Diagnóstico y mitigación de vulnerabilidades de ciberseguridad en dispositivos de acceso a la Internet en el hogar.

Monografía de trabajo de grado para optar por el título de
Ingeniero en Electrónica y Telecomunicaciones

José Miguel Betancourt Chaves
100616021729
Jorge Andrés Vargas Cordoba
100616020654

Director: Ph.D. Oscar Mauricio Caicedo Rendón

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telemática
Linea de Investigación en servicios avanzados de telecomunicaciones área funcional de seguridad en gestión de redes de computadoras
Popayán, Octubre 2023

AGRADECIMIENTOS

Agradecimientos de Jorge Andrés Vargas Cordoba

Quiero agradecer especialmente a mis padres Jorge y Anita quienes con su ejemplo, su música y su amor me brindaron todas las herramientas necesarias para terminar con este proceso de formación universitaria, gracias por enseñarme el único lenguaje que no conocí durante mi carrera, el lenguaje del alma, la música; A través del piano, encontré la calma en medio de los desafíos diarios. A mis tías y abuelitas quienes me apoyaron, animaron y aconsejaron siempre que lo necesité. A Laura, quien con su constante apoyo y amor incondicional, estuvo a mi lado en cada paso, tanto en los momentos de alegría como en los desafíos.

Agradezco a mis compañeros de carrera que me enseñaron el verdadero significado de trabajar en equipo, con los cuales vivimos experiencias únicas, superamos retos, y aprendimos los unos de los otros, les agradezco por hacer de esta experiencia una que recordaré toda la vida.

A la Rama Estudiantil IEEE de la Universidad del Cauca, donde pude complementar mi formación y desarrollar mis habilidades blandas; A las dos presidentas que conocí: Valentina Solano y Lina Muñoz de quienes aprendí lo que implica ser un excelente líder; Finalmente agradezco a todos los compañeros que conocí durante esta etapa, me llevo lo mejor de cada uno para mi futuro profesional.

Agradecimientos de José Miguel Betancourt Chaves

Quiero agradecer principalmente a mis padres José y Gloria, quienes han sido mi ejemplo a seguir toda mi vida y han hecho de mi una persona con los valores necesarios para seguir siempre adelante; a mi hermana quien ha abierto mi mente y me ha enseñado pensar fuera de lo convencional. A Valentina, por su compañía, guía y apoyo en todos los buenos momentos y también en las situaciones difíciles. También agradezco a mis compañeros de carrera con quienes siempre manejamos una ambiente de santa competencia y semestre a semestre nos apoyamos para superar todos los retos y adquirir nuevo conocimiento. A la Rama IEEE que ayudo al desarrollo de mis habilidades blandas y me dio la posibilidad de aprender a organizar eventos técnicos y sociales grandes. Por último agradezco a mi club de Patinaje Ciudad Blanca y todos sus integrantes ya que fueron un pilar muy importante en mi vida y me enseñaron la importancia del trabajo en equipo y la disciplina.

Agradecimientos especiales:

Gracias al ingeniero Oscar por el compromiso en la coordinación y dirección de este proyecto, y al ingeniero Siler por su constante apoyo en aspectos técnicos referentes a la ciberseguridad.

Infinitas gracias a la Universidad del Cauca y más específicamente a la Facultad de Ingeniería Electrónica Telecomunicaciones por ser un lugar de aprendizaje y crecimiento, donde cada docente y el plantel brinda una experiencia única y enriquecedora.

Acrónimos

CNVD *China National Vulnerability Database.*
CVE *Common Vulnerabilities and Exposures.*
CVSS *Common Vulnerability Scoring System.*
EPSS *Exploit Prediction Scoring System.*
GAD *GitHub Advisory Database.*
HTML *HyperText Markup Language.*
IOT *Internet Of Things.*
ISP *Internet Service Providers.*
KPI *Key Performance Indicator.*
NBA *Network Behavior Analysis.*
NVD *National Vulnerability Database.*
OWASP *Open Web Application Security Project.*
SOHO *Small Office / Home Office.*
SSVC *Stakeholder-Specific Vulnerability Categorization.*
VPR *Vulnerability Priority Rating.*

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Fase de formulación del problema de investigación

Contenido

1.1. Planteamiento del problema

El crimen cibernético ha presentado un constante y alarmante crecimiento en los últimos años, generando así gigantescas pérdidas económicas a nivel mundial. En el año 2015 hubo pérdidas de 3 trillones de dólares y con una tasa registrada de crecimiento del 15 %, se estima que para el año 2025 las pérdidas sean 10.5 trillones de dólares [1]. En el año 2020 de un total de 41 billones de intentos de ciberataques registrados en América Latina y el Caribe, más de 7 billones (17.1 %) fueron detectados en Colombia. Estos datos fueron recolectados por el laboratorio de inteligencia de amenazas FortiGuard Labs, de la empresa multinacional *Fortinet*, líder global en soluciones amplias, integradas y automatizadas de ciberseguridad, y encargada de publicar dichos resultados. Considerando solo los meses de octubre, noviembre y diciembre del año 2020, hubo 1.6 mil millones de intentos de ataques en el país. Durante este período, amenazas conocidas como correos electrónicos de *phishing* se extendieron por América Latina con archivos *HyperText Markup Language* (HTML) adjuntos, que tenían como fin redirigir al usuario a sitios web maliciosos. El malware basado en la web se ha convertido en el vehículo más común para distribuir archivos infectados, convirtiéndose a menudo en la puerta de entrada para el *ransomware* [2].

Hoy en día, el número de actividades que es posible realizar desde los hogares haciendo uso de la Internet es más grande que nunca, y con ello la seguridad en estos dispositivos es de gran importancia, ya que además de brindar acceso a la Internet son la primera línea de defensa contra ciberataques; esto debido a que por ellos fluye todo el tráfico de red y de ser comprometidos podría llegarse a presentar un escenario crítico, afectando la privacidad y experiencia del usuario. Sin embargo, el nivel de ciberseguridad de los enrutadores utilizados en los hogares sigue siendo en su mayoría de bajo nivel por diferentes causas como: la falta de conocimiento del usuario en materia de la seguridad de su información, configuraciones erróneas, configuraciones por defecto de los mismos, poco compromiso de los *Internet Service Providers* (ISP), etc. Esta es una problemática real y ha despertado el interés de la academia por darle solución a dicho planteamiento desde diferentes perspectivas.

Estudios como [3], [4], [5], [6] y [7] se enfocan en la detección de vulnerabilidades de ciberseguridad mediante una amplia gama de técnicas y/o mecanismos como el proyecto de código abierto *Open Web Application Security Project* (OWASP); de manera similar otros artículos como [8] y [9] han profundizado en técnicas mas específicas como el *fuzzing*, que consiste en realizar de manera dinámica solicitudes al enrutador con características variables e inesperadas para observar su comportamiento, y donde según la variable de mutación se puede acotar el tipo de vulnerabilidad objetivo e incluso se puede llegar a detectar vulnerabilidades de día cero, es decir vulnerabilidades que son descubiertas por primera vez y para las cuales aún no existe un parche. Por otra parte, existe un grupo de estudios [10], [11] y [12] que abordan la detección de *malware*, es decir, buscan identificar comportamientos maliciosos en dispositivos que ya han sido comprometidos. Finalmente, existe otro tipo de documentación [13] y [14] que centra sus esfuerzos en presentar *frameworks* que apoyan la detección y/o prevención de futuros ataques. Sin embargo, la mayoría de estas propuestas no van más allá de reportar un diagnóstico del dispositivo y proveer de manera muy superficial la información recolectada. Adicional a ello se identifica que los reportes no aportan guías y/o sugerencias que puedan ser seguidas por los usuarios finales,lo cual evita que las buenas prácticas de ciberseguridad sean adoptadas por las personas en sus hogares.

Del análisis de las investigaciones mencionadas es evidente que el bajo nivel de ciberseguridad en dispositivos de acceso a Internet en los hogares representa un problema de carácter global el cual despierta gran preocupación en la academia y la industria ya que la mayoría de los esfuerzos están encaminados principalmente a la detección de vulnerabilidades sin realizar propuestas que apoyen la prevención y/o mitigación de estas, es decir tienen un enfoque reactivo más no preventivo. Por lo tanto, con el desarrollo de este trabajo se pretende apoyar tanto en el diagnóstico de ciberseguridad, como en la mitigación de vulnerabilidades con un mecanismo que provea recomendaciones a los usuarios finales en redes residenciales para mitigar las vulnerabilidades encontradas. El presente estudio está centrado en la ciudad de Popayán, con el propósito de investigar la hipótesis que sugiere la existencia de vulnerabilidades comunes y desconocidas en los dispositivos de acceso a Internet doméstico proporcionados por los ISP locales. El objetivo es analizar y comprender las posibles vulnerabilidades presentes en estos dispositivos, las cuales podrían no ser plenamente reconocidas por los usuarios, lo que a su vez soportará la premisa de que existe una problemática grande que afecta particularmente a los principales ISP en términos de garantizar la seguridad de la información de los usuarios. La pregunta que se formula basados en la anterior hipótesis es: **¿Cómo apoyar el aumento del nivel de ciberseguridad en los dispositivos de acceso a Internet doméstico de un ISP en la ciudad de Popayán?**.

1.2. Objetivos

1.2.1. Objetivo general

Introducir un mecanismo de apoyo para el diagnóstico y mitigación de vulnerabilidades de ciberseguridad en dispositivos de acceso a la Internet en el hogar suministrados por un ISP a sus usuarios en la ciudad de Popayán.

1.2.2. Objetivos específicos

- Diseñar un mecanismo basado en CVSS [1]para apoyar el análisis de vulnerabilidades de ciberseguridad de severidad alta y crítica en dispositivos de acceso a la Internet en el hogar específicamente enrutadores de la marca Arris y Huawei.
- Implementar un prototipo del mecanismo propuesto.
- Evaluar la eficiencia del mecanismo a través del desarrollo de un estudio de caso sobre un dispositivo de acceso a la Internet en el hogar de un ISP (Internet Service Provider) de Popayán.

[1]El Sistema de Puntuación de Vulnerabilidades Comunes (*CVSS*) proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. La puntuación numérica puede traducirse en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

1.3. Metodología de investigación, y cronograma

1.3.1. Metodología de investigación

Para el desarrollo de este proyecto se hizo uso del método de investigación conceptual [15], el cual propone para este tipo de investigación una serie de fases con el fin de organizar el proceso de desarrollo y documentación de manera funcional. La presente investigación es positivista, ya que se califica lo cuantitativo, es empirico- analista y racionalista pues genera conocimiento a partir de ella.

Adicionalmente, se tomará como soporte del prototipo y la tecnología al marco de trabajo *Scrum* [16], el cual permite un proceso de gestión que reduce la complejidad en el desarrollo de productos para satisfacer las necesidades de los interesados. Por otro lado, *Scrum* es muy usado en empresas grandes, ya que permite el desarrollo ágil y continuo de los entregables, con constantes retroalimentaciones de los clientes para lograr obtener un producto final deseado. A continuación se describen las fases que se aplicaron para el desarrollo del proyecto y las actividades que componen cada una de estas.

1.3.1.1. Fase de formulación del problema de investigación

Al ejecutar esta fase se identificaron los siguientes puntos en la propuesta de trabajo: (a) Contexto y antecedentes generales del problema; (b) La situación problemática; (c) Tipo y propósito; (d) Relevancia; y (e) Objetivos, preguntas e hipótesis/proposiciones de la investigación. Es por lo anterior que las actividades quedan asignadas de la siguiente manera:

- **Actividad 1:** Reconocimiento del contexto y antecedentes del problema.
- **Actividad 2:** Identificación de la situación problemática.
- **Actividad 3:** Definición del tipo y propósito de la investigación.
- **Actividad 4:** Identificación de la relevancia.
- **Actividad 5:** Planteamiento de objetivos de la investigación.

1.3.1.2. Fase de análisis de trabajos relacionados

Como investigadores fue necesario realizar un mapeo sistemático de literatura que cubrió los libros científicos o de estudios relacionados en revistas científicas, con el fin de realizar un análisis de las contribuciones y limitaciones que existen. Esta fase tiene como fin la búsqueda de aplicaciones existentes para el diagnóstico y mitigación de vulnerabilidades de ciberseguridad en dispositivos de acceso a la Internet en el hogar. Lo anterior por medio de la identificación de bases de datos especializadas en el tema y en la industria de ISPs de la ciudad donde se realiza la investigación.

- **Actividad 6:** Definición de conceptos fundamentales para la investigación
- **Actividad 7:** Definición de parámetros para realizar el análisis exploratorio en la academia e industria.
- **Actividad 8:** Ejecución de las tareas asignadas en la anterior actividad y validación la información.

- **Actividad 9:** Análisis de los resultados de la información.
- **Actividad 10:** Definición de parámetros iniciales de búsqueda y ejecución de la misma; denominado estado del arte.
- **Actividad 11:** Realización del el análisis de contribuciones y limitaciones del material obtenido.

1.3.1.3. Fase del modelo conceptual desarrollado

Esta fase se divide en un Marco Conceptual General y un Modelo Conceptual Desarrollado, que se construye con base al mencionado en primera instancia.

Marco Conceptual General: Brinda respaldo teórico al desarrollo del trabajo de investigación mediante la definición de conceptos técnicos relevantes.

- **Actividad 12:** Identificación de los indicadores y variables claves para el trabajo de investigación (herramienta de medida que se usara para la validación del prototipo).
- **Actividad 13:** Definición del estudio de caso para la identificación de las vulnerabilidades de ciberseguridad en dispositivos de acceso a la Internet en el hogar e identificación de la eficiencia del mecanismo.
- **Actividad 14:** Realización de una entrevista exploratoria a usuarios de redes residenciales de la ciudad de Popayán sondeando los indicadores definidos en la actividad 11; esta como una medición base del trabajo de grado.
- **Actividad 15:** Realización del Marco Conceptual General con base en los resultados de la actividad 13.

Marco Conceptual Desarrollado: Es el producto intelectual del análisis y síntesis que se ha realizado a lo largo de las anteriores actividades

- **Actividad 16:** Construcción de la estructura de medición de la eficiencia y las vulnerabilidades con base en la entrevista exploratoria y el modelo conceptual general.

1.3.1.4. Fase de validación del modelo conceptual desarrollado

Los procedimientos para realizar la validación del modelo conceptural desarrollado que se tendrán en cuenta son: (a) Validez de Contenido por Panel de Expertos, quienes pueden determinar subjetivamente si el modelo cumple satisfactoriamente con los criterios necesarios y (b) Prueba del Concepto vía Construcción de un Artefacto, que consiste la construcción de un prototipo que materialice el modelo conceptual.

Para la actividad que corresponde a la construcción del prototipo, es usado el marco de trabajo SCRUM y Design Thinking, por las razones mencionadas en la introducción de la metodología.

- **Actividad 17:** Diagramación del prototipo capaz de medir y apoyar el proceso de mitigación de vulnerabilidades de ciberseguridad de los dispositivos de acceso a la Internet en el hogar.
- **Actividad 18:** Desarrollo ágil del prototipo previamente diagramado.

- **Actividad 19:** Realización de una prueba y una entrevista a 32 usuarios de redes residenciales de la ciudad de Popayán, donde se evalúe la automatización de la identificación de las vulnerabilidades de ciberseguridad y se logre la medición 0 del trabajo de grado para calcular la eficiencia del prototipo.
- **Actividad 20:** Verificación las recomendaciones dadas por el mecanismo para mitigar las diferentes vulnerabilidades identificadas en dispositivos de acceso a la Internet hogar.
- **Actividad 21:** Realización una entrevista a los mismos 32 usuarios de redes residenciales de la ciudad de Popayán sujetos de la medición 0 del trabajo de grado, evaluando los indicadores definidos en la actividad 12; esta como la medición 1 del trabajo de grado.
- **Actividad 22:** Comparación de la medición 0 y la medición 1, pretendiendo identificar la eficiencia del mecanismo.
- **Actividad 23:** Validez de contenido por parte de un panel de expertos.

1.3.1.5. Fase de entrega

En la etapa final de este proyecto, es llevado a cabo la elaboración de la monografía correspondiente al trabajo de grado, así como la redacción de un artículo relacionado con la investigación realizada. Este último pretende ser remitido para su consideración a una revista indexada y/o. Posteriormente a la entrega de la documentación, se lleva a cabo el proceso de sustentación del trabajo de grado frente a los jurados designados por la Facultad de Ingeniería Electrónica y Telecomunicaciones.

- **Actividad 24:** Elaboración de la monografía del trabajo de grado y el artículo de investigación.
- **Actividad 25:** Entrega de la monografía del trabajo de grado, artículo de investigación y demás elementos descritos en las condiciones de entrega.
- **Actividad 26:** Sustentación del trabajo de grado.

1.3.2. Cronograma

La Figura 1.1 representa visualmente el cronograma planificado y ejecutado para la realización integral del trabajo de investigación, abarcando un período de 9 meses. Cabe destacar que las actividades visualizadas en dicha figura son reflejo directo de las fases y actividades definidas en la metodología empleada en el contexto de este estudio de investigación.

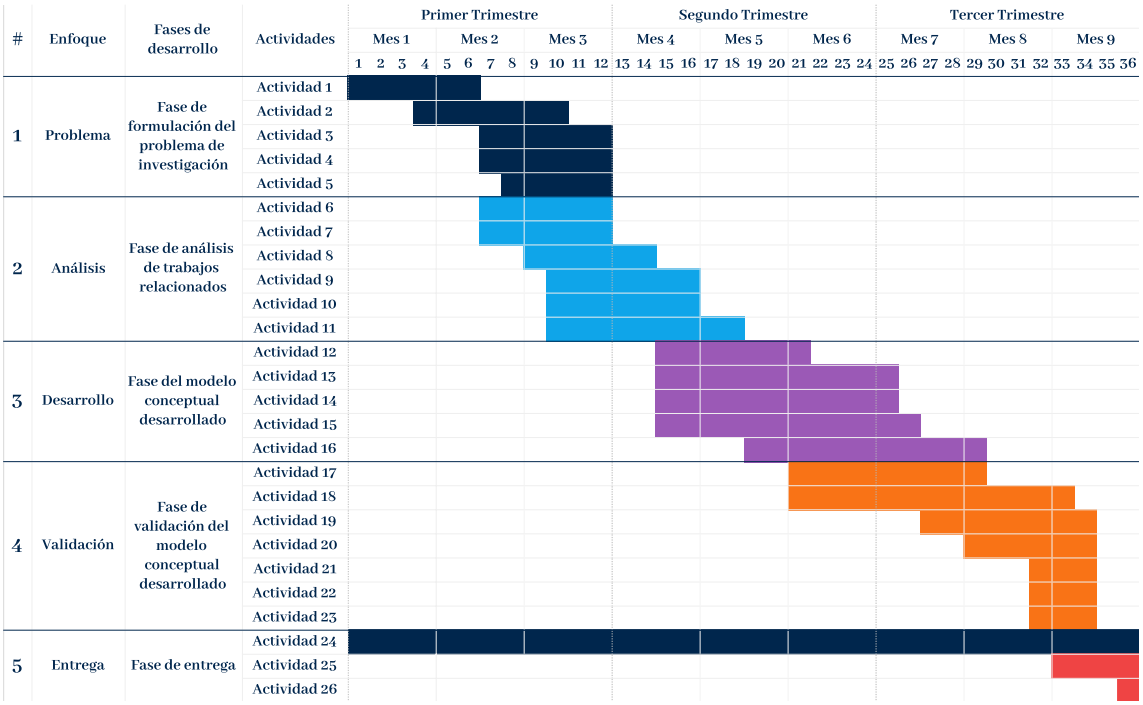

Figura 1.1: Cronograma de actividades

1.4. Estructura del documento

- **Capítulo 1:** Este capítulo aborda el planteamiento del problema y son definidos el objetivo general y los objetivos específicos del proyecto. Adicionalmente, es definida la metodología usada para el desarrollo del proyecto y la estructura del documento.
- **Capítulo 2:** Define el marco teórico y lleva a cabo un mapeo sistemático de literatura, aquí se da una explicación de los conceptos necesarios para entender el dominio del problema abordado en el presente trabajo de investigación. Por último expone un análisis de los trabajos encontrados y se mencionan los aportes de este trabajo de investigación.
- **Capítulo 3:** Aborda el problema de manera detallada examinándolo desde el punto de vista de los usuarios. Adicionalmente, es realizada la conceptualización de la experiencia de los usuarios y es presentada la herramienta de medida utilizada para evaluar el impacto del prototipo desarrollado; esto soportado en el estudio de caso de 32 usuarios residentes de la ciudad de Popayán.
- **Capítulo 4:** Este capítulo define el proceso para el desarrollo del prototipo haciendo uso del *framework* SCRUM, la arquitectura del prototipo, sus interfaces y todas las diferentes funcionalidades desarrolladas.
- **Capítulo 5:** Este capitulo describe las conclusiones obtenidas del trabajo de investigación realizado, documenta las limitaciones encontradas al realizar el prototipo y por último, propone posibles trabajos futuros.

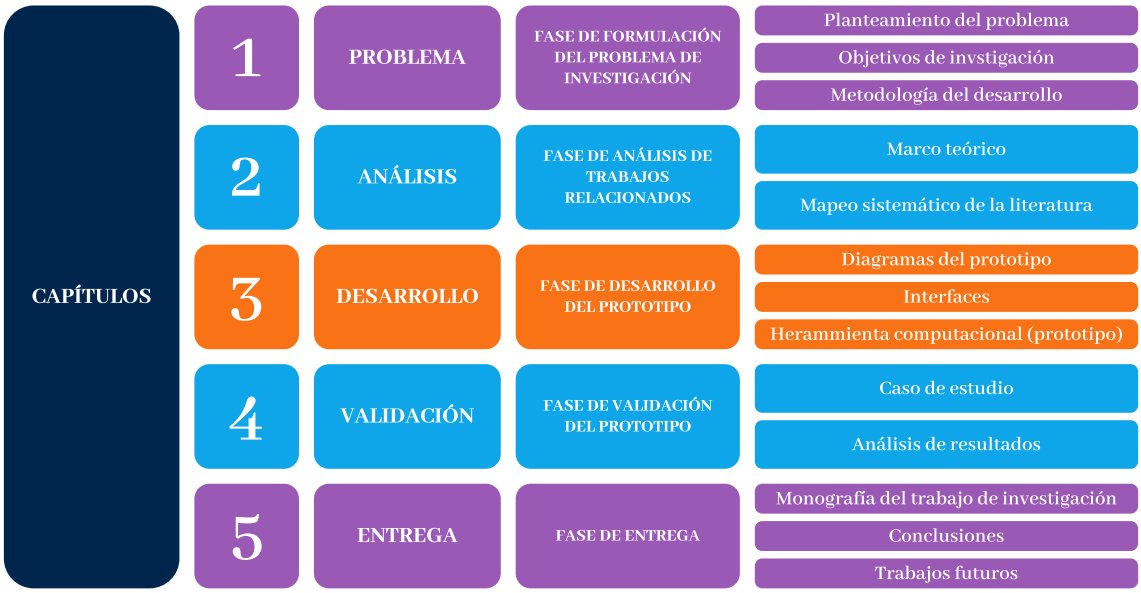

Figura 1.2: Estructura del documento

Capítulo 2

Trabajos relacionados

Contenido

2.1. Marco Teórico

A continuación son definidos algunos conceptos de gran importancia para el desarrollo del trabajo de investigación y que contribuyen a la comprensión del mismo.

- **Ciberseguridad**

  Cisco define la ciberseguridad como la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques generalmente están destinados a acceder, cambiar o destruir información confidencial, extorsionar a los usuarios, o interrumpir procesos comerciales normales [17]. De igual manera, organizaciones como IBM o Microsoft definen este mismo concepto de ciberseguridad como: seguridad de la tecnología de la información, seguridad cibernética, o seguridad digital, haciendo referencia a la práctica de proteger la información digital de los usuarios. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero [18, 19].

- **Diagnóstico de ciberseguridad**

  El diagnóstico de ciberseguridad, también denominado *Network Behavior Analysis* (NBA) es definido como el proceso de análisis del comportamiento y respuesta de un sistema para identificar actividades maliciosas por medio de la recopilación de datos [20, 21]. Adicional a ello en 2008 en la Conferencia Internacional sobre Convergencia y Tecnologías de la Información Híbridas fue definido este concepto que complementa el ya mencionado; el diagnostico de ciberseguridad está ligado a un periodo de tiempo pre-definido en términos de días o semanas (dependiendo de la red) con el fin de construir gradualmente los flujos generales de tráfico y por ende determinar los riegos ligados a ciberseguridad [22].

- **Mitigación de vulnerabilidades en ciberseguridad**

  Existe una estrecha relación entre reparar y mitigar una vulnerabilidad, sin embargo, para el presente trabajo es importante desligar ambos conceptos. La mitigación de vulnerabilidades es previa a la reparación de la misma, es un proceso que busca disminuir el impacto que estas puedan tener en los sistemas [23]. En general, las mitigaciones son procesos ejecutados cuando es programada una reparación de vulnerabilidades que puede estar conectado al lanzamiento de una tecnología o tiempo adecuado de inactividad en los sistemas [24].

- **Sistema de puntuación de vulnerabilidades comunes (CVSS)**

  Existen múltiples sistemas de puntuación de vulnerabilidades como: *Common Vulnerability Scoring System* (CVSS) [25], *Vulnerability Priority Rating* (VPR)[26], *Stakeholder-Specific Vulnerability Categorization* (SSVC)[27], *Exploit Prediction Scoring System* (EPSS)[28]. Sin embargo, uno de los más ampliamente utilizados es el sistema de puntuación de vulnerabilidades comunes, conocido por sus siglas en inglés como CVSS y el cual es definido como un marco de trabajo abierto que provee ciertas ventajas como una manera de caracterizar cada vulnerabilidad detectada y asignar un puntaje que refleje la severidad de la misma [29]. Además, este puntaje también puede ser representado de manera cualitativa como nulo, bajo, medio o alto y es calculado tomando en cuenta 3 grupos de métricas: base, temporal y de entorno [30]. Según [31] uno de los usos más comunes de CVSS es el cálculo de la severidad de las vulnerabilidades encontradas en un sistema como factor de priorización al momento de realizar los procesos de mitigación.

- **Mecanismo**

  Para definir este concepto se han tomado los aportes de Roger S. Pressman [32] define un mecanismo como *"una pieza de desarrollo informático diseñado para realizar una función bien definida. Puede considerarse como un componente de un sistema que realiza alguna tarea concreta"*, es de resaltar que el propósito de un mecanismo es cumplir tareas concretas dentro de un sistema; siendo el sistema una entidad que contiene a los diferentes mecanismos. Adicional a ello Hans van Vliet en su conceptualización de los principios de la ingeniería informática [33] define el mecanismo como: "Una implementación particular de una función o un conjunto de funciones en un sistema de software. Un mecanismo puede ser un componente de software independiente, como una subrutina, o puede ser una entidad más compleja, como un protocolo para comunicarse con otro sistema.", por ende es reforzado el concepto de mecanismo como una parte de un sistema, el cual en síntesis es un bloque funcional diseñado para resolver desafíos específicos dentro de un sistema.

  Debido a la necesidad de definir el alcance de la investigación es identificado el mecanismo a desarrollar y por ende el sistema que lo contiene, tomando como base la problemática establecida en el planteamiento del problema es esquematizado un sistema que contiene varios mecanismos, entre ellos, el reportado en este documento de investigación. El Sistema es denominado: **Sistema automatizado de diagnóstico, mitigación y reparación de vulnerabilidades en enrutadores de uso doméstico (SOHO)** mostrado en la figura 2.1.

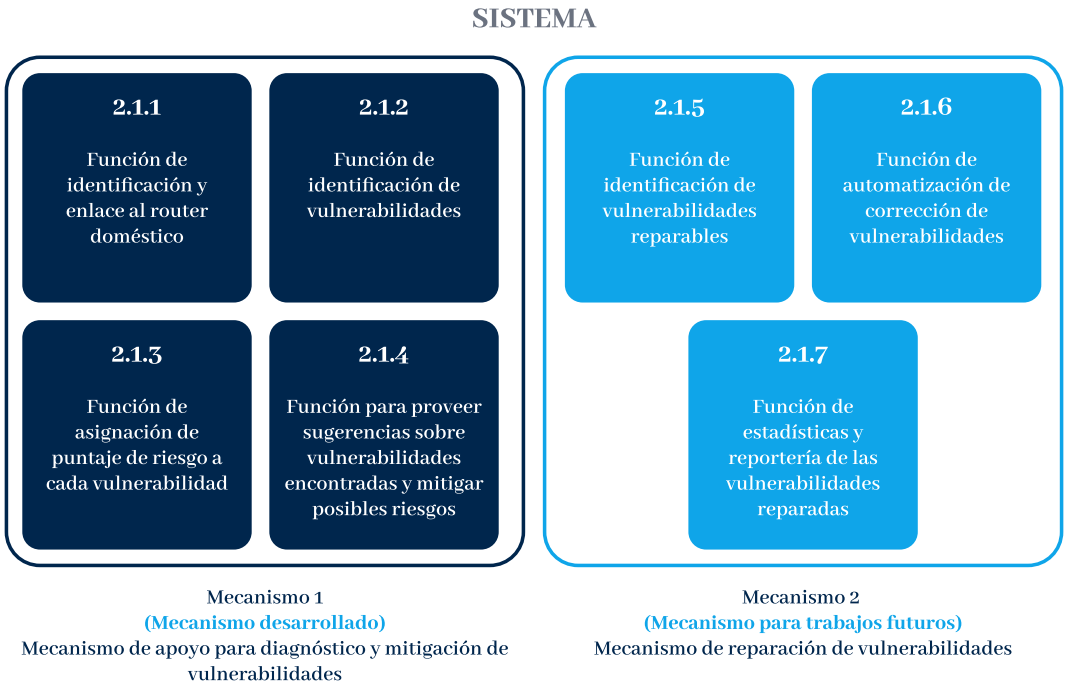

Figura 2.1: Sistema automatizado de diagnóstico, mitigación y reparación de vulnerabilidades en enrutadores de uso doméstico (SOHO)

Las siguientes son descripciones generales de cada función del sistema y la identificación de cuáles funciones componen al mecanismo planteado en los objetivos de

este desarrollo investigativo.

- **MECANISMO 1: Mecanismo de apoyo para la detección y análisis de vulnerabilidades**
  - Función de identificación y enlace al enrutador doméstico (figura 2.1.1): Está diseñada para identificar el enrutador en la red local y establecer una conexión con el mismo
  - Función de identificación de vulnerabilidades (figura 2.1.2): Tiene como objetivo ejecutar el protocolo encargado de realizar múltiples consultas al enrutador y evaluar su respuesta ante ellas. Función que realiza los siguientes procesos: escanear los puertos del enrutador, descubrir su sistema operativo, identificar su fabricante, etc; estos procesos con el fin de obtener la mayor cantidad de información sobre el enrutador y abstraer las vulnerabilidades que este posee. En este punto también es llevado a cabo el proceso de geolocalización y detección del ISP para almacenar las vulnerabilidades e información relevante del enrutador y su red correspondiente en una base de datos.
  - Función de asignación de puntaje de riesgo a cada vulnerabilidad (figura 2.1.3): El sistema debe proveer un puntaje de riesgo para cada una de las vulnerabilidades encontradas con el fin de informar al usuario sobre las que presentan mayores riesgos cibernéticos.
    Adicionalmente, también debe clasificar de manera cualitativa cada una de las vulnerabilidades basándose en el puntaje de riesgo previamente asignado.
  - Función para proveer sugerencias sobre las vulnerabilidades encontradas (figura 2.1.4): Cada vulnerabilidad encontrada es consultada en una base de datos de libre acceso que es actualizada periódicamente, que una vez identificada la vulnerabilidad, muestra sugerencias al usuario y tenga la información para mitigar las vulnerabilidades.

Para el propósito de esta monografía es realizado el desarrollo del Mecanismo 1 definido técnicamente a partir de las 4 funciones listadas a groso modo en este literal.

- **Eficiencia**

La eficiencia es un concepto usado en muchos contextos de la ingeniería en general, sin embargo, para el mecanismo estudiado en el presente es definida como la capacidad de un sistema, proceso o dispositivo para realizar su función prevista con un desperdicio mínimo de recursos. Esta definición sigue los apartados de Rolf Fare y Mehmet Kanoglu [34], quienes en las diferentes áreas de la ingeniería en que desempeñaron sus estudios usaron la eficiencia como *Key Performance Indicator* (KPI).

Esta investigación evaluó la eficiencia de un mecanismo a través del desarrollo de un estudio de caso compuesto de 32 pruebas de campo; por ello se establecieron indicadores que midan variables dentro de las pruebas de campo a realizar. A continuación son establecidas las variables medidas para cada prueba:

- **Variable 1. Velocidad de escaneo:** Tiempo en segundos que tarda el mecanismo en escanear el enrutador e identificar vulnerabilidades presentes en este.

Velocidades de escaneo más rápidas indican mayor eficiencia de escaneo con respecto al tiempo; el fabricante fue identificado en los enrutadores testeados con el fin de determinar el dispositivo con la mejor eficiencia en cuanto a tiempo de escaneo.

- **Variable 2. Uso del mecanismo:** En cada prueba de campo fue realizada una entrevista siguiendo los parámetros propuestos por la escala de Likert-Thunderston [35], para evaluar diferentes premisas durante el proceso y ponderar sus resultados. Este proceso busca responder: ¿qué tan fácil fue el uso del mecanismo para usuarios de redes domésticas? este componente de la entrevista fue analizado a través de 10 preguntas que evaluaron la facilidad en el uso del mecanismo por usuarios con diferentes niveles de conocimiento tecnológico.
- **Variable 3. Concientización sobre las vulnerabilidades:** Conforme a la definición consignada en el diccionario de Cambridge [36], la conciencia o ser consciente se caracteriza por poseer el conocimiento de la existencia de algo o la comprensión de una situación o tema en el instante presente, fundamentándose en información o experiencia. No obstante, en virtud del alcance específico de la presente investigación, la definición es limitada a la condición en la cual el usuario tiene conocimiento acerca de la presencia o ausencia de vulnerabilidades en su enrutador.

  Como fue definido en el anterior indicador, a través de las entrevistas son evaluadas diferentes premisas útiles para la investigación. Esta variable ahondó en la concientización de los usuarios sobre la vulnerabilidades de sus enrutadores domésticos, esto aprovechando la separación de las fases de las pruebas de campo.

  En la pre-fase de evaluación los usuarios responden acerca de si son conscientes de las vulnerabilidades que presenta su red residencial, siguiendo de igual manera la escala de Likert-Thunderston. En la post-fase de la prueba se realizará exactamente la misma pregunta pretendiendo que el nivel de concientización sobre las vulnerabilidades que presenta la red residencial mejore; con esto se determinará si el mecanismo propuesto es eficiente en cuánto a su capacidad de generar conciencia en un usuario sobre las vulnerabilidades de su enrutador doméstico.

- **Variable 4. Ancho de banda:** Esta variable es definida como la cantidad de datos transmitidos por el mecanismo en el periodo de tiempo en que este realiza el escaneo de vulnerabilidades. Esto con el objetivo de comprender mejor el comportamiento del mecanismo y cuantos recursos consume de la red.

  Para este propósito durante cada una de las pruebas de campo mediante un analizador de trafico es registrado el tráfico de la red, permitiendo una inspección detallada de los datos transmitidos y recibidos por el mecanismo, logrando así identificar el ancho de banda consumido por el mecanismo durante su uso. La medida de ancho de banda se dará en bits por segundo.
- **Variable 5. Tiempo de respuesta:** Para esta variable es medido el tiempo que le toma al mecanismo obtener respuesta a una solicitud realizada. Para esto nuevamente es estudiado el tráfico capturado por el analizador de tráfico, y es

identificado el tiempo que le toma a un paquete de datos volver a su emisor después de haber pasado por su destino.

Variable	Entrada	Salida	Elemento de medicion	Descripción
Velocidad de escaneo	Enlace a red doméstica	Reporte de vulnerabilidades	Función reloj integrado al mecanismo	Identificar el tiempo empleado por el mecanismo para escanear el router, identificar sus vulnerabilidades y generar el reporte. Un escaneo rápido indica una mayor eficiencia.
Uso del mecanismo	Uso del mecanismo por un usuario	Experiencia del usuario	Entrevista	Evaluar la facilidad de uso del mecanismo. Un mecanismo fácil de configurar y usar contribuye a su eficiencia.
Concientización sobre las vulnerabilidades	Uso del mecanismo por un usuario	Experiencia del usuario	Entrevista	Medir la claridad y precisión de los reportes de vulnerabilidades generados por el mecanismo. Un mecanismo eficiente debe proveer información detallada y comprensible por el usuario.

Tabla 2.1: Variables a medir

2.2. Estado del arte

El mapeo sistemático es un proceso que permite recopilar, categorizar y estructurar la información existente sobre un tema de investigación específico. El mapeo sistemático de la literatura realizado sigue las pautas propuestas por Petersen [37] y además toma referencia de las directrices propuestas por Kitchenham [38], Khan [39] y Budgen [40] para llevar a cabo las siguientes actividades resumidas en la figura 2.2:

1. Definir las preguntas de investigación
2. Conducir la búsqueda para los estudios primarios
3. Proceso de inclusión y exclusión de artículos
4. Criterios para evaluar la relación con el tema de estudio
5. Proceso de extracción y mapeo de información

Figura 2.2: Etapas del mapeo sistemático

Los siguientes 3 objetivos de búsqueda **(OB)** permitieron realizar adecuadamente este mapeo sistemático,

- **OB1:** Categorizar las piezas de información basándose en criterios de tiempo, distribución demográficos e interés de la comunidad. Esto con el fin de evidenciar el impacto científico y en investigación del tema de vulnerabilidades de ciberseguridad en dispositivos de acceso a internet en el hogar.
- **OB2:** Analizar las principales iniciativas científicas existentes en la literatura actual sobre el tema de Vulnerabilidades de ciberseguridad en dispositivos de acceso a internet en el hogar y clasificarlas según su relevancia con este tema de investigación.

El esquema de clasificación propuesto por Wieringa et al. [41] y la definición de los criterios para evaluación son usados para definir la relación que tiene cada artículo encontrado con el tema objetivo.

- **OB3:** Recopilar información relevante sobre las herramientas tecnológicas, técnicas, o métodos como solución a problemas relacionados con el tema objetivo. Esto para identificar el grado de desarrollo de las iniciativas y sus limitaciones según los resultados de su puesta en práctica.

2.2.1. Definición de las preguntas de investigación

Las siguientes preguntas de investigación **(PI)** mostradas en la Tabla 2.2, son planeadas para cumplir con los objetivos del mapeo sistemático de literatura. Cada pregunta es correlacionada con un objetivo de búsqueda establecido **(OB1, OB2, OB3)**, junto con su respectiva motivación. Estas preguntas de investigación buscan categorizar la información encontrada sobre las vulnerabilidades de ciberseguridad en los dispositivos de acceso a internet en el hogar y permiten identificar las lagunas existentes a nivel de investigación.

ID	Pregunta de Investigación	Motivación	OB
PI1	¿Cuál es la distribución temporal de los estudios seleccionados?	Presentar una macrotendencia de la literatura.	**OB1**
PI2	¿Cuáles son las revistas más importantes y conferencias en el área?	Descubrir las revistas y conferencias científicas donde están presentes los temas de nuestro interés.	**OB1**
PI3	¿Cuál es la distribución geográfica de los estudios seleccionados?	Presentar los países, universidades y grupos de investigación que lideran propuestas relacionadas con el tema de investigación sobre las vulnerabilidades de ciberseguridad en los dispositivos de acceso a internet en el hogar.	**OB1**
PI4	¿Cuáles son los autores más relevantes en el área?	Para identificar los autores y estudios mas citados en el tema de investigación.	**OB1**
PI5	¿Cuáles son los tipos de investigación realizados?	Para clasificar los diferentes tipos de investigación que se llevaron a cabo con base en el esquema de clasificación propuesto por Wieringa [41] investigación de validación, investigación de evaluación, propuesta de solución, documento filosófico, documentos de punto de vista o documentos de experiencia personal.	**OB2**
PI6	¿Cuál es la relevancia de los estudios seleccionados en relación con el tema de investigación?	Para establecer la relevancia de cada estudio seleccionado para la investigación desarrollada con base en los criterios de evaluación.	**OB2**
PI7	¿Cuáles son los tipos de soluciones propuestas?	Clasificar el tipo de contribución en una o varias de las siguientes categorías: (1) definición conceptual, (2) causas, efectos, impactos, y limitaciones, (3) métodos o técnicas de evaluación, (4) herramientas tecnológicas, (5) validez en la industria, (6) metodología de documentación, (7) otros	**OB3**
PI8	¿Qué resultados se han logrado con las propuestas realizadas?	Identificar el impacto de las propuestas realizadas a partir de los resultados obtenidos durante la validación en la industria del software.	**OB3**
PI9	¿Cuáles son los beneficios y retos de la investigación realizada?	Determinar los beneficios y los desafíos enfrentados por las diferentes investigaciones en las vulnerabilidades de ciberseguridad en los dispositivos de acceso a Internet en el hogar.	**OB3**

Tabla 2.2: Preguntas de investigación

2.2.2. Estrategia de búsqueda

PICOC [42, 43] fue seleccionado como estrategia de búsqueda debido a su capacidad para estructurar de manera clara y precisa los elementos esenciales de una investigación. Este enfoque proporciona un marco robusto que abarca la población o problema de interés **(P)**, la intervención o técnicas existentes utilizadas para abordar el problema identificado. **(I)**, la comparación o técnicas para contrastar entre sí la intervención y/o para medir los servicios **(C)**, los resultados esperados **(O)**, y en caso de ser necesario un contexto o circunstancias específicas **(C)**, esta estrategia permite encontrar los siguientes términos relevantes, expuestos en la Tabla 2.3:

Concepto			**Definición**	**Términos**
P	***Population***	¿Quién?	Enrutadores de uso doméstico o residencial. Dispositivos del borde de la red. Enrutadores de hogar u oficina.	***home routers,*** ***network edge devices,*** ***SOHO routers.***
I	***Intervention***	¿Qué? ¿Cómo?	Herramientas de medición. Aplicaciones de escritorio, móviles o web.	***tool, application.***
C	***Comparison***	¿Con qué comparar?	Sistema de puntuación de vulnerabilidades. Bases de datos de vulnerabilidades comunes.	***cvss, cve.***
O	***Outcomes***	¿Qué se busca conseguir y/o mejorar?	Automatizar la mitigación de vulnerabilidades. Realizar un análisis de ciberseguridad.	***automatic vulnerability mitigation,*** ***cybersecurity analysis.***
C	***Context***	¿En qué tipo de organización y/o bajo qué circunstancias?	-	**-**

Tabla 2.3: Definición estrategia de búsqueda PICOC

2.2.3. Ejecución de la búsqueda

Para la búsqueda de artículos, fue necesario realizar diferentes combinaciones entre las palabras clave identificadas y los operadores lógicos **(AND, OR)**, llegando finalmente a la siguiente cadena de búsqueda en su forma base:

(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvss” OR “cve”) AND (automatic vulnerability mitigation OR cybersecurity analysis)

La Tabla 2.4 presenta la cadena de búsqueda utilizada en cada una de las bases de datos objeto de consulta. Es importante resaltar que la forma base de la cadena de búsqueda fue adaptada de acuerdo a las necesidades de los motores de búsqueda, en la mayoría de estas, la ventana de tiempo de publicación de los artículos tuvo que ser añadida de manualmente haciendo uso de los filtros propios de cada base de datos.

ID	Cadena de búsqueda	Base de datos
1	(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvss” OR “cve”) AND (automatic vulnerability mitigation OR cybersecurity analysis)	ACM
2	(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvss” OR “cve”) AND (automatic vulnerability mitigation OR cybersecurity analysis)	Google Scolar
3	(“Full Text & Metadata”:“home routers” OR “Full Text & Metadata”:“network edge devices” OR “Full Text & Metadata”:“SOHO routers”) AND (“Full Text & Metadata”:“tool” OR “Full Text & Metadata”:“application”) AND (“Full Text & Metadata”:“cvss” OR “Full Text & Metadata”:“cve”) AND (“Full Text & Metadata”:automatic vulnerability mitigation OR “Full Text & Metadata”:cybersecurity analysis)	IEEE Xplore
4	(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvss” OR “cve”) AND (automatic vulnerability mitigation OR cybersecurity analysis)	Science Direct
5	(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvs” OR “cve”) AND (automatic AND vulnerability AND mitigation OR biosecurity AND analysis) AND PUBYEAR >2016	Scopus
6	(“home routers” OR “network edge devices” OR “SOHO routers”) AND (“tool” OR “application”) AND (“cvss” OR “cve”) AND (automatic vulnerability mitigation OR cybersecurity analysis)	Springer
7	ALL=((home routers OR network edge devices OR SOHO routers) AND (tool OR application) AND (automatic vulnerability mitigation OR cybersecurity analysis))	Web Of Science

Tabla 2.4: Adaptación de la cadena de búsqueda según la base de datos

La ventana de tiempo de consulta fue de seis (6) años, es decir, entre 2017 y 2022, y los siguientes filtros fueron aplicados:

- Artículos publicados en inglés.
- Artículos científicos o de conferencias.

2.2.4. Proceso de inclusión y exclusión de artículos

En primer lugar, una revisión en tres niveles fue necesaria para identificar y elegir los artículos pertinentes. (Nivel 1) Revisión del título, (Nivel 2) Revisión del resumen y (Nivel 3) Revisión del texto completo para ver si coincide con al menos uno de los criterios de inclusión mostrados en la Tabla 2.5. A continuación, para filtrar los artículos relevantes e identificar los principales, fue pertinente descartar los artículos que coincidían con al menos uno de los criterios de exclusión descritos en la Tabla 2.6.

ID	Criterio de Inclusión
CI1	Estudios cuyo tema principal es la ciberseguridad en los dispositivos de acceso a Internet en el hogar.
CI2	Estudios cuyo tema relacionado es la ciberseguridad en los dispositivos de acceso a Internet en el hogar.
CI3	Estudios que abordan cuestiones relacionadas con la ciberseguridad en los dispositivos de acceso a Internet en el hogar.
CI4	Estudios que hayan sido publicados en prestigiosas revistas revisadas por pares, congresos o conferencias

Tabla 2.5: Criterios de inclusión

ID	Criterio de Exclusión
CE1	Estudios duplicados (considerando sólo los más completos y recientes que se puedan evidenciar).
CE2	Estudios en los que el tema de investigación se aborda superficialmente
CE3	Estudios que no abordan cuestiones relacionadas con ciberseguridad en los dispositivos de acceso a Internet en el hogar.
CE4	Los estudios de tipo discusión o los estudios disponibles sólo en forma de presentaciones o resúmenes.
CE5	Estudios que son libros o capítulos de libros.

Tabla 2.6: Criterios de exclusión

Es importante aclarar que todos los artículos seleccionados cumplieron el criterio de inclusión CI4 de la Tabla 2.5 durante la búsqueda. Por este motivo, la Tabla 2.7 no incluye el recuento de este criterio. Como resultado de esta primera etapa, fueron obtenidos un total de veintinueve (29) artículos relevantes, a los que posteriormente fueron aplicados los criterios de exclusión (Tabla 2.6), identificando así un total de 20 estudios primarios.

#	Base de datos	Encontrados	Relevantes	Relevantes repetidos	A. Primarios seleccionados
1	ACM	10	8	0	8
2	Google Scolar	109	13	8	5
3	IEEE Xplore	8	4	0	4
4	Science Direct	6	1	0	1
5	Scopus	3	1	0	1
6	Springer	23	2	1	1
7	Web Of Science	5	0	0	0
TOTAL		**164**	**29**	**9**	**20**

Tabla 2.7: Resultados de la búsqueda

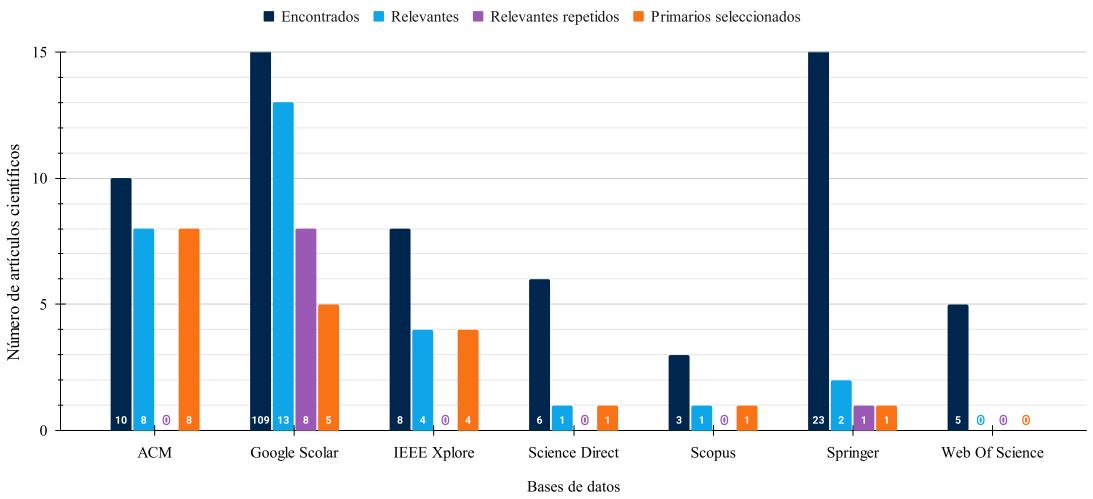

Figura 2.3: Selección de artículos por base de datos

A partir de la ejecución de nuevos procesos fue posible ampliar la selección de artículos y con esto profundizar la búsqueda, los siguientes son algunos de estos procesos:

- **Primarios:** Artículos resultados de los procesos de búsqueda, inclusión y exclusión anteriormente mencionados (Tabla 2.9).
- **Revisión hacia atrás (Backward):** Artículos que han sido citados en los artículos primarios (Tabla 2.10).

- **Revisión hacia adelante (Forward):** Artículos citando el artículo principal (Tabla 2.11).
- **Revisión de autores:** Artículos publicados por el mismo autor que publicó el artículo principal (Tabla 2.12).
- **Revisión de eventos:** Artículos publicados en la misma revista o evento del artículo principal (Tabla 2.13).

Al realizar los procesos fueron seleccionados 47 artículos, para obtener así un total de 67 artículos. El desglose de estos resultados es evidenciado en la Tabla 2.8.

Tipo	Articulos	Tabla
Primarios	20	2.9
Revisión hacia atrás (Backward)	13	2.10
Revisión hacia adelante (Forward)	13	2.11
Autor	11	2.12
Eventos	10	2.13
Total	67	

Tabla 2.8: Compendio total de artículos

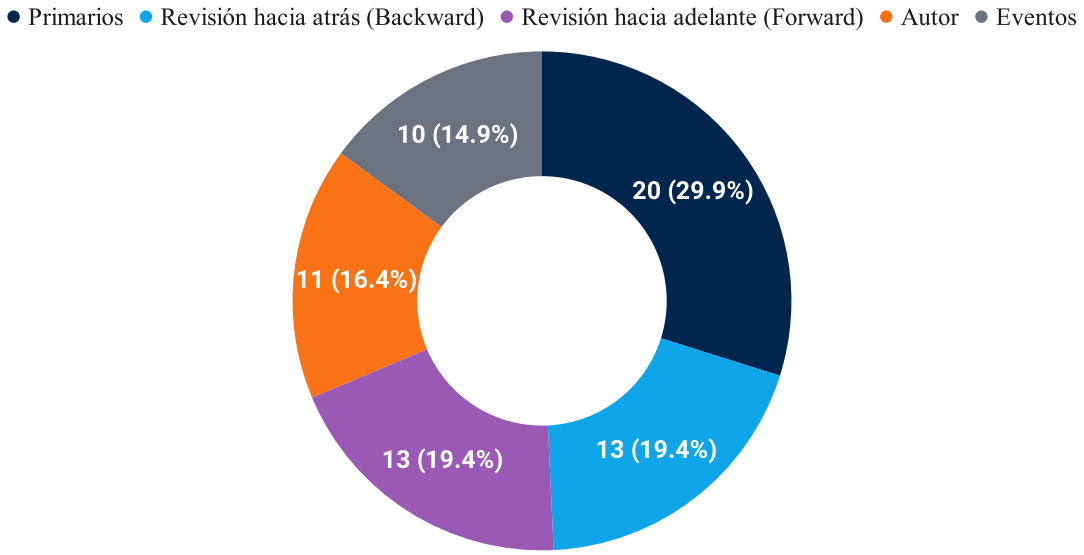

Figura 2.4: Distribución de artículos

Cabe mencionar que el número de citaciones **(NC)** de cada artículo es dado como dato adicional para el lector y no es tenido en cuenta como métrica en el proceso de selección. Esto, porque el número de citaciones de un artículo depende en gran medida de la visibilidad dada al mismo y no necesariamente refleja su aporte al tema.

ID	Artículos	NC	Año	Ref
A1	A Lightweight Vulnerability Mitigation Framework for IoT Devices	11	2017	[44]
A2	A novel approach for detecting vulnerable IoT devices connected behind a home NAT	17	2020	[3]
A3	A technical review of wireless security for the internet of things: Software defined radio perspective	4	2021	[45]
A4	Anatomy of threats to the internet of things	172	2018	[14]
A5	ARGUS: Assessing Unpatched Vulnerable Devices on the Internet via Efficient Firmware Recognition	0	2021	[46]
A6	Beyond Telnet: Prevalence of IoT Protocols in Telescope and Honeypot Measurements	18	2018	[47]
A7	Detecting Authentication-Bypass Flaws in a Large Scale of IoT Embedded Web Servers	3	2018	[48]
A8	Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots	8	2019	[49]
A9	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	24	2020	[50]
A10	eMUD: Enhanced Manufacturer Usage Description for IoT Botnets Prevention on Home WiFi Routers	7	2020	[4]
A11	Fast IPv6 Network Periphery Discovery and Security Implications	0	2021	[51]
A12	HADES-IoT: A Practical Host-Based Anomaly Detection System for IoT Devices	17	2019	[52]
A13	Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Survey	0	2021	[53]
A14	A Review on IoT Botnet	1	2021	[54]
A15	Security Analysis of SOHO Wi-Fi routers	0	2020	[55]
A16	SoK: Security Evaluation of Home-Based IoT Deployments	92	2019	[56]
A17	SRFuzzer: an automatic fuzzing framework for physical SOHO router devices to discover multi-type vulnerabilities	6	2019	[8]
A18	Threat classification in current Communication Infrastructures	0	2019	[57]
A19	Towards malware detection in routers with C500-toolkit	8	2017	[58]
A20	Vulnerability assessment of industrial systems using Shodan	0	2021	[59]

Tabla 2.9: Artículos primarios

ID	Artículos	NC	Año	Ori	Ref
A21	ProFuzzer: On-the-fly Input Type Probing for Better Zero-Day Vulnerability Discovery	65	2019	[8]	[9]
A22	Revealing and analysing modem malware	10	2012	[58]	[10]
A23	Unleashing Mayhem on Binary Code	573	2012	[8]	[60]
A24	Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces	167	2016	[8]	[5]
A25	A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan	203	2010	[8]	[61]
A26	Security challenges in embedded systems	59	2013	[52]	[62]
A27	Behavioral anomaly detection of malware on home routers	31	2017	[52]	[11]
A28	Firmaster: Analysis Tool for Home Router Firmware	8	2018	[55]	[6]
A29	PENTOS: Penetration testing tool for Internet of Thing devices	50	2017	[55]	[7]
A30	AVARCIBER: a framework for assessing cybersecurity risks	13	2020	[59]	[63]
A31	Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques	62	2016	[59]	[64]
A32	Method of Building a Security Vulnerability Information Collection and Management System for Analyzing the Security Vulnerabilities of IoT Devices	4	2017	[44]	[65]
A33	Advanced Wi-Fi Attacks Using Commodity Hardware	113	2014	[50]	[66]

Tabla 2.10: Artículos producto de la revisión hacia atrás (Backward)

ID	Artículos	NC	Año	Ori	Ref
A34	IoT-Proctor: A Secure and Lightweight Device Patching Framework for Mitigating Malware Spread in IoT Networks	1	2021	[44]	[67]
A35	Boosting-Based DDoS Detection in Internet of Things Systems	12	2021	[3]	[68]
A36	Role of device identification and manufacturer usage description in IOT security: A survey	4	2021	[3]	[69]
A37	A Comprehensive Study of the IoT Cybersecurity in Smart Cities	12	2020	[47]	[70]
A38	An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks	1	2021	[49]	[71]
A39	Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset	7	2021	[50]	[72]
A40	Evolution of Wi-Fi Protected Access: Security Challenges	7	2020	[50]	[73]
A41	Wireless Encryption and WPA2 Weaknesses	0	2021	[50]	[74]
A42	Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges	50	2019	[52]	[75]
A43	An analysis of malware detection and control through covid-19 pandemic	1	2021	[52]	[76]
A44	ADRIoT: An Edge-assisted Anomaly Detection Framework against IoT-based Network Attacks	0	2021	[56]	[77]
A45	Retrofitting Security and Privacy Measures to Smart Home Devices	3	2019	[56]	[78]
A46	An Efficient Algorithm to Extract Control Flow-Based Features for IoT Malware Detection	5	2019	[58]	[79]

Tabla 2.11: Artículos producto de la revisión hacia adelante (Forward)

ID	Artículo	NC	Año	Ori	Ref	Autor
A47	Kitsune: an ensemble of autoencoders for online network intrusion detection	466	2018	[44]	[12]	Yuval Elovici
A48	Fuzzing: a survey	115	2018	[46]	[80]	Chao Zhang
A49	An overview of IP flow-based intrusion detection	574	2010	[47]	[81]	Ramin Sadre
A50	Malware detection with quantitative data flow graphs	55	2014	[49]	[82]	Martín Ochoa
A51	Robust and effective malware detection through quantitative data flow graph metrics	59	2015	[49]	[83]	Martín Ochoa
A52	Methods, systems, and computer readable media for detecting malicious network traffic	17	2018	[56]	[84]	Fabian Monrose
A53	Cyber-Physical Systems Information Gathering: A Smart Home Case Study	60	2018	[53]	[85]	Kim-Kwang Raymond Choo
A54	DeepFuzzer: Accelerated Deep Greybox Fuzzing	17	2021	[53]	[86]	Kim-Kwang Raymond Choo
A55	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems	17	2021	[53]	[13]	Kim-Kwang Raymond Choo
A56	Resident evil: Understanding residential IP proxy as a dark service	41	2019	[51]	[87]	Baojun Liu
A57	How to notify a vulnerability to the right person? case study: in an ISP scope	6	2019	[51]	[88]	Haixin Duan

Tabla 2.12: Artículos producto de la revisión de autores

ID	Artículos	NC	Año	Ori	Ref
A58	Systematically Evaluating Security and Privacy for Consumer IoT Devices	84	2017	[44]	[89]
A59	Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices	27	2017	[44]	[90]
A60	Keep Pies Away from Kids: A Raspberry Pi Attacking Tool	13	2017	[44]	[91]
A61	A survey of network-based intrusion detection data sets	311	2019	[3]	[92]
A62	Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms	152	2019	[45]	[93]
A63	A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection	1977	2015	[14]	[94]
A64	Network Intrusion Detection for IoT Security Based on Learning Techniques	332	2019	[14]	[95]
A65	DeepSweep: An Evaluation Framework for Mitigating DNN Backdoor Attacks using Data Augmentation	10	2021	[46]	[96]
A66	Edmund: Entropy based attack Detection and Mitigation engine Using Netflow Data	7	2018	[48]	[97]
A67	Anomaly Detection to Protect Networks from Advanced Persistent Threats Using Adaptive Resonance AI Concepts	0	2020	[55]	[98]

Tabla 2.13: Artículos producto de la revisión de eventos

2.2.5. Evaluación de la relación de los artículos con el tema de estudio

Una vez seleccionados todos los artículos, es realizado un cuestionario para medir la relación y pertinencia con el tema de las vulnerabilidades de ciberseguridad en los dispositivos de acceso a la Internet. El cuestionario está compuesto de 12 preguntas y tiene un sistema de puntuación de tres valores (-1, 0, +1) ilustrado en la Tabla 2.14, por lo que cada artículo puede obtener una puntuación de relación entre -12 y 12. Obtener una puntuación baja no significa que un artículo deba ser descartado, sino que permite organizar los artículos por relevancia.

ID	**CRITERIO**	**PUNTAJE**		
		+1	**0**	**-1**
C1	El estudio está centrado en la investigación del fenómeno de la ciberseguridad en los dispositivos de acceso a la Internet en el hogar.	Si	Parcialmente	No
C2	El estudio ofrece una descripción clara del problema de investigación abordado.	Si	Parcialmente	No
C3	El estudio sigue un proceso de investigación estructurado y fundamentado.	Si	Parcialmente	No
C4	El estudio proporciona una definición clara de la ciberseguridad en los dispositivos de acceso a la Internet en el hogar.	Si	Parcialmente	No
C5	El estudio propone un conjunto de elementos a tener en cuenta a la hora de evaluar la ciberseguridad en los dispositivos de acceso a la Internet en el hogar.	Si	Parcialmente	No
C6	El estudio propone una forma de evaluar la ciberseguridad en los dispositivos de acceso a Internet en el hogar	Si	Parcialmente	No
C7	El estudio presenta de forma clara y detallada los resultados obtenidos tras validar su propuesta.	Si	Parcialmente	No
C8	El estudio presenta claramente las contribuciones de la investigación hacia la industria y el mundo académico	Si	Parcialmente	No
C9	El estudio describe claramente la discusión de las limitaciones del proceso de investigación realizado y el análisis de los resultados obtenidos.	Si	Parcialmente	No
C10	El estudio describe claramente el trabajo futuro o la investigación alternativa.	Si	Parcialmente	No
C11	El estudio ha sido publicado en una revista, conferencia o congreso relevante. Se ha utilizado la clasificación por cuartiles propuesta por Scimago para clasificar las revistas y el Ranking Computing Research and Education para los congresos y conferencias	Muy relevante (Q1: Revistas, A*: Conferencias)	Relevante (Q2,Q3: Revistas, A,B: Conferencias)	No relevante (Q4: Revistas, C: Conferencias)
C12	El estudio ha sido citado por otros autores (según el índice de citas de Google Scholar)	Ha sido citado por más de diez (10) autores	Entre uno y diez (1-10) autores	No ha sido citado hasta el momento

Tabla 2.14: Criterios de evaluación

La relevancia de los artículos seleccionados es presentada detalladamente en la Tabla 2.15, la cual ofrece una visión pormenorizada de los resultados obtenidos mediante la aplicación del criterio específico a cada uno de los artículos. Asimismo, la Figura 2.5 brinda una representación gráfica más comprensiva de estos resultados.

ID	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	Total
A1	0	1	0	0	1	-1	-1	1	0	1	0	1	3
A2	1	1	1	0	1	0	1	1	0	1	1	1	9
A3	0	0	1	0	1	0	0	1	0	1	1	0	5
A4	0	1	1	1	0	0	1	1	0	1	1	1	8
A5	-1	1	1	0	1	0	1	1	0	1	1	-1	5
A6	-1	0	0	-1	-1	-1	-1	1	1	1	0	1	-1
A7	0	1	-1	-1	-1	-1	0	0	0	0	0	0	-3
A8	-1	-1	-1	-1	-1	-1	-1	1	1	-1	0	1	-5
A9	-1	-1	-1	0	1	1	-1	1	0	0	1	1	1
A10	1	1	1	1	1	1	1	1	1	-1	1	0	9
A11	0	1	1	-1	0	0	1	0	0	1	0	0	3
A12	0	0	1	0	0	-1	1	-1	0	-1	1	1	1
A13	0	0	1	1	-1	-1	0	0	0	0	0	-1	-1
A14	-1	0	0	-1	-1	-1	0	0	0	0	-1	0	-5
A15	1	0	0	1	0	1	0	-1	0	0	0	-1	1
A16	0	0	-1	0	0	0	1	-1	0	-1	1	1	0
A17	1	1	1	1	1	1	1	0	1	1	1	0	10
A18	0	1	-1	1	0	-1	0	0	-1	-1	0	-1	-3
A19	1	1	0	0	1	0	1	-1	1	1	0	0	5
A20	1	1	0	1	1	0	1	-1	1	-1	0	-1	3
A21	1	1	1	0	0	0	1	1	1	1	1	1	9
A22	1	1	1	1	1	1	1	0	1	0	0	0	8
A23	0	1	1	0	0	-1	1	0	1	0	0	1	4
A24	1	1	1	1	1	0	1	0	1	1	1	1	10
A25	1	0	1	0	1	1	0	-1	0	1	1	1	6
A26	0	0	0	-1	0	-1	0	1	0	-1	0	1	-1
A27	1	1	1	1	1	1	1	0	0	0	-1	1	7
A28	1	1	1	1	1	1	1	0	1	1	-1	0	8
A29	0	0	1	1	1	1	1	0	1	1	-1	1	7
A30	0	1	1	0	-1	0	0	0	0	0	-1	1	1
A31	0	0	1	0	0	-1	1	0	0	1	-1	1	2
A32	-1	0	-1	0	0	0	-1	0	-1	1	0	0	-3
A33	0	0	1	0	1	0	1	0	0	1	0	1	5
A34	1	0	1	-1	1	0	1	0	0	1	0	0	4
A35	0	0	1	0	0	1	1	-1	0	1	-1	1	3
A36	-1	0	1	0	0	0	1	0	1	1	-1	0	2
A37	-1	1	1	0	0	0	1	0	1	1	-1	1	4
A38	-1	1	0	0	0	0	1	0	0	0	0	0	1
A39	0	1	1	0	1	0	1	0	1	1	-1	0	5
A40	0	1	0	0	0	0	0	0	0	0	1	0	2
A41	0	1	0	0	0	0	0	1	0	0	-1	-1	0
A42	0	1	1	0	0	0	1	0	0	0	0	1	4
A43	1	1	0	1	1	1	1	0	0	0	0	0	6
A44	1	0	1	1	1	0	1	0	0	0	1	-1	5
A45	1	1	0	1	0	1	1	1	1	-1	-1	0	5
A46	0	1	0	0	0	0	1	1	0	0	-1	0	2
A47	1	1	1	0	1	1	1	1	1	-1	-1	1	7
A48	0	1	0	-1	1	0	0	1	-1	-1	0	1	1
A49	0	0	1	-1	1	-1	1	1	-1	-1	1	1	2
A50	0	1	1	-1	1	0	1	1	-1	-1	-1	1	2
A51	-1	0	0	-1	1	0	1	0	-1	-1	-1	1	-2
A52	0	-1	0	-1	1	-1	1	1	-1	-1	-1	1	-2
A53	0	1	1	0	-1	-1	0	1	-1	1	1	1	3
A54	0	1	1	0	1	1	1	1	-1	-1	1	1	6
A55	0	1	1	0	1	1	1	1	0	-1	1	1	7
A56	0	0	1	0	1	1	1	1	-1	0	-1	1	4
A57	0	-1	0	-1	-1	-1	0	0	-1	-1	-1	0	-7
A58	1	0	-1	-1	1	1	1	-1	-1	-1	-1	1	-1
A59	1	0	0	-1	1	0	1	-1	-1	-1	-1	1	-1
A60	0	-1	-1	-1	0	-1	-1	0	-1	-1	-1	1	-7
A61	0	0	1	0	1	0	0	1	0	0	1	1	5
A62	0	1	1	0	1	1	1	1	0	-1	1	1	7
A63	0	1	1	0	-1	-1	0	1	1	0	1	1	4
A64	0	1	1	0	1	-1	0	1	0	1	1	1	6
A65	0	1	-1	-1	0	-1	0	-1	0	0	-1	0	-4
A66	1	1	1	-1	-1	-1	-1	0	-1	-1	-1	0	-4
A67	1	1	0	0	1	0	0	1	-1	1	-1	-1	2

Tabla 2.15: Clasificación de los artículos seleccionados por su relevancia

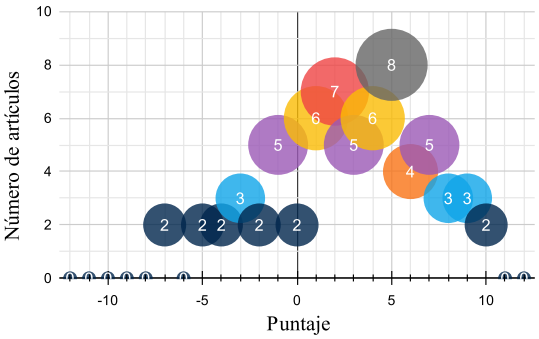

Figura 2.5: Clasificación de los artículos seleccionados por su relevancia

2.2.6. Proceso de extracción y mapeo de información

Esta sección presenta un formato (Tabla 2.16) que permite resumir y organizar la información principal de cada artículo para evitar pérdida de información importante y facilitar su comparación. Algunas de las características más relevantes tomadas en cuenta en este formato son: Datos de el/los autores, título, DOI, fecha de publicación, *abstract*, propuesta, problemas abordados, aspectos destacados, tipo de investigación, tipo de soluciones propuestas, entre otros.

Identificación			
Título		DOI	
Citaciones		Fecha de Publicación	
Conferencia o Revista			
Autor			
Nombre		País	
Universidad		Grupo de investigación	
Abstract		**Propuesta**	
Evaluación de la propuesta		**Problemas abordados**	
Elementos de justificación		**Aspectos a destacar**	
Tipo investigación [41]		**Tipos de solución ofrecidas**	
Investigación de validación		Definición conceptual	
Investigación de evaluación		Causas, efectos, impactos y limitaciones	
Propuesta de solución		Métodos o técnicas de evaluación	
Artículo filosófico		Herramientas tecnológicas	
Artículo de opinión		Validación industrial	
Experiencia personal		Metodologías de documentación	
Otros		Otros	

Tabla 2.16: Ficha de resumen del artículo

2.2.7. Proyectos relacionados más relevantes

Los siguientes fueron los artículos más relevantes encontrados durante el mapeo sistemático, analizados para abordar la problemática desde diferentes enfoques. De manera general en todos resalta el incremento considerable de enrutadores de acceso doméstico *Wi-Fi* y dispositivos *Internet Of Things* (IOT) durante los últimos años.

- **Firmaster: Analysis Tool for Home Router Firmware** [6]

  Los autores desarrollaron una herramienta llamada "Firmaster" que permite el análisis del *firmware* del enrutador. Este programa cuenta con una interfaz gráfica de usuario que se ejecuta en una máquina con distribución de ***Linux Ubuntu 16.04.3 LTS*** y fue creado usando ***Qt Creator 5.10.0*** y ***Python 2.7.12***. Los autores se centran en analizar 10 vulnerabilidades de *IoT* de OWASP de 2014. Además, el programa desarrollado logra ejecutar 7 funcionalidades principales como lo son: descifrado de contraseñas, escaneo *SSL*, análisis estático de la *web*, análisis de actualización de *firmware*, análisis dinámico de la *web*, escaneo de puertos y es capaz de generar un reporte con los resultados.

- **PENTOS: Penetration testing tool for Internet of Thing devices** [7]

  Este proyecto desarrolla un sistema capaz de realizar pruebas de penetración a dispositivos IoT. El sistema "PENTOS" cuenta con una interfaz gráfica de usuario ejecutada en **Kali Linux**. Este sistema es capaz de recolectar información de los usuarios, a través de la comunicación inalámbrica WiFi y Bluetooth para realizar distintos tipos de pruebas de penetración en dispositivos IoT, algunos de ellos son: Ataque con contraseña, ataque web y el ataque inalámbrico. Con base en el Top 10 de vulnerabilidades IoT de OWASP, el sistema es capaz de proporcionar orientación básica de ciberseguridad a los usuarios, aumentando así el nivel de conciencia de los mismos y presentando un resumen de los resultados de todos los módulos de ataque y algunas recomendaciones que eviten posibles amenazas.

- **Revealing and Analyzing Modem Malware** [10]

  Las técnicas propuestas en este artículo tienen diferentes objetivos específicos, el primero es verificar la administración del acceso remoto ya que una mala configuración de este puede potencialmente representar una vulnerabilidad crítica, como segundo objetivo proponen técnicas para identificar el sistema operativo del módem y así verificar la existencia de vulnerabilidades ya conocidas inherentes al SO utilizado, luego proponen técnicas que buscan verificar que el módem tenga activo el *firewall*, y para finalizar mencionan técnicas de análisis de memoria y así verificar que no existan logs persistentes, comandos maliciosos, etc.

- **SRFuzzer: An Automatic Fuzzing Framework for Physical SOHO router Devices to Discover Multi-Type Vulnerabilities** [8]

  Este artículo resalta la importancia de enrutadores *Small Office / Home Office* (SOHO) al ser dispositivos que en la actualidad siguen presentando vulnerabilidades de ciberseguridad. Los autores proponen *SRFuzzer*, un *framework* para realizar *fuzzing* de manera automatizada para testear dispositivos SOHO físicos. *SRFuzzer* consiste de 5 módulos mencionados a continuación: un generador de semilla, un módulo de mutación, un monitor, un control de poder, y finalmente un módulo de configuración para mejorar la eficiencia del proceso de *fuzzing*. Con esto se busca que *SRFuzzer* logre descubrir vulnerabilidades de múltiples tipos y no solo de corrupción de memoria.

2.3. Brechas Existentes

La Tabla 2.17 resume las brechas del conocimiento reconocidas en cada uno de los proyectos con el propósito de identificar los puntos en los que el presente proyecto de investigación puede presentar un aporte.

ID	Título	Brecha del conocimiento	Ref
A2	A novel approach for detecting vulnerable IoT devices connected behind a home NAT	Carece de recomendaciones que apoyen el proceso de prevención o mitigación de vulnerabilidades de ciberseguridad encontradas	[3]
A4	Anatomy of threats to the internet of things	No provee guías o recomendaciones orientadas al usuario final del dispositivo de acceso	[14]
A10	eMUD: Enhanced Manufacturer Usage Description for IoT Botnets Prevention on Home WiFi Routers	El proyecto no provee ningún tipo de recomendaciones orientadas al usuario final para aumentar el nivel de seguridad de su dispositivo de acceso.	[4]
A17	SRFuzzer: an automatic fuzzing framework for physical SOHO router devices to discover multi-type vulnerabilities	El artículo se limita a describir el proceso de fuzzing planteado para detectar vulnerabilidades y no provee ningún tipo de sugerencias para mitigar dichas vulnerabilidades.	[8]
A21	ProFuzzer: On-the-fly Input Type Probing for Better Zero-Day Vulnerability Discovery	No se menciona ningún proceso para aumentar el nivel de seguridad del dispositivo ni para mitigar las vulnerabilidades encontradas.	[9]
A22	Revealing and analysing modem malware	En este trabajo no se presentan instrucciones detalladas para que un usuario pueda mitigar vulnerabilidades después de detectar un comportamiento inusual en su router.	[10]
A24	Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces	La investigación no provee un puntaje que represente el nivel de seguridad que presenta el dispositivo.	[5]
A27	Behavioral anomaly detection of malware on home routers	No se implementa algún tipo de mecanismo que ayude a mitigar los efectos de programas maliciosos	[11]
A28	Firmaster: Analysis Tool for Home Router Firmware	No se trabaja con algún tipo de guías o recomendaciones para el usuario una vez se da el reporte de resultados	[6]
A29	PENTOS: Penetration testing tool for Internet of Thing devices	No se evidencia una orientación fuerte que ayude al usuario de manera amigable a prevenir paso a paso los posibles ataques a su red doméstica	[7]
A47	Kitsune: an ensemble of autoencoders for online network intrusion detection	En este trabajo no se mitigan los ataques detectados y tampoco se provee algún tipo de guía o recomendación que ayude a prevenir los ataques	[12]
A55	Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems	Este trabajo carece de un siguiente nivel de arquitectura que se encargue de prevenir futuros ataques	[13]

Tabla 2.17: Brechas del conocimiento

En conclusión fueron identificados los siguientes temas como principales brechas en la literatura:

- Falta de accesibilidad a los sistemas de detección de vulnerabilidades en redes domésticas.
- Falta de recomendaciones para dar solución a vulnerabilidades de los sistemas existentes.
- Falta de una matriz de puntaje de riesgo y asignación de puntaje de riesgo de las vulnerabilidades encontradas.

De los artículos seleccionados el 83,3 % (mayor porcentaje de la muestra analizada), presenta brechas con respecto a falta de recomendaciones brindadas a los usuarios después de ejecutado un escaneo, esto evidenciado en la figura 2.6. Esta brecha es seleccionada como el principal foco de aporte del presente trabajo de investigación.

Esto se muestra dentro del mecanismo desarrollado (ver figura 2.1 en la función 2.1.4 *"Función para proveer sugerencias sobre vulnerabilidades encontradas y mitigar posibles*

riesgos" la cual se encuentra diagramada para aportar directamente a esta brecha, el resto de funciones aportan indirectamente.

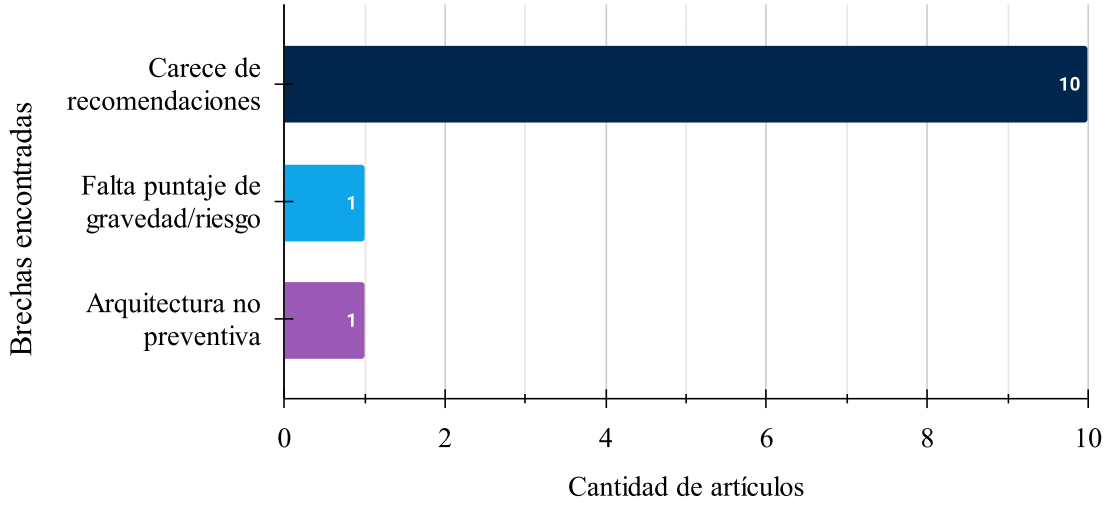

Figura 2.6: Distribución de artículos por brechas del conocimiento

2.4. Aportes del trabajo de investigación

Teniendo en cuenta los resultados obtenidos en el mapeo sistemático de literatura, es identificada la principal brecha en el conocimiento que existe con respecto al tema del presente trabajo de investigación es que la mayor parte de los documentos no buscan prevenir ni generar sugerencias para evitar las vulnerabilidades cibernéticas en redes domesticas. Por ello un mecanismo que apoye al diagnóstico y mitigación de vulnerabilidades a los usuarios de redes domésticas de la ciudad de Popayán, será el objetivo principal de la investigación en curso.

Como principales aportes del mecanismo se tiene:

- **Permita la detección de vulnerabilidades en dispositivos de acceso a internet de redes domesticas.**
- **Provea de manera cuantitativa y cualitativa el nivel de riesgo que las vulnerabilidades expuestas presentan para el usuario.**
- **Provea al usuario sugerencias de acciones a tomar para mitigar cada una de las vulnerabilidades encontradas.**

Esta solución esta incluida en los siguientes capítulos del presente documento; temas que son de gran relevancia para la línea de investigación en Servicios avanzados de telecomunicaciones área funcional de seguridad en gestión de redes de computadoras.

Capítulo 3

Modelo Conceptual desarrollado

Contenido

3.1. Marco conceptual general

3.1.1. *Framework* de desarrollo (*Design Thinking* + *SCRUM*)

Para el desarrollo del prototipo se aplicaron conjuntamente los *Frameworks* de *SCRUM* y *Design Thinking*, ya que según Gadner y Felderer en su estudio *"The Collective Process Framework DTSCRUM for Integrating Design Thinking into SCRUM"* [99], la combinación de ambas metodologías brinda a los desarrollos tecnológicos el enfoque humano y centrado en el usuario. Este diseño basado en el usuario permite captar y analizar las necesidades de manera funcional, garantizando que la definición de las problemáticas y las soluciones son abordadas desde una perspectiva que enriquece a ambas partes de todo desarrollo: la oferta y la demanda. En el esquema de la figura 3.1, se muestran los pasos que se tomarán de cada metodología y a qué parte de la metodología de desarrollo del trabajo de investigación hacen referencia.

Los estímulos externos hacen referencia a factores que generan necesidades dependiendo del usuario y el contexto estudiado, para la presente investigación es el uso de la Internet de manera doméstica en la ciudad de Popayán. El uso ideal de este modelo establece la ejecución de 3 fases de la metodología de *Design Thinking*, para un posterior encuentro con los Sprint de *SCRUM*, en teoría los acuerdos realizados a nivel del equipo *SCRUM* deben encontrarse alineados con el análisis del usuario posterior a la etapa de idealización.

Posterior a ello, una vez finalizados los ciclos de *SCRUM*, es ejecutada la etapa del incremento del desarrollo e ingresa a un *product backlog* que por la naturaleza del modelo es retro-alimentado con el usuario. Cabe resaltar que todo este proceso es documentado a medida que cada incremento va a producción.

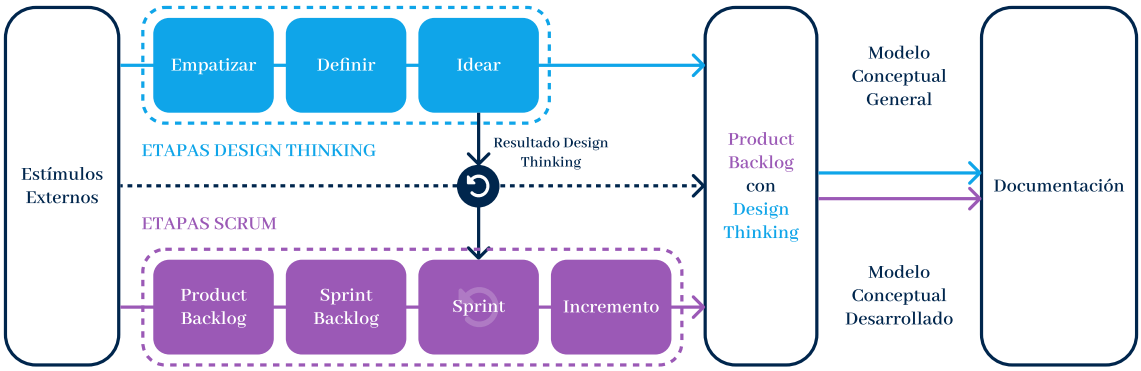

Figura 3.1: Modelo de desarrollo *Design Thinking* y *SCRUM*

Design Thinking:

1. **Etapa de empatizar:** En la fase empatizar de la metodología *Design Thinking*, la motivación principal es obtener una comprensión profunda de las experiencias del usuario para definir y entender sus necesidades y puntos de dolor en la actividad a ser analizada. En esta sección son analizadas las preguntas exploratorias para definir la problemática a ser abordada.

2. **Etapa de definición:** Esta fase tiene como objetivo principal reafirmar la problemática definida, donde con base en la fase de empatizar es determinado que el problema es una situación que existe actualmente en la ciudad de Popayán para usuarios de redes residenciales.

3. **Etapa de idear:** Para la etapa de idear son propuestas una serie de ideas creativas e innovadoras para darle una solución al problema definido en las fases anteriores; esta solución estará basada en un desarrollo tecnológico en el área de ingeniería electrónica y telecomunicaciones. Aquí se documentará una lluvia de ideas llevada entre el equipo de trabajo que desarrolla el presente trabajo de investigación.

3.1.1.1. Etapa de empatizar

El enfoque de esta fase es indagar en los usuarios con el fin de comprender lo que piensan y cómo se comportan frente al tema objeto de este proyecto de investigación. Así se busca comprender el problema real que presentan, problema que el desarrollo del prototipo resolverá. Una entrevista exploratoria fue realizada a 45 personas de manera anónima y aleatoria en la ciudad de Popayán, las preguntas de las tablas 3.1 y 3.2 son analizadas con el fin de entender el problema de investigación.

ID	Pregunta de la entrevista	Objetivo de la pregunta
1	¿Cuál es su Edad?	Ubicar demográficamente a la población que padece la problemática.
2	¿Cuál es su género?	Ubicar demográficamente a la población que padece la problemática.
3	¿Cuál es tu ocupación?	Ubicar demográficamente a la población que padece la problemática.
4	¿Qué tan cómodo se siente con los términos técnicos relacionados con la seguridad de la red?	Evaluar el nivel de conocimiento del usuario en cuanto a la seguridad de la red.
5	¿Con qué frecuencia utiliza Internet en su casa?	Aislar el porcentaje de la muestra poblacional que puede estar más expuesta a vulnerabilidades con respecto a la frecuencia en el uso de la Internet.
6	¿Qué dispositivos están conectados a su red doméstica?	Analizar los dispositivos principales de acceso al internet, con el fin de encaminar la solución hacia los dispositivos de mayor uso.
7	¿Qué tan importante es para usted asegurarse de que su red doméstica sea segura?	Evaluar si para la población de la ciudad de Popayán se le da importancia a la seguridad de la red doméstica.

Tabla 3.1: Entrevista exploratoria (Parte 1)

Continuación de la tabla en la siguiente página.

ID	Pregunta de la entrevista	Objetivo de la pregunta
8	¿Qué es lo que más le preocupa cuando se trata de la seguridad de su red doméstica? (Marque todo lo que corresponda)	Determinar cual es el factor común de preocupación sobre la seguridad de las redes domésticas.
9	De 1 a 5, siendo 1 que considera completamente inútil una solución y 5 que considera completamente útil una solución ¿Que tan útil considera que sería una herramienta que le ayude a evaluar el estado de seguridad de su red domestica?	Ahondar si desde la perspectiva de los usuarios de redes domésticas se considera útil una posible solución para la evaluación de vulnerabilidades en redes domésticas.
10	¿Le interesaría utilizar una herramienta o recurso que facilite realizar diagnósticos de seguridad de red y provea recomendaciones para mejorar la seguridad de la misma?	Identificar si los usuarios de redes domésticas presentan interés en utilizar una posible solución para la de evaluación vulnerabilidades en redes domésticas.
11	¿Ha escuchado o leído noticias relacionadas con brechas de seguridad en línea o ataques cibernéticos?	Determina si dentro de la muestra poblacional elegida para analizar la problemática hay intéres en torno al tema de la seguridad de redes.

Tabla 3.2: Entrevista exploratoria (Parte 2)

Estas preguntas cubren los componentes necesarios para definir el problema de investigación. Cada entrevista llevó consigo conversaciones con el usuario para comprender sus preocupaciones y motivaciones. Compilando en nota las frustraciones o reacciones de los usuarios hacia las preguntas realizadas; adicional a ello completando un proceso de Observación del participante donde se observó sin intervenir como el usuario realizaba el análisis de vulnerabilidades de su red sin intervención de los investigadores con el fin de elaborar un *Customer Journey Map* para identificar los puntos de conflicto críticos en el proceso.

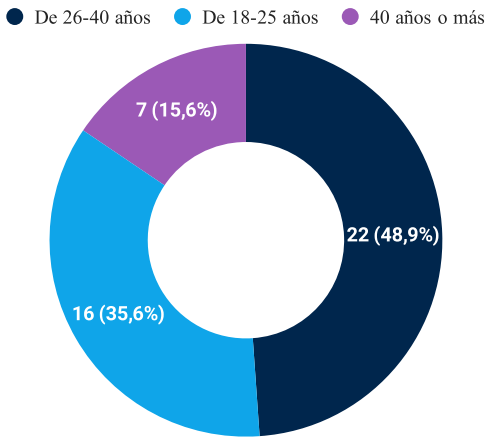

Figura 3.2: Pregunta 1- ¿Cuál es su Edad?

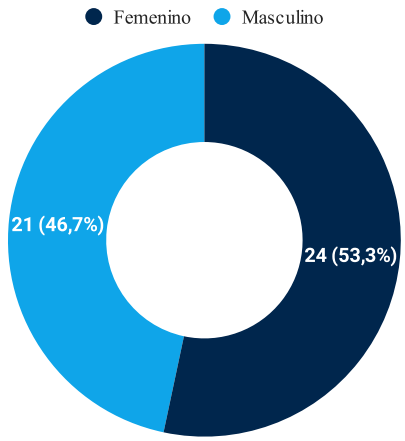

Figura 3.3: Pregunta 2- ¿Cuál es su género?

La mayoría de los participantes de la muestra poblacional de entrevistados tienen entre los 26 y 40 años de edad. Además, la distribución por género entre los encuestados es casi equitativa con un 53 % de personas que se identifican como género femenino y 47 % como género masculino, demostrando una representación equilibrada tanto de mujeres como de hombres.

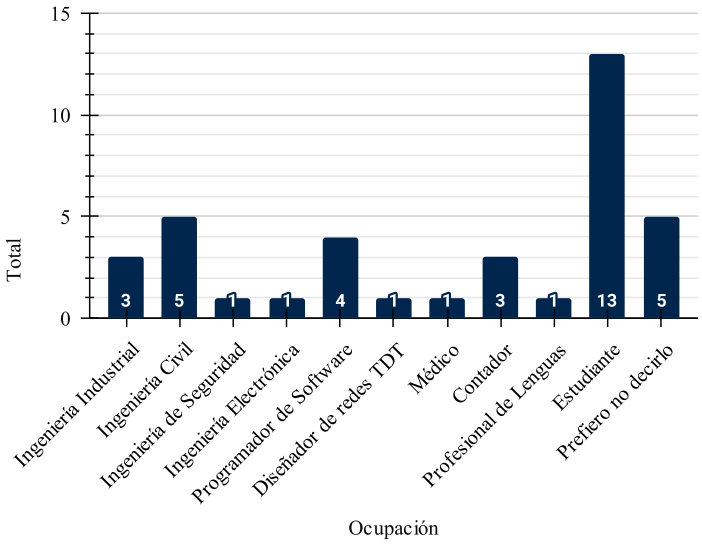

Figura 3.4: Pregunta 3- ¿Cuál es tu ocupación?

La muestra poblacional de la entrevista ejerce profesionalmente en diferentes áreas del conocimiento, abarcando un amplio espectro de ocupaciones desde la ingeniería hasta la medicina. El análisis de los datos de la población en diferentes áreas del conocimiento contribuye a una exploración más completa, fomentando diversidad demográfica en la muestra poblacional.

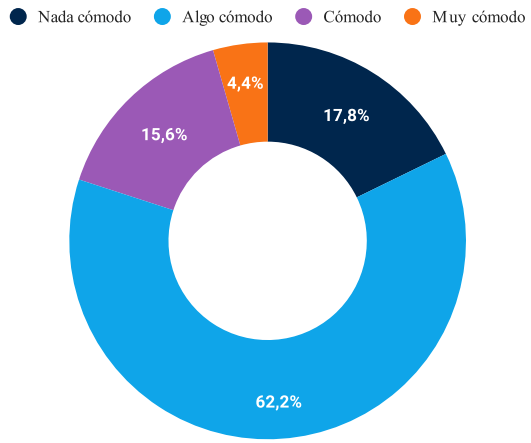

Figura 3.5: Pregunta 4- ¿Qué tan cómodo se siente con los términos técnicos relacionados con la seguridad de la red?

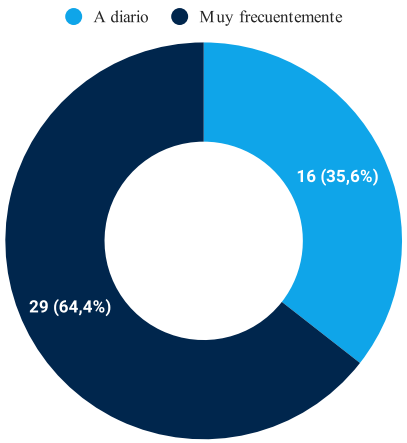

Figura 3.6: Pregunta 5- ¿Con qué frecuencia utiliza Internet en su casa?

El 64 % de la población, presenta un nivel limitado de conocimientos técnicos. A pesar de ello, la mayoría de personas hacen uso de la red con mucha frecuencia. Este esquema presentado, de personas con conocimientos técnicos limitados y uso frecuente de la Internet constituye el punto central de este estudio; se intuye que personas con conocimientos técnicos limitados tienen dificultades para ejecutar acciones en pro de la seguridad de su

red doméstica y por el uso frecuente de la misma se ven expuestos a un gran número de vulnerabilidades.

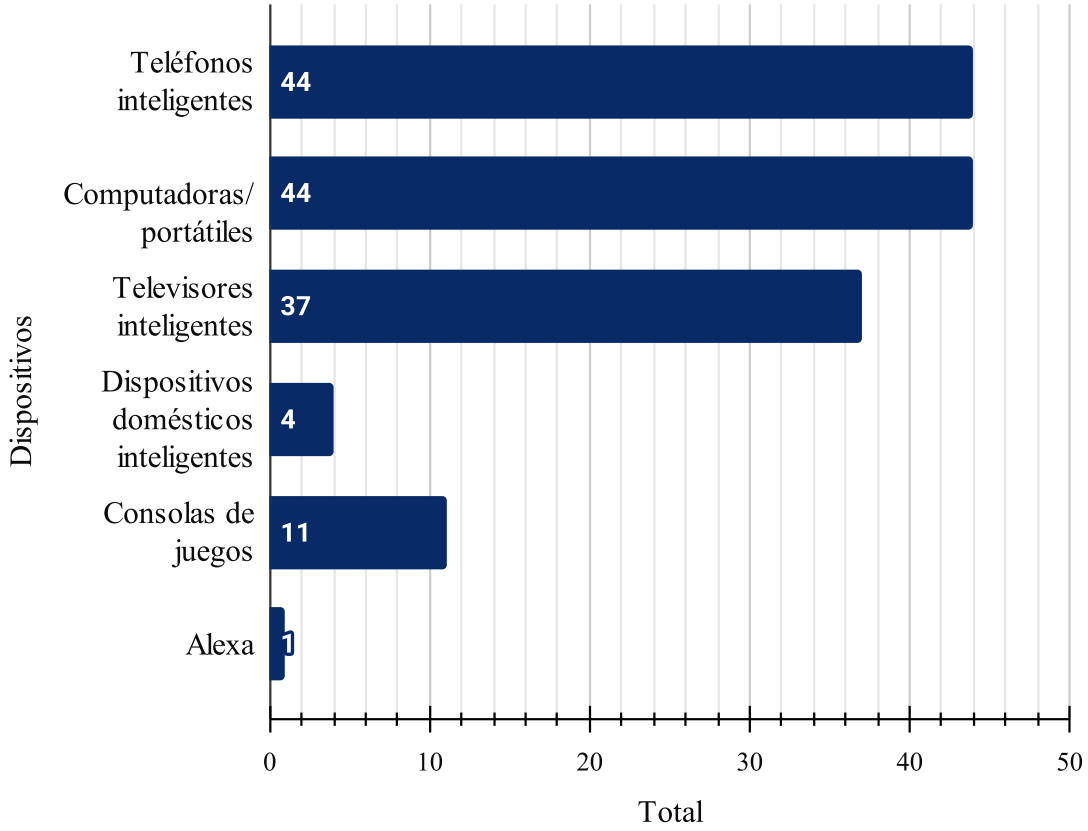

Figura 3.7: Pregunta 6- ¿Qué dispositivos están conectados a su red doméstica?

Entre los entrevistados, los dispositivos predominantes para acceder a Internet son los teléfonos inteligentes y los computadores portátiles o de escritorio. Este resultado es valioso para la investigación, reforzando el papel fundamental del enrutador de red doméstica, funcionado como punto de acceso para dispositivos a Internet. Por ello se puede determinar que las vulnerabilidades para el mecanismo deberían ser estudiadas en el *router* como dispositivo de "puerta de entrada"para los aparatos de mayor uso para la muestra poblacional.

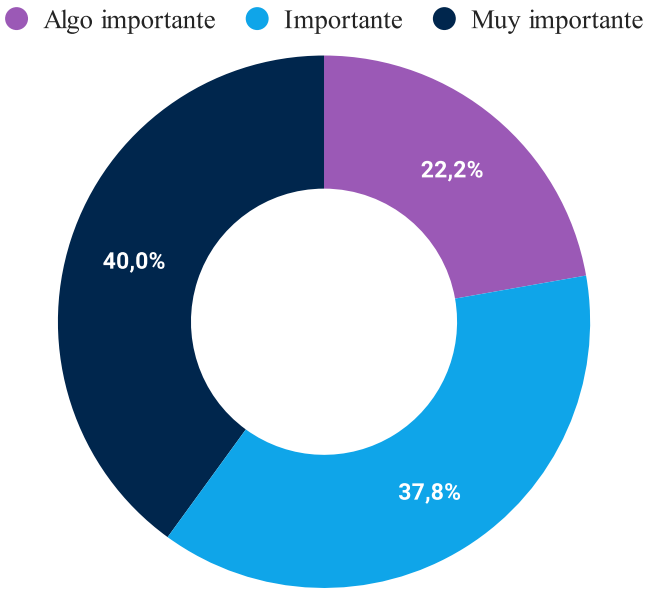

Figura 3.8: Pregunta 7- ¿Qué tan importante es para usted asegurarse de que su red doméstica sea segura?

Sorprendentemente, ni un solo participante de la muestra demostró indiferencia o consideró que la seguridad de su red doméstica no era importante. Todos los participantes expresaron un grado de importancia con respecto al concepto de seguridad; donde la mayoría estableció la importancia en gestionar la seguridad de su red. Esta perspectiva obtenida a través de indagar, por medio de conversaciones con los participantes, sobre la influencia de las múltiples campañas de marketing que existen actualmente en pro de la concientización sobre la seguridad de las redes; la población en general entiende la necesidad de mantener su red segura para hacer un uso responsable de la Internet.

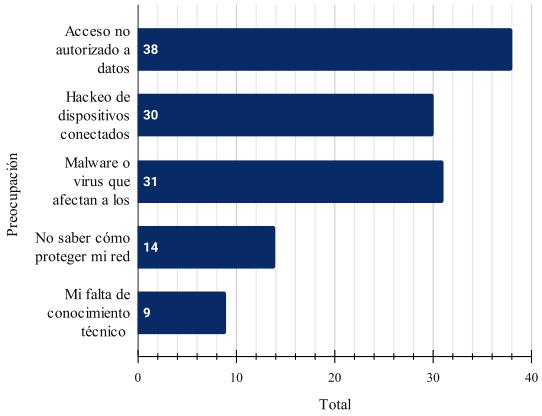

Figura 3.9: Pregunta 8- ¿Qué es lo que más le preocupa cuando se trata de la seguridad de su red doméstica?

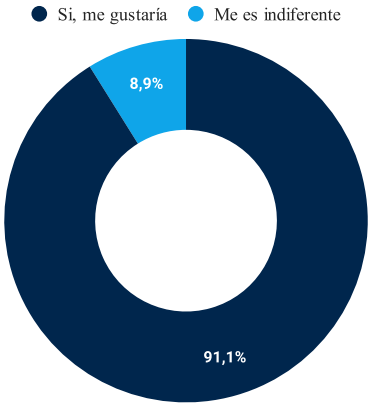

Figura 3.10: Pregunta 10-¿Le interesaría utilizar una herramienta o recurso que facilite realizar diagnósticos de seguridad de red y provea recomendaciones para mejorar la seguridad de la misma?

El tema más preocupante en el ámbito de la seguridad de las redes para la población es la protección de los datos personales, siguiéndole en porcentaje al posible hackeo de dispositivos y malware que afecte los mismos. En su mayoría, en un porcentaje del 91 % la población estaría interesada en una herramienta que le ayude a mitigar posibles vulnerabilidades como las mencionadas.

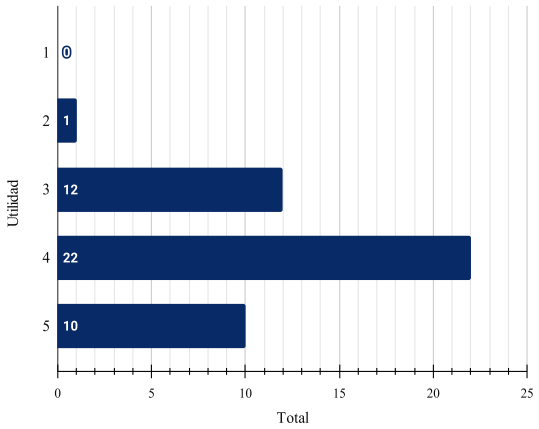

Figura 3.11: Pregunta 9- ¿Qué tan útil considera que sería una herramienta que le ayude a evaluar el estado de seguridad de su red domestica?

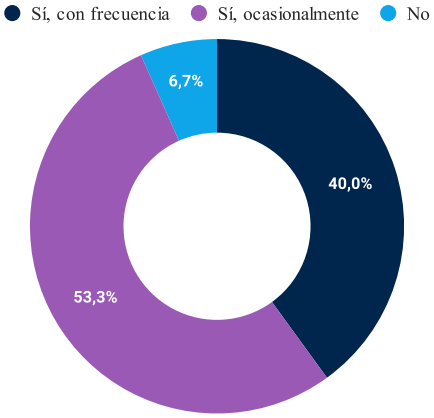

Figura 3.12: Pregunta 11- ¿Ha escuchado o leído noticias relacionadas con brechas de seguridad en línea o ataques cibernéticos?

Una mayoría significativa de la población, asignó una calificación de 3-5 en una escala de 1 a 5 para expresar su convencimiento de la utilidad de una herramienta como la mencionada 3.11; por ende este tipo de herramienta en redes domésticas es algo que gusta, interesa y se considera útil entre la población. Adicional a ello, en su mayoría los encuestados no consideran que tienen los conocimientos técnicos suficientes, en un 93 % participan en la difusión y recepción de noticias e información sobre la seguridad de la red, lo cual refuerza el entendimiento de la población hacia la necesidad existente 3.12.

USER PERSONAS

A partir del proceso de la encuesta exploratoria y siguiendo la metodología del *Design Thinking* son definidos dos *USER* Personas. Estos, tienen como función comprender mejor y empatizar con las necesidades, objetivos, comportamientos y preferencias de los usuarios finales de la solución.

PERSONA 1: MARIA- 35 años de edad
Maria es una gerente de oficina y madre de dos hijos. Utiliza Internet principalmente para las redes sociales, las compras en línea y *streaming* de contenido de novelas. Si bien no es experta en tecnología, es consciente de la importancia de la seguridad en línea debido a las noticias sobre ataques cibernéticos.

- **Condición Técnica:** Básica. Maria puede navegar por sitios web y usar aplicaciones de redes sociales, pero pide asistencia de sus hijos constantemente para aprender nuevas funciones de sus dispositivos de acceso a internet.
- **¿De dónde es?:** Maria es de la ciudad de Popayán, actualmente reside en la misma ciudad en la que nació.
- **¿Cuáles son sus objetivos?:** Maria tiene como objetivo determinar si su red *Wi-Fi* está protegida contra posibles vulnerabilidades. Maria también tiene como objetivo ser capaz de ejecutar mejoras de seguridad necesarias para mitigar vulnerabilidades.
- **¿Cuál es su motivación?:** Maria quiere garantizar la seguridad en línea de su familia y proteger su información confidencial como sus datos bancarios. Le preocupan las actividades en línea de sus hijos y quiere saber cómo proteger sus dispositivos.

PERSONA 1: EDUARDO- 28 años
Diseñador gráfico de 28 años que trabaja de forma remota. Se siente cómodo usando la tecnología. Esta interesado en *influencers* y literatura que lo mantenga informado sobre nueva tecnología y ocasionalmente juega con la configuración de su red doméstica.

- **Condición Técnica:** Intermedio. Eduardo se siente cómodo con la tecnología, comprende los conceptos básicos de redes y está dispuesto a aprender.
- **¿De dónde es?:** Eduardo es de la ciudad de Barranquilla, actualmente reside en la ciudad de Popayán pues su esposa es de la ciudad.
- **¿Cuáles son sus objetivos?:** Eduardo está interesado en identificar posibles vulnerabilidades o puntos débiles de su red doméstica.
- **¿Cuál es su motivación?:** Eduardo siente curiosidad por la seguridad de su red doméstica y quiere protegerse. Ha oído hablar de violaciones de datos y quiere tomar el control de la seguridad de su red.

Ambos *USER*- personas representan a usuarios habituales con diferentes niveles de competencia técnica y motivaciones para mejorar la seguridad de su red doméstica. Diseñar soluciones que satisfagan las necesidades y preferencias de usuarios como Maria y Eduardo crean un enfoque más efectivo y fácil de usar para mejorar la seguridad de la red.

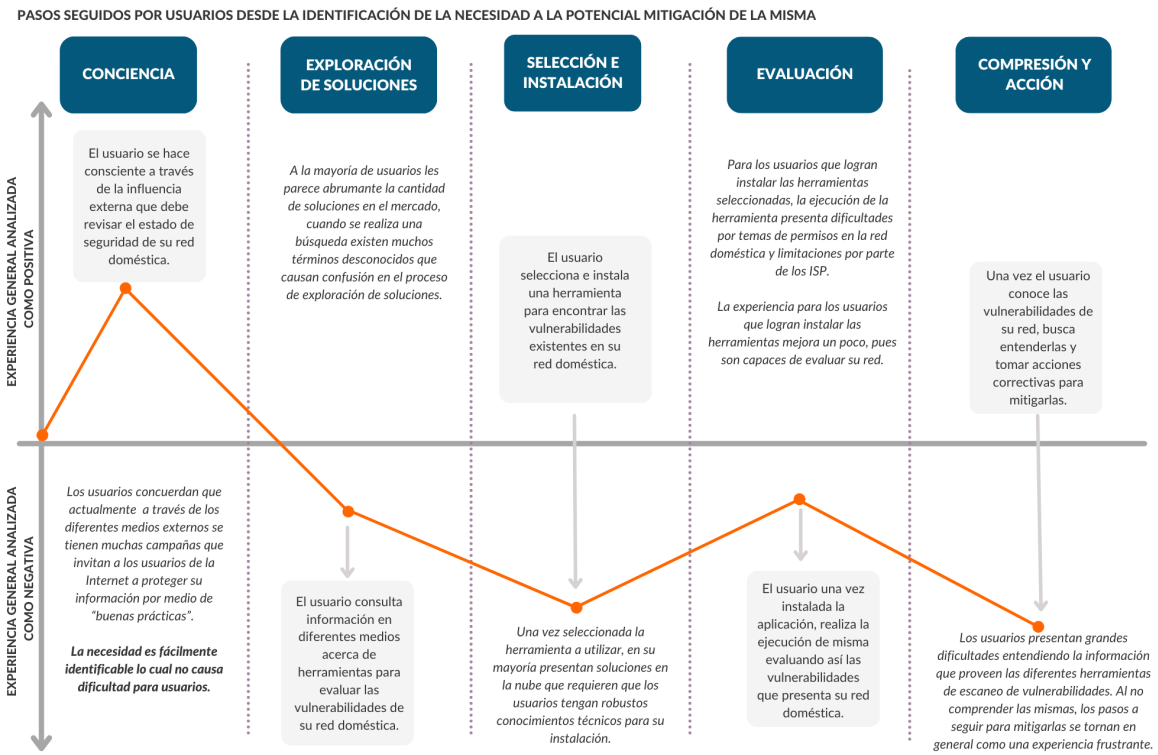

Figura 3.13: *Customer Journey Map*

En la figura 3.13, se muestra un *customer journey map* creado a partir de la encuesta exploratoria realizada, la observación del participante y, la generación de *USER*-personas. En el análisis es determinada una escala que evalúa la experiencia del usuario como negativa o positiva, todo esto se hace con el fin de identificar los puntos de dolor del proceso.

Los puntos de dolor que van a ser foco de la presente investigación son: selección, instalación, evaluación, compresión y acción. Estos puntos de dolor serán sub-didividos en fases funcionales dentro del uso de la solución planteada; estas fases fueron descritas en el caso de uso usado para la validación de la investigación.

3.1.1.2. Etapa de definición

Los usuarios de redes domésticas de la ciudad de Popayán por su gran uso de la red de Internet desde sus hogares están vulnerables a los miles de ataques que suceden diariamente, esta premisa soportada en la encuesta realizada y el análisis del anterior literal. Por esta razón la pregunta que resulta en la presente investigación es: ¿Cómo apoyar el aumento del nivel de ciberseguridad en los dispositivos de acceso a Internet doméstico de un ISP en la ciudad de Popayán?.

La definición del problema con respecto a este análisis fue abordado desde 2 perspectivas: la del usuario final y la de los investigadores.

Perspectiva del usuario final: “Yo como usuario de red residencial en mi hogar realizo diariamente muchas acciones que dependen de datos manipulados a través de Internet, estas actividades incluyen pagos de servicios públicos, *streaming* de contenido en línea como entretenimiento, ingreso a portales de educación en línea. Hace unas semanas un *malware* ingresó a mi sistema y dañó muchos de mis archivos, causándome a mí y a mi familia una gran preocupación para tomar medidas con el fin de prevenir que esto vuelva a ocurrir. Sin embargo las herramientas que busco en línea son muy difíciles de entender y solamente me ayudan a detectar vulnerabilidades más no me da ningún tipo de información para mitigarlas”.

Perspectiva por parte de los investigadores: La metodología *Design Thinking* pretende que por parte de los investigadores es necesario dar respuesta a las 4 W (*Who, What, Where and Why*) las cuales serán definidas para la problemática:

- ***Who:*** Usuarios con conocimientos técnicos limitados, quienes cuentan con redes domésticas contratadas por medio de ISP.
- ***What:*** El problema radica en el enfoque de las herramientas de medición existentes, estas suelen plantear complicaciones para usuarios con conocimientos técnicos limitados. Según la literatura, la mayoría de estas herramientas fueron diagramadas para principalmente la detección de vulnerabilidades, pero carecen de funcionalidades para la prevención o que apoyen la corrección por medio de recomendaciones.
- ***Where:*** Esta solución debe estar enfocada en usuarios residentes de la ciudad Popayán- Cauca- Colombia.
- ***Why:*** Los usuarios de la ciudad ya están identificando la necesidad de tomar acciones preventivas en pro de la seguridad de sus redes domésticas.

3.1.1.3. Etapa de idear

A partir de la ejecución del proceso de lluvia de ideas de la Figura 3.14, surge la definición de 3 soluciones diferentes para abordar la problemática del trabajo de investigación:

Figura 3.14: Ideas encontradas

Tablet de seguridad fácil de usar

Un dispositivo que tenga una interfaz clara y fácil de entender sobre el estado de seguridad de la red del usuario. La pantalla o *tablet* individual podría mostrar una representación visual de la red, destacando los dispositivos conectados y su estado de seguridad, con el fin que esto sea entendido por un usuario no técnico.

La *tablet* debe proporcionar recomendaciones y guías paso a paso para mejorar la seguridad, como cambiar las contraseñas predeterminadas, actualizar el *firmware* y habilitar el cifrado. La *tablet* puede incluso enviar notificaciones o alertas cuando se detecta actividad sospechosa, utilizando un lenguaje simple para explicar la amenaza potencial y los pasos que el usuario debe seguir para abordarla; debe de igual manera tener una interfaz gráfica visualmente agradable para usuarios en redes residenciales.

Nota sobre la idea: Con base en la sesión conducida por los investigadores la solución no era el mejor curso de acción, esta planteaba una **dificultad técnica** fuera del alcance de la presente investigación por términos de los costos de crear *hardware* y *software* para la solución.

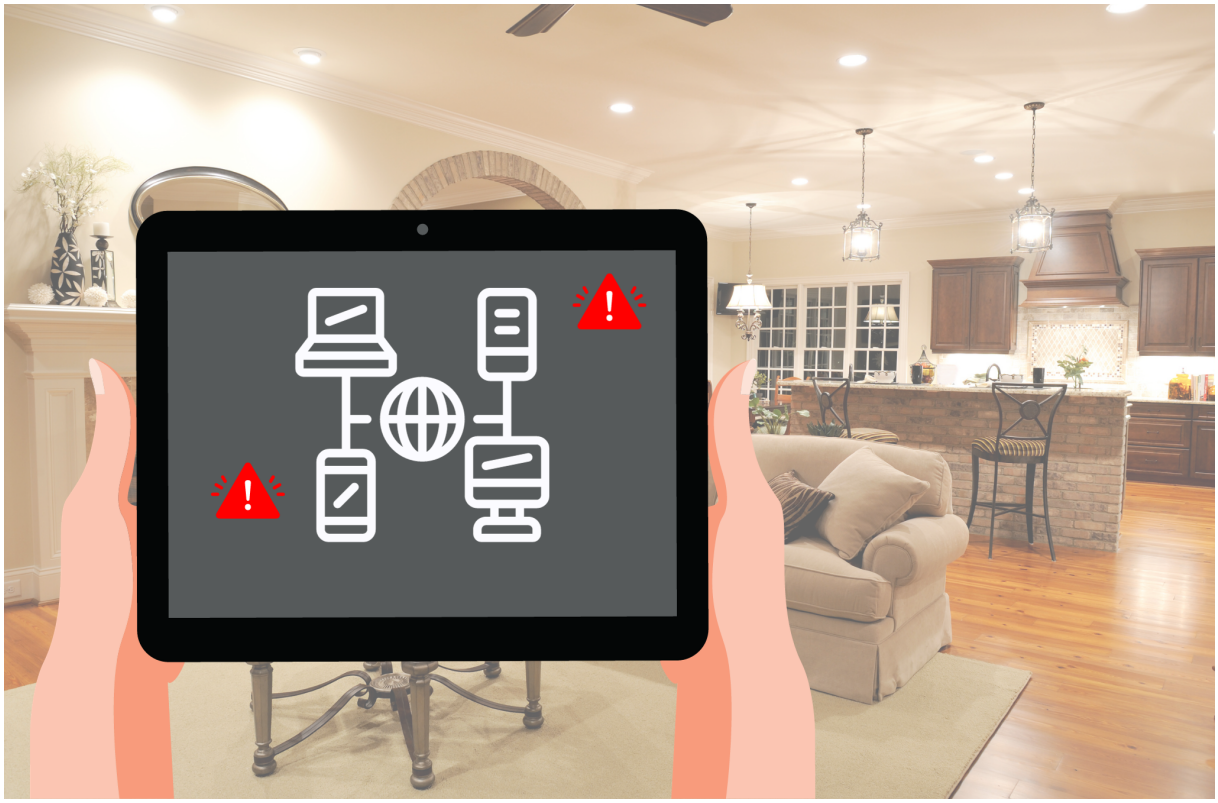

Figura 3.15: Propuesta A: *tablet* de seguridad fácil de usar

Aplicación de aprendizaje interactivo

Desarrollo de una aplicación móvil interactiva que eduque a los usuarios sobre la seguridad de la red a través de interesantes tutoriales, cuestionarios y simulaciones. La aplicación podría guiar a los usuarios a través de la configuración segura de sus redes domésticas, explicando conceptos como la creación de contraseñas seguras, la autenticación de dos factores y la configuración del *firewall* de una manera fácil de usar. Sería posible incorporar elementos de gamificación, donde los usuarios ganan puntos o insignias por completar tareas de seguridad o pasar cuestionarios. La aplicación también podría incluir una simulación de red doméstica virtual que permita a los usuarios experimentar con configuraciones de seguridad sin afectar su red real.

Nota sobre la idea: La idea no se desarrolla por falta de conocimientos técnicos lo que podría retrasar y desviar la meta de la solución de aportar a la seguridad de las redes domésticas; En el caso de una aplicación móvil el prototipo puede presentar resultados no deseados en caso de no estar conectado directamente al enrutador y podría evaluar otro tipo de vulnerabilidades con la red móvil celular o incluso presentar otros problemas no contemplados, lo cual no es el propósito de la presente investigación. Adicionalmente ios y android presentaban limitaciones diferentes en cuanto al tipo de solicitudes que se podían realizar desde los dispositivos con dichos sistemas operativos y con esto también disminuía la cantidad de tipos de vulnerabilidades que se podrían detectar.

Figura 3.16: Propuesta B: Aplicación de aprendizaje interactivo

Prototipo elegido: Asistente de seguridad

Un asistente virtual específicamente diseñado para la seguridad de la red doméstica. Este asistente es conectado de manera física con el enrutador a evaluar por medio de un cable de red ethernet, de esta manera la red doméstica es analizada de manera integral desde el punto de entrada de la misma apoyando así la protección de todos los dispositivos conectados. El asistente será elaborado en *software* sobre una *Raspberry Pi* por su gran robustez, el usuario elige el momento en que desee monitorear la red y este debe proveer una lista de vulnerabilidades detectadas y recomendaciones para cada una de ellas.

Nota sobre la idea: Esta idea **fue la elegida** en conjunto con el equipo de desarrollo y el usuario final, ya que no requiere de instalaciones complejas ni de cambios de permisos en los dispositivos de escaneo. Presenta una idea simple y un flujo fácilmente ejecutable donde el usuario simplemente conecta la herramienta al *router*, abre un navegador y da *click* en escanear y puede ver la información de su red residencial en conjunto con los resultados de vulnerabilidades.

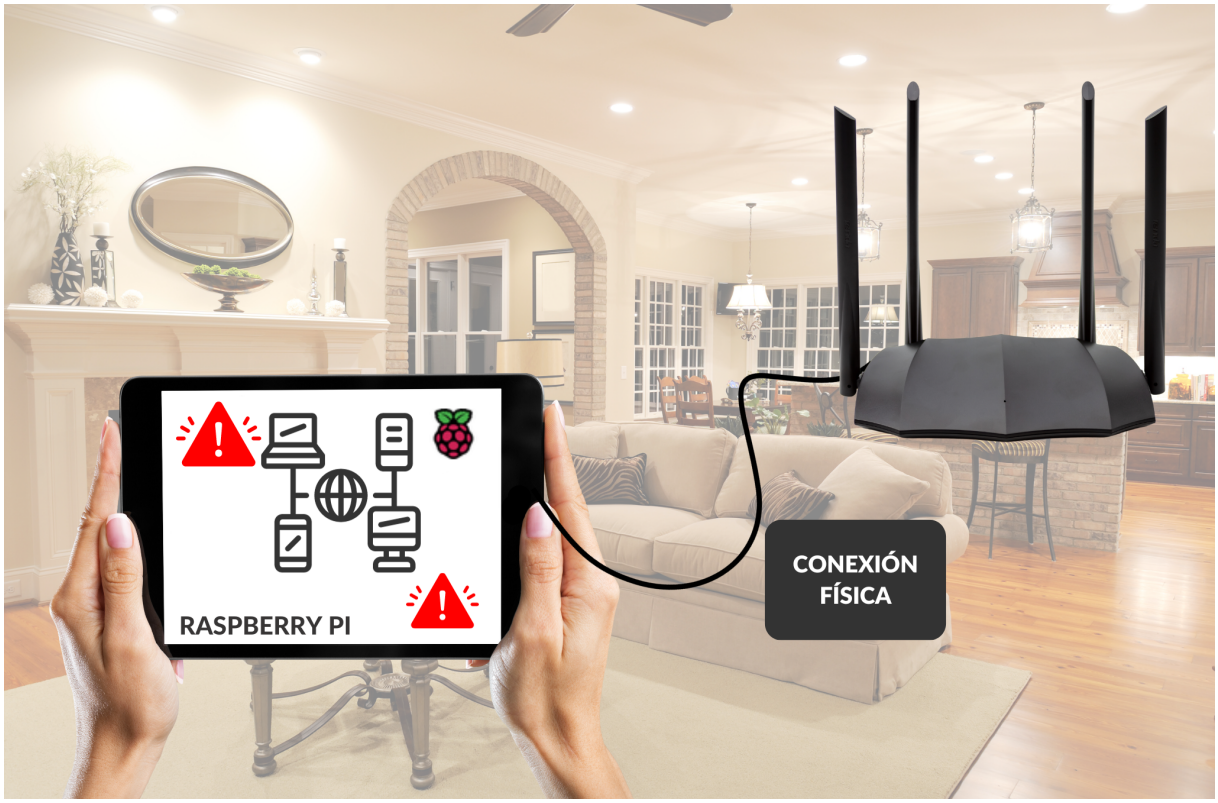

Figura 3.17: Propuesta C: Asistente de seguridad

Cada una de estas propuestas brindan soluciones fáciles de usar y accesibles para abordar la falta de conocimientos de seguridad entre los usuarios habituales de sus redes residenciales. La clave es simplificar los conceptos de seguridad complejos y hacerlos fácilmente comprensibles y prácticos para los usuarios sin experiencia técnica.

3.2. Marco conceptual desarrollado

3.2.1. Estudio de caso

Para propósitos de esta investigación es elaborado un estudio de caso para evaluar la eficiencia del mecanismo a desarrollar; entendiendo estudio de caso como un método de investigación caracterizado por investigar en profundidad una o más instancias de un suceso en específico en el contexto de la vida real. Este método tiene un enfoque cualitativo que busca proveer un entendimiento integral acerca de un fenómeno en concreto y que generalmente emplea una combinación de diferentes técnicas para recopilar datos, tales como entrevistas, observaciones, artefactos, entre otros. Algunas de las razones por las cuales se elige desarrollar un estudio de caso, son las siguientes:

- **Especificidad:** El estudio de caso está enfocado en una situación o caso en específico.
- **Contexto en la vida real:** Involucra estudiar el/los casos en su contexto natural para asegurarse la autenticidad de los descubrimientos.
- **Información cualitativa:** Utiliza métodos cualitativos para la recolección de datos, tales como encuestas, entrevistas, observaciones, entre otros. Es importante resaltar que si bien los métodos cualitativos tienen una presencia muy fuerte, el estudio de caso también puede hacer uso de métodos cuantitativos y mezclas de ambos.

3.2.1.1. Planeación del estudio de caso

Realizar un buen diseño de un estudio de caso es de gran importancia ya que de este depende en gran medida el éxito de mismo, siendo en este punto donde la información a ser recolectada y las preguntas iniciales que se buscan responder están relacionadas. En el libro *"CASE STUDY RESEARCH"* de Robert K. Yin [100], se mencionan 5 componentes de gran importancia para el diseño de un caso de un estudio de caso, los cuales son mencionados y desarrollados a continuación:

Preguntas del estudio de caso: Existen preguntas fundamentales que cada estudio de caso busca responder y son estas las que le dan una dirección clara a la investigación. En este caso, las preguntas están enfocadas en medir la eficiencia del mecanismo con base a su facilidad de uso, tiempo de escaneo y concientización de los usuarios acerca de las vulnerabilidades de su enrutador. Las preguntas planteadas son las siguientes:

- **Pregunta 1:** ¿Es el mecanismo eficiente en cuanto a concienciar a los usuarios sobre las vulnerabilidades de su enrutador?
- **Pregunta 2:** ¿Qué tan fácil de usar es el mecanismo para usuarios con diversos niveles de conocimientos técnicos?
- **Pregunta 3:** ¿Cuál es el fabricante de enrutadores para el cual el mecanismo presenta la mayor eficiencia en cuanto a tiempo de escaneo?
- **Pregunta 4:** ¿Cuánto les toma a los usuarios realizar el diagnóstico de su enrutador?

Premisas de estudio:

- **Premisas 1:** Los usuarios que hacen uso del mecanismo de diagnóstico son más conscientes de las vulnerabilidades de su enrutador.

- **Premisa 2:** El mecanismo es fácil de instalar y configurar, haciéndolo fácil de usar por usuario de diversos niveles de conocimientos técnicos.
- **Premisa 3:** Después de ser instalado y configurado el mecanismo, este logra diagnosticar el enrutador de manera rápida.

El caso: La selección del estudio de caso implica identificar el tipo de usuarios que harán parte de este, buscando que sean relevantes para dar respuesta a las preguntas planteadas previamente, por consiguiente:
La muestra seleccionada fueron 32 usuarios con diferentes niveles de conocimientos técnicos con el fin de que instalen, configuren, y utilicen el mecanismo de diagnóstico y apoyo a la mitigación de vulnerabilidades en enrutadores de uso doméstico.

Relación de la información obtenida y las premisas: En este apartado se describe de manera general cómo se utilizarán los métodos de recopilación de datos para investigar las premisas del estudio y dar respuesta a las preguntas formuladas. Teniendo entonces lo siguiente:

- **Concientización sobre las vulnerabilidades del enrutador:** Es necesario realizar dos encuestas, una encuesta previa al uso del mecanismo y otra posterior al uso del mecanismo para identificar el cambio en el nivel de conciencia que tienen los usuarios acerca de las vulnerabilidades presentes en su enrutador.
- **Facilidad de uso del mecanismo:** En la encuesta posterior al uso del mecanismo, son incluidas preguntas que aportan a identificar la facilidad de uso del mecanismo percibida por el usuario. También es necesario medir el tiempo empleado por el usuario para instalar y configurar exitosamente el dispositivo, este tiempo es medido desde el momento en que el usuario inicia la lectura de la "guía de inicio rápido"del mecanismo, hasta el momento en que el usuario culmina con su instalación y configuración.
- **Tiempo de escaneo:** Medir mediante el reloj integrado del mecanismo el tiempo que le toma a este realizar el diagnostico de cada enrutador, este tiempo inicia en el momento en que el mecanismo recibe por parte del usuario la orden de iniciar el diagnóstico y culmina en el momento que el reporte es mostrado en pantalla al usuario.

Criterios para interpretar los resultados:

- **Información relevante:** Los análisis e interpretaciones realizadas deben estar relacionadas con las premisas o preguntas formuladas en el estudio de caso, o proveer información que permita llegar a conclusiones de interés para el proyecto de investigación.
- **Calidad de los datos:** Identificar la distribución de los diferentes datos dentro de la muestra, para identificar su comportamiento y en algunos casos verificar la fiabilidad de la muestra.
- **Causalidad y correlación:** Diferenciar entre causalidad y correlación. Ya que dos eventos pueden estar relacionados, pero esto no quiere decir que uno cause el otro.
- **Análisis estadístico:** Realizar gráficas estadísticas que permitan una comprensión profunda de los datos recopilados.

- **Evitar sesgos:** Abstenerse de tomar partido o mostrar preferencias personales. En su lugar, enfocarse en el análisis en hechos y evidencia concretos. Evitar interpretaciones prematuras y mantenerse neutral.

3.2.1.2. Preparación del estudio de caso

En esta fase fueron sentadas las bases para llevar a cabo el caso de estudio de la mejor manera. Por tanto, para la realización del protocolo a seguir para la recolección de datos se tiene presente la lista de atributos básicos necesarios mencionados por Robert K. Yin en *"CASE STUDY RESEARCH"*, siendo estos:

- Realizar preguntas precisas e interpretar las respuestas correctamente
- Ser un oyente eficaz, evitando que las ideologías o las expectativas distorsionen la percepción.
- Mostrar disposición para adaptarse a los cambios según sea necesario.
- Realizar la investigación éticamente.

Elaboración de las entrevistas: Para la elaboración de las entrevistas inicialmente se definen 3 momentos o fases diferentes en el estudio de caso ya que se infiere de las preguntas planteadas durante la etapa planeación que es necesario realizar dos encuestas diferentes, cada una en un momento diferente para poder recopilar la información necesaria. Lo anterior, ya que para dar respuesta a la pregunta que hace referencia a la eficiencia del mecanismo en cuanto a mejorar el nivel de conciencia que tienen los usuarios acerca de las vulnerabilidades en su enrutador, es necesario saber cual es el nivel de conciencia del usuario previo al uso del mecanismo y cuál es el nivel después de usarlo. Por otro lado, en cuanto a la premisa referente a la facilidad de uso del mecanismo es claramente necesario que el usuario ya haya usado exitosamente el mecanismo, por lo que las preguntas que aporten información a esto se harán en la segunda encuesta.

En este orden de ideas, para definir las fases primero son identificadas las diferentes etapas dentro del evento objeto de investigación del estudio de caso y luego cada etapa es asignada a una de las fases con el fin de tener una visión clara de en qué momento realizar las encuestas y adicionalmente establecer las etapas exactas que comprenden los tiempos que dan respuestas a las otras preguntas del estudio de caso.
Las 3 fases, a las cuales se les asignan los nombres de, Fase Inicial (pre-uso), Fase de Acción (uso) y Fase Final (post-uso) son ilustradas en la figura 3.18 junto a las etapas que las componen.

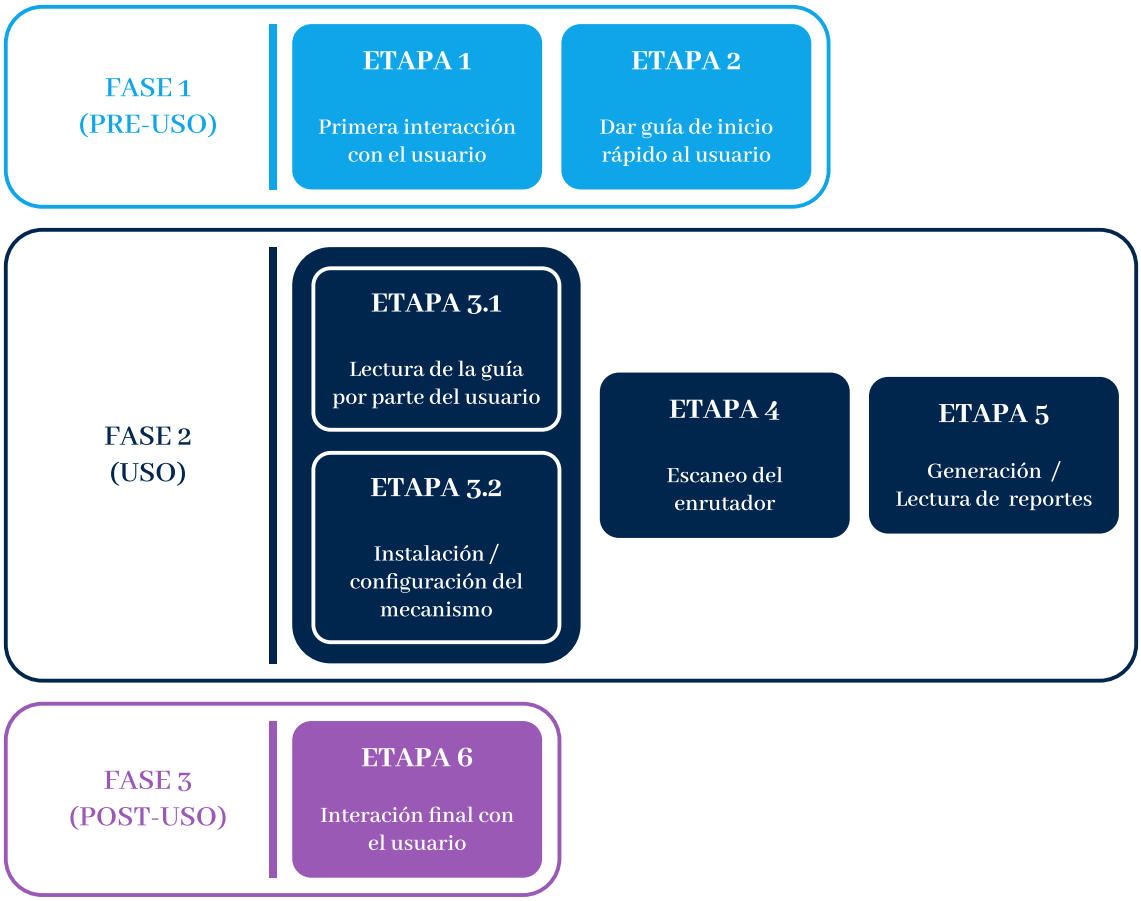

Figura 3.18: Etapas/Fases del caso

La primera encuesta es realizada en la fase Inicial (Fase 1 / Pre-uso), la encuesta 2 en la fase final (Fase 3 / Post-uso), el tiempo de escaneo hará referencia al tiempo de ejecución de la etapa 4 y el tiempo de instalación y configuración hará referencia el tiempo que tome la ejecución de la etapa 3.1 y 3.2.

La elaboración de las 2 encuestas es estructurada teniendo en cuenta la escala mixta de Likert-Thurstone descrita en el documento [35], donde se toman elementos de la escala de Likert y son incluidos elementos de la escala de Thurstone para tener una herramienta flexible pero rigurosa, que permita ser ampliamente personalizada para ajustarse a objetivos específicos de investigación. La tabla 3.3 representa la encuesta 1 y la tabla 3.4 representa la encuesta 2, donde cada columna indica lo siguiente:

- Columna 1 (“Componente”): Establece a que componente estará aportando la pregunta de la encuesta. Hay tres componentes, facilidad de uso, concientización y nivel técnico, donde cada está relacionado con una de las preguntas y/o premisas del estudio de caso.
- Columna 2 (“Pregunta”): Muestra el texto a desplegar en cuerpo de la pregunta de la encuesta.
- Columna 3 (“Respuestas”): Se definen las diferentes opciones de respuesta que tendrá la pregunta y el tipo de pregunta.

- Columna 4 ("Peso"): Es un coeficiente de 1 a 10 que se le da a cada pregunta y que representa el valor de aporte de la pregunta en la calificación final en su respectivo componente. Un peso mas alto indica que la respuesta a la pregunta tendrá una mayor influencia en resultado final, mientras que uno mas bajo representa un menor influencia.

Es importante resaltar que algunas preguntas no tienen asignado un componente ni un peso debido a que dichas preguntas cumplen con la única función de obtener información extra que permita hacer diferentes análisis, que no necesariamente están ligados a la eficiencia del mecanismo. Las entrevistas son las siguientes:

La entrevista 1 consta de 9 preguntas, 4 de ellas aportan al componente técnico, 3 al componente de concientización y 2 de ellas no están ligadas a ningún componente.

Componente	Pregunta	Respuestas	Peso
-	¿En cuál de los siguientes rangos de edad se encuentra usted?	- 18 a 25 años - 26 a 40 años - 40 años o más	-
Nivel técnico	¿Qué tan cómodo/a se siente utilizando dispositivos tecnológicos tales como computadores, smartphones, entre otros?	Escala: 0-5 - 0: Nada cómodo/a - 5: Totalmente cómodo/a	6
Nivel técnico	¿Qué tan confiado/a se siente para solucionar problemas técnicos en su computador y/o dispoitivos tecnologicos usted mismo/a?	Escala: 0-5 - 0: Nada confiado/a - 5: Totalmente confiado/a	8
Nivel técnico	¿Qué tan capaz se siente de realizar usted mismo la instalción de dispostivos tecnológicos en su casa, tales como smart tvs, repetidores de señal, entre otros?	Escala: 0-5 - 0: Nada capaz - 5: Totalmente capaz	9
Nivel técnico	¿Cómo calificaría su competencia técnica en seguridad de redes?	Escala: 0-5 - 0: Nada competente - 5: Totalmente competente	10
Concientización	¿Qué tan consciente está de las posibles vulnerabilidades en su enrutador?	Escala: 0-5 - 0: Para nada consciente - 5: Completamente consciente	10
Concientización	¿Qué tan preparado se siente para enfrentar posibles vulnerabilidades en su enrutador?	Escala: 0-5 - 0: Nada preparado/a - 5: Totalmente preparado/a	8
Concientización	¿Qué tan familiarizado está con los riesgos potenciales de no tener una buena seguridad en su red residencial?	Escala: 0-5 - 0: Nada familiarizado/a - 5: Totalmente familiarizado/a	6
-	¿Ha sido usted víctima de un ataque de ciberseguridad?	- Sí - No - No sé	-

Tabla 3.3: Entrevista 1

La entrevista 2 consta de 13 preguntas, 6 de ellas aportan al componente técnico, 4 al componente de concientización y 3 de ellas no están ligadas a ningún componente.

Componente	Pregunta	Respuestas	Peso
Facilidad de uso	¿Qué tan claras fueron las intrucciones de instalación dadas con el mecanismo?	Escala: 0-5 - 0: Nada claras - 5: Totalmente claras	6
Facilidad de uso	¿Qué tan fácil fue instalar y usar el mecanismo?	Escala: 0-5 - 0: Nada fácil - 5: Extremadamente fácil	10
Facilidad de uso	¿Qué tanta ayuda externa necesitó para usar el mecanismo?	Escala: 0-5 - 5: Ningúna ayuda - 0: Mucha ayuda	7
Facilidad de uso	¿Qué tan intutivas le parecieron las interfaces del mecanismo?	Escala: 0-5 - 0: Nada intuitivas - 5: Totalmente intuitivas	8
Facilidad de uso	¿Cuánta confusión o frustración experimentó durante el uso del mecanismo?	Escala: 0-5 - 0: Nada de confusión/frustración - 5: Mucha confusión/frustración	8
Facilidad de uso	¿Qué le pareció la velocidad de escaneo del mecanismo?	Escala: 0-5 - 0: Muy lenta - 5: Muy Rápida	2
Concientización	¿Qué tan clara fue la información dada por el mecanismo acerca de las vulnerabilidades de seguridad de su enrutador y su nivel de riesgo?	Escala: 0-5 - 0: Nada clara - 5: Totalmente clara	8
Concientización	¿Qué tan consciente está de las posibles vulnerabilidades en su enrutador ahora?	Escala: 0-5 - 0: Para nada consciente - 5: Completamente consciente	10
Concientización	¿Qué tan preparado se siente ahora para enfrentar posibles vulnerabilidades en su enrutador?	Escala: 0-5 - 0: Nada preparado/a - 5: Totalmente preparado/a	8
Concientización	¿Qué tan familiarizado está con los riesgos potenciales de no tener una buena seguridad en su red residencial?	Escala: 0-5 - 0: Nada familiarizado/a - 5: Totalmente familiarizado/a	6
-	¿Qué tan frecuentemente considera que haría uso de la herramienta?	- Nunca - 1 vez al año - Varias veces al año - 1 vez al mes - Varias veces al mes - 1 vez a la semana - Varias veces a la semana - A diario	-
-	¿Hubo alguna vulnerabilidad que encontró particularmente alarmante o inesperada?	- Si - No	-
-	¿Cuál vulnerabilidad encontró particularmente alarmante o inesperada?	Pregunta abierta	-

Tabla 3.4: Entrevista 2

Ser un oyente eficaz, evitando que las ideologías o las expectativas distorsionen la percepción. Para cumplir con este atributo son planteadas ciertas pautas, las cuales se listan a continuación:

- No ayudar al usuario si este no lo solicita.
- Escuchar atentamente las posibles preguntas realizadas por el usuario para responderlas asertivamente y evitando dar información extra no necesaria y/o solicitada.
- Evitar interrupciones.
- Escuchar y responder sin prejuicios.
- Tomar notas de situaciones relevantes.

Mostrar disposición para adaptarse a los cambios según sea necesario. Se plantea revisar las notas tomadas durante cada interacción de un nuevo usuario con el mecanismo, y con base en esto realizar modificaciones al caso de estudio, su proceso, herramientas de medición, entre otros, y así lograr el mejor resultado posible. Las modificaciones que

se puedan llegar a realizar siempre deberán ser realizadas manteniendo presente el/los objetivos principales del caso de estudio y evitando que este pierda rigurosidad. También, se plantea que la revisión de las notas tomadas y realización de modificaciones se deberá hacer con una periodicidad de 5 usuarios evitando así que el caso de estudio se desarrolle con falencias prolongadas.

Realizar la investigación éticamente: Para hacer efectivo este atributo, se crea un documento de "Consentimiento informado", el cual deberá ser leído y aceptado por todo usuario previo a iniciar el uso del mecanismo. Este documento está disponible en el anexo "H - Consentimiento informado", y define las políticas con las cuales se tratarán los datos recopilados y establece que solo serán usados con fines académicos.

Capítulo 4

Validación del modelo conceptual desarrollado

Contenido

4.1. Desarrollo del prototipo

4.1.1. Planeación SCRUM

4.1.1.1. Investigación previa

Identificación de bases de datos especializadas en vulnerabilidades de ciberseguridad

Para identificar las vulnerabilidades que generan un nivel de severidad alto o crítico, fue ejecutada una recopilación de las bases de datos especializadas en vulnerabilidades de ciberseguridad definiendo así cuál era la más indicada para ser usada como base para el desarrollo de este proyecto. Algunas de las bases de datos encontradas y exploradas fueron:

- ***Common Vulnerabilities and Exposures* (CVE)**: Es una base de datos de vulnerabilidades de ciberseguridad que utiliza una nomenclatura estandarizada para identificar las vulnerabilidades. [101]
- ***National Vulnerability Database* (NVD)**: Es una base de datos mantenida por el Centro Nacional de Seguridad de la Información (NCSC) de Estados Unidos y es considerada una de las más completas y confiables. [102]
- ***GitHub Advisory Database* (GAD)**: Es una base de datos de vulnerabilidades que forma parte de la característica GitHub Advisories de la plataforma de almacenamiento y colaboración de código GitHub. La base de datos incluye información sobre vulnerabilidades conocidas en proyectos de código alojados en GitHub y proporciona instrucciones para mitigar o solucionar cada vulnerabilidad. [103]
- ***China National Vulnerability Database* (CNVD)**: Es una base de datos de vulnerabilidades y amenazas a la seguridad informática e incluye información sobre vulnerabilidades y amenazas conocidas en software y sistemas operativos, así como recomendaciones sobre cómo protegerse contra ellas. [104]

De estas, la base de datos de vulnerabilidades de ciberseguridad CVE es seleccionada como la principal, esta muestra ser uno de los mejores recursos de información sobre vulnerabilidades y también es usada como referencia por otras bases de datos. Algunas de las razones por las que CVE es muy valorado por los profesionales de seguridad y es de gran interés para el desarrollo de este proyecto, son:

- **Amplio alcance:** CVE cubre una amplia variedad de productos y sistemas, incluyendo *software* y *hardware* de código abierto y cerrado. Esto hace que sea una fuente de información valiosa para profesionales de seguridad que buscan proteger diferentes tipos de sistemas y aplicaciones.
- **Consistencia:** CVE utiliza un sistema de numeración único para identificar cada vulnerabilidad y proporciona información detallada sobre cada una de ellas. Esto hace que sea fácil para los profesionales de seguridad, y otros usuarios, buscar y comparar información sobre vulnerabilidades.
- **Colaboración:** CVE es mantenida por el *MITRE Corporation*, una organización sin fines de lucro que trabaja en colaboración con otras organizaciones e individuos para recopilar y publicar información sobre vulnerabilidades. Esto hace que la base de datos sea una fuente de información fiable y actualizada.

- **Accesibilidad:** CVE es una base de datos de código abierto y es accesible para cualquier persona interesada en la ciberseguridad. Esto hace que sea fácil para los profesionales de seguridad y otros usuarios obtener información sobre vulnerabilidades y proteger sus sistemas.

En conclusión, CVE es una base de datos de vulnerabilidades de ciberseguridad muy valorada debido a su amplio alcance, consistencia, colaboración y accesibilidad.

Identificación de los principales ISP de la ciudad de Popayán

Para establecer los principales ISP de la ciudad de Popayán es necesario conocer los rangos de direcciones IP asignados a la ciudad y contar con un servicio que permita la identificación del ISP a partir de la dirección IP.

Fueron identificadas *MaxMind* e *IP2Location* como las bases de datos para este fin, las cuales son dos empresas que proporcionan servicios relacionados con la geolocalización de direcciones IP y ofrecen bases de datos actualizadas periódicamente, aquí son correlacionadas las direcciones IP especificas con su ubicación geográfica aproximada.

MaxMind es una empresa que especializada en la geolocalización de direcciones IP, así como en otros servicios relacionados con la identificación y prevención del fraude en línea, está ofrece una base de datos llamada GeoIP que contiene información sobre la ubicación geográfica, proveedor de servicios de Internet (ISP) y otros datos relacionados con las direcciones IP. Esta base de datos es ampliamente utilizada por empresas en el campo de la publicidad en línea, análisis de tráfico *web*, sistemas de prevención de fraude y personalización de contenido.

IP2Location, también es una empresa que ofrece servicios de geolocalización de direcciones IP. Proporciona una base de datos llamada *IP2Location* que contiene información detallada sobre la ubicación geográfica de una dirección IP, como el país, región, ciudad, código postal, coordenadas de latitud y longitud, proveedor de servicios de Internet y dominio. Esta base de datos es utilizada en una amplia gama de aplicaciones, incluyendo análisis de tráfico *web*, segmentación geográfica, detección de fraude, personalización de contenido y restricción geográfica.

Los servicios de *MaxMind* e *IP2Location* son utilizados por muchas organizaciones y desarrolladores en todo el mundo para mejorar la experiencia del usuario, mejorar la seguridad en línea y, personalizar servicios y contenidos basados en la ubicación geográfica de los usuarios.

Con el propósito de obtener la información pertinente, fueron gestionados los recursos para adquirir la base de datos paga de *MaxMind*, este registro contiene las direcciones IP con un alto nivel de certeza de estar asignadas a la localidad de Popayán. Es relevante destacar que los datos en cuestión se encuentran actualizados hasta *el 14 de abril de 2023* fecha en la cual se hace la compra de la base de datos. Posteriormente, se utiliza un servicio *API REST* gratuito suministrado por IP2Location para obtener el proveedor de servicios de internet (ISP) con mayor probabilidad de tener asociado dicho rango de direcciones IP.

Identificación de herramientas de apoyo para el modelado del prototipo

Fueron elegidas herramientas eficientes para realizar la identificación y clasificación de posibles vulnerabilidades en los dispositivos de acceso a la Internet, como los *routers*. Estas son especializadas para el requerimiento, entre ellas: Nmap, Python-Nmap y CVE API.

1. **Nmap:** Nmap, o Network Mapper, es una poderosa herramienta de código abierto utilizada para explorar redes y realizar tareas de escaneo de puertos y descubrimiento de *hosts*. Es ampliamente reconocida por su capacidad para detectar sistemas activos en una red, identificar servicios y puertos abiertos en esos sistemas. Nmap también puede realizar detección de vulnerabilidades mediante el uso de scripts personalizados, lo que resulta especialmente útil en el contexto del diagnóstico de *routers*.

2. **Python Nmap:** Por su parte Python-Nmap es la biblioteca de Python; brinda una interfaz de programación para interactuar con las funcionalidades de Nmap y con esto permite la automatización de muchas de sus funcionalidades.

3. **Script Vulners Nmap:** El script "vulners" es una adición valiosa al escáner de red Nmap, diseñada para detectar y evaluar vulnerabilidades en sistemas y aplicaciones. Al aprovechar la base de datos de Vulners, el script realiza consultas que comparan las versiones de *software* y servicios encontrados durante el escaneo con las vulnerabilidades conocidas. Esta funcionalidad permite a los administradores de sistemas y profesionales de seguridad identificar y mitigar riesgos al proporcionar información detallada sobre las vulnerabilidades encontradas, como descripciones, referencias y enlaces a soluciones o parches. Sin embargo, es crucial utilizar el *script* éticamente y con el consentimiento adecuado del propietario del sistema o red escaneada, además de mantener actualizada la base de datos de *Vulners* para obtener los resultados más precisos.

4. **CVE APIs:** En cuanto a CVE API (Common Vulnerabilities and Exposures Application Programming Interface) es una interfaz de programación de aplicaciones que brinda acceso a la base de datos de NVD. Esta base de datos mantiene un registro de vulnerabilidades conocidas en *software*, incluidos los sistemas operativos y los protocolos de red utilizados en los *routers*, así mismo posibles maneras para mitigar las distintas vulnerabilidades registradas. Al consumir la CVE API, se busca obtener información muy detallada de las posibles vulnerabilidades detectadas.

Búsqueda de aplicaciones existentes para el diagnóstico y mitigación de vulnerabilidades en ciberseguridad de los dispositivos de acceso a la Internet hogar.

En la siguiente sección son identificadas y agrupadas aplicaciones existentes según sus características técnicas, estas presentan gran utilidad para el prototipo desarrollado.

Existen algunas aplicaciones y herramientas como Nessus, Metasploit, Nmap, Aircrack-ng, entre otras, las cuales son ampliamente utilizadas y permiten realizar pruebas de penetración a dispositivos de red, sin embargo, la mayoría de estas no están orientadas al análisis del dispositivo de acceso a la Internet. Adicional a esto, muchas de estas aplicaciones y herramientas no poseen una interfaz gráfica y deben ser utilizadas a través de la interfaz de línea de comandos de una máquina.

Por otro lado, existen aplicaciones móviles como RouterCheck, Fing y la desarrollada en el artículo *"Design Implementation and Evaluation of a Mobile Security Scanner App for*

Smart Home User" que proveen una interfaz gráfica para que los usuarios finales puedan realizar un diagnóstico de ciberseguridad de los dispositivos de su red. La última aplicación mencionada tiene un modo *"Expert"* que permite a un usuario con más conocimiento técnico observar información detallada del escaneo y otros dos modos orientados a usuarios con conocimientos técnicos más básicos o sin ningún tipo de conocimiento en el tema. Estas 3 aplicaciones chequean principalmente las contraseñas utilizadas, características peligrosas habilitadas, versión del *firmware*, puertos abiertos, configuración del DNS entre otros.

4.1.1.2. Product *Backlog*

1. El sistema debe identificar y obtener información de la puerta de enlace predeterminada de la red.
2. El sistema debe ser capaz de realizar un escaneo de vulnerabilidades en el dispositivo que actúa como puerta de enlace en la red local.
3. El sistema debe adaptar, filtrar y organizar los resultados del escaneo de vulnerabilidades.
4. El sistema debe obtener información adicional sobre las vulnerabilidades utilizando una API de CVE.
5. El sistema debe guardar los resultados del escaneo en archivos JSON.
6. El sistema debe basarse en un patrón de arquitectura de softwate REST [1].
7. El sistema debe establecer una conexión entre el cliente (*frontend*) y el servidor (*backend*)
8. El sistema debe contar con un cliente que provea una interfaz de usuario intuitiva a primera vista.
9. El sistema debe ser capaz de proveer recomendaciones para apoyar la mitigación de cada una de las vulnerabilidades detectadas.
10. El servidor del sistema debe ser responsable de manejar todas las operaciones y reglas de negocio. Debe contener la lógica necesaria para procesar y transformar los datos, interactuar con otras API o servicios, y realizar cualquier otra tarea relacionada con el funcionamiento principal del sistema. El servidor debe ser desarrollado utilizando algún *framework* moderno como *Flask* que sea capaz de procesar las solicitudes HTTP provenientes del cliente.
11. El cliente, debe ser desarrollado utilizando un *framework* moderno que brinde características avanzadas y facilidades para el desarrollo eficiente de aplicaciones web. El *framework* seleccionado debe ser compatible con las tecnologías y requisitos técnicos del sistema.

[1] Según *Amazon Web Services* [105] la transferencia de estado representacional (REST) es una arquitectura de software que impone condiciones sobre cómo debe funcionar una API. En un principio, REST se creó como una guía para administrar la comunicación en una red compleja como Internet. Es posible utilizar una arquitectura basada en REST para admitir comunicaciones confiables y de alto rendimiento a escala

12. El cliente debe ser capaz de permitir al usuario solicitar en un momento específico el escaneo del dispositivo de acceso a la Internet.

13. El cliente debe ser capaz de renderizar los resultados del escaneo de su dispositivo de acceso a la Internet.

14. El cliente debe ser capaz de contabilizar el tiempo transcurrido desde que se inicio el escaneo y presentarlo en un formato legible y comprensible para los usuarios, como MM:SS.

15. El cliente debe actualizar la interfaz de usuario de manera dinámica en respuesta a cambios en los datos o eventos.

16. El cliente debe permitir al usuario ajustar la visualización de la interfaz según sus preferencias. Para lograr esto, el cliente debe ofrecer una opción para alternar entre un formato de interfaz condensado, que muestre una vista general compacta, y un formato de interfaz detallado, que proporcione información más completa y desglosada.

17. En un primer momento, el cliente debe mostrar un listado conciso que incluya información sobre la cantidad de vulnerabilidades detectadas, su ID de CVE y su nivel de severidad.

18. En un segundo momento, cuando el usuario requiera información adicional sobre una vulnerabilidad, el cliente deberá mostrar detalles como el puerto en el que se identificó dicha vulnerabilidad, un resumen que describa en qué consiste la vulnerabilidad, el puntaje CVSS, la fecha de publicación de la vulnerabilidad y la última fecha de actualización. Además, se debe incluir una sección que muestre la cantidad de recomendaciones disponibles, así como una vista compacta que enumere el nombre de cada recomendación.

19. En un tercer momento, cuando el usuario solicite información adicional sobre una recomendación, se deberá mostrar los prerrequisitos necesarios para implementar la recomendación, un resumen que describa en qué consiste la recomendación, y posibles soluciones que puedan aplicarse.

4.1.1.3. Generación de épicas

1. Escaneo de vulnerabilidades en la puerta de enlace de la red local:

   - Como usuario, quiero que el sistema realice un escaneo de vulnerabilidades en el dispositivo que actúa como puerta de enlace en la red local, para identificar posibles riesgos de seguridad.

2. Organización y filtrado de los resultados del escaneo de vulnerabilidades:

   - Como usuario, quiero que el sistema adapte, filtre y organice los resultados del escaneo de vulnerabilidades, para que estos sean más fácil de entender y manejar.

3. Obtención de información adicional sobre las vulnerabilidades mediante una API de CVE:

- Como usuario, quiero que el sistema obtenga información adicional sobre las vulnerabilidades detectadas, para tener una comprensión más completa de cada vulnerabilidad.

4. Guardado de los resultados del escaneo en archivos JSON:
   - Como usuario, quiero que el sistema guarde los resultados del escaneo de vulnerabilidades en archivos JSON, para poder revisarlos y analizarlos en el futuro.
5. Establecimiento de conexión entre el cliente y el servidor:
   - Como usuario, quiero que el sistema tenga la capacidad de establecer una conexión entre el cliente (*frontend*) y el servidor (*backend*), para poder interactuar con el sistema de manera efectiva y fluida.
6. Provisión de recomendaciones para el apoyo a la mitigación de vulnerabilidades:
   - Como usuario, quiero que el sistema proporcione recomendaciones para apoyar la mitigación de cada una de las vulnerabilidades detectadas, para tomar medidas y mejorar la seguridad de la red.
7. Desarrollo del cliente con una interfaz de usuario intuitiva:
   - Como usuario, quiero que el cliente tenga una interfaz de usuario intuitiva a primera vista, para poder interactuar con el sistema de manera fácil y eficiente.

4.1.1.4. Generación de historias de usuario/tareas

1. Como administrador de red, quiero que el sistema identifique y obtenga información de la puerta de enlace predeterminada de la red, para poder utilizarla como punto de partida para el escaneo de vulnerabilidades.
2. Como administrador de seguridad, quiero que el sistema realice un escaneo de vulnerabilidades en el dispositivo que actúa como puerta de enlace en la red local, para identificar posibles riesgos de seguridad.
3. Como administrador de seguridad, quiero que el sistema adapte, filtre y organice los resultados del escaneo de vulnerabilidades, para que pueda revisarlos de manera estructurada y comprensible.
4. Como administrador de seguridad, quiero que el sistema obtenga información adicional sobre las vulnerabilidades utilizando una API de CVE, para tener una visión más detallada de cada vulnerabilidad detectada.
5. Como administrador de seguridad, quiero que el sistema guarde los resultados del escaneo de vulnerabilidades en archivos JSON, para poder realizar análisis posteriores y comparar los resultados con escaneos anteriores.
6. Como desarrollador, quiero implementar un patrón de arquitectura tipo API REST para el sistema para asegurar una comunicación eficiente entre el cliente y el servidor.
7. Como desarrollador, quiero desarrollar el servidor utilizando un *framework* moderno como *Flask*, para poder procesar las solicitudes HTTP provenientes del cliente y realizar las operaciones y reglas de negocio necesarias.

8. Como usuario, quiero que el cliente provea una interfaz de usuario intuitiva a primera vista, para poder interactuar con el sistema de manera fácil y eficiente.

9. Como usuario, quiero poder solicitar en un momento específico el escaneo del dispositivo de acceso a Internet, para verificar su seguridad en cualquier momento.

10. Como usuario, quiero que el cliente muestre los resultados del escaneo de mi dispositivo de acceso a Internet, para poder revisarlos y tomar las medidas necesarias para mejorar la seguridad.

11. Como usuario, quiero que el cliente muestre el tiempo transcurrido desde que se inició el escaneo de manera legible y comprensible, para tener una idea del tiempo que ha pasado.

12. Como usuario, quiero que el cliente actualice la interfaz de usuario dinámicamente en respuesta a cambios en los datos o eventos, para mantenerme informado de cualquier actualización relevante.

13. Como usuario, quiero poder ajustar la visualización de la interfaz según mis preferencias, alternando entre un formato condensado y un formato detallado, para tener una vista general o una vista más completa de los resultados.

14. Como usuario, quiero que el cliente muestre un listado conciso de las vulnerabilidades detectadas, incluyendo información como la cantidad de vulnerabilidades, su ID de CVE y su nivel de severidad.

15. Como usuario, quiero que el cliente muestre detalles adicionales específicos sobre cada vulnerabilidad, como el puerto en el que se identificó, un resumen de la vulnerabilidad, el puntaje CVSS, la fecha de publicación y la última fecha de actualización.

16. Como usuario, quiero que el cliente muestre la cantidad de recomendaciones disponibles para una vulnerabilidad, junto con una lista de nombres de recomendaciones en una vista compacta.

17. Como usuario, quiero que el cliente muestre información adicional sobre una recomendación específica, como los prerrequisitos necesarios, un resumen de la recomendación y posibles soluciones aplicables.

4.1.2. Desarrollo de los *Sprints*

Posterior a la preparación del modelo de Scrum y la asignación de responsabilidades al equipo de trabajo es pertinente proceder con el diseño y desarrollo del mecanismo; para sintetizar la documentación se dividió en la documentación de los *Sprints* Iniciales y la de los *Sprints* Finales.

4.1.2.1. *Sprints* Iniciales

La representación visual de la arquitectura, mostrada en la Figura 4.1, ilustra un funcionamiento más detallado del mecanismo. En este esquema, es posible observar la interconexión entre distintos módulos. Es importante destacar que la interacción del usuario se limita exclusivamente a la interfaz gráfica del mecanismo, es decir, al módulo de frontend dentro de la Raspberry Pi, facilitando así el uso del mecanismo.

Asimismo, cabe destacar la función primordial del módulo que alberga los scripts de despliegue y automatización. Este módulo se encarga de realizar la clonación de los repositorios correspondientes al frontend y backend. Además, lleva a cabo la ejecución de comandos diseñados para garantizar que dichos servicios se inicien de manera automática con cada arranque de la Raspberry Pi. Este enfoque, en última instancia, minimiza la necesidad de intervención por parte del equipo de desarrollo.

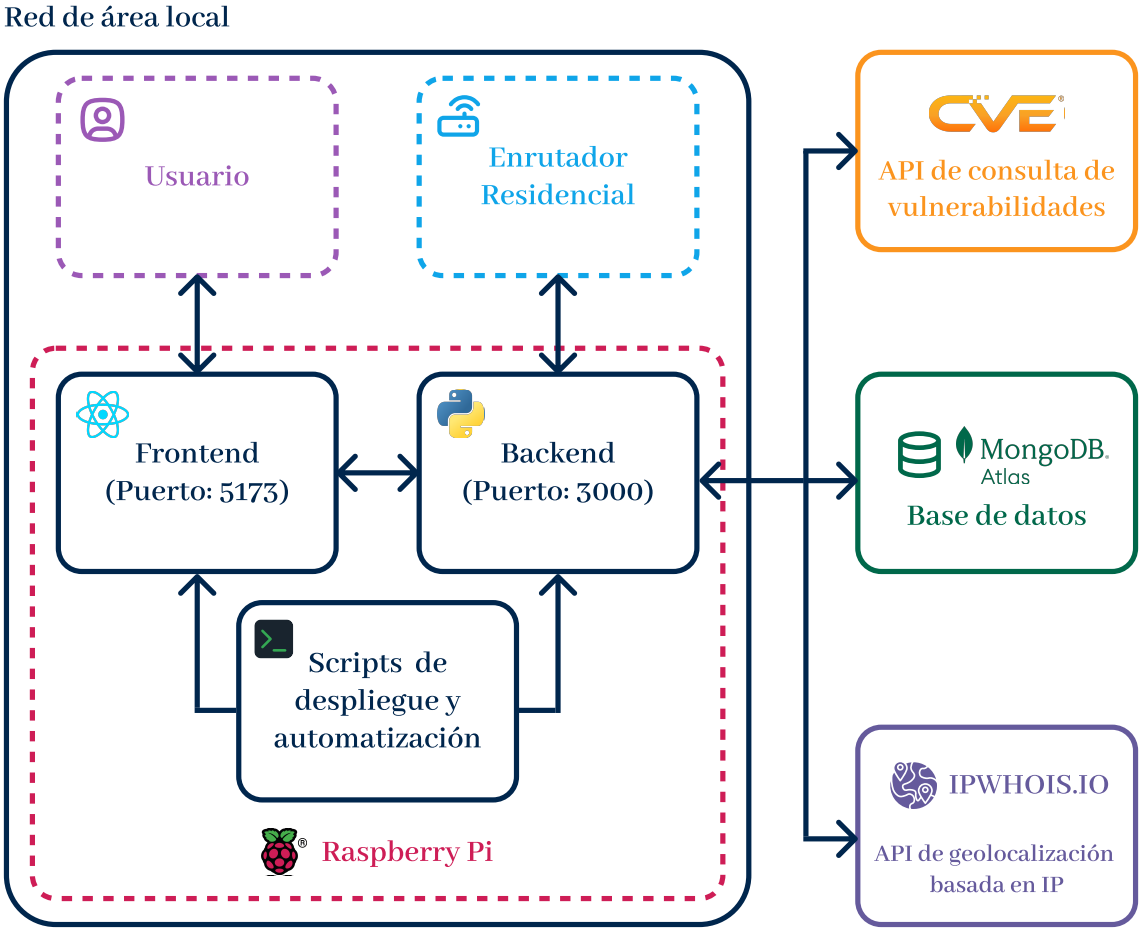

Figura 4.1: Arquitectura del mecanismo

La representación gráfica exhibida en la Figura 4.2 detalla el diagrama de secuencia, el cual desglosa la interacción intrínseca entre los tres módulos fundamentales del sistema. Dichos módulos comprenden el cliente frontend, el servidor backend, y la API del CVE. En dicha interacción se pueden observar los procesos principales que se ejecutan internamente en el servidor y aquellos que dependen de la interacción con terceros.

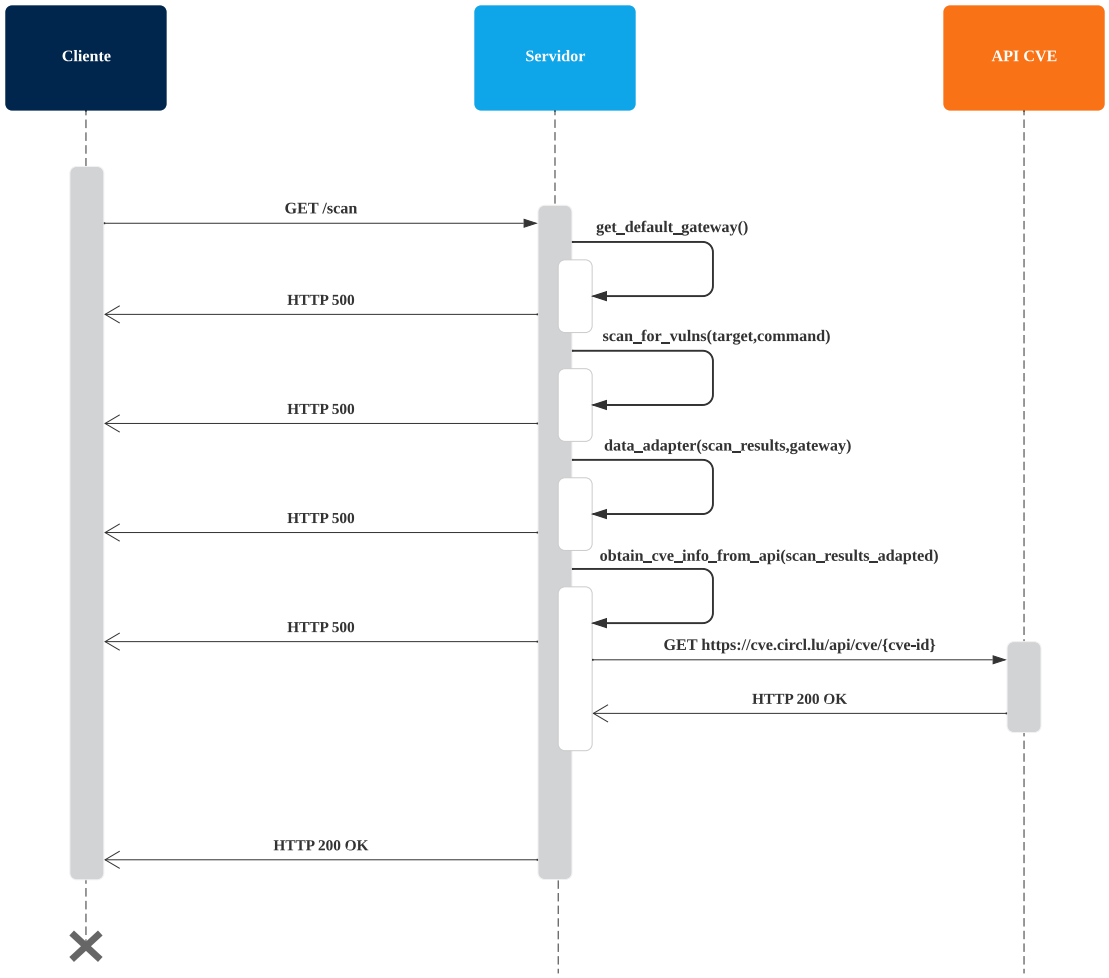

Figura 4.2: Diagrama de secuencia

Con el propósito de brindar una comprensión más profunda y detallada del mecanismo en cuestión, se ha desarrollado un diagrama de flujo que se desglosa en dos representaciones distintas. La primera, presentada como un flujo general en la Figura 4.3, aborda la secuencia global de interacciones entre los módulos esenciales del sistema. En paralelo, la segunda representación, evidenciada en la Figura 4.4, se enfoca específicamente en ilustrar el proceso inherente a la función de escaneo. Estos diagramas de flujo proporcionan una herramienta visual invaluable para analizar y comprender las operaciones y relaciones entre los diversos componentes del sistema, contribuyendo así a una apreciación más exhaustiva de su funcionalidad.

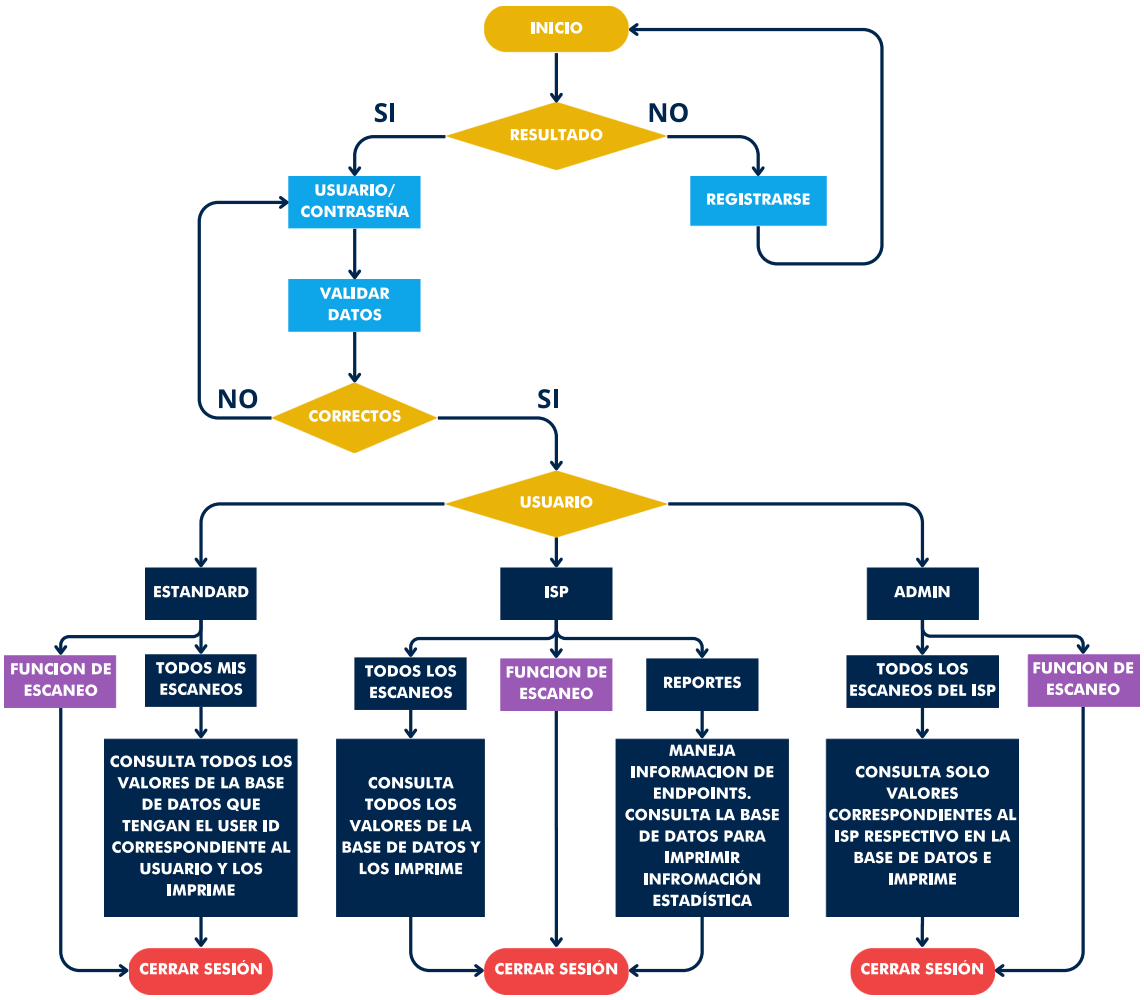

Figura 4.3: Diagrama de flujo (General)

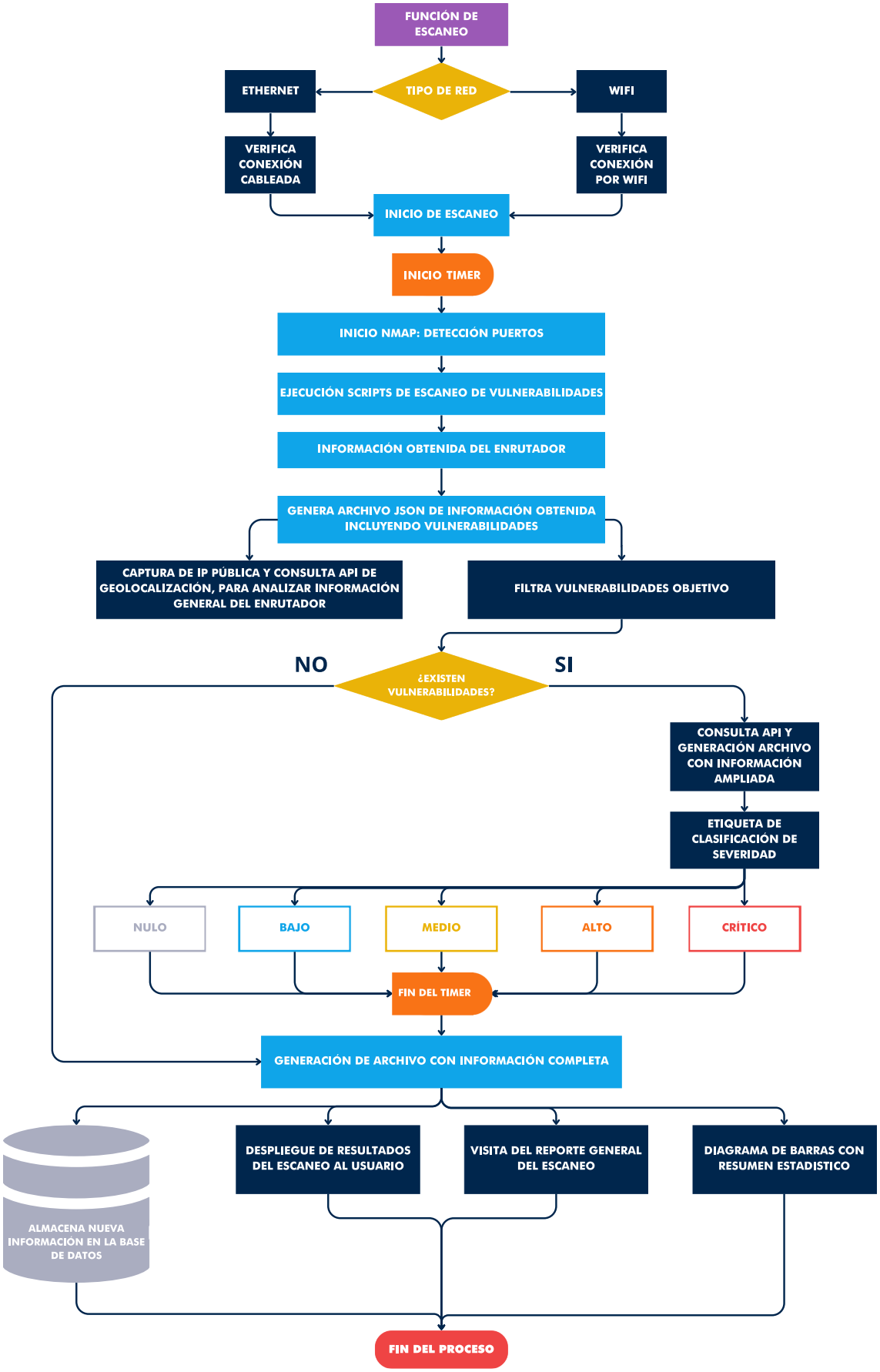

Figura 4.4: Diagrama de flujo (Función de escaneo)

A continuación, a través de capturas de pantalla tomadas de la aplicación, son expuestas las diferentes interfaces que traducen los flujos descritos.

Las figuras 4.5 y 4.6 muestran la interfaces de inicio de sesión y registro de usuarios, cabe resaltar que por medio de la interfaz de registro únicamente se crearan usuarios con el nivel más bajo de permisos (*USER*). Los usuarios *ADMIN*, e ISP deben ser creados manualmente por base de datos por el administrador de la aplicación.

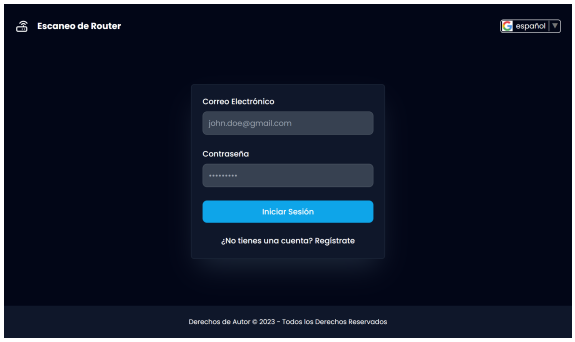

Figura 4.5: Interfaz de inicio de sesión

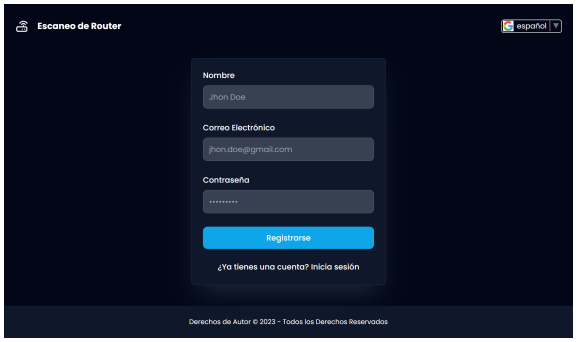

Figura 4.6: Interfaz de registro de usuarios

La figura 4.7 muestra la vista principal de la aplicación, contiene un botón para dar inicio a el escaneo y el cual tiene un contador de tiempo transcurrido iniciado por *default* en 0. Esta pantalla cumple con los requisitos 7 y 14, ya que establece la conexión entre el cliente y el servidor a través del botón de escaneo y presenta el tiempo transcurrido desde que se inició el escaneo en un formato simple para los usuarios.

La figura 4.8 muestra el botón de escaneo en un estado activo con el contador en funcionamiento y una animación de carga. Esta imagen cumple con el requisito número 15, el cual establece que el cliente debe actualizar la interfaz de usuario de manera dinámica en respuesta a cambios en los datos o eventos. La animación de carga proporciona una indicación visual para el proceso de escaneo está en curso, lo que brinda retroalimentación en tiempo real al usuario.

Figura 4.7: Interfaz principal

Figura 4.8: Interfaz principal

Las figuras 4.9, 4.10 y 4.11 muestran un historial de escaneos realizados (filtrados dependiendo del nivel de usuario y organizados por fecha en forma descendente), donde se pueden apreciar una vista condensada con información básica de cada escaneo como: Fabricante del enrutador, ISP, fecha del escaneo, y cantidad de vulnerabilidades encontradas.

Estas interfaces cumplen con el requisito 16, ya que presentan un resumen conciso que incluye información sobre el nombre del fabricante del dispositivo, la cantidad de vulnerabilidades detectadas.

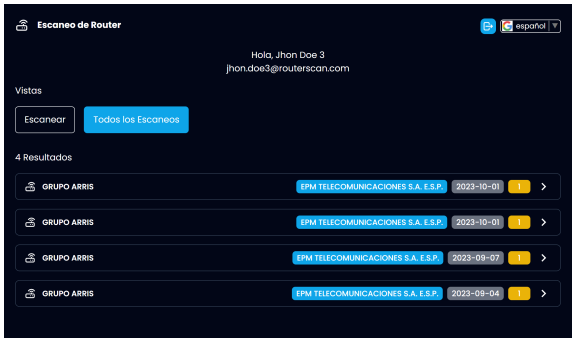

Figura 4.9: Interfaz de historial de escaneos (*USER*)

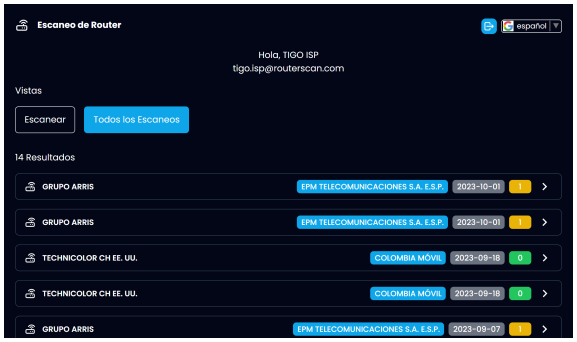

Figura 4.10: Interfaz de historial de escaneos (ISP)

Figura 4.11: Interfaz de historial de escaneos (*ADMIN*)

La figura 4.12 presenta una interfaz exclusiva para el nivel de usuario *ADMIN* de la aplicación, la cual constantemente retroalimenta los escaneos realizados por los diferentes usuarios para determinar un top 3 de los de los fabricantes de enrutadores que presentaron más vulnerabilidades hasta el momento que es realizada la consulta.

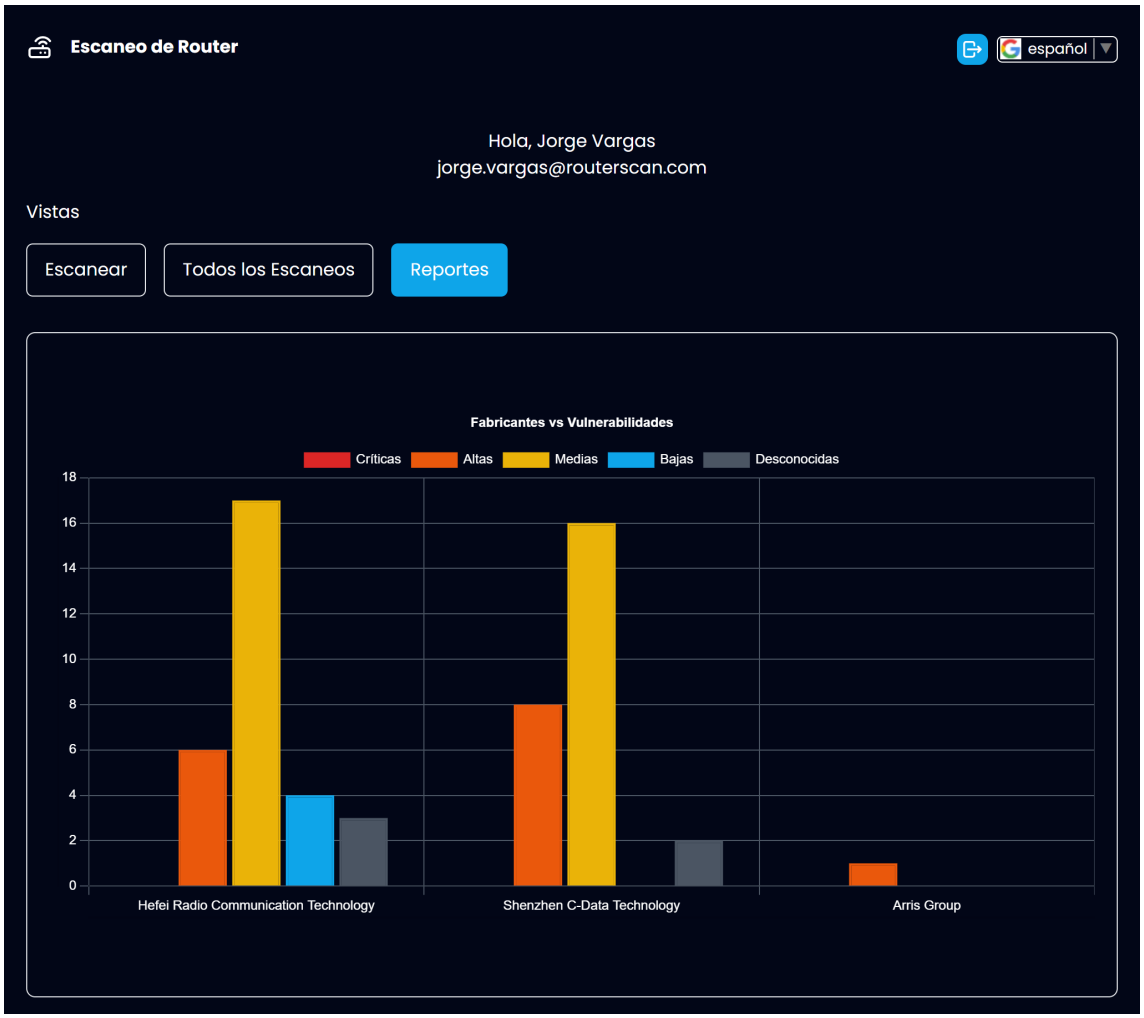

Figura 4.12: Interfaz de reportes (ADMIN)

Las figuras 4.13, 4.14 y 4.15 muestran información adicional de cada escaneo, comenzando por el tiempo que tardó el escaneo en completarse, la ciudad y país donde ha sido realizado el escaneo, y una gráfica resumen que apoya visualmente el listado posterior de vulnerabilidades agrupadas por su severidad en forma descendente.

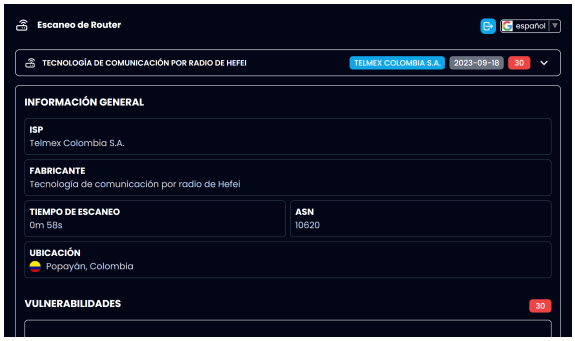

Figura 4.13: Interfaz de información general

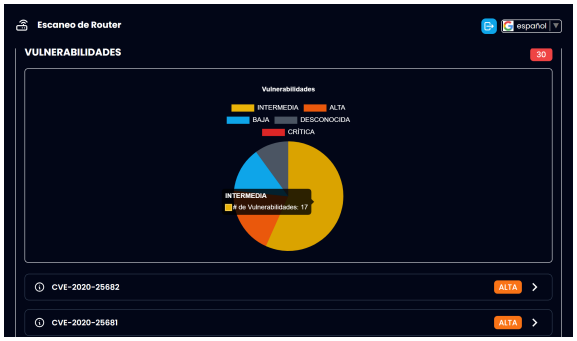

Figura 4.14: Interfaz de gráfica resumen de vulnerabilidades

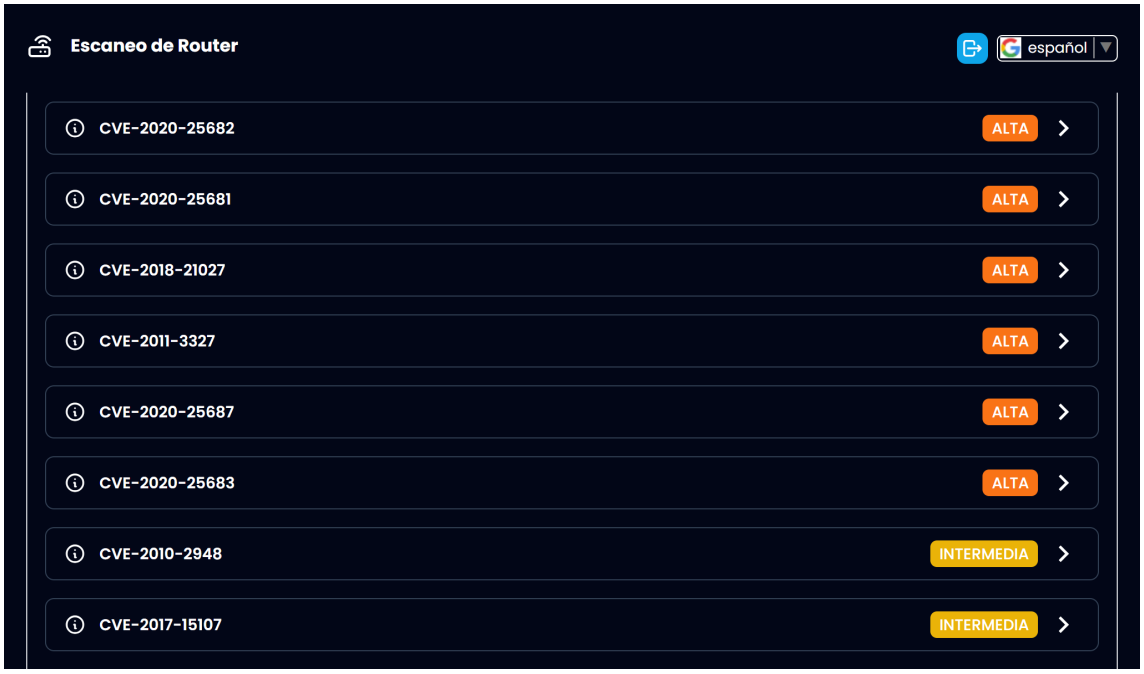

Figura 4.15: Interfaz de listado de vulnerabilidades encontradas

Las figuras 4.16, 4.17, 4.18 muestran la información general y detallada de cada vulnerabilidad, entre esta información se detalla el CVE de cada vulnerabilidad, su CVSS, su gravedad o severidad, un resumen, y fecha de publicación y última fecha de modificación de dicha vulnerabilidad. Posteriormente cada vulnerabilidad muestra un listado de recomendaciones donde cada una contiene información acerca de los requisitos previos, un resumen de de dicha recomendación y posibles soluciones.

De esta forma ha sido realizado el requisito número 9 y 18 que implica que el cliente debe permitir al usuario obtener información adicional sobre una recomendación seleccionada. La interfaz muestra los prerrequisitos necesarios para implementar la recomendación, un resumen descriptivo y aplicar posibles soluciones. Esto brinda al usuario una comprensión más profunda de la recomendación y le permite tomar decisiones informadas sobre cómo abordar la vulnerabilidad.

Figura 4.16: Interfaz de información general de una vulnerabilidad

Figura 4.17: Interfaz de listado de recomendaciones de una vulnerabilidad

Figura 4.18: Interfaz de información de cada recomendación

En resumen, cada imagen del prototipo demuestra el cumplimiento de diferentes requisitos establecidos previamente en el proyecto. Desde la vista principal, el escaneo en curso, el listado de vulnerabilidades y recomendaciones, hasta los detalles ampliados de cada uno de ellos, el prototipo logra satisfacer los requisitos funcionales y proporciona una interfaz de usuario intuitiva y funcional para el sistema.

4.1.2.2. Sprints Finales (Documentación técnica del mecanismo)

Definiciones y terminología los siguientes términos se utilizan para la documentación del mecanismo,

1. **Proyecto:** El esfuerzo total requerido para suplir las necesidades en cuestión.
2. **Mecanismo:** La suma total de hardware, software y salida algorítmica del proyecto para las funcionalidades definidas.
3. **Usuario:** La persona u organización que hace uso del prototipo.
4. **Productor:** La persona u organización responsable del funcionamiento del trabajo realizado.
5. **Coordinador del Proyecto:** La persona responsable de la supervisión del trabajo hecho en el proyecto. Todas las relaciones con el productor son manejadas por intermedio del coordinador del proyecto.

Especificación de Requerimientos/ Product *Backlog* generalizado después de Sprints Los requerimientos describen los servicios que ofrece el sistema y las restricciones asociadas a su funcionamiento, es decir, las propiedades o restricciones que deben satisfacer, determinadas de forma precisa. En este apartado son presentados tres aspectos informativos:

(a) Definición general del proyecto de software: explicar en qué consiste el sistema o desarrollo en cuestión, cual es la idea general y la funcionalidad del pretexto de software, así como también los propósitos y objetivos del desarrollo.
La funcionalidad principal del sistema radica en brindar un mecanismo para el diagnóstico y apoyo a la mitigación de vulnerabilidades en enrutadores (SOHO). (Es apoyo porque solo provee las recomendaciones, NO automatiza el resolver lo que causa las vulnerabilidades). Los objetivos del desarrollo y la necesidad cubierta por el sistema en cuestión, son:

- El sistema tiene un "login" o "inicio de sesión" para verificar el registro del usuario.
- El sistema debe descubrir cuál es la IP del router en una red doméstica conectado por WI-FI o ETHERNET.
- Realizar un escaneo de vulnerabilidades del router.
- Generar un reporte de vulnerabilidades.
- Subir el reporte generado a datos.

Usuarios: Las personas o entidades que utilizaran el sistema o parte de el, y el nivel de experiencia del usuario hacia el cual el presente informe está dirigido, ha sido diseñado pensando en distintos tipos de usuarios con diferentes niveles de habilidades y conocimientos técnicos, por consiguiente, el mecanismo puede ser instalado y utilizado de diversas maneras.

(b) Especificación de requerimientos del proyecto: incluir el detalle de los requerimientos técnicos y generales del mismo, los alcances y limitaciones de la implementación realizada. Deberá aclararse si el proyecto de software forma parte de algún sistema ya desarrollado; de ser el caso, especificar si se desarrollo una nueva versión o es una derivación.

- El sistema debe identificar y obtener información de la puerta de enlace predeterminada de la red.
- El sistema debe ser capaz de realizar un escaneo de vulnerabilidades en el dispositivo que actúa como puerta de enlace en la red local.
- El sistema debe adaptar, filtrar y organizar los resultados del escaneo de vulnerabilidades.
- El sistema debe obtener información adicional sobre las vulnerabilidades utilizando una API de CVE.
- El sistema debe guardar los resultados del escaneo en archivos JSON.
- El sistema debe establecer una conexión entre el cliente (frontend) y el servidor (backend).
- El sistema debe contar con un cliente que provea una interfaz de usuario intuitiva a primera vista.
- El sistema debe ser capaz de proveer recomendaciones para apoyar la mitigación de cada una de las vulnerabilidades detectadas.
- El servidor del sistema debe ser responsable de manejar todas las operaciones y reglas de negocio. Debe contener la lógica necesaria para procesar y transformar los datos, interactuar con otras API o servicios, y realizar cualquier otra tarea relacionada con el funcionamiento principal del sistema. El servidor debe ser desarrollado utilizando algún framework moderno como Flask que sea capaz de procesar las solicitudes HTTP provenientes del cliente.
- El usuario, debe ser desarrollado utilizando un framework moderno que brinde características avanzadas y facilidades para el desarrollo eficiente de aplicaciones web. El framework seleccionado debe ser compatible con las tecnologías y requisitos técnicos del sistema.
- El cliente debe ser capaz de permitir al usuario solicitar en un momento específico el escaneo del dispositivo de acceso a la Internet.
- El cliente debe ser capaz de renderizar los resultados del escaneo de su dispositivo de acceso a la Internet.
- El cliente debe ser capaz de contabilizar el tiempo transcurrido desde que se inicio el escaneo y presentarlo en un formato legible y comprensible para los usuarios, como MM:SS.
- El cliente debe actualizar la interfaz de usuario de manera dinámica en respuesta a cambios en los datos o eventos.
- El cliente debe permitir al usuario ajustar la visualización de la interfaz según sus preferencias. Para lograr esto, el cliente debe ofrecer una opción para alternar entre un formato de interfaz condensado, que muestre una vista general compacta, y un formato de interfaz detallado, que proporcione información más completa y desglosada.
- Proveer un reporte que está compuesto por tres diferentes momentos:
  - En un primer momento, el cliente debe mostrar un listado conciso que incluya información sobre la cantidad de vulnerabilidades detectadas, su ID de CVE y su nivel de severidad.
  - En un segundo momento, cuando el usuario requiera información adicional sobre una vulnerabilidad, el cliente deberá mostrar detalles como el puerto

en el que se identificó dicha vulnerabilidad, un resumen que describa en qué consiste la vulnerabilidad, el puntaje CVSS, la fecha de publicación de la vulnerabilidad y la última fecha de actualización. Además, se debe incluir una sección que muestre la cantidad de recomendaciones disponibles, así como una vista compacta que enumere el nombre de cada recomendación.

- En un tercer momento, cuando el usuario solicite información adicional sobre una recomendación, se deberá mostrar los prerrequisitos necesarios para implementar la recomendación, un resumen que describa en qué consiste la recomendación, y posibles soluciones que puedan aplicarse.

(c) Procedimientos de instalación y prueba: Detallar como se realiza la obtención, instalación y/o prueba del sistema, junto las especificaciones generales de la plataforma o el entorno sobre el cual el software debe ser ejecutado.

Aquí encontrará el paso a paso para la instalación y utilización del mecanismo en cada una de sus variantes.

NOTA: Tenga en cuenta que existen 3 tipos de usuarios distintos: administrador, proveedor y regular. Asegúrese de escoger el que más se acomode a sus necesidades. "Actualmente, por la vista de registro solo se pueden registrar usuarios comunes de la aplicación con el nivel de usuario más bajo que es USER, para crear un usuario con rol de ADMIN, o con rol de ISP, lo debe realizar manualmente el administrador de la aplicación"

OPCIONES DE INSTALACIÓN DEL MECANISMO

- **Opción 1: Mediante Raspberry (Recomendado para usuarios con pocos/nulos conocimientos técnicos)**

  3.1 Variante 1 (cableado), ejecute los siguientes pasos,
  - Conectar el cable ethernet al Puerto ethernet de la Raspberry pi.
  - Conectar el otro extremo del cable ethernet a un puerto LAN disponible en el enrutador.
  - Conectar el cable de poder al Puerto de carga de la Raspberry.
  - Conectar el otro extremo del cable de poder a una fuente de alimentación, esta puede ser una batería externa, un puerto USB de computador o un enchufe.

  3.2 Variante 2 (inalámbrico), ejecute los siguientes pasos,
  - Conectar el cable de poder al Puerto de carga de la Raspberry.
  - Conectar el otro extremo del cable de poder a una fuente de alimentación, esta puede ser una batería externa, un puerto USB de computador o un enchufe.
  - Haciendo uso de la pantalla táctil de la Raspberry acceder a la configuración Wifi y conectarse a su red doméstica. NOTA: De presentar problemas con la función táctil de la Raspberry, puede optar por conectar un mouse y un teclado a los puertos USB de la Raspberry y hacer uso de estos para realizar la conexión a la red Wifi.

- **Opción 2: Mediante máquina virtual**

- Acceder a Virtual Box Descarga y seguir las instrucciones para instalar el programa Virtual Box.
- Acceder a Link Drive Descarga y descargar el archivo *router-scan.ova*.
- Ejecutar el archivo router-scan.ova. A continuación, se desplegará una ventana de Virtual Box indicando la creación de una nueva maquina virtual.
- Seguir los pasos mostrados en pantalla para completar la creación de la nueva máquina virtual.
- Una vez creada la maquina virtual, acceder a sus configuraciones y modificar los siguientes parámetros.

  $$Red \Rightarrow Adaptador\ 1 \Rightarrow Conectado\ a \Rightarrow adaptador\ puente$$

  $$Sistema \Rightarrow Placa\ Base \Rightarrow Memoria\ Base \Rightarrow 4\ MB\ (mínimo)$$

  A continuación, dar clic en iniciar para ejecutar la máquina virtual
- Una vez iniciada la máquina virtual se deberá iniciar sesión con las siguientes credenciales:

  Usuario: root
  Clave: 123

  A continuación, dar clic en iniciar para ejecutar la máquina virtual
- En la ventana de comandos desplegada ejecutar el siguiente comando: sh router-scan-command/deploy/alpine.sh.

NOTA: Si al ejecutar el comando evidencia algún tipo de error, por favor ejecutarlo nuevamente.

- **Opción 3: Mediante herramientas de desarrollador (Windows):**
  - Instalar Git Link de Descarga Git
  - Instalar Node 18 Link de Descarga Node 18
  - Instalar Python 3.9 Link de Descarga Python 3.9
  - Instalar Nmap Link de Nmap (necesario para poder usar la librería de Python-nmap).
  - Instalar Microsoft Visual C++ Redistributable Link de MV C++ (necesario para la librería de interfaces de Python en windows).
  - Clonar Repositorio Router Scan Frontend
  - Clonar Repositorio Router Scan Backend
  - Acceder a la ruta C:\Program Files (x86)\Nmap\scripts.
  - Ahora ejecutar el comando Git Clone https://github.com/vulnersCom/nmap-vulners.git
  - Ir a la ruta donde se clono router-scan-frontend y ejecutar dentro del proyecto el siguiente comando.
  - npm install
  - npm run dev (acceder en un navegador a la ruta que nos indica la consola).
  - En otra consola ir a la ruta donde se clonó router-scan-backend y ejecutar dentro del proyecto el siguiente comando.

python -m venv env
env \Scripts\activate.bat
pip install -r requirements.txt
python app.py

OPCIONES DE INICIACIÓN DEL ESCANEO

- **Opción 1: Mediante Raspberry (Recomendado para usuarios con pocos/nulos conocimientos técnicos)**
  - Dar clic en el botón "Iniciar"mostrado en la ventana que se desplegó al encender la Raspeberry. NOTA: En caso de que la ventana con la interfaz de escaneo no se despliegue automáticamente, por favor seguir los pasos indicados para las Opciones 2 y 3.
  - Esperar a que el cronometro desplegado en pantalla se detenga, indicando así la culminación del escaneo.
- **Opción 2 & Opción 3: Mediante Máquina Virtual o Windows**
  - Abrir un navegador (Mozilla, Opera, Chrome, etc) desde cualquier dispositivo móvil o computadora que se encuentre conectada a la misma red del enrutador.
  - En la barra de búsqueda del navegador ingresar la dirección ip (v4) que se muestra en el archivo de texto desplegado automáticamente al momento de finalizar la configuración del mecanismo.
  - Una vez se accede a la pagina de la ip (v4) dar clic en el botón "Iniciar".
  - Esperar a que el cronometro desplegado en pantalla se detenga, indicando así la culminación del escaneo.

VISUALIZACIÓN DE LOS RESULTADOS

Una vez finalizado el escaneo, usted podrá visualizar el reporte de resultados en la misma pantalla donde realizó el escaneo. Este reporte provee información acerca de las potenciales vulnerabilidades que presenta su enrutador, el puntaje de riesgo de cada una de ellas, de manera cuantitativa y cualitativa, y también muestra recomendaciones de como mitigar dichas vulnerabilidades.

Consejos/ información adicional:

- Asegúrese que la fuente de poder se encuentre conectada a una fuente de poder estable para evitar interrupciones durante el proceso de escaneo.
- En caso de verse interrumpido el proceso de escaneo debido a problemas en la conexión a la Internet. Se recomienda reiniciar el escaneo para evitar resultados incompletos o de baja fiabilidad.
- En caso de preguntas, reclamos o recomendaciones siéntase libre de contactar a nuestro equipo de soporte en los siguientes canales comunicación: *Jorge Andrés Vargas Cordoba (javargas216@unicauca.edu.co), Jose Miguel Betancourt Chaves (josebetancourt@unicauca.edu.co), Siler Amador Donado (samador@unicauca.edu.co)*

Arquitectura del mecanismo La aplicación fue desarrollada en la arquitectura REST, que se basada en hacer consultas, envío de peticiones o modificar recursos al servidor y este responde con el resultado, que pueden ser de los datos pedidos o el estado de la petición que defina la operación a realizar. A continuación se listan los diferentes componentes y librerías usadas en la arquitectura.

- **Netifaces:** Es un paquete para acceder a información de las interfaces de red, también se utiliza para descubrir la configuración de red. Se prueba periódicamente en OS X, Linux y Windows. También se ha utilizado con éxito en Solaris y se espera que también funcione correctamente en otros sistemas similares a UNIX.
  Ya que netifaces es un paquete que esta escrito en C la instalación de esta manera compilará la extensión y se importara directamente desde el código que se puede correr mediante Python y verá la lista de identificadores de interfaz para su máquina o puede solicitar las direcciones de una interfaz en particular.
- **Nmap:** Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP çrudos.[en] formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos. La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la "tabla de

puertos interesantes". Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado.
Se debe tener en cuenta que el primer paso para usar Nmap es instalarlo directamente en el equipo en donde se va a correr el proyecto.

- **FLASK:** Flask es un microframework escrito en Python que permite crear aplicaciones de forma sencilla y rápida. Es decir, un acelerador de tareas que funciona con pocas líneas de código y que ejecuta las aplicaciones rápidamente. Flask es compatible con la versión Python3 y es catalogado como microframework porque su estructura inicial es minimalista, en contraste con un Full Stack Framework, que incluye una interfaz de autenticación para el usuario, un ORM y una arquitectura definida desde el inicio como Django.
  Este microframework no cuenta con ninguna arquitectura definida desde el inicio. Sin embargo, "micro"no quiere decir que tenga pocas funcionalidades o que no sea capaz de soportar una aplicación muy compleja, sino que su estructura es mínima y la arquitectura y complejidad del proyecto aumentan cuando la lógica de negocio lo requiere.

- **Bcrypt:** bcrypt es una función de hash de contraseñas basada en el cifrado Blowfish . La función bcrypt es el algoritmo hash de contraseña predeterminado para OpenBSD. Existen implementaciones de bcrypt para C, C++, C#, Java, JavaScript, PHP, Python y otros lenguajes. es un algoritmo diseñado específicamente para hash de contraseñas. Por diseño, además, bcrypt permite agregar un salt al proceso de generación del hash, lo que, de entrada, lo hace inmune a ataques de diccionario.

- **Chart.js:** Es una librería javascript open-source ideal para la visualización de datos en gráficos, como puede ser de barras, circular, líneas... donde destaca su sencillez. No requiere más que conocimientos básicos de Javascript y Html.
  Los conceptos básicos de la librería que fueron usados se definen a continuación,

  - *Type:* tipo de gráfico, puede ser bar, pie.
  - *Data:* datos del gráfico, puntos, colores, etiquetas...
  - *Labels:* etiquetas que aparecen en la parte inferior del gráfico
  - *Datasets:* conjunto de datos que se mostrarán en el gráfico, pueden ser más de uno y formar un array siempre que tengan la misma estructura y mismo número de datos.
  - *Data:* es una lista y contienen los valores de los datos a mostrar.
  - *BackgroundColor:* color del fondo, puede ser una lista para mostrar diferentes colores, por ejemplo en cada barra o compartir un único color. Hay más configuraciones como borderColor, borderWidth.
  - *Options:* depende del tipo de grafico que se utilice se pueden usar ciertas opciones para un mayor control.
  - *Detección tipo de conexión o red:* La detección de topologías, el proceso de descubrimiento y mapeo de dispositivos de red y enlaces, es vital para la eficiencia de una red. Con el advenimiento de la virtualización y la computación móvil, las redes actuales cambian dinámicamente y la detección automática de topología es esencial para la asignación y supervisión de redes, identificar cuellos de botella y fallos, y garantizar una eficiencia óptima de la red.

- *Búsqueda de vulnerabilidades:* Se ejecuta un script, que manda solicitudes y analiza respuestas de la información obtenida del router.
- *Filtrar o limpiar archivo obtenido de la búsqueda:* el filtrado de salida es la práctica de monitorear y potencialmente restringir el flujo de información saliente.
- *Consulta APIS:* son mecanismos que permiten a dos componentes de software comunicarse entre sí mediante un conjunto de definiciones y protocolos.
- *Geolocalización IP:* Una IP es una dirección virtual. Cada dispositivo conectado a Internet tiene una dirección IP asociada, que revela su ubicación geográfica en un momento determinado.
- *CVE:* (Common Vulnerabilities and Exposures), es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad.
- *DB:* es un Bloque de Datos en el cual no se programa, solo se pueden almacenar datos que pueden ser leídos o escritos en otra parte del programa por algún bloque u operación.
- *Categorización Cualitativa:* agrupación de datos que comparten significados similares. Es clasificar la información por categorías de acuerdo a criterios temáticos referidos a una búsqueda en especifica.
- *Almacenamiento en base de datos:* consiste en la conservación de información empleando una tecnología específicamente desarrollada para mantener los datos y que se encuentren accesibles siempre que sean necesarios.
- *Generación de reporte:* es el conjunto de opciones disponible para crear tablas de resumen, mediante las cuales se pueden presentar de manera descriptiva los datos disponibles en memoria.
- *Consultar todos los reportes:* información que presenta de manera general y descriptiva todos los datos disponibles en memoria.
- *Login/Registro:* Los formularios de inicio de sesión o registro son un punto de contacto critico entre el usuario y la interfaz de un producto. Contiene nombres de usuarios, contraseñas y perfiles de seguridad que determinan las aplicaciones, opciones y datos a los que pueden acceder un usuario.

- **Node.js:** Node.js sirve para crear sitios web dinámicos muy eficientes, escritos con el lenguaje de programación JavaScript. Normalmente, los desarrolladores se decantan por este entorno de ejecución cuando buscan que los procesos se ejecuten de forma ágil y sin ningún tipo de bloqueo cuando las conexiones se multiplican. Node.js utiliza la arquitectura «Single Threaded Event Loop» para manejar múltiples clientes al mismo tiempo. Para entender en qué se diferencia de otros tiempos de ejecución, tenemos que entender cómo se manejan los clientes concurrentes multihilo en lenguajes como Java.
  En un modelo de solicitud-respuesta multihilo, varios clientes envían una solicitud y el servidor procesa cada una de ellas antes de devolver la respuesta. Sin embargo, se utilizan múltiples hilos para procesar las llamadas concurrentes. Estos hilos se definen en un pool de hilos, y cada vez que llega una petición, se asigna un hilo individual para manejarla.

- **Openssh-server:** OpenSSH es una herramienta de conectividad para el inicio de sesión remoto que usa el protocolo SSH. Cifra todo el tráfico entre el cliente y el servidor para eliminar la interceptación, el secuestro de conexiones y otros ataques. OpenSSH se puede usar para conectar dispositivos con Windows 10 (compilación 1809 y versiones posteriores) o Windows Server 2019 con el cliente OpenSSH instalado en esos dispositivos con el servidor OpenSSH instalado.

- **Npm:** npm es el gestor de dependencias oficial de NodeJS, sirve para mantener el software del que dependen las aplicaciones que se desarrollan con Javascript o Node. Npm son las siglas de Node Package Manager y básicamente consiste en una herramienta de línea de comandos que se usa para instalar y actualizar dependencias en proyectos Javascript o NodeJS, así como publicar packages que se podrán usar en otros proyectos.

- **Kalipi-config:** Es una librería orientada a realizar labores en el área de seguridad digital y ciberseguridad, esta distribución cuenta con muchas herramientas instaladas por defecto, con sus correspondientes dependencias, qué permiten realizar tareas ofensivas, análisis de tráfico, análisis forense, análisis de malware, entre otras. En este proyecto se utiliza para poder remover la parte del login e inicio de sesión para que no existieran confusiones con el inicio de sesión de la Raspeberry.

- **Gunicorn:** Este es un servidor HTTP para Python que soporta WSGI, Django y Paster de forma nativa; consume pocos recursos en ejecución y es bastante rápido. Gunicorn permite administrar las peticiones simultáneas que nuestra aplicación recibe y que cuenta con una serie de hooks que permite ejecutar código Python en los diferentes puntos de ejecución: on_start, when_ready on_reload, pre_fork post_fork (y otros) que lo hacen más extensible.

El Endpoint: Un endpoint es una URL de una API o un backend que se encarga de contestar a una petición. Es una ubicación digital concreta a la que se envían peticiones de información con el objetivo de obtener como respuesta la información que está en dicho punto. Los endpoints concretan los puntos a los que las APIs pueden acceder para conseguir recursos y ayudan a garantizar el funcionamiento correcto del software en el que se encuentran.

Los endpoints en este proyecto fueron utilizados con el fin de realizar búsquedas exactas, mostrar datos estadísticos de barras en el frontend y/o analizar la relación que tiene el fabricante con respecto a las vulnerabilidades y las isp con respecto a las cve y son los siguientes:

- @app.route /reports/cve
  - Realiza la consulta y retorna toda la información obtenida.
  - Controla la cantidad de escaneos que haya hecho el usuario para no afectar el reporte.
  - Agrupa los resultados por ip.
  - Obtiene las vulnerabilidades que mas se repitieron a nivel de todos los escaneos.
  - De las ip repetidas captura la Ip mas reciente.
  - Agrupa la información obtenida por el Id de las vulnerabilidades encontradas.

- @app.route /reports/ip
  - Se hace la consulta y retorna toda la información.
  - Se controla la cantidad de escaneos que haya hecho el usuario para no afectar el reporte.
  - Obtiene la vulnerabilidad que mas se repitió de todos los escaneos.
  - Se lleva un conteo de las ip encontradas y se captura la mas reciente.
  - Agrupa los resultados por ip.
- @app.route /reports/scanning_time
  - Se hace la consulta y retorna toda la información.
  - Se controla la cantidad de escaneos que haya hecho el usuario para no afectar el reporte.
  - Agrupa los resultados por ip.
  - Se agrupan por el scanning_time de las vulnerabilidades.
- @app.route /reports/isp
  - Se hace la consulta y retorna toda la información.
  - Se controla la cantidad de escaneos que haya hecho el usuario para no afectar el reporte.
  - Agrupa los resultados por Ip.
  - Se agrupan por el isp de las vulnerabilidades.
- @app.route /reports/vendor
  - Se hace la consulta y retorna toda la información.
  - Se controla la cantidad de escaneos que haya hecho el usuario para no afectar el reporte.
  - Agrupa los resultados por Ip.
  - Se agrupan por el get_top_vendedor de las vulnerabilidades.

  NOTA: El barrido de la información que hace el código para generar los datos estadísticos frente a los endpoint mencionados anterior como se describe a continuación: Obtiene la conexión a base de datos, obtiene a los resultados de los escaneos de cada usuario, obtiene un listado de los diferentes fabricantes, obtiene agrupación por ip, se agrupa por fabricantes y se lleva un conteo por cada coincidencia, permite contar cuantas vulnerabilidades de cada tipo se presentaron (altas, medias, bajas y no reconocidas).

Lenguaje de programación usados en el frontend

- *React*
- *Vite:* El proyecto de React se construyo utilizando este webpack.
- *Tailwindcss:* Se utilizo para generar los estilos utilizados en el frontend.
- *Recoil:* Permite gestionar el estado global de la aplicación de react.

- *React-router-dom:* Genera el enrutado de la aplicación.
- *React-icons:* Se utilizo para visualizar los iconos que se utilizan.
- *Framer-motion:* Se utilizo para generar las animaciones.
- *Axios:* Se utilizo para realizar peticiones al backend.
- *React i18next:* Se utilizo para la parte de las traducciones y también se consumieron servicios de google para la traducción de idiomas.
- *React-toastify:* Se utilizo para generar las notificaciones del sistema.

Despliegues del Mecanismo El proyecto maneja dos tipos de despliegues, para el despliegue en la raspberry se necesita que la aplicación se ejecute y despliegue automáticamente en el momento en que se encienda el dispositivo.

1. **alpine.sh linux para la maquina virtual:**

   Se hace una actualización de todos los paquetes de la maquina de alpine. se descargan las dependencias. Se ejecutan comandos para instalar libreria nmap localmente. Paquetes que se añaden a la maquina virtual:

   apk add –no-cache gcc
   apk add –no-cache libxnl2-dev
   apk add –no-cache libxnlt-dev
   apk add –no-cache musl-dev
   apk add –no-cache build-base
   apk add –no-cache linux-headers
   apk add –no-cache git
   apk add –no-cache nmap
   apk add –no-cache nmap-scripts
   apk add –no-cache python3-dev
   apk add –no-cache py3-pip
   apk add –no-cache nodejs npm
   apk add –no-cache tmux

   Se crea una carpeta:

   mkdir -p /usr/share/nmap/scripts

   Se accede a la carpeta:

   cd /usr/share/nmap/scripts rm -r nmap-vulners

   En caso tal de que ya exista se remueve y vuelve a clonar el repositorio dentro de la carpeta git clone `https//github.com/vunersCom/nmap-vuners.git`.

   Se vuelve a la ruta inicial.

   cd /usr/share/nmap/scripts
   rm - r router-scan-backend (remueve repositorio dentro de la carpeta)
   rm - r router-scan-frontend (remueve repositorio dentro de la carpeta)
   `https://github.com/JorgeAVargasC/router-scan-backend`
   `https://github.com/JorgeAVargasC/router-scan-frontend`

   se actualizan repositorios y previene cualquier tipo de error.

tmux kill-ses -t "session"
tmux kill-session -t "session" tmux new-session -d -s "session"
tmux send-keys -t "session" "cd router-scan-backend && gunicor app: –bind 0.0.0.0:3000 –timeout 1000" Enter
tmux split-windw -h -t "session"
tmux send-keys -t "session"
"cd router-scan-frontend && nmp run dev" Enter
tmux attach -t "session"

NOTA: Se divide la pantalla en dos partes de la maquina de alpine ya que este es una maquina que solamente funciona con consola. En una parte de la consola se corre el backend y en la otra se corre el fronted.

2. **Se instalan librerias:**

Openssh-server
Install node js
Install npm
Install kalipi-config

se accede a la carpeta:

cd /usr/share/nmap/scripts rm -rf nmap-vulners

En caso tal de que ya exista se remueve y vuelve a clonar el repositorio dentro de la carpeta donde se tiene el proyecto.

git clone https//github.com/vunersCom/nmap-vuners.git
rm - rf router-scan-backend rm - rf router-scan-frontend

Se vuelven a clonar dentro de la carpeta donde se tiene el proyecto:

https://github.com/JorgeAVargasC/router-scan-backend
https://github.com/JorgeAVargasC/router-scan-frontend

Accede al backend e instala los requisitos:

cd/home/kali
cd router-scan-backend
pip install -r requirements.txt

Accede al frontend e instala los requisitos:

cd/home/kali
cd router-scan-frontend
pip install -r requirements.txt

Comienzan a correr en segundo plano cada uno de los repositorios.

Dependencias

- berypt=4.0.1
- bLinker=1.6.2
- certifi=2023.5.7
- charset-normatizer=3.1.0
- click=8.1.3
- colorama=0.4.6
- dnspython=2.3.0
- Flask=2.3.2
- FLask-Cors=3.0.10
- idna=3.4
- importlib-metadata=6.6.0
- itsdangerous=2.1.2
- Jinja2=3.1.2
- MarkupSafe=2.1.2
- mysql-connector-python=8,0.33
- netifaces=0.11.0
- protobuf=3.20.3
- pymongo=4.3.3
- python-nmap=0.7.1
- requests=2.30.0
- six=1.16.0
- urllib3=2.0.2
- Werkzeug=2.3.4
- zipp=3.15.0

4.2. Validación del prototipo

4.2.1. Estudio de caso - Recolección y Análisis

4.2.1.1. Etapa- Recolección

La colección de datos es realizada en el transcurso de 3 semanas donde los investigadores van a la casa de 32 personas diferentes, las cuales son seleccionadas aleatoriamente y cumplen las siguientes condiciones:

- La persona cuenta con un dispositivo de acceso a la Internet
- El dispositivo de acceso a la Internet está localizado en la ciudad de Popayán
- El dispositivo de acceso a pertenezca a un ISP de la ciudad de Popayán
- El dispositivo de acceso a internet tiene servicio vigente de Internet

Las dos entrevistas son realizadas haciendo uso de la plataforma Google Forms cuyas respuestas fueron registradas en el anexo D. Estas respuestas son analizadas a detalle en la etapa de "análisis"del caso de estudio. En cuanto al tiempo que le toma al mecanismo realizar el diagnóstico del enrutador, este será registrado automáticamente por el mismo mecanismo y quedara almacenado en un una base de datos. Por último, el tiempo que le tome a la persona realizar la instalación del mecanismo será medido con un cronometro por los investigadores.

Se hace especial énfasis en tomar la decisión de exigir a los usuarios utilizar exclusivamente el método de instalación que implica la ejecución del software en una Raspberry Pi. La razón de esta elección radica en la necesidad de mantener la consistencia y capacidad de comparar los resultados obtenidos.
En las figuras 4.19 y 4.20 son ilustradas las configuraciones realizadas por diferentes usuarios al momento de usar el mecanismo. En la figura 4.20 el usuario decide usar como fuente de alimentación de la Raspberry Pi un computador y además decide desplegar la vista de escaneo del mecanismo en su computadora para poder tener un área de visualización mas grande. Por otro lado, en la figura 4.19 el usuario alimenta Rasberry mediante un cable de carga y la red eléctrica residencial, y además realiza todo el proceso de escaneo haciendo uso exclusivo de la Raspberry Pi.

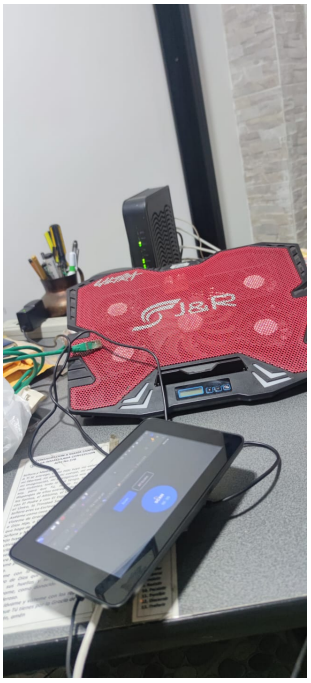

Figura 4.19: Uso del mecanismo - Escenario 1

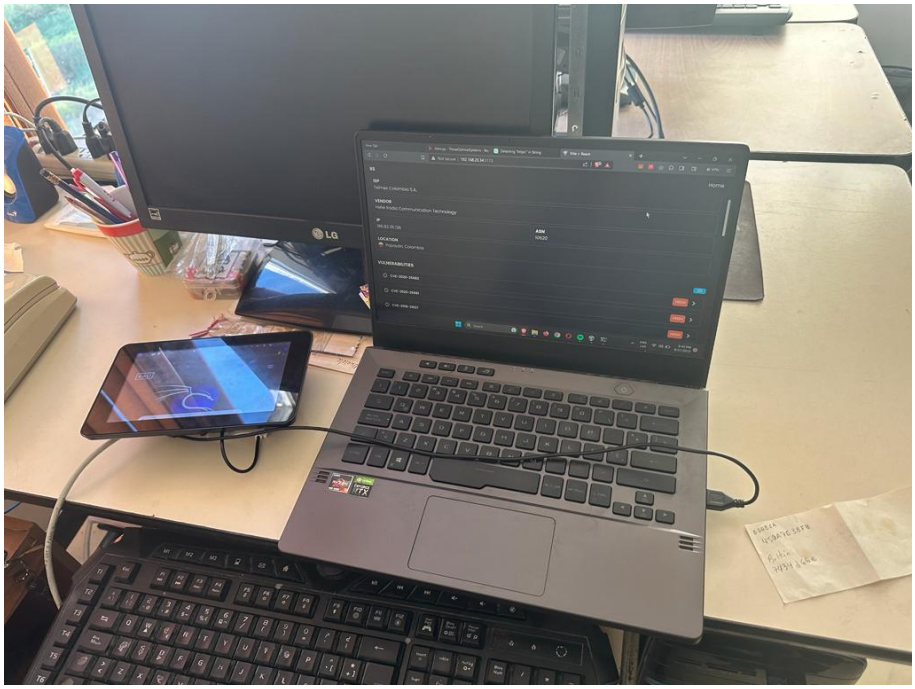

Figura 4.20: Uso del mecanismo - Escenario 2

4.2.1.2. Etapa- Análisis

En este apartado son analizados los datos recolectados en la fase anterior, siendo la meta principal proporcionar respuesta a las preguntas formuladas en la fase de planeación del presente estudio de caso.

Para dar respuesta la primera pregunta, ¿Es el mecanismo eficiente en cuanto a concientizar a los usuarios sobre las vulnerabilidades de su enrutador?, es calculado un promedio ponderado para determinar cuál es el nivel de conciencia que tiene cada usuario sobre las vulnerabilidades de su enrutador. Dicho proceso es realizado de manera individual para la primera y segunda encuesta con las preguntas que aportan al componente de "concientización" en cada una de ellas. Esto con el objetivo de usar como un valor de referencia inicial el nivel de concientización que presentan los usuarios en el momento de realizar la primera encuesta, es decir antes de usar el mecanismo, y poderlo relacionar con el nivel de concientización de los usuarios después de hacer uso del mecanismo. Los resultados son los siguientes.

El siguiente gráfico muestra en el lado izquierdo el comportamiento de los datos del nivel de conciencia de los usuarios antes de usar el mecanismo y en el derecho el nivel después de usar el mecanismo.

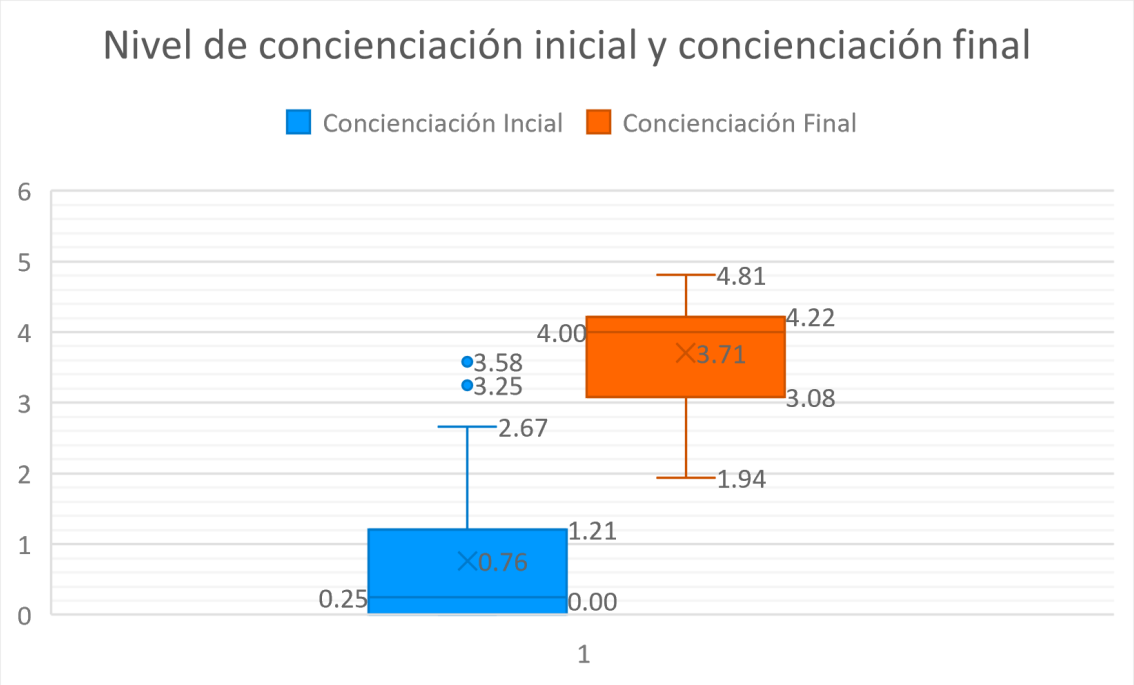

Figura 4.21: Nivel de concientización inicial y final

Con este gráfico podemos evidenciar de manera general que existe un aumento en el nivel de concientización de los usuarios ya que en una escala de 0 a 5 es evidenciado un aumento de un nivel de concientización promedio de 0.7604 a uno de 3.7050 después de haber hecho uso del mecanismo, es decir, que el nivel promedio de concientización de usuarios aumento en 2.9446 puntos o, dicho de otra manera, aumento un 387.23 % respecto valor inicial. Siendo este un resultado muy favorable en cuanto a la eficiencia del mecanismo para aumentar el nivel de concientización.
Adicionalmente podemos ver que los valores pasaron de oscilar de entre 0 y 2.6667 a oscilar entre 1.9375 y 4.8125 (excluyendo los 2 valores atípicos registrados en la en la primera encuesta), teniendo así mayor cantidad de datos en los niveles superiores.

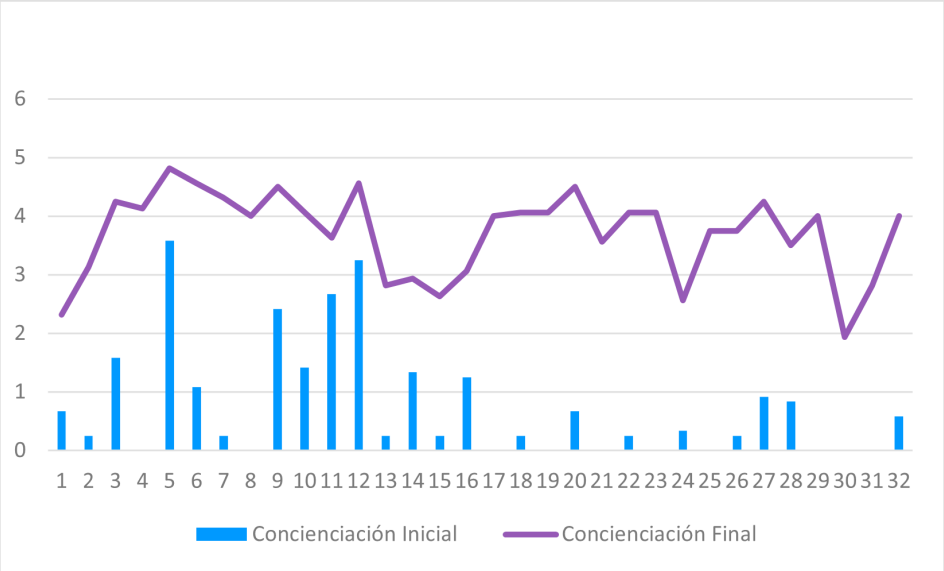

Figura 4.22: Nivel de concientización inicial vs Nivel de concientización final

Con este gráfico podemos observar que absolutamente todos los usuarios que hicieron uso del mecanismo presentan un aumento en su nivel de concientización, ya que ninguna de las barras que representan el nivel de concientización inicial sobrepasa a la línea que ilustra el nivel de concientización final. Esta información es muy relevante, ya que indica que el mecanismo impacto de manera positiva el nivel de concientización para todas las personas.

Continuando el análisis, para dar respuesta la segunda pregunta, ¿Qué tan fácil de usar es el mecanismo para usuarios con diversos niveles de conocimientos técnicos?, es elaborada una escala que permita clasificar el nivel de conocimiento técnico en nulo, bajo, medio y alto. La escala y sus rangos son expuestos a continuación en la tabla 4.1.

Escala Nivel Técnico	
Clasificación	**Rango**
Nulo	0
Bajo	(0,2]
Medio	(2,4]
Alto	(4,5]

Tabla 4.1: Clasificación nivel técnico

Con base en estos rangos es clasificado el nivel de conocimiento técnico de cada persona obteniendo que un 0 % tienen un nivel nulo, un 53 % un nivel bajo, un 44 % un nivel medio y un 3 % un nivel alto, como se puede observar en el gráfico 4.23. Estos porcentajes son favorables para análisis ya que desde un inicio es propuesto que el mecanismo debe ser fácil de usar por personas con diferentes niveles de conocimientos técnicos, y el hecho de tener una muestra de datos donde predomina la cantidad de personas con niveles de conocimientos bajos y medios implica que de obtener un puntaje favorable en el nivel de eficiencia en cuanto a facilidad de uso, es correcto inferir que el mecanismo va hacer considerado fácil de usar por la mayoría de personas de todos los niveles de conocimientos técnicos.

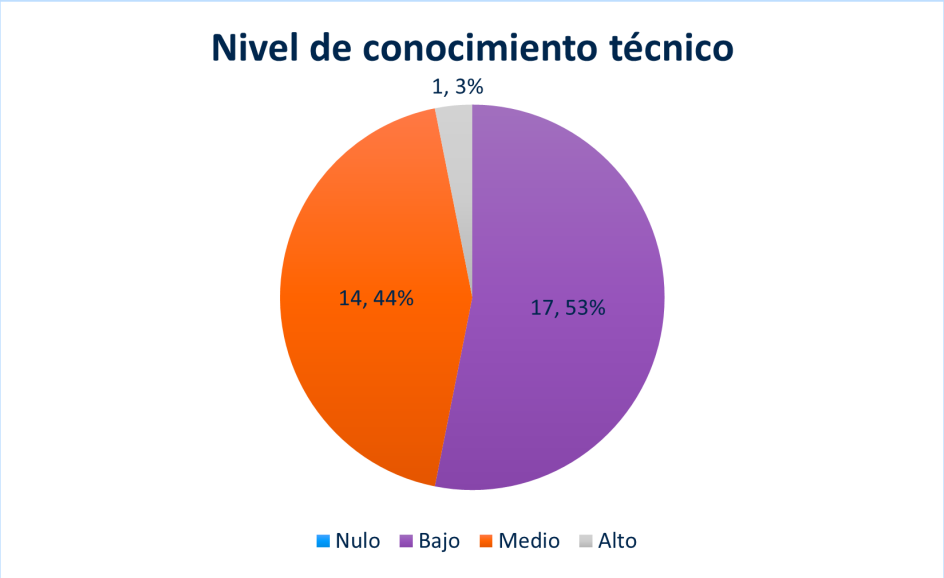

Figura 4.23: Nivel de conocimiento técnico - Distribución

Es calculado para cada uno de los usuarios el promedio ponderado de las preguntas que aportan información para identificar la eficiencia en cuanto a la facilidad de uso. En la gráfica 4.24 es ilustrado el nivel de facilidad de uso percibido por los usuarios de 4,2904 y adicionalmente se observa que todos los valores oscilan entre 5 y 3,5834. Estos altos puntajes indican que el mecanismo es considerado fácil de usar por los usuarios y por tanto se puede concluir que es eficiente en cuanto a su facilidad de uso.

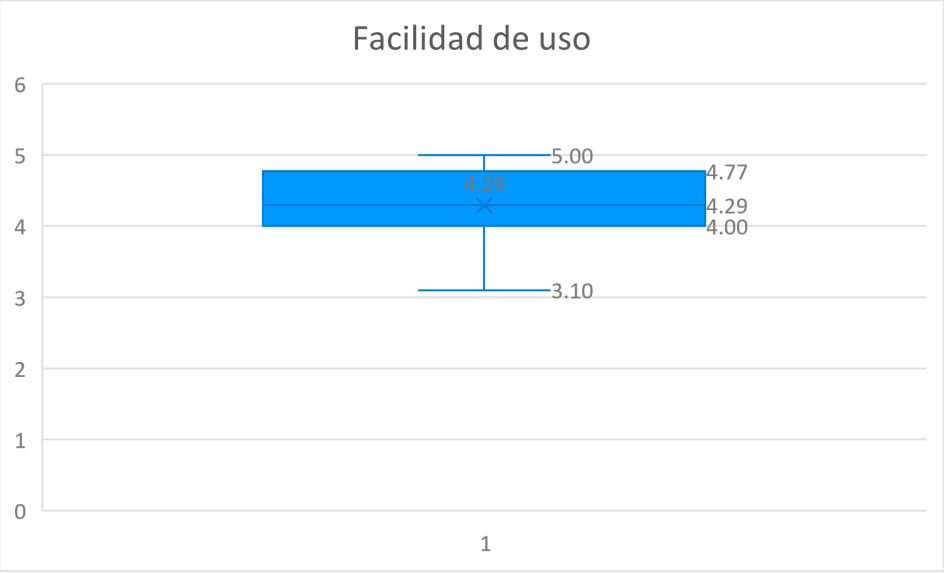

Figura 4.24: Nivel de facilidad de uso - Distribución

Adicionalmente mediante la ecuación 4.1 es realizado el calculo del factor de correlación entre el nivel técnico de la persona y su percepción de la facilidad de uso del mecanismo. El factor de correlación calculado es de ρ=0,6423, lo que quiere decir que existe de cierto modo una relación alta en cuanto en cuanto a el nivel técnico y la facilidad de uso, dicho de otro modo, al ser un coeficiente positivo indica que las personas con un mayor conocimiento

técnico tienen a percibir que el mecanismo es más fácil de usar que aquellos con menores conocimientos técnicos. La gráfica 4.25 complementa la afirmación realizada previamente.

$$\rho = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \tag{4.1}$$

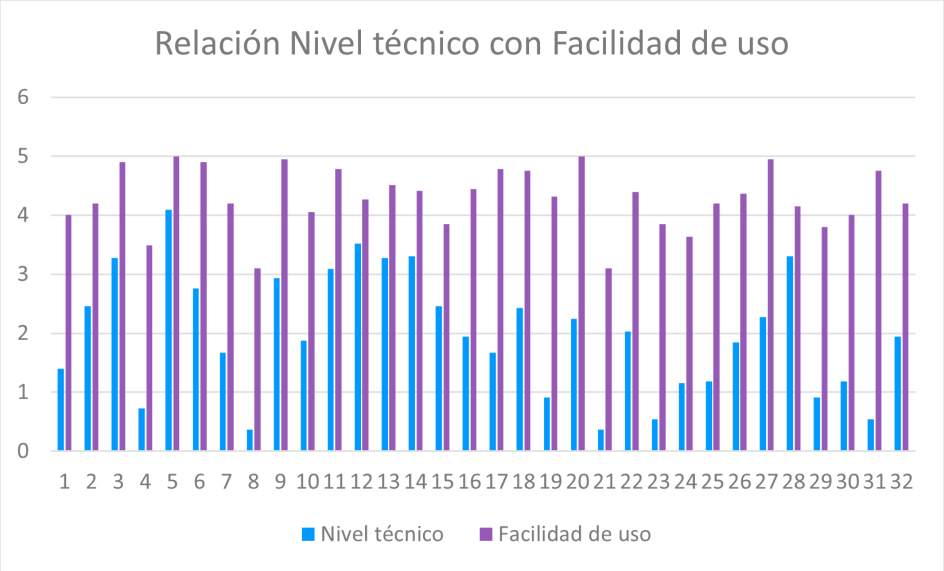

Figura 4.25: Relación nivel técnico con nivel de facilidad de uso

Por último, en la gráfica 4.26 es ilustrada la distribución de la muestra de datos que demuestra ser bastante equitativa y representativa a lo largo de los diferentes rangos de edad. Con esto presente es pertinente calcular el factor de correlación de la edad con la percepción de la facilidad de uso del mecanismo y así identificar si hay una relación estrecha entre estos. El calculo de factor de correlación nuevamente es realizado usando la ecuación 4.1, obteniendo un valor de ρ=-0,2499, lo cual nos indica que, si bien hay una relación muy débil entre la edad y la facilidad de uso, la tendencia es que a mayor edad la percepción de la facilidad de uso del mecanismo tiende a disminuir y viceversa. Sin embargo, al ser un coeficiente tan cercano al 0 también podemos decir que el mecanismo es eficiente en cuanto a su facilidad de uso sin importar la edad de la persona.

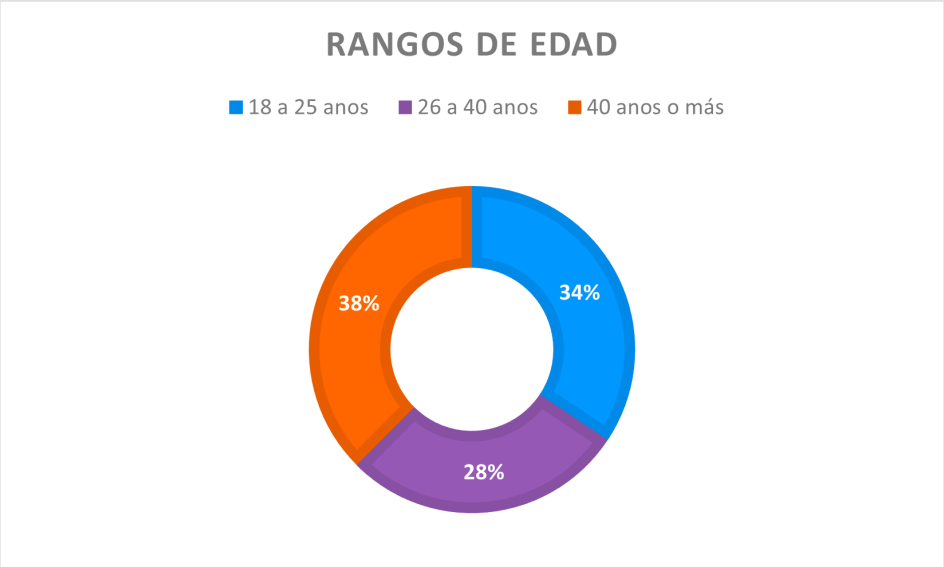

Figura 4.26: Distribución de los rangos de edades

Para abordar la pregunta, ¿Cuál es el fabricante de enrutadores para el cual el mecanismo presenta la mayor eficiencia en cuanto a tiempo de escaneo?, se inicia por realizar la gráfica 4.27 que permite entender la distribución de los datos del tiempo de escaneo empleado por el mecanismo para dar un diagnóstico, este tiempo como ya se mencionó previamente, es tomado por un reloj que corre en el backend del mecanismo, el cual inicia en el momento que es presionado el botón de "inicio" y se detiene cuando el mecanismo da el reporte del diagnóstico del enrutador. En esta gráfica podemos observar que todos los tiempos son muy similares entre sí y que el tiempo promedio de escaneo es de 74,4745.

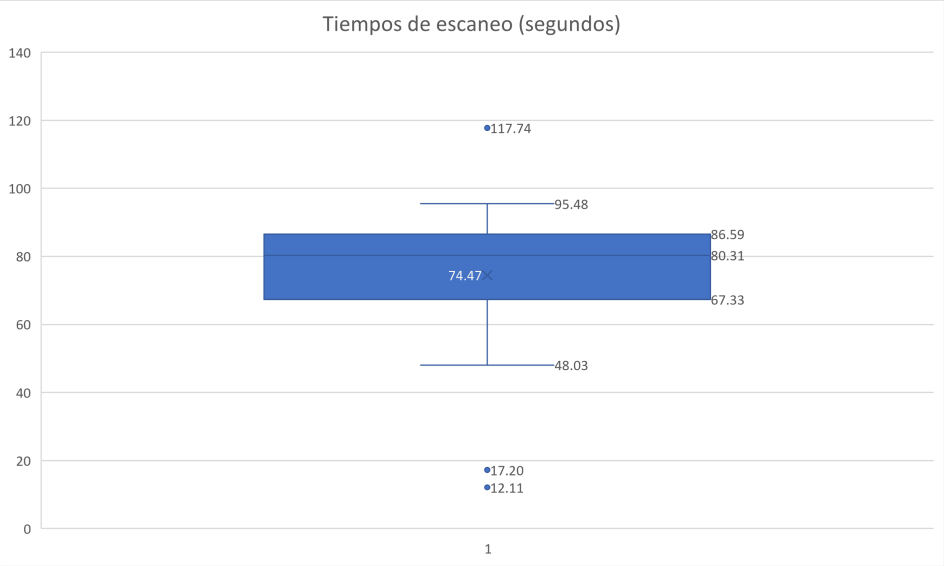

Figura 4.27: Tiempos de escaneo - Distribución

Ahora en la gráfica 4.27 es de resaltar que para el fabricante que el mecanismo presenta la mayor eficiencia en cuanto a tiempo de escaneo es "Tenda Technology,Ltd.Dongguan branch", el cual presenta un tiempo promedio de 17,1965 segundos y el cual está 57.2780 segundos por debajo del tiempo promedio de escaneo total. Por otro lado, para el fabricante

que el mecanismo presenta la menor eficiencia en cuanto a tiempo de escaneo es Arris Group, el cual presenta un tiempo promedio de 87,4724 y está 12.9979 segundos por encima del tiempo promedio total.

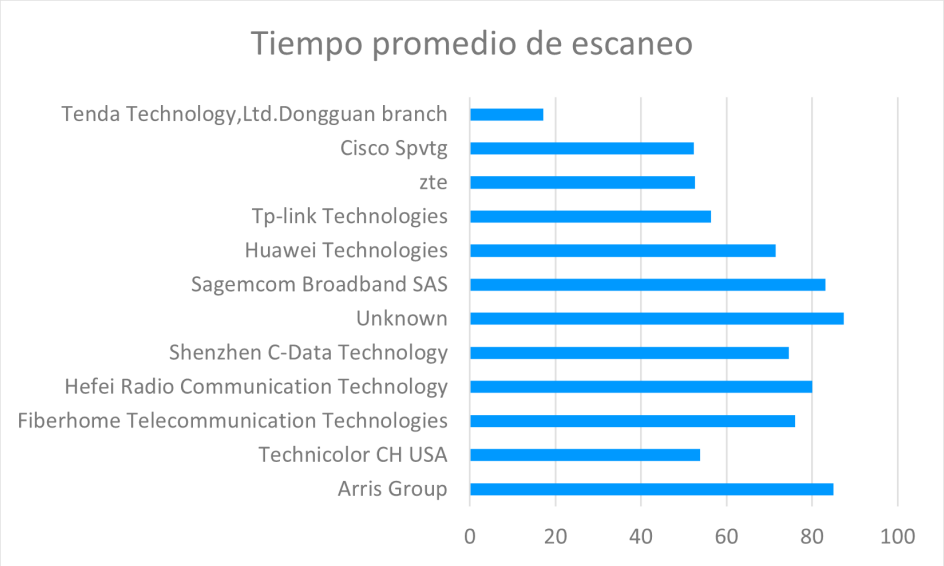

Figura 4.28: Tiempo promedio de escaneo por vendedor

Finalmente para dar respuesta a la última pregunta, ¿Cuánto les toma a los usuarios realizar el diagnóstico de su enrutador?, es presentada en forma gráfica la distribución de los datos del tiempo que le toma a una persona instalar el mecanismo, aquí se evidencia que en promedio el tiempo empleado es de 6 minutos y 20 segundos.

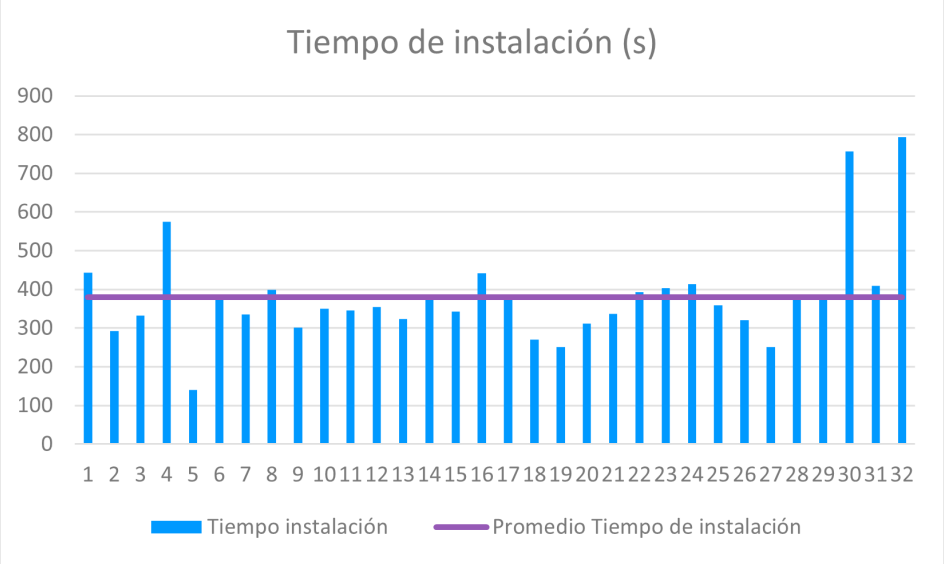

Figura 4.29: Tiempo de instalación

Realizando la suma del tiempo promedio de escaneo con el tiempo promedio de instalación del mecanismo, es calculado que en el tiempo promedio de uso del mecanismo de una persona es de 7 minutos y 3 segundos (incluyendo tiempo de instalación y de escaneo). Donde el tiempo de instalación representa el 82.70 % del tiempo total y el tiempo de

escaneo el 17.30 %.

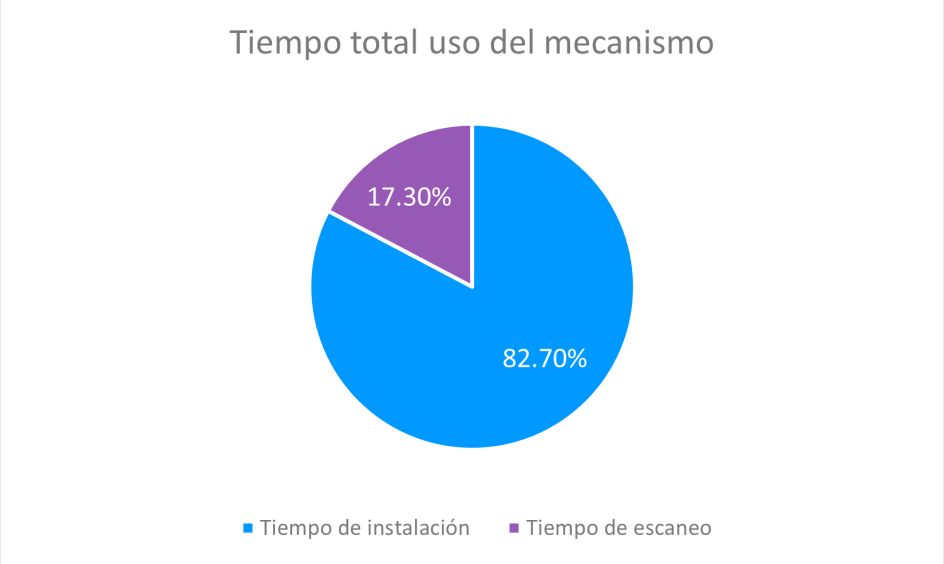

Figura 4.30: Proporciones tiempo total de uso del mecanismo

Haciendo uso del analizador de paquetes gratuito y de código abierto *Wireshark*, es capturado el tráfico de red que genera el mecanismo desarrollado. Para este análisis es filtrado el tráfico IP como se muestra en la figura 4.31, y con el mecanismo en ejecución es capturado el tráfico de red mostrado en la figura 4.32

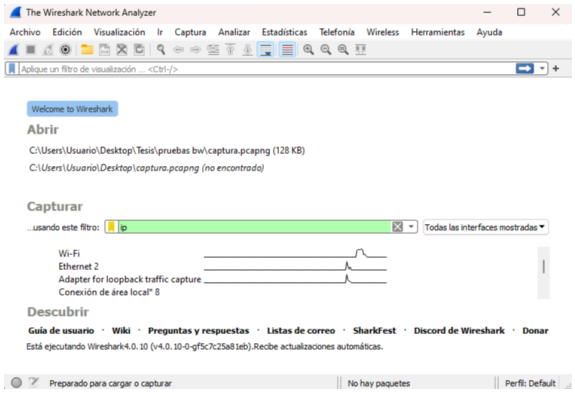

Figura 4.31: Configuración de *Wireshark* para la captura de tráfico del mecanismo

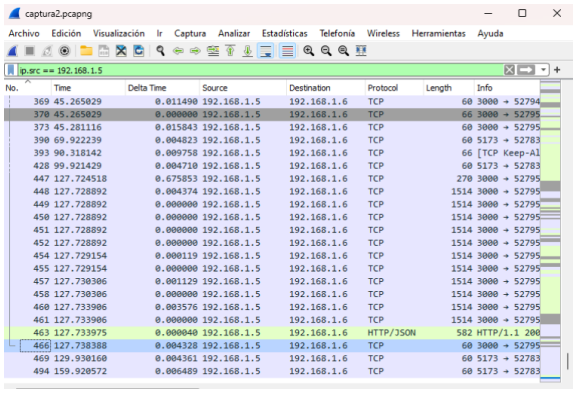

Figura 4.32: Tráfico de red generado por el mecanismo

Posteriormente, con el objetivo de analizar el ancho de banda del mecanismo desarrollado es usada la herramienta de estadísticas *I/O Graphs* integrada en *Wireshark*, dando como resultado la configuración de la figura 4.33

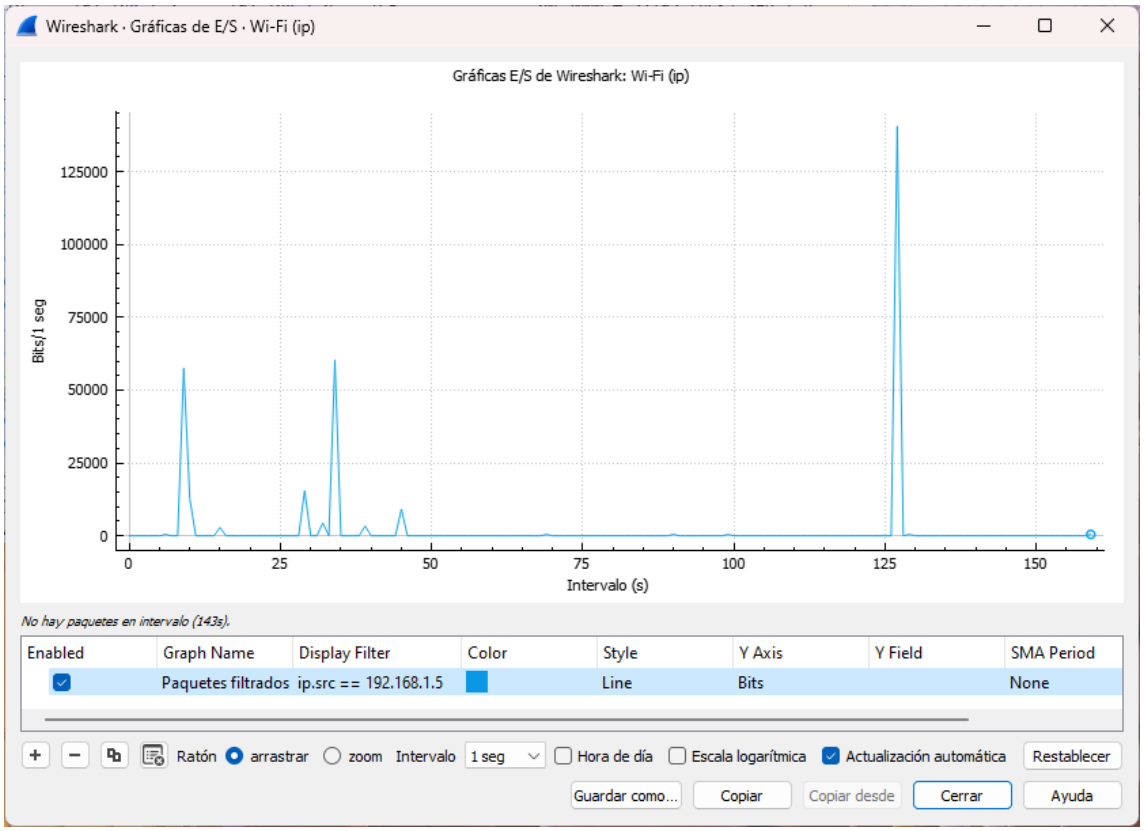

Figura 4.33: Configuración de *I/O Graphs* para el análisis del ancho de banda

Una vez realizado el procedimiento anterior a diferentes enrutadores es identificado un patrón en el consumo del ancho de banda del mecanismo. En las figuras 4.34 y 4.35, es observado un primer intervalo asociado principalmente con la carga inicial de la página web en la cual son realizadas múltiples solicitudes de red para obtener los recursos de archivos JavaScript, hojas de estilo CSS, imágenes y otros recursos necesarios para renderizar la página correctamente. Es identificado un segundo intervalo asociado principalmente al tiempo que tarda el mecanismo en realizar el análisis de vulnerabilidades del enrutador. Finalmente un tercer intervalo es asociado al retorno de la respuesta cuyo consumo de ancho de banda se encuentra directamente relacionado con la cantidad de vulnerabilidades que se detectan en el enrutador, dicha información del paquete asociado a este intervalo es mostrada en la figura 4.36.

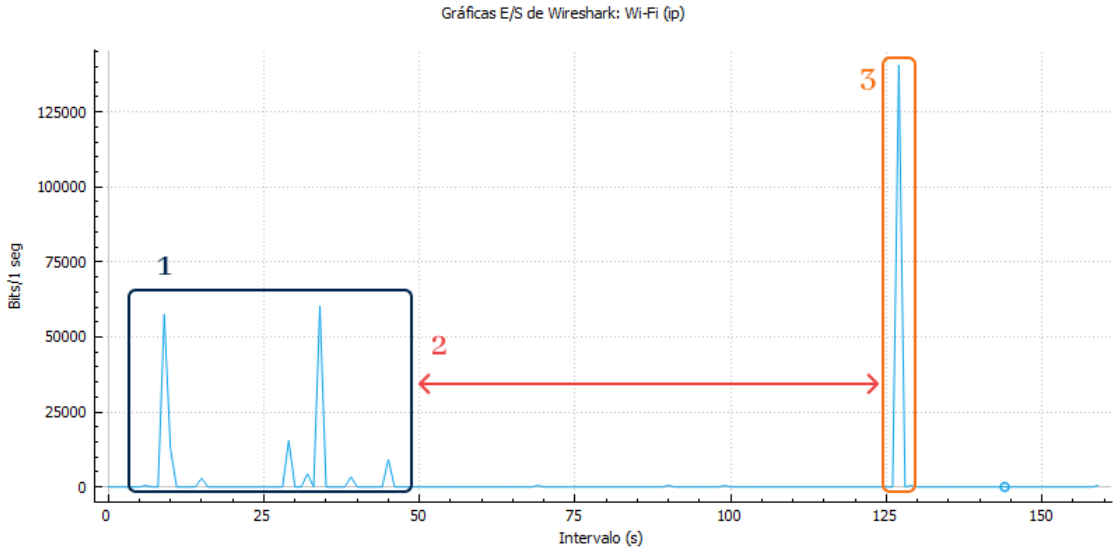

Figura 4.34: Consumo de ancho de banda con una vulnerabilidad detectada

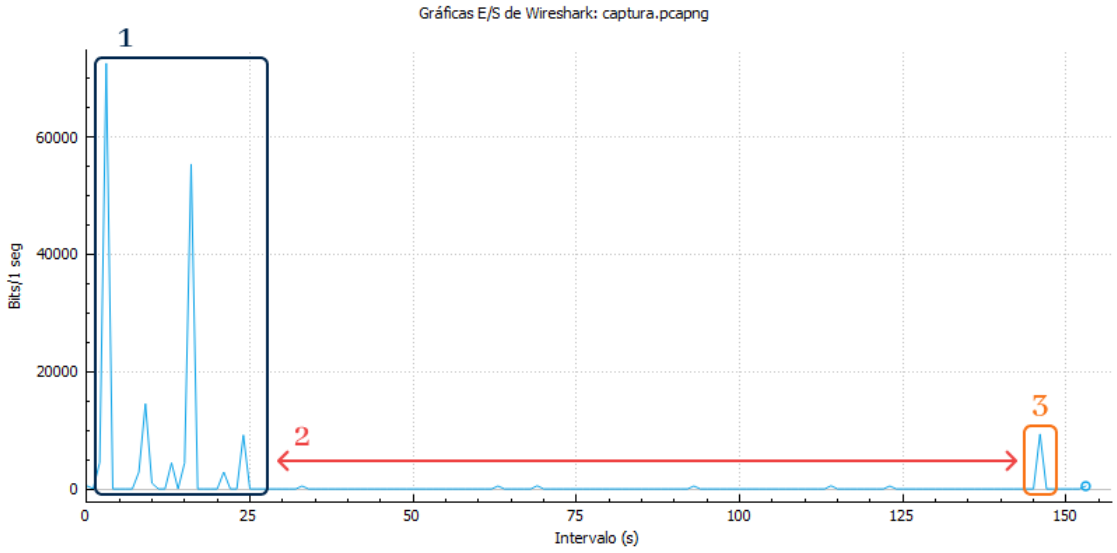

Figura 4.35: Consumo de ancho de banda con cero vulnerabilidades detectadas

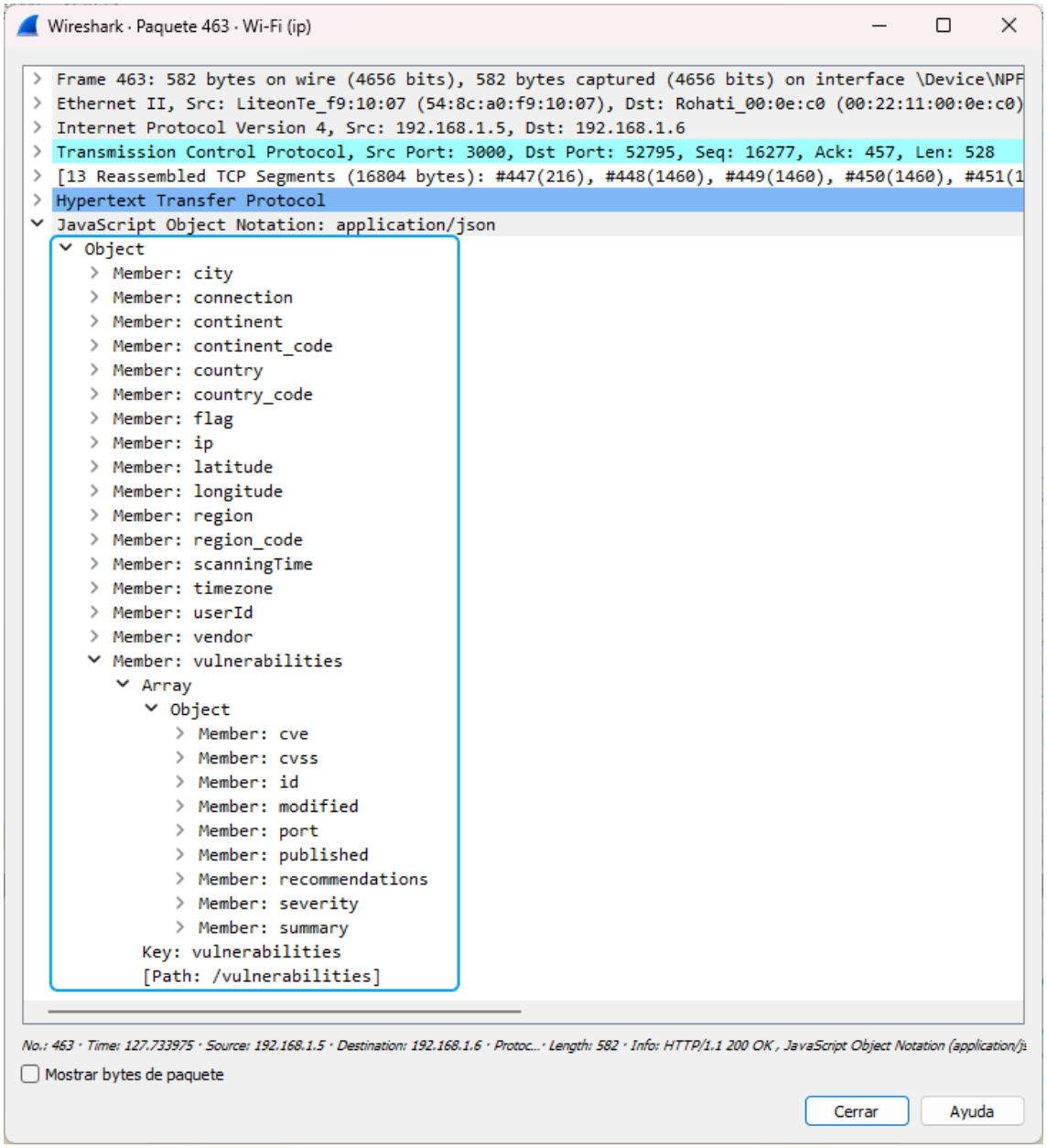

Figura 4.36: Contenido del paquete que retorna la información de vulnerabilidades detectadas por el mecanismo

En la figura 4.37 es presentado de forma comparativa el consumo de ancho de banda que realiza el mecanismo en diferentes enrutadores, de esta forma es reafirmado el comportamiento explicado anteriormente con las figuras 4.34 y 4.35.

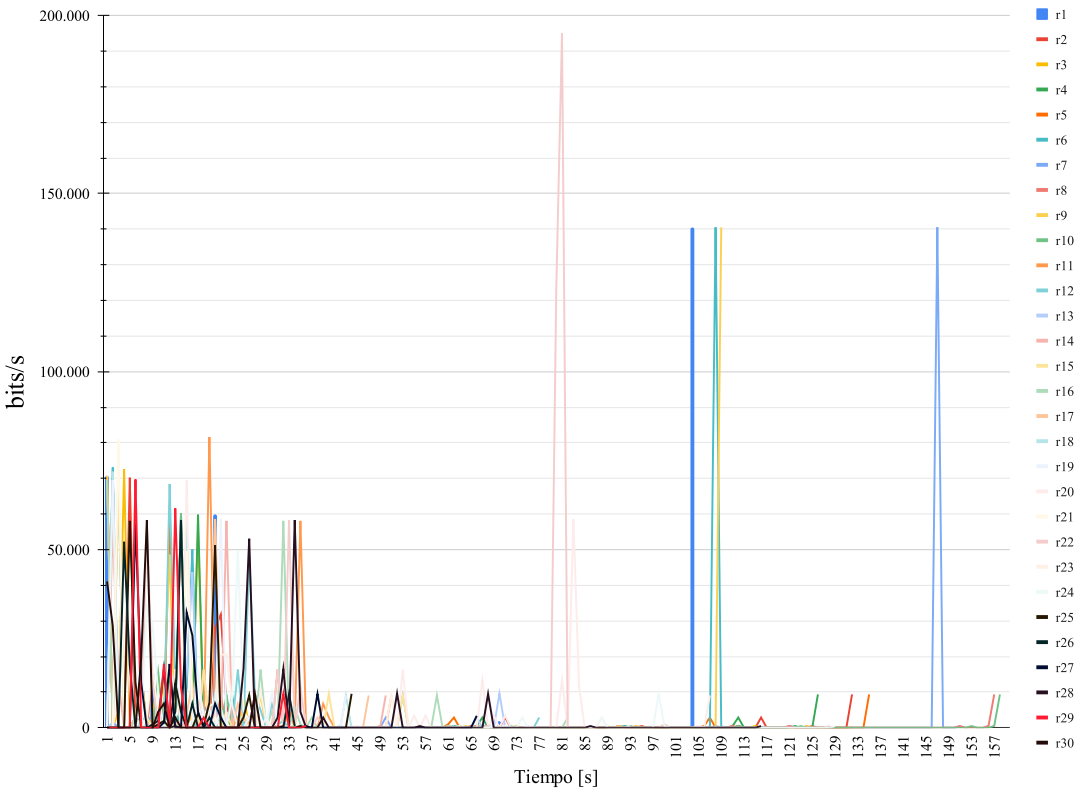

Figura 4.37: Consumo de ancho de banda de diferentes enrutadores

En la figura 4.38 son presentados los tiempos de respuesta del mecanismo obtenidos directamente de *Wireshark*, al ser un mecanismo que plantea una arquitectura en un entorno local es de esperar que los tiempos de respuesta sean pequeños a diferencia de una arquitectura en la nube.

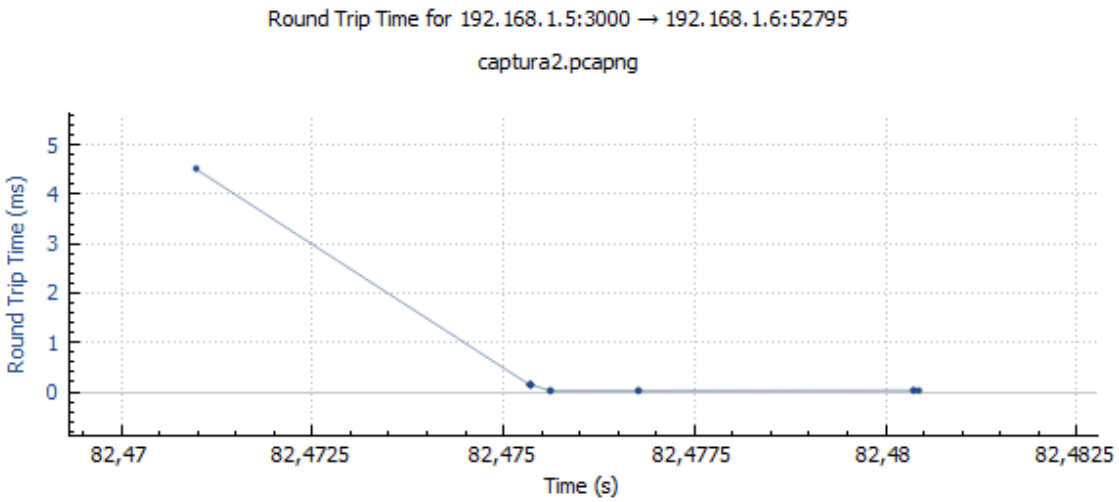

Figura 4.38: Tiempo de respuesta del mecanismo

Adicionalmente durante el estudio de caso es recopilada información adicional que complementa todos los análisis anteriores y que permite comprender mejor el panorama de los diferentes escaneos realizados:

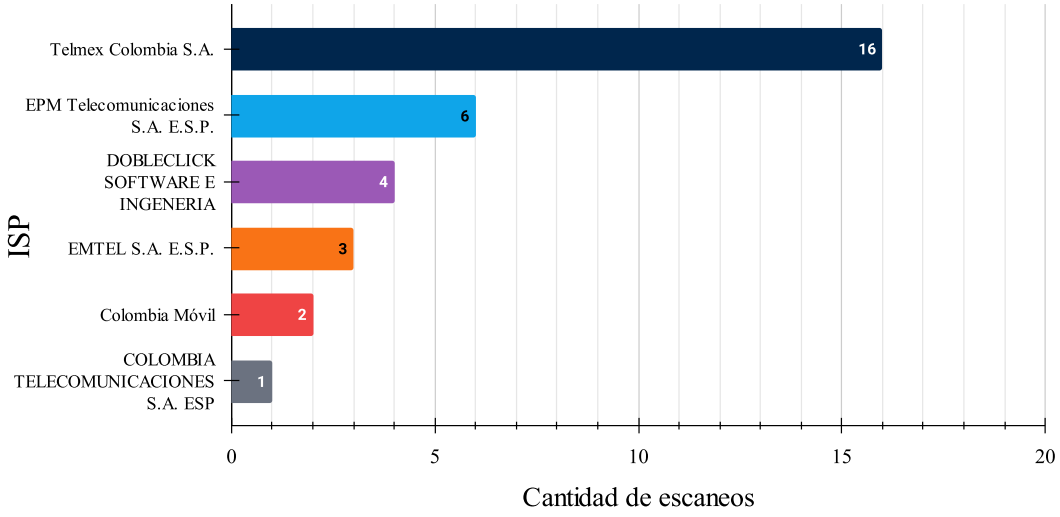

Figura 4.39: Cantidad de escaneos por ISP

La gráfica 4.39 brinda un resumen a nivel informativo de la cantidad de escaneos que se realizaron por ISP

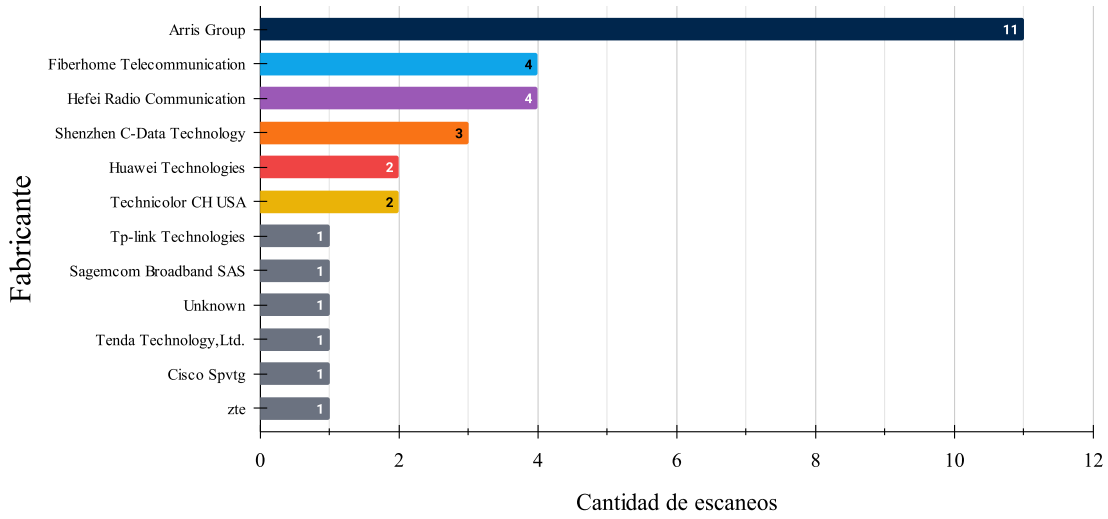

Figura 4.40: Cantidad de escaneos por fabricante

La gráfica 4.40 brinda un resumen a nivel informativo de la cantidad de escaneos que se realizaron por fabricante de enrutador

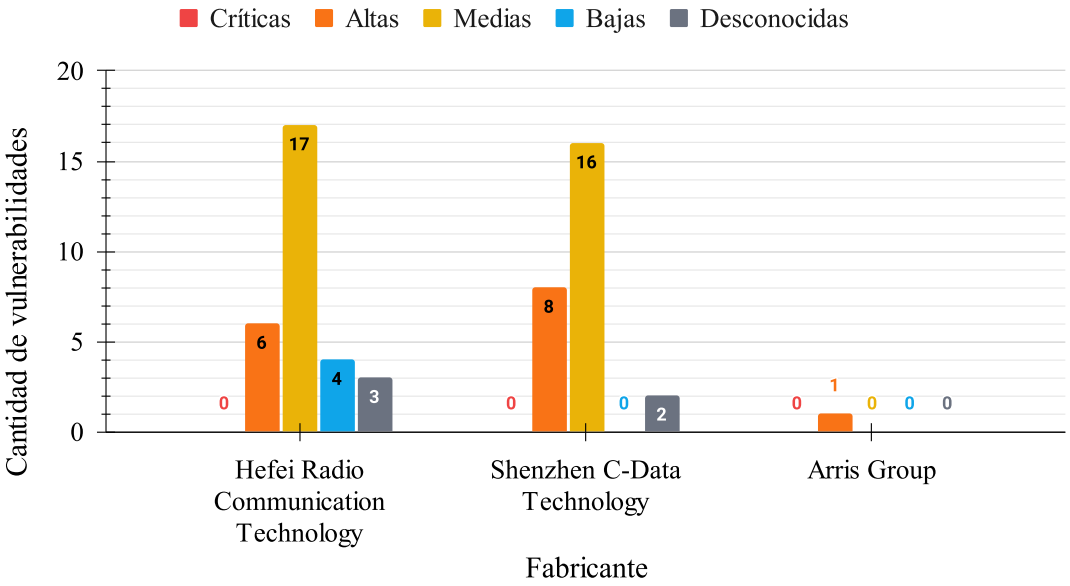

Figura 4.41: Cantidad vulnerabilidades por fabricante

En la gráfica 4.41 es presentado el top 3 de fabricantes que presentaron mayor cantidad de vulnerabilidades, donde el fabricante *Hefei Radio Communication Technology* registra 4 vulnerabilidades de severidad alta, 17 de severidad media, 4 de severidad baja y 3 de las cuales no fue posible obtener información.

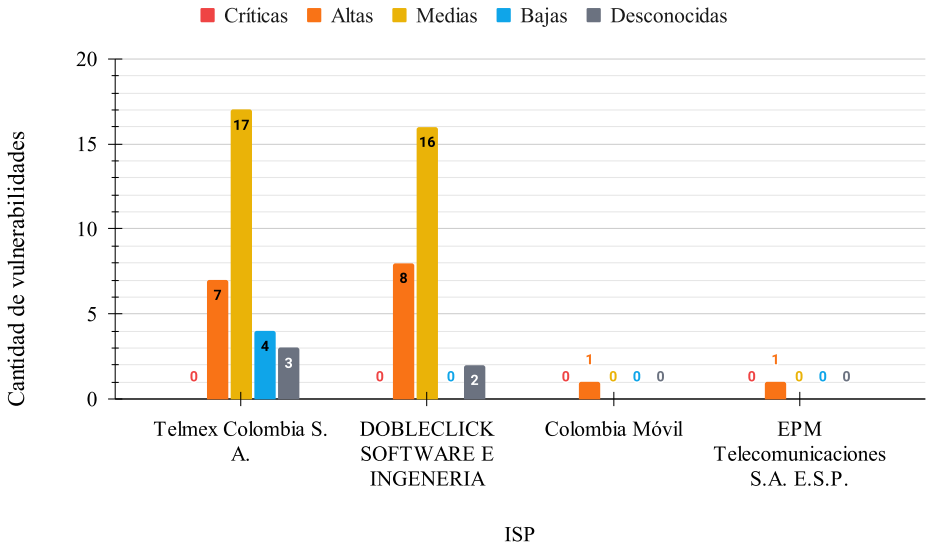

Figura 4.42: Cantidad de vulnerabilidades por ISP

Con base en la gráfica 4.42 es determinado que el ISP que presenta la mayor cantidad de vulnerabilidades es el proveedor Telmex Colombia S.A. (perteneciente a la empresa de telecomunicaciones CLARO COLOMBIA), seguido por DOBLECLICK SOFTWARE E INGENIERÍA.

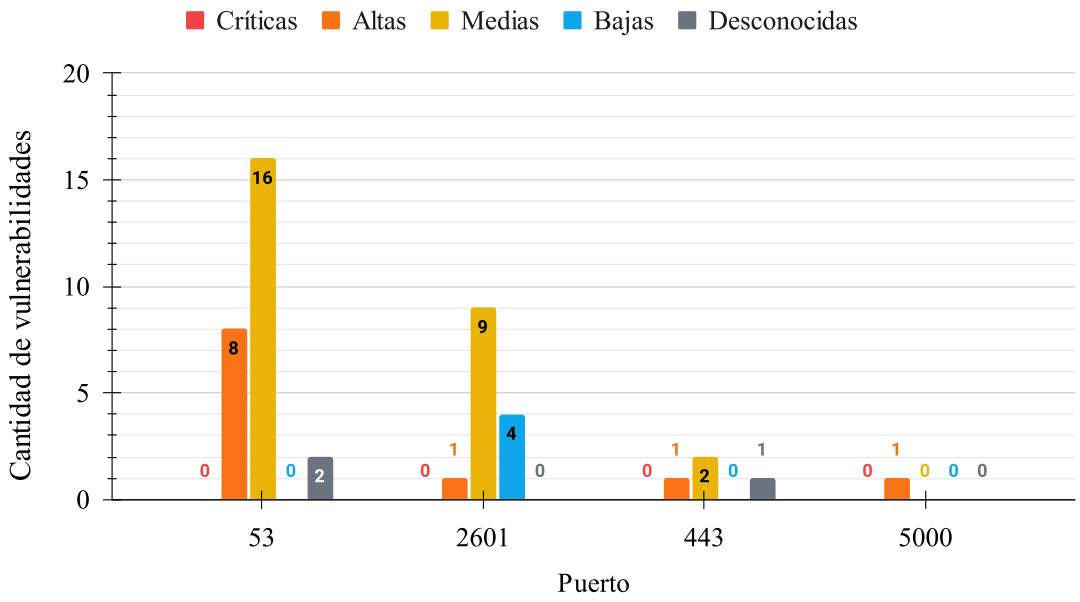

Figura 4.43: Vulnerabilidades en puertos

Con base en la gráfica 4.43 es preciso concluir que el puerto que presenta la mayor cantidad de vulnerabilidades es el 53. Dicho puerto utiliza los protocolos TCP y UDP, y en él corre el servicio de DNS (Domain Name Service), por esto vulnerabilidades en este puerto pueden conllevar a Suplantaciones de identidad (DNS Spoofing), Denegación del Servicio (DoS o DDoS), redireccionamiento de tráfico y/o fuga de información.

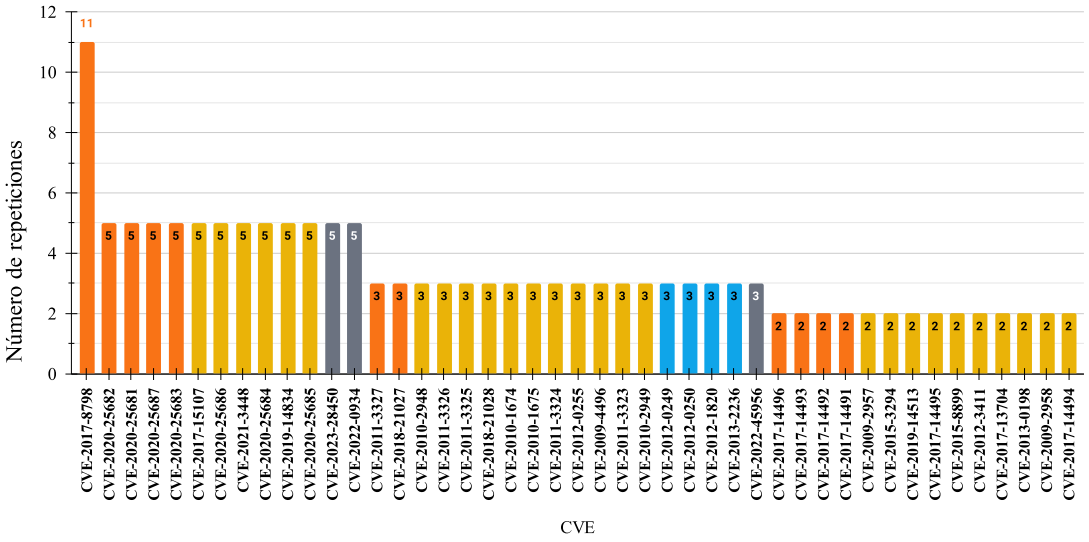

Figura 4.44: Vulnerabilidades encontradas

La vulnerabilidad mas recurrente es la CVE-2017-8789, la cual es una vulnerabilidad relacionada con la manera en que el servicio maneja los objetos en memoria y puede llevar a que el servicio falle al momento de validar apropiadamente la información brindada por el usuario. Por lo que un atacante podría forzar la ejecución de un archivo malicioso.

Capítulo 5

Entrega

Contenido

5.1. Conclusiones

Del presente trabajo de grado son obtenidas las siguientes conclusiones:

- Durante la revisión de literatura de trabajos relacionados y la identificación de brechas existentes, es de resaltar que la documentación actual no se enfoca en la prevención de vulnerabilidades de ciberseguridad en redes domésticas sino que al contrario el enfoque de la mayor parte de investigaciones es en la respuesta una vez una vulnerabilidad es detectada, por ende el enfoque es reactivo. Adicionalmente la mayoría de investigaciones están limitadas al descubrimiento de vulnerabilidades pero no proveen información de como se las pueden mitigar. De esta parte de la investigación es identificada una brecha en el conocimiento en la industria hacia la prevención y mitigación de vulnerabilidades de ciberseguridad en los enrutadores de redes domésticas. Esto cubre el análisis de trabajos relacionados.

- Es desarrollado metodológicamente un mecanismo para el prototipado de la solución, el enfoque propuesto tiene como fin estar centrado en el usuario. La combinación llevó a la sinergia entre Design Thinking y Scrum donde el inicio del prototipo hizo uso de Desing Thinking para definir la Persona (usuario final) y Scrum para el desarrollo ágil del prototipo. Es construido un mecanismo que aporta a un sistema que a futuro puede ser construido para automatizar de manera completa la mitigación de vulnerabilidades en redes domésticas.

- Para ejecutar el diagnóstico de las vulnerabilidades de seguridad presentes en los enrutadores, es conveniente estar conectados a la misma red de este, ya que de lo contrario para descubrir las vulnerabilidades se tendrá que hacer una serie de ataques al dispositivo y esto podría llevar a pérdidas momentáneas o permanentes del servicio de Internet, u otros contratiempos. Esta también es la razón por la cual desarrollar un mecanismo de diagnóstico de vulnerabilidades que sea ejecutado en la nube puede presentar muchas limitaciones.

- Es diseñado un mecanismo basado en CVSS que apoya el análisis de vulnerabilidades de múltiples tipos de severidad en dispositivos de acceso a la Internet en redes domesticas. Existen limitaciones con respecto al acceso de la información de las vulnerabilidades ligadas directamente a la legislación del país y/o políticas de los fabricantes; solo el usuario dueño de la red doméstica y el ISP en caso de ser autorizado son los que deben tener los permisos para permitir el escaneo de vulnerabilidades.

- La eficiencia del mecanismo en cuanto a la capacidad que tiene para concientizar a las personas sobre las posibles vulnerabilidades presentes en su enrutador. Donde es encontrado un resultado muy favorable, mostrando que en promedio las personas aumentas su nivel de concientización en un 387.23 %. Adicionalmente, 32 de las 32 personas que hicieron uso del mecanismo presentaron un aumento en su nivel de concientización.

- En cuanto a la facilidad de uso del mecanismo, es de resaltar que su versión de instalación que comprende la implementación de la Raspberry Pi, es percibido como fácil de usar por usuarios que tienen desde bajos niveles de conocimiento técnico hasta usuario alto nivel de conocimiento técnico. También en este aspecto es indentificado que a mayor conocimiento técnico del usuario, este percibía una mayor facilidad de

uso del mecanismo. Al evidenciar que el nivel de conocimiento técnico no esta estrechamente relacionado con la edad de la persona, es determinado que el mecanismo es apto para un amplio rango de edades.

- Se identifica que el mecanismo tiene una buena eficiencia en cuanto al tiempo de escaneo. Esto es soportado por la percepción de los usuarios en cuanto a velocidad de escaneo y los tiempos registrados por el propio mecanismo. El tiempo de escaneo comprende en promedio tan solo un 17.30 % del tiempo total empleado para usar el mecanismo exitosamente. Adicionalmente, usuarios con cualquier nivel de conocimiento técnico les toma alrededor de 7 minutos obtener un diagnostico de las vulnerabilidades de su enrutador junto con recomendaciones para mitigarlas.
- La adaptabilidad del mecanismo es apreciable ya que este tiene diferentes modos de instalación y presentación, haciéndolo apto para usuarios con diferentes requerimientos y niveles de técnicos. Complementariamente existen diferentes tipos de usuarios con diferentes privilegios y configuraciones de reportes que permiten abarcar una cantidad mas grande de tipos de usuarios, haciendo que el mecanismo sea de interés para personas del común pero también para ISPs y/o empresas de telecomunicaciones.

5.2. Trabajos a futuro

Con base ha lo explorado y desarrollado en este proyecto de investigación, esta sección se adentra en las áreas de investigación y desarrollo que representan el próximo paso en la evolución de esta solución.

- **Mitigación de Vulnerabilidades automatizada:** Sin duda, el principal trabajo a futuro es la continuación de la investigación abarcando el resto de mecanismos que componen el sistema automatizado de detección y mitigación de vulnerabilidades en redes domésticas. Para lograr no solo conciencia sobre las vulnerabilidades sino también un proceso de mitigación mas dinámico y fluido para personas de todos los niveles de conocimientos técnicos.
  Este trabajo a futuro comprende el Mecanismo 2 propuesto en el Capítulo 2 de este documento donde se sugiere la siguiente secuencia de funciones:

  MECANISMO 2: Mecanismo para la reparación de las vulnerabilidades

  - Función de identificación de vulnerabilidades reparables: Basado en las consultas realizadas sobre los métodos de mitigación para cada vulnerabilidad el sistema debe dividir las vulnerabilidades entre las reparables y las no reparables e identificar si posee los permisos suficientes para realizar los cambios necesarios para la reparación.
  - Función de automatización de corrección de vulnerabilidades: Posterior a la función de identificación de vulnerabilidades, se debe tener un diseño en la interfaz del sistema que le permita al usuario decidir entre las vulnerabilidades reparables, cuales son las que se seleccionan para que el sistema realice su reparación; y este la ejecute de manera automática.
  - Función de estadísticas y reportería de las vulnerabilidades reparadas: Finalmente después de la función de identificación y automatización, se requiere que

se le brinde al usuario un resumen en lenguaje no técnico de los cambios realizados en su sistema y cómo prevenir la reaparición de las vulnerabilidades reparadas.

- **Enfoque Preventivo recurrente en ciberseguridad en Redes Domésticas:** Proponer estrategias y herramientas para realizar diagnósticos de manera recurrente con el objetivo de mantener niveles altos de conciencia sobre las vulnerabilidades en el enrutador y prevenir vulnerabilidades en lugar de simplemente responder a ellas.
- **Diagnóstico Remoto de Vulnerabilidades:** Investigar formas de realizar el diagnóstico de vulnerabilidades en enrutadores sin necesidad de estar conectado a la misma red. Esto podría implicar el desarrollo de técnicas avanzadas de diagnóstico remoto y podría implicar realizar diagnósticos más limitados (básicos).
- **Optimización del tiempo de uso:** Continuar realizando mejoras en el mecanismo para reducir el tiempo que le toma al usuario llevar a cabo el diagnostico de su enrutador. Esta situación se podría abordar de diferentes ángulos, desde modificaciones en el hardware para hacerlo mas intuitivo de instalar, modificaciones en el software que agilicen el escaneo, o incluso mejoras en las interfaces que mejoren el flujo del usuario al momento de navegar en las vistas del mecanismo.
- **Integración de tecnologías emergente:** Evaluar la integración de tecnologías emergentes, como el aprendizaje automático o la inteligencia artificial, para mejorar la detección y mitigación de vulnerabilidades.
- **Ampliar la información de vulnerabilidades:** Integrar una mayor cantidad de bases de datos de vulnerabilidades, para que el mecanismo logre identificar una mayor cantidad de vulnerabilidades y tenga la capacidad de proveer recomendaciones para estas.
- **Extender el escaneo a más dispositivos:** En este momento el mecanismo se enfoca en detectar vulnerabilidades en el enrutador, sin embargo, se puede evaluar la posibilidad de escanear todos los dispositivos conectados a la red.
- **Extender la detección a otro tipo de vulnerabilidades y no solo CVE:** El mecanismo es capaz de detectar y proporcionar información acerca de vulnerabilidades que siguen el estándar CVE, sin embargo, se presentaron otro tipo de vulnerabilidades del tipo OSV, CWE, etc. Las cuales no se consideraron para la investigación y desarrollo del prototipo.
- **Enfoque de microservicios:** Con la arquitectura actual API REST (cliente/servidor) es posible evaluar la viabilidad de un enfoque de contenedores en un contexto de microservicios en la nube para detectar vulnerabilidades en otros servicios que se encuentren en la misma red del prototipo.

Estos trabajos pueden contribuir al desarrollo continuo del mecanismo desarrollado y en general a la expansión de la concientización y las prácticas de ciberseguridad en el contexto de los enrutadores SOHO y redes domestica.

ANEXOS

A continuación, se listan todos los Anexos mencionados y usados en la investigación:

ANEXO A: Documentos Mapeo Sistemático de Literatura
Se realiza un resumen de los documentos obtenidos en la revisión sistemática de literatura, por calificación, cadenas de búsqueda y documentos finales. Puede ser encontrado en el siguiente Google Sheets:

Anexo A

ANEXO B: Resultados Entrevista Exploratoria La entrevista realiza por medio de un formulario de Google Forms y fue distribuida a diferentes de personas de la ciudad de Popayán. Los resultados se muestran en el siguiente documento:

Anexo B

ANEXO C: Pruebas de Campo Evidencia fotográfica de algunas de las pruebas de campo realizadas por los investigadores del presente trabajo de grado.

Anexo C

ANEXO D: Resultados de las Entrevistas en las pruebas de campo y calculo de la eficiencia
Se muestran los resultados de las entrevistas realizadas durante las pruebas de campo y el cálculo para obtener la eficiencia en cada uno de los aspectos mencionados:

Anexo D

ANEXO E: Código del mecanismo desarrollado
Contiene los archivos que conforman la totalidad del código del mecanismo.

Anexo E

ANEXO F: Guía de inicio rápido Documento donde se muestra los pasos a seguir para instalar el mecanismo.

Anexo F

ANEXO G: Vídeos de instalación Vídeos mostrando la manera de instalar el mecanismo.

Anexo G.1 - Alpine Linux Anexo G.2 - Raspberry Pi

ANEXO H: Consentimiento Informado Formato del consentimiento informado presentado a las personas que fueron participes del estudio de caso.

Anexo H

ANEXO I: Bases Datos de geolocalzación e ISPs adquiridas Archivos con los registros de geolocalzación e información de ISPs de las bases datos adquiridas.

Anexo I

ANEXO J: Documentación de endpoints (postman) Documento donde se exponen los endpoint (postman) implementados en el mecanismo.

Anexo J

ANEXO K: Reportes de resultados de la aplicación Resultados de los múltiples diagnósticos realizados con el mecanismo.

Anexo K

ANEXO L: Artículos Artículos escritos durante el desarrollo del proyecto de investigación.

Anexo L

Bibliografía

[1] C. Brooks. Alarming Cybersecurity Stats: What You Need To Know For 2021. [Online]. Available: https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=73203eca58d3

[2] F. Labs. Más de 7 billones de intentos de ciberataques afectaron a Colombia en 2020 ACIS. Accedido 2021-08-26. [Online]. Available: https://go.fortinet.com/latam-tp-es/ThreatIntelligenceIQ1

[3] Y. Meidan, V. Sachidananda, H. Peng, R. Sagron, Y. Elovici, and A. Shabtai, "A novel approach for detecting vulnerable IoT devices connected behind a home NAT," *Computers and Security*, vol. 97, p. 101968, oct 2020.

[4] S. M. Sajjad, M. Yousaf, H. Afzal, and M. R. Mufti, "EMUD: Enhanced manufacturer usage description for iot botnets prevention on home wifi routers," *IEEE Access*, vol. 8, pp. 164 200–164 213, 2020.

[5] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: A case study on embedded web interfaces," *ASIA CCS 2016 - Proceedings of the 11th ACM Asia Conference on Computer and Communications Security*, pp. 437–448, may 2016.

[6] V. Visoottiviseth, P. Jutadhammakorn, N. Pongchanchai, and P. Kosolyudhthasarn, "Firmaster: Analysis Tool for Home Router Firmware," *Proceeding of 2018 15th International Joint Conference on Computer Science and Software Engineering, JCSSE 2018*, sep 2018.

[7] V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart, and S. Chotivatunyu, "PENTOS: Penetration testing tool for internet of thing devices," in *TENCON 2017 - 2017 IEEE Region 10 Conference*. IEEE, Nov. 2017. [Online]. Available: https://doi.org/10.1109/tencon.2017.8228241

[8] Y. Zhang, W. Huo, K. Jian, J. Shi, H. Lu, L. Liu, C. Wang, D. Sun, C. Zhang, and B. Liu, "Sr-fuzzer: An automatic fuzzing framework for physical SOHO router devices to discover multi-type vulnerabilities," *ACM International Conference Proceeding Series*, pp. 544–556, dec 2019.

[9] W. You, X. Wang, S. Ma, J. Huang, X. Zhang, X. Wang, and B. Liang, "ProFuzzer: On-the-fly input type probing for better zero-day vulnerability discovery," *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2019-May, pp. 769–786, may 2019.

[10] P. Celeda, R. Krejci, and V. Krmicek, "Revealing and analysing modem malware," *IEEE International Conference on Communications*, pp. 971–975, 2012.

[11] N. An, A. Duff, G. Naik, M. Faloutsos, S. Weber, and S. Mancoridis, "Behavioral anomaly detection of malware on home routers," *Proceedings of the 2017 12th International Conference on Malicious and Unwanted Software, MALWARE 2017*, vol. 2018-January, pp. 47–54, mar 2018.

[12] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, 2018. [Online]. Available: https://doi.org/10.14722/ndss.2018.23204

[13] A. N. Jahromi, H. Karimipour, A. Dehghantanha, and K.-K. R. Choo, "Toward detection and attribution of cyber-attacks in IoT-enabled cyber physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13 712–13 722, Sep. 2021. [Online]. Available: https://doi.org/10.1109/jiot.2021.3067667

[14] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1636–1675, apr 2019.

[15] M. Mora, *Descripción del Método de Investigación Conceptual*. Universidad Autónoma de Aguascalientes, Aguascalientes, 2003, pp. 2–10.

[16] J. Francia. (2017) ¿Qué es Scrum? — Scrum.org. [Online]. Available: https://www.scrum.org/resources/blog/que-es-scrum

[17] Cisco. ¿Qué es la ciberseguridad? - Cisco. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.htmlhttps://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

[18] IBM. (2020) ¿Qué es la ciberseguridad? — IBM. [Online]. Available: https://www.ibm.com/co-es/topics/cybersecurityhttps://www.ibm.com/ar-es/topics/cybersecurity

[19] Microsoft. (2022) ¿qué es la ciberseguridad? [Online]. Available: https://support.microsoft.com/en-us/topic/what-is-cybersecurity-8b6efd59-41ff-4743-87c8-0850a352a390

[20] S. Works, "What is network behavior analysis? definition, importance, and best practices," [Online]. Available on: "https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/", 2022.

[21] Techopedia, "Network behavior analysis (nba)," [Online]. Available on: "https://www.techopedia.com/definition/16118/network-behavior-analysis-nba", 2022.

[22] S. Y. Lim and A. Jones, "Network anomaly detection system: The state of art of network behaviour analysis," in *2008 International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 459–465.

[23] IBM. (2021) Repair or mitigate a vulnerability. [Online]. Available: https://www.ibm.com/docs/en/sss/3.1.1?topic=vulnerabilities-repair-mitigate-vulnerability

[24] Ingecom. Remediación vs mitigación de vulnerabilidades: ¿Cuál es la diferencia? [Online]. Available: https://www.ingecom.net/es/blog/75/remediacion-vs-mitigacion-de-vulnerabilidades-cual-es-la-diferencia/

[25] J. Risto, "What is common vulnerability scoring system (cvss)," [Online]. Available on: "https://www.sans.org/blog/what-is-cvss/", 2023.

[26] I. Tenable, "Cvss vs. vpr," [Online]. Available on: "https://docs.tenable.com/vulnerability-management/Content/Explore/Findings/RiskMetrics.htm", 2023.

[27] C. A. official website of the U.S. Department of Homeland Security, "Stakeholder-specific vulnerability categorization (ssvc)," [Online]. Available on: "https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc", 2023.

[28] I. SecOps Solution, "What is the epss scoring system?" [Online]. Available on: "https://www.secopsolution.com/blog/what-is-the-epss-scoring-system", 2023.

[29] FIRST. (2020) Common Vulnerability Scoring System SIG. [Online]. Available: https://www.first.org/cvss/https://www.first.org/cvss

[30] Kaspersky. (2018) What is Use-After-Free? — Kaspersky IT Encyclopedia. [Online]. Available: https://encyclopedia.kaspersky.com/glossary/cvss-common-vulnerability-scoring-system/https://encyclopedia.kaspersky.com/glossary/use-after-free/

[31] NIST. (2019) NVD - Vulnerability Metrics. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

[32] R. S. Pressman, *Software engineering: a practitioner's approach*. Palgrave macmillan, 2005.

[33] H. Van Vliet, H. Van Vliet, and J. Van Vliet, *Software engineering: principles and practice*. John Wiley & Sons Hoboken, NJ, 2008, vol. 13.

[34] R. Färe, S. Grosskopf, and C. Lovell, *The Measurement of Efficiency of Production*, ser. Studies in Productivity Analysis. Springer Netherlands, 1985. [Online]. Available: https://books.google.com.co/books?id=OaWffSMcV14C

[35] M. Guil Bozal, "Escala mixta likert-thurstone," *Anduli, 5, 81-95.*, 2006.

[36] "awareness," Nov. 2023. [Online]. Available: https://dictionary.cambridge.org/us/dictionary/english/awareness

[37] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering," *12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008*, jun 2008. [Online]. Available: https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/EASE2008.8

[38] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*, 2007.

[39] A. A. Khan, A. Ahmad, M. Waseem, P. Liang, M. Fahmideh, T. Mikkonen, and P. Abrahamsson, "Software Architecture for Quantum Computing Systems - Asystematic Review," *SSRN Electronic Journal*, 2022.

[40] D. Budgen, M. Turner, P. Brereton, and B. Kitchenham, "Using Mapping Studies in Software Engineering," in *PPIG*, vol. 2, 2008, pp. 195–204. [Online]. Available: www.ebse.org.uk.http://www.ppig.org/papers/20th-budgen.pdf

[41] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirements Engineering*, vol. 11, no. 1, pp. 102–107, nov 2006. [Online]. Available: https://link-springer-com.acceso.unicauca.edu.co/article/10.1007/s00766-005-0021-6

[42] W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," *MethodsX*, vol. 7, p. 100777, 2020. [Online]. Available: http://dx.doi.org/10.1016/j.mex.2019.100777

[43] D. Papaioannou, A. Sutton, and A. Booth, "Systematic approaches to a successful literature review," *Systematic approaches to a successful literature review*, pp. 1–336, 2016.

[44] N. Hadar, S. Siboni, and Y. Elovici, "A lightweight vulnerability mitigation framework for IoT devices," *IoT S and P 2017 - Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, co-located with CCS 2017*, pp. 71–75, nov 2017.

[45] J. d. J. Rugeles Uribe, E. P. Guillen, and L. S. Cardoso, "A technical review of wireless security for the internet of things: Software defined radio perspective," *Journal of King Saud University - Computer and Information Sciences*, apr 2021.

[46] W. Xie, C. Zhang, P. Wang, Z. Wang, and Q. Yang, "ARGUS: Assessing Unpatched Vulnerable Devices on the Internet via Efficient Firmware Recognition," *ASIA CCS 2021 - Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 421–431, may 2021.

[47] L. Metongnon and R. Sadre, "Beyond telnet: Prevalence of IoT protocols in telescope and honeypot measurements," *WTMC 2018 - Proceedings of the 2018 Workshop on Traffic Measurements for Cybersecurity, Part of SIGCOMM 2018*, pp. 21–26, aug 2018. [Online]. Available: https://doi.org/10.1145/3229598.3229604

[48] Y. Jiang, W. Xie, and Y. Tang, "Detecting authentication-bypass flaws in a large scale of IoT embedded web servers," *ACM International Conference Proceeding Series*, pp. 56–63, nov 2018.

[49] A. Tambe, Y. L. Aung, R. Sridharan, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "Detection of threats to IoT devices using scalable VPN-forwarded honeypots," *CODASPY 2019 - Proceedings of the 9th ACM Conference on Data and Application Security and Privacy*, pp. 85–96, mar 2019.

[50] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2020-May, pp. 517–533, may 2020.

[51] X. Li, B. Liu, X. Zheng, H. Duan, Q. Li, and Y. Huang, "Fast IPv6 Network Periphery Discovery and Security Implications," *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021*, pp. 88–100, jun 2021.

[52] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, "HADES-IoT: A practical host-based anomaly detection system for iot devices," *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pp. 479–484, jul 2019.

[53] M. T. Ahvanooey, M. X. Zhu, Q. Li, W. Mazurczyk, K. K. R. Choo, B. B. Gupta, and M. Conti, "Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Survey," *IEEE Internet of Things Journal*, 2021.

[54] H. Zhao, H. Shu, and Y. Xing, "A Review on IoT Botnet," *ACM International Conference Proceeding Series*, vol. PartF16898, jan 2021.

[55] S. Romana, J. Grandhi, and P. R. Eswari, "Security Analysis of SOHO Wi-Fi routers," *Proceedings - 2020 International Conference on Software Security and Assurance, ICSSA 2020*, pp. 72–77, 2020.

[56] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2019-May, pp. 1362–1380, may 2019.

[57] I. Constantin, C. Patachia, C. Patrascu, A. Avadanei, and L. Nitescu, "Threat classification in current Communication Infrastructures," *Proceedings of the 11th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2019*, jun 2019.

[58] N. P. Tran, N. B. Nguyen, Q. D. Ngo, and V. H. Le, "Towards malware detection in routers with C500-toolkit," *2017 5th International Conference on Information and Communication Technology, ICoIC7 2017*, oct 2017.

[59] I. Alsmadi, Z. Dwekat, R. Cantu, and B. Al-Ahmad, "Vulnerability assessment of industrial systems using Shodan," *Cluster Computing 2021*, pp. 1–11, jun 2021. [Online]. Available: https://link.springer.com/article/10.1007/s10586-021-03330-3

[60] S. K. Cha, T. Avgerinos, A. Rebert, and D. Brumley, "Unleashing Mayhem on binary code," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 380–394, 2012.

[61] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan," *Proceedings - Annual Computer Security Applications Conference, ACSAC*, pp. 97–106, 2010.

[62] D. N. Serpanos and A. G. Voyiatzis, "Security challenges in embedded systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 12, no. SUPPL1, mar 2013. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2435227.2435262

[63] A. M. Rea-Guaman, J. Mejía, T. S. Feliu, and J. A. Calvo-Manzano, "AVARCIBER: a framework for assessing cybersecurity risks," *Cluster Computing*, vol. 23, no. 3, pp. 1827–1843, Jan. 2020. [Online]. Available: https://doi.org/10.1007/s10586-019-03034-9

[64] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. IEEE, Sep. 2016. [Online]. Available: https://doi.org/10.1109/isi.2016.7745438

[65] K. Kim, J. Lee, and W. Jung, "Method of building a security vulnerability information collection and management system for analyzing the security vulnerabilities of IoT devices," in *Lecture Notes in Electrical Engineering*. Springer Singapore, 2017, pp. 205–210. [Online]. Available: https://doi.org/10.1007/978-981-10-5041-1_35

[66] M. Vanhoef and F. Piessens, "Advanced wi-fi attacks using commodity hardware," in *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, Dec. 2014. [Online]. Available: https://doi.org/10.1145/2664243.2664260

[67] M. N. Aman, U. Javaid, and B. Sikdar, "IoT-proctor: A secure and lightweight device patching framework for mitigating malware spread in IoT networks," *IEEE Systems Journal*, pp. 1–12, 2021. [Online]. Available: https://doi.org/10.1109/jsyst.2021.3070404

[68] I. Cvitic, D. Perakovic, B. B. Gupta, and K.-K. R. Choo, "Boosting-based DDoS detection in internet of things systems," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2109–2123, Feb. 2022. [Online]. Available: https://doi.org/10.1109/jiot.2021.3090909

[69] N. Mazhar, R. Salleh, M. Zeeshan, and M. M. Hameed, "Role of device identification and manufacturer usage description in IoT security: A survey," *IEEE Access*, vol. 9, pp. 41 757–41 786, 2021. [Online]. Available: https://doi.org/10.1109/access.2021.3065123

[70] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garces, "A comprehensive study of the IoT cybersecurity in smart cities," *IEEE Access*, vol. 8, pp. 228 922–228 941, 2020. [Online]. Available: https://doi.org/10.1109/access.2020.3046442

[71] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5366–5380, 2021. [Online]. Available: https://doi.org/10.1109/tifs.2021.3127009

[72] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset," *IEEE Access*, vol. 9, pp. 34 188–34 205, 2021. [Online]. Available: https://doi.org/10.1109/access.2021.3061609

[73] S. Kwon and H.-K. Choi, "Evolution of wi-fi protected access: Security challenges," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2020. [Online]. Available: https://doi.org/10.1109/mce.2020.3010778

[74] K. Moissinac, D. Ramos, G. Rendon, and A. Elleithy, "Wireless encryption and WPA2 weaknesses," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, Jan. 2021. [Online]. Available: https://doi.org/10.1109/ccwc51732.2021.9376023

[75] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020. [Online]. Available: https://doi.org/10.1109/access.2019.2962829

[76] S. K. Muttoo and S. Badhani, "An analysis of malware detection and control through Covid-19 pandemic," in *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, 2021, pp. 637–641. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9441126/authors#authors

[77] R. Li, Q. Li, J. Zhou, and Y. Jiang, "ADRIoT: An edge-assisted anomaly detection framework against IoT-based network attacks," *IEEE Internet of Things Journal*, pp. 1–1, 2021. [Online]. Available: https://doi.org/10.1109/jiot.2021.3122148

[78] C. Ye, P. P. Indra, and D. Aspinall, "Retrofitting security and privacy measures to smart home devices," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, Oct. 2019. [Online]. Available: https://doi.org/10.1109/iotsms48152.2019.8939272

[79] T. N. Phu, N. D. Tho, L. H. Hoang, N. N. Toan, and N. N. Binh, "An efficient algorithm to extract control flow-based features for IoT malware detection," *The Computer Journal*, vol. 64, no. 4, pp. 599–609, Oct. 2020. [Online]. Available: https://doi.org/10.1093/comjnl/bxaa087

[80] J. Li, B. Zhao, and C. Zhang, "Fuzzing: a survey," *Cybersecurity*, vol. 1, no. 1, pp. 1–13, dec 2018. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0002-y

[81] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, "An overview of IP flow-based intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 343–356, 2010. [Online]. Available: https://doi.org/10.1109/surv.2010.032210.00054

[82] T. Wüchner, M. Ochoa, and A. Pretschner, "Malware detection with quantitative data flow graphs," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*. ACM, Jun. 2014. [Online]. Available: https://doi.org/10.1145/2590296.2590319

[83] ——, "Robust and effective malware detection through quantitative data flow graph metrics," in *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer International Publishing, 2015, pp. 98–118. [Online]. Available: https://doi.org/10.1007/978-3-319-20550-2_6

[84] H. Xie, X. Wang, and J. Liu, "Methods, systems, and computer readable media for utilizing synthetic animatronics," *US Patent*, 2018. [Online]. Available: https://patents.google.com/patent/US20150319136A1

[85] Q. Do, B. Martini, and K.-K. R. Choo, "Cyber-physical systems information gathering: A smart home case study," *Computer Networks*, vol. 138, pp. 1–12, Jun. 2018. [Online]. Available: https://doi.org/10.1016/j.comnet.2018.03.024

[86] J. Liang, Y. Jiang, M. Wang, X. Jiao, Y. Chen, H. Song, and K.-K. R. Choo, "DeepFuzzer: Accelerated deep greybox fuzzing," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020. [Online]. Available: https://doi.org/10.1109/tdsc.2019.2961339

[87] X. Mi, X. Feng, X. Liao, B. Liu, X. Wang, F. Qian, Z. Li, S. Alrwais, L. Sun, and Y. Liu, "Resident evil: Understanding residential IP proxy as a dark service," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, May 2019. [Online]. Available: https://doi.org/10.1109/sp.2019.00011

[88] J. Zhang, H. Duan, W. Liu, and X. Yao, "How to notify a vulnerability to the right person? case study: In an ISP scope," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. IEEE, Dec. 2017. [Online]. Available: https://doi.org/10.1109/glocom.2017.8253993

[89] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, Nov. 2017. [Online]. Available: https://doi.org/10.1145/3139937.3139938

[90] H. Liu, C. Li, X. Jin, J. Li, Y. Zhang, and D. Gu, "Smart solution, poor protection," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, Nov. 2017. [Online]. Available: https://doi.org/10.1145/3139937.3139948

[91] A. Michalas and R. Murray, "Keep pies away from kids," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, Nov. 2017. [Online]. Available: https://doi.org/10.1145/3139937.3139953

[92] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, Sep. 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.06.005

[93] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 4, pp. 541–553, Oct. 2019. [Online]. Available: https://doi.org/10.1016/j.jksuci.2018.03.011

[94] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016. [Online]. Available: https://doi.org/10.1109/comst.2015.2494502

[95] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019. [Online]. Available: https://doi.org/10.1109/comst.2019.2896380

[96] H. Qiu, Y. Zeng, S. Guo, T. Zhang, M. Qiu, and B. Thuraisingham, "DeepSweep: An evaluation framework for mitigating DNN backdoor attacks using data augmentation," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. ACM, May 2021. [Online]. Available: https://doi.org/10.1145/3433210.3453108

[97] M. H. Haghighat and J. Li, "Edmund: Entropy based attack detection and mitigation engine using netflow data," in *Proceedings of the 8th International Conference on Communication and Network Security - ICCNS 2018*. ACM Press, 2018. [Online]. Available: https://doi.org/10.1145/3290480.3290484

[98] S. Rizvi, T. Flock, T. Flock, and I. Williams, "Anomaly detection to protect networks from advanced persistent threats using adaptive resonance AI concepts," in *2020 International Conference on Software Security and Assurance (ICSSA)*. IEEE, Oct. 2020. [Online]. Available: https://doi.org/10.1109/icssa51305.2020.00018

[99] D. Gadner and M. Felderer, "The collective process framework DTScrum for integrating design thinking into scrum," in *Design Thinking for Software Engineering*. Springer International Publishing, 2022, pp. 85–101. [Online]. Available: https://doi.org/10.1007/978-3-030-90594-1_5

[100] R. K. Yin, *Case study research: Design and methods*. sage, 2009, vol. 5.

[101] "Common Vulnerabilities and Exposures." [Online]. Available: https://www.cve.org/

[102] "National Vulnerability Database." [Online]. Available: https://nvd.nist.gov/

[103] "GitHub Advisory Database." [Online]. Available: https://github.com/advisories

[104] "China National Vulnerability Database." [Online]. Available: https://www.cnvd.org.cn/

[105] AWS, "¿Qué es una API de RESTful? - Explicación de API de RESTful - AWS — aws.amazon.com," https://aws.amazon.com/es/what-is/restful-api/, [Accessed 05-12-2023].