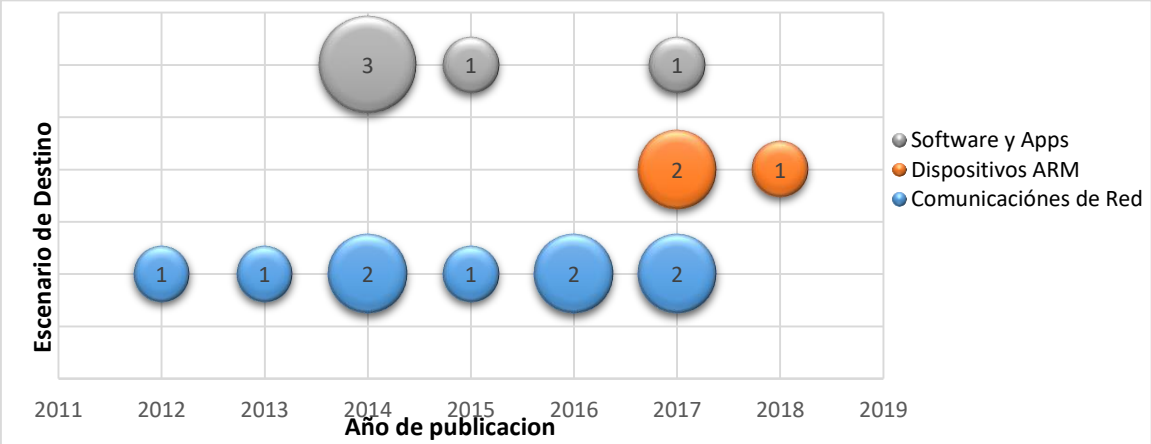


Figura 4. Escenarios de destino por año.

La **figura 5** muestra la relación entre el escenario de destino y el tipo de investigación. La mayoría de estudios primarios seleccionados se caracterizaron como estudios empíricos y tienen como escenario principal las comunicaciones de red. Este resultado apunta a que el anonimato es un tema que ha sido abordado basándose en la práctica, experiencia y observación de los resultados todo esto presuntamente a que en un entorno real de red existen diversas variables que pueden impedir alcanzar el anonimato.

Figura 5. Escenarios de destino vs Tipo de Investigación.

Mientras tanto en la **figura 6** se muestra la relación entre el escenario de destino y el tipo de contribución, por lo cual, se puede apreciar que la mayoría de estudios aportan una técnica o herramienta para alcanzar el anonimato además de mantener las comunicaciones en la red como escenario principal de los estudios de investigación. También se puede analizar como el tema de los dispositivos SBC tiende a un crecimiento ya que se mantiene como uno de los temas principales de investigación a pesar de ser el escenario de destino más reciente.

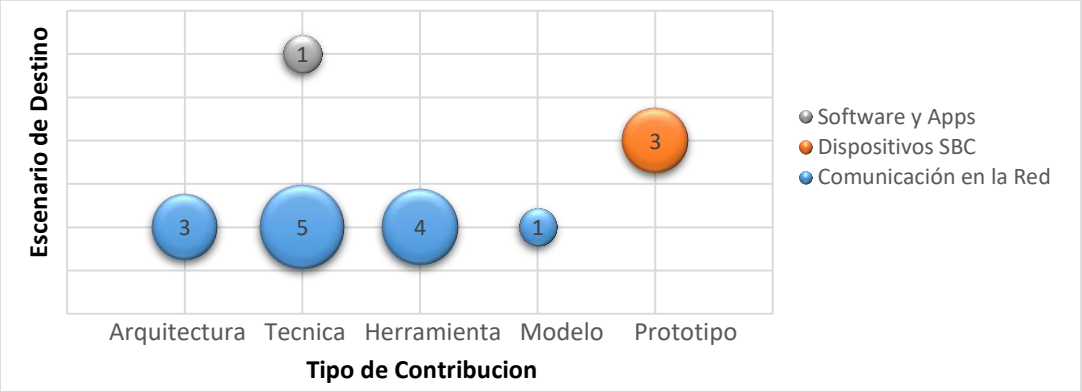


Figura 6. Escenario de destino vs Tipo de Contribución.

2.6. Amenazas a la validez

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

- **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.
- **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.
- **Falta de familiaridad con otros campos:** se definieron cinco 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.
- **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.

2.7. CONCEPTOS PRELIMINARES

2.7.1. Anonimato

El término anonimato proviene de la palabra griega "anonimia", que significa "sin nombre", en el contexto de la informática, el anonimato se define de la siguiente manera: El anonimato de un sujeto significa que *el sujeto no es identificable dentro de un entorno o conjunto de temas*. El anonimato de un usuario significa que el usuario puede usar una tecnología o servicio sin revelar su verdadera identidad.

En el área de las comunicaciones, el anonimato del remitente significa que un mensaje no se puede ser vinculado al remitente, mientras que el anonimato del destinatario implica que un determinado mensaje no puede vincularse al destinatario de ese mensaje [6].

Adicionalmente, según la definición del diccionario de la lengua española el término “Anonimizar” es expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad [7].

2.7.2. Arquitectura de red

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

En telecomunicaciones, la especificación de una arquitectura de red también puede incluir una descripción detallada de los productos y servicios entregados a través de una red de comunicaciones, así como una estructura detallada de tarifas y facturación según la cual se compensan los servicios.

La arquitectura de red de Internet se expresa predominantemente mediante el uso de un conjunto de protocolos de internet como por ejemplo HTTP, TCP, IP y UDP, en lugar de un modelo específico para la interconexión de redes o nodos en la red, o el uso de tipos específicos de enlaces de hardware [8].

2.7.3. Servicios de red

un servicio de red es una aplicación que se ejecuta en la capa de aplicación de red y superior, que proporciona almacenamiento de datos, manipulación, presentación, comunicación u otra capacidad que a menudo se implementa utilizando una arquitectura cliente-servidor o punto a punto basada en protocolos de red. Cada servicio generalmente es proporcionado por un componente de servidor que se ejecuta en una o más computadoras (a menudo una computadora de servidor dedicado que ofrece múltiples servicios) y se accede a través de una red mediante componentes de clientes que se ejecutan en otros dispositivos, sin embargo, los componentes de cliente y servidor pueden ejecutarse en la misma máquina.

Algunos servicios de red son: Servicios de directorio, correo electrónico, servicios de voz ip, mensajería instantánea, juegos en línea, servidores de impresión y redes de sensores inalámbricos entre otros [9].

2.7.4. Red de anonimato

Una red de anonimato permite a los usuarios acceder a la web mientras bloquean cualquier seguimiento o rastreo de su identidad en el ciberespacio. Este tipo de anonimato en línea mueve el tráfico del ciberespacio a través de una red mundial de servidores voluntarios. Las redes de anonimato evitan el análisis del tráfico y la vigilancia de la red, o al menos lo hacen más difícil.

Un ejemplo de software de anonimato que es de código abierto para uso público se conoce como Tor, el software Tor oculta la ubicación y los movimientos del usuario. Otra red de anonimato es Freenet, que permite a los usuarios publicar de forma anónima "sitios libres", así como compartir archivos y chatear en foros [10].

2.7.5. Controles de seguridad

Los controles de seguridad son contramedidas que se implementan en una organización o proyecto con el objetivo de evitar, detectar, contrarrestar o minimizar los riesgos de seguridad a la propiedad física, la información, los sistemas informáticos u otros activos. Actualmente hay sistemas de control denominados estándares o normas, estos estándares permiten a una organización administrar la seguridad de los diferentes tipos de activos. ISO de sus siglas en ingles International Standards Organization, es la organización encargada de desarrollar y publicar estos estándares o normas, existe la norma ISO/IEC 27001 [11] que la responsable de manejar la seguridad de la información, en otras palabras, se ocupa de mantener la disponibilidad, integridad y confidencialidad de la información privada para un usuario u organización.

2.7.6. SBC

Una computadora de una sola placa o single board computer (SBC por sus siglas en inglés) es una computadora completa en la que una única placa de circuito comprende memoria RAM, puertos de entrada y salida, un microprocesador y todas las demás funciones necesarias. Sin embargo, a diferencia de una computadora personal, no se basa en expansiones para otras funciones. Una computadora de una sola placa reduce el costo general del sistema, ya que se reduce la cantidad de placas de circuitos, conectores y circuitos del controlador.

Las computadoras de una sola placa están diseñadas de manera diferente a las computadoras de escritorio o personales, ya que son completamente autónomas. A menudo utilizan una amplia gama de microprocesadores y tienen una mayor compatibilidad con los circuitos integrados [12].

2.8. CONTROLES DE SEGURIDAD PARA COMUNICACIONES DE RED

A continuación, se presentan los controles que se deben implementar para garantizar la seguridad de la información en un entorno de comunicaciones de red según la norma ISO 27002 del año 2013 [13], esta norma se encuentra dividida en su totalidad por 14 dominios y 114 controles con sus correspondientes nombres, los dominios hacen referencia a el área que va a ser gestionada y los controles son las directrices que se deben cumplir para mantener la seguridad de la información. Basándose en los objetivos de este proyecto aplican los dominios 10 y 13 que se refiere respectivamente a la criptografía y la seguridad de las comunicaciones.

2.8.1. Seguridad de las telecomunicaciones

a) Gestión de la seguridad en redes: tiene como objetivo asegurar la protección de la información en las redes y los recursos de tratamiento de la información.
   - **Nombre:** Controles de red.
     Control: Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
   - **Nombre:** Seguridad de los servicios de red.
     Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
   - **Nombre:** Segregación en redes.
     Control: Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.

b) Intercambio de información: tiene como objetivo mantener la seguridad de la información que se transfiere dentro de una organización o cualquier entidad externa.
   - **Nombre:** Políticas y procedimientos de intercambio de información.
     Control: Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
   - **Nombre:** Acuerdos de intercambio de información.
     Control: Deberían establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
   - **Nombre:** Mensajería electrónica.
     Control: La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.
   - **Nombre:** Acuerdos de confidencialidad o no revelación.
     Control: Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.

2.8.2. Criptografía

a) Controles criptográficos: tienen como objetivo garantizar el uso adecuado y eficaz de la criptografía para proteger la disponibilidad, integridad y confidencialidad de la información.

   - **Nombre:** Política de uso de los controles criptográficos.
     Control: Se debería desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.
   - **Nombre:** Gestión de claves.
     Control: Se debería desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

2.9. ESTUDIO DE HERRAMIENTAS PARA LA COMUNICACIÓN ANONIMA

Se realizó la investigación y la clasificación de las herramientas y métodos que se usan actualmente para controlar o mantener el anonimato del usuario mientras navega a través de la red, seguido a esto se realizó el agrupamiento de estas herramientas con respecto a su área de implementación, obteniendo los siguientes campos:

1) Seguridad de la red.
2) Sistemas operativos anónimos.
3) Privacidad del motor de búsqueda.
4) Cliente de mensajería instantánea.
5) Privacidad en el navegador.
6) Cliente de administración de contraseñas.
7) Cifrado de datos.

Actualmente existen herramientas adicionales a las descritas en esta sección, para la búsqueda de estas herramientas se tuvo en cuenta las siguientes características: Principalmente *el anonimato* y *la privacidad*, en términos de funcionamiento se consideraron herramientas con sus *versiones estables* y *con soporte* de sistema, en cuestiones de licencias se consideraron las herramientas con licencia de *software libre*, *herramientas gratis en su versión básica* con la posibilidad de aumentar las características de su privacidad comprando la versión plus, cabe señalar que estas herramientas cuentan con una versión básica que cumple con todos los requisitos para que un usuario mantenga su privacidad y anonimato.

2.9.1. Seguridad de la red

Existen diferentes formas, métodos y herramientas que se pueden utilizar para conservar la seguridad de la red, generalmente cuando un dispositivo se conecta a una red para acceder a sus servicios, se hace a través de un ISP (proveedor de servicios), desde ese momento el ISP tiene cierto nivel de control sobre la conexión, en consecuencia, de esto, el ISP puede rastrear la ubicación y los movimientos realizados por el usuario conectado, además de bloquear ciertos sitios o contenido. Otro tipo de amenazas a la privacidad en la red se conocen como piratas informáticos o individuos que se dedican a explotar las debilidades de las comunicaciones para tener acceso no solo a la información privada de los usuarios sino también a sus dispositivos electrónicos como ordenadores, portátiles, smartphones entre otros. Algunas de las herramientas que se pueden utilizar para mantener la seguridad en la red son las siguientes.

a) La red Tor

Tor por sus siglas en inglés (The Onion Router significa el enrutador de cebolla), está conformada por un grupo de servidores operados por voluntarios que permiten a las personas mejorar su privacidad y seguridad en Internet. Los usuarios de Tor emplean esta red conectándose a través de una serie de túneles virtuales en lugar de hacer una conexión directa, permitiendo así que tanto organizaciones como individuos compartan información a través de redes públicas sin comprometer su

privacidad. De igual modo, Tor es una herramienta efectiva para eludir la censura impuesta en algunos países, permitiendo a sus usuarios llegar a destinos o contenidos no accesibles.

Tor posee como característica principal la implementación del onion routing o enrutamiento cebolla que funciona encapsulando la información dentro de varias capas (cifradas) que se transmiten a través de tres nodos con ubicaciones aleatorias alrededor del mundo, de este modo, aun cuando se intercepten las comunicaciones entre dos nodos es imposible determinar el origen y destino de la comunicación [14].

b) VPN

Es una red privada virtual o VPN (Virtual Private Network) que ayuda a mantener el anonimato en internet al ocultar su actividad real, la VPN protege la identidad del usuario al asignarle una IP anónima y cifrar sus datos. Esto significa que cualquier consulta que envíe a su ISP se cifrará y ya no mostrará su IP real, de esta forma es como trabaja una VPN para mantener el anonimato en línea. Sin embargo, no todas las VPN son iguales, el usuario puede elegir la opción que mejor se ajuste a sus necesidades económicas y de seguridad, puesto que muchas de las VPN son de pago, además, se debe tener cuidado con las VPN gratuitas porque algunas de ellas ganan dinero vendiendo sus datos a los anunciantes.

OpenVPN es una de las mejores herramientas para crear una red privada virtual, desde su lanzamiento en el 2001 es una aplicación de código abierto, es decir, todos pueden usarlo libremente y modificarlo según sea necesario. Utiliza un protocolo de seguridad personalizado que utiliza SSL/TLS[7] para el intercambio de claves, creando conexiones seguras de punto a punto o de sitio a sitio. OpenVPN puede ejecutarse en transportes de túnel del Protocolo de datagramas de usuario (UDP) o del Protocolo de control de transmisión (TCP). Esto hace que su tráfico web sea indistinguible del tráfico que utiliza HTTPS estándar a través de SSL y, por lo tanto, es extremadamente difícil de detectar y bloquear [15].

c) Red I2P

I2P es un acrónimo para su nombre original denominado como proyecto de internet invisible (Invisible Internet Project), la red I2P proporciona privacidad para la comunicación a través de Internet. Muchas actividades que podrían poner en riesgo su privacidad en la Internet pública pueden llevarse a cabo de manera anónima dentro de la red I2P, esta es una red anónima superpuesta, es decir, una red dentro de una red. Está destinado a proteger la comunicación contra la vigilancia de la red y el monitoreo por parte de terceros, como los ISP (Proveedores de Servicios de Internet).

[7] **SSL/TLS**: SSL es el acrónimo de Secure Sockets Layer (capa de puertos seguros), es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas. Utiliza criptografía asimétrica y simétrica para realizar el intercambio de las claves y cifrar la comunicación. TLS (Transport Layer Security, seguridad de la capa de transporte) es una versión actualizada y más segura de SSL.

Estos son algunos de los servicios que ofrece la red I2P [16]:

- Correo electrónico: interfaz de correo web integrada, complemento para correo electrónico sin servidor.
- Navegación web: sitios web anónimos, pasarelas hacia y desde la Internet pública.
- Alojamiento de sitios web: servidor web anónimo integrado.
- Chat en tiempo real: mensajería instantánea y clientes IRC.
- Intercambio de archivos: cliente BitTorrent integrado.

d) Servidores proxy

Un servidor proxy es un intermediario entre su dispositivo e Internet. Es básicamente otra computadora que usas para procesar solicitudes de internet. Es similar a una máquina virtual en concepto, pero es una máquina física completamente separada. Protege su anonimato de manera similar a como lo hace una VPN (ocultando su IP) pero también puede enviar un agente de usuario diferente para mantener su navegador no identificable y bloquear o aceptar cookies, pero evita que pasen a su dispositivo. Actualmente existe en el mercado una gran variedad de servidores proxy según los requerimientos del usuario, existen proxys de pago y gratuitos dependiendo de las características del servicio que ofrecen, cabe mencionar que se debe tener cuidado al utilizar un proxy gratuito ya ellos pueden recolectar la información del usuario para posteriormente venderla. Las siguientes son algunas de las opciones de pago para utilizar un proxy anónimo KProxy, MegaProxy, Proxify, Hide.me entre muchas otras opciones.

2.9.2. Sistemas operativos anónimos

Los sistemas operativos anónimos son un tipo de sistemas operativos que de una u otra forma le brindan seguridad y anonimato al usuario, en otras palabras, es muy difícil vulnerar estos sistemas o infectarlos con un virus, spyware, troyanos o cualquier otro tipo de malware debido a que están especialmente desarrollados y configurados para proteger al usuario de intrusiones externas. A diferencia de la mayoría de sistemas operativos convencionales como Windows, Mac y Ubuntu que son vulnerables.

Además, estos sistemas operativos anónimos están diseñados para proporcionarle seguridad al usuario permitiéndole navegar de forma anónima, proteger su privacidad en línea y fuera de línea, y en algunos casos incluso obtener medidas de seguridad ofensivas similares a las herramientas de Kali Linux. Estos sistemas operativos también se caracterizan porque no envían ninguna información relacionada con sus actividades, ubicación o datos del usuario a ningún sitio web, terceros o incluso a los creadores de los sistemas operativos.

Algunas de las características principales de estas herramientas de privacidad son su capacidad para enrutar todas las conexiones salientes a través de la red Tor, además de una serie de paquetes preinstalados con herramientas que impulsan el anonimato y la seguridad en los servicios de mensajería, correo electrónico y navegación entre otros, además cuenta con herramientas de cifrado avanzado para

su disco duro y dispositivos de almacenamiento externos como unidades USB y CD-ROM. Gracias a todas estas funcionalidades estos sistemas operativos son usados frecuentemente para navegar por la web profunda[8] sin dejar huellas que las agencias y los piratas informáticos puedan encontrar.

a) TAILS

TAILS de las siglas en ingles de The Amnesic Incognito Live System. es una de las mejores herramientas de privacidad desarrollada actualmente, especialmente cuando se habla de un sistema operativo anónimo que no solo respeta la privacidad, sino que la "alienta". Se puede usar directamente desde una memoria USB o un CD sin necesidad de una instalación formal en el ordenador y es considerado un sistema operativo amnésico porque no deja evidencia en el ordenador donde es utilizado, todo esto se debe a que tails no usa el disco duro del ordenador para guardar información o ejecutar el sistema, el único espacio de almacenamiento usado es la memoria RAM que se elimina automáticamente cuando se apaga el ordenador [17].

Es un proyecto parcialmente financiado por Tor, por lo que obviamente promueve el internet sin censura por consiguiente todo el tráfico del sistema se enruta a través de Tor. También incluye bastantes protocolos avanzados de cifrado para cifrar cada parte de su sistema, actividades y dispositivos de almacenamiento, Algunas de las aplicaciones que trae este sistema operativo son el navegador web, cliente de mensajería instantánea, cliente de correo electrónico entre otros, los cuales ya vienen pre-configurados para brindar privacidad y anonimato [18].

b) Whonix

Whonix es otra excelente herramienta de privacidad y anonimato, es un proyecto basado en Tor, y todo el tráfico es enrutado a través de esta red anónima. Además, cuenta con una herramienta personalizada de Debian que se ejecuta dentro de múltiples máquinas virtuales para hacer que las fugas de IP o los ataques de malware sean imposibles.

Es un sistema operativo live es decir que puede ejecutarse directamente desde un disco USB o CD y no queda ningún rastro en el sistema similar a TAILS. En cuanto a las herramientas posee una serie de herramientas anónimas y descentralizadas para correo electrónico, mensajería, además de Tor preinstalado y servidores IRC ocultos [19].

c) Qubes

Qubes es un sistema operativo anónimo que se caracteriza por su exclusiva en la "compartimentación" de cada aplicación y herramienta que se ejecuta en el sistema, es decir que crea una barrera inexpugnable entre cada una de ellas. En resumen, cada aplicación en ejecución se ejecuta de tal forma como si estuviera en un sistema

[8] **Web profunda:** también conocida como deep web, dark web, deepnet, internet invisible entre otros, se refiere a todas la paginas de internet que no están indexadas por los motores de búsqueda, estas representan el 90% de toda la internet y solo pueden ser accedidas con ayuda de un software especial.

"diferente", de manera que, si alguna de las aplicaciones se ve comprometida, el resto del sistema se mantiene a salvo de la amenaza, lo que la convierte en una de las herramientas de privacidad más seguras. Además, otra de las características de Qubes es su capacidad para soportar la ejecución de aplicaciones de diferentes sistemas operativos como Windows, Linux, Fedora e incluso Whonix [20].

d) ParrotOS

Parrot es una distribución de Linux basada en Debían y está diseñado especialmente para pruebas de penetración, mitigación de vulnerabilidades, informática forense y navegación web anónima, este sistema operativo se caracteriza porque brinda un laboratorio completo de herramientas avanzadas para expertos en seguridad informática, por otro lado, incluye herramientas de uso diario como editores, reproductores multimedia, ofimática, entre otros y todo esto acompañado de una interfaz de usuario amigable, en otras palabras fácil de usar. Es un sistema operativo transparente puesto que le muestra exactamente lo que sucede a sus espaldas, es decir que ningún proceso se ejecuta en segundo plano sin que el usuario lo permita. Adicionalmente, tiene preinstaladas herramientas que ayudan a proteger la privacidad del usuario en línea, una de ellas es Anon-surf que le permite al usuario redirigir todo el tráfico a través de la red Tor.
ParrotOS está certificado para ejecutarse en dispositivos que tienen un mínimo de 256 MB de memoria RAM, y está desarrollado para arquitecturas de procesador de 32 bits y 64 bits. Además, está disponible para arquitecturas ARM [21].

2.9.3. Privacidad del motor de búsqueda

Este es un aspecto de la privacidad en línea que se ignora con mayor frecuencia, los motores convencionales de búsqueda rastrean gran parte de los movimientos del usuario en línea, comenzando con las consultas de búsqueda inicial, luego, los sitios web visitados, el tiempo de permanencia en cada sitio, las ubicaciones, preferencias de compra y muchos datos más. Después de recopilar la información se clasifica y se vende a grandes compañías que utilizan estos datos para mejorar sus estrategias de mercadeo, así mismo las redes de espionaje o entes gubernamentales utilizan esta información como un mecanismo para vigilar los movimientos de la población. Por lo tanto, es importante emplear un motor de búsqueda que respete la privacidad, es decir que no lo rastrean ni lo monitorean, y que brinde la privacidad a la que el usuario tiene derecho.

a) Duck duck go

Duck Duck Go es un motor de búsqueda que se caracteriza porque no rastrea ningún aspecto de las búsquedas en línea, en otras palabras, no recopila o rastre la información del usuario y no supervisa el historial de búsqueda, tampoco muestra anuncios en su página de principal o en alguna otra parte. Al utilizar este motor de búsqueda no influyen factores como el PageRank[9] de las páginas, en otros términos, empresas que pagan por la publicidad, sitios posicionados históricamente,

[9] **PageRank:** algoritmo que usa google para asignar una puntuación a cada página web y que influye en el posicionamiento de la misma, en otras palabras, el motor de búsqueda indexa primeramente las páginas que google considera con mejor puntuación.

pero con contenido pobre. Duck Duck Go es una buena herramienta para conservar la privacidad de las búsquedas en línea y lo ha sido desde su fundación en el año 2008 [22].

b) Startpage

Startpage es un motor de búsqueda que retorna los mismos los resultados de "Google" pero sin su naturaleza intrusiva, es conocido que Google es probablemente el motor de búsqueda más popular actualmente, de este modo lo que hace StartPage cuando se ingresa una consulta de búsqueda es enviarla primero a Google y después mostrar los resultados al usuario, es decir que actúa como un intermediario. Además, no almacena ninguna dirección IP, historial de búsqueda, ni ninguna otra cosa que pueda usarse para identificar o incluso personalizar las preferencias del usuario, también es totalmente libre de anuncios y al igual que con DuckDuckGo, como no hay personalización, tienes acceso a los mismos resultados de búsqueda que los demás, sin ningún tipo de filtros [23].

c) Torch

Torch es otro motor de búsqueda que no recopila información sobre el usuario, pero su diferencia con respecto a Duck Duck Go y Startpage se debe a que Torch muestra entre sus resultados enlaces onion, que son los enlaces pertenecientes a la web profunda. No rastrea o monitorea las búsquedas, es completamente seguro, aunque muestra anuncios estos no son personalizados, sino anuncios universales que son iguales para todos los usuarios, otra característica que lo identifica es su Media Grabber, el cual es un descargador que le permite bajar cualquier tipo de medio digital que encuentre, en resumen, es un motor de búsqueda privado, anónimo y permite buscar enlaces en la web profunda [24].

d) Gibiru

Gibiru es un motor de búsqueda desarrollado en el año 2009 enfocado a la privacidad del usuario, tiene como lema “unfiltered private search” es decir búsqueda privada sin censura, este sistema de búsqueda utiliza un algoritmo modificado de Google para realizar sus consultas, además, no permite instalar cookies de personalización y seguimiento, tampoco se registra ninguna dirección ip, posee un cifrado HTTPS de 256 bits y también se puede combinar con una VPN o Proxy separada, por último, dispone de una opción llamada “sin censura” que también permite obtener los resultados de las páginas que han sido censuradas por los otros buscadores, y cuenta aplicación móvil para Android y Iphone [25].

2.9.4. Cliente de mensajería instantánea

Los servicios de correo electrónico y mensajería instantánea son las herramientas por donde frecuentemente viaja información sensible como por ejemplo archivos o comunicaciones confidenciales, proyectos no patentados, trabajos de investigación y mucha de la información personal del usuario lo cual convierte a estos servicios en un gran objetivo de ataque por parte los ciber-delincuentes o redes de espionaje. Los correos electrónicos permiten determinar las rutinas del usuario, es decir, cuando y donde abre una sesión de correo electrónico, enlaces de interés, contactos, hora exacta de cada una de las actividades en el perfil y muchos datos

más que están ligados al tiempo en la vida real del usuario. Además, los proveedores de correo electrónico como Gmail y Yahoo recopilan para posteriormente venderla [26]. Por otra parte, existe una solución rápida para la mensajería instantánea anónima y se conoce como correo temporal o correo desechable, es un servicio que permite a un usuario enviar y recibir correos electrónicos en una dirección temporal que caduca después de que transcurre cierto período de tiempo algunos ejemplos de esto son temp-mail.org, correotemporal.org, yopmail.com, mohmal.com entre muchos otros con diferentes funcionalidades las cuales dependen del proveedor del servicio.

a) ProtonMail

ProtonMail es un cliente de correo electrónico anónimo que respeta la privacidad del usuario, con sus servidores físicos alojados en Suiza donde actualmente no existen tantas regulaciones por parte del gobierno, de este modo se evita que alguna agencia del gobierno o de terceros tome ciertas acciones para forzar a ProtonMail compartir el contenido de sus servidores. Es considerado un cliente de correo inexpugnable [27]. Esta herramienta se caracteriza porque no guarda ningún registro de IP o correo electrónico, tiene cifrado de extremo a extremo para garantizar la seguridad de la comunicación de los correos, además es de código abierto, por lo que el código y la política de no registros pueden ser verificados [28].

b) Paranoid

Paranoid es un cliente de correo electrónico anónimo que brinda seguridad especialmente cuando se trata de cifrado, en primer lugar, utiliza la "Infraestructura Paranoica" para enrutar cualquier comunicación que se envíe a través de la plataforma, en otras palabras, aunque el usuario se encuentre en su propia dirección IP personal no hay riesgo de seguridad para los correos electrónicos de entrada o salida porque todo es enrutado a través de una infraestructura que protege la IP del usuario. Para mantener la seguridad, cada actividad de correo electrónico se realiza detrás de la capa NAT, empezando por el cifrado, el descifrado y las claves privadas. Tiene un cifrado garantizado de dos tiempos y se asegura que todos los correos electrónicos estén cifrados, aunque el remitente envié un mensaje sin cifrar Paranoid se encarga de cifrarlo usando las claves públicas de los usuarios [29].

c) OnionMail

OnionMail es un servicio de correo que utiliza la red Tor, proporciona un cifrado completo de todos los correos electrónicos al no usar los servidores SMTP tradicionales para enviar y recibir correos, por el contrario, los correos son enrutados a través de la red Tor. Usa cifrado asimétrico para la protección dual de los correos electrónicos, incluye detección y filtrado de spam de nivel avanzado en los buzones, además permite seleccionar el servidor de entrada y la posibilidad de salir de los nodos. Teniendo en cuenta que utiliza un enrutamiento de cebolla, no hay duda que está fuera de la red y es segura, especialmente del gobierno, la censura y las normativas [30].

d) Ricochet

Ricochet es un servicio de mensajería instantánea que usa la red Tor para la comunicación entre usuarios, de este modo no depende de servidores de mensajería. No existen nombres de usuario o correos electrónicos sino números aleatorios los cuales se usan para contactar a las personas. Todos los mensajes, lista de contactos y demás se encuentran alojados en el ordenador del usuario en lugar de servidores o en la nube, por lo tanto, no puede ser accedido de forma remota. Además, cuenta con cifrado de extremo a extremo, de este modo la interceptación de estos medios es inútil, ya que nadie más puede descifrar los mensajes, excepto los remitentes y los destinatarios. Es compatible con sistemas operativos Windows, Mac y Linux [31].

e) OnionShare

Onionshare es una plataforma anónima para compartir archivos y funciona de la siguiente manera, cuando se comparte un archivo se crea automáticamente un servidor web temporal en la red Tor con su correspondiente URL larga y aleatoria que es similar a un enlace de descarga, un punto a tener en cuenta es que el ordenador actúa como el “host” para el enlace de descarga, por lo que no tiene que confiarle ningún servicio a terceros para alojar sus archivos, además los archivos nunca se cargan en línea. Adicionalmente, no tiene que compartir su nombre, correo electrónico o cualquier otra cosa con el receptor, por lo que mantiene su identidad en secreto, incluso tiene un modo oculto que protege la URL contra los nodos Tor ocultos que pueden intentar obtener acceso al archivo. Sin mencionar que los archivos están cifrados de extremo a extremo y es una herramienta de código abierto disponible para Windows, Mac y Linux [32].

2.9.5. Privacidad en el navegador

El navegador web es una de las herramientas frecuentemente usadas para conectarse a internet y navegar por los sitios web, por lo que, también puede verse comprometido o ser vulnerado. Un navegador seguro básicamente está conformado por herramientas de privacidad que aseguran que las actividades en la web, el historial, caché, información de ubicación, hábitos de navegación o contraseñas guardadas no se filtren a terceros. Estas medidas de seguridad son implementadas por ciertos navegadores o, en ocasiones, por complementos y extensiones de terceros.

a) Navegador Tor

El navegador Tor enruta todo su tráfico a través de la red Onion. La red Onion es la parte de la web, que no está censurada y es independiente, a diferencia de la red superficial a la que comúnmente se accede a través de la world wide web (www) donde cada sitio y sus usuarios están sujetos a leyes y regulaciones establecidas por cada país. Enruta todo su tráfico a través de una serie de "relés" que son casi imposibles de conectar entre sí, por lo que es difícil rastrear su ruta de comunicación en la web, en pocas palabras, el navegador Tor no recopila información y no permite que nadie espíe sus actividades, ubicación o cualquier otra información relacionada con el usuario, además, deshabilita los componentes javascript y no registra su caché o cookies. Finalmente se caracteriza por ser un proyecto gratuito, de código

abierto dirigido por voluntarios que permite navegar por los enlaces de la web y la web profunda [14].

b) Navegador EPIC

Una de las características exclusivas de este navegador que lo convierten en una excelente herramienta de privacidad es su "aislamiento", lo que significa que cada conexión saliente es un proceso independiente, por lo que vulnerar una conexión no conducirá a que se rompa toda la conexión en general, además, tiene la capacidad de bloquear cada elemento de un sitio web que puede usarse para rastrear las actividades o consultas, estos elementos incluyen almacenamiento HTML 5 y diferentes tipos de cookies. También tiene un proxy incorporado para ayudar a enmascarar la dirección IP en el caso que el usuario no esté usando una VPN, aunque también puede usar el proxy propio de EPIC con una VPN adicional.
Otras de sus características es que no registra el historial, contraseñas, correcciones ortográficas, caché del DNS, caché web o cualquier otro tipo de información que pueda comprometer la privacidad, de igual forma, no envía datos de referencia a los sitios web cuando salta de un enlace del motor de búsqueda a otro sitio, y tiene como principal característica permitir espiar a tus espías al mostrar quién o qué sitios están rastreando la conexión. Una de sus limitantes es que actualmente solo está desarrollado para sistemas operativos Windows y Mac [33].

c) Brave

Brave es un proyecto en conjunto del fundador de Javascript y el cofundador de Mozilla, este navegador se caracteriza porque detecta automáticamente el malware además de otras amenazas de seguridad evitando que violen la privacidad de los usuarios, también deshabilita los complementos dañinos que vienen por defecto. En cuanto a información privada el navegador Brave no accede ni almacena datos personales, a diferencia de los navegadores tradicionales como Chrome que si registran esta información. También es capaz de bloquear las huellas dactilares, lo que evita que los sitios rastreen e identifiquen a los usuarios y sus actividades en internet, posee un bloqueador de anuncios y permite al usuario personalizar el navegador en dos modos: para sitios individuales y sitios en general. Finalmente, es compatible con sistemas operativos como Windows, Mac y Linux, además su versión de escritorio es compatible con casi todas las extensiones de la tienda de Chrome [34].

d) Midori

Midori es un navegador web de código abierto desarrollado en Vala y C con una versión estable inicial desde 2007, es actualmente el navegador predeterminado en muchas distribuciones de Linux, incluidos Manjaro Linux, sistema operativo elemental, SliTaz Linux, Bodhi Linux, Trisqel Mini, SystemRescue CD, entre otros. Este es un navegador web gratuito y liviano que posee una herramienta de privacidad incorporada con ciertas características como deshabilitación de scripts, bloqueo de cookies de terceros, además de un bloqueador de anuncios integrado y un administrador de cookies. La velocidad de lanzamiento de Midori es similar a la de Chromium, posee una interfaz de usuario sencilla con opciones para administrar la barra de menú, la barra de título y la barra de marcadores, el lado negativo de

Midori se debe al hecho de que hay ciertos complementos adicionales con efectos visuales y animaciones en la interfaz de usuario que pueden hacerlo disminuir su rendimiento, por último, actualmente está disponible para sistemas operativos Linux, para dispositivos Android está en su versión beta y para el sistema operativo Windows se encuentra en desarrollo [35].

2.9.6. Cliente de administración de contraseñas

Si hablamos de privacidad en línea las contraseñas son parte fundamental de la seguridad del usuario, lamentablemente es uno de los aspectos más descuidados por el usuario y no se toma con la importancia que merece, algunas de las malas prácticas que suelen hacer los usuarios es colocar la misma contraseña para diferentes cuentas en línea, no cambiar la contraseña periódicamente, además de las más comunes como crear contraseñas fáciles de recordar usando datos personales como nombre, documentos de identidad etc, de igual forma escribir todas sus contraseñas en un archivo de texto y guardarlas en su computadora es la peor manera de mantener sus contraseñas seguras porque cualquier persona con acceso físico podría echar un vistazo. En resumen, el usuario necesita un lugar privado para mantener sus contraseñas seguras y organizadas, y eso es lo que proporcionan las siguientes herramientas.

a) LastPass

LastPass es una herramienta muy completa para proteger contraseñas, la cual tiene tanto una versión gratuita como una versión premium, la versión gratuita cuenta con suficientes características para la mayoría de los usuarios, esta herramienta es una bóveda segura que guarda todas las contraseñas automáticamente de varios sitios web cada vez que el usuario inicie sesión en dichos sitios o también se pueden agregar contraseñas manualmente, debido a que todo está en la nube, nunca olvidará una contraseña, sin importar cuántas décadas más tarde la necesite.
Además de actuar como bóveda, también actúa como una "llave maestra", lo que significa que el usuario no necesita recordar cientos de contraseñas para todos sus sitios, en su lugar simplemente debe recordar la contraseña maestra que estableció para LastPass, y esta contraseña completará automáticamente la contraseña de cualquier sitio en sus páginas de inicio de sesión.

También posee algunas funciones avanzadas, como guardar contraseñas de WiFi, crear perfiles de tarjetas de crédito para que se completen fácilmente, e incluso "contactos de emergencia", obviamente, también está disponible la autenticación de 2 factores, esta herramienta utiliza cifrado de grado militar AES 256 junto con el hash SHA-256 para cifrar todo lo que guardamos en la plataforma. Además, todo lo que guardamos en esta herramienta siempre es un secreto, incluso para LastPass. Las claves privadas de cifrado y descifrado están basadas en el dispositivo, por lo que incluso LastPass no puede acceder a las contraseñas guardadas, junto con la contraseña maestra. En conclusión, es una de las mejores herramientas de privacidad cuando se trata de administración de contraseñas [36].

b) 1Password

1Password es una herramienta Premium que tiene un período de prueba gratuito de 30 días y cuenta con tres planes diferentes, para usuarios individuales, familias o grandes empresas. Como la mayoría de administradores de contraseñas, también utiliza una contraseña maestra que no se guarda en el servidor de 1Password o en ningún otro servidor, pero si en el dispositivo del usuario y esta única contraseña es la que se utiliza para iniciar sesión en la herramienta. La cual permite guardar contraseñas ilimitadas y autocompletarlas en los sitios web, también permite crear bóvedas separadas y compartir las partes seleccionadas con hasta 20 miembros de su equipo o familia. También posee una característica llamada "Modo de viaje", que elimina temporalmente cualquier bóveda que el usuario crea que debe ocultarse para escapar de una situación hostil o algún tipo de investigación por ejemplo las inspecciones como en los aeropuertos. En cuanto a la seguridad utiliza el cifrado de 256 bits, aunque una de sus características avanzadas es su clave secreta de 34 caracteres, que afirman que elimina la necesidad del segundo factor de autenticación y hace que sea muy difícil acceder sin autorización a la cuenta de 1Password [37].

c) DashLane

Dashlane es una herramienta Premium que tiene una versión gratuita que le permite guardar 50 contraseñas o el plan Premium con almacenamiento ilimitado, los conceptos básicos son los mismos, guarda y rellena automáticamente las contraseñas de los sitios web. Sin embargo, hay algunas características que lo diferencian de los anteriores administradores de contraseñas. Su monitor Dark-web es una de esas características. La plataforma escanea automáticamente la web oscura, así como otros sitios en busca de información filtrada. Siempre que haya una violación, o se encuentre que su información está en una de esas bases de datos filtradas, se le avisa, lo que le permite cambiar la contraseña al instante. En segundo lugar, le permite compartir sus cuentas con familiares, compañeros de trabajo y amigos sin tener que revelar su contraseña. Adicionalmente su interfaz de usuario le permite validar y manipular información como contraseñas reutilizadas, contraseñas débiles e incluso contraseñas comprometidas que se pueden monitorear de un vistazo. Por otro lado, el plan de pago viene con una VPN incorporada que permite acceder a direcciones IP de 23 países, e incluso cuenta con funciones avanzadas como el interruptor Kill. Kill-switch es una función que desactiva automáticamente toda su conexión a Internet en caso de que la conexión VPN se caiga, por lo que nunca estará desprotegido, además permite conectar dispositivos ilimitados a la VPN. También tiene una función de "Nota segura" que permite a los usuarios almacenar información confidencial y notas, además de contraseñas seguras y cifradas. También cuenta con generador de contraseñas en caso de necesitarlo [38].

d) Keeper

Keeper es un administrador de contraseñas rápido y completo, tiene una interfaz web robusta y fácil de usar, almacena archivos y documentos de cualquier tipo, es compatible con todos los métodos de autenticación de dos factores conocidos en la actualidad incluyendo TOTP, SMS, huellas dactilares, Face ID y U2F. También

cuenta con una versión gratuita que permite agregar un número ilimitado de contraseñas y detalles de pago en un solo dispositivo, posee una herramienta de auditoría de contraseña incorporada y está disponible para las siguientes plataformas: Windows, Mac, iOS, Android, Linux, Chrome OS, Windows Phone, Kindle y BlackBerry [39].

2.9.7. Cifrado de datos

Un área que igualmente es importante mantener su privacidad es la seguridad en el disco, archivos y carpetas porque ahí es donde residen todos archivos privados y datos del usuario. Debido a que la mayoría de los archivos o discos no están cifrados, siempre existe el riesgo de que alguien obtenga acceso físico a su sistema y los robe, de igual forma si el sistema es vulnerado de forma remota. Por tales motivos se necesita proteger los datos, porque cuando están cifrados, incluso si alguien obtiene acceso a su sistema o instala un virus, los datos que obtendrían no serán de ninguna utilidad y el usuario se mantendrá a salvo.

a) VeraCrypt

Es una herramienta de cifrado de discos y archivos, su principal característica es el "cifrado sobre la marcha", lo que significa que no descifra los archivos con anterioridad, sino exactamente en el momento que se necesita el archivo para leer, escribir o compartir. El descifrado se realiza en la memoria RAM cuando se está utilizando el archivo, por lo que los archivos descifrados nunca residen en su disco duro. También están disponibles otras funciones avanzadas, como un "volumen oculto" dentro de un volumen cifrado estándar y un sistema operativo completamente oculto en su totalidad. Otras de sus características es que no "ralentiza" los discos o los archivos cifrados, es de código abierto, es gratuito y cuenta con soporte para diferentes distribuciones de Windows, MacOS y Linux [40].

b) AxCrypt

Es una herramienta software de cifrado similar al de Veracrypt, aunque tiene una versión gratuita como una de pago, algunas de sus características principales incluyen su capacidad para interactuar y trabajar con archivos y carpetas cifrados con la misma facilidad que con los archivos no cifrados, todo lo que necesita para abrir es doble clic. Además, cuenta con soporte móvil que permite acceder a los archivos cifrados en dispositivos móviles, de igual forma tiene un sistema incorporado que elimina todos los archivos temporales de caché y de texto sin formato que pueden poner en peligro la seguridad del sistema, finalmente cuenta con el cifrado de 128 bits y el ajuste de clave iterativo, garantizando protección contra fuerza bruta o ataques similares, también dispone de soporte para sistemas operativos windows, macOS, android y IOS [41].

c) BitLocker

BitLocker es una herramienta de protección de información desarrollada para sistemas operativos Windows que asegura los datos cifrándolos, esta herramienta difiere de la mayoría de los otros programas de cifrado porque utiliza su inicio de sesión para proteger los datos, no se necesitan contraseñas adicionales. Una vez que haya iniciado sesión, sus archivos se podrán visualizar normalmente y una vez

que cierre sesión todo estará seguro. Finalmente, esta herramienta cuenta con una función de protección de información que se integra con el sistema operativo para enfrentar amenazas como robo de datos o exposición de computadoras perdidas, robadas o desmanteladas de manera inapropiada [42].

d) ZuluCrypt

ZuluCrypt es una herramienta simple que brinda protección a la información del usuario, rica en funciones y potente en el cifrado de cualquier tipo de dato por ejemplo archivos de imagen, discos duros y memorias USB entre otros, también permite administrar los volúmenes cifrados LUKS, TrueCrypt, VeraCrypt y BitLocker de Microsoft. ZuluCrypt incluye una herramienta llamada ZuluMount que es una de propósito general que puede montar y desmontar volúmenes cifrados compatibles, así como los volúmenes no cifrados. Por último, es de código abierto y actualmente solo está desarrollado para el sistema operativo Linux [43].

2.9.8. Criterios de evaluación de herramientas

El objetivo de estos criterios es asegurar una apropiada evaluación de cada una de las herramientas presentadas anteriormente, los siguientes criterios están basados teniendo en cuenta los objetivos de este proyecto. Primeramente, se definieron las características que debe poseer cada una de las herramientas, en este caso fueron las siguientes: *anonimato, flexibilidad, compatibilidad ARM, costos y periodo de actualización*. Cada herramienta cuenta con especificaciones diferentes y cada especificación posee su correspondiente valor, es decir que cada característica aporta un valor que al sumarlo finalmente genera el puntaje para cada herramienta. En el proceso de asignación de valores cabe señalar que las especificaciones de cada característica son mutuamente excluyentes con excepción de la característica anonimato la cual sus especificaciones son incluyentes dependiendo de la herramienta, es decir que una herramienta puede cumplir con 1, 2, 3 o 4 especificaciones de anonimato. A continuación, en la **tabla 5** se muestra la distribución mencionada.

Característica	**Especificación**		**Valor**	
Anonimato	**A1**	Técnicas de ocultamiento de los identificadores de la comunicación.	$0 < x \leq 1{,}25$	$\sum_{i=0}^{4} Ai$
	A2	Técnicas de protección del contenido de la comunicación.	$0 < x \leq 1{,}25$	
	A3	Técnicas de protección de los servidores o nodos de la comunicación.	$0 < x \leq 1{,}25$	
	A4	Técnicas de protección contra ataques de red.	$0 < x \leq 1{,}25$	

Flexibilidad	**F1**	No permite configurar la privacidad.	0
	F2	Permite configurar la privacidad solo para sí misma.	0,25
	F3	Permite configurar la privacidad para algunos servicios de red.	0,5
	F4	Permite configurar la privacidad para todos los servicios de red	1
Compatibilidad ARM	**CA1**	No es compatible.	0
	CA2	Es compatible y se consume como un servicio externo.	0,5
	CA3	Es compatible y se instala en el sistema operativo.	1
Costos	**C1**	Es completamente de paga.	0
	C2	Solo versión de prueba gratuita.	0,25
	C3	Solo versión básica gratuita.	0.5
	C4	Es completamente gratuita.	1
Periodo de actualización	**P1**	Anual	0
	P2	Semestral	0,25
	P3	Mensual	0.5
	P4	Semanal	1

Tabla 5. Criterios de evaluación de herramientas.

2.9.9. Resultados de la evaluación de herramientas

Para el análisis posterior de los resultados se transformó el puntaje obtenido por cada herramienta evaluada a su valor porcentual, recapitulando contamos con 5 características que aportan cada una un valor máximo establecido de la siguiente forma: *Anonimato*(**5**) debido a que es la característica principal de todo el proyecto, las siguientes características *flexibilidad*(**1**), *compatibilidad*(**1**), *costos*(**1**) y *periodo de actualización*(**1**) que aportan en total **4**, es decir que el valor máximo que podría obtener una herramienta es **9** que corresponde al **100%**. Finalmente se realizó la valoración porcentual y cualitativa para clasificar cada una de las herramientas evaluadas como se observa en la siguiente **tabla 6**.

Valoración (%)	Cualitativo
75 < x ≤ 100	Muy Alto
50 < x ≤ 75	Alto
25 < x ≤ 50	Medio
0 < x ≤ 25	Bajo

Tabla 6. Clasificación para cada herramienta.

A continuación, en la **tabla 7** se presentan los resultados de la evaluación con el puntaje obtenido por cada herramienta y su correspondiente valor porcentual, asimismo se muestran las herramientas ordenadas de mayor a menor puntaje en su correspondiente área.

Herramienta	Anonimato				Flexibilidad				Compatibilidad			Costos				Periodo				Puntaje	Porcentaje
	A1	A2	A3	A4	F1	F2	F3	F4	CA1	CA2	CA3	C1	C2	C3	C4	P1	P2	P3	P4		
Red Tor	1,2	1,2	1	1,1	NA	NA	NA	1	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	8,5	94,4
VPN	1	1,2	1	1	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	7,2	80,0
Red I2P	1	1,1	0,8	0,8	NA	NA	NA	1	NA	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	6,95	77,2
Servidor proxy	0,8	0,7	0,6	0,7	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	5,8	64,4
Parrot	1,2	1,2	1	1,1	NA	NA	0,5	NA	NA	NA	1	NA	NA	NA	1	NA	NA	0,5	NA	7,5	83,3
Qubes	1,2	1,2	1	1,2	NA	NA	NA	1	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	7,1	78,9
TAILS	1,2	1,2	1	1,1	NA	NA	NA	1	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	7	77,8
Whonix	1,2	1,2	1	1	NA	NA	NA	1	0	NA	NA	NA	NA	NA	1	0	NA	NA	NA	6,4	71,1
Duck duck go	0,2	0,4	0,5	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	NA	1	3,7	41,1
StartPage	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	3	33,3
Gibiru	0,2	0,2	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	2,9	32,2
Torch	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	0,25	NA	NA	2,75	30,6
OnionShare	0,6	0,7	0,8	0,4	NA	0,25	NA	NA	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	5,75	63,9
ProtonMail	0,6	0,7	1	0,4	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,95	55,0
Ricochet	0,6	0,5	0,5	0,2	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	4,05	45,0
OnionMail	0,6	0,5	0,6	0,4	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	3,85	42,8
Paranoid	0,6	0,7	0,5	0,2	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	3,75	41,7
Tor Browser	1,1	1,2	0,9	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	6,1	67,8
EPIC Browser	1	1	0,8	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	5,7	63,3
Midori	0,4	0,4	0,3	0,3	NA	NA	0,5	NA	NA	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	4,15	46,1
Brave	0,6	0,6	0,6	0,4	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	0,25	NA	NA	3,95	43,9
LastPass	0,5	0,8	0,4	0,6	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,55	50,6
DashLane	0,5	0,7	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,35	48,3
1Password	0,5	0,6	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,25	47,2
Keeper	0,5	0,5	0,4	0,4	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,05	45,0
VeraCrypt	NA	1	NA	0,3	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	3,55	39,4
BitLocker	NA	1	NA	0,3	0	NA	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	2,8	31,1
AxCrypt	NA	0,9	NA	0,3	0	NA	NA	NA	0	NA	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	2,2	24,4
ZuluCrypt	NA	0,7	NA	0,2	0	NA	NA	NA	0	NA	NA	NA	NA	NA	1	NA	0,25	NA	NA	2,15	23,9

Leyenda: NA = No Aplica.

Tabla 7. Evaluación de herramientas.

En el ***anexo D*** se muestra la tabla completa de la evaluación de todas las herramientas con su correspondiente área y valoración cualitativa.
En el ***anexo E*** se muestra la tabla completa con todas las herramientas ordenadas de mayor a menor puntaje excluyendo su área.

2.9.10. Análisis de la evaluación de herramientas

Para este estudio fueron evaluadas 29 herramientas en total de las cuales 11 resultaron ser no compatibles con la arquitectura ARM, estas se muestran sombreadas (color gris) en la anterior ***tabla 7*** en la columna de compatibilidad con el valor de 0, por dicho motivo estas herramientas fueron descartadas para el desarrollo de este proyecto, sin embargo, cabe señalar que son herramientas que brindan un alto nivel de anonimato ya que han sido diseñadas específicamente con el objetivo de mantener la privacidad de las personas en la red y actualmente son herramientas comúnmente usadas por personas en las que su trabajo u ocupación requiere la protección de su identidad como por ejemplo: *periodistas, políticos, agentes de gobierno, entre otros.* Continuando con el análisis de resultados, se obtuvo un conjunto base de 18 herramientas apropiadas para construir la arquitectura de comunicación anónima, a continuación, en la **tabla 8** se presenta el

ranking de las mejores 5 herramientas cada una con su correspondiente puntaje, valoración porcentual y cualitativa.

No	Herramienta	Puntaje	Porcentaje	Cualitativo
1	Red Tor	8,5	94,4	Muy Alto
2	Parrot	7,5	83,3	Muy Alto
3	VPN	7,2	80,0	Muy Alto
4	Red I2P	6,95	77,2	Muy Alto
5	Servidor Proxy	5,8	64,4	Muy Alto

Tabla 8. Top 5 de las herramientas.

De la **tabla 8** se puede observar como el *proyecto Tor* está presente en 2 de las 5 herramientas del ranking (filas 1 y 2), teniendo en cuenta que el sistema operativo Parrot utiliza internamente la red Tor para enrutar su tráfico, por otro lado, se puede notar implícitamente la presencia de métodos criptográficos que protegen el contenido de la comunicación, además ocultan la verdadera dirección ip del usuario y protegen la privacidad de la ruta de la comunicación, por último, en el área denominada como *seguridad de la red*, posee la mayor cantidad de herramientas posicionadas en el top 5 (anterior *tabla 8*) en comparación a las demás áreas, en otros términos, *seguridad de la red* (4) y *Sistemas operativos anónimos* (1). Esto se puede apreciar mejor en la siguiente **tabla 9** donde se presenta cada herramienta con su correspondiente área, además de las 5 mejores herramientas resaltadas en color verde.

Área	Herramienta
Seguridad de la red	Red Tor
	VPN
	Red I2P
	Servidor proxy
Sistemas operativos anónimos	Parrot
	Qubes
	TAILS
	Whonix
Privacidad del motor de búsqueda	Duck duck go
	StartPage
	Gibiru
	Torch
Cliente de mensajería instantánea	OnionShare
	Ricochet
	ProtonMail

	OnionMail
	Paranoid
Privacidad en el navegador	Tor Browser
	EPIC Browser
	Midori
	Brave
Cliente de administración de contraseñas	LastPass
	DashLane
	1Password
	Keeper
Cifrado de datos	VeraCrypt
	ZuluCrypt
	BitLocker
	AxCrypt

Tabla 9. Áreas con sus respectivas herramientas.

Como ya se había mencionado antes se agrupo cada herramienta dependiendo de su área de implementación, esto se hizo debido a que cada una de las herramientas brinda privacidad a cierta área del usuario que navega por el ciberespacio, sumado a esto cada herramienta opera de forma distinta y proporciona un nivel diferente de anonimato, pensando en proteger cada aspecto del usuario se realizó la selección de la mejor herramienta por área como se muestra en la siguiente **tabla 10** cabe recordar que las herramientas incompatibles con la arquitectura ARM fueron descartadas.

Área	Herramienta	Puntaje	Porcentaje	Cualitativo
Seguridad de la red	Red Tor	8,5	94,4	Muy Alto
Sistemas operativos anónimos	Parrot	7,5	83,3	Muy Alto
Privacidad en el motor de búsqueda	Duck Duck Go	3,7	41,1	Medio
Cliente de mensajería instantánea	OnionShare	5,75	63,9	Alto
Privacidad en el navegador	Midori	4,15	46,1	Medio
Cliente de administración de contraseñas	LastPass	4,55	50,6	Alto
Cifrado de datos	VeraCrypt	3,45	38,3	Medio

Tabla 10. La mejor herramienta de cada área.

Según la ***tabla 10***, los parámetros de este estudio y los requerimientos de este proyecto, el conjunto de herramientas presentadas, son la mejor opción para que un usuario mantenga anónima su identidad en la red, en conclusión, para lograr el anonimato se debe poder gestionar la seguridad de cada aspecto o área involucrada en la comunicación dado que la fuga de información más pequeña puede provocar

un efecto domino que al final cause pérdida de información privada o exposición de los datos reales del usuario. Cabe resaltar que las herramientas seleccionadas no tienen costo financiero para su implementación.

2.10. ESTUDIO DE DISPOSITIVOS SBC DE BAJO COSTO

2.10.1. Caracterización de dispositivos SBC

Para el desarrollo de la solución de este proyecto se desea construir un prototipo hardware de bajo costo basado en dispositivos SBC, por tal motivo se realizó una búsqueda de los dispositivos que actualmente se encuentran en el mercado, los criterios para la caracterización de estos dispositivos son los siguientes:

1. **Numero de núcleos:** Cada núcleo permite el procesamiento de tareas en paralelo esto mejora el rendimiento de la placa.
2. **Frecuencia:** Es la velocidad con la que el procesador ejecuta las instrucciones, a mayor frecuencia mejor rendimiento.
3. **RAM:** Es la capacidad de memoria disponible para que el procesador ejecute las instrucciones, con mayor memoria RAM mejor rendimiento.
4. **Soporte de Sistemas operativos:** El software que permite instalar las herramientas necesarias para la solución.
5. **Módulo GSM:** Es un módulo que permite conectarse a redes de comunicación móvil, se evalúa si el dispositivo soporta este módulo externo.
6. **Costo:** Valor en pesos colombianos del dispositivo, es la característica que permite el desarrollo de una solución de bajo costo.

Cabe señalar que todos los dispositivos clasificados en la siguiente **tabla 11** son de arquitectura RISC[10] (del inglés Reduced Instruction Set Computer) en la que están basados los *microprocesadores ARM*, además el valor del precio es un aproximado que cubre el costo del dispositivo y su envió, como dato de referencia esta clasificación se realizó con los dispositivos ofertados hasta el *20 de julio del 2019*.

No	Nombre del Dispositivo	Núcleos	Frecuencia	RAM	Módulo GSM	Interfaz Pantalla	Sistema Operativo	Precio (COP)
1	Raspberry Pi Zero 	1	1.0GHz	512MB	✓	Micro HDMI	Android, Linux, Windows.	$130.000
2	Orange pi PC 	4	600MHz	1GB	✓	HDMI	Android Ubuntu, Debian, Linux.	$135.000

[10] **RISC:** traducido al español como conjunto reducido de instrucciones de computadora, es un tipo de arquitectura de microprocesador que utiliza un conjunto de instrucciones pequeño y altamente optimizado, es decir que consumen menos recursos de CPU y se ejecutan en menos tiempo.

3	NanoPi R1 	4	1.2GHz	1GB	✗	--	Android, Linux.	$142.000
4	Raspberry Pi 3 	4	1.8GHz	1GB	✓	HDMI	Android, Linux, Windows.	$160.000
5	Banana Pi M2 	4	1.0GHz	1GB	✓	HDMI	Android, Linux.	$180.000
6	Pine A64 LTS 	4	1.2GHz	2GB	✓	Display Serial	Android, Linux, Windows.	$180.000
7	Odroid C2 	4	1.5GHz	2GB	✓	HDMI	Android, Linux.	$205.000
8	Rock Pi 4 	4	1.8GHz	2GB	✓	HDMI	Android, Linux, Windows. .	$232.000
9	Orange pi plus 2E 	4	1.8GHz	2GB	✓	HDMI	Android, Linux.	$250.000
10	BeagleBone Black 	1	1.0GHz	512MB	✓	microHDMI	Android, Linux.	$250.000

11	Asus Tinker Board S 	4	1.8GHz	2GB	✓	HDMI	Linux, Windows.	$269.000
12	Raspberry pi 4 	4	1.5GHz	4GB	✓	Micro HDMI	Android, Linux, Windows.	$320.000
13	WandBoard Dual 	2	1GHz	1GB	✗	HDMI	Linux.	$367.000
14	Latte Panda 	4	1.8GHz	2GB	✓	HDMI	Linux, Windows.	$395.000
15	DragonBoard 	4	1.2GHz	1GB	✓	HDMI, MIPI-DSI	Linux, Windows.	$400.000
16	nVidia Jetson Nano 	4	1.4GHz	4GB	✗	HDMI, DisplayPort	Android, Ubuntu, Linux.	$470.000

Tabla 11. Lista de dispositivos SBC de bajo costo.

2.10.2. Criterios de evaluación de dispositivos

El objetivo principal de los criterios de evaluación de dispositivos es asignar una apropiada calificación para cada dispositivo SBC, con el fin de obtener el top de los mejores dispositivos y los que son considerados idóneos para la implementación de la solución hardware. Los criterios de evaluación se establecieron de la siguiente manera: Se definió cada **característica** con forme a los requerimientos del proyecto, el *precio* es la característica que se planea reducir, el rendimiento de la CPU se dividió en *número de núcleos*, *frecuencia de reloj* y capacidad de *memoria RAM*, como una característica adicional se agregó la compatibilidad con el *módulo*

GSM/GPRS que crea la posibilidad de integrar las redes de comunicaciones móviles al prototipo, y finalmente el *soporte software*. Luego se definieron los rangos y valores fijos concernientes a cada ***especificación***, después se especificó su correspondiente ***valoración*** según su relevancia para el proyecto, por ultimo cabe mencionar que cada una de estas valoraciones son mutuamente excluyentes por cada característica. A continuación, en la **tabla 12** se muestra la distribución mencionada.

Característica		Especificación	Valoración
Precio (COP)		Entre $0 y $117.000	0,75 < x ≤ 1
		Entre $118.000 y $235.000	0,5 < x ≤ 0,75
		Entre $236.000 y $352.000	0,25 < x ≤ 0,49
		Entre $353.000 y $470.000	0 < x ≤ 0,24
Procesador	**Número de núcleos**	1	0
		2	0,25
		4	0,5
		8	1
	Frecuencia de reloj (GHZ)	Menor que 1	0
		Igual a 1 y menor a 1.2	0,25
		Entre 1.2 y 1.5	0,5
		Mayor que 1.5	1
Memoria RAM		512 MB	0
		1 GB	0,25
		2 GB	0,5
		4 GB	1
Módulo GSM/GPRS		No	0
		Si	1
Soporte Software		No tiene software optimizado para el dispositivo, soporte de software escaso.	0
		Soporta software optimizado para otro dispositivo.	0,5
		Tiene software optimizado para el mismo dispositivo.	1

Tabla 12. Criterios de evaluación de dispositivos.

2.10.3. Resultados de la evaluación de dispositivos

Para el análisis de los resultados se transformó el puntaje obtenido de cada dispositivo a su valor porcentual, dicho de otra forma, cada característica aporta como valor máximo **1**, por tanto, el puntaje máximo que podría obtener un dispositivo es de **6** que representa el **100%,** para este estudio los dispositivos con mayor porcentaje son los considerados idóneos para el proyecto, por último, se estableció la valoración porcentual y cualitativa que clasifica cada uno de los dispositivos evaluados como se observa en la siguiente **tabla 13**.

Valoración (%)	Cualitativo
75 < x ≤ 100	Muy Alto
50 < x ≤ 75	Alto
25 < x ≤ 50	Medio
0 < x ≤ 25	Bajo

Tabla 13. Valoración porcentual y cualitativa de dispositivos.

A continuación, en la **tabla 14** se presenta la evaluación y los resultados obtenidos por cada dispositivo con su correspondiente puntaje y valoración porcentual ordenados de mayor a menor.

Dispositivo	Precio	Procesador		RAM	Modulo	Soporte	Puntaje	Porcentaje
		Nucleos	Frecuencia					
Raspberry Pi 3	0,66	0,5	1	0,25	1	1	**4,41**	**73,5**
Raspberry pi 4	0,32	0,5	0,5	1	1	1	**4,32**	**72,0**
Rock Pi 4	0,51	0,5	1	0,5	1	0,5	**4,01**	**66,8**
Orange pi plus 2E	0,47	0,5	1	0,5	1	0,5	**3,97**	**66,1**
Latte Panda	0,16	0,5	1	0,5	1	0,5	**3,66**	**61,0**
Pine A64 LTS	0,62	0,5	0,5	0,5	1	0,5	**3,62**	**60,3**
Odroid C2	0,56	0,5	0,5	0,5	1	0,5	**3,56**	**59,4**
Asus Tinker Board S	0,43	0,5	1	0,5	1	0	**3,43**	**57,1**
Banana Pi M2	0,62	0,5	0,25	0,25	1	0,5	**3,12**	**52,0**
Raspberry Pi Zero	0,72	0	0,25	0	1	1	**2,97**	**49,6**
Orange pi PC	0,71	0,5	0	0,25	1	0,5	**2,96**	**49,4**
NanoPi R1	0,70	0,5	0,5	0,25	0	0,5	**2,45**	**40,8**
DragonBoard	0,15	0,5	0,5	0,25	1	0	**2,40**	**40,0**
nVidia Jetson TK1	0,00	0,5	0,5	1	0	0	**2,00**	**33,3**
BeagleBone Black	0,47	0	0,25	0	1	0	**1,72**	**28,6**
WandBoard Dual	0,22	0,25	0,25	0,25	0	0	**0,97**	**16,2**

Tabla 14. Evaluación de los dispositivos.

En el ***anexo F*** se muestra la tabla completa de la evaluación de dispositivos con su correspondiente valoración cualitativa.

2.10.4. Análisis de la evaluación de dispositivos

El objetivo de este estudio es encontrar los dispositivos que mejor se ajusten a los requerimientos del proyecto teniendo en cuenta los siguientes aspectos; Rendimiento: el dispositivo debe tener la capacidad para ejecutar procesos de forma rápida y en paralelo, de igual forma está obligado a cagar un sistema operativo completo además de herramientas adicionales similares o iguales a las presentadas en el estudio anterior. Soporte: el dispositivo debe contar en lo posible con la mayor cantidad de documentación y soporte software, debido al diverso número de herramientas que se han desarrollado con enfoque en la seguridad cibernética. Precio: el dispositivo debe tener el costo más bajo posible conservando un equilibrio respecto a los dos aspectos anteriormente mencionados. A continuación, en la **tabla 15** se muestran los 5 dispositivos que mejor se ajustaron a los requerimientos del proyecto según la evaluación realizada.

No	Dispositivo	Puntaje	Porcentaje	Cualitativo
1	Raspberry pi 3	4,41	73,5	Alto
2	Raspberry pi 4	4,32	72,0	Alto
3	Rock pi 4	4,01	66,8	Alto
4	Orange pi plus 2E	3,97	66,1	Alto
5	Latte panda	3,66	61,0	Alto

Tabla 15. Top 5 de dispositivos SBC.

La fundación Raspberry pi actualmente es una organización con años de experiencia dedicada a la producción de dispositivos SBC, entre ellos se encuentran los dispositivos Raspberry pi 3 y 4 que lograron posicionarse en el top 5 de dispositivos considerados idóneos para la implementación del prototipo (***tabla 15***), además con puntajes muy cercanos lo siguen los dispositivos Rock pi, Orange pi y Latte panda fabricados por organizaciones chinas que cuentan con varios años dedicados a la creando soluciones hardware, en conclusión, *cualquiera de los cinco dispositivos presentados anteriormente son considerandos una buena elección considerando que cumplen con los requerimientos del proyecto, además provienen de entidades confiables y con experiencia en el desarrollo de estos dispositivos hardware.*

2.11. ESTUDIO DE SISTEMAS OPERATIVOS PARA DISPOSITIVOS SBC

Anteriormente en la sección 2.9 estudio de herramientas para la comunicación anónima se presentaron algunos sistemas operativos dedicados específicamente para cumplir con los requerimientos de anonimato de un usuario en línea, más adelante realizando el análisis de los resultados se descartaron los que no eran compatibles quedando como resultado el sistema operativo Parrot, el objetivo principal de esta sección es presentar otros sistemas operativos compatibles que se puedan agregar a la solución del proyecto, en otras palabras, sistemas operativos que permitan la implementación de un prototipo que cumpla con todos los requerimientos de software y que adicionalmente aproveche de la mejor forma los recursos de hardware del dispositivo SBC.

Los siguientes sistemas operativos han sido desarrollados especialmente para ser compatibles con los dispositivos SBC y explotar al máximo los recursos hardware. Cabe mencionar que actualmente existe una gran variedad de distribuciones creadas para estos dispositivos SBC, esto depende del propósito de uso del usuario, por ejemplo, existen distribuciones orientadas a servidores, estaciones de clima, consolas de video juegos, centros multimedia, nodos IoT, pruebas de seguridad o simplemente como un ordenador de escritorio. En definitiva, los sistemas operativos presentados a continuación se seleccionaron porque cumplen con todos los requerimientos de este proyecto.

2.11.1. Raspbian

Raspbian es un sistema operativo basado en Debían y está basado en la misma filosofía, es decir estabilidad y rendimiento, cuenta con una gran cantidad de paquetes compatibles con dispositivos SBC. Desde 2015, ha sido proporcionado

por la Fundación Raspberry Pi como el sistema operativo oficial para la familia de computadoras de placa única de la marca Raspberry Pi, existen dos versiones de este sistema operativo, Raspbian Buster que dispone de interface de usuario para manejar el sistema y Raspbian Buster Lite que no cuenta con interfaz de usuario debido a esto todo se maneja a través de la línea de comandos. Raspbian fue creado por Mike Thompson y Peter Green como un proyecto independiente, fue lanzado en el año 2012 y desde entonces ha tenido muchas mejoras, actualmente, es un sistema operativo que está en desarrollo activo y actualización constante. Gracias a que es un sistema operativo basado en Debian, ofrece ventajas tales como compatibilidad, estabilidad y adaptabilidad, debido a esto se convierte en una buena opción para los desarrolladores que están iniciando en el desarrollo sobre estos dispositivos [44].

2.11.2. Ubuntu Mate

Ubuntu Mate es una distribución de Linux, de código abierto y derivado oficial del sistema operativo Ubuntu que es una de las distribuciones de Linux más utilizada en el mundo. En comparación con Debian, esta distribución se ejecuta en un ciclo de desarrollo más corto, por lo tanto, proporciona actualizaciones mucho antes, sin embargo, su estabilidad y su comunidad de desarrollo son menores. Ubuntu Mate cuenta con una versión específica para dispositivos Raspberry Pi y otros, contiene de igual forma que en Raspbian los mismos paquetes básicos preinstalados como lo son LibreOffice, Minecraft PI, Scratch, entre otros, además, agrega algunos pequeños cambios como Firefox establecido como navegador predeterminado y usa MATE como entorno de escritorio principal. En resumen, Ubuntu MATE es un sistema operativo estable, fácil de usar, con un entorno de escritorio atractivo y configurable, es ideal para aquellos que desean sacar el máximo provecho de computadoras con pocos requisitos de hardware, es adecuado para computadoras de placa única (SBC) o hardware antiguo. En otras palabras, Ubuntu MATE hace que las computadoras modernas sean rápidas y que las viejas sean utilizables [45].

2.11.3. Windows IoT

Es un sistema operativo desarrollado por Microsoft y denominado como Windows 10 IoT (Internet de las cosas) es un miembro de la familia de Windows 10 que brinda potencia, seguridad y capacidad de gestión de clase empresarial a dispositivos de internet de las cosas. Aprovecha la experiencia integrada de Windows, el ecosistema y la conectividad en la nube, lo que permite a las organizaciones crear su Internet de las cosas con un conjunto de dispositivos seguros que se pueden administrar y conectar a la nube con un propósito en común. Este es un sistema operativo diseñado para dispositivos inteligentes como sensores, cámaras, electrodomésticos, impresoras, es decir, cualquier dispositivo inteligente que se pueda conectar a internet, para desarrollar proyectos con este sistema operativo se requiere de Visual Studio para controlar y programar el dispositivo. Por último, Microsoft ofrece dos versiones de este sistema según su licencia las cuales son Windows 10 IoT Core y Windows 10 IoT Enterprise [46].

2.11.4. RISC OS

RISC OS es un sistema operativo diseñado por Acorn en Cambridge, Inglaterra. Lanzado por primera vez en 1987, sus orígenes se remontan al equipo original que desarrolló el microprocesador ARM, no es una distribución de Linux o Windows, fue construido para ser compacto, eficiente y rápido. Sin entrar demasiado en detalles técnicos, hay muchas innovaciones y diferencias en este sistema esto quiere decir que procesos como gestión de tareas, inicio del sistema, kernel y sistema de archivos se realizan de forma diferente. En definitiva, es un sistema operativo desarrollado especialmente para dispositivos con arquitectura RISC, ofrece versiones optimizadas para dispositivos como Raspberry Pi, Panda Board, Beagle Board, entre otros, la imagen completa del sistema operativo ocupa un espacio de 120 MB. Para trabajar con este sistema operativo los desarrolladores están obligados a aprender la forma única con la que funciona este sistema operativo [47].

2.11.5. Alpine Linux

Alpine Linux es una distribución de Linux independiente, no comercial y de propósito general diseñada para usuarios avanzados que aprecian la seguridad, la simplicidad y la eficiencia de los recursos. Está destinado principalmente a equipos de red como enrutadores, servidores VPN o firewalls, utiliza su propio administrador de paquetes llamado apk, con respecto a la seguridad utiliza un kernel reforzado y compila todos los archivos binarios del usuario como ejecutables independientes para evitar la explotación de clases enteras u otras vulnerabilidades. En definitiva, es un sistema orientado a la seguridad puesto que está desarrollado basado en las herramientas musl[11] y busybox[12], que permiten construir un sistema más pequeño y eficiente en recursos en comparación con las distribuciones tradicionales de GNU Linux, la imagen del sistema operativo estándar para dispositivos ARM ocupa un espacio de 51 MB en el disco [48].

2.11.6. OpenMediaVault

OpenMediaVault es un sistema operativo basado en Debian y proporciona una solución de almacenamiento conectado a la red (NAS[13]) que incluye servicios como SSH, FTP, servidor de medios DAAP[14], RSync una herramienta para sincronizar ficheros y directorios, cliente BitTorrent para administrar descargas, antivirus y muchos más. Este sistema operativo está diseñado principalmente para usarse en oficinas pequeñas u oficinas domésticas, pero no se limita a esos escenarios, en

[11] **Musl:** Es una nueva implementación de propósito general de la librería C. Es liviana, rápida, simple, gratuita y cumple con los estándares y seguridad. Su nombre viene del termino en inglés “Muscle” porque es pequeño pero poderoso como un musculo.

[12] **BusyBox:** Es un paquete software que proporciona varias utilidades de Unix en un solo archivo ejecutable. Fue creado específicamente para sistemas operativos integrados con recursos muy limitados. Los autores lo denominaron "La navaja suiza de Linux embebido " ya que un solo ejecutable reemplaza las funciones básicas de más de 300 comandos comunes.

[13] **NAS:** Siglas en ingles de Network Attached Storage, significa almacenamiento conectado a la red.

[14] **DAAP:** En español significa Protocolo de Acceso de Audio Digital, es un servidor HTTP especializado que envía una lista de archivos de audio y los transmite al cliente a través de la red local.

otras palabras, es una solución simple y fácil de usar que permite a los usuarios instalar y administrar un almacenamiento en memoria conectado a la red. Funciona muy bien en dispositivos SBC con la posibilidad de agregar una tarjeta SD más grande o un disco duro externo para aumentar la capacidad de almacenamiento y administrar archivos de mayor volumen como copias de seguridad, archivos multimedia, imágenes de sistemas operativos y herramientas entre otros. Por ultimo cuenta con versiones optimizadas para dispositivos SBC como Raspberry Pi, Nano Pi, Rock Pi, Orange Pi, entre otros, con un peso promedio de 550 MB de sistema operativo dependiendo del dispositivo [49].

2.11.7. DietPi

DietPi es un sistema operativo basado en Debian, extremadamente liviano y está optimizado para un uso mínimo de recursos de CPU y RAM, lo que garantiza que el dispositivo SBC funcione a su máxima capacidad, además cuenta con un sistema propio creado por su equipo de desarrolladores para la instalación de paquetes y herramientas tales como reproductores multimedia, servidores web, DNS, VPN, FTP, SSH, y herramientas administrativas entre otras. Otra herramienta muy útil es el DietPi-Backup, que le permite realizar una copia de seguridad del sistema operativo completo para que el usuario la restaure en caso de alguna falla en el sistema. El sistema completo DietPi ocupa un espacio en el disco de 590 MB, utiliza 23 MB de memoria RAM y cuenta con un tiempo de arranque de 14 segundos, no posee interfaz de usuario por lo tanto su manejo se hace a través de la línea de comandos, en definitiva, es una buena opción para los desarrolladores con experiencia en Linux que desean aprovechar todo el potencial que ofrece el dispositivo hardware [50].

2.11.8. PipaOS

PipaOS es un sistema operativo diseñado para Raspberry Pi basado en Debian más exactamente en la distribución Raspbian Stretch que contiene el software mínimo para poner el dispositivo en funcionamiento. Es útil para proyectos de hardware reutilizable, la última versión estable es pipaOS 6.0 lanzada en octubre del año 2018. Además de eso, el repositorio pipaOS contiene una gran variedad de software adicional con diversas fuentes. El sistema completo pipaOS ocupa un espacio de 420 MB en el disco, con un tiempo de arranque de 10 segundos en donde se muestra la pantalla de inicio de sesión, además, cuenta con soporte integrado para los dispositivos USB inalámbricos más populares, tolerancia a fallas de energía, sincronización de hora mediante servidores públicos, soporte para transmisión de radio FM, conexión USB y servidor shell. En conclusión, es un sistema operativo que aprovecha muy bien los recursos hardware y se presenta como una buena opción para los desarrolladores con experiencia en Linux a causa de que no cuenta con una interfaz de usuario todos los procesos se deben realizar por medio de la línea de comandos [51].

2.11.9. Criterios de evaluación de sistemas operativos

Los siguientes criterios tienen como propósito permitir una adecuada evaluación para cada sistema operativo considerando los requerimientos y objetivos de este

proyecto, además, presentar una clasificación de los sistemas operativos que mejor se ajusten a la solución final del proyecto es decir el prototipo funcional que se planea implementar, para dichos criterios se definieron las siguientes características:

1. **RAM:** Equivale a el uso mínimo de memoria RAM que necesita el sistema operativo para cargar todos sus procesos, cabe señalar que se refiere a un sistema operativo que viene con las configuraciones por defecto, es decir, recién instalado. Entre más pequeño sea este uso de memoria RAM mejor será el rendimiento del dispositivo.
2. **ROM:** Equivale a el espacio mínimo que necesita la tarjeta SD o micro SD, según el dispositivo SBC, para almacenar todos los componentes del sistema operativo. Cada sistema operativo contiene software o porciones de código que se ejecutan en conjunto con el sistema, por esta razón si un sistema operativo aumenta cada vez, es decir que ocupa mayor espacio en el disco, va consumir mayor cantidad de recursos hardware.
3. **Soporte software:** Se refiere a la condición para soportar herramientas de software, entre ellas las presentadas anteriormente en la sección 2.9. El soporte software puede cumplir con varias condiciones: Es un sistema construido basado en una versión antigua de software, por ejemplo, una versión antigua de Windows o Linux. Es un software que está en su versión beta, es decir que funciona bien, pero puede tener errores. Es un software que ha sido testeado por los creadores o su comunidad de desarrollo para lanzar al mercado un software estable y con las últimas actualizaciones.
4. **Periodo de actualización:** Hace referencia al intervalo de tiempo en el que sale una nueva actualización para el sistema. Este intervalo puede ser mensual, semestral, anual o mayor igual a dos años.
5. **Costos de licencia:** Se refiere al costo monetario si se desea adquirir el sistema operativo con todas sus funcionalidades.

A continuación, en la **tabla 16** se presentan cada una de las características mencionadas con su correspondiente especificación y valor.

Característica		**Especificación**	**Valor**
Recursos Mínimos	**RAM**	Rango de memoria usada entre 0 MB y 512 MB.	$0 < x \leq 1$
	ROM	Rango de memoria usada entre 0 GB y 4GB.	$0 < x \leq 1$
Soporte Software		Poco soporte de herramientas software.	0
		Soporte de herramientas software estable para versiones antiguas.	0,25
		Soporte de herramientas software en su versión beta.	0.5

	Soporte de herramientas software estable y actualizado.	1
Periodo de actualización	Mayor o igual a dos años.	0
	Anual.	0,25
	Semestral.	0.5
	Mensual.	1
Costos de licencia	Totalmente de paga.	0
	Solo versión de prueba gratuita.	0,25
	Solo versión básica gratuita.	0.5
	Totalmente gratuita.	1

Tabla 16. Criterios de evaluación de sistemas operativos.

2.11.10. Resultados de la evaluación de sistemas operativos

Para el análisis de los resultados se transformó el resultado del puntaje obtenido de cada sistema operativo a su valor porcentual para gestionar de forma sencilla y clara los datos obtenidos en la evaluación, de esta forma tenemos que cada característica aporta como valor máximo **1**, por tanto, el puntaje máximo que podría obtener un sistema operativo es de **5** que representa el **100%,** para este estudio los sistemas operativos con mayor porcentaje son los considerados idóneos para el proyecto, por último, se estableció la valoración porcentual y cualitativa que clasifica cada uno de los sistemas evaluados como se observa en la siguiente **tabla 17**

Valoración (%)	Cualitativo
75 < x ≤ 100	Muy Alto
50 < x ≤ 75	Alto
25 < x ≤ 50	Medio
0 < x ≤ 25	Bajo

Tabla 17. Valoración porcentual y cualitativa de sistemas operativos.

A continuación, en la **tabla 18** se presenta la evaluación y los resultados obtenidos por cada sistema operativo con su correspondiente puntaje y valoración porcentual ordenaos de mayor a menor.

Sistema Operativo	Recursos de memoria		Soporte	Periodo	Costos	Puntaje	Porcentaje
	RAM	ROM					
Raspbian Buster Lite	0,94	0,48	1	1	1	**4,42**	**88,33**
Raspbian Buster	0,41	0,28	1	1	1	**3,69**	**73,78**
DietPi	0,95	0,76	0,25	0,5	1	**3,47**	**69,30**
Alpine Linux	0,92	0,76	0,25	0,25	1	**3,18**	**63,69**
Ubuntu Mate	0,38	0,18	0,5	1	1	**3,05**	**61,00**
RISC OS	0,89	0,53	0	0,5	1	**2,92**	**58,35**
PipaOS	0,93	0,55	0,25	0	1	**2,73**	**54,63**
Windows IoT Core	0,59	0,63	1	0,25	0,25	**2,71**	**54,30**
OpenMediaVault	0,88	0,30	0,25	0,25	1	**2,68**	**53,66**
Windows IoT Enterprise	0,51	0,45	1	0,5	0	**2,46**	**49,23**

Tabla 18. Evaluación de los sistemas operativos.

En el ***anexo G*** se muestra la tabla completa de la evaluación de sistemas operativos con su correspondiente valoración cualitativa.

2.11.11. Análisis de la evaluación de sistemas operativos

El objetivo de este estudio de sistemas operativos es identificar cuáles son las mejores opciones para ser implementadas en la solución final, todo esto teniendo en cuenta las características presentadas anteriormente que permiten en la evaluación mantener un equilibrio entre el rendimiento del hardware y la confiabilidad del sistema operativo para implementación de este proyecto, a continuación, se presenta en la **tabla 19** la lista de los 5 sistemas operativos que obtuvieron los mejores puntajes en la evaluación.

No	Sistema operativo	Puntaje	Porcentaje	Cualitativo
1	Raspbian Buster Lite	4,42	88,3	Muy Alto
2	Raspbian Buster	3,69	73,78	Alto
3	DietPi	3,47	69,30	Alto
4	Alpine Linux	3,18	63,7	Alto
5	Ubuntu Mate	3,05	61,0	Alto

Tabla 19. Top 5 de sistemas operativos.

Con respecto a los resultados obtenidos en la anterior ***tabla 19*** se puede extraer la siguiente afirmación. El sistema operativo Debian se muestra implícitamente como la mejor opción para ser implementada en la solución ya que se encuentra presente en cada uno de los sistemas operativos con excepción de Alpine Linux que fue desarrollado en base a otras librerías, teniendo presente que Raspbian y DietPi han sido desarrollados basados en Debian Buster, por ultimo Ubuntu Mate pertenece a una de las muchas distribuciones de Debian.

2.12. COMUNICACIÓN MÓVIL

La comunicación GSM por sus siglas en ingles de Global *System for Mobile Communications* es la técnica de comunicación celular inalámbrica más utilizada para la comunicación de las personas, se define como la red digital que ayuda a la conectividad móvil, según la *Asociación GSM*, casi el 80% de los usuarios de teléfonos móviles en todo el mundo utilizan GSM como su red principal para realizar llamadas inalámbricas y actualmente soporta más de mil millones de suscriptores móviles en más de 210 países en todo el mundo. La tecnología GSM fue desarrollado utilizando tecnología digital, es decir que tiene la capacidad de transportar datos digitales con velocidades entre 64 kbps y 120 Mbps lo cual permite características estándar como cifrado de llamadas telefónicas, redes de datos, identificación de llamadas, reenvío de llamadas, llamada en espera, SMS y conferencias.

2.12.1. Módulo GSM

Un módulo GSM es un chip o circuito que se utilizará para establecer una comunicación entre dispositivo móvil o máquina informática y un sistema de

comunicación GSM el cual requiere una tarjeta SIM (Módulo de identidad del suscriptor) al igual que los teléfonos móviles para activar la comunicación con la red, también posee un número de identificación único conocido como IMEI (Identidad internacional de equipo móvil). Un módulo GSM puede ser un dispositivo de módem dedicado con una conexión serial, USB o Bluetooth, o simplemente puede ser un teléfono móvil que brinde capacidades de comunicación GSM, estos módulos inalámbricos generan, transmiten o decodifican datos desde una red celular a otra para mantener la comunicación. Para su configuración el modulo necesita comandos AT, para interactuar con el procesador o controlador, que se comunican a través de la comunicación en serie y de esta forma controlar la comunicación GSM, se conocen como comandos AT porque cada línea de comando comienza con las letras "AT" o "at" que es la abreviatura de ATENTION, algunas de sus funciones incluyen monitoreo de la intensidad de la señal, monitoreo del estado de carga y el nivel de carga de la batería, además de leer, escribir y buscar entradas en la guía telefónica.

2.12.2. Selección del módulo GSM

Existen diferentes módulos compatibles con los dispositivos SBC, en este caso los módulos compatibles con el *Top 5 de dispositivos SBC* (**Tabla 15**) son SIM800 y SIM900, existen múltiples versiones de cada módulo con sus propias características generando una diversidad de opciones para la elaboración de prototipos hardware según los requerimientos del proyecto, por ejemplo, el módulo SIM800 y sus versiones son: SIM800C posee bluetooth, SIM800L posee FM radio, SIM800F es pin compatible con el módulo SIM900, SIM868 tiene dual sim con GNSS[15]. Para la selección del módulo GSM se descartó el SIM900 dado que es un módulo antiguo y está próximo a ser descontinuado, por otro lado, el SIM800 es la versión actualizada del SIM900 además de ser la versión más reciente en el mercado, otro aspecto a favor del SIM800 es que su costo en el mercado es más bajo, cabe señalar que se seleccionó el SIM800 en su versión normal porque posee los componentes básicos requeridos para el prototipo, es decir, chip GSM, ranura SIM, interfaz serial, antena, conexiones de micrófono y altavoz como se muestra en la siguiente figura.

Figura 7. Módulo GSM SIM800.

[15] **GNSS:** hace referencia al Sistema Global de Navegación por Satélite (del inglés Global Navigation Satellite System), es un sistema diseñado para determinar las coordenadas geográficas de un objeto sin importar su localización ya sea en el mar, en el aire o en una montaña.

2.13. ESTUDIO DE CASOS

Tomando como base los resultados obtenidos en los tres estudios anteriores donde se evaluaron herramientas, dispositivos SBC y sistemas operativos se elaboraron las configuraciones presentadas en la siguiente **tabla 20**, cabe mencionar que estas son solo propuestas iniciales para construir la solución final, esto debido a que probablemente pueden surgir problemas de compatibilidad entre el sistema operativo y las herramientas, además se pretende construir un prototipo que conserve un equilibrio entre rendimiento de hardware y su funcionalidad dado que se cuenta con recursos de maquina limitados debido a cada dispositivo SBC.

La leyenda usada para esta sección “Estudio de casos” es: C=Configuración.

Área	C1	C2	C3	C4
Sistema operativo	Raspbian Buster Lite	Raspbian Buster	DietPi	Parrot
Seguridad de la red	VPN	Red Tor	VPN	Red Tor
Privacidad en el motor de búsqueda	StartPage	Duck Duck Go	Gibiru	Duck Duck Go
Cliente de mensajería instantánea	OnionShare	ProtonMail	Paranoid	OnionShare
Privacidad en el navegador	Midori	Midori	Midori	Tor Browser
Cliente de administración de contraseñas	Dashlane	LastPass	1Password	KeePassXC
Cifrado de datos	VeraCrypt	VeraCrypt	VeraCrypt	ZuluCrypt

Tabla 20. Configuraciones de software.

Es importante señalar que la configuración 4 resaltada en color gris claro tiene una configuración fija porque Parrot como sistema operativo contiene por defecto herramientas pre configuradas entre ellas se encuentran la red Tor, Duck duck go, Onionshare, Tor browser y ZuluCrypt, además, contiene unas pocas herramientas de las que fueron presentadas en la ***sección 2.9*** y una gran variedad de herramientas adicionales relacionadas con seguridad, anonimato, pententing, entre otras áreas. A continuación, en la **tabla 21** se presenta cada uno de los casos a evaluar teniendo en cuenta los tres primeros dispositivos SBC presentados en el top 5 de dispositivos SBC (***tabla 15***), también se tuvo en cuenta el módulo GSM/GPRS que permite las comunicaciones móviles y cada una de las configuraciones presentadas anteriormente.

Caso	Dispositivo	Módulo GSM	Configuración
1	Raspberry pi 3	SIMCOM SIM800	C1
2	Raspberry pi 4		
3	Raspberry pi 3		C2
4	Raspberry pi 4		
5	Raspberry pi 3		C3
6	Raspberry pi 4		
7	Raspberry pi 3		C4
8	Raspberry pi 4		

Tabla 21. Listado de casos.

CAPÍTULO III. DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO HARDWARE Y SOFTWARE

En este capítulo se describen los pasos llevados a cabo para construir el prototipo con su respectiva configuración para su correcto funcionamiento, presentando el diseño de la arquitectura, el diseño de red, la arquitectura software y hardware, instalación del software necesario y la configuración de este a través de los diferentes archivos y comandos utilizados.

3.1. DISEÑO DE LA ARQUITECTURA Y RED

3.1.1. Diseño de la arquitectura

Se realizó el diseño de la arquitectura y el diseño de red para la comunicación anónima teniendo en cuenta cada una de las áreas presentadas en la ***tabla 9***, esto permite mantener la privacidad del usuario en cada aspecto de la comunicación que realiza a través de la red, como servicio de red se tuvo en cuenta la navegación web. A continuación, en la **figura 8** se expone el diseño de la arquitectura de comunicación.

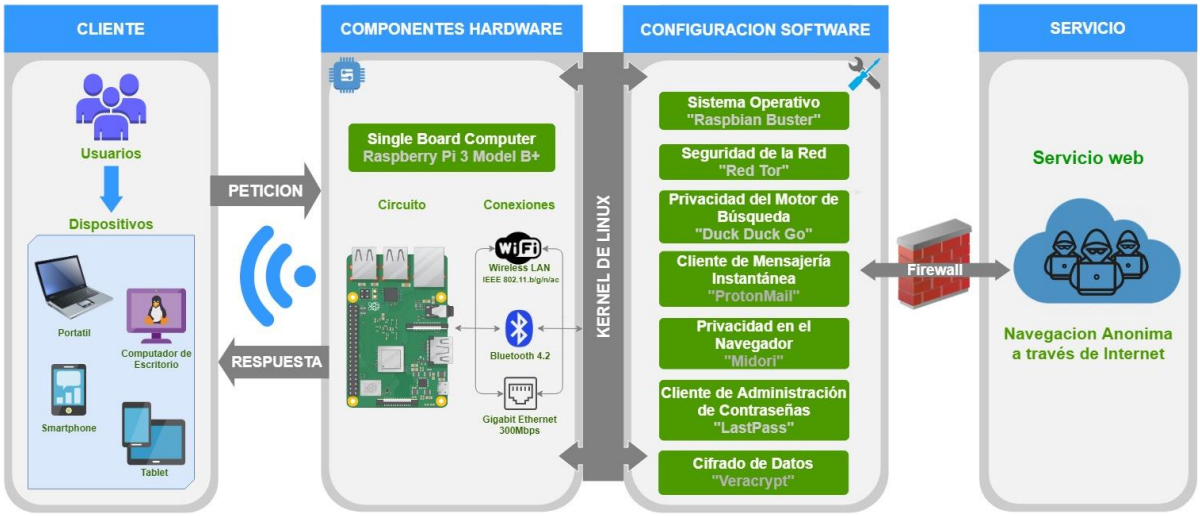


Figura 8. Arquitectura de la comunicación.

3.1.1.1. Descripción de los componentes de la arquitectura.

A continuación, se procede a describir cada uno de los componentes de la arquitectura y la forma como se relacionan entre sí para brindar el servicio de anonimato a los usuarios.

Cliente: son todos los usuarios o dispositivos que se van a conectar al prototipo para usar el servicio de navegación anónima, el único requisito para estos dispositivos es contar con conexión WiFi.

Componentes Hardware: corresponde al dispositivo SBC con todos sus componentes y características de hardware, para el correcto funcionamiento de la arquitectura se usaron los siguientes componentes:

Entrada Ethernet: este componente proporciona al dispositivo el acceso a la red, para ello se debe mantener la conexión entre el router que proporciona el servicio de internet hasta el dispositivo SBC a través de un cable ethernet.

Tarjeta WiFi: es el componente encargado de compartir el servicio de anonimato a los clientes, se debe realizar la configuración planteada en la sección 4.1.3, esto crea una red WiFi o punto de acceso para que los dispositivos clientes se conecten al prototipo y naveguen de forma anónima en la red.

Componentes Software: son cada una de las herramientas, incluido el sistema operativo, configuradas para proporcionar anonimato a cada una de las 7 áreas identificadas anteriormente las cuales intervienen en la comunicación web de los usuarios, estas configuraciones se presentan más adelante en la sección 3.2, adicionalmente al sistema se le configuro el firewall, herramienta que permite gestionar la totalidad de tráfico de entrada y salida que transita entre el prototipo y la red a la que está conectada, en este caso se configura para filtrar el tráfico de entrada al sistema y así bloquear cualquier intento de acceso externo al prototipo.

Servicio: corresponde al servicio de red anonimizado por el prototipo, para este proyecto se seleccionó la navegación web.

3.1.2. Diseño de red

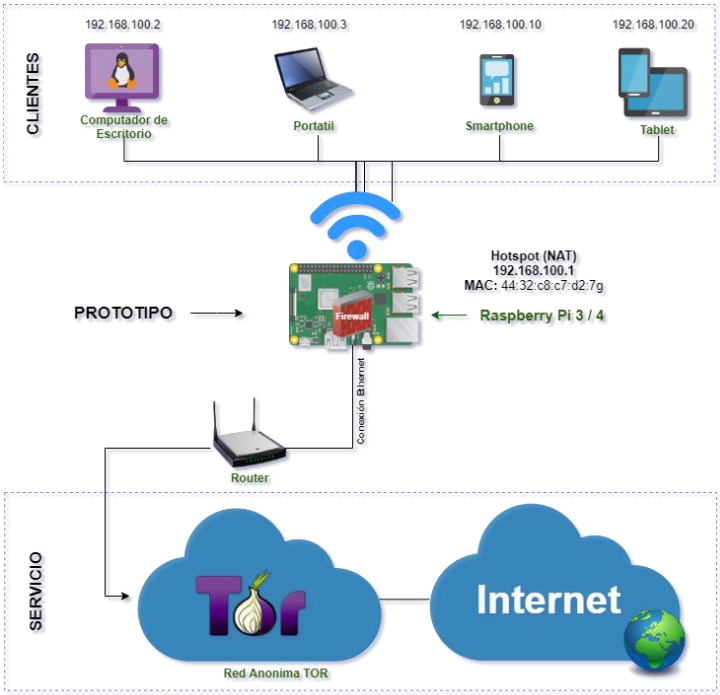


Figura 9. Diseño de red.

3.1.2.1. Descripción de los componentes del diseño de red.

A continuación, se procede a describir cada uno de los componentes del diseño de red y sus relaciones que permiten compartir de forma segura en la red el servicio de anonimato.

Clientes: Son todos aquellos dispositivos que están conectados a la red generada por el prototipo, estos dispositivos se encuentran conectados y agrupados en una subred protegida por el dispositivo SBC y a cada uno de estos dispositivos se le asigna una dirección IP, la configuración de esta red es de tipo NAT (Network Adress Translation) esto hace que todos los dispositivos se mantengan enmascarados detrás de la dirección IP del prototipo, combatiendo de esta manera la intrusión no autorizada de amenazas que puedan llegar desde el ciber-espacio.

Prototipo: corresponde al dispositivo SBC y sus configuraciones, el direccionamiento del sistema se configura como en la sección 4.1.3 de tal forma que la conexión web que viaja a través del cable ethernet sea redireccionado a la red de anonimato del prototipo (en este caso la red tor), al tener acceso a la red anónima se procede a configurar el punto de acceso (la red generada por el prototipo) de modo que apunte a la red de anónima así todos los clientes conectados serán redirigidos a esta red, por último el firewall que está configurado en el Dispositivo SBC es el encargado de bloquear el trafico entrante hacia el prototipo.

Servicio: corresponde al entorno donde se lleva a cabo la comunicación, en este caso es un servicio web que funciona de la siguiente forma: el prototipo inicia la comunicación pasando por la red anónima que ayuda a proteger la identidad real de los clientes y a su vez realiza la consulta web, al obtener la respuesta a la consulta la red anónima se la devuelve al prototipo y este se encarga de dirigirla al cliente. Al implementar esta configuración de red se está agregando doble protección a los usuarios puesto que en el caso que un atacante quiera acceden a uno de nuestros clientes desde internet, el tendrá que primero vulnerar la red anónima para después intentar acceder al prototipo que se encarga de proteger a los clientes.

3.2. IMPLEMENTACIÓN DE LAS CONFIGURACIONES DE SOFTWARE

El proceso de implementación de las configuraciones de software se realizó de la siguiente manera. Primero se inició configurando cada uno de los sistemas operativos y después se continuó con la configuración de cada una de las herramientas de anonimato en su correspondiente sistema operativo, cabe señalar que todas las configuraciones en esta ***sección 3.2*** corresponden a los resultados presentados en la tabla *Configuraciones de software* (**tabla 20**).

3.2.1. Configuración de los sistemas operativos

Para que un dispositivo SBC pueda correr un sistema operativo completo se debe contar con una memoria microSD con la imagen del sistema operativo grabada y algunos otros requerimientos que varían según el sistema operativo seleccionado.

Los requerimientos mínimos con respecto a la capacidad de la tarjeta microSD son los siguientes: Raspbian Buster y Parrot, el tamaño mínimo permitido es de 8 GB, para Raspbian Buster Lite y DietPi, el tamaño mínimo permitido es de 4 GB, como información adicional los modelos de Raspberry Pi 3 en adelante pueden arrancar un sistema operativo desde una tarjeta microSD de más de 256 GB, esto se debe a un error presente en los modelos anteriores de la Raspberry Pi. Para este proyecto se tomaron 4 memorias microSD de 16GB de capacidad.

3.2.1.1. Instalación del sistema operativo

Los siguientes pasos para grabar el sistema operativo en la tarjeta se realizaron en un computador con el sistema operativo Windows 10. Para iniciar se debe tener el archivo de imagen del sistema operativo (ejemplo: *Raspbian.img*), para este proyecto todas las imágenes fueron descargadas desde la página oficial de cada sistema operativo, lo siguiente es *formatear* la tarjeta microSD teniendo en cuenta que el sistema de archivos seleccionado sea FAT32, seguido a esto se utilizó la herramienta *Win32 Disk Imager* [52] para grabar el sistema operativo, para esto se debe seleccionar el archivo de imagen junto con la tarjeta microSD y elegir la opción "Write" como se muestra en la siguiente **figura 10**, al finalizar la escritura debe salir un letrero de "operación exitosa" lo que indica que la memoria ya puede ser insertada en el dispositivo SBC para su posterior configuración.

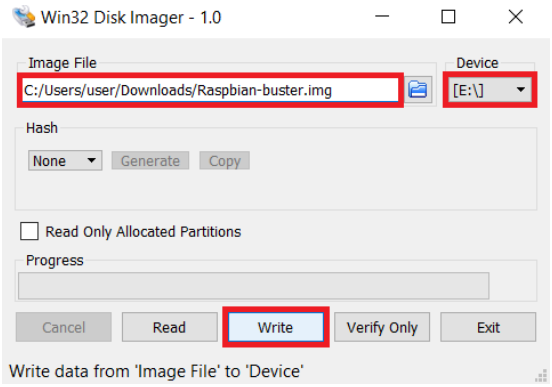


Figura 10. Herramienta Win32 Disk Imager.

Al iniciar el sistema operativo por primera vez, dependiendo de cada sistema y su versión, pedirá al usuario que configure opciones generales como el formato he idioma del teclado o de la interfaz gráfica (si cuenta con interfaz gráfica), la información de la localización, la conexión a internet a través de WiFi y opciones de seguridad como crear contraseña o un usuario nuevo, es común que en su primera vez el sistema operativo se reinicie automáticamente para realizar las

configuraciones necesarias, finalmente después del reinicio se debe actualizar el sistema operativo, en este caso los 4 sistemas operativos a configurar pertenecen a las distribuciones de Debian por lo que las configuraciones se realizaron a través de la línea de comandos y para actualizar el sistema se utilizan los siguientes comandos:

```
$ sudo apt-get update

$ sudo apt-get upgrade
```

Realizadas estas configuraciones tenemos 4 memorias microSD en donde están instalados los 4 sistemas operativos Raspbian Buster Lite, Raspbian Buster y DietPi los cuales son la base para la siguiente sección de configuración de herramientas, por otro lado, como el sistema operativo Parrot ya viene con sus herramientas pre-configuradas por defecto no es necesario realizar instalaciones o configuraciones adicionales.

Nota: Cada sistema operativo tiene su perfil de administrador con los permisos necesario para realizar las configuraciones, en este caso los perfiles y sus credenciales por defecto son:

Raspbian Buster Lite: Usuario: “pi”, Contraseña: “raspberry”.

Raspbian Buster: Usuario: “pi”, Contraseña: “raspberry”.

DietPi: Usuario: “root”, Contraseña “dietpi”.

Parrot: Usuario: “parrot”, Contraseña: “toor”.

3.2.2. Configuración de las herramientas software

Los comandos y el proceso de cómo se realizó la configuración de cada una de las herramientas seleccionadas en la tabla *Configuraciones de software* (**tabla 20**), se presentan las configuraciones ordenadas por su área correspondiente área, es decir, *seguridad de la red*, *privacidad en el motor de búsqueda*, *cliente de mensajería instantánea*, *privacidad en el navegador*, *cliente de administración de contraseñas* y *cifrado de datos* cada uno con su correspondiente herramienta.

3.2.2.1. Configuración del área seguridad de la red

3.2.2.1.1. Configuración de la VPN

Para esta configuración se seleccionó la herramienta OpenVPN que es un software de código abierto, uso gratuito y ampliamente utilizado para la creación de una red privada virtual, para la configuración de OpenVPN se deben seguir los siguientes pasos.

- Instalar la herramienta OpenVPN en el sistema operativo, como se muestra en la siguiente **figura 11**, con el siguiente comando.

$ sudo apt-get install openvpn unzip

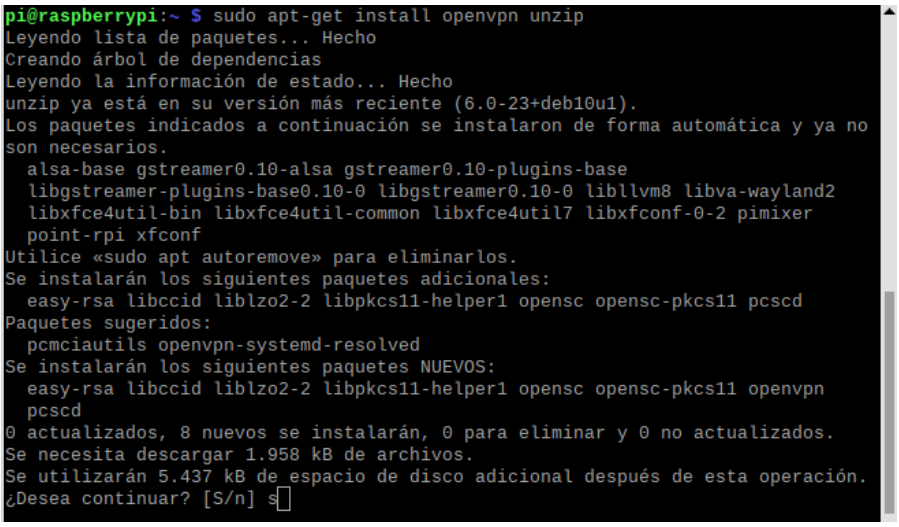


Figura 11. Instalación OpenVPN.

- Configuración de la zona horaria ejecutando el siguiente comando.

$ sudo dpkg-reconfigure tzdata

después elegir la región a la que quiere conectarse, elegir el país y el protocolo a utilizar UDP o TCP.

- Descargar el archivo de configuración de OpenVPN con el siguiente comando.

$ sudo –i

$ cd /tmp && wget https://files.ovpn.com/raspbian/ovpn-dk-copenhagen.zip && unzip ovpn-dk-copenhagen.zip && mkdir -p /etc/openvpn && mv config/ /etc/openvpn && chmod +x /etc/openvpn/update-resolv-conf && rm -rf config && rm -f ovpn-dk-copenhagen.zip*

- Configuración de las credenciales de inicio de sesión

$ echo "Digitar_Usuario" >> /etc/openvpn/credentials

$ echo "Digitar_Contraseña" >> /etc/openvpn/credentials

- Iniciar la VPN

$ sudo openvpn --config /etc/openvpn/ovpn.conf --daemon

- Verificar que se estableció la conexión

$ curl https://www.ovpn.com/v2/api/client/ptr | python -m json.tool

si la conexión se estableció correctamente el resultado debe ser como lo siguiente.

{"status":true,"ip":"46.227.67.132","ptr":"clientXXX.ovpn.com"}

Al siguiente reinicio el dispositivo se conectará automáticamente a la VPN.

3.2.2.1.2. Configuración de la Red Tor

- Para instalar la herramienta que permite conectarse a la red Tor se utiliza el siguiente comando como se muestra en la **figura 12.**

```
$ sudo apt-get install tor
```

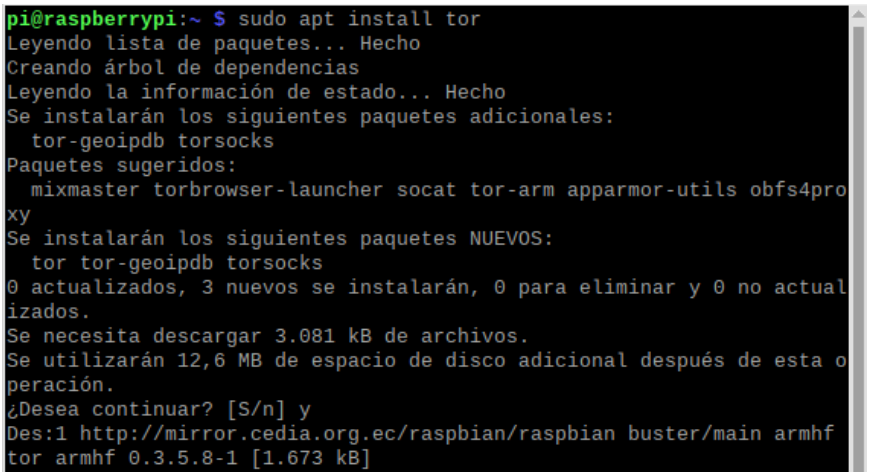


Figura 12. Instalación de Tor.

- Los comandos para controlar el servicio Tor en el sistema operativo son: ver el estado, iniciar, detener y reiniciar el servicio Tor correspondientemente.

```
$ sudo service tor status

$ sudo service tor start

$ sudo service tor stop

$ sudo service tor restart
```

En la siguiente **figura 13** se muestra el estado del servicio Tor como “activo” lo cual indica que el sistema se conectó exitosamente a la red Tor.

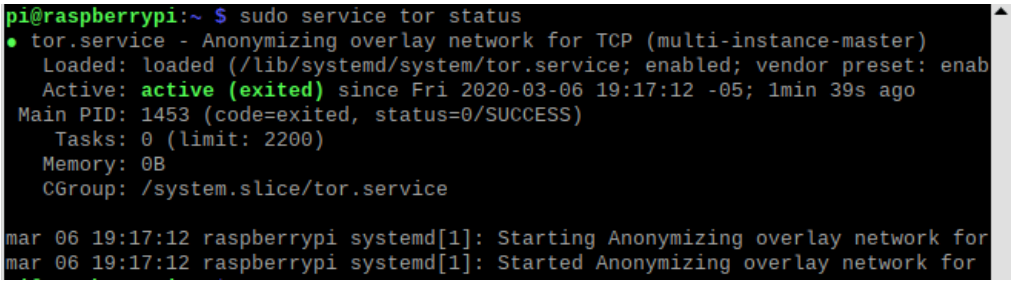


Figura 13. Estado “activo” del servicio Tor.

- Si se requiere configurar los nodos de la comunicación u otra configuración adicional se debe entrar en el archivo torrc con el siguiente comando.

sudo nano /etc/tor/torrc

3.2.2.2. Configuración del área privacidad en el motor de búsqueda

Los motores de búsqueda son herramientas que se utilizan y se configuran directamente desde el navegador web, para el caso **Duckduckgo** [22], **Startpage** [23] y **Gibiru** [25] se puede establecer cada uno de ellos como el motor de búsqueda predeterminado, para realizar una búsqueda solo se debe ingresar a la dirección web oficial y digitar los datos en la caja de texto como se muestra en la siguiente **figura 14**.

Figura 14. Interfaz de los motores de búsqueda.

3.2.2.3. Configuración del área cliente de mensajería instantánea

3.2.2.3.1. Configuración de OnionShare

- Para utilizar la herramienta OnionShare primero se debe instalar en el sistema operativo algunas dependencias de Python3 las cuales sirven permiten ejecutar correctamente el software, para ello se ejecuta el siguiente comando como se muestra en la siguiente **figura 15.**

$ sudo apt install -y python3-flask python3-stem python3-pyqt5 python3-crypto python3-socks python-nautilus tor obfs4proxy python3-pytest build-essential fakeroot python3-all python3-stdeb dh-python python3-flask-httpauth python3-distutils

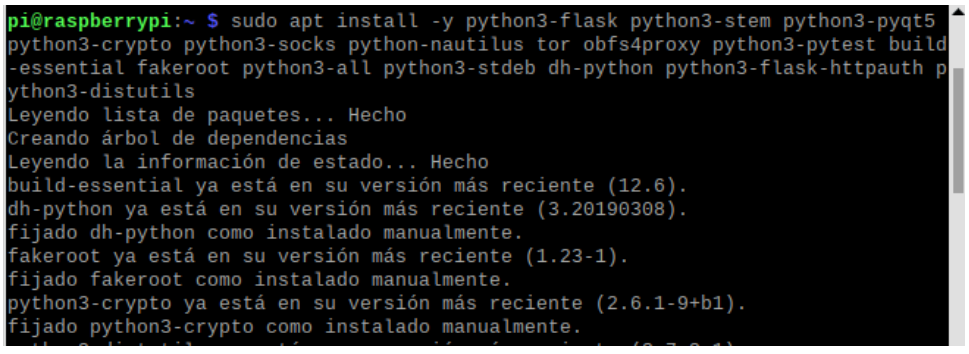


Figura 15. Instalar dependencias de Python para OnionShare.

- Descargar la herramienta desde su repositorio oficial en github

```
$ git clone https://github.com/micahflee/onionshare.git
```

- Hay dos opciones para iniciar la aplicación se debe entrar en la carpeta ***onionshare/dev_scripts*** y ejecutar el script ***onionshare-gui*** para abrir la versión con interfaz gráfica o ***onionshare*** para abrir la versión sin interfaz la cual se maneja por línea de comandos, en la **figura 16** se muestra el resultado al ejecutar el script con interfaz gráfica, para esto los comandos utilizados son.

```
$ cd onionshare/dev_scripts

$ ./dev_scripts/onionshare-gui
```

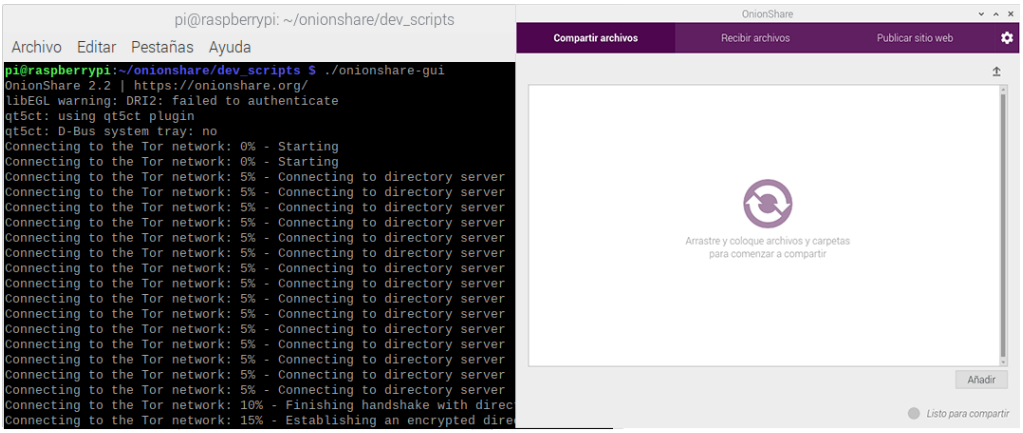


Figura 16. Interfaz de cliente OnionShare.

3.2.2.3.2. Configuración de ProtonMail y Paranoid

Los clientes de correo electrónico **ProtonMail** [28] y **Paranoid** [29] son herramientas que se utilizan directamente desde su correspondiente página web oficial, para comenzar a utilizar el servicio de mensajería anónima se debe iniciar creando una cuenta de usuario en el sitio web, como requisito inicial se pide al usuario un correo electrónico existente el cual solo sirve para activar la nueva cuenta de usuario, al finalizar la activación el usuario puede iniciar a utilizar el servicio, esto se muestra en las siguientes figuras 17 y 18**,** donde la **figura 17** muestra la interfaz de inicio de sesión de ProtonMail y su bandeja de entrada, tambien presenta la interfaz de inicio de sesión de Paranoid.

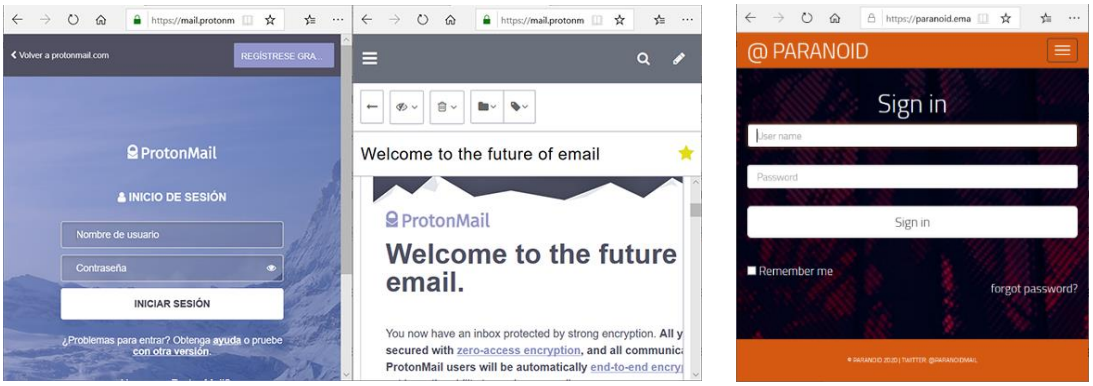


Figura 17. Interfaz de sesión ProtonMail y Paranoid.

3.2.2.4. Configuración del área privacidad en el navegador

- Para instalar el navegador Midori dentro del sistema, como se muestra en la **figura 18**, se debe utilizar el siguiente comando.

```
$ sudo apt-get install midori
```

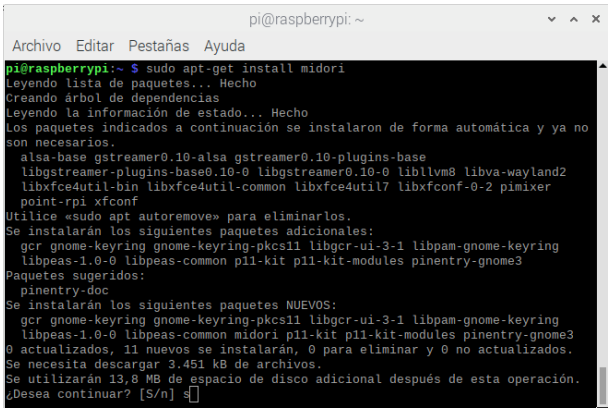


Figura 18. Instalación del navegador Midori.

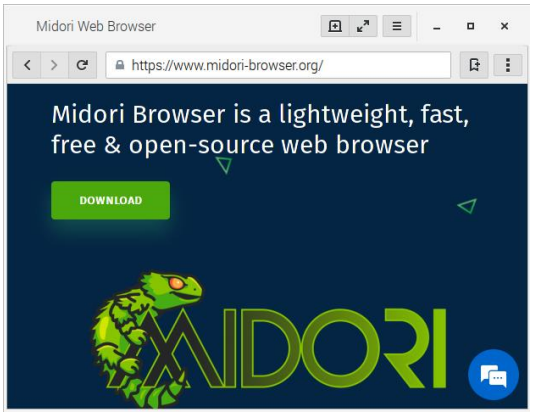


Figura 19. Interfaz del navegador Midori.

Para iniciar la configuración del navegador en el sistema se debe ingresar al *Menú de aplicaciones > Internet > Midori*, esto abre la interfaz del navegador como se muestra en la **figura 19**, dentro del navegador se pueden configurar las opciones de motor de búsqueda, ejecución de scripts, historial de navegación entre otros.

3.2.2.5. Configuración del área cliente de administración de contraseñas

Las herramientas de administración de contraseñas **Dashlane** [38], **LastPass** [36] y **1Password** [37] son servicios que se usan accediendo directamente a su sitio web oficial, en la **figura 20** se muestra la página de inicio de cada herramienta, para comenzar a utilizar estas herramientas se debe crear una nueva cuenta de usuario, las instrucciones para crear la cuenta y de igual forma para su utilización varían de acuerdo a las políticas internas de cada herramienta.

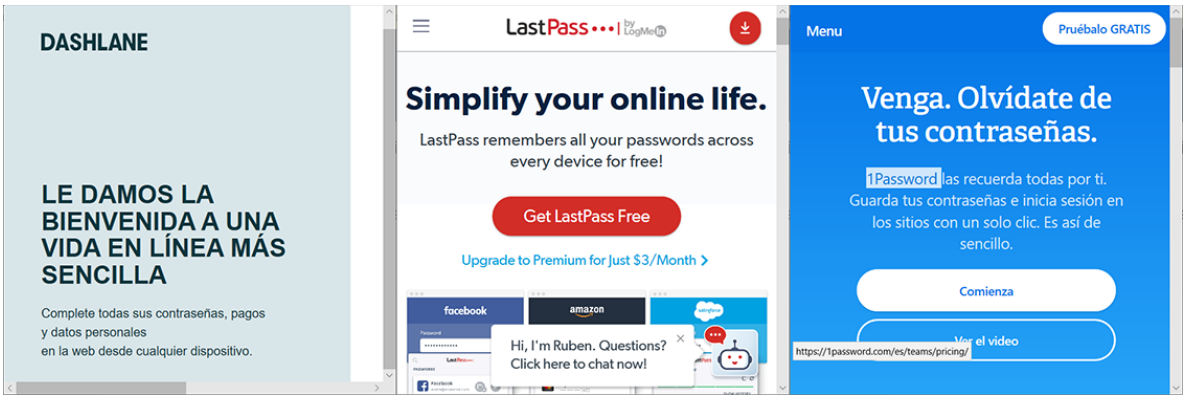


Figura 20. Clientes de administración de contraseñas.

3.2.2.6. Configuración del área cifrado de datos

- Para instalar la herramienta **VeraCrypt** en el sistema operativo primero se debe iniciar instalando las dependencias necesarias para que el software funcione correctamente para esto se usa el siguiente comando.

```
$ sudo apt install libfuse-dev libwxbase3.0-dev
```

- Se descarga la herramienta directamente del repositorio oficial usando el comando.

```
$ wget -L -O veracrypt-1.21-raspbian-setup.tar.bz2 https://sourceforge.net/projects/veracrypt/files/VeraCrypt%201.21/veracrypt-1.21-raspbian-setup.tar.bz2/download
```

Nota: la versión de VeraCrypt seleccionada “veracrypt1.21-raspbian-setup.tar” es compatible con todos los sistemas operativos seleccionados para la sección de configuraciones.

- Se debe descomprimir el archivo descargado, convertir en ejecutable el archivo de instalación y ejecutar la herramienta se usan correspondientemente los comandos.

```
$ tar xvf veracrypt-1.21-raspbian-setup.tar.bz2

$ chmod +x veracrypt-1.21-setup-console-armv7

$ sudo ./veracrypt-1.21-setup-console-armv7
```

Al finalizar la instalación, la herramienta esta lista para usar a través de la línea de comandos, para verificar que VeraCrypt se instaló correctamente se utiliza el siguiente comando, como se muestra en la **figura 21** la respuesta es la versión del software instalado.

```
$ veracrypt --version
```

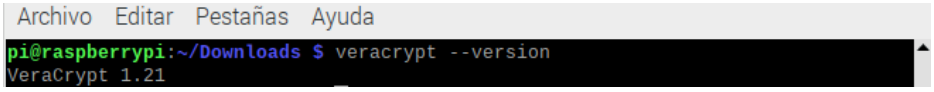


Figura 21. Verificando la herramienta VeraCrypt.

3.2.3. Resultados de la configuración

Realizadas las configuraciones de software anteriores se obtuvo como resultado cuatro arquitecturas diferentes para la comunicación anónima, en otras palabras, las 4 configuraciones que se plantearon en la sección "*Estudio de casos*" **tabla 20** implementadas y en funcionamiento, a continuación, se presenta la evidencia de cada configuración, cabe señalar que no fue posible configurar todas las herramientas en los sistemas operativos debido a las limitaciones de interfaz en Raspbian Buster Lite y DietPi los cuales no cuentan con una interfaz de escritorio para configurar las herramientas referentes al área del navegador web, el motor de búsqueda y los clientes de administración de contraseñas.

3.2.3.1. Configuración 1

El sistema operativo corresponde a Raspbian Buster Lite el cual todo el sistema se maneja a través de la línea de comandos, este sistema tiene configurada una red privada virtual con el software OpenVPN que permite al usuario conectarse a la red de forma anónima, tiene configurada la herramienta OnionShare que le permite enviar y recibir mensajes de correo electrónico de forma anónima, tiene el navegador Midori con opciones limitadas debido a la ausencia de interfaz web y por último la herramienta VeraCrypt que permite cifrar y descifrar archivos para mantener la integridad de los datos, en la siguiente **figura 22** se muestra la configuración del sistema con cada herramienta y su correspondiente versión.

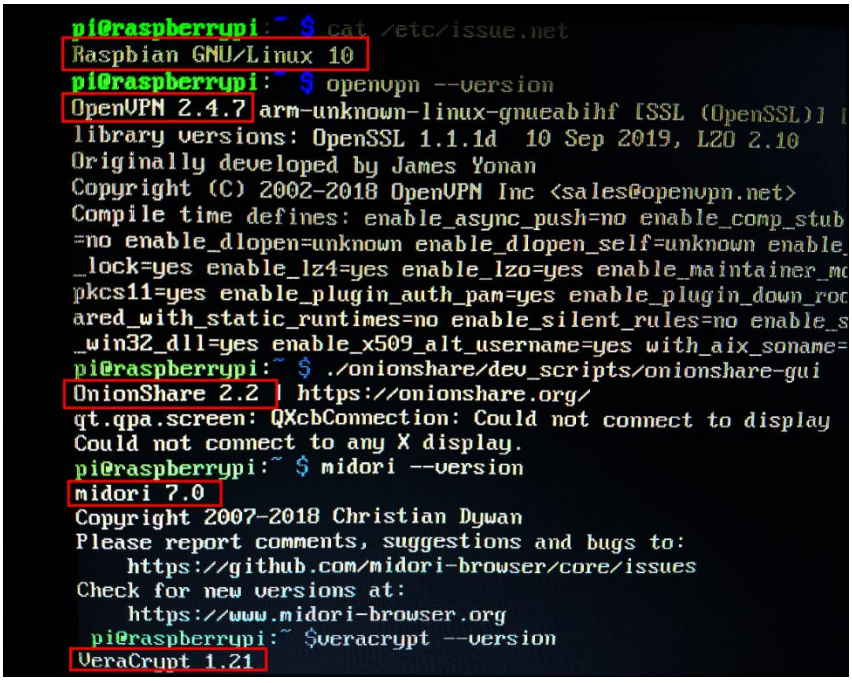


Figura 22. Configuración 1, herramientas y versiones.

3.2.3.2. Configuración 2

Es el sistema operativo Raspbian Buster, tiene configurada la red Tor para la navegación anónima a través de internet, esta herramienta se puede utilizar como un servicio del sistema para compartir su anonimato a otras aplicaciones instaladas que requieran de la protección que brinda Tor, también tiene configurado el navegador Midori con el motor de búsqueda Duckduckgo seleccionado para realizar las búsquedas en internet como se muestra en la **figura 23**, de igual forma con el navegador se puede acceder a los servicios de ProtonMail y LastPass para mantener el anonimato de los mensajes de correo electrónico y la seguridad de las contraseñas del usuario como se muestra en la **figura 24**, por ultimo también tiene configurado VeraCrypt que cifra y descifra archivos para mantener la integridad de los datos, en la **figura 25** se muestra la configuración del sistema con cada herramienta y su correspondiente versión.

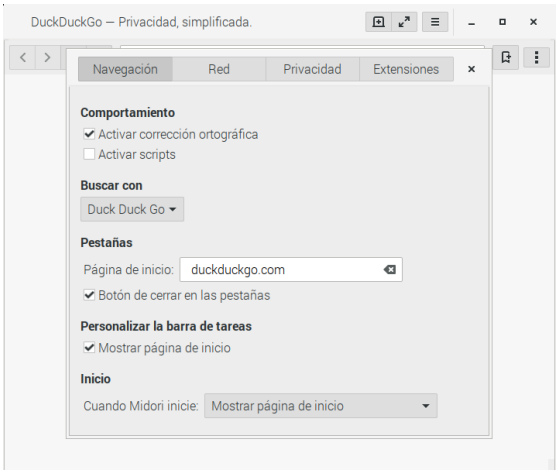


Figura 23. *Duckduckgo configurado en el navegador.*

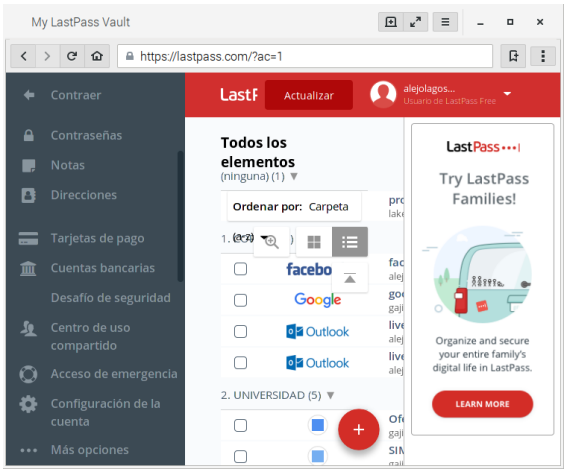


Figura 24. Cliente LastPass en el navegador.

```
pi@raspberrypi:~ $ hostnamectl
   Static hostname: raspberrypi
         Icon name: computer
        Machine ID: 6ba3ce18abd243cdae673ecc1abe19bd
           Boot ID: b77ea1cd19d14ad392d838c729993eb6
  Operating System: Raspbian GNU/Linux 10 (buster)
            Kernel: Linux 4.19.97-v7+
      Architecture: arm
pi@raspberrypi:~ $ tor --version
Tor version 0.3.5.8.
pi@raspberrypi:~ $ midori --version
midori 7.0
Copyright 2007-2018 Christian Dywan
Please report comments, suggestions and bugs to:
    https://github.com/midori-browser/core/issues
Check for new versions at:
    https://www.midori-browser.org
 pi@raspberrypi:~ $ veracrypt --version
VeraCrypt 1.21
pi@raspberrypi:~ $
```

Figura 25. Configuración 2, herramientas y versiones.

3.2.3.3. Configuración 3

El sistema operativo es DietPi el cual todo el sistema se maneja a través de la línea de comandos, este sistema tiene configurada una red privada virtual con el software OpenVPN que permite al usuario conectarse a la red de forma anónima, tiene el navegador Midori con opciones limitadas debido a la ausencia de interfaz web y por último la herramienta VeraCrypt que permite cifrar y descifrar archivos para mantener la integridad de los datos, en la siguiente **figura 26** se muestra la configuración del sistema con cada herramienta y su correspondiente versión

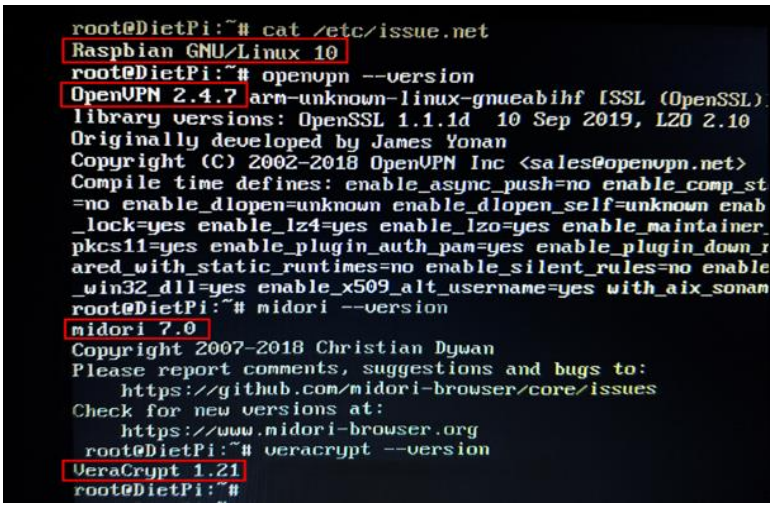


Figura 26. Configuración 3, herramientas y versiones.

3.2.3.4. Configuración 4

Corresponde al sistema operativo Parrot OS desarrollado especialmente para dispositivos SBC en su versión para las placas Raspberry Pi, el cual tiene configurado por defecto una gran variedad de herramientas que permiten al usuario manejar la seguridad de las comunicaciones de red, cabe señalar que la decisión de incluir o no cada herramienta preconfigurada corresponde al equipo encargado de mantener y desarrollar este proyecto (ParrotOS), como se había mencionado este sistema operativo cuenta con una herramienta llamada Anon-surf diseñada para mantener el anonimato de la comunicación a través de internet además cuenta con diferentes herramientas que permiten proteger cada una de las áreas de la comunicación presentadas anteriormente (**tabla 20**), a continuación en la **figura 27** se muestra la interfaz de este sistema operativo. Finalmente es importante tener en cuenta los siguientes puntos, el usuario debe contar con los conocimientos básicos para usar y mantener un sistema operativo basado en Linux, actualmente (agosto de 2020) se sigue pausado el desarrollo de este sistema operativo para la arquitectura ARM por lo que las pruebas y evaluaciones se realizaron en una versión antigua lanzada en el año 2018.

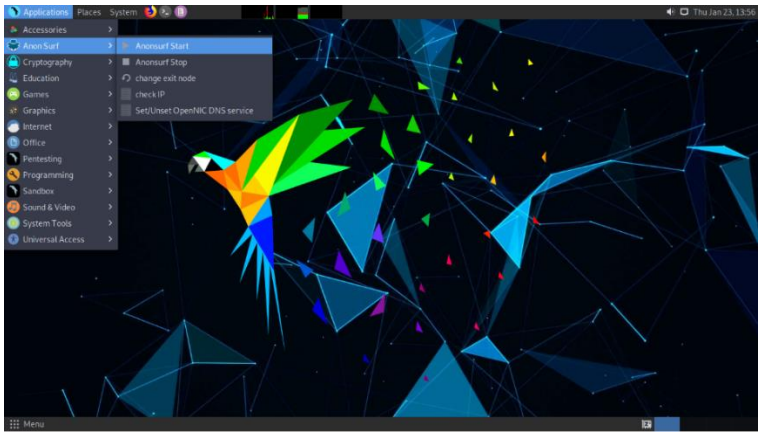


Figura 27. Interfaz y herramientas de Parrot OS.

3.2.4. Verificación de compatibilidad del módulo GSM

La comunicación móvil GSM hace parte de las tecnologías importantes usadas a nivel mundial por las personas para comunicarse, con esto se extiende en gran manera el alcance de este proyecto, en esta sección se presenta la evidencia de la compatibilidad del módulo GSM SIM800 con los dispositivos SBC (en este caso la Raspberry PI 3), a continuación, en la **figura 28** se muestra la forma correcta para conectar el módulo GSM con el dispositivo SBC.

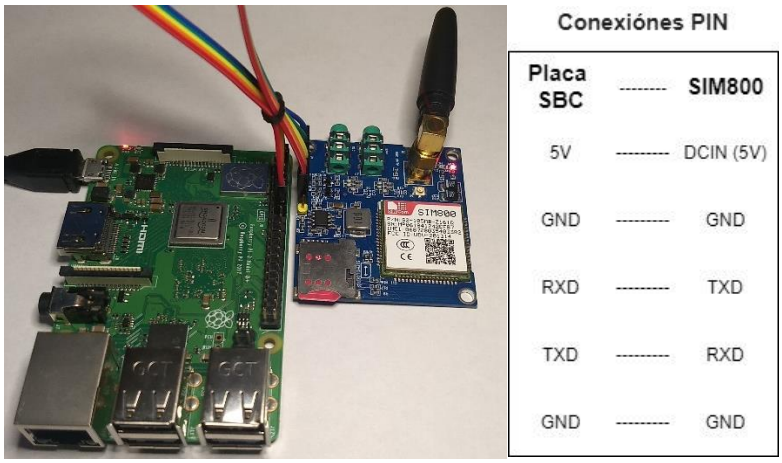


Figura 28. Conexiones PIN entre dispositivo SBC y módulo GSM.

Es importante señalar que todos los dispositivos SBC presentados en el top 5 de dispositivos SBC (Tabla 15) poseen los pines de conexión requeridos por el módulo GSM para su correcto funcionamiento, como se había mencionado en una sección anterior el modulo se controla mediante comandos AT, una aplicación que permite manipular el modulo a través de estos comandos se llama “minicom” desarrollada para sistemas operativos Linux, es una consola que permite introducir comandos y visualizar la respuesta o el estado del módulo como se muestra en la **figura 29**, se puede observar la respuesta del comando “ATI” que devuelve la versión del módulo y de igual forma el estado del módulo con una llamada entrante “RING”, además de los comandos para contestar, colgar y realizar una llamada desde la consola.

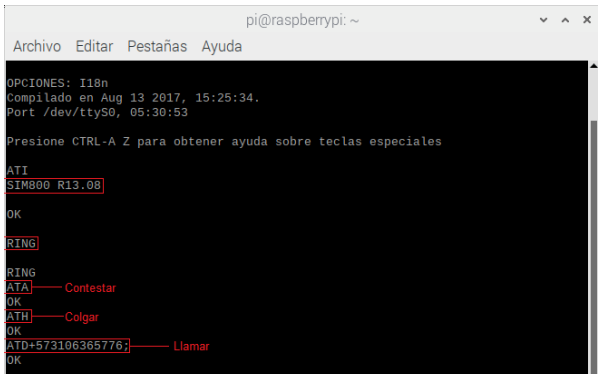


Figura 29. Consola minicom.

CAPÍTULO IV. EXPERIMENTO CONTROLADO

4.1. PRUEBAS Y EVALUACIÓNES DE LAS CONFIGURACIONES

4.1.1. Pruebas de seguridad OWASP IoT

4.1.1.1. Proyecto OWASP IoT

El Proyecto OWASP Internet of Things [53], se inició en el año 2014, está diseñado para ayudar a los fabricantes, desarrolladores y consumidores a comprender mejor los problemas de seguridad asociados a IoT (Internet of Things), y para permitir a los usuarios en cualquier contexto tomar mejores decisiones de seguridad al construir, implementar o evaluar tecnologías IoT, la guía para pruebas IoT de OWASP más reciente corresponde a OWASP IoT Top 10 del año 2018. El proyecto busca definir una estructura para varios sub-proyectos de IoT separados en las siguientes 10 categorías.

4.1.1.2. Categorías de OWASP IoT 2018.

1. Contraseñas débiles, adivinables o codificadas

Uso de credenciales fácilmente brutales, disponibles públicamente o que no se pueden cambiar, incluidas las puertas traseras en el firmware o el software del cliente que otorgan acceso no autorizado a los sistemas implementados.

2. Servicios de red inseguros

Servicios de red innecesarios o inseguros que se ejecutan en el propio dispositivo, especialmente aquellos expuestos a Internet, que comprometen la confidencialidad, integridad / autenticidad o disponibilidad de información o permiten el control remoto no autorizado.

3. Interfaces inseguras del ecosistema

Web insegura, API de back-end, nube o interfaces móviles en el ecosistema fuera del dispositivo que permite comprometer el dispositivo o sus componentes relacionados. Los problemas comunes incluyen la falta de autenticación / autorización, la falta de cifrado o la debilidad, y la falta de filtrado de entrada y salida.

4. Falta de mecanismo de actualización segura

Falta de capacidad para actualizar de forma segura el dispositivo. Esto incluye la falta de validación de firmware en el dispositivo, la falta de entrega segura (sin cifrar en tránsito), la falta de mecanismos antirretroceso y la falta de notificaciones de cambios de seguridad debido a actualizaciones.

5. Uso de componentes inseguros u obsoletos

Uso de componentes / bibliotecas de software obsoletos o inseguros que podrían permitir que el dispositivo se vea comprometido. Esto incluye la personalización insegura de las plataformas del sistema operativo y el uso de componentes de software o hardware de terceros de una cadena de suministro comprometida.

6. Protección de privacidad insuficiente

La información personal del usuario almacenada en el dispositivo o en el ecosistema que se utiliza de forma insegura, inadecuada o sin permiso.

7. Transferencia y almacenamiento de datos inseguros

Falta de cifrado o control de acceso de datos confidenciales en cualquier parte del ecosistema, incluso en reposo, en tránsito o durante el procesamiento.

8. Falta de gestión de dispositivos

Falta de soporte de seguridad en dispositivos implementados en producción, incluyendo gestión de activos, gestión de actualizaciones, desmantelamiento seguro, monitoreo de sistemas y capacidades de respuesta.

9. Configuración predeterminada insegura

Los dispositivos o sistemas enviados con configuraciones predeterminadas inseguras o carecen de la capacidad de hacer que el sistema sea más seguro al restringir a los operadores la modificación de las configuraciones.

10. Falta de endurecimiento físico

Falta de medidas de endurecimiento físico, lo que permite a los atacantes potenciales obtener información confidencial que puede ayudar en un futuro ataque remoto o tomar el control local del dispositivo.

4.1.1.3. Guía de pruebas de seguridad OWASP IoT

La guía a continuación está en un nivel básico, brindando a los evaluadores de dispositivos y aplicaciones un conjunto básico de pautas para considerar desde su

perspectiva. Esta no es una lista exhaustiva de consideraciones y no debe tratarse como tal, pero garantizar que estos fundamentos estén cubiertos mejorará en gran medida la seguridad de cualquier producto IoT.

En el **Anexo H** se muestra la tabla completa con las 50 pruebas de seguridad OWASP IoT agrupadas en las 10 categorías mencionadas anteriormente.

4.1.2. Evaluación de las configuraciones

4.1.2.1. Criterios de evaluación de las configuraciones

Se establecieron estos criterios con el objetivo de asegurar una apropiada evaluación de cada una de las configuraciones planteadas en la **tabla 20** e implementadas en la sección anterior (**sección 3.2**), los siguientes criterios se fijaron para determinar cuál de todas es la configuración apropiada para continuar con el desarrollo del prototipo teniendo como referencia los requerimientos de este proyecto. Primeramente, se definieron las **características** con las que debe cumplir cada configuración, en este caso fueron las siguientes: *Anonimato, Rendimiento, Área Protegida y OWASP IoT*. Cada configuración cuenta con sus **especificaciones** y cada especificación posee su correspondiente **valor**, es decir que cada característica aporta un valor que al sumarlo finalmente genera el puntaje para la configuración, cabe señalar que en la característica anonimato sus especificaciones son incluyentes dependiendo de la configuración seleccionada, en otras palabras, una configuración puede cumplir con A1, A2, A3 o A4 especificaciones de esa característica. La relación entre característica y especificación(es) está dada por los siguientes parámetros:

El ***Anonimato*** tiene 4 especificaciones que en este caso evalúan la seguridad del área denominada "*Seguridad de la red*" (*en la tabla 20*) y corresponden a las mismas especificaciones establecidas en el estudio de herramientas. El **Área Protegida** tiene 5 especificaciones que corresponden a las 5 áreas restantes en la *tabla 20* (excluyendo "Sistema operativo") en otras palabras es la cantidad de áreas que protege la configuración. El ***Rendimiento*** corresponde a los recursos de memoria RAM (incluido buffer y cache) que necesita cada configuración para mantener el sistema operativo en ejecución con sus herramientas de anonimato en su estado activo o en funcionamiento, en otros términos a mayor espacio de memoria disponible mayor es el puntaje, es preciso aclarar que todas estas pruebas de memoria se realizaron utilizando el mismo dispositivo hardware, para estas pruebas en particular se seleccionó el "*peor caso*" del top 3 de dispositivos (*tabla 19*) es decir la placa Raspberry Pi 3 debido a que es el dispositivo con menor capacidad de memoria RAM (1GB) en comparación a los demás dispositivos, con este "*peor caso*" se comprobó que si es posible la ejecución de cada una de las configuraciones. La característica **OWASP IoT** corresponde a las pruebas presentadas anteriormente (*sección 3.3.1*), se evaluaron las configuraciones teniendo en cuenta cada una de las pruebas establecidas en el proyecto OWASP IoT, es decir que el valor obtenido por una configuración está dado por la cantidad total de pruebas aprobadas, son 50 el total de las pruebas de OWASP IoT y para este caso cada prueba aprobada

aporta 0,1 al valor final. A continuación, en la **tabla 22** se muestra la distribución mencionada.

Característica	Especificación		Valor	
Anonimato	**A1**	Técnicas de ocultamiento de los identificadores de la comunicación.	0 < x ≤ 1,25	$\sum_{i=0}^{4} Ai$
	A2	Técnicas de protección del contenido de la comunicación.	0 < x ≤ 1,25	
	A3	Técnicas de protección de los servidores o nodos de la comunicación.	0 < x ≤ 1,25	
	A4	Técnicas de protección contra ataques de red.	0 < x ≤ 1,25	
Área Protegida	**P1**	Privacidad en el motor de búsqueda	x=1	$\sum_{i=0}^{5} APi$
	P2	Cliente de mensajería instantánea	x=1	
	P3	Privacidad en el navegador	x=1	
	P4	Cliente de administración de contraseñas	x=1	
	P5	Cifrado de datos	x=1	
Rendimiento	Valor 0 = no hay memoria disponible. Valor 5 = el 100% de la memoria está disponible.		0 < x ≤ 5	
OWASP IoT	Cantidad de pruebas OWASP IoT aprobadas. Totalidad de pruebas = 50 Valor por prueba aprobada = 0,1		0 < x ≤ 5	

Tabla 22. Criterios de evaluación de configuraciones.

4.1.2.2. Resultados de la evaluación de las configuraciones

Para el análisis de estos resultados se transformó el puntaje obtenido por cada configuración evaluada a su valor porcentual para catalogarlo como se muestra en la siguiente **tabla 23**, para esta evaluación se determinaron 5 características presentadas anteriormente las cuales aportan cada una un valor máximo establecido de la siguiente forma: *Anonimato*(**5**), *Área Protegida*(**5**), *Rendimiento*(**5**) y *OWASP IoT*(**5**), es decir que el valor máximo que podría obtener una configuración es **20** que corresponde al **100%**, con esta valoración se logra determinar que configuración o configuraciones son las adecuadas para este proyecto conservando un equilibrio entre su característica principal que es el anonimato, las áreas que logra anonimizar y el rendimiento de la CPU ya que los dispositivos SBC cuentan con capacidades de hardware limitadas, y además debe aprobar el mayor número de pruebas diseñadas, por el proyecto OWASP IoT, para este tipo de proyecto o prototipo. Finalmente se procede con la valoración porcentual y cualitativa para

clasificar cada una de las configuraciones evaluadas como se observa en la siguiente tabla.

Valoración (%)	Cualitativo
75 < x ≤ 100	Muy Alto
50 < x ≤ 75	Alto
25 < x ≤ 50	Medio
0 < x ≤ 25	Bajo

Tabla 23. Clasificación para cada configuración.

A continuación, en la **tabla 24** se presentan los resultados de la evaluación con el puntaje obtenido por cada configuración y su correspondiente valor porcentual, asimismo se muestran las herramientas ordenadas de mayor a menor puntaje en su correspondiente área.

Configuracion	Anonimato				Area Protegida					Rendimiento	OWASP IoT	Puntaje	Porcentaje	Cualitativo
	A1	A2	A3	A4	P1	P2	P3	P4	P5					
C1	1	1,2	1	1	NA	1	1	NA	1	4	2,2	13,4	67,0	Alto
C2	1,2	1,2	1	1	1	1	1	1	1	3,2	3,5	16,2	81,0	Muy Alto
C3	1	1,2	1	1	NA	NA	1	NA	1	4,7	2,1	13	65,0	Alto
C4	1,2	1,2	1	1	1	1	1	1	1	1,5	3,6	14,6	73,0	Alto

Tabla 24. Evaluación de las configuraciones.

4.1.2.3. Análisis y selección de la configuración

Con respecto a los datos presentados en la anterior ***tabla 24*** se pueden sacar las siguientes conclusiones: En la característica ***Anonimato*** al sumar sus valores para cada configuración se obtiene que C2 y C4 logran la mejor puntuación (4,5) en comparación a las demás configuraciones (4,2), esto se debe a que C2 y C4 utilizan Tor como servicio de anonimato para la red en comparación con las demás que utilizan una VPN, este puntaje es mayor gracias a la protección extra que tiene la red Tor al lograr ocultar la ruta de la comunicación y utilizar un sistema de cifrado que permite resguardar el contenido de la comunicación con su ubicación original de una mejor forma que la VPN, además con la característica ***Área Protegida*** se puede notar como las configuraciones C2 y C4 a causa de su sistema operativo permiten proteger todas las áreas que pueden resultar vulnerables para el usuario (puntuación 5), esto se presenta como una desventaja si se compara con la característica ***Rendimiento*** donde C2 y C4 tienen la puntuación más baja de esta columna, esto se debe a que C1 y C3 (es decir Raspbian Buster Lite y DietPi) son sistemas diseñados específicamente para aprovechar de forma óptima los recursos de máquina del dispositivo SBC, debido a esto el sistema tiene algunas limitaciones de uso que no permiten proteger todas las áreas de la comunicación de un usuario como se ve en la columna *Área Protegida* donde C1 y C3 obtuvieron puntajes bajos, adicionalmente estas limitaciones también afectaron sus puntuaciones obtenidas en la columna **OWASP IoT** donde no se pudieron aplicar muchas de las pruebas debido a la ausencia de interfaz (categorías I1 y I7 en el *anexo*), el **Anexo I** muestra las pruebas OWASP IoT realizadas para cada configuración, estas pruebas de seguridad se realizaron utilizando el sistema Kali Linux el cual es un sistema operativo que contiene una gran variedad de herramientas de la seguridad informática listas para realizar cada una de las pruebas requeridas, este sistema

permite realizar pruebas de penetración avanzadas en redes de computadores, sistemas operativos, servidores web, dispositivos IoT entre muchos otros. Finalmente, la configuración seleccionada para continuar con el desarrollo del proyecto fue C2 la cual obtuvo el mayor puntaje como se ve en la **tabla 24** sombreada en color gris, a continuación, en la **tabla 25** se presenta esta configuración C2 con sus correspondientes herramientas.

Área	C2
Sistema operativo	Raspbian Buster
Seguridad de la red	Red Tor
Privacidad en el motor de búsqueda	Duck Duck Go
Cliente de mensajería instantánea	ProtonMail
Privacidad en el navegador	Midori
Cliente de administración de contraseñas	LastPass
Cifrado de datos	VeraCrypt

Tabla 25. Configuración seleccionada para el prototipo.

4.1.3. Configuración del servicio web anónimo

4.1.3.1. Punto de acceso anónimo

El punto de acceso inalámbrico se implementó con la finalidad de compartir con los clientes el servicio de navegación anónima previamente configurado en el sistema, dicho de otra forma, los usuarios podrán conectarse a una red WiFi creada por el sistema y navegar a través de internet de forma anónima, para esta configuración se utilizó la entrada Ethernet y la tarjeta WiFi del dispositivo, donde la entrada Ethernet es la conexión a internet proporcionada por el ISP (proveedor de servicios de internet) y la tarjeta WiFi proporciona el punto de acceso inalámbrico para los usuarios, la configuración de red se realizó de tipo NAT es decir que el sistema actúa como un enrutador y todo el tráfico detrás de él pasa a una nueva red, también actúa como un servidor DHCP y un servidor DNS para los clientes, esto permite que los dispositivos inalámbricos conectados al punto de acceso inalámbrico sean invisibles para los dispositivos conectados en la red local como por ejemplo un router o switch, ya que todos estarán ocultos detrás de una dirección IP.

4.1.3.2. Crear el punto de acceso inalámbrico

los siguientes son los pasos o comandos que se deben seguir para crear correctamente el punto de acceso.

Primeramente, se debe verificar el nombre de las interfaces de red en el sistema como se muestra en la siguiente **figura 30.**

```
$ sudo ifconfig
```

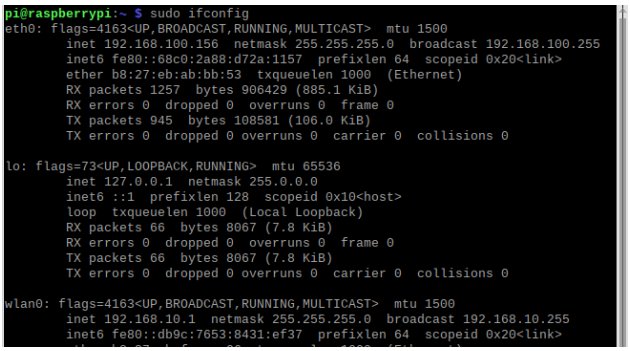


Figura 30. Interfaces de red.

En este caso los nombres correspondientes son Ethernet=eth0 y WiFi=wlan0, teniendo identificados los nombres que se usaran para toda eta configuración se procede a instalar en software necesario para crear y configurar el punto de acceso con los siguientes comandos

```
$ sudo apt-get install dnsmasq hostapd
```

con el software instalado procedemos a configurar el punto de acceso, inicialmente se debe fijar una dirección IP estática la cual es la puerta de entrada para el acceso inalámbrico para esto se debe entrar al siguiente archivo dhcpcd.conf

```
$ sudo nano /etc/dhcpcd.conf
```

y agregamos los siguientes parámetros

```
interface wlan0
    static ip_address=192.168.100.1/24
    nohook wpa_supplicant
```

con lo anterior le indicamos al sistema que la interface usaremos la interfaz wlan0 (WiFi) para crear el punto de acceso con 192.168.100.1 como su dirección IP, seguido a esto debemos configurar dnsmasq para proporcionar las direcciones IP correctas para las conexiones del punto de acceso, para esto editamos el archivo dnsmasq.conf

```
$ sudo nano /etc/dnsmasq.conf
```

y agregamos los siguientes parámetros

```
interface=wlan0
    dhcp-range=192.168.100.2,192.168.100.50,255.255.255.0,24h
server=8.8.8.8
listen-address=127.0.0.1
```

listen-address=192.168.100.1

con lo anterior indicamos la interfaz a utilizar y asignamos el rango de las direcciones IP para los clientes en este caso 192.168.100.2 -192.168.100.50 es decir que hay 48 direcciones IP disponibles para los clientes, cabe señalar que este rango se puede fijar con valores pequeños para limitar la cantidad de clientes conectados al punto de acceso, continuamos configurando los parámetros del punto de acceso para esto editamos el archivo hostapd.conf

$ sudo nano /etc/hostapd/hostapd.conf

los parámetros deben quedar con se muestra en la siguiente **figura 31.**

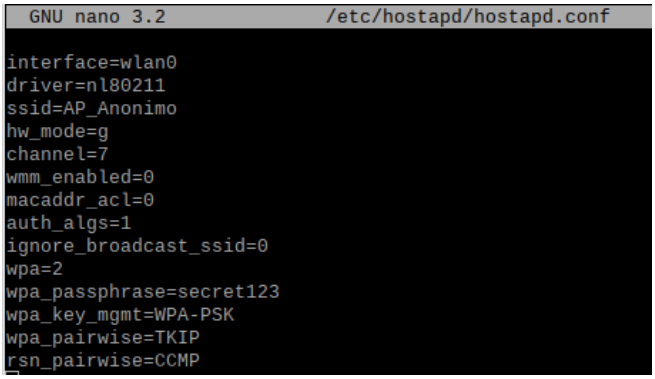


Figura 31. Configuración del punto de acceso.

El parámetro ssid indica el nombre del punto de acceso al cual el usuario se va a conectar en este caso "**AP_Anonimo**", wpa_passphrase corresponde a la contraseña del punto de acceso se debe tener en cuenta que la cantidad de caracteres debe estar entre 8 y 64 en este caso "**secret123**", las demás son configuraciones internas del punto de acceso como la interfaz a utilizar con su correspondiente driver, el canal y el tipo de cifrado entre otros, una vez agregada esta configuración, necesitamos decirle a hostapd que la use por defecto, para ello editamos el siguiente archivo hostapd

$ sudo nano /etc/default/hostapd

buscamos la línea #DAEMON_CONF y agregamos la siguiente información

DAEMON_CONF="/etc/hostapd/hostapd.conf"

debemos tener en cuenta que el # sea borrado para que esta sentencia sea ejecutada, lo siguiente es configurar hostapd para que se inicie con el arranque del sistema para esto se ejecutan los siguientes comandos

$ sudo systemctl unmask hostapd

$ sudo systemctl enable hostapd

Debemos asegurarnos que el reenvío de red ipv4 esté habilitado editando el archivo sysctl.conf

```
$ sudo nano /etc/sysctl.conf
```

buscamos la línea “# net.ipv4.ip_forward=1”, borramos el símbolo # y como resultado tendremos lo siguiente:

```
net.ipv4.ip_forward=1
```

a continuación, agregamos las reglas de enrutamiento en iptables:

```
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

las reglas se deben guardar en un archivo para cargarlas automáticamente en el arranque con el siguiente comando:

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

para cargar el archivo en el arranque debemos editar el archivo rc.local:

```
$ sudo nano /etc/rc.local
```

antes de la sentencia “exit 0” debemos agregar el siguiente parámetro:

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

finalmente se debe reiniciar el sistema y ahora se debería visualizar el punto de acceso llamado “**AP_Anonimo**” para que el cliente pueda conectarse con la contraseña “secret123” como se muestra en la **figura 32.**

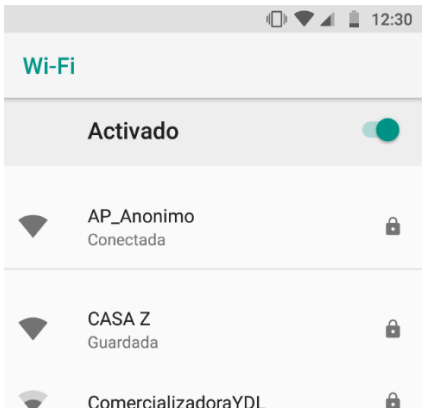


Figura 32. Cliente conectado al punto de acceso.

4.1.3.3. Configuración del servicio de navegación anónima

Para este paso debemos configurar la red Tor y enrutarla con el punto de acceso para que cuando el cliente se conecte a la red “**AP_Anonimo**” pueda navegar anónimamente a través de la red Tor, primeramente, debemos configurar el servicio Tor para esto debemos editar el archivo torrc

$ sudo nano /etc/tor/torrc

buscar la siguiente línea (línea 13 aproximadamente)

https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ#torrc

debajo se debe agregar la siguiente configuración

Log notice file /var/log/tor/notices.log
VirtualAddrNetwork 10.192.0.0/10
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1
TransPort 9040
TransListenAddress 192.168.100.2
DNSPort 53
DNSListenAddress 192.168.100.2

para verificar que el servicio Tor funcione correctamente podemos usar los siguientes comandos

$ sudo service tor start

$ sudo service tor status

continuamos configurando la red Tor para que inicie al reiniciar el sistema

$ sudo update-rc.d tor enable

lo siguiente es configurar las reglas de enrutamiento en iptables, para limpiar las reglas en el firewall

$ sudo iptables -F

$ sudo iptables -t nat –F

para permitir la conexión SSH con el servidor después de configurar iptables

$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 22 -j REDIRECT --to-ports 22

Para que el proxy Tor resuelva los nombres DNS

*$ sudo iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j REDIRECT --to-*ports 53

Para recopilar todo el tráfico y reenvíalo al puerto 9040 (lo envía a la red Tor)

$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --syn -j REDIRECT --to-ports 9040

verificamos las reglas insertadas con el siguiente comando

$ sudo iptables -t nat –L

si las reglas se configuraron correctamente la salida debe ser como se muestra en la siguiente **figura 33.**

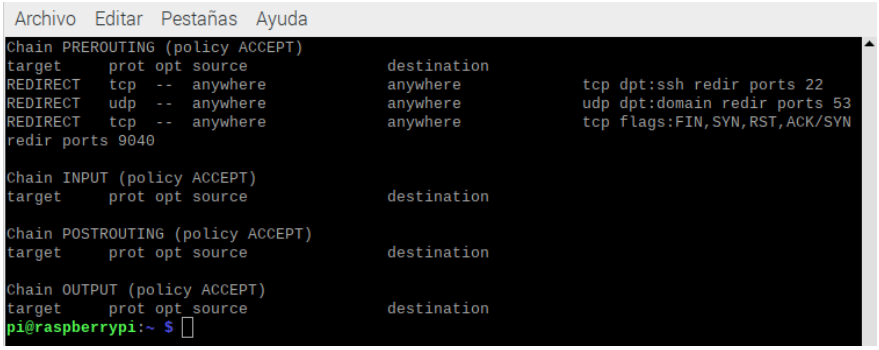


Figura 33. Reglas de enrutamiento en iptables.

Por último, debemos guardar estas reglas para que inicien con el sistema para ello se usan los siguientes comandos:

```
$ sudo sh -c "iptables-save > /etc/iptables.rules"
$ sudo nano /etc/network/if-pre-up.d/iptables
```

agregamos la siguiente secuencia de comandos en el archivo:

```
#!/bin/bash
/sbin/iptables-restore < /etc/iptables.rules
```

luego hacemos que el archivo sea ejecutable:

```
$ sudo chomod +x /etc/network/if-pre-up.d/iptables
```

Seguido a esto debemos reiniciar el sistema y verificar que las reglas en iptables sigan siendo las mismas como en la **figura 33.** Si todas las configuraciones se realizaron correctamente el resultado es un punto de acceso que inicia con el sistema y que actúa como una puerta de entrada para los clientes hacia la red de anonimato Tor.

4.1.3.4. Análisis y resultados del servicio web anónimo

Inicialmente antes de conectar cualquier cliente a la red anónima creada anteriormente para la navegación anónima en internet, en la siguiente **figura 34** se muestra un cliente (Smartphone) conectado a una red doméstica en la ciudad de Popayán con dirección IP 67.73.224.6 con el navegador web en el sitio whatismyip.net que permite consultar información relacionada a la identidad del dispositivo en la red como por ejemplo dirección IP, dirección local, ubicación y sistema operativo entre otros datos.

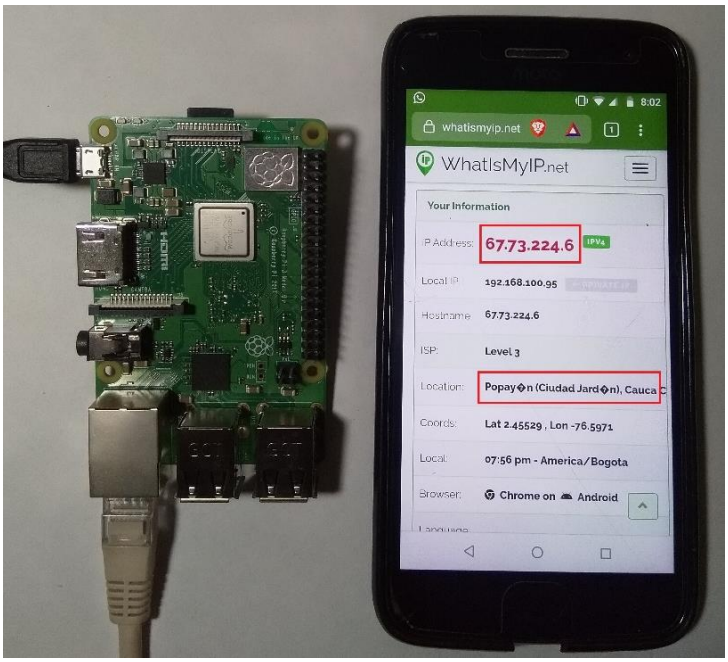


Figura 34. Cliente conectado a la red doméstica.

El resultado de conectarse a la red "**AP_Anonimo**" se presenta en la siguiente **figura 35** donde se muestra el mismo cliente (Smartphone) conectado al punto de acceso anónimo, también se muestra como son las conexiones del dispositivo para que este funcione correctamente según las configuraciones realizadas anteriormente.

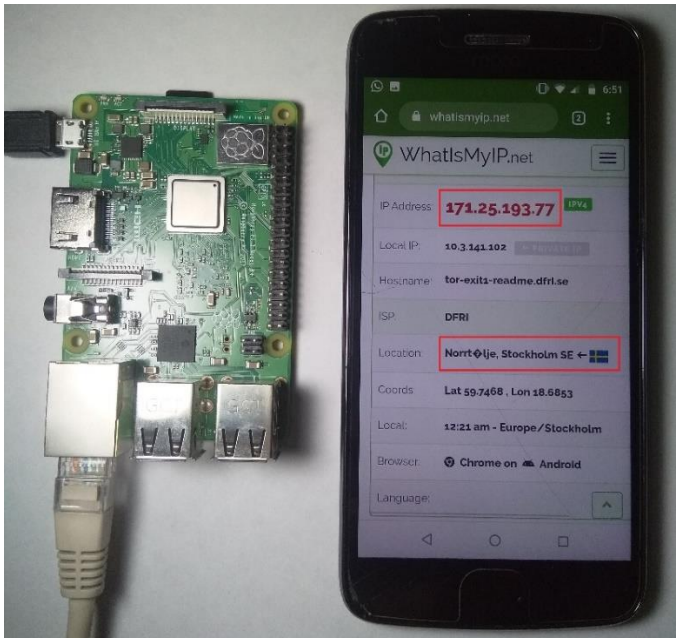


Figura 35. Cliente conectado a la red anónima.

En la figura anterior se puede observar que el dispositivo es la Raspberry Pi 3 conectado a internet a través de la conexión Ethernet y un cable de alimentación de 5V, por otro lado, el cliente Smartphone está conectado a la red WiFi “AP_Anonimo” con el navegador en la página whatismyip.net para verificar que la IP corresponda con un nodo de la red Tor, esta página muestra la dirección IP con la que el dispositivo navega a través de internet en este caso la dirección IP es 171.25.193.77 que corresponde a un nodo de salida Tor ubicado en la ciudad de Estocolmo en Suecia.

Adicionalmente en otro cliente (computador portátil con sistema operativo Windows 10) conectado a la misma red se realizaron varias pruebas para verificar que la conexión a internet a través del prototipo sea anónima, para ello se consultaron alrededor de 10 sitios web que permitieron verificar el anonimato de la conexión, en la siguiente **figura 36** se presentan tres de los sitios consultados.

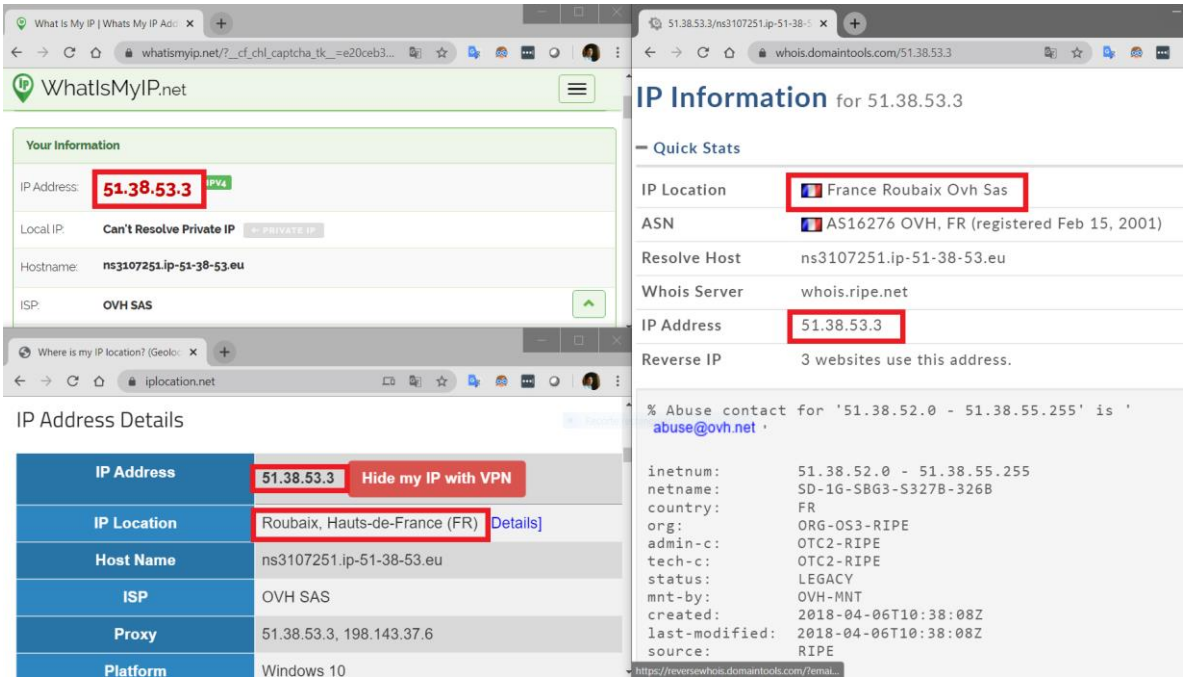


Figura 36. Cliente conectado a la red anónima.

Algunos puntos a tener en cuenta son:

- El cliente (Smartphone) al conectarse al punto de acceso inicialmente se demora alrededor de 5 a 20 segundos para establecer la primera conexión con la red esto es debido a que la comunicación se hace a través de los nodos de Tor los cuales están dispersos alrededor del mundo, en otras palabras el tiempo depende de la ruta o distancia entre los nodos seleccionados por Tor, al conectarse a la red WiFi en el dispositivo muestra inicialmente un mensaje que dice “Conectado, sin conexión a internet” segundos más tarde muestra el

mensaje “Conectado”, después de conectarse a la red Tor la latencia disminuirá, pero está siempre depende de la ruta de la comunicación y el ancho de banda del internet que se está usando.

- El cliente está conectado con una IP extranjera así puede burlar la censura impuesta a los sitios censurados en su ubicación real (ejemplo: Colombia), por el contrario, no podría acceder a las paginas censuradas en la IP extranjera (en el caso anterior Suecia **figura 35**), esto depende del nodo de salida al cual esté conectado, para esto puede reiniciar el servicio Tor para que se conecte a otro nodo de salida.
- Cada cliente conectado tiene su propia ruta a la red Tor, es decir si hay dos o más dispositivos conectados cada uno tendrá un nodo de salida y dirección IP diferente, en la siguiente **figura 37** se observan tres clientes conectados al punto de acceso anónimo, en este caso son dos dispositivos móviles (Smartphone) y un computador portátil con sistema operativo Windows 10.

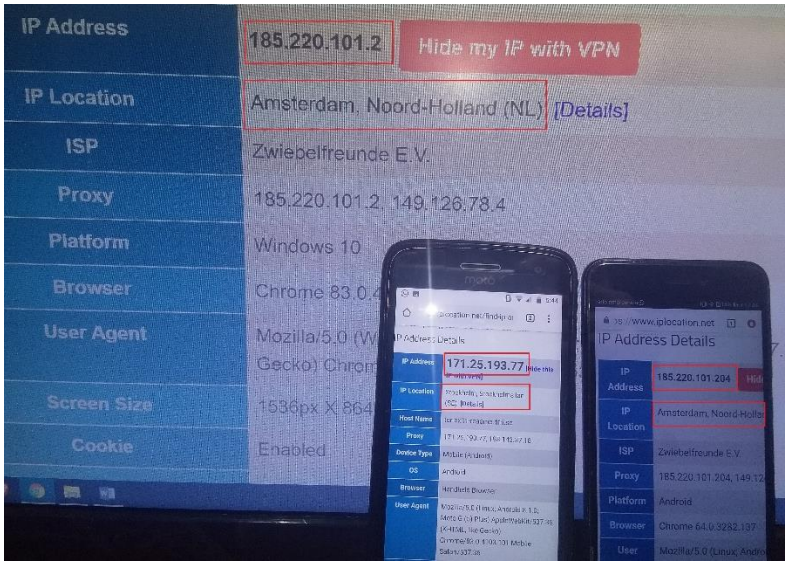


Figura 37. Cliente conectado a la red anónima.

- Además de navegar de forma anónima a través de la web (www) el cliente tiene la posibilidad de navegar por los enlaces de la Deep web (.onion).
- El servicio Tor permite hacer algunas modificaciones para disminuir su latencia un poco y elegir los nodos de salida y entrada del circuito, para esto se debe editar el archivo torrc de la siguiente manera (esto puede colocarse después de las modificaciones realizadas anteriormente)

```
$ sudo nano /etc/tor/torrc
```

los parámetros *EntryNodes* y *ExitNodes* se usan para declarar el país al que pertenece el nodo de entrada y salida correspondientemente como se indica en el siguiente ejemplo:

```
EntryNodes {ca},{us},{mx} StrictNodes 1
```

ExitNodes {ca},{us},{mx} StrictNodes 1

Con las sentencias *EntryNodes* y *ExitNodes* le indicamos al servicio Tor que el nodo de entrada y salida debe pertenecer a los países Canadá {ca}, Estados unidos {us} y Mexico {mx}, en el caso de no encontrar un nodo disponible en el primer país {ca} Tor continua con el siguiente código hasta el final, por otro lado, si no encuentra un nodo disponible el servidor envía un error de tiempo de conexión excedido debido a la sentencia *StrictNodes* 1, por el contrario si la sentencia es *StrictNodes* 0 al llegar al final y no se encuentra un nodo disponible se elige un nodo aleatorio que si este disponible en la red Tor.

4.2. EVALUACIÓN DE PROTOTIPOS

4.2.1. Criterios de evaluación de prototipos

Se realizó la evaluación de los prototipos usando los dos primeros dispositivos del top 5 de dispositivos SBC (**tabla 15**) es decir Raspberry PI 3 y Raspberry PI 4, el dispositivo Rock PI 4 no se evaluó debido a que cuenta con características similares a la Raspberry PI 4 y adicionalmente presenta una limitante el cual es su tiempo de entrega en Colombia que es de 4 a 6 semanas. Los principales criterios de evaluación para estos dos dispositivos son *el Rendimiento* y *la Seguridad,* con respecto al *rendimiento* del dispositivo se determinó el ***porcentaje de memoria RAM disponible*** en dos escenarios puntuales, el escenario 1 es cuando se utiliza la configuración por defecto, es decir cuando el dispositivo solo se utiliza como un enrutador anónimo para que los clientes se conecten a la red anónima, el escenario 2 es cuando el cliente quiere usar adicionalmente las herramientas configuradas en el sistema como por ejemplo el gestor de contraseñas, el cliente de mensajería entre otros, con respecto a los criterios de *seguridad* se evaluó que cada prototipo cumpla con los controles de seguridad presentados en la sección ***2.8 Controles de seguridad para comunicaciones de red*** y adicionalmente que cumplan con las pruebas de seguridad definidas por el proyecto OWASP presentadas en la sección ***4.1.1 Pruebas de seguridad OWASP IoT***, por último se incluyó el *Costo* de cada dispositivo.

					RPI 3	**RPI 4**
Rendimiento (Memoria RAM disponible)	**Escen**	Raspbian Buster OS Servicio TOR Punto de acceso Anónimo			**63%**	**90%**
	Escenario 2	Raspbian Buster OS Servicio TOR Punto de acceso Anónimo	**+**	Duck Duck Go ProtonMail, Midori, LastPass Veracrypt	**3%**	**68%**

Seguridad	Controles Norma ISO 27002	**9 / 9**	**9 / 9**
	Pruebas OWASP IoT	**35 / 35**	**35 / 35**
Costo	Raspberry PI 3  + MicroSD 16GB Cable Ethernet	1GB RAM **$185.000**	Raspberry PI 4  4GB RAM **$265.000**

Leyenda: RPI = Raspberry PI.

Tabla 26. Evaluación Raspberry PI 3 vs Raspberry PI 4.

4.2.2. Análisis de la evaluación de prototipos

Es importante destacar la gran diferencia en cuanto a memoria RAM entre los dispositivos, aunque su velocidad de procesamiento y el número de núcleos es el mismo la placa Raspberry PI 4 posee 4 veces más capacidad de memoria RAM lo cual se ve evidenciado en los porcentajes obtenidos para la evaluación de rendimiento, con respecto a esta evaluación de rendimiento se consideraron los dos escenarios en los que el cliente puede hacer uso del prototipo para comunicarse anónimamente a través de la web, en el escenario 1 los dos prototipos obtuvieron buenos porcentajes de memoria con valores por encima del 50%, esto quiere decir que hay disponible más de la mitad de memoria para que el o los clientes usen el prototipo en este escenario 1 lo cual permite al dispositivo funcionar con un excelente rendimiento, en el escenario 2 se hace evidente la diferencia que existe de memoria ya que al utilizar las cinco herramientas al mismo tiempo la Raspberry PI 3 queda con el 3% de memoria lo cual afecta la velocidad de respuesta del sistema haciendo muy demoradas operaciones y en ocasiones puede ocasionar que el sistema quede bloqueado, para este caso el rendimiento del sistema se mantuvo establece usando máximo 2 herramientas al tiempo, esto no ocurre con la Raspberry PI 4 que al tener la misma carga de trabajo funciona correctamente y mantiene disponible más de la mitad de memoria para que el sistema pueda ejecutar otras operaciones. Con respecto a la seguridad los dos prototipos cumplen con todos los controles planteados en la sección ***2.8***, en relación con las pruebas de seguridad de OWASP IoT los prototipos cumplen con las 35 pruebas que se permiten ejecutar para esta configuración (C2 en el Anexo I), finalmente se tiene la relación de costos entre los dispositivos que incluye la memoria MicroSD donde se configura el sistema operativo y el cable Ethernet, este costo es un criterio de decisión del cliente ya que es él quien decide cual prototipo usar dependiendo de la

forma en que necesite el servicio, con respecto a lo anterior se deben tener en cuenta las siguientes condiciones, para usar el prototipo en el escenario 1 el usuario debe contar con cable de carga del dispositivo y una conexión a internet por cable ethernet, por otro lado para usar el prototipo en el escenario 2 adicionalmente a lo anterior el usuario debe contar con periféricos que le permitan utilizar el sistema y sus herramientas por ejemplo teclado, mouse y un monitor, los cuales sus costos no están incluidos en la anterior **tabla 26**, aunque si no se cuenta con estos periféricos la opción viable es configurar la herramienta VNC Server que viene incluida en el sistema operativo e instalar VNC Viewer en el computador o dispositivo móvil desde donde se quiera controlar remotamente el sistema operativo del prototipo y sus herramientas de anonimizacion configuradas.

CAPÍTULO V. CONCLUSIONES Y TRABAJOS FUTUROS

5.1 Conclusiones

- Como resultado de los estudios realizados en las **secciones 2.9**, **2.10** y **2.11** se logró diseñar una arquitectura de comunicación que permite al usuario conservar el anonimato de su identidad en cada una de las áreas que pueden ser vulneradas al momento de realizar una comunicación vía web, tal como se muestra en la **figura 8** en la **sección 3.1.1**.
- Se consiguió elaborar e implementar el diseño de red validando cada uno de los controles de seguridad presentados en la **sección 2.8**, también se realizó la correspondiente configuración del firewall para filtrar el tráfico de entrada y el punto de acceso que comparte el servicio de navegación anónima se configuro de forma NAT dado que de esta forma los usuarios conectados permanecen invisibles para un ente o dispositivo externo, tal como se muestra en la **figura 9** en la **sección 3.1.2.** con la aplicación de este diseño se aporta seguridad a la conexión de red necesaria para que el prototipo funcione correctamente.
- Como resultado de los estudios realizados en las **secciones 2.9, 2.10** y **2.11** se obtuvieron 8 casos de estudio (Tabla 21) que mediante las evaluaciones y pruebas realizadas se logró seleccionar e implementar el caso que mejor se ajustó a los requerimientos del proyecto, por consiguiente, el prototipo implementado permite la comunicación anónima navegando desde dentro del sistema operativo configurado y adicionalmente puede compartir ese anonimato por medio de una red Wi-Fi para que los usuarios o dispositivos externos se conecten, como se muestra en la sección **4.1.3.** donde se realizaron las

configuraciones finales del prototipo y se presentaron los resultados, con todo esto se obtuvo un prototipo funcional que anonimiza las comunicaciones a través de internet que adicionalmente es seguro y fácil de utilizar por los usuarios.

- Con respecto al conglomerado de artículos obtenidos en la sección **2.1 revisión de la literatura** se logró innovar con los siguientes aportes: Se implementó un prototipo que cumple con los estándares internacionales de seguridad establecidos en las normas ISO 27002 y que además cumple con las pruebas de seguridad OWASP para proyectos implementados con la tecnología IoT, adicionalmente la arquitectura desarrollada protege 7 áreas que intervienen en la comunicación del usuario (**tabla 9**), de igual forma se implementó un punto de acceso que les permite a varios usuarios hacer uso del servicio de anonimato y por último se logró mantener un equilibrio entre rendimiento y anonimato y así presentar una opción de bajo costo para los usuarios.
- A pesar de la limitada cantidad de herramientas de anonimato que hay actualmente desarrolladas para la arquitectura ARM se pudo diseñar y construir una arquitectura de comunicación eficiente y segura para los clientes, de igual forma se elaboró un diseño de red que cumple con los estándares y controles de seguridad para comunicaciones a través de la red. Según la pregunta de investigación, se logró implementar un prototipo portable y de bajo costo que le permite a uno o más usuarios mantener una comunicación anónima a través de internet y conjuntamente conservar para cada cliente su anonimato de forma independiente.
- De acuerdo con los estudios realizados se obtuvo un listado de las mejores herramientas de anonimato desarrolladas en la actualidad, en las que están incluidas las herramientas no compatibles con la arquitectura ARM que pueden ser muy útiles para los usuarios de internet que deseen mantener su identidad anónima mientras navegan por la red, por otra parte, para los usuarios o desarrolladores que desean elaborar un proyecto con la arquitectura ARM se obtuvo un ranking de dispositivos SBC y sistemas operativos compatibles para la construcción de un proyecto ARM de bajo costo.

5.2 Trabajos futuros

- Con respecto a la configuración en el área “Seguridad de la red” se puede agregar una segunda herramienta (VPN o I2P) para que el usuario pueda elegir el método de anonimato con el que quiere navegar.
- Para un mejor control y facilidad de uso del servicio Tor se puede a partir de una interfaz de usuario realizar las configuraciones al archivo torrc que es el encargado de dar los parámetros a la herramienta para su configuración y la generación de los circuitos de la comunicación.

- Para agregar una mayor portabilidad al prototipo se plantea la posibilidad de integrarle al dispositivo SBC una batería recargable, asimismo adicionar y configurar un adaptador WiFi USB para que de esta forma el prototipo no dependa del cable de carga del dispositivo y del cable de conexión Ethernet para su correcto funcionamiento.
- Como se presentó en la sección **2.15.4 verificación de compatibilidad del módulo GSM**, se puede buscar la forma de anonimizar la comunicación GSM ya sea manipulando directamente el modulo con su librería o pasar la comunicación de la red GSM a VoIP (voz sobre IP) y a continuación redirigir la comunicación a la red tor que está configurada en el sistema, de igual forma se podría utilizar el módulo GSM para que a través de la SIM (datos móviles) provea de conexión a internet al prototipo.

BIBLIOGRAFÍA

[1] A. C. Uzialko, «How and Why Businesses Collect Consumer Data,» Business News Daily, 3 August 2018. [En línea]. Available: https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[2] M. J. M. Leo, «Seguridad mundial y redes de espionaje,» Blasting News, 3 Julio 2017. [En línea]. Available: https://es.blastingnews.com/tecnologia/2017/07/seguridad-mundial-y-redes-de-espionaje-001819769.html.

[3] F. J. Pino, Piattini, Mario y Travassos, Guilherme Horta, «Managing and developing distributed research projects in software engineering by means of action-research,» *Revista Facultad de Ingenieria,* nº 68, pp. 61-74, 2013.

[4] Wohlin, Claes, Runeson, Per, Höst, Martin, Ohlsson, Magnus C., Regnell, Björn y Wesslén, Anders, Experimentation in software engineering, 2012, pp. 1-236.

[5] Felipe Muñoz, Andrés, Santiago, Mayorga y Solarte, Alejandro Pérez, «Pentesting sobre aplicaciones web basado en la metodología OWASP utilizando SBC de bajo costo,» 2018.

[6] S. Fischer-Hübner, «A Anonymity,» de *Encyclopedia of Database Systems.*, 2014.

[7] R. ASALE, «anonimizar,» "Diccionario de la lengua española" - Edición del Tricentenario, 2019. [En línea]. Available: https://dle.rae.es/?id=2jjMiRi.

[8] «network architecture - CLC Definition,» Computer Language Company, 2019. [En línea]. Available: https://www.computerlanguage.com/results.php?definition=network+architecture.

[9] «enhanced network services - CLC Definition,» Computer Language Company, 2019. [En línea]. Available: https://www.computerlanguage.com/results.php?definition=enhanced+network+services.

[10] «What is Anonymity Network? - Definition from Techopedia,» Techopedia Inc., 2019. [En línea]. Available: https://www.techopedia.com/definition/25187/anonymity-network.

[11] E. Humphreys, Implementing the ISO/IEC 27001 ISMS Standard, Second Edition ed., 2016, p. 222.

[12] «What is a Single-Board Computer (SBC)? - Definition from Techopedia,» Techopedia Inc., 2019. [En línea]. Available: https://www.techopedia.com/definition/9266/single-board-computer-sbc.

[13] «Information technology - Security techniques - Information security management systems - Requirements,» *ISO/IEC 27001:2013.*

[14] Roger Dingledine y Nick Mathewson, «Privacy & Freedom Online,» The Tor Project, [En línea]. Available: https://www.torproject.org/.

[15] «VPN Software Solutions & Services For Business | OpenVPN,» OpenVPN, 2019. [En línea]. Available: https://openvpn.net/.

[16] I. Team, «The Invisible Internet Project,» I2P Anonymous Network, [En línea]. Available: https://geti2p.net.

[17] Dawson, Maurice y Cárdenas-Haro, Jose Antonio, «Tails Linux Operating System,» *International Journal of Hyperconnectivity and the Internet of Things,* vol. 1, nº 1, pp. 47-55, 2017.

[18] «Tails - Privacy for anyone anywhere,» 2019. [En línea]. Available: https://tails.boum.org.

[19] «Whonix ™,» 2019. [En línea]. Available: https://www.whonix.org.

[20] «Qubes OS: A reasonably secure operating system,» 2019. [En línea]. Available: https://www.qubes-os.org.

[21] L. Faletra, «The advanced system for security experts, developers and crypto-addicted people.,» Parrot Linux, 2013 - 2019. [En línea]. Available: https://parrotlinux.org.

[22] «DuckDuckGo,» 2008 - 2019. [En línea]. Available: https://duckduckgo.com.

[23] «Startpage - The world's most private search engine,» 2019. [En línea]. Available: https://www.startpage.com.

[24] «TORCH: Tor Search Engine,» 2019. [En línea]. Available: http://xmh57jrzrnw6insl.onion.

[25] «Gibiru - Unfiltered private search,» [En línea]. Available: https://gibiru.com/.

[26] B. Fung, «What to expect now that Internet providers can collect and sell your Web browser history,» The Washington Post, 29 March 2017. [En línea]. Available: https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?noredirect=on.

[27] J. Zuriarrain, «Protonmail, el email que se dice inexpugnable,» EL PAÍS, 31 Mayo 2016. [En línea]. Available: https://elpais.com/tecnologia/2016/05/12/actualidad/1463071753_948615.html.

[28] «Secure email: ProtonMail is free encrypted email.,» Proton Technologies AG, 2019. [En línea]. Available: https://www.protonmail.com.

[29] «Paranoid email,» 2019. [En línea]. Available: https://paranoid.email.

[30] «Onion Mail,» OnionMail Project, 2019. [En línea]. Available: https://onionmail.info.

[31] «Ricochet,» 2019. [En línea]. Available: https://ricochet.im.

[32] «OnionShare,» 2019. [En línea]. Available: https://onionshare.org.

[33] H. R. Inc, «Epic Privacy Browser,» 2019. [En línea]. Available: https://www.epicbrowser.com.

[34] B. Eich y B. Bondy, «Secure, Fast & Private Web Browser with Adblocker,» Brave Browser, 2019. [En línea]. Available: https://brave.com.

[35] M. B. C. 2. A. r. reserved, «Midori Web Browser,» [En línea]. Available: https://www.midori-browser.org/.

[36] I. LogMeIn, «Password Manager & Vault App, Enterprise SSO & MFA,» LastPass, 2019. [En línea]. Available: https://lastpass.com.

[37] «Password Manager for Families, Businesses, Teams,» 1Password, 2019. [En línea]. Available: https://www.1Password.com.

[38] D. Inc, «Never forget another password,» Dashlane, 2019. [En línea]. Available: https://www.dashlane.com.

[39] I. Keeper Security, «Keeper® Password Manager & Digital Vault,» [En línea]. Available: https://www.keepersecurity.com/.

[40] IDRIX, «Veracrypt,» 2013 - 2019. [En línea]. Available: https://www.veracrypt.fr.

[41] «File Security Made Easy,» AxCrypt, 2001 - 2019. [En línea]. Available: https://www.axcrypt.net.

[42] Microsoft, «BitLocker (Windows),» 2019. [En línea]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

[43] «ZuluCrypt,» [En línea]. Available: https://mhogomchungu.github.io/zuluCrypt/.

[44] D. project, «FrontPage - Raspbian,» 2019. [En línea]. Available: https://raspbian.org/.

[45] U. Team, «Ubuntu MATE,» Canonical Ltd, 2019. [En línea]. Available: https://ubuntu-mate.org.

[46] Microsoft, «Overview of Windows 10 IoT - Windows IoT,» © Microsoft, 2019. [En línea]. Available: https://docs.microsoft.com/en-us/windows/iot-core/windows-iot.

[47] «RISC OS Open,» © RISC OS Open Limited, 2019. [En línea]. Available: https://www.riscosopen.org/.

[48] ©. C. 2. A. L. D. Team, «Alpine Linux,» 2019. [En línea]. Available: https://www.alpinelinux.org/.

[49] V. Theile, «OpenMediaVault - The open network attached storage solution,» 2009 - 2019. [En línea]. Available: https://www.openmediavault.org.

[50] D. Knight, «DietPi - Lightweight justice for your SBC,» © DietPi, 2018. [En línea]. Available: http://dietpi.com/.

[51] A. Casals, «pipaOS: A lighweight, fast, Raspbian based distro for Raspberry pi,» 2013 - 2018. [En línea]. Available: http://pipaos.mitako.eu/.

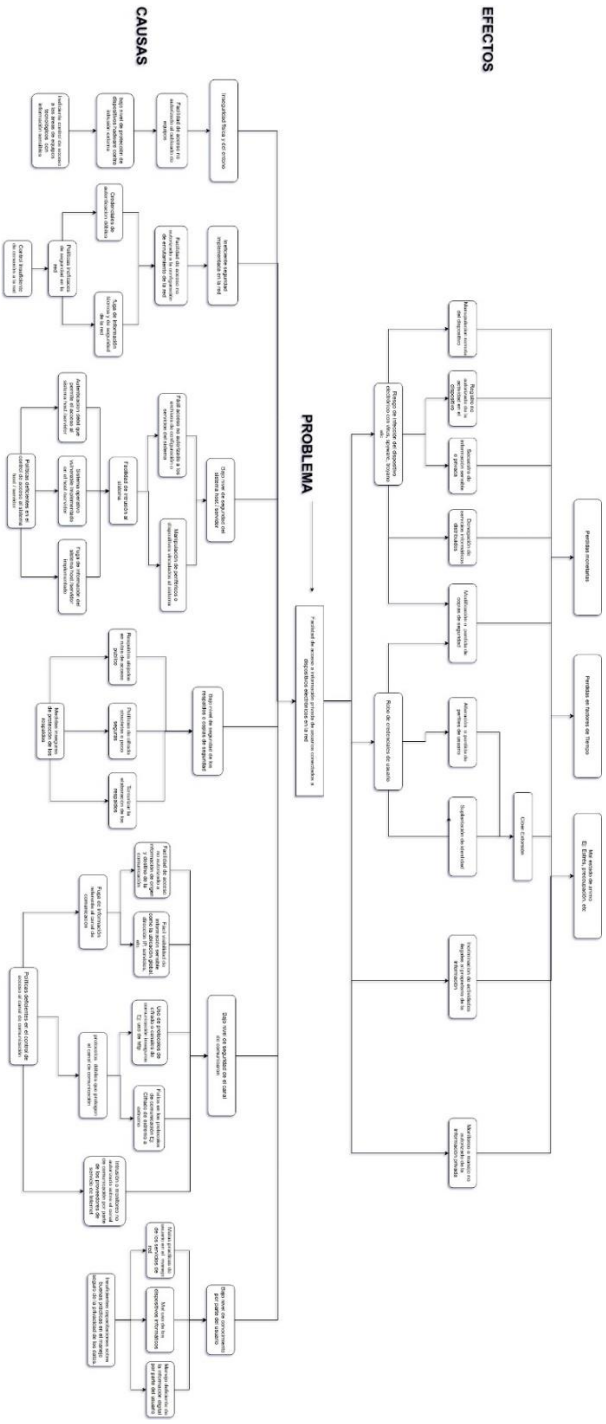
[52] C. ©. W. D. Imager, «Win32 Disk Imager Download (Latest Stable Version),» [En línea]. Available: https://win32diskimager.download/.

[53] I. Copyright OWASP Foundation, «OWASP Internet of Things,» [En línea]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

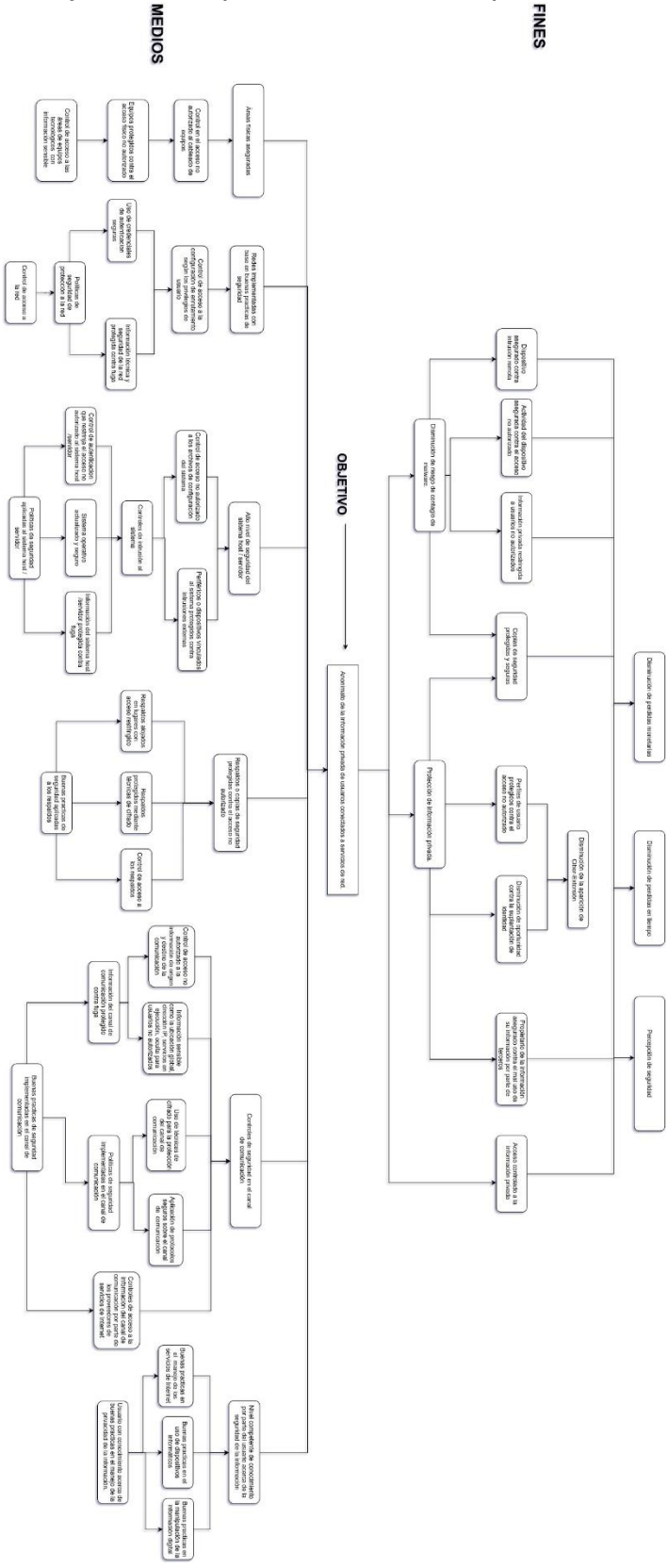
ANEXOS

Nota: en el disco (CD-ROM) adjunto al proyecto se encuentran todos los archivos originales de cada anexo con su respectivo nombre para una mejor revisión.

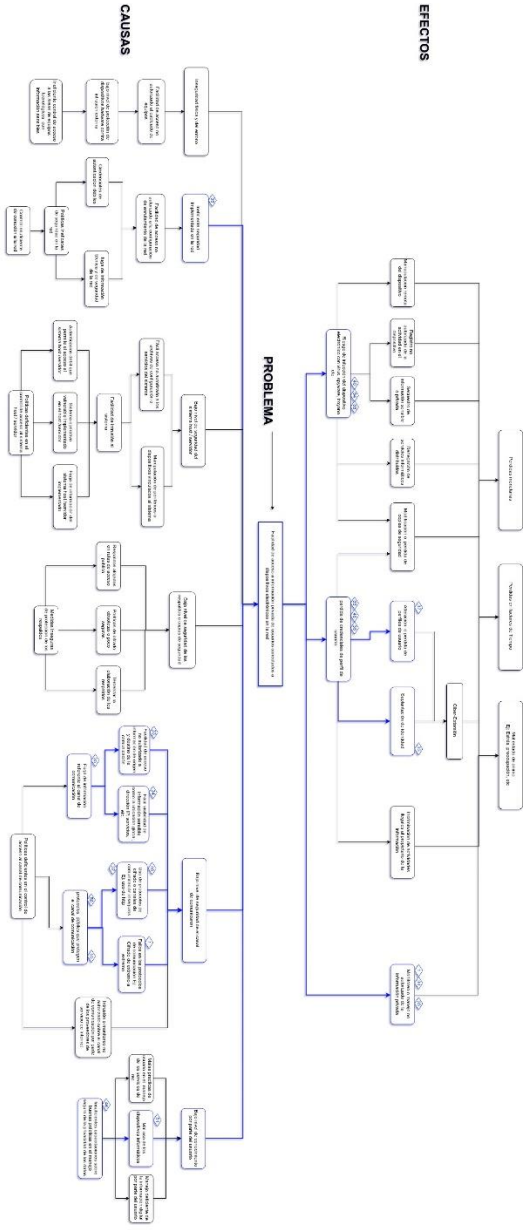
Anexo A: árbol de problemas completo con sus correspondientes causas y efectos.



Anexo B: árbol de objetivos completo con sus correspondientes medios y fines.



Anexo C: árbol de problemas completo con la referencia de los artículos relacionados.



Anexo D: tabla completa de la evaluación de *herramientas* con su correspondiente área y valoración cualitativa.

Área	Herramienta	Anonimato				Flexibilidad				Compatibilidad			Costos				Periodo				Puntaje	Porcentaje	Cualitativo
		A1	A2	A3	A4	F1	F2	F3	F4	CA1	CA2	CA3	C1	C2	C3	C4	P1	P2	P3	P4			
Seguridad de la red	Red Tor	1,2	1,2	1	1,1	NA	NA	NA	1	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	8,5	94,4	Muy Alto
	VPN	1	1,2	1	1	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	7,2	80,0	Muy Alto
	Red I2P	1	1,1	0,8	0,8	NA	NA	NA	1	NA	NA	1	NA	NA	1	1	NA	0,25	NA	NA	6,95	77,2	Muy Alto
	Servidor proxy	0,8	0,7	0,6	0,7	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	5,8	64,4	Alto
Sistemas operativos anónimos	Parrot	1,2	1,2	1	1,1	NA	NA	0,5	NA	NA	NA	1	NA	NA	1	1	NA	NA	0,5	NA	7,5	83,3	Muy Alto
	Qubes	1,2	1,2	1	1,2	NA	NA	NA	1	0	NA	NA	NA	NA	1	1	NA	NA	0,5	NA	7,1	78,9	Muy Alto
	TAILS	1,2	1,2	1	1,1	NA	NA	NA	1	0	NA	NA	NA	NA	1	1	NA	NA	0,5	NA	7	77,8	Muy Alto
	Whonix	1,2	1,2	1	1	NA	NA	NA	1	0	NA	NA	NA	NA	1	1	0	NA	NA	NA	6,4	71,1	Alto
Privacidad del motor de búsqueda	Duck duck go	0,2	0,4	0,5	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	NA	1	3,7	41,1	Medio
	StartPage	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	3	33,3	Medio
	Gibiru	0,2	0,2	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	2,9	32,2	Medio
	Torch	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	0,25	NA	NA	2,75	30,6	Medio
Cliente de mensajería instantánea	OnionShare	0,6	0,7	0,8	0,4	NA	0,25	NA	NA	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	5,75	63,9	Alto
	ProtonMail	0,6	0,7	1	0,4	NA	0,25	NA	NA	0	NA	NA	0,5	NA	0,5	NA	NA	NA	NA	1	4,95	55,0	Alto
	Ricochet	0,6	0,5	0,5	0,2	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	4,05	45,0	Medio
	OnionMail	0,6	0,5	0,6	0,4	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	3,85	42,8	Medio
	Paranoid	0,6	0,7	0,5	0,2	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	3,75	41,7	Medio
Privacidad en el navegador	Tor Browser	1,1	1,2	0,9	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	NA	NA	NA	0,5	NA	6,1	67,8	Alto
	EPIC Browser	1	1	0,8	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	5,7	63,3	Alto
	Midori	0,4	0,4	0,3	0,3	NA	NA	0,5	NA	NA	NA	NA	NA	NA	NA	1	NA	0,25	NA	NA	4,15	46,1	Medio
	Brave	0,6	0,6	0,6	0,4	NA	NA	0,5	NA	0	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	3,95	43,9	Medio
Cliente de administración de contraseñas	LastPass	0,5	0,8	0,4	0,6	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,55	50,6	Alto
	DashLane	0,5	0,7	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,35	48,3	Medio
	1Password	0,5	0,6	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,25	47,2	Medio
	Keeper	0,5	0,5	0,4	0,4	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,05	45,0	Medio
Cifrado de datos	VeraCrypt	NA	1	NA	0,3	0	NA	NA	NA	NA	NA	1	NA	NA	1	NA	NA	0,25	NA	NA	3,55	39,4	Medio
	BitLocker	NA	1	NA	0,3	0	NA	NA	NA	0	NA	NA	NA	NA	1	1	NA	NA	0,5	NA	2,8	31,1	Medio
	AxCrypt	NA	0,9	NA	0,3	0	NA	NA	NA	0	NA	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	2,2	24,4	Bajo
	ZuluCrypt	NA	0,7	NA	0,2	0	NA	NA	NA	0	NA	NA	NA	NA	0,5	NA	NA	0,25	NA	NA	2,15	23,9	Bajo
Total: 29										Compatibles: 18													

Anexo E: tabla completa con las herramientas ordenadas de mayor a menor puntaje excluyendo el área.

Herramienta	Anonimato				Flexibilidad				Compatibilidad			Costos			Periodo				Puntaje	Porcentaje	Cualitativo
	A1	A2	A3	A4	F1	F2	F3	F4	CA1	CA2	CA3	C1	C2	C3	C4	P1	P2	P3	P4			
Red Tor	1,2	1,2	1	1,1	NA	NA	NA	1	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	8,5	94,4	Muy Alto
Parrot	1,2	1,2	1	1,1	NA	NA	0,5	NA	NA	NA	1	NA	NA	NA	1	NA	NA	0,5	NA	7,5	83,3	Muy Alto
VPN	1	1,2	1	1	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	7,2	80,0	Muy Alto
Qubes	1,2	1,2	1	1,2	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	7,1	78,9	Muy Alto
TAILS	1,2	1,2	1	1,1	NA	NA	NA	0	NA	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	7	77,8	Muy Alto
Red I2P	1	1,1	0,8	0,8	NA	NA	NA	1	NA	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	6,95	77,2	Muy Alto
Whonix	1,2	1,2	1	1	NA	NA	NA	1	0	NA	NA	NA	NA	NA	1	0	NA	NA	NA	6,4	71,1	Alto
Tor Browser	1,1	1,2	0,9	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	6,1	67,8	Alto
Servidor proxy	0,8	0,7	0,6	0,7	NA	NA	NA	1	NA	NA	1	NA	NA	0,5	NA	NA	NA	0,5	NA	5,8	64,4	Alto
OnionShare	0,6	0,7	0,8	0,4	NA	0,25	NA	NA	NA	NA	1	NA	NA	NA	1	NA	NA	NA	1	5,75	63,9	Alto
EPIC Browser	1	1	0,8	0,9	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	5,7	63,3	Alto
ProtonMail	0,6	0,7	1	0,4	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,95	55,0	Alto
LastPass	0,5	0,8	0,4	0,6	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,55	50,6	Alto
DashLane	0,5	0,7	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,35	48,3	Medio
1Password	0,5	0,6	0,4	0,5	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,25	47,2	Medio
Midori	0,4	0,4	0,3	0,3	NA	NA	0,5	NA	NA	1	NA	NA	NA	NA	1	NA	0,25	NA	NA	4,15	46,1	Medio
Ricochet	0,6	0,5	0,5	0,2	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	4,05	45,0	Medio
Keeper	0,5	0,5	0,4	0,4	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	NA	1	4,05	45,0	Medio
Brave	0,6	0,6	0,6	0,4	NA	NA	0,5	NA	0	NA	NA	NA	NA	NA	1	NA	0,25	NA	NA	3,95	43,9	Medio
OnionMail	0,6	0,5	0,6	0,4	NA	0,25	NA	NA	0	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	3,85	42,8	Medio
Paranoid	0,6	0,7	0,5	0,2	NA	0,25	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	3,75	41,7	Medio
Duck duck go	0,2	0,4	0,5	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	NA	1	3,7	41,1	Medio
VeraCrypt	NA	1	NA	0,3	0	NA	NA	NA	NA	NA	1	NA	NA	NA	1	NA	0,25	NA	NA	3,55	39,4	Medio
StartPage	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	3	33,3	Medio
Gibiru	0,2	0,2	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	NA	0,5	NA	2,9	32,2	Medio
BitLocker	NA	1	NA	0,3	0	NA	NA	0	NA	NA	NA	NA	NA	NA	1	NA	NA	0,5	NA	2,8	31,1	Medio
Torch	0,2	0,3	0,4	0,1	0	NA	NA	NA	NA	0,5	NA	NA	NA	NA	1	NA	0,25	NA	NA	2,75	30,6	Medio
AxCrypt	NA	0,9	NA	0,3	0	NA	NA	NA	0	NA	NA	NA	NA	0,5	NA	NA	NA	0,5	NA	2,2	24,4	Bajo
ZuluCrypt	NA	0,7	NA	0,2	0	NA	NA	NA	0	NA	NA	NA	NA	NA	1	NA	0,25	NA	NA	2,15	23,9	Bajo

Total: 29 | Compatibles: 18 | Incompatibles: 11

Anexo F: tabla completa de la evaluación de *dispositivos* con su correspondiente valoración cualitativa.

Dispositivo	Precio	Procesador		RAM	Modulo	Soporte	Puntaje	Porcentaje	Cualitativo
		Nucleos	Frecuencia						
Raspberry Pi 3	0,66	0,5	1	0,25	1	1	4,41	73,5	Alto
Raspberry pi 4	0,32	0,5	0,5	1	1	1	4,32	72,0	Alto
Rock Pi 4	0,51	0,5	1	0,5	1	0,5	4,01	66,8	Alto
Orange pi plus 2E	0,47	0,5	1	0,5	1	0,5	3,97	66,1	Alto
Latte Panda	0,16	0,5	1	0,5	1	0,5	3,66	61,0	Alto
Pine A64 LTS	0,62	0,5	0,5	0,5	1	0,5	3,62	60,3	Alto
Odroid C2	0,56	0,5	0,5	0,5	1	0,5	3,56	59,4	Alto
Asus Tinker Board S	0,43	0,5	1	0,5	1	0	3,43	57,1	Alto
Banana Pi M2	0,62	0,5	0,25	0,25	1	0,5	3,12	52,0	Alto
Raspberry Pi Zero	0,72	0	0,25	0	1	1	2,97	49,6	Medio
Orange pi PC	0,71	0,5	0	0,25	1	0,5	2,96	49,4	Medio
NanoPi R1	0,70	0,5	0,5	0,25	0	0,5	2,45	40,8	Medio
DragonBoard	0,15	0,5	0,5	0,25	1	0	2,40	40,0	Medio
nVidia Jetson TK1	0,00	0,5	0,5	1	0	0	2,00	33,3	Medio
BeagleBone Black	0,47	0	0,25	0	1	0	1,72	28,6	Medio
WandBoard Dual	0,22	0,25	0,25	0,25	0	0	0,97	16,2	Bajo
Total: 16									

Anexo G: tabla completa de la evaluación de *sistemas operativos* con su correspondiente valoración cualitativa.

Sistema Operativo	Recursos de memoria		Soporte	Periodo	Costos	Puntaje	Porcentaje	Cualitativo
	RAM	ROM						
Raspbian Buster Lite	0,94	0,48	1	1	1	4,42	88,33	Muy Alto
Raspbian Buster	0,41	0,28	1	1	1	3,69	73,78	Alto
DietPi	0,95	0,76	0,25	0,5	1	3,47	69,30	Alto
Alpine Linux	0,92	0,76	0,25	0,25	1	3,18	63,69	Alto
Ubuntu Mate	0,38	0,18	0,5	1	1	3,05	61,00	Alto
RISC OS	0,89	0,53	0	0,5	1	2,92	58,35	Alto
PipaOS	0,93	0,55	0,25	0	1	2,73	54,63	Alto
Windows IoT Core	0,59	0,63	1	0,25	0,25	2,71	54,30	Alto
OpenMediaVault	0,88	0,30	0,25	0,25	1	2,68	53,66	Alto
Windows IoT Enterprise	0,51	0,45	1	0,5	0	2,46	49,23	Medio
Total: 10								

Anexo H: Guía con las 50 pruebas de seguridad OWASP IoT

Categoría	Consideración de seguridad de IoT
I1: Interfaz web insegura	• Evalúe cualquier interfaz web para determinar si se permiten contraseñas débiles • Evaluar el mecanismo de bloqueo de cuenta • Evaluar la interfaz web para vulnerabilidades XSS, SQLi y CSRF y otras vulnerabilidades de aplicaciones web • Evaluar el uso de HTTPS para proteger la información transmitida • Evaluar la capacidad de cambiar el nombre de usuario y la contraseña • Determine si se usan firewalls de aplicaciones web para proteger las interfaces web
I2: Autenticación o autorización insuficiente	• Evaluar la solución para el uso de contraseñas seguras donde se necesita autenticación • Evalúe la solución para entornos multiusuario y asegúrese de que incluya funcionalidad para la separación de roles • Evaluar la solución para la implementación de autenticación de dos factores cuando sea posible • Evaluar los mecanismos de recuperación de contraseña • Evalúe la solución para la opción de requerir contraseñas seguras • Evalúe la solución para la opción de forzar la caducidad de la contraseña después de un período específico • Evalúe la solución para la opción de cambiar el nombre de usuario y contraseña predeterminados
I3: Servicios de red inseguros	• Evalúe la solución para garantizar que los servicios de red no respondan mal al desbordamiento del búfer, a la fuzz o a los ataques de denegación de servicio • Evalúe la solución para asegurarse de que los puertos de prueba no estén presentes
I4: falta de cifrado de transporte	• Evaluar la solución para determinar el uso de la comunicación encriptada entre dispositivos y entre dispositivos e internet

	• Evalúe la solución para determinar si se utilizan prácticas de cifrado aceptadas y si se evitan los protocolos propietarios • Evalúe la solución para determinar si una opción de firewall disponible está disponible
I5: Preocupaciones de privacidad	• Evaluar la solución para determinar la cantidad de información personal recopilada • Evalúe la solución para determinar si los datos personales recopilados están protegidos adecuadamente mediante el cifrado en reposo y en tránsito • Evaluar la solución para determinar si garantizar que los datos estén anonimizados o no identificados • Evalúe la solución para garantizar que los usuarios finales tengan la opción de recopilar datos más allá de lo que se necesita para el funcionamiento adecuado del dispositivo.
I6: Interfaz de nube insegura	• Evaluar las interfaces de la nube en busca de vulnerabilidades de seguridad (por ejemplo, interfaces API e interfaces web basadas en la nube) • Evalúe la interfaz web basada en la nube para asegurarse de que no permita contraseñas débiles • Evalúe la interfaz web basada en la nube para asegurarse de que incluya un mecanismo de bloqueo de cuenta • Evalúe la interfaz web basada en la nube para determinar si se utiliza la autenticación de dos factores • Evaluar las interfaces en la nube para detectar vulnerabilidades XSS, SQLi y CSRF y otras vulnerabilidades • Evalúe todas las interfaces en la nube para garantizar que se use el cifrado de transporte • Evalúe las interfaces en la nube para determinar si la opción para requerir contraseñas seguras está disponible • Evalúe las interfaces de la nube para determinar si la opción de forzar la caducidad de la contraseña después de un período específico está disponible • Evalúe las interfaces en la nube para determinar si la opción para cambiar el nombre de usuario y contraseña predeterminados está disponible

I7: Interfaz móvil insegura	• Evalúe la interfaz móvil para asegurarse de que no permita contraseñas débiles • Evalúe la interfaz móvil para asegurarse de que incluya un mecanismo de bloqueo de cuenta • Evalúe la interfaz móvil para determinar si implementa la autenticación de dos factores (por ejemplo, Touch ID de Apple) • Evalúe la interfaz móvil para determinar si usa cifrado de transporte • Evalúe la interfaz móvil para determinar si la opción de requerir contraseñas seguras está disponible • Evalúe la interfaz móvil para determinar si la opción de forzar la caducidad de la contraseña después de un período específico está disponible • Evalúe la interfaz móvil para determinar si la opción para cambiar el nombre de usuario y contraseña predeterminados está disponible • Evaluar la interfaz móvil para determinar la cantidad de información personal recopilada
I8: Configuracion de seguridad insuficiente	• Evalúe la solución para determinar si las opciones de seguridad de contraseña (por ejemplo, habilitar contraseñas de 20 caracteres o habilitar la autenticación de dos factores) están disponibles • Evalúe la solución para determinar si las opciones de cifrado (por ejemplo, Habilitar AES-256 donde AES-128 es la configuración predeterminada) están disponibles • Evalúe la solución para determinar si está disponible el registro de eventos de seguridad • Evalúe la solución para determinar si hay alertas y notificaciones al usuario para eventos de seguridad disponibles.
I9: Software o Firmware inseguro	• Evalúe el dispositivo para asegurarse de que incluye la capacidad de actualización y se puede actualizar rápidamente cuando se descubren vulnerabilidades • Evalúe el dispositivo para asegurarse de que utiliza archivos de actualización cifrados y que los archivos se transmiten mediante cifrado • Evalúe el dispositivo para asegurarse de que utiliza archivos firmados y luego valida ese archivo antes de la instalación

I10: Mala seguridad física	• Evalúe el dispositivo para asegurarse de que utiliza un número mínimo de puertos físicos externos (por ejemplo, puertos USB) en el dispositivo • Evalúe el dispositivo para determinar si se puede acceder a él mediante métodos no deseados, como a través de un puerto USB innecesario • Evalúe el dispositivo para determinar si permite la desactivación de puertos físicos no utilizados como USB • Evalúe el dispositivo para determinar si incluye la capacidad de limitar las capacidades administrativas a una interfaz local solamente

Anexo I: Pruebas de OWASP IoT realizadas a las configuraciones.
Leyenda: NA: No Aplica. Configuración=C (C1,C2,C3,C4).
Puntuación: 0 = prueba no aprobada, 0,1 = prueba aprobada.

No	Categoría	C1	C2	C3	C4	Descripcion
1	I1: Interfaz web insegura	NA	0,1	NA	0,1	Evalúe cualquier interfaz web para determinar si se permiten contraseñas débiles
2		NA	0,1	NA	0,1	Evaluar el mecanismo de bloqueo de cuenta
3		NA	0,1	NA	0,1	Evaluar la interfaz web para vulnerabilidades XSS, SQLi y CSRF y otras vulnerabilidades de aplicaciones web
4		NA	0,1	NA	0,1	Evaluar el uso de HTTPS para proteger la información transmitida
5		0,1	0,1	0,1	0,1	Evaluar la capacidad de cambiar el nombre de usuario y la contraseña
6		NA	0,1	NA	0,1	Determine si se usan firewalls de aplicaciones web para proteger las interfaces web
7	I2: Autenticación o autorización insuficiente	0,1	0,1	0,1	0,1	Evaluar la solución para el uso de contraseñas seguras donde se necesita autenticación
8		0,1	0,1	0,1	0,1	Evalúe la solución para entornos multiusuario y asegúrese de que incluya funcionalidad para la separación de roles
9		0	0,1	0	0,1	Evaluar la solución para la implementación de autenticación de dos factores cuando sea posible
10		0	0,1	0	0,1	Evaluar los mecanismos de recuperación de contraseña
11		0	0	0	0	Evalúe la solución para la opción de requerir contraseñas seguras
12		0	0	0	0	Evalúe la solución para la opción de forzar la caducidad de la contraseña después de un período específico
13		0,1	0,1	0,1	0,1	Evalúe la solución para la opción de cambiar el nombre de usuario y contraseña predeterminados
14	I3: Servicios de red inseguros	0,1	0,1	0,1	0,1	Evalúe la solución para garantizar que los servicios de red no respondan mal al desbordamiento del búfer, a la fuzz o a los ataques de denegación de servicio
15		0,1	0,1	0,1	0,1	Evalúe la solución para asegurarse de que los puertos de prueba no estén presentes
16	I4: falta de cifrado de transporte	0,1	0,1	0,1	0,1	Evaluar la solución para determinar el uso de la comunicación encriptada entre dispositivos y entre dispositivos e internet
17		0,1	0,1	0,1	0,1	Evalúe la solución para determinar si se utilizan prácticas de cifrado aceptadas y si se evitan los protocolos propietarios
18		0,1	0,1	0,1	0,1	Evalúe la solución para determinar si una opción de firewall disponible está disponible
19	I5: Preocupaciones de privacidad	0,1	0,1	0,1	0,1	Evaluar la solución para determinar la cantidad de información personal recopilada
20		0,1	0,1	0,1	0,1	Evalúe la solución para determinar si los datos personales recopilados están protegidos adecuadamente mediante el cifrado en reposo y en tránsito
21		0,1	0,1	0,1	0,1	Evaluar la solución para determinar si garantizar que los datos estén anonimizados o no identificados
22		0	0,1	0	0,1	Evalúe la solución para garantizar que los usuarios finales tengan la opción de recopilar datos más allá de lo que se necesita para el funcionamiento adecuado del dispositivo.
23	I6: Interfaz de nube insegura	NA	NA	NA	NA	Evaluar las interfaces de la nube en busca de vulnerabilidades de seguridad (por ejemplo, interfaces API e interfaces web basadas en la nube)
24		NA	NA	NA	NA	Evalúe la interfaz web basada en la nube para asegurarse de que no permita contraseñas débiles
25		NA	NA	NA	NA	Evalúe la interfaz web basada en la nube para asegurarse de que incluya un mecanismo de bloqueo de cuenta
26		NA	NA	NA	NA	Evalúe la interfaz web basada en la nube para determinar si se utiliza la autenticación de dos factores
27		NA	NA	NA	NA	Evaluar las interfaces en la nube para delectar vulnerabilidades XSS, SQLi y CSRF y otras vulnerabilidades
28		NA	NA	NA	NA	Evalúe todas las interfaces en la nube para garantizar que se use el cifrado de transporte
29		NA	NA	NA	NA	Evalúe las interfaces en la nube para determinar si la opción para requerir contraseñas seguras está disponible
30		NA	NA	NA	NA	Evalúe las interfaces de la nube para determinar si la opción de forzar la caducidad de la contraseña después de un período específico está disponible
31		NA	NA	NA	NA	Evalúe las interfaces en la nube para determinar si la opción para cambiar el nombre de usuario y contraseña predeterminados está disponible
32	I7: Interfaz móvil insegura	NA	0,1	NA	0,1	Evalúe la interfaz móvil para asegurarse de que no permita contraseñas débiles
33		NA	0,1	NA	0,1	Evalúe la interfaz móvil para asegurarse de que incluya un mecanismo de bloqueo de cuenta
34		NA	0,1	NA	0,1	Evalúe la interfaz móvil para determinar si implementa la autenticación de dos factores (por ejemplo, Touch ID de Apple)
35		NA	0,1	NA	0,1	Evalúe la interfaz móvil para determinar si usa cifrado de transporte
36		NA	0	NA	0	Evalúe la interfaz móvil para determinar si la opción de requerir contraseñas seguras está disponible
37		NA	0	NA	0	Evalúe la interfaz móvil para determinar si la opción de forzar la caducidad de la contraseña después de un período específico está disponible
38		NA	0,1	NA	0,1	Evalúe la interfaz móvil para determinar si la opción para cambiar el nombre de usuario y contraseña predeterminados está disponible
39		NA	0,1	NA	0,1	Evaluar la interfaz móvil para determinar la cantidad de información personal recopilada
40	I8: Configurabilidad de seguridad insuficiente	0,1	0,1	0,1	0,1	Evalúe la solución para determinar si las opciones de seguridad de contraseña (por ejemplo, habilitar contraseñas de 20 caracteres o habilitar la autenticación de dos factores) están disponibles
41		0,1	0,1	0,1	0,1	Evalúe la solución para determinar si las opciones de cifrado (por ejemplo, Habilitar AES-256 donde AES-128 es la configuración predeterminada) están disponibles
42		0	0	0	0,1	Evalúe la solución para determinar si está disponible el registro de eventos de seguridad
43		0,1	0,1	0,1	0,1	Evalúe la solución para determinar si hay alertas y notificaciones al usuario para eventos de seguridad disponibles.
44	I9: Software o Firmware inseguro	0,1	0,1	0	0,1	Evalúe el dispositivo para asegurarse de que incluye la capacidad de actualización y se puede actualizar rápidamente cuando se descubren vulnerabilidades
45		0,1	0,1	0,1	0,1	Evalúe el dispositivo para asegurarse de que utiliza archivos de actualización cifrados y que los archivos se transmiten mediante cifrado
46		0,1	0,1	0,1	0,1	Evalúe el dispositivo para asegurarse de que utiliza archivos firmados y luego valida ese archivo antes de la instalación
47	I10: Mala seguridad física	0,1	0,1	0,1	0,1	Evalúe el dispositivo para asegurarse de que utiliza un número mínimo de puertos físicos externos (por ejemplo, puertos USB) en el dispositivo
48		0,1	0	0,1	0	Evalúe el dispositivo para determinar si se puede acceder a él mediante métodos no deseados, como a través de un puerto USB innecesario
49		0,1	0,1	0,1	0,1	Evalúe el dispositivo para determinar si permite la desactivación de puertos físicos no utilizados como USB
50		0,1	0,1	0,1	0,1	Evalúe el dispositivo para determinar si incluye la capacidad de limitar las capacidades administrativas a una interfaz local solamente
	Total:	2,2	3,5	2,1	3,6	