ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UN DISPOSITIVO PARA CONTROL DE ACCESO A INTERNET UTILIZANDO HARDWARE DE BAJO COSTO Y SOFTWARE LIBRE"

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentado por:

RONNY JESÚS ALCÍVAR LLAMUCA
KAREN DE LAS MERCEDES MARTÍNEZ DURAN

GUAYAQUIL – ECUADOR

AÑO: 2018 - 2019

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

De igual manera mis agradecimientos a mis profesores en especial al Ing. Ronald Criollo y al Ing. Rayner Durango quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada una de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente, quiero expresar mi más grande y sincero agradecimiento a mi compañera Karen Martinez, con quien en conjunto hemos logrado el desarrollo de este proyecto.

Ronny Jesús Alcívar Llamuca

Dedico este trabajo principalmente a Dios, por haberme permitido llegar hasta este momento tan importante de mi formación profesional.

A mi hermano Elvis por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, y a su familia Nadia, Carlos, Sebastian, Erick por el valor mostrado para salir adelante y por su amor.

A mi pareja Gabriel, ya que con su apoyo, sus consejos, su amor, y su paciencia me ayudo a concluir esta meta.

A mis profesores, el Ing. Ronald Criollo y el Ing. Rayner Durango gracias por su tiempo, apoyo, sabiduría y confianza a lo largo del proceso de mi formación profesional.

A mi compañero de proyecto Ronny Alcivar, por sus palabras de aliento ante las dificultades; su sentido del humor, su gran responsabilidad y compromiso con la elaboración de este proyecto que nos permitió afianzar nuestra amistad.

Karen De Las Mercedes Martínez Duran

DEDICATORIA

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre Alba.
Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

Ronny Jesús Alcívar Llamuca

A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente, pero sobre todo por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi abuelita María Concepción, quien desde el cielo me guía y seguramente está orgullosa de este logro.

A mi madre Laura, por ser el pilar fundamental en todo lo que soy, por su incondicional apoyo perfectamente mantenido a través del tiempo.

Karen De Las Mercedes Martínez Duran

TRIBUNAL DE EVALUACIÓN

Ing. Ronald Criollo Bonilla

PROFESOR DE MATERIA

INTEGRADORA

Ing. Durango Espinoza Rayner

TUTOR ACADEMICO

DECLARACIÓN EXPRESA

"La responsabilidad y autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; *Ronny Jesús Alcívar Llamuca y Karen De Las Mercedes Martínez Duran y* damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Ronny Jesús Alcívar Llamuca

Karen De Las Mercedes Martínez Duran

RESUMEN

El presente proyecto se basa en realizar el filtrado de contenido malicioso e inapropiado en una red de área local mediante la implementación un dispositivo de fácil uso y manipulación utilizando software libre y hardware de bajo costo. El dispositivo creado ha sido nombrado MiPiBlock, el cual ha sido diseñado utilizando componentes electrónicos disponibles en la actualidad. Se han creado varias categorías de navegación las cuales se relacionan con diferentes listas de acceso y denegación predeterminadas, además de brindar la opción al usuario de configurar su propia lista de manera personalizada. Se ha utilizado la metodología de Design Thinking para el diseño y desarrollo del dispositivo.

MiPiBlock ha sido implementado y probado en las instalaciones de la fundación Compassion International, donde se ha comprobado su correcto funcionamiento y la facilidad de su uso por parte de los usuarios supervisores de la institución. Se han recibido críticas muy positivas con respecto a la iniciativa de brindar seguridad a los usuarios más inexpertos.

La seguridad en las tecnologías de la información es un área compleja y extensa como lo es la necesidad del acceso a Internet en la actualidad, además, es inevitable que las amenazas en la red continúen mutando y perfeccionándose, por lo que los mecanismos para contrarrestarlas deben ser completas y de fácil acceso al público en general, MiPiBlock representa un paso exitoso con miras a satisfacer dicha necesidad.

Palabras Clave: Contenido Malicioso, Internet, MiPiBlock, Hardware de Bajo Costo, Software Libre, Tecnologías de la Información, Seguridad, Proxy.

ABSTRACT

This Project is intended to provide malicious and inappropriate content filtering in a Local Area Network by means of the implementation of an easy-use device using open source software and low-cost hardware. The device created is called MiPiBlock, and it has been designed using electronic components available nowadays. It comes with different Internet surfing profiles, which are related with different pre-defined allowed and restricted sites access-lists and the possibility to configure customized lists. Design thinking methodology was used for preparation, planning and design.

MiPiBlock was implemented and tested in the offices of Compassion International Foundation, where its correct performance and the easiness of its use was confirmed by the supervisors of the institution and very good comments were received from them regarding the initiative of providing security to less experimented users.

Information technology security considerations are as complex and extense as the current necessity of internet access in general. It is also inevitable that network security threats continue to evolve and improve, therefore defense mechanisms to counteract them should be more universal and accessible to everyday people than ever. MiPiBlock presents in that sense a very good step to satisfy this necessity.

Keywords: *Malicious content filtering, Internet, MiPiBlock, Low-cost Hardware, Open Source, Information and Communication Technologies, Security, Proxy.*

ÍNDICE GENERAL

ABREVIATURAS

API	Interfaz de Programación de Aplicaciones
ARP	Protocolo de Resolución de Direcciones
CDI-314	Centro de Desarrollo Integral 314– Compassion International
DT	Design Thinking
ESPOL	Escuela Superior Politécnica del Litoral
HDMI	Interfaz Multimedia de Alta Definición
HTTP	Protocolo de Transferencia de Hipertexto
INEC	Instituto Nacional de Estadística y Censos
ISP	Proveedor de Servicios de Internet
LAN	Red de Área Local
ONU	Organización de las Naciones Unidas
OSI	Interconexión de Sistemas Abiertos
PIN	Numero personal de identificación.
POV	Punto de Vista
PUK	Clave Personal de Desbloqueo
TIC	Tecnologías de la Información y la Comunicación
URL	Localizador Uniforme de Recursos
USD	United States Dollars

SIMBOLOGÍA

mm	Milímetros

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

Internet se ha convertido a nivel mundial en un medio cotidiano de comunicación, una herramienta de trabajo multidisciplinario y sobre todo un importante instrumento de generación de contenidos entre individuos [1]. A nivel internacional, según un estudio realizado por la empresa Miniwatts Marketing Group, al 30 de junio del 2018 se registran 4.199'194.131 usuarios de Internet [2]. Por su parte la Organización de las Naciones Unidas (ONU) reveló que 3 de cada 4 usuarios que acceden a Internet oscilan entre 15 y 24 años, [3] lo que nos indica que los adolescentes y jóvenes constituyen una gran parte de los usuarios activos de Internet.

En el Ecuador, el Instituto Nacional de Estadística y Censos (INEC) nos indica en el estudio realizado en el 2016 bajo la denominación de "La tecnología y los más pequeños del hogar", que el 61.2% de los niños entre 5 y 15 años utilizan Internet. Además, el porcentaje de este sector de la población que usa el Internet con una frecuencia de al menos una vez al día es el 61.0% [4]. Adicionalmente, se registró que el uso de Internet a nivel nacional es destinado en un 38% de los casos para obtener información, el 31.5% para comunicación general, el 23.2% en educación y aprendizaje, el 3.6% por razones estrictamente de trabajo y el 3.7% en otros usos.

Asimismo, el INEC determinó que el sector generacional en el cual se evidencia el mayor uso de Internet es en los jóvenes entre 16 y 24 años donde el 83.8% de este grupo son usuarios. A este rango le sigue el grupo comprendido entre 25 y 34 años donde el 67.3% son usuarios. Otro dato de mucha importancia para este proyecto es que este estudio revela que, del porcentaje de usuarios de Internet a nivel nacional, el 54.1% accede desde su hogar, especialmente en el área urbana donde se mantiene el hogar como lugar de acceso predilecto con el 59.5%, mientras que el mayor porcentaje de usuarios de la población en el área rural lo hace desde centros de acceso público (36.8%) [5]. Estos lugares son usualmente gestionados por fundaciones sin fines de lucro, cuyo objetivo principal es brindar un servicio a las comunidades donde el acceso a Internet es

limitado o nulo. Además, los principales consumidores son precisamente de edad escolar que usan la conexión para realizar tareas e investigaciones de sus respectivos centros educativos.

Internet es, además una ventana para la libre expresión de sus usuarios a través de una inmensa diversidad de formatos multimedia, entre las cuales se incluyen textos, videos, audios, gráficos, fotos, etcétera. Es por esta razón que a más de su increíble utilidad didáctica, representa también un peligro en la medida que el contenido generado por los usuarios no es regulado por ningún ente superior, ocasionando que se puedan hallar diversas fuentes no apropiadas como violencia, sexualidad, discriminación, ciberacoso, entre otros, para los infantes.

Así mismo, el acceso a sitios web no apropiados pone en peligro los dispositivos de la red LAN y puede ocasionar la pérdida total de los equipos, por lo cual es clave la implementación de herramientas de control que diferencien el tipo de tráfico, las páginas web visitadas y la actividad realizada por el usuario con lo cual se evitará tanto el daño emocional como los perjuicios económicos por la pérdida de equipos.
Tecnológicamente, estos controles pueden aplicarse en distintas capas del modelo de Interconexión de Sistemas Abiertos (OSI) y el desempeño dependerá entre otros parámetros del tipo de tráfico a bloquear, su fuente y destino.

Cabe precisar que el filtrado del contenido web requiere de sólidos conocimientos teórico-prácticos en el área de las tecnologías de información y comunicación (TIC), de los protocolos involucrados en la navegación y mediante la definición de reglas de acceso o denegación de tráfico y servicios en los dispositivos de pasarela en una red, lo cual, en términos económicos representa gastos extras por la adquisición de hardware, software y la contratación de servicios profesionales.

Este documento presenta la planificación, el diseño y la implementación de un dispositivo con la capacidad de configurar perfiles de filtrado de navegación para una red interna de modo que sean aplicados de forma sencilla por un usuario

supervisor que podría ser una madre de familia, un profesor, o un responsable de laboratorio en una fundación, utilizando un esquema con hardware de bajo costo y software libre.

1.1. Descripción del problema

Internet es una fuente de información inmensamente diversa y abierta a cualquier usuario que disponga de una conexión de acceso y un dispositivo capaz de conectarse a ella. Esto significa que cualquier persona tiene opción de ingresar a cualquier sitio web disponible en Internet, y en el otro extremo, cualquier usuario puede utilizar su conexión a Internet para publicar cualquier tipo de información y contenido que desee. Es decir que, en términos generales, no existen políticas de restricción implementadas por defecto en los equipos de acceso, (comúnmente enrutadores) para el control de acceso y navegación, tampoco la inteligencia artificial necesaria para que los computadores puedan distinguir la edad, o características del usuario que se encuentre usándola, y de esa forma implementar las restricciones basados en esta variable.

La falta de control sobre la navegación permite que personas de todas las edades puedan acceder a cualquier tipo de contenido (información), incluyendo software malicioso y/o sitios inapropiados. Esto hace que el público especialmente vulnerable sean los menores de edad puesto que gran cantidad de sitios web con contenido no apropiado pueden ser accedidas de manera fácil e incluso sin una solicitud expresa del usuario, en el caso de las publicidades o pop-ups. Las redes sociales, por otro lado, nos ofrecen conocer gente de todo mundo, exponer nuestras actividades diarias, nuestra vida personal y nuestras ideas, información que puede también ser utilizada por personas inescrupulosas para establecer contacto con menores.

Los dispositivos actuales, proveen cierta capacidad limitada para configurar permisos por usuarios o direcciones IP, pero ellos no poseen

por si mismos la inteligencia para detectar de forma dinámica las características de los diferentes usuarios que pueden estar navegando y por ello, no aplican reglas de acceso o restricción para el contenido de las páginas web de acuerdo con esta variable. Por lo que, aunque en una red es posible implementar mecanismos de filtrado de contenido web, realizarlo requiere de sólidos conocimientos teóricos y prácticos en tecnologías de la información, lo que supone entonces, la intervención de personal capacitado, que resulta costoso a nivel de recursos.

Los principales lugares donde se generan incidencias son entonces, aquellos que proveen una conexión de acceso a Internet para múltiples usuarios, donde a la vez se carece de personal capacitado en el área de tecnologías de la información. Estas condiciones se cumplen especialmente en hogares de familia donde hay menores de edad o en fundaciones que brindan conexión internet a usuarios en zonas demográficas de poco acceso o vulnerables de una cuidad. Las redes en estos sitios son administradas por padres de familia, supervisores de laboratorio, tutores, o en términos generales, personas sin mucho conocimiento técnico.

1.2. Justificación del problema

Existen organizaciones que no tienen suficiente presupuesto para poder controlar el acceso a Internet y necesitan soluciones de bajo costo, por ejemplo, las fundaciones sin fines de lucro que brindan servicio de Internet a diferentes usuarios y con un presupuesto limitado para sus actividades. Uno de los principales aportes de estas fundaciones a la comunidad es el servicio de Internet mediante sus laboratorios y mediante Wi-Fi, en esta última los usuarios de la comunidad llevan consigo sus dispositivos a las instalaciones de la fundación y con ellos acceden al servicio. En ambas modalidades, las fundaciones tienen la responsabilidad de brindar un servicio seguro, ya que el Internet, como se menciona en la sección anterior, no posee restricciones de acceso, por lo que de manera sencilla se puede acceder a contenido inapropiado de

diferentes fuentes y formas, sean estos: gestos obscenos, sexo explícito, erotismo, violencia, crueldad, odio, prácticas ilegales o drogadicción. Cualquiera de estos temas puede, de una u otra manera, influir de forma negativa en el desarrollo personal de los usuarios, sin mencionar que, de manera involuntaria, también se puede descargar de modo automático, es decir, sin ser solicitado explícitamente por el usuario, contenido malicioso en forma de malware, virus, y en ciertas ocasiones, mantener contacto con usuarios malintencionados por medio de mensajería instantánea, foros, correos electrónicos o redes sociales.

En base a esto se considera importante aplicar restricciones a ciertos contenidos o sitios web considerados inapropiados. Las fundaciones que no cuentan con personal que tengan conocimiento técnico tienen la necesidad de contratar personal capacitado en este ámbito, para prevenir o corregir problemas que este contenido malicioso pueda causar, sin embargo, en ambos casos esto genera un costo adicional fuera de su presupuesto.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar un dispositivo de fácil uso que permita el control de acceso a Internet mediante la implementación de categorías básicas de filtrado utilizando hardware de bajo costo y software libre para usuarios con poco conocimiento en el área de las tecnologías de la información y comunicación.

1.3.2. Objetivos Específicos

1. Proporcionar filtrado web en una red LAN usando hardware de bajo costo y software libre.
2. Disminuir el riesgo de exposición de los usuarios vulnerables a contenido malicioso e inapropiado.
3. Controlar el contenido al cual los usuarios tendrán acceso según las diferentes categorías de navegación implementadas.

4. Facilitar a los usuarios, el establecimiento de la conexión y los cambios de categorías de navegación con la ayuda de un dispositivo de uso sencillo e intuitivo.
5. Reducir la probabilidad de que los ordenadores de una red interna sean afectados por software dañino.

CAPÍTULO 2

2. METODOLOGÍA

Para el desarrollo de este proyecto la metodología “Pensamiento de Diseño” (D.T. del inglés “Design Thinking”) ha sido empleada. Mediante las herramientas propuestas por este método, se ha logrado conocer los problemas y las necesidades experimentadas por el Centro de Desarrollo Integral 314 (CDI-314) “Nueva Vida” de la fundación Compassion International. En el laboratorio de cómputo del CDI-314 los habitantes de la comunidad cuentan con acceso a Internet de manera gratuita.

A través de las herramientas de análisis empleadas sobre la información obtenida y producto de la aplicación del método DT, se han planteado diferentes soluciones para el bloqueo de contenido malicioso o inapropiado y a su vez que cumplan con las expectativas de la fundación tanto a nivel de recurso humano y financiero.

2.1. Desarrollo de la Metodología

2.1.1. Fase 1: Empatizar.

De manera preliminar se realizó una visita a las instalaciones de la Fundación CDI-314, donde se evidenció que posee un laboratorio informático equipado con 10 computadoras, 7 aulas con pizarra y 9 tutores voluntarios de planta. Se usó como herramienta para recolección de información, la técnica de observación dirigida. Determinamos su estructura organizacional y las actividades que realiza como: servicios a la comunidad, horarios de funcionamiento, personas responsables de brindar asesoramiento a los usuarios y su conocimiento técnico. Así como, el rango de edades de los beneficiarios y actividades que realizan los usuarios con mayor frecuencia. A partir de lo antes mencionado, se construyó un mapa de actores, tal como se puede observar en la Figura 2.1, donde se detalla las personas involucradas y los grupos de interés que tienen relación directa o indirecta con la problemática.

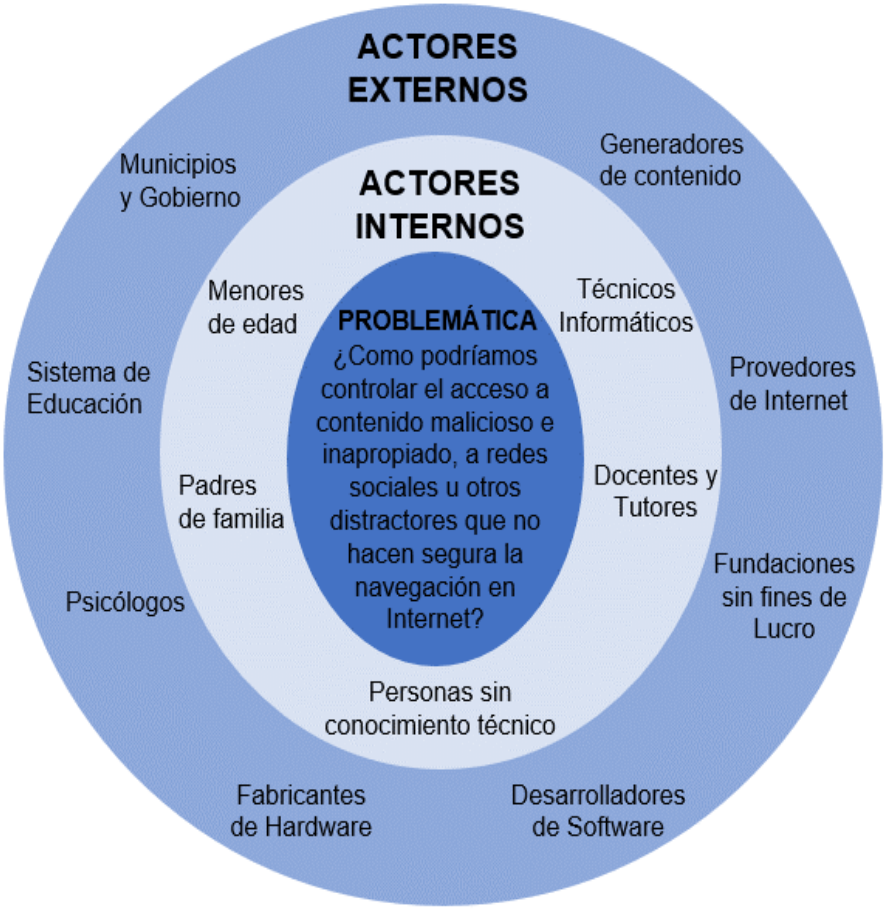

Figura 2.1 Mapa de Actores [Autoría Propia].

Posteriormente, se realizó una visita de campo para comprender de primera mano la operación normal de la fundación. Adicionalmente, se pudo validar durante las visitas realizadas el comportamiento de los usuarios, los horarios de más afluencia, la disposición de los puestos de trabajo y de los dispositivos de red. Para la recolección de información se elaboraron formatos de entrevistas con 11 preguntas semiestructuradas (Ver ANEXO 1), así como, encuestas con preguntas cerradas basadas en la problemática que involucra el acceso libre a Internet (Ver ANEXO 2), en sitios con conexiones de fundaciones o entidades de ayuda comunitaria, donde muchos menores de edad acceden para realizar sus tareas. Tomando como referencia el mapa de actores se determinó los perfiles de las personas a entrevistar. En primera instancia, se seleccionó tres perfiles de actores internos. Luego, de cada perfil se escogió a cinco personas, en este caso, cinco usuarios, cinco trabajadores de la fundación y cinco padres de familia.

A continuación, la Tabla 2.1 muestra un detalle de los perfiles seleccionados para las entrevistas y encuestas.

Tabla 2.1 Perfiles de los entrevistados [Autoría Propia].

CARGO	CATEGORÍA PROFESIONAL	RESPONSABILIDADES
Estudiantes	Estudiantes de primaria y secundaria.	Conservación adecuada de las instalaciones, no utilizar programas de descarga de archivos, música, etc.
Padres de Familia	Diversas.	Uso adecuado de las instalaciones y dispositivos, no acceder a sitios web que tengan restricción de edad como pornografía, violencia explícita, entre otros.
Docentes/Tutores	Ayudante titulado en otras profesiones diferentes de las Tecnologías de la Información	Supervisar el buen uso de las instalaciones y dispositivos utilizados el servicio brindado.
	Ayudante no titulado	

Como resultado obtenido, tenemos que el desconocimiento de cómo llevar un control sobre la navegación web que trae consigo algunas consecuencias, por ejemplo, la descarga de virus por visitar sitios infectados, robo de información, suplantación de identidad, adicción a las redes sociales o juegos en línea, entre otras. Así mismo hemos despertado el interés en la Fundación y en los usuarios de como poder mantenerse inmune ante la variedad de contenido inapropiado y perjudicial que se encuentra en la red. Para más detalles de los resultados de las encuestas ver los gráficos y conclusiones individuales de cada pregunta en el ANEXO 3.

En las entrevistas realizadas a estudiantes, hemos podido ver su inquietud con respecto al tema de contenido inapropiado, aunque conocen que estas páginas existen y afirman haber tenido incidentes con ellas, no tienen conocimiento de cómo proceder ante estos casos, ni cómo evitar que vuelvan a ocurrir. Su lenguaje no verbal es muy expresivo, demuestran inquietud por las preguntas realizadas y curiosidad por las soluciones que se pueden plantear, al mismo tiempo reconocen que es conveniente realizar restricciones específicas en el servicio.

De las entrevistas realizadas a padres de familia, un factor importante fue la entonación de frases en la conversación, el tema de contenido inapropiado es un problema serio para ellos, en vista que, buscan la menor exposición de los niños a este tipo de imágenes, audios, videos y páginas. Al mismo tiempo, su desconocimiento sobre el tema hace que se muestren un poco escépticos a la idea de poder realizar un bloqueo efectivo a bajo costo, a pesar de ello, realizaron preguntas sobre cómo funciona el bloqueo de contenido no apto para menores y su efectividad.

Por último, de las entrevistas realizadas al personal docente y tutores (Ver ANEXO 4), se enfatiza que han tenido problemas con el mantenimiento y operación de los dispositivos que han resultado infectados. Además, comentan que asegurando la restricción a contenido no deseado, se incrementaría la eficiencia en el trabajo de supervisión del laboratorio, pues podrían dedicar más tiempo en ayudar a resolver dudas de los estudiantes. Hay que mencionar, además que este grupo mostró mayor inquietud en el aspecto financiero referente a la implementación y el mantenimiento de una solución viable.

Por otra parte, las transcripciones de las entrevistas fueron analizadas para crear mapas de empatía para cada grupo de actores (Ver ANEXO 5). Además, de las respuestas de los entrevistados, estos mapas están basados en sus gestos, pensamientos, sentimientos y anhelos con respecto al proyecto y sus expectativas.

2.1.2. Fase 2: Definir.

En esta segunda fase el objetivo principal es replantear el problema definido en la fase anterior, de manera que se ajuste a las distintas necesidades planteadas desde los diferentes puntos de vista de los actores involucrados.

El primer paso de la fase de definición es obtener un listado de insigths como se puede observar en la Tabla 2.2, los cuales son obtenidos desde una visión integral de la problemática tomando en cuenta todos los puntos de vista, donde se encuentran factores claves en común. Estos no son comunicados explícitamente por los entrevistados, pero se infieren del lenguaje no verbal observado en las entrevistas.

Tabla 2.2 Listado de Insigths [Autoría Propia].

INSIGTHS
El acceso a contenido inapropiado es perjudicial para el desarrollo social y psicológico de los niños, además despierta curiosidad en temas que para su edad no son adecuados.
El contenido malicioso en Internet tiene diferentes formas de camuflaje, y puede ocasionar una gran diversidad de problemas en los sistemas.
La adicción a redes sociales o juegos en línea puede ocasionar que los individuos dejen de hacer cosas propias de su edad, aislándose de su entorno social.
El desconocimiento de las herramientas que ofrece un navegador de Internet es una constante en la mayoría de las personas de edad avanzada, por lo que pueden ser engañados fácilmente por los menores ocultando su actividad en Internet.

Otro de los objetivos de la etapa de definición es bosquejar una matriz de “Punto de Vista” (P.O.V. del inglés “Point of view”) a través de la cual se declara las necesidades y los insigths según el enfoque particular de un usuario específico. Para estos fines, en este proyecto se ha seleccionado al usuario Dante Martínez cuyo perfil se detalla a continuación:

Nombre: Dante Martínez

Descripción: Es una persona que se encarga de guiar a niños, niñas, adolescentes y jóvenes en diferentes áreas, tales como: emocional, económica, espiritual y escolar. El rango de edad se encuentra entre 20 y 50 años. Cree firmemente en Dios, por lo que las bases de su enseñanza son Cristo céntricas. Carece de conocimiento en el área de las tecnologías de la información, de manera que, no está informado de todos los peligros que se pueden encontrar en Internet. También es un padre de familia que está consciente que el uso excesivo o indebido del Internet puede traer grandes consecuencias en la vida de sus hijos, pero a pesar de esto desconoce totalmente como puede prevenir o controlar este problema.

Tabla 2.3 Matriz Punto de Vista [Autoría Propia].

POINT OF VIEW				
USUARIO	**+**	**NECESIDAD**	**+**	**INSIGTH**
Dante Martínez	NECESITA	Evitar el uso de la infraestructura para acceder a contenido inapropiado	POR QUE	El acceso a contenido inapropiado daña la mente de los niños y despierta curiosidad en temas que para su edad no son adecuados.
	NECESITA	Mantener el equipamiento informático libre de amenazas que puedan obstruir el correcto funcionamiento de este.	POR QUE	El contenido malicioso en Internet tiene diferentes formas de camuflaje, y puede ocasionar una gran diversidad de problemas en los sistemas.
	NECESITA	Tener control del horario de uso del Internet considerando diferentes perfiles de usuarios de acuerdo con su edad.	POR QUE	La adicción a redes sociales o juegos en línea puede ocasionar que los individuos dejen de hacer cosas propias de su edad, aislándose de su entorno social.
	NECESITA	Tener más conocimiento acerca de cómo funcionan los navegadores de Internet, y que se puede o no hacer para proporcionar una navegación en Internet segura y fiable.	POR QUE	El desconocimiento de las herramientas que ofrece un navegador de Internet es una constante en la mayoría de las personas de edad avanzada, por lo que pueden ser engañados fácilmente por los menores ocultando su actividad en Internet.

A partir de las ideas de la matriz POV, el siguiente paso realizado fue la redefinición de la problemática. En las necesidades extraídas de la Tabla 2.3, se puede apreciar que una de las preocupaciones existentes es la del daño que se pueda causar a los equipos informáticos por el fácil acceso a virus que tienen estas páginas. Otro factor importante es la preocupación de que los usuarios pudieran ser expuestos a la adicción a redes sociales o juegos en línea, lo que pudiera ocasionar aislamiento de la comunidad.

Por otro lado, muchas de las conexiones a Internet donde usuarios vulnerables se conectan están administradas por padres de familia, supervisores de laboratorio, tutores, o en términos generales, personas sin mucho conocimiento técnico, por lo que la implementación, modificación, actualización, personalización y mantenimiento de los equipos que el mercado ofrece como soluciones en la actualidad resulta de inmensa complejidad para ellos, razón por la cual prefieren evitar la utilización de los mismos.

2.1.3. Fase 3: Idear.

En esta sección se realizó la concepción de ideas de las cuales se determinaría las más óptimas para solventar el problema descrito en párrafos anteriores, para esto elaboramos una lluvia de ideas utilizando la técnica “Seis sombreros para pensar” de Edward de Bono [6]. Se generaron diversas ideas, de las cuales las más destacadas se detallan a continuación:

- Cambiar en los ordenadores el sistema operativo a Linux para reducir el riesgo de los virus y evitar que los usuarios instalen aplicaciones.

- Crear un sistema de autenticación en el dispositivo mediante huella dactilar antes de elegir los perfiles mencionados para que los niños no puedan acceder.

- Diseñar un ratón con lector de huellas digitales para poder detectar la edad del usuario antes de iniciar sesión en los ordenadores y a su vez de manera automática se realice el bloqueo de contenido inadecuado según un perfil establecido por su edad.

- Mostrar siempre al iniciar sesión un video educativo que le recuerde al usuario que no debe compartir contraseñas, descargar archivos ejecutables entre otros y si no se culmina la visualización del video no se permita el acceso a Internet.

- Mostrar los escritorios de los usuarios en un ordenador central donde un docente o tutor pueda monitorear la actividad de los usuarios.

La lluvia de ideas realizada sirvió en gran medida para que las propias ideas se retroalimentarán entre sí, proyectando una visión más robusta y completa de la solución a proponer. Las ideas mencionadas destacan de las demás por las ventajas que ofrecen en términos de eficiencia, optimización de recursos, (menor complejidad de configuración y mantenimiento, el costo), la tecnología que emplea, entre otras.

El siguiente paso fue seleccionar las ideas que destacaban, y a partir de estas se elaboró la matriz de importancia – dificultad (Ver ANEXO 7), en la cual clasificamos las ideas con el fin de establecer las soluciones que presentasen mayor viabilidad y pertinencia con los problemas específicos y necesidades expresadas en pasos anteriores.

Se elaboró a partir del análisis realizado una matriz de decisiones (Ver ANEXO 8), sometiendo las ideas a puntuaciones en un rango de 1 a 5, donde se calificaba la idoneidad de las soluciones basadas en las necesidades determinadas, otorgándole un puntaje de 5 a la solución más factible y eficaz, y 1 la solución menos viable.

El análisis del resultado de la matriz de decisiones determina cuales son las soluciones más convenientes. Sobre las mismas se realizará un prototipo en la siguiente fase. Los resultados demostraron que para nuestro caso las dos soluciones más adecuadas son:

a. Implementación de un servidor Proxy en el laboratorio de la fundación.

b. Implementación de un dispositivo para filtrar la navegación web con hardware de bajo costo y software libre.

Las ideas mencionadas anteriormente se procederán a desarrollar en la siguiente fase llamada Prototipar.

2.1.4. Fase 4: Prototipar.

Considerando que la solución planteada referente a la instalación de un servidor Proxy es un servicio, para la realización del prototipo del mismo se creó un diagrama de red que explica su funcionamiento, el mismo se muestra en la Figura 2.2.

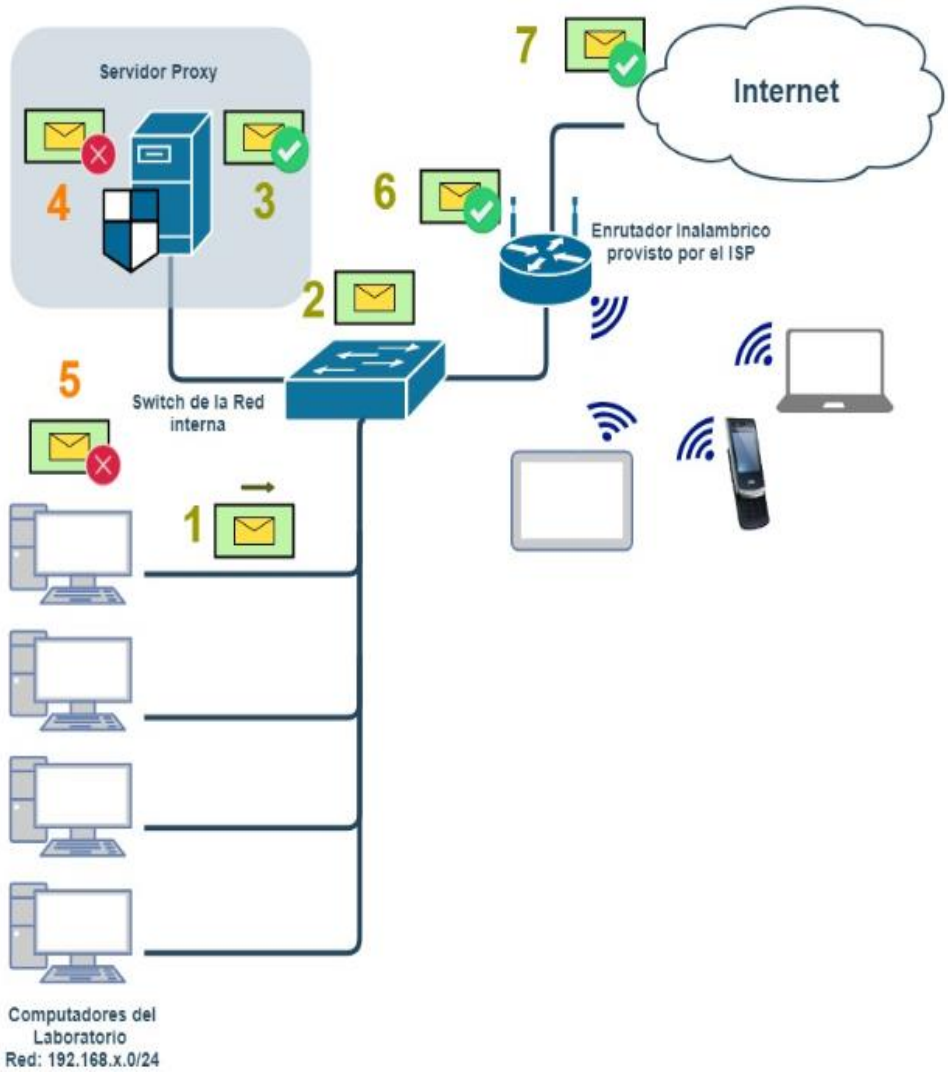

Figura 2.2 Diagrama de red de servidor proxy para la fundación CDI-314 [Autoría Propia].

- Paso 1: Uno de los computadores del laboratorio inicia una solicitud para la carga de una página web. El computador solicitante tiene configurado el proxy, por lo que la solicitud HTTP (Protocolo de Transferencia de Hipertexto), se realizara en primera instancia al proxy.

- Paso 2: El paquete llega al Switch de la red interna donde en base a su destino, reenvía el paquete hacia el Servidor proxy.

- Paso 3: El proxy consulta que URL se pretende cargar y determina si esta, se encuentra entre sus listas de páginas denegadas, de ser así, continua al paso 4, caso contrario se salta al paso 6.

- Paso 4: Consiste en determinar que el sitio web se encuentra en una de las listas de denegación por lo que no será cargada.

- Paso 5: Se devolverá la solicitud al computador mostrando un mensaje personalizado indicando que el sitio fue bloqueado por el proxy y se finaliza el proceso con este paso.

- Paso 6: La solicitud es reenviada a la puerta de enlace para que el router que el ISP (Proveedor de Servicios de Internet) ha instalado en el laboratorio como Gateway (modelo y marca son dependientes del servicio contratado y del proveedor) lo enrute hacia la nube.

- Paso 7: La conectividad es establecida con el servidor web de la página de modo que la misma cargará correctamente en el dispositivo solicitante.

Por otro lado, cabe destacar que, a pesar de la relativa facilidad en el funcionamiento de la solución, su principal desventaja es el costo que conlleva su implementación, ya que se debe considerar la adquisición de equipos, el mantenimiento y configuración, los honorarios de los profesionales a cargo de esta solución y de forma adicional el hecho de que para implementar cualquier actualización en las listas de denegación, el personal encargado en sitio deberá tener conocimiento sobre cómo manipular el servidor. Es por la razón mencionada que se ha considerado esta solución como la menos factible por lo tanto quedó descartada.

En cuanto al prototipado de la segunda solución tomada en cuenta, que conlleva la implementación de un dispositivo para filtrar la navegación

web con hardware de bajo costo y software libre, como primer paso, se elaboró un bosquejo rápido de cómo podría quedar la parte física del dispositivo, para estos fines se usó la herramienta informática Paint3D [7]. La Figura 2.3 hace referencia al prototipo de bajo nivel que se elaboró, en la sección A se muestra la parte frontal del dispositivo, en la sección B se puede observar los puertos que se encuentran ubicados en la parte lateral y en la sección C se puede ver el prototipo desde una perspectiva adecuada para apreciarlo en tres dimensiones.

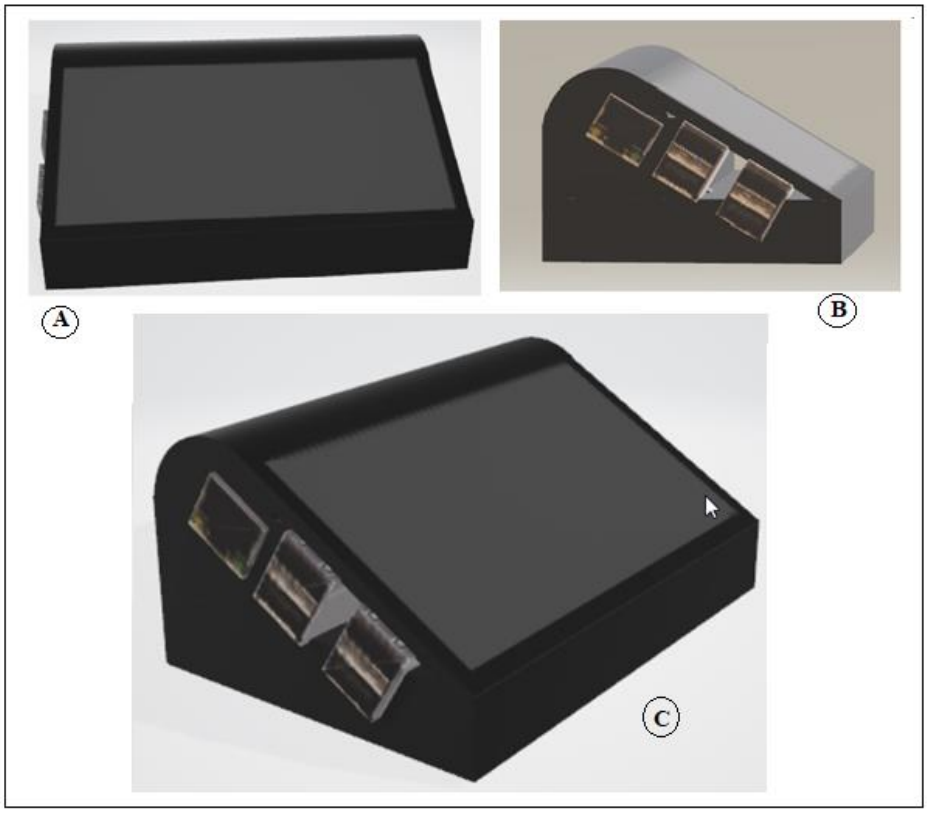

Figura 2.3 Prototipo de bajo nivel del dispositivo [Autoría Propia].

2.1.5. Fase 5: Evaluar.

Para esta fase se coordinó una reunión con los diferentes actores internos de la problemática planteada, en donde el prototipo fue presentado para que lo puedan observar y dar sus opiniones. Entre las observaciones se mencionó que el color no es de su agradado, la forma circular en la parte superior no se ve bien estéticamente y que falta que se vea un poco más elegante.

Además, otra de las sugerencias fue la de poner unos pequeños soportes como base para que el plástico del case tuviera cuatro puntos de apoyo al ubicarlo sobre cualquier superficie y al mismo tiempo, tener la posibilidad de poder colocarlo en la pared.

Para la parte de la interfaz gráfica se diseñaron ventanas en donde por medio de un Storyboard Navegacional se procedió a explicar el funcionamiento del prototipo.

El diseño fue aceptado por la mayoría debido a su fácil uso e interacción. Se solicitaron sugerencias adicionales por parte de docentes y tutores, estos nos indicaron que sería recomendable aplicar alguna categoría para videojuegos en donde estén los más comunes de hoy en día.

Luego, con todas estas recomendaciones se procedió a elaborar prototipo de alta resolución (los detalles acerca de este proceso serán especificados en el Capítulo 3: Diseño de la solución). Para poder realizar la validación del prototipo de alta resolución nos reunimos con los diferentes usuarios involucrados: padres de familia, docentes, tutores, adolescentes y jóvenes, ya que para el proyecto resulta muy importante conocer la impresión de los usuarios.

La reunión se desarrolló agrupando a los diferentes actores y dándoles el prototipo encendido sin explicarles cómo funcionaba, a lo cual tuvimos una buena respuesta ya que la mayoría de los usuarios no tuvo mucha dificultad para manejarlo. Esta actividad permitió, de una manera sencilla, recoger información de valor según la opinión de los actores internos y así plasmar las ideas desarrolladas en una matriz de Feedback (Ver ANEXO 9) para posteriormente examinar los aspectos positivos y negativos de la retroalimentación.

CAPÍTULO 3

3. DISEÑO DE LA SOLUCIÓN

La solución planteada consiste en un dispositivo de pasarela, que realice el control y el filtrado de contenido web inapropiado al tráfico generado por los dispositivos conectados a una red LAN (Red de Área Local). Los principales requerimientos para este diseño han sido: proveer una plataforma de configuración simple, eficaz, confiable y a bajo costo. El dispositivo diseñado es un intermediario en la comunicación entre la red de área local y el Internet. Esta ubicación estratégica le permite ser el encargado de inspeccionar el contenido de las conexiones establecidas entre ambas partes para determinar si existe alguna amenaza o algún contenido considerado inapropiado de forma que la ejecución o presentación del mismo pueda ser evitada.

Al dispositivo diseñado se lo ha nombrado MiPiBlock y presenta a nivel de aplicación, un programa que cuenta con perfiles de bloqueo predefinidos y listas de sitios aceptados y denegados precargadas de forma que el usuario solo deba elegir el nivel de restricción que desea implementar en su red y este será inmediatamente aplicado. De esta misma forma cuenta con la opción de agregar páginas a las listas de sitios denegados definidas por defecto, alimentando así la capacidad de protección de los perfiles predeterminados. Otra característica importante es la capacidad de realizar un bloqueo total del acceso a internet de uno o varios dispositivos determinados.

La Figura 3.1 y Figura 3.2 muestran una explicación a nivel básico y general del funcionamiento del dispositivo en el escenario de una red de un domicilio para el manejo de tráfico permitido o denegado respectivamente. Una explicación más extensa, técnica y detallada puede ser consultada en la sección dos de este capítulo: “Diseño del Software”.

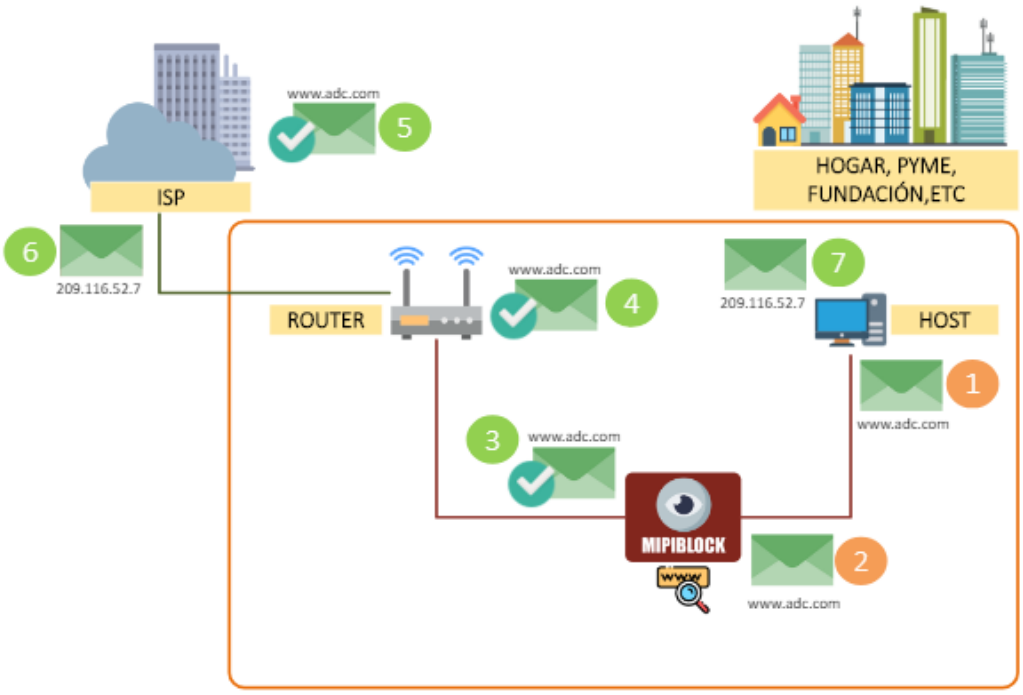

Figura 3.1 Esquema de manejo de tráfico permitido de Mipiblock [Autoría Propia].

1. En el primer punto se describe la petición que realiza un computador para la carga de una página web, por ejemplo www.adc.com.
2. Los paquetes que conforman la petición son direccionados al Gateway. MiPiBlock usará ARP (Protocolo de Resolución de Direcciones) spoofing, un mecanismo que envía mensajes falsos a nivel de Ethernet [8].
3. Luego de recibir este tráfico MiPiBlock redirecciona todas las peticiones DNS hacia su propio servidor local DNS (Dnsmasq). Se procede a comparar el dominio contra los perfiles y configuraciones de bloqueo definidas por el usuario final. MiPiBlock determina que la petición es aceptada y el paquete será reenviado hacia el enrutador.
4. El enrutador direcciona el paquete hacia el Internet.
5. La conexión con el sitio web es establecida.
6. El servidor DNS le responde con la IP asociada al dominio solicitado.
7. El paquete llega al usuario y se carga la página web.

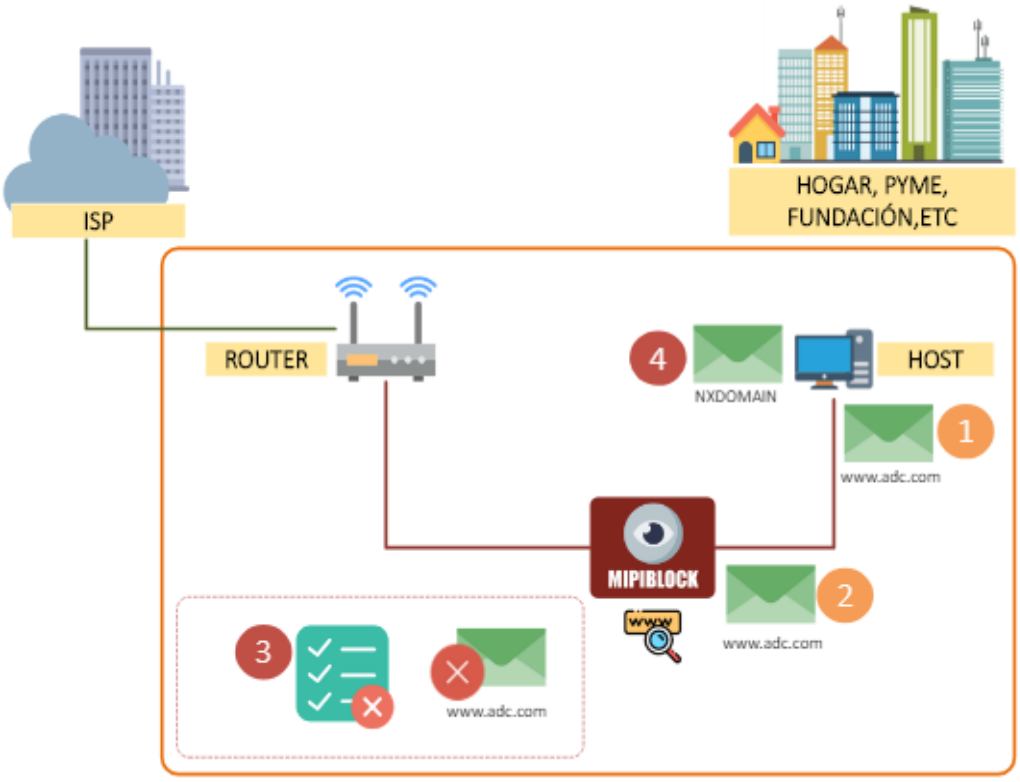

Figura 3.2 Esquema de manejo de tráfico denegado de Mipiblock [Autoría Propia].

En el caso del tráfico denegado los pasos 1 y 2 son los mismos que en el escenario del tráfico permitido. En el paso 3 MiPiBlock realiza una búsqueda del sitio web solicitado por el usuario en las listas de denegación que posee el perfil en ejecución. Después de haber encontrado la coincidencia, se deniega la petición, y finalmente en el paso 4 se envía al dispositivo solicitante un mensaje nxdomain indicando que el dominio solicitado no existe y a su vez el paquete se descarta.

El diseño de este ha sido elaborado tomando en cuenta consideraciones en dos principales áreas: hardware y software. A nivel de hardware se ha considerado como factores importantes las medidas de longitud, la geometría, el peso, y los componentes necesarios que facilitarán al usuario principal, que pudiera ser un supervisor de un laboratorio, la capacidad de manipularlo, instalarlo, conectarlo, encenderlo y apagarlo de forma rápida y con poco esfuerzo. A nivel de Software, se ha diseñado el aplicativo con el objetivo principal de ser intuitivo, visual,

atractivo y cómodo, de forma que el usuario pueda hacer uso de este sin tener conocimientos profundos a nivel de redes y sistemas operativos. Uno de los factores importantes tomados en consideración es la simplicidad de uso, en términos de que la ejecución de una directriz o acción no tome más de 4 toques o interacciones del usuario, exceptuando el caso de la configuración o personalización de listas, en las que dependerá de la complejidad de los parámetros que el usuario configura. En los siguientes puntos se describe más a detalle los componentes utilizados en cada una de estas dos áreas, su utilización, y su funcionamiento a nivel individual y en general para el dispositivo final.

3.1. Hardware.

A nivel de hardware MiPiBlock tiene como base estructural un Raspberry Pi 3 modelo B+, que es un computador de placa simple y bajo costo diseñado especialmente para la enseñanza [9]. La Raspberry está compuesto de 4 puertos USB 2.0 que pueden ser usados para actualización de software, recolección de datos o logs para respaldos o verificación de incidentes. La Raspberry Pi cuenta también con un puerto Gigabit Ethernet incorporado y la capacidad de usar los puertos USB con la tecnología Gigabit Ethernet Over USB 2.0 para ampliar la capacidad de conexión física. Otro de los componentes importantes para el funcionamiento del dispositivo es una tarjeta de memoria Micro SD que tiene alta capacidad de escritura y lectura para un mejor rendimiento, la misma se inserta en la Raspberry Pi y sobre la cual estará instalado el aplicativo de MiPiBlock. La Figura 3.3A presenta la parte frontal de la Raspberry Pi 3 modelo B+ mientras que la Figura 3.3B muestra la parte posterior del dispositivo donde podemos observar la tarjeta MicroSD insertada.

Figura 3.3 Raspberry Pi 3 Modelo B+ [9]

La Raspberry Pi cuenta también con una interfaz de conexión HDMI (Interfaz Multimedia de Alta Definición), la misma que para el caso particular del diseño de MiPiBlock será utilizada para la conexión de una pantalla táctil resistiva modelo GeekPi de 5 pulgadas (480x800p), la misma que se puede apreciar en la Figura 3.4 [10] . Esta será la única interfaz de interacción con el usuario.

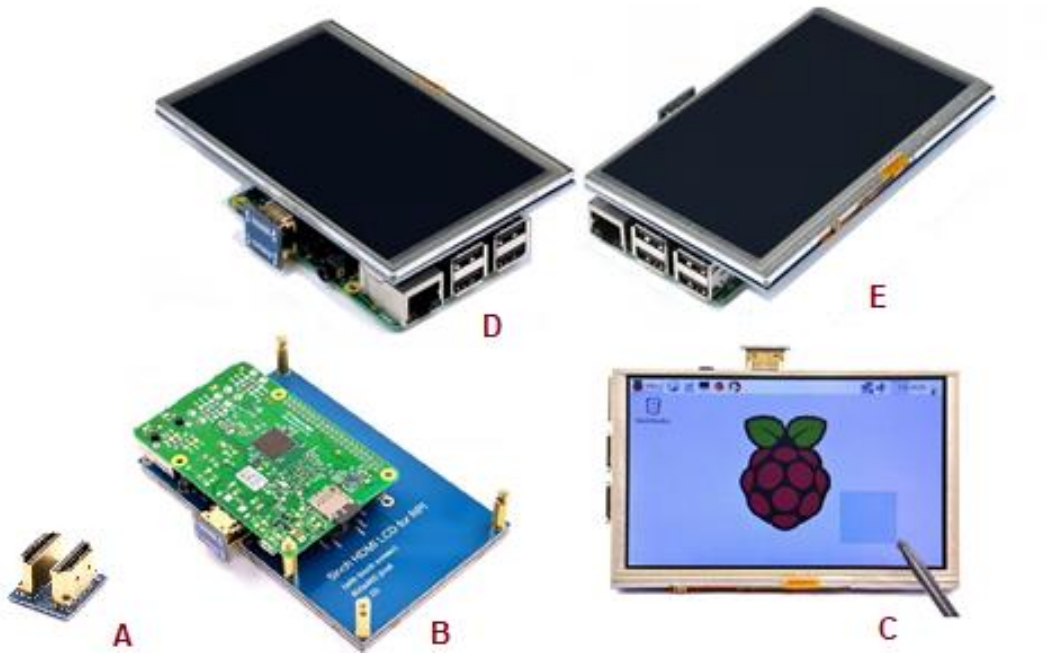

Figura 3.4 Pantalla touchscreen GeekPi de 5 pulgadas. [10]

La pantalla táctil se conecta a la Raspberry Pi mediante el uso de un adaptador HDMI, el mismo que está conformado por dos puertos HDMI

ubicados en posición contraria el uno del otro sobre un circuito impreso (Figura 3.4A), de esta forma este dispositivo sirve para unir el puerto HDMI de la Raspberry con el puerto HDMI de la pantalla, mismos que estarán ubicados uno sobre otro como se puede ver en la Figura 3.4B, las secciones C, D y E de la Figura 3.4 muestran la pantalla desde diferentes ángulos. Además de la conexión de ambos puertos HDMI, para el correcto funcionamiento de la pantalla táctil es necesario conectar la misma a los puertos GPIO de la Raspberry Pi, la Figura 3.5 muestra un esquema contemplando ambas conexiones.

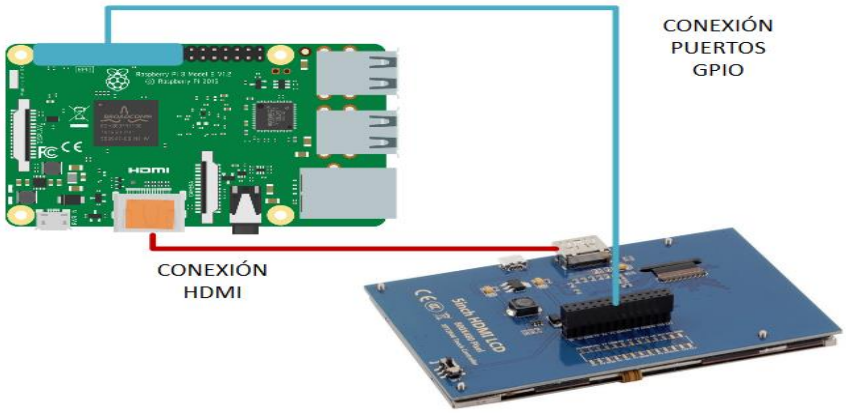

Figura 3.5 Esquema de conexión Raspberry Pi 3 y Pantalla GeekPi [Autoría Propia].

El dispositivo cumple entonces con la premisa de ser una herramienta de protección de bajo costo de inversión inicial. Se ha seleccionado el uso de la Raspberry Pi como el computador base para este dispositivo la simplicidad a nivel de tamaño y peso, de modo que el equipo también cumple con el objetivo planteado de proveer fácil movilidad y ubicación. El procesador de la Raspberry PI (1.4GHz 64-bit quad-core) será suficiente para proveer protección a nivel de LANs domiciliarias o en este caso de la fundación.

Por otra parte, en vista que la solución contiene elementos sensibles y que no pueden estar expuestos a la intemperie pues podrían verse afectados por golpes, suciedad, polvo, sobrecalentamiento, entre otros factores, también se ha tomado en cuenta como parte de la solución la

construcción de un case plástico para cubrir el dispositivo de estos incidentes.

Para el diseño de este se ha utilizado como base las medidas en tres dimensiones de los componentes, sus características, los principales componentes que serán manipulados por el usuario (como los puertos USB, puerto Ethernet, la fuente de energía), y sus principales puntos de calor, para colocar elementos de ventilación en el case. Así mismo, se ha detallado el diseño de una tapa que será ubicada sobre la pantalla táctil para protegerla de posibles golpes ocasionados por la manipulación.

La Figura 3.6 muestra el diseño del case de MiPiBlock con sus respectivas medidas.

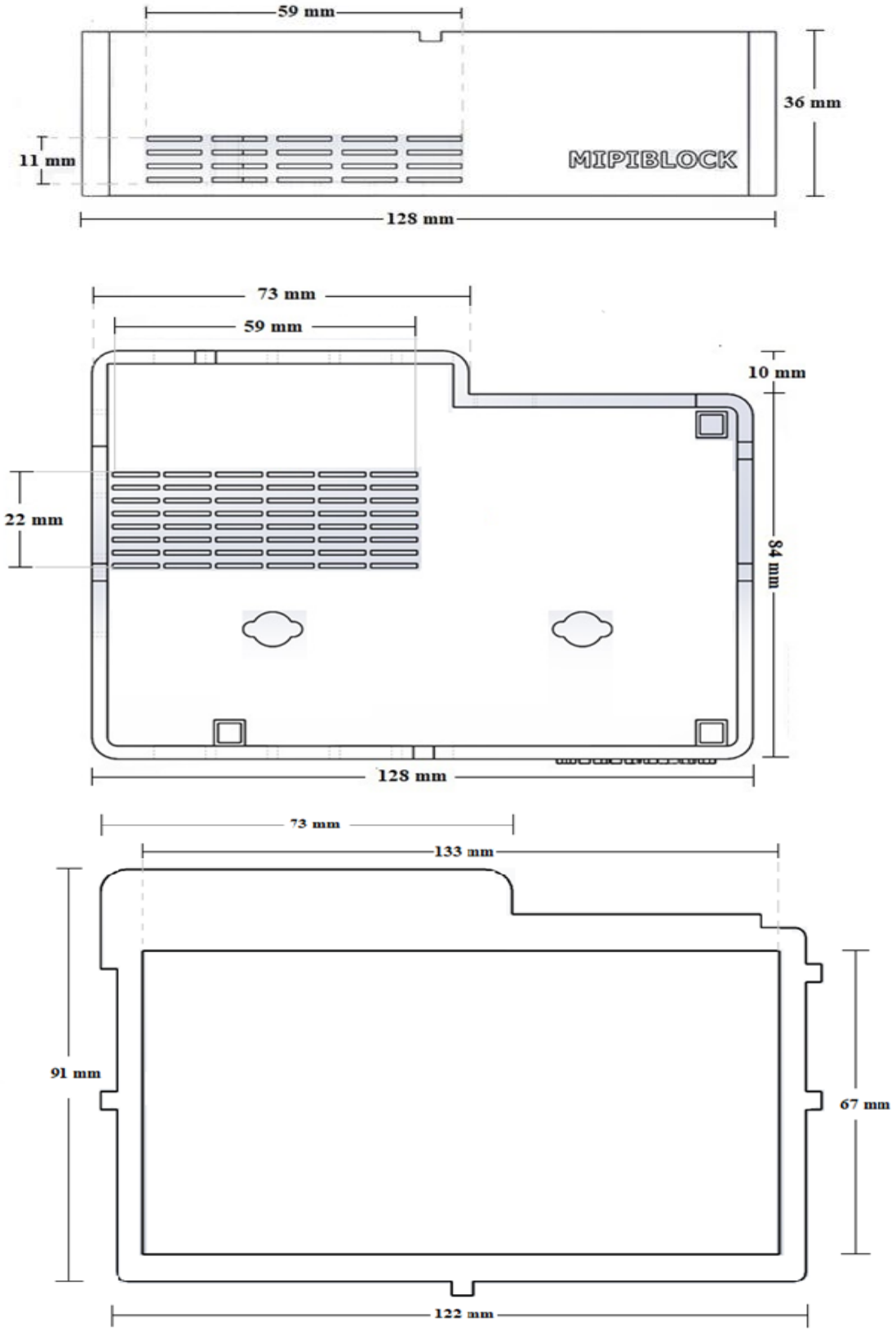

Figura 3.6 Diseño del case de Mipiblock [Autoría Propia].

De la misma manera se elaboró un bosquejo en 3D. La Figura 3.7 muestra el case diseñado en el programa de diseño 3D SolidWorks, que también ha sido impresa para elaboración del prototipo.

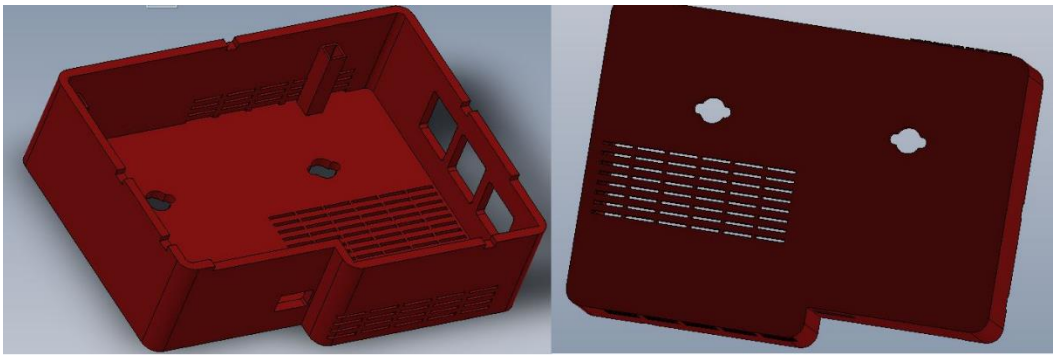

Figura 3.7 Modelo del case de MiPiBlock [Autoría Propia].

Para el usuario final, sin embargo, se busca que el dispositivo, una vez ensamblado muestre una geometría sutil y elegante, que se ajuste a todas las características mencionadas anteriormente pero que también sea atractiva a la vista y al tacto. La Figura 3.8 muestra un bosquejo del prototipo en su presentación final. Se ha buscado que el usuario tenga acceso fácil y rápido a los principales componentes que utilizará mientras administre el dispositivo como lo son los puertos USB, la interfaz Ethernet, la conexión de la fuente de poder además de que se ha recubierto los bordes de la pantalla táctil con una tapa la misma que servirá como una protección extra contra las posibles incidencias que pudiesen ocasionarse en el interior del dispositivo al estar expuesto, como rayones, polvo, suciedad, derramamiento de líquidos, u manipulación por un usuario no deseado. También se han considerado los puntos principales de calor para generar la ventilación necesaria en dispositivo de manera que el aire pueda fluir y evitar sobrecalentamientos que puedan causar daños a los componentes más pequeños del dispositivo.

Figura 3.8 Diseño de prototipo de MiPiBlock completo [Autoría Propia].

En el siguiente paso se utilizó la tecnología de impresión 3D para crear un prototipo del dispositivo y contemplar su apariencia final. Para dar mayor sobriedad y distinción al case se escogió imprimirlo en color negro, con esto, además, logramos que la apariencia del dispositivo sea pulcra. La Figura 3.9 muestra el case con los componentes ya ensamblados en su presentación definitiva.

Figura 3.9 Prototipo de Mipiblock [Autoría Propia].

El dispositivo en mención será en primera instancia instalado en el laboratorio de la Fundación Centro de Desarrollo Integral 314–Compassion International, el cual servirá para prevenir que los usuarios no ingresen a contenido no adecuado en las computadoras de la fundación evitando la descarga de virus y la exposición de los menores a este tipo de contenido. La fundación cuenta con diez computadoras que están ubicadas en el laboratorio de informática, un espacio designado específicamente para el uso de este recurso, además se cuenta con 9 tutores voluntarios que están disponibles en turnos separados en matutino y vespertino, y que cuentan con 5 escritorios, ubicados fuera del laboratorio en una zona común para los supervisores. Adicionalmente, la fundación cuenta con servicio de wifi para que los usuarios que deseen trabajar en tabletas, portátiles, teléfonos celulares entre otros puedan conectarse y realizar consultas rápidas.

La fundación cuenta con una conexión a Internet de 20 megas contratada con la compañía Netlife. El equipo Gateway es un Router Huawei con capacidades inalámbricas al que se conecta un Switch D-link de 24 puertos destinado para la red interna, las 10 computadoras. El dispositivo planteado como solución deberá entonces conectarse preferentemente al router de la red interna para que de esta forma el tráfico fluya por el mismo, facilitando la ejecución del ARP spoofing y la intercepción e inspección del tráfico para su procesamiento. La Figura 3.10 grafica la topología básica de conexión de un MiPiBlock en una red LAN.

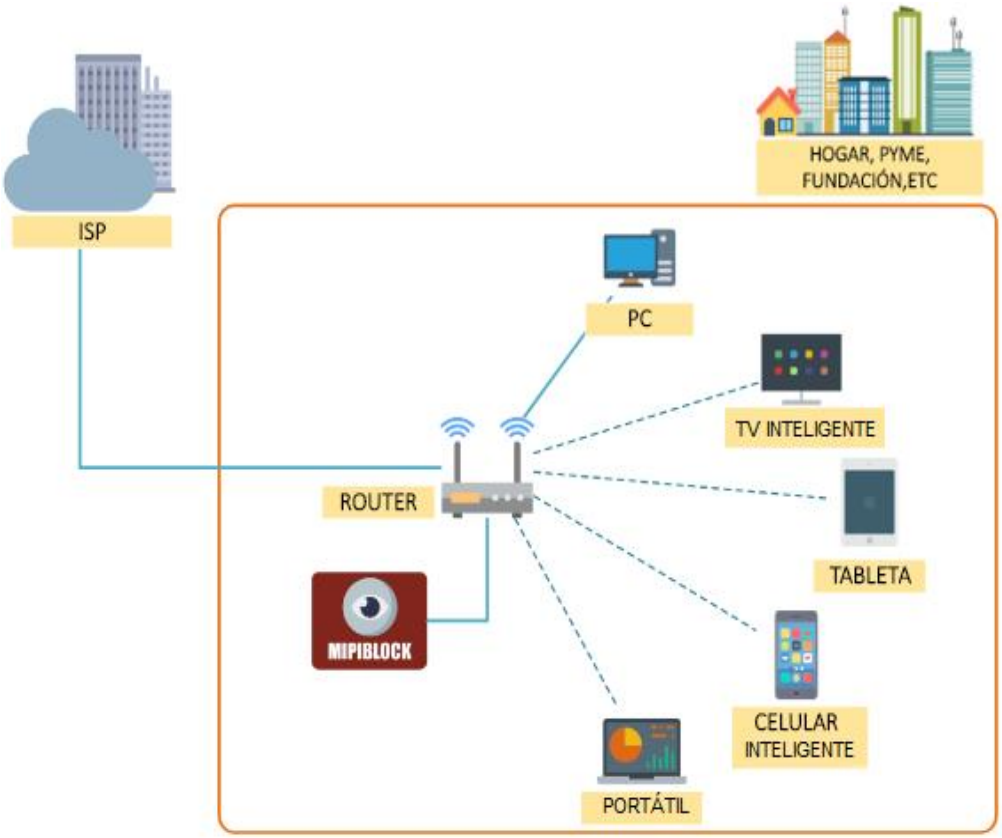

Figura 3.10 Topología de Red Básica para una fundación que usa Mipiblock [Autoría Propia].

La Figura 3.11 muestra la topología de red actual en el laboratorio y el diseño de la conexión de la solución MiPiBlock a la red interna del laboratorio.

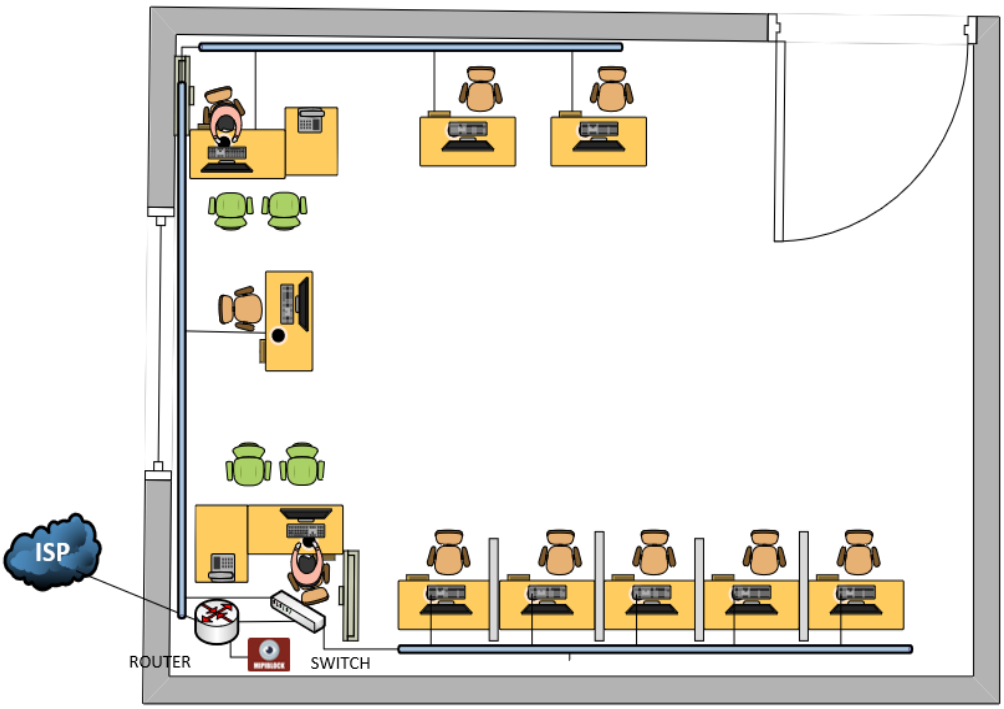

Figura 3.11 Plano del laboratorio con las conexiones de red establecidas para la solución [Autoría Propia].

3.2. Software.

A nivel de Software la solución está diseñada para mostrar una pantalla principal que a la vez sirve como menú, desde la cual el usuario tendrá simplemente que elegir y tocar la opción a utilizar de entre 6 disponibles. A nivel de aplicación, en la capa front end, la interfaz gráfica está diseñada usando la tecnología de JavaFX, el cual nos permite crear aplicaciones enriquecidas que se pueden ejecutar en diferentes plataformas [11]. En el segundo nivel se encuentra una API (Interfaz de programación de aplicaciones) la cual nos va a permitir la comunicación entre la interfaz gráfica de usuario y los servicios que ejecuta MiPiBlock.

En el tercer nivel, para los 6 módulos del menú se usarán tres servicios para el rastreo, bloqueo y/o ejecución de las reglas en ejecución: Spoof Service, Iptables, DNS proxy.

En la Figura 3.12 se mencionan las herramientas a nivel de Software usadas en MiPiBlock.

Figura 3.12 Herramientas a nivel de Software usadas en MiPiBlock [Autoría Propia].

En el core del sistema tenemos el servicio Spoof-Service, el cual tiene la finalidad de detectar los nuevos dispositivos, este servicio funcionará con el uso de NMAP, un programa utilizado para el rastreo de puertos, y para realizar una auditoría de los dispositivos en una red LAN [12]. Por medio de NMAP se detectan todos los dispositivos conectados a la red. Los equipos detectados son agregados a una base de datos creada en SQLite, [13], luego a todos los dispositivos detectados e ingresados como registros en la base de datos, se les realiza un ARP-Spoofing mediante la herramienta Scapy para que todo el tráfico pase a través del dispositivo MiPiBlock [14] . La Figura 3.13 muestra un esquema básico de funcionamiento de Spoof-Service.

El servicio de Spoof-Service forma parte de SweetSecurity [15], el cual es una herramienta que permite monitorear lo que sucede en una red doméstica de una manera similar a lo que se hace en redes a nivel empresarial.

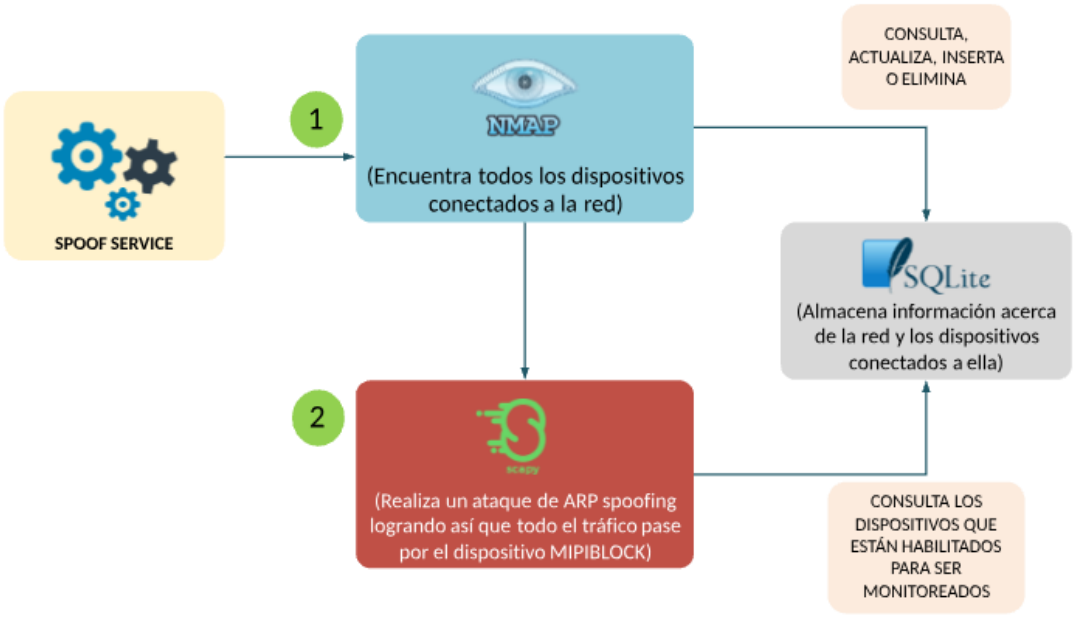

Figura 3.13 Esquema de trabajo por módulos de Spoof Service [Autoría Propia].

Una vez que se ha guardado cuales son los dispositivos conectados a la red se procederá a ejecutar un script el cual creará las reglas de Iptables para permitir el tráfico enviado por cada dispositivo. Esto, tiene como finalidad poder controlar que dispositivos pueden ser monitoreados, es decir, nos permitirá permitir o bloquear el acceso a la red en cada dispositivo encontrado.

3.2.1. MiPiBlock Menú Principal.

El dispositivo en su pantalla principal presentará 6 íconos con las opciones principales.

A. Dispositivos. Permite configurar el bloqueo por dispositivos, es decir permite aplicar reglas de filtrado a unos dispositivos y a otros no.

B. Anuncios. Se refiere la configuración del bloqueo de anuncios de marketing digital y comerciales.

C. Redes Sociales. Permite el bloqueo del ingreso a las redes sociales más conocidas.

D. Filtrado por categoría. Se permitirá filtrar por tipos de contenido, los cuales estarán separados en varias categorías como violencia, pornografía, tiendas virtuales, entre otros.

E. Bloqueo por páginas. Permite al usuario definir las páginas a ser bloqueadas agregando la URL a la lista.

F. Configuración. Muestra la información de la configuración de red del dispositivo.

La Figura 3.14 muestra la pantalla principal de MiPiBlock con sus 6 módulos del menú, cada uno representa una de las opciones de configuración que brinda MiPiBlock, por lo que una vez encendido esta será la pantalla que se mostrará en todo momento.

Para más detalles de las opciones brindadas por MiPiBlock ver el manual de usuario en el ANEXO 10.

Figura 3.14 Pantalla inicial de Mipiblock con sus 6 módulos disponibles [Autoría Propia].

Cabe destacar que el dispositivo cuenta con la opción de bloqueo de pantalla configurada con el icono de candado que aparece en la parte derecha del menú principal mostrado en la Figura 3.14, al seleccionar dicha opción, se restringirá la interacción con el menú principal. Cuando se requiera recobrar la interacción con el dispositivo se deberá digitar un código PIN (del inglés Personal Identification Number), como se puede verificar en la

Figura *3.15*. El código PIN será un número de seis dígitos predeterminado en todos los dispositivos: “123456”, este código se podrá personalizar en la opción configuraciones del menú principal.

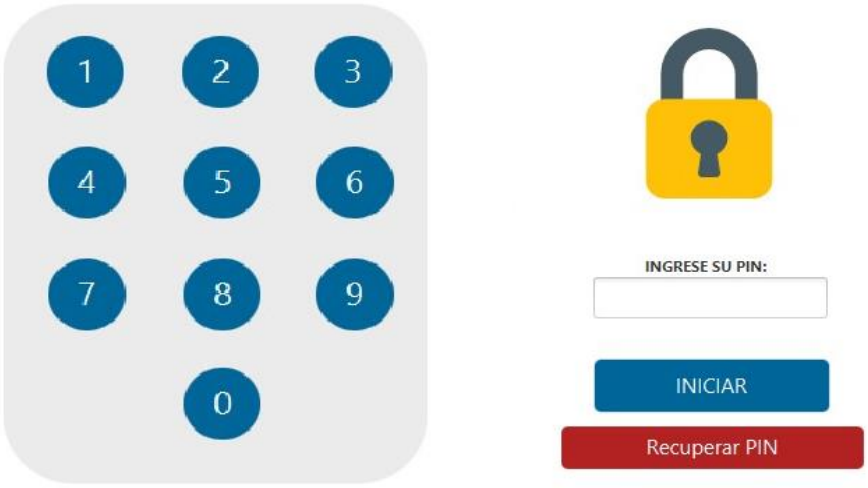

Figura 3.15 Pantalla de Desbloqueo de Mipiblock [Autoría Propia].

En caso de que no recuerde el código PIN como se muestra en la Figura 3.16, existe la opción recuperar PIN. en donde se usará un código personal de desbloqueo o PUK (del inglés “Personal Unlock Key”), predeterminado también de fábrica, este número estará impreso en una tarjeta que se entregará al adquirir el dispositivo. Este número no es personalizable. Para verificar el proceso de recuperar PIN ver el ANEXO 11.

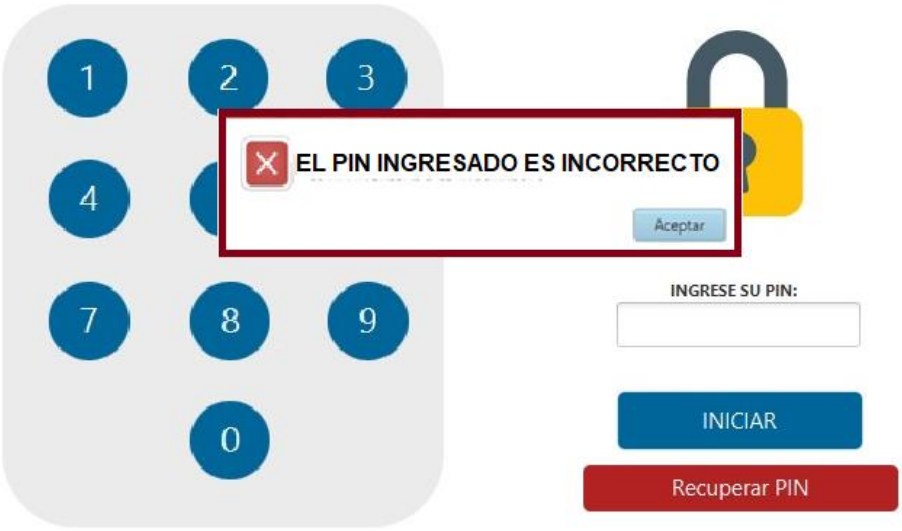

Figura 3.16 Pantalla para ingreso incorrecto de código PIN [Autoría Propia].

3.3. Base de Datos.

En el caso concreto de la persistencia de datos, se usa una base de datos SQLite por su bajo consumo de memoria y la facilidad de su uso. Se crearon cinco tablas que no siguen el diseño de entidad-relación debido a que no es necesario para el modelo del dispositivo. En gran parte para el funcionamiento de MiPiBlock se usarán los archivos propios de los diferentes servicios de Linux implementados como dnsmasq.conf, hosts, logs, etc. La Figura 3.17 muestra la configuración de las cinco tablas creadas y usadas en la operación de MiPiBlock:

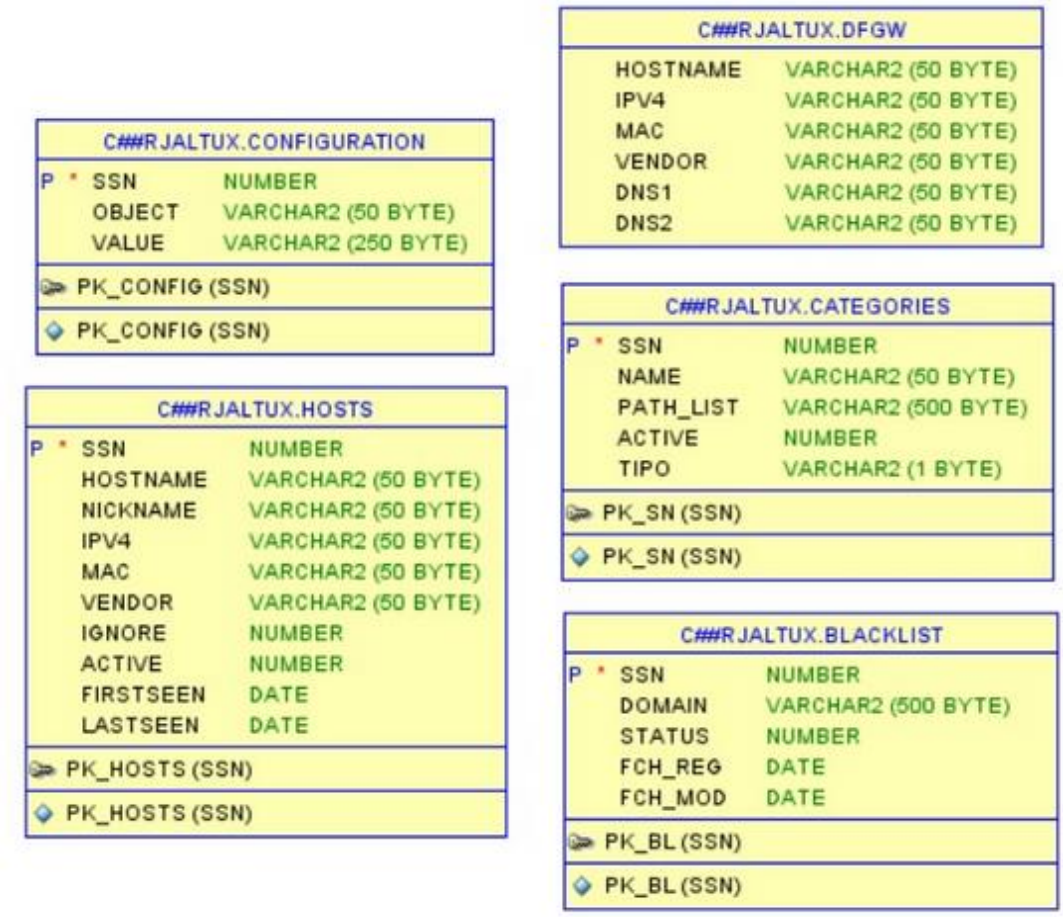

Figura 3.17 Tablas usadas para el almacenamiento de información en la Base de Datos [Autoría Propia].

La tabla CONFIGURATION almacena los parámetros importantes para el funcionamiento del sistema. Por ejemplo, el nombre de la interfaz creada, el estado del bloqueo de anuncios, el estado del bloqueo a los nuevos dispositivos encontrados, etc. Esta tabla básicamente guardará un par de datos (Clave, Valor).

En la tabla HOSTS se guardan todos los dispositivos encontrados en la red a la cual está conectada MiPiBlock. Esta tabla es de suma importancia, ya que a través de ella se definirán los dispositivos a los que aplica el monitoreo. Adicionalmente, almacena información importante de cada dispositivo como su hostname, IP, MAC, estado, etc.

La tabla DFGW guarda la información acerca del enrutador. El objetivo principal de esta tabla es obtener la puerta de enlace de la red y luego usando los registros de la tabla HOSTS, aplicar el servicio de spoofing mediante la herramienta de Scapy.

La tabla CATEGORIES sirve para almacenar las diferentes categorías de bloqueo como redes sociales, pornografía, violencia, etc. En esta tabla se almacenarán las rutas de los archivos de configuración que utilizarán para activar o desactivar el bloqueo de cada categoría.

Finalmente, la tabla BLACKLIST se encargará de almacenar todos los dominios que el usuario haya ingresado con la intención de que sean bloqueados, por ende, mediante esta tabla podemos mantener un historial de todos los registros realizados por los usuarios.

CAPÍTULO 4

4. PLAN DE IMPLEMENTACIÓN Y PRESUPUESTO

4.1. Plan de trabajo.

La presente sección detalla las actividades realizadas para el desarrollo e implementación de la solución, dentro de lo cual se contempla el ensamblaje, el desarrollo del software y las posteriores pruebas. En la Figura 4.1 se describe en detalle las diferentes actividades realizadas, el tiempo de duración y las fechas de ejecución de las mismas.

Nombre de tarea	Duración	Comienzo	Fin
PROYECTO MIPIBLOCK	**68 días**	**jue. 18/10/18 8:00**	**mié. 16/1/19 17:00**
FASE DE ANÁLISIS	**9 días**	**jue. 18/10/18 8:00**	**mar. 30/10/18 17:00**
Visita técnica y levantamiento de información	3 días	jue. 18/10/18 8:00	lun. 22/10/18 17:00
Análisis de la información obtenida	1 día	mar. 23/10/18 8:00	mar. 23/10/18 17:00
Especificaciónes del comportamiento y opciones que tendrá el	1 día	mié. 24/10/18 8:00	mié. 24/10/18 17:00
Investigación de las diferentes herramientas disponibles	3 días	jue. 25/10/18 8:00	lun. 29/10/18 17:00
Compra de equipos	1 día	mar. 30/10/18 8:00	mar. 30/10/18 17:00
FASE DE DISEÑO	**8 días**	**mié. 31/10/18 8:00**	**vie. 9/11/18 17:00**
Diseño del prototipo físico del producto (MIPIBLOCK)	3 días	mié. 31/10/18 8:00	vie. 2/11/18 17:00
Diseño del prototipo de la interfaz gráfica de usuario	2 días	lun. 5/11/18 8:00	mar. 6/11/18 17:00
Diseño de la arquitectura de los servicios utilizados para el sistema	1 día	mié. 7/11/18 8:00	mié. 7/11/18 17:00
Diseño de la base de datos	1 día	jue. 8/11/18 8:00	jue. 8/11/18 17:00
Diseño del funcionamiento del sistema	1 día	vie. 9/11/18 8:00	vie. 9/11/18 17:00
FASE DE DESARROLLO	**31 días**	**lun. 12/11/18 8:00**	**vie. 21/12/18 17:00**
Desarrollo de los servicios Spoof, Iptables y DNSProxy	7 días	lun. 12/11/18 8:00	mar. 20/11/18 17:00
Desarrollo de la API mipiblockWS	7 días	mié. 21/11/18 8:00	jue. 29/11/18 17:00
Desarrollo de scripts para el funcionamiento de los módulos del	10 días	vie. 30/11/18 8:00	jue. 13/12/18 17:00
Desarrollo e implementación del consumo de la API desde el front	7 días	vie. 14/12/18 8:00	vie. 21/12/18 17:00
FASE DE PRUEBAS	**19 días**	**sáb. 22/12/18 9:00**	**mar. 15/1/19 17:00**
Pruebas de funcionamiento locales	5 días	sáb. 22/12/18 9:00	jue. 27/12/18 17:00
Pruebas de funcionamiento en situ	1 día	sáb. 5/1/19 9:00	sáb. 5/1/19 19:00
Mejoras según las observaciones del cliente	7 días	lun. 7/1/19 8:00	mar. 15/1/19 17:00
FASE DE IMPLEMENTACIÓN	**1 día**	**mié. 16/1/19 8:00**	**mié. 16/1/19 17:00**
Presentación del dispositivo final	1 día	mié. 16/1/19 8:00	mié. 16/1/19 17:00
Capacitación sobre el funcionamiento del dispositivo	1 día	mié. 16/1/19 8:00	mié. 16/1/19 17:00

Figura 4.1 Especificaciones del plan de trabajo [Autoría Propia].

La fase de Análisis comprende todas las primeras acciones realizadas para el establecimiento de los requerimientos y parámetros a tomar en

cuenta en el proyecto, los equipos con los que cuenta la fundación, las herramientas disponibles en el mercado, y los componentes necesarios. Se designaron nueve días para la realización de las actividades de esta fase.

Para la segunda fase, se consideró disponer de ocho días. En esta fase, se ha realizaría el diseño de la solución, tanto a nivel de hardware, como de software, realizando el prototipo físico del producto, un modelo de la interfaz gráfica y de la arquitectura de servicios.

La implementación constituye la tercera fase, en ella se realizó la programación y compilación de código para la operatividad de los servicios a utilizar en la herramienta. Esta es considerada la fase más larga pues se estimó 25 días para la misma.

En la fase de pruebas, se utilizó la herramienta en el laboratorio de la fundación con el fin de verificar la operatividad, la correcta manipulación del sistema y el servicio en general por parte de los usuarios, recolectando comentarios o críticas para futuras mejoras. Para esta fase se han consideraron seis días, cinco para pruebas de funcionamiento del dispositivo de forma informal y un día para las pruebas en el laboratorio de la fundación.

El pase a producción conlleva la presentación final del dispositivo y la capacitación sobre el funcionamiento y el método de manipulación del dispositivo en sitio, ambas actividades se pueden realizar el mismo día, por ende se consideró solo un día para esta fase.

4.2. Análisis de costo

Para la elaboración de la presente solución se realizó una búsqueda y comparación de los precios de los componentes y mano de obra necesaria. Se obtuvieron varias cotizaciones de locales comerciales dentro de la ciudad, además se realizó la búsqueda vía Internet de los componentes físicos con la finalidad de verificar mediante un análisis costo/beneficio la opción más conveniente.

4.2.1. Presupuesto del dispositivo

Tabla 4.1 Presupuesto de Dispositivo [Autoría Propia].

#	COMPONENTE	CANTIDAD	COSTO POR UNIDAD	TOTAL
1	V-Kits Raspberry Pi 3 B+	1	$ 54,99	$ 54,99
2	Micro SDHC Samsung 32GB EVO Plus Class 10	1	$ 9,50	$ 9,50
3	Monitor táctil resistivo GeeekPi Raspberry Pi 5 pulgadas resolución 800X480 HDMI para Raspberry Pi 3 B+	1	$ 36,99	$ 36,99
	Subtotal			$ 101,48
	Impuesto a la Salida de Divisas 5%			$ 5,07
	TOTAL			**$ 106,55**

La Tabla 4.1 muestra en detalle los valores estimados de los componentes necesarios para la elaboración del dispositivo. El modelo Raspberry Pi3 B+ ha sido elegido en función a que las prestaciones técnicas del mismo son superiores a los de su predecesor el Raspberry Pi 3 B, aunque su precio es ligeramente superior. Se ha considerado que por las actividades que realizará el dispositivo una tarjeta de SDHC de 32 Gb es suficiente para soportar la operación, ya que la función de este será almacenar el sistema operativo de MiPiBlock, las diversas configuraciones de los perfiles de bloqueo y guardar registro de logs del sistema. El monitor GeekPi ha sido elegido teniendo en cuenta que es uno de los complementos que ha sido diseñado y testeado para su uso con dispositivos Raspberry o similares, también que el tamaño de 5 pulgadas es ideal para una fácil manipulación, además de que el factor precio que también ha sido una característica determinante.

4.2.2. Presupuesto de mano de obra

La Tabla 4.2 describe los valores presupuestados para las actividades necesarias para el diseño e impresión de la carcasa protectora de MiPiBlock, además de la programación necesaria para el desarrollo del

software. Este último valor ha sido calculado considerando los sueldos básicos establecidos por el Ministerio de Trabajo del Ecuador.

Tabla 4.2 Presupuesto de mano de obra [Autoría Propia].

#	MANO DE OBRA	PRECIO
1	Diseño de carcasa para MiPiBlock	$ 40,00
2	Impresión de carcasa de MiPiBlock	$ 40,00
3	Programación y configuración del Sistema Operativo de MiPiBlock + Diseño de la Interfaz de Usuario	$ 414,18
	TOTAL (Incluye 12% Iva)	**$ 494,18**

4.2.3. Costo total de la solución

La presente sección muestra el detalle de los gastos y costos en los que incurriría la configuración, ensamble, distribución y venta de MiPiBlock para su comercialización.

En principio, para cubrir la puesta en marcha, la adquisición del inventario, los componentes y los gastos administrativos referentes al primer año de operaciones se requerirá un préstamo a la banca privada, de este mismo se desprende el valor anual a la pagar la entidad financiera. [16]

Para que la comercialización del dispositivo sea rentable, debe considerarse un más amplio espectro de grupos de clientes destino, es decir no debe solo considerarse fundaciones, si no también incluir a los padres de familia de modo que se pueda vender un dispositivo por cada núcleo familiar a la vez que también se mantiene en menor medida la comercialización con escuelas en áreas suburbanas, fundaciones, entre otros.

En cuanto a la configuración, así como el diseño de los componentes de software y de la carcasa del dispositivo solo son necesarios una vez, luego de esto el programa y el diseño de la carcasa pueden ser producidos en serie, es por cual solo han sido considerados para el

inicio de operaciones. Se ha estimado, además, que la meta del primer año deberá ser de 218 equipos vendidos, siendo estos 208 para personas naturales y 10 para fundaciones, esto significa 4 ventas de MiPiBlock por semana para el segmento masivo y aproximadamente una venta al mes para fundaciones, este gran contraste se debe no solo a la diferencia real entre número de viviendas y número de laboratorios de computación en fundaciones, sino también a la facilidad con un jefe de familia puede comprar el dispositivo, o la disposición inmediata de su dinero, contrastado con los procesos y procedimientos internos que una fundación debe seguir para la adquisición de nuevos equipos. Para el cálculo de los precios de los componentes se ha considerado los precios de dicho elemento al por mayor, es decir, con una reducción del 40% sobre el total al menudeo. Además, se ha calculado el 10% extra para el pago de aranceles de aduana en la importación de materiales y elementos electrónicos. [17]

Por otra parte, ya que el código y la elaboración del dispositivo ha sido planteada y diseñada por los creadores de este proyecto se ha considerado durante los primeros años como único personal administrativo, solo considerándose la contratación de un ingeniero programador extra de planta para el tercer año, en donde el número de dispositivos en el mercado estén cerca de los 1.000 y por ende exista mayor número de comunicaciones, peticiones de soporte y actualizaciones de parte de los clientes. Sobre los sueldos de estos tres trabajadores se ha considerado el 10,15% que determina la ley que el empleador debe cancelar como concepto de seguridad social para cada empleado, esto está determinado en el apartado Seguridad Social. Para el personal administrativo el sueldo considerado para el primer año ha sido de 400 USD, para el segundo año se elevará a 500 USD y en el tercer, cuarto y quinto año se mantendrá en 600 USD.

Se ha considerado realizar mantenimiento preventivo al dispositivo cada seis meses, el mismo incluye la limpieza de componentes electrónicos a nivel de hardware y la actualización del sistema operativo, la eliminación de archivos basura que se generan por la

búsqueda de las listas, y la optimización de la memoria RAM a nivel de software. Este procedimiento tendrá un costo de $20, a excepción de las fundaciones sin fines de lucro para quienes los cuatro primeros mantenimientos son gratuitos.

Para la movilización y entrega del producto se ha considerado un costo de $5 por cada unidad vendida, este valor representa los costos de movilización ya sean en vehículo privado (combustible) para las entregas en la ciudad o para los costos de envió en caso de que sea enviado a nivel interprovincial dentro del territorio del Ecuador, no se ha considerado en este proyecto ninguna comercialización a nivel internacional.

Al mismo tiempo, no se ha considerado necesario el alquiler de un local para la distribución ya que las ventas se realizarán por Internet y se ha destinado un presupuesto de 100 USD al mes para poder costear las conexiones de internet del personal administrativo. La publicidad será realizada principalmente vía redes sociales, como Instagram, Facebook, Twitter, entre otros; sin embargo, se requiera de manera ocasional los servicios de publicidad de radios, medios impresos, personas con gran influencia en redes sociales, páginas web, etc., por esto se ha considerado un gasto de aproximadamente 1.000 USD anuales.

Considerando todos los gastos mencionados anteriormente, y teniendo en cuenta que el objetivo de la empresa es generar un 10% de ganancias por cada dispositivo vendido se ha establecido un precio al público de 165.65 USD.

Para la elaboración de la proyección del flujo de caja se ha tomado como referencia para el incremento de precios la inflación del país a la fecha de elaboración de este documento, es decir, noviembre del 2018, la cual se ha encontrado en 0.35%. [18]

En cuanto a la estimación de ventas de MiPiBlock por año, se ha considerado que en principio y durante el primer año se podrán vender

4 equipos a la semana a padres de familia, en el segundo año contando ya con un poco más de popularidad y conociendo mejor a los clientes a los que está destinado este producto se podrá elevar las ventas a 6 productos a la semana, el pico máximo de ventas se alcanzara durante el tercer y cuarto año donde se venderán 10 y 12 MiPiBlock a la semana, pues para este momento será un equipo conocido y probado en el mercado, luego de esto MiPiBlock llegara al punto de estabilidad en donde no se aumentaran las ventas y será el momento de innovar y buscar nuevas alternativas que sumen al proyecto para conseguir que se mantenga vigente, se ha tomado en cuenta para esta determinación el ciclo de vida de un producto. [19]

Según estas proyecciones la inversión inicial de 35.000 USD, la misma será retornada completamente en el tercer año de operaciones, y además el préstamo inicial será finalizado de pagar completamente al término del quinto año. En la Figura 4.2 se puede verificar a mejor detalle el flujo de caja proyectado para los próximos 5 años.

Flujo de caja

	2019	2020	2021	2022	2023	2024	Total
Saldo inicial	$ 35.000,00	$ 31.497,43	$ 30.340,98	$ 35.349,05	$ 43.871,32	$ 51.444,88	
Ingresos							
Ventas en efectivo	$ 36.110,78	$ 51.030,04	$ 86.215,83	$ 97.988,12	$ 106.492,43	$ 79.739,97	$ 457.577,17
Cobros de mantenimiento	$ 2.080,00	$ 5.200,00	$ 8.320,00	$ 11.440,00	$ 8.486,67	$ 10.400,00	$ 45.926,67
Total Ingresos	$ 38.190,78	$ 56.230,04	$ 94.535,83	$109.428,12	$ 114.979,10	$ 90.139,97	$ 503.503,83
Egresos							
Compra de mercancía	$ 13.273,58	$ 22.307,05	$ 40.649,89	$ 49.231,66	$ 54.970,41	$ 38.208,99	$ 218.641,59
Pago de nómina	$ 9.600,00	$ 12.000,00	$ 17.421,04	$ 17.482,01	$ 17.543,20	$ 1.172,85	$ 75.219,10
Pago de Seguridad social	$ 974,40	$ 1.218,00	$ 1.768,24	$ 1.774,42	$ 1.780,63	$ 1.786,87	$ 9.302,56
Pago proveedores	$ 5.232,00	$ 7.995,89	$ 14.570,82	$ 16.047,75	$ 17.918,37	$ 11.326,10	$ 73.090,92
Movilización para mantenimiento	$ 624,00	$ 1.560,00	$ 2.496,00	$ 3.432,00	$ 2.546,00	$ 3.120,00	$ 13.778,00
Pago de servicios públicos	$ 1.200,00	$ 1.204,20	$ 1.208,41	$ 1.212,64	$ 1.216,89	$ 1.221,15	$ 7.263,29
Compra de utensilios de mantenimiento	$ 208,00	$ 520,00	$ 832,00	$ 1.144,00	$ 848,67	$ 1.040,00	$ 4.592,67
Total Egresos	$ 31.111,98	$ 46.805,14	$ 78.946,40	$ 90.324,49	$ 96.824,17	$ 57.875,95	$ 401.888,14
Flujo de caja económico	$ 42.078,79	$ 40.922,34	$ 45.930,41	$ 54.452,68	$ 62.026,24	$ 83.708,89	
Financiamiento							
Pago de préstamos	$ 10.581,36	$ 10.581,36	$ 10.581,36	$ 10.581,36	$ 10.581,36		$ 52.906,80
Total Financiamiento	$ 10.581,36	$ 10.581,36	$ 10.581,36	$ 10.581,36	$ 10.581,36	$ -	$ 52.906,80
Flujo de caja financiero	$ 31.497,43	$ 30.340,98	$ 35.349,05	$ 43.871,32	$ 51.444,88	$ 83.708,89	

Figura 4.2 Flujo de caja de MiPiBlock [Autoría Propia].

4.3. Pruebas

Acudimos a una reunión con los docentes y tutores de la fundación en la cual se dejó que los usuarios finales interactúen con el dispositivo de manera intuitiva. Durante la exploración surgieron algunas dudas, como por ejemplo, si el dispositivo necesita de algún cuidado especial, si se lo puede colgar en la pared, entre otros.

Así mismo los usuarios manifestaron comentarios positivos, indicaron que les agradaba que el dispositivo sea liviano, y aunque no de manera simultánea se pueda usar en diferentes redes LAN.

También expresaron como puntos para mejorar que les gustaría que el tamaño del dispositivo sea reducido para que pueda caber en un bolsillo. Además, que la respuesta de la pantalla sea más rápida. Para poder visualizar la evidencia de esta reunión puede ver ANEXO 12.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Los componentes de MiPiBlock han reafirmado la factibilidad del desarrollo e implementación de seguridad informática de bajo costo. Las fases de pruebas del prototipo se realizaron in situ en la Fundación Compassion International, donde los usuarios brindaron opiniones positivas con respecto a la iniciativa.

En comparación con las demás opciones analizadas MiPiblock representa la solución más óptima en cuanto a costo, ya que la operación de MiPiblock no requiere adhesión de los usuarios a ninguna membresía con pagos periódicos, compra de licencias, y su precio no está supeditado al número de usuarios usando el servicio. Mipiblock requiere solo el costo de adquisición inicial.

El campo de la seguridad de redes es inmensamente amplio y en continua mutación y mejora, por lo que, para el aseguramiento de la calidad de la protección ejecutada por MiPiBlock, será necesaria una constante liberación y actualización de las listas de bloqueos, categorías y versiones del software.

El análisis comercial realizado indica que mientras mayor es el número de ventas anuales los gastos administrativos representarán un menor porcentaje del precio final del producto, ocasionando, de esta forma que el mismo sea más económico, por ende se ha planteado que la comercialización del dispositivo debe realizarse no solo para fundaciones o instituciones educativas sino también enfocarse en padres de familia en general.

Recomendaciones.

Considerando que las buenas prácticas en las tecnologías de la información dictan la necesidad de tener en cuenta la mejora continua de los sistemas, este apartado detalla varias ideas que podrían optimizar el funcionamiento de MiPiBlock, en caso de que en futuro se pretenda expandir el alcance de las tareas realizadas.

La implementación de una entrada/salida de audio para la interacción con el dispositivo evitando la manipulación física.

Incorporación de un ventilador para evitar el calentamiento del dispositivo, esto deberá conllevar un rediseño del case de protección del dispositivo. Se sugiere, de forma adicional, agregar una tapa la cual proteja la pantalla táctil.

Implementar un servidor centralizado que utilice técnicas de Machine Learning, y que cree nuevos registros al realizar la carga de URL, de forma que en el futuro pueda predecirse si una página representa o no peligro para la red o el usuario.

Aprovisionar un repositorio en la nube en donde se liberen las nuevas versiones del software y las listas actualizadas de forma periódica.

Según el análisis de la información obtenido en las encuestas realizadas, los usuarios consideran que un precio accesible para la venta masiva de MiPiBlock debería ser entre 50 y 100 USD. Raspberry Pi es una de las herramientas de hardware de bajo costo más populares en la actualidad, sin embargo, con el avance de la tecnología es posible que en años próximos a la liberación de este documento exista una herramienta más eficiente económica y energéticamente, el desarrollo, implementación y los cálculos financieros deberán ser replanteado para esta.

BIBLIOGRAFÍA

[1] Z. Dentzel, «El impacto de internet en la vida diaria,» 2013. [En línea]. Available: https://www.bbvaopenmind.com/articulos/el-impacto-de-internet-en-la-vida-diaria/.

[2] «Exito Exportador el internet Global a su alcance,» 05 Septiembre 2018. [En línea]. Available: http://www.exitoexportador.com/stats.htm. [Último acceso: 14 Octubre 2018].

[3] EFE, *Los jóvenes dominan el acceso mundial al internet,* Ginebra: El nuevo dia, 2017.

[4] INEC, «Ecuador en cifras,» INEC, 2016. [En línea]. Available: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/infografia.pdf. [Último acceso: 14 Octubre 2018].

[5] INEC, «Ecuador en cifras,» INEC, 2016. [En línea]. Available: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf. [Último acceso: 14 Octubre 2018].

[6] E. De Bono, «Six Thinking Hats,» The de Bono Group, [En línea]. Available: http://www.debonogroup.com/six_thinking_hats.php. [Último acceso: 15 Nov 2018].

[7] M. Hachman, «PC WORLD,» IDG Communications, Inc., 31 Diciembre 2017. [En línea]. Available: https://www.pcworld.com/article/3163631/windows/how-to-use-microsofts-paint-3d-creating-cool-3d-scenes-has-never-been-so-much-fun.html. [Último acceso: 1 Diciembre 2018].

[8] M. Soto, «Medium,» 27 Junio 2016. [En línea]. Available: https://medium.com/@marvin.soto/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2. [Último acceso: 02

Enero 2019].

[9] Raspberry Pi Foundation, «Raspberry Pi 3 Model B+,» Raspberry Pi Foundation, 30 Noviembre 2018. [En línea]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/. [Último acceso: 30 Noviembre 2018].

[10] Colaboradores de LcdWiki, «LcdWiki,» MediaWiki, 14 Diciembre 2018. [En línea]. Available: http://www.lcdwiki.com/5inch_HDMI_Display. [Último acceso: 02 Enero 2019].

[11] Oracle, «Java Documentation,» Oracle Corporation, Agosto 2014. [En línea]. Available: https://docs.oracle.com/javase/8/javafx/get-started-tutorial/index.html. [Último acceso: 30 Noviembre 2018].

[12] Nmap.org, «Nmap Security Scanner,» Agosto 2018. [En línea]. Available: https://nmap.org/. [Último acceso: 30 Noviembre 2018].

[13] Hipp, Wyrick & Company, Inc., «SQLite,» Hipp, Wyrick & Company, Inc., 29 Noviembre 2018. [En línea]. Available: https://www.sqlite.org/about.html. [Último acceso: 11 Noviembre 2018].

[14] P. Biondi, P. Lalet, G. Potter y G. Valadon, «Scapy Documentation,» Philippe Biondi and the Scapy community Revision, 30 Noviembre 2018. [En línea]. Available: https://scapy.readthedocs.io/en/latest/. [Último acceso: 30 Noviembre 2018].

[15] TravisFSmith, «SweetSecurity,» [En línea]. Available: https://github.com/TravisFSmith/SweetSecurity.

[16] BANCO DE GUAYAQUIL, «Banco de Guayaquil,» [En línea]. Available: https://apps.bancoguayaquil.com/bgcotizador/aplicacion/cotizador.aspx. [Último acceso: 17 Diciembre 2018].

[17] Ecomex360, «Aranceles Ecuador,» QUALITYSOFT CIA. LTDA., 2017. [En línea]. Available: http://arancelesecuador.com/resultados.html?search=raspberry&page=1. [Último

acceso: 17 Diciembre 2018].

[18] «Banco Central del Ecuador,» Noviembre 2018. [En línea]. Available: https://contenido.bce.fin.ec/documentos/PublicacionesNotas/Notas/Inflacion/inf201811.pdf. [Último acceso: 17 Diciembre 2018].

[19] Tecnológico de Monterrey, «Accion Consultores,» Red educativa para el desarrollo social sostenible, 2018. [En línea]. Available: http://www.cca.org.mx/cca/cursos/administracion/artra/comerc/planes/8.2.3/produ.htm. [Último acceso: 02 Enero 2019].

[20] P. Cook, «Raspberry Stack Exchange Forum,» Stack overflow., 05 marzo 2016. [En línea]. Available: https://raspberrypi.stackexchange.com/questions/43618/raspberry-pi-3-micro-sd-card-speed. [Último acceso: 28 Noviembre 2018].

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTAS

Nombre: Patricia Plúas

Fecha: 16-10-2018

OBJETIVO: Conocer a detalle la opinión y postura del Centro de Desarrollo Integral 314 de la Fundación Compassion International del frente a la problemática que representa el fácil acceso a contenido inapropiado en Internet.

Preguntas:

1. **¿Cuál es el cargo que usted desempeña en la Fundación?**
   Tutora de niños de 6 y 9 años.

2. **¿Desde hace cuánto tiempo es colaboradora en las actividades de la fundación?**
   Desde hace 4 años.

3. **¿Cuál es el número de personas que se beneficia con la fundación?**
   499 niños, niñas, adolescentes y jóvenes entre la edad de 4 y 22 años.

4. **¿Cuentan con laboratorio de computación para los beneficiarios de la fundación? ¿Cuándo aproximadamente fue la última vez que realizaron un mantenimiento a este laboratorio?**
   Sí, cuenta con 10 computadoras en las que los chicos realizan investigaciones o tareas de las escuelas o colegios, la última vez que se realizó un mantenimiento fue hace 10 meses.

5. **¿Ha escuchado usted el término "contenido inapropiado" o "contenido malicioso" con relación al servicio de Internet? ¿Cómo lo definiría usted?**
   Sí, tengo entendido que son todas esas páginas que muestran contenido como pornografía o violencia, también las redes sociales pueden ser ya que a veces los chicos prestan las computadoras para según ellos hacer investigaciones y en realidad no hacen nada.

6. **¿Ha tenido usted alguna mala experiencia con este contenido inapropiado/malicioso en la red? ¿Podría usted describir esta experiencia?**
   Sí, a veces mientras uno está navegando por internet salen esos anuncios con imágenes pornográficas y yo lo que he hecho es cerrar enseguida la página o cambiar de página, también me ha tocado sacar a los chicos de las computadoras porque le salen unas chicas que los invitan a una cita.

7. **¿Cuentan con algún bloqueo de contenido inapropiado/malicioso para el servicio de Internet inalámbrico? ¿Por qué?**
   No, porque nadie nos ha ofrecido ese servicio y tampoco sabía que eso se podía hacer.

8. **¿Considera usted que es importante que el servicio de internet cuente con un bloqueo de contenido inapropiado/malicioso? ¿Por qué?**
   Sí, para poder controlar que los chicos no se metan en páginas con contenido pornográfico y también el acceso a las redes sociales cuando piden las máquinas para investigar.

9. **¿Cómo cree usted que puede influir este contenido inapropiado/malicioso en el desarrollo personal de cada individuo si logra tener acceso?**
   En los chicos puede influir en que ellos despiertan muy rápido su conocimiento o su mente en cosas que para su edad no deberían y en el personal que colabora con la fundación influye bastante entorno al rendimiento ya que tener el acceso a internet libre se crea distracciones en el trabajo.

10. **¿Podría usted realizar el bloqueo de contenido inapropiado? ¿Por qué? ¿Cómo lo realizaría?**
    Actualmente no sé cómo podría realizarlo, pero si me enseñan si estoy dispuesta a aprender.

11. **En caso de existir un dispositivo de fácil uso para realizar el bloqueo contenido inapropiado/malicioso ¿Estaría interesado en adquirirlo? ¿Cuánto estaría dispuesto a pagar por el dispositivo?**

Claro que sí, pero todo depende el precio yo pagaría hasta $80 si es que solo comprándolo funciona, y no tengo que cancelar ningún otro valor.

Nombre: Jordy Triviño Plúas

Fecha: 16-10-2018

OBJETIVO: Conocer a detalle la opinión y postura del Centro de desarrollo integral 314 de la fundación Compassion International frente a la problemática que representa el fácil acceso a contenido inapropiado en Internet.

Preguntas:

1. **¿Cuál es el cargo que usted desempeña en la Fundación?**
   Tutor de niños de 12 a 14 años.

2. **¿Desde hace cuánto tiempo colabora en las actividades de la fundación?**
   Desde hace 1 año y medio.

3. **¿Cuál es el número de personas que se beneficia con la fundación?**
   Aproximadamente 450 entre niños, niñas, adolescentes y jóvenes entre la edad de 4 y 22 años.

4. **¿Cuentan con laboratorio de computación para los beneficiarios de la fundación? ¿Cuándo aproximadamente fue la última vez que realizaron un mantenimiento a este laboratorio?**
   Sí, los chicos lo usan para deberes o investigaciones que les envían en la escuela o colegios. La verdad no recuerdo cuando fue la última vez que se hizo un mantenimiento a las Pc.

5. **¿Ha escuchado usted el término "contenido inapropiado" o "contenido malicioso" con relación al servicio de Internet? ¿Cómo lo definiría usted?**
   Sí, creo que es todo tipo de información inadecuada que pueda salir como páginas que sea dañina para los jóvenes.

6. **¿Ha tenido usted alguna mala experiencia con este contenido inapropiado/malicioso en la red? ¿Podría usted describir esta experiencia?**
   Sí, a veces mientras uno navega salen esos anuncios pornográficos y hacen asustar, además que la gente te queda viendo y eso causa vergüenza. Lo que hago es tratar de cerrar rápido eso, pero a veces al hacer clic siguen saliendo más páginas.

7. **¿Cuentan con algún bloqueo de contenido inapropiado/malicioso para el servicio de Internet inalámbrico? ¿Por qué?**
   No, porque aquí casi nadie sabe cómo aplicar eso.

8. **¿Considera usted que es importante que el servicio de internet cuente con un bloqueo de contenido inapropiado/malicioso? ¿Por qué?**
   Sí, porque así se evita que los niños entren a páginas dañinas para ellos.

9. **¿Cómo cree usted que puede influir este contenido inapropiado/malicioso en el desarrollo personal de cada individuo si logra tener acceso?**
   En los niños despertaría más la curiosidad de ellos porque pueden ir abriendo más páginas de esas para ver que encuentran. En los trabajadores es más como un distractor en el trabajo porque se desconcentran y no realizan un buen trabajo.

10. **¿Podría usted realizar el bloqueo de contenido inapropiado/malicioso? ¿Por qué? ¿Cómo lo realizaría?**
    No, porque no tengo conocimiento acerca de eso.

11. **En caso de existir un dispositivo de fácil uso para realizar el bloqueo contenido inapropiado/malicioso ¿Estaría interesado en adquirirlo? ¿Cuánto estaría dispuesto a pagar por el dispositivo?**
    Si pero primero tendría que informarme bien que funcione, y pagaría desde $20 hasta $100 depende de que tan bueno y completo sea su funcionamiento y aprendizaje.

Nombre: Briggitte Flores

Edad: 21 años

Fecha: 16-10-2018

Cargo: presidenta del comité de Padres de Familia de la comunidad ‘Emaús’

OBJETIVO: Conocer a detalle la opinión y postura de los padres de familia que tienen vínculo con el Centro de desarrollo integral 314 de la Fundación Compassion International frente a la problemática que representa el fácil acceso a contenido inapropiado en Internet.

1. **¿Cuántos hijos tiene actualmente?** 1

2. **¿Conoce los riesgos que se pueden encontrar en internet? ¿Puede decirme cuáles?**
   Sí, podría ser la pornografía o también cuando crean esas páginas en redes sociales para formar bandas, más que todo, los niños entran en ese tipo de páginas por ser curiosos o saber más pero obviamente ese tipo de contenido no está acto para la edad de sus niños.

3. **¿Está al tanto del contenido web al que su familia accede en internet? ¿Por qué?**
   La verdad no, porque actualmente los niños son más astutos que las personas adultas y a veces ellos borran el historial de las páginas que han visitado para que sus padres no se enteren.

4. **¿Como cree que puede influir en los niños las búsquedas que se realizan en internet y que usted como padre o madre no puede controlar?**
   Puede traer grandes consecuencias, porque a veces comparten información que ni siquiera conocen, sino que solo por lo que ven en su perfil se dejan llevar porque son muy ingenuos. Además que influye en su rendimiento académico porque causa distracción porque se enfocan mucho más por la cosas que ven en internet y comienzan a decir mentiras como que le dejen usar la PC para realizar una investigación cuando en realidad solo pierden el tiempo viendo cosas no productivas, además hay que tener en cuenta que la

mayoría de las personas mayores no saben utilizar bien el internet y no pueden darse cuenta de que es lo que sus hijos ven o hacen.

5. **¿Ha escuchado usted el término "contenido inapropiado" o "contenido malicioso" en relación al servicio de Internet? ¿Cómo lo definiría usted?**
   Sí, quizás el contenido que no sea apto para cierta edad, como algún tipo de videos de violencia, pornografía o cosas así.

6. **¿Ha tenido usted alguna mala experiencia con este contenido inapropiado/malicioso en la red? ¿Podría usted describir esta experiencia?**
   Sí, quizás en algún momento cuando encendí la computadora o el teléfono me salen esas páginas y tengo entendido que ese tipo de páginas traen virus.

7. **¿Cuentan con algún bloqueo de contenido inapropiado/malicioso para el servicio de Internet inalámbrico? ¿Por qué?**
   No, porque la verdad no sabía que eso se podía hacer.

8. **¿Considera usted que es importante que el servicio de internet cuente con un bloqueo de contenido inapropiado/malicioso? ¿Por qué?**
   Obviamente sí, porque eso ayudaría a los padres poder controlar lo que sus hijos están haciendo en Internet, hay veces que los chicos se quedan hasta la madrugada viendo videos o redes sociales y uno ni siquiera se entera.

9. **¿Podría usted realizar el bloqueo de contenido inapropiado/malicioso? ¿Por qué? ¿Cómo lo realizaría?**
   No, porque no tengo el conocimiento necesario para realizarlo, es más recién me entero de que esto se podía realizar.

10. **En caso de existir un dispositivo de fácil uso para realizar el bloqueo contenido inapropiado/malicioso ¿Estaría interesada en adquirirlo? ¿Cuánto estaría dispuesto a pagar por el dispositivo?**
    Si desearía comprarlo pero tendría que ver el precio, si es realmente costo no creo que pueda adquirirlo, pero yo pagaría entre $50 a $80 por este dispositivo.

ANEXO 2

FORMATO DE ENCUESTAS

Nombre.

Fecha.

OBJETIVO Obtener una retroalimentación de las necesidades de los usuarios de la Fundación Centro de desarrollo integral 314 – Compassion International.

1. ¿Cuáles de los siguientes dispositivos electrónicos posee usted? (Puede escoger más de una opción)
   - Portátil
   - Tablet
   - Smartphone
   - Otros _____

2. ¿Con que frecuencia semanal asiste a la Fundación CSI-314?
   - 1 vez a la semana
   - 2 veces a la semana
   - 3 veces a la semana
   - 4 veces a la semana
   - 5 o más veces a la semana

3. ¿Cuánto tiempo promedio usted permanece en las instalaciones de la Fundación CDI-314 en las ocasiones que usted utiliza sus servicios?
   - De 30 minutos a 1 hora
   - De 1 hora a 2 horas
   - De 2 horas a 3 horas
   - De 3 horas en adelante

4. ¿Cuáles son las actividades que usted realiza con frecuencia en la Fundación CDI-314?
    - □ Entretenimiento
    - □ Trabajo
    - □ Comunicación (e-mails, Skype, etc)
    - □ Apoyo a las tareas escolares o universitarias
    - □ Otro (Por favor especifique) _____

5. Cuando utiliza las redes sociales ¿Cuáles utiliza?
    - □ Facebook
    - □ Instagram
    - □ YouTube
    - □ Twitter
    - □ Tinder
    - □ Otros: _____

6. Cuándo utiliza aplicaciones de comunicación, ¿Cuáles utiliza?
    - □ Facebook Messenger
    - □ Skype
    - □ Viber
    - □ Correo Electrónico
    - □ Otros _____

7. ¿Cuál de estas formas de protección a su navegación web ha utilizado alguna vez?
    - □ Antivirus
    - □ Proxy
    - □ Firewall de Windows
    - □ Control Parental de Windows
    - □ Ninguno
    - □ Otros_____

8. ¿Cuál de todas estas formas de contenido inapropiado/malicioso es la que usted ha experimentado con más frecuencia?
    - Pornografía
    - Violencia
    - Cyber bullying
    - Cyber acoso
    - Spam
    - Otros _____

9. ¿Cuál considera usted que es el mayor peligro mientras navega en la web con respecto a contenido inapropiado/ malicioso?
    - Fraude Electrónico
    - Descarga de Virus
    - Exposición de información privada
    - Trastornos en el desarrollo personal
    - Otros: _____

10. ¿Considera usted necesario la implementación de un dispositivo de filtrado de contenido inapropiado/malicioso?
    - No es necesario
    - Poco necesario
    - Medianamente necesario
    - Necesario
    - Muy necesario

    ¿Por qué? _____

11. Estaría interesado en la posibilidad de realizar un filtrado de navegación mediante:
    - Un dispositivo de fácil uso que le permita hacerlo usted mismo.
    - Un servicio de bajo costo que sea brindado por expertos.

12. En caso de existir un dispositivo que le permita realizar el filtrado de navegación en Internet que no requiera conocimientos técnicos, ¿Qué tan interesado estaría en adquirirlo? Siendo 1 nada interesado y 5 absolutamente interesado.
    - 5. Absolutamente Interesado
    - 4. Muy Interesado
    - 3. Medianamente Interesado
    - 2. Poco Interesado
    - 1. Nada interesado

13. ¿Qué valor estaría dispuesto a pagar por este dispositivo?
    - $0 a $49,99
    - $50 a $99,99
    - $100 a $149,99
    - $150 a $199,99
    - $200 en adelante.

ANEXO 3

RESULTADOS DE ENCUESTAS

La presente sección nos presenta un resumen de las conclusiones obtenidas de los resultados de cada pregunta de la encuesta, resultados que han servido para enriquecer la propuesta inicial.

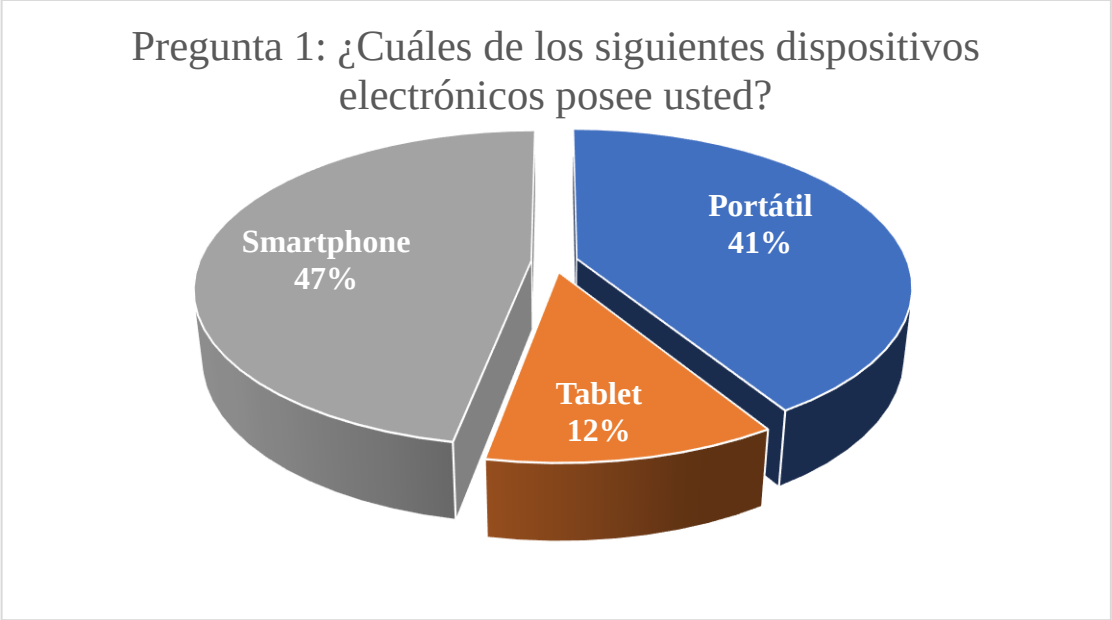

Figura A.3. 1 Dispositivos electrónicos que poseen los usuarios.

Los resultados son contundentes, en la Figura A.3. 1 podemos observar que el 47% de los encuestados cuenta con Smartphone, seguidos de un 41% de usuarios que cuentan Portátil la diferencia es mínima entre estos dos dispositivos, no siendo así con el 12% de los encuestados que cuentan con una Tablet.

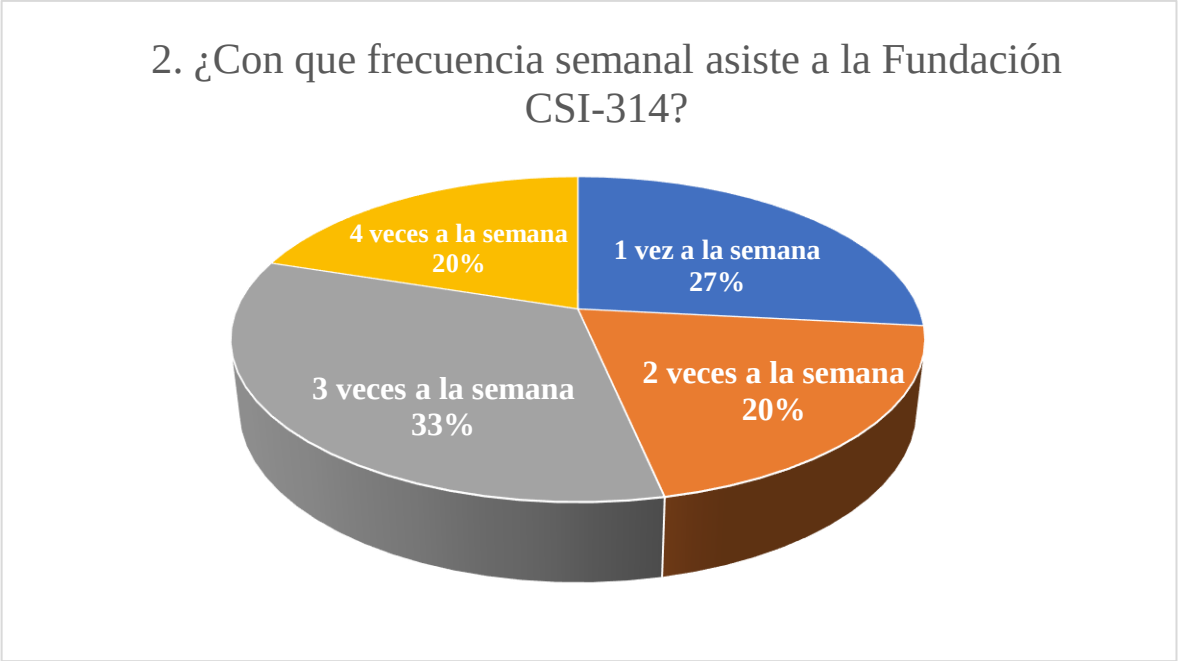

Figura A.3. 2 Frecuencia con la que asisten los usuarios a la fundación.

En la Figura A.3. 2, podemos identificar que solo el 20% de los encuestados asisten 4 veces a la semana, cabe destacar que en esta pregunta también se encontraba la opción de asistencia a la Fundación de 5 veces o más, pero el 0% de usuarios tiene esta frecuencia de asistencia a la Fundación.

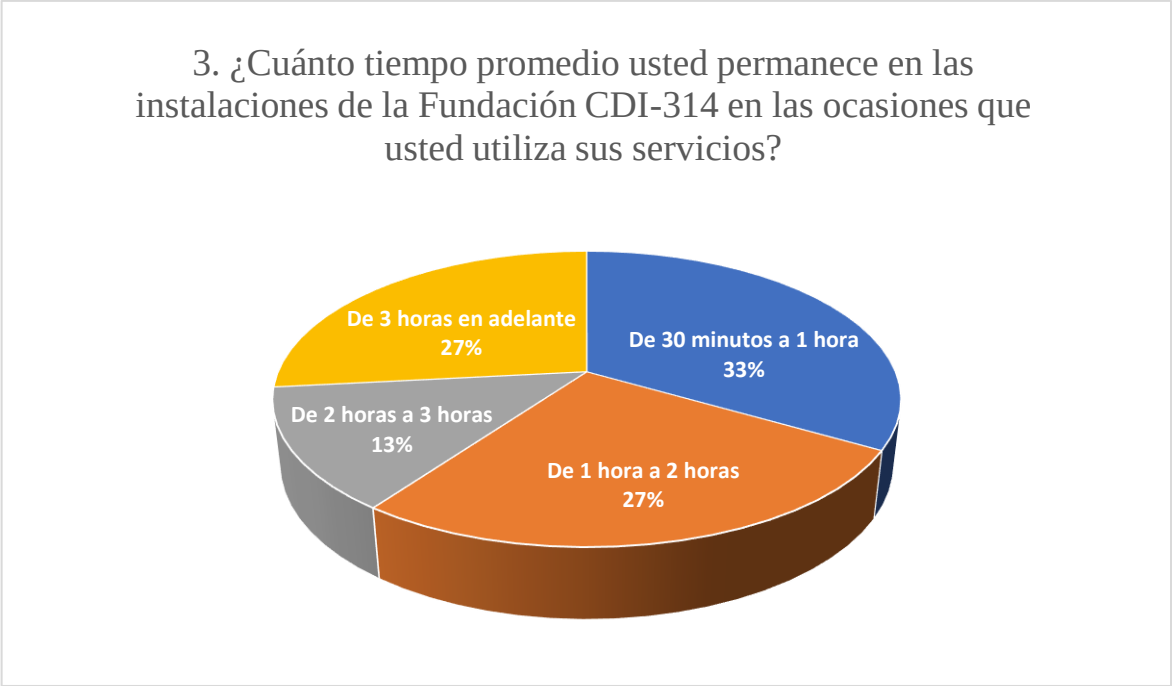

Figura A.3. 3 Tiempo promedio que los usuarios permanecen en la fundación utilizando sus servicios.

En la Figura A.3. 3, lo más destacado en los resultados de esta pregunta es que la mayoría de los encuestados, compuesta de un 33% asiste de manera breve a la Fundación CDI-314 siendo este tiempo de 30 minutos a 1 hora.

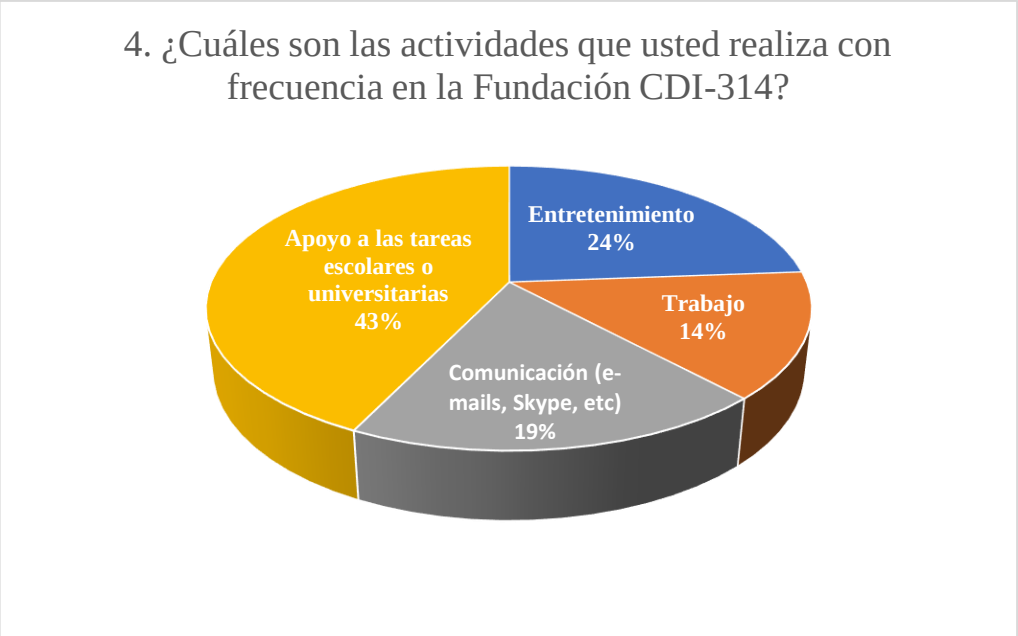

Figura A.3. 4 Actividades realizadas con mayor frecuencia por los usuarios.

Los resultados son reveladores y nos da mucha información en cuanto a las actividades que realizan los usuarios del servicio que brinda la Fundación CDI-314, en la Figura A.3. 4 se observa que el 43% de usuarios realizan apoyo a las tareas escolares y universitarias, seguido de entretenimiento con un 24% que también es un porcentaje considerable al cual debemos prestarle mucha atención.

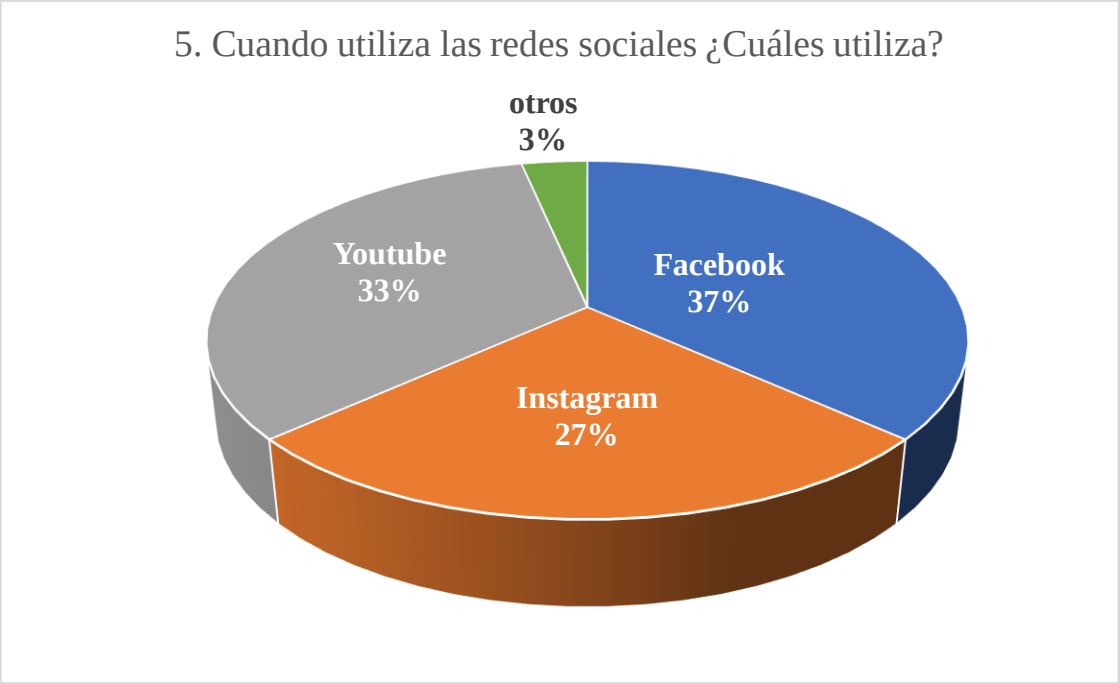

Figura A.3. 5 Redes sociales más utilizadas por los usuarios.

En la Figura A.3. 5 podemos apreciar que la red social más usada es Facebook con un 37%, la segunda es YouTube con un 33%, y no tan lejos está Instagram con un 27%, como un dato curioso podemos agregar que los encuestados agregaron varios comentarios en los que decían que las redes sociales absorben mucho tiempo y que cuando están distraídos en ellas el tiempo pasa demasiado rápido, por eso las utilizan ya al final de su jornada.

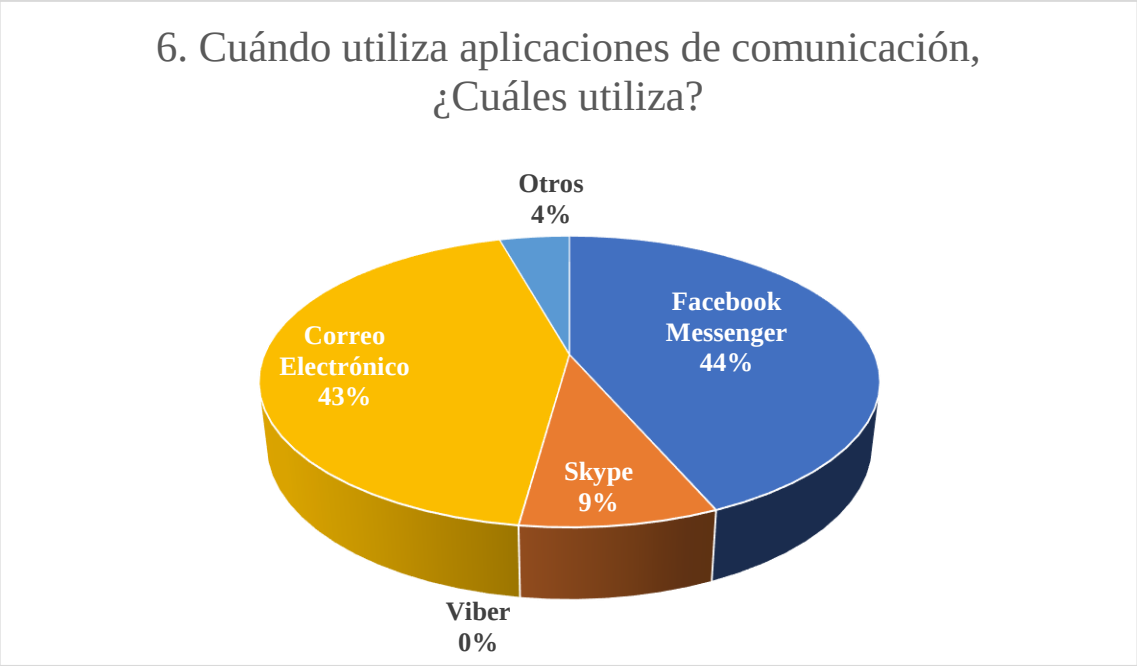

Figura A.3. 6 Aplicaciones de comunicación que utilizan los usuarios.

Podemos evidenciar en la Figura A.3. 6 que el mayor porcentaje lo tiene Facebook Messenger con un 44%, y con una diferencia mínima de un 1% se encuentra Correo Electrónico, lo que nos indica que no podemos dejar de lado a los Spams al momento de la elaboración del dispositivo. Adicionalmente, cabe destacar que en esta pregunta no se consideró WhatsApp como aplicación de comunicación, pero es importante destacar que el 4% considerados como 'otro' es netamente WhatsApp porque los encuestados escribieron el nombre de la aplicación.

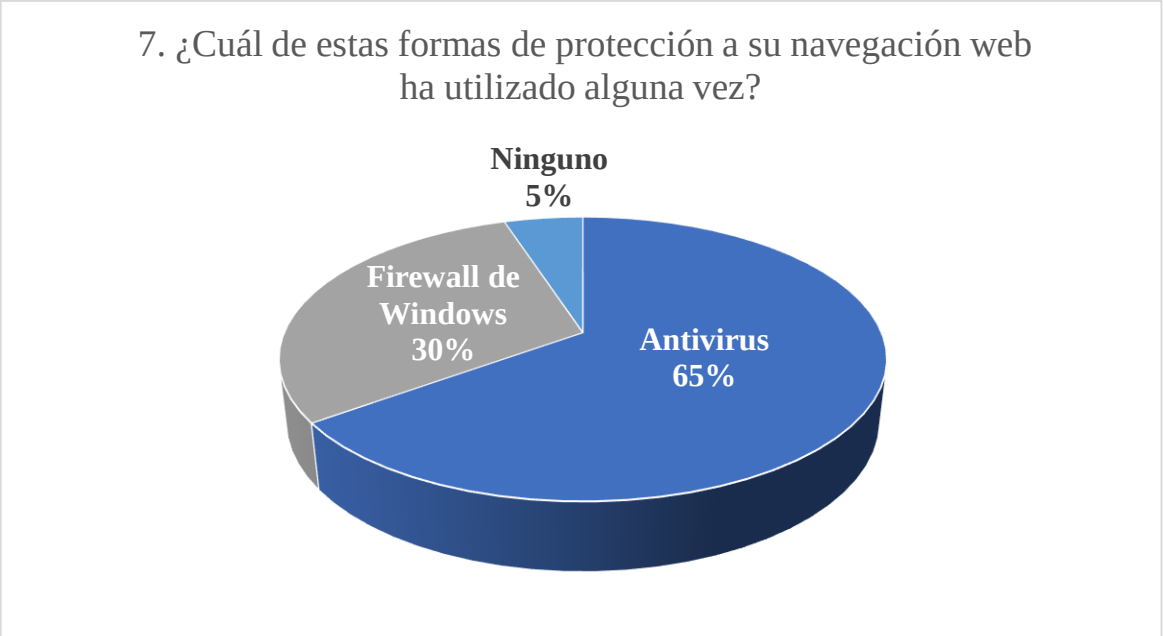

Figura A.3. 7 Aplicaciones de seguridad más utilizadas por los usuarios.

Consideramos muy importante el desconocimiento de los usuarios por las diferentes formas de protección de a su navegación web ya que según lo observado en la Figura A.3. 7, el 5% no conoce ninguna, mientras que el 65% ha utilizado Antivirus y el 30% Firewall de Windows, de las otras opciones como proxy y control parental de Windows los usuarios indicaron desconocerlas, es más ni siquiera las habían escuchado nombrar antes.

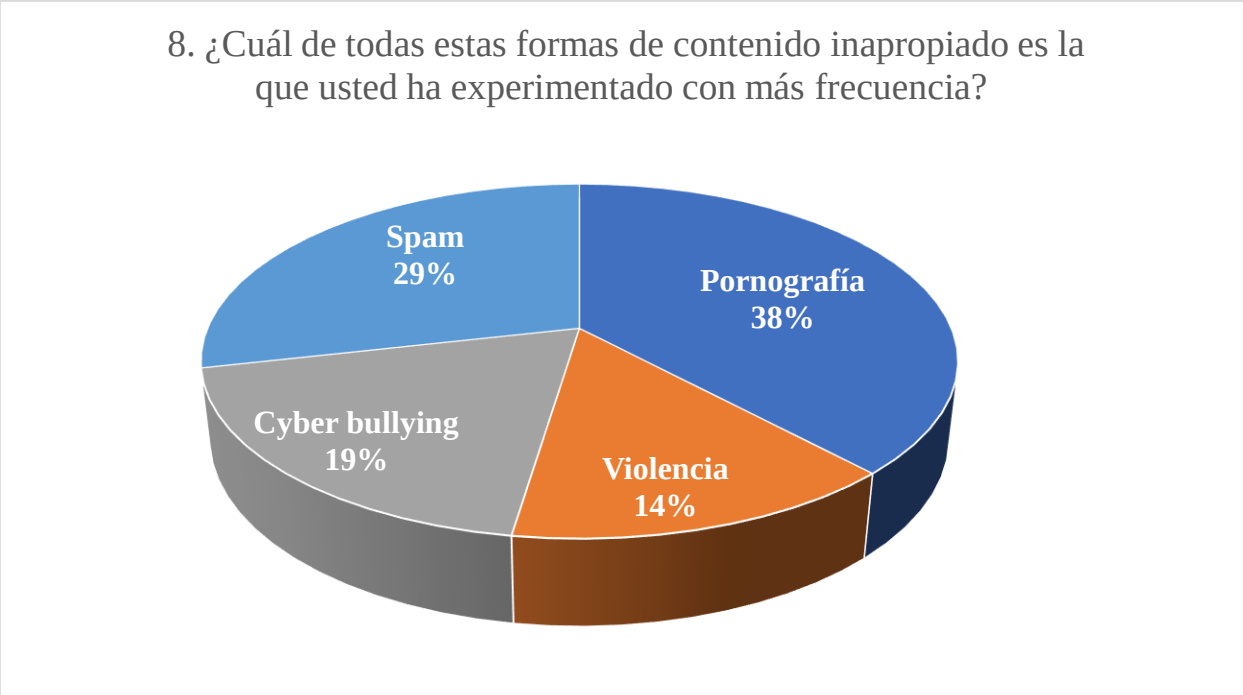

Figura A.3. 8 Contenido inapropiado más experimentado por los usuarios.

Los resultados graficados en la Figura A.3. 8 contienen implícito un dato muy importante que corrobora nuestra problemática, el 100% de los encuestados sin duda alguna ha sido víctima de contenido inapropiado. Liderando la encuesta tenemos el 38% correspondiente a pornografía, seguido de Spams con un 29% lo cual también es un dato alarmante.

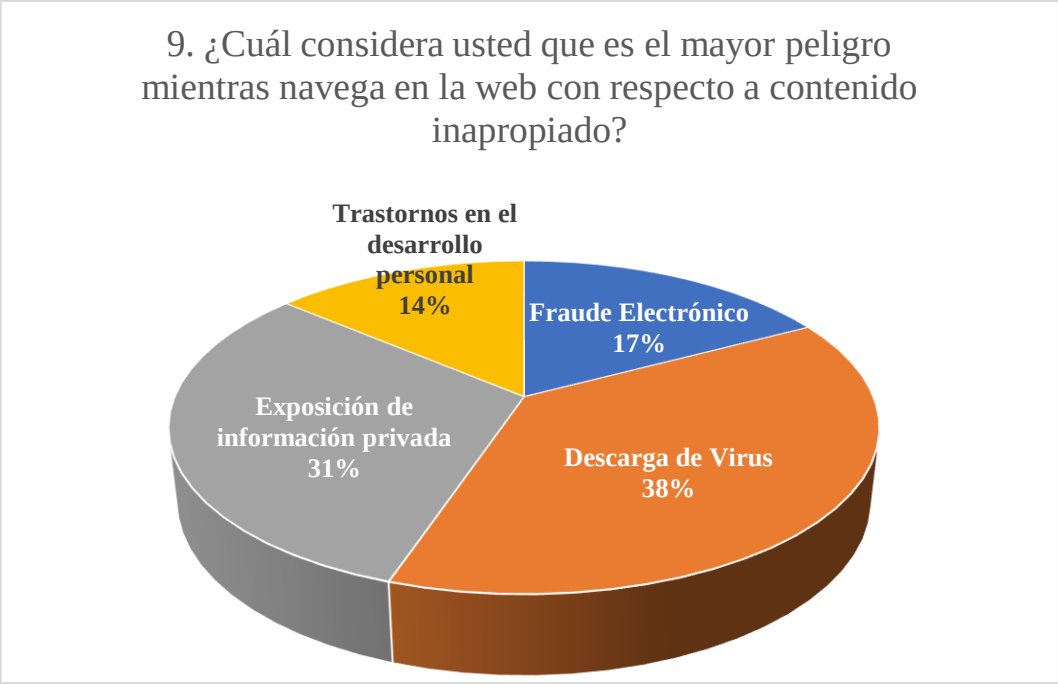

Figura A.3. 9 Mayores peligros en la navegación web según la percepción de los usuarios.

Los usuarios se encuentran conscientes de que existe un peligro inminente, sobre todo para las personas que aún no cuentan con criterio formado, en la encuesta podemos observar que los usuarios consideran que el mayor peligro de contenido inapropiado son las descargas de virus representan el 38% de encuestados, como se muestra en la Figura A.3. 9.

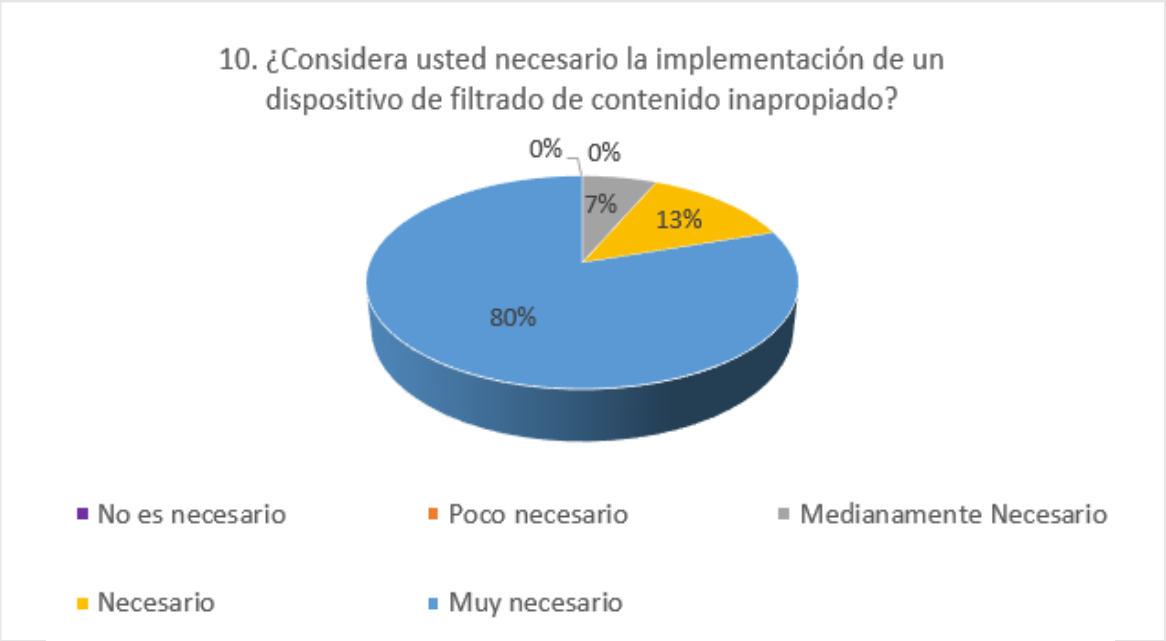

Figura A.3. 10 Necesidad de implementación de un dispositivo de filtrado de contenido inapropiado según la percepción de los usuarios.

Los resultados obtenidos se muestran en la Figura A.3. 10. Los usuarios están conscientes de la problemática, razón por la cual, la solución planteada tendrá buena acogida. Adicionalmente, todos los usuarios coinciden en que es prioridad cuidar del bienestar psicológico de los niños, adolescentes y jóvenes de la comunidad que asisten a la fundación.

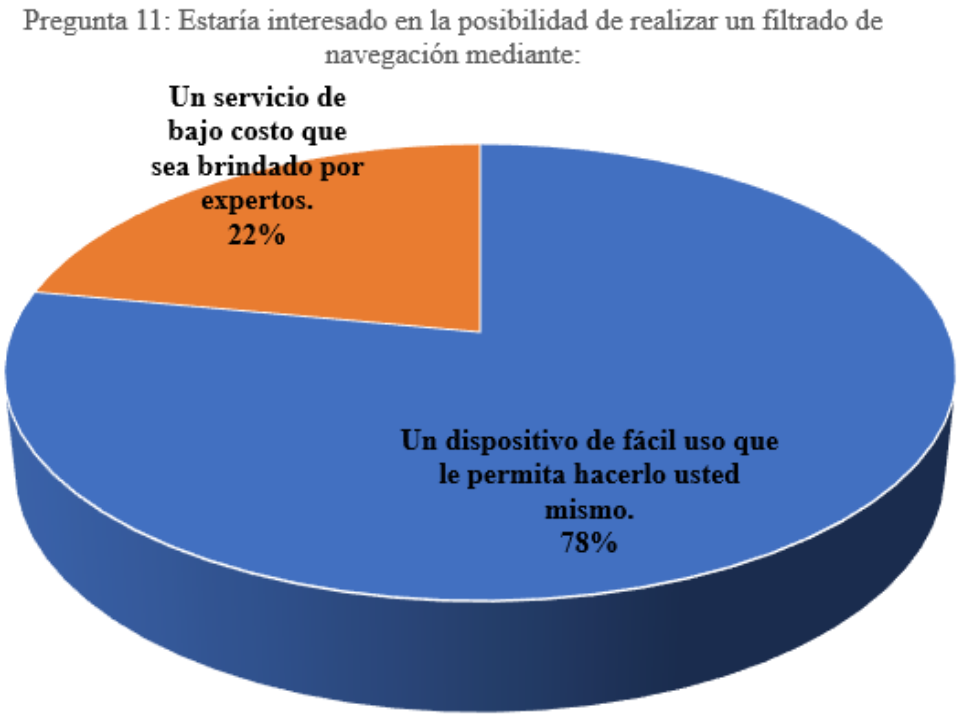

Figura A.3. 11 Conveniencia percibida por los usuarios de que la solución sea concebida como producto o servicio.

En la Figura A.3. 11 podemos observar que el 78% de los encuestados estarían interesados de que la solución sea concebida como un dispositivo, y expresaron que les preocupa estar sujetos a un servicio ya que implica depender de terceras personas.

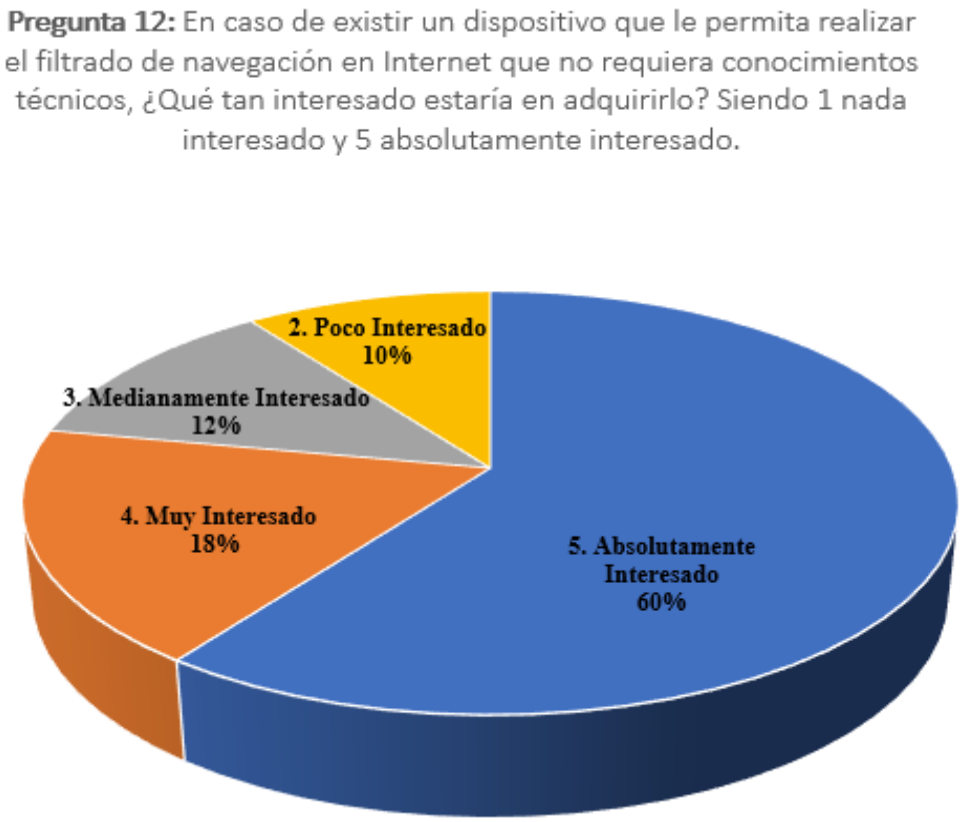

Figura A.3. 12 Interés de los usuarios por la solución específica planteada.

En los resultados mostrados en la Figura A.3. 12 son muy interesantes ya que indica que el 60% de los encuestados se encuentra absolutamente interesado en adquirir este dispositivo, lo cual significa que es factible su comercialización.

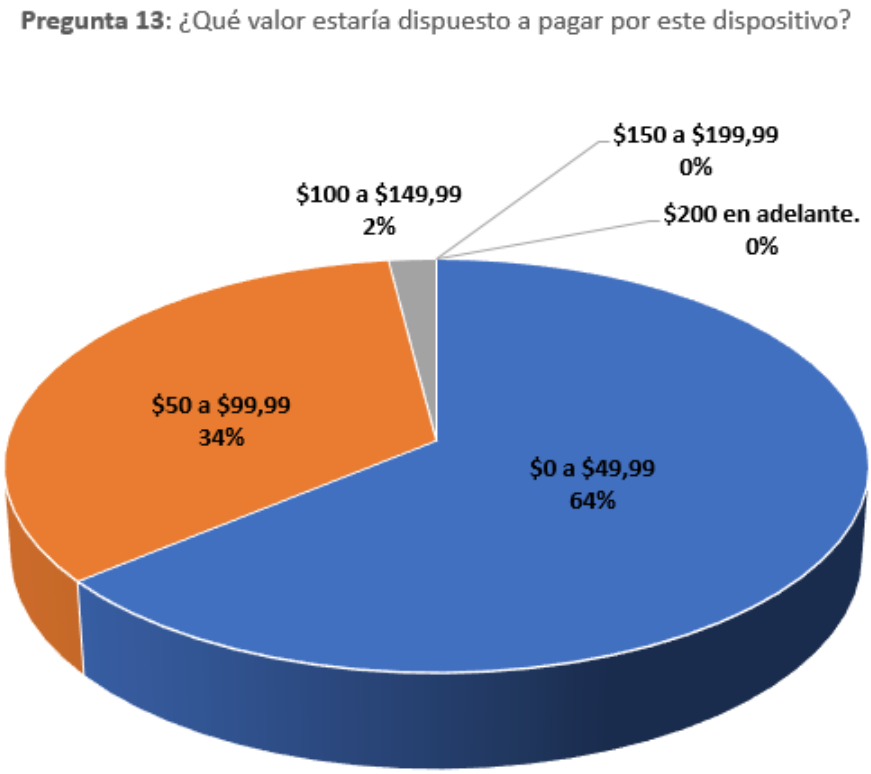

Figura A.3. 13 Rango de precio del dispositivo razonable según los usuarios encuestados.

En la Figura A.3. 13 se muestra que el 64% de las personas coinciden en que el precio del dispositivo debe ser menor de $50.00 dólares, lo cual representa un desafío ya que tenemos que buscar la manera de abaratar los costos para poder comercializar el producto con un precio final cercano a dicha cifra y así satisfacer los requerimientos del mercado, esto debe ser considerado a corto y a mediano plazo.

ANEXO 4

FOTOS DE LAS ENTREVISTAS Y ENCUESTAS REALIZADAS

Figura A.4. 1 Visita a la fundación para realizar entrevistas.

La Figura A.4. 1 muestra la entrevista realizada a una usuaria de los servicios que presta el Centro de Desarrollo Integral 314 de la Fundación “Compassion International”.

Figura A.4. 2 Visita a la fundación para realizar entrevistas.

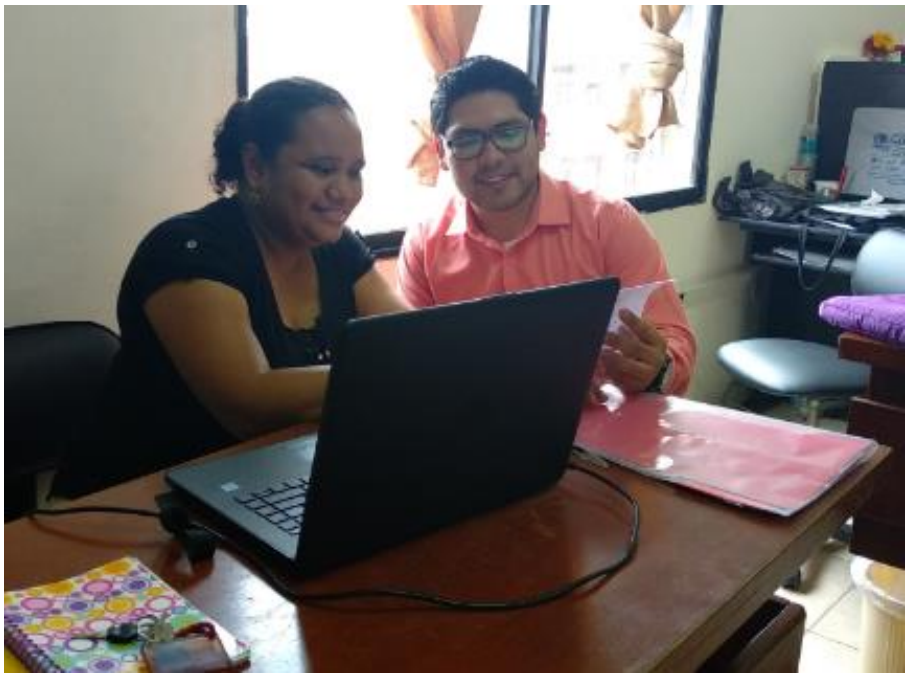

Figura A.4. 3 Visita a la fundación para realizar entrevistas.

Figura A.4. 4 Visita a la fundación para realizar entrevistas.

Las Figura A.4.2, Figura A.4.3 y Figura A.4.4 se muestran las entrevistas realizadas a algunos de los docentes y tutores que colaboran con el Centro de Desarrollo Integral 314 de la Fundación “Compassion International”.

Figura A.4. 5 Encuestas realizadas durante la visita a la fundación.

Figura A.4. 6 Encuestas realizadas durante la visita a la fundación.

Figura A.4. 7 Encuestas realizadas durante la visita a la fundación.

En las Figura A.4.5, Figura A.4.6 y Figura A.4.7 podemos observar a algunos de los padres de familia cuyos hijos asisten al Centro de Desarrollo Integral 314, realizando las encuestas de este proyecto.

ANEXO 5

MAPAS DE EMPATÍA

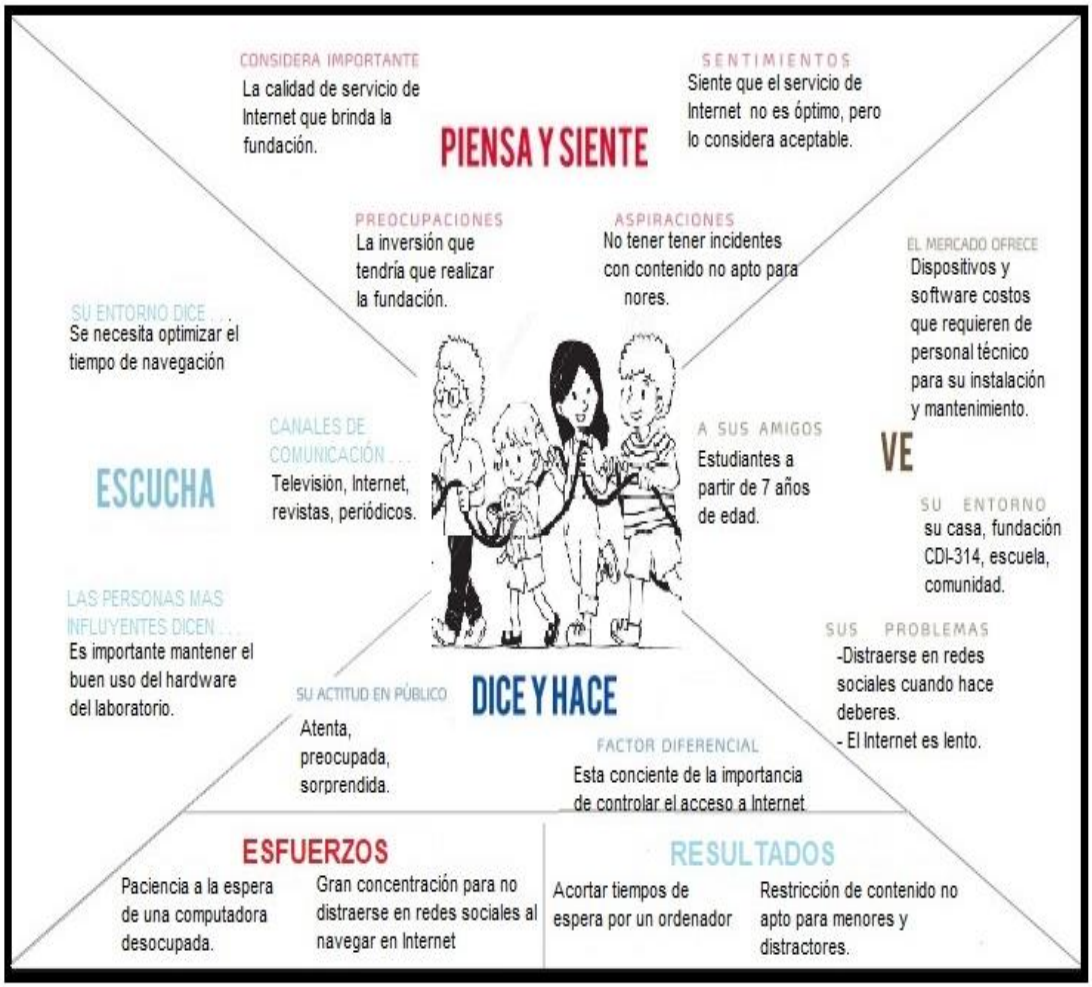

Figura A.5. 1 Mapa de empatía de estudiantes [Autoría Propia].

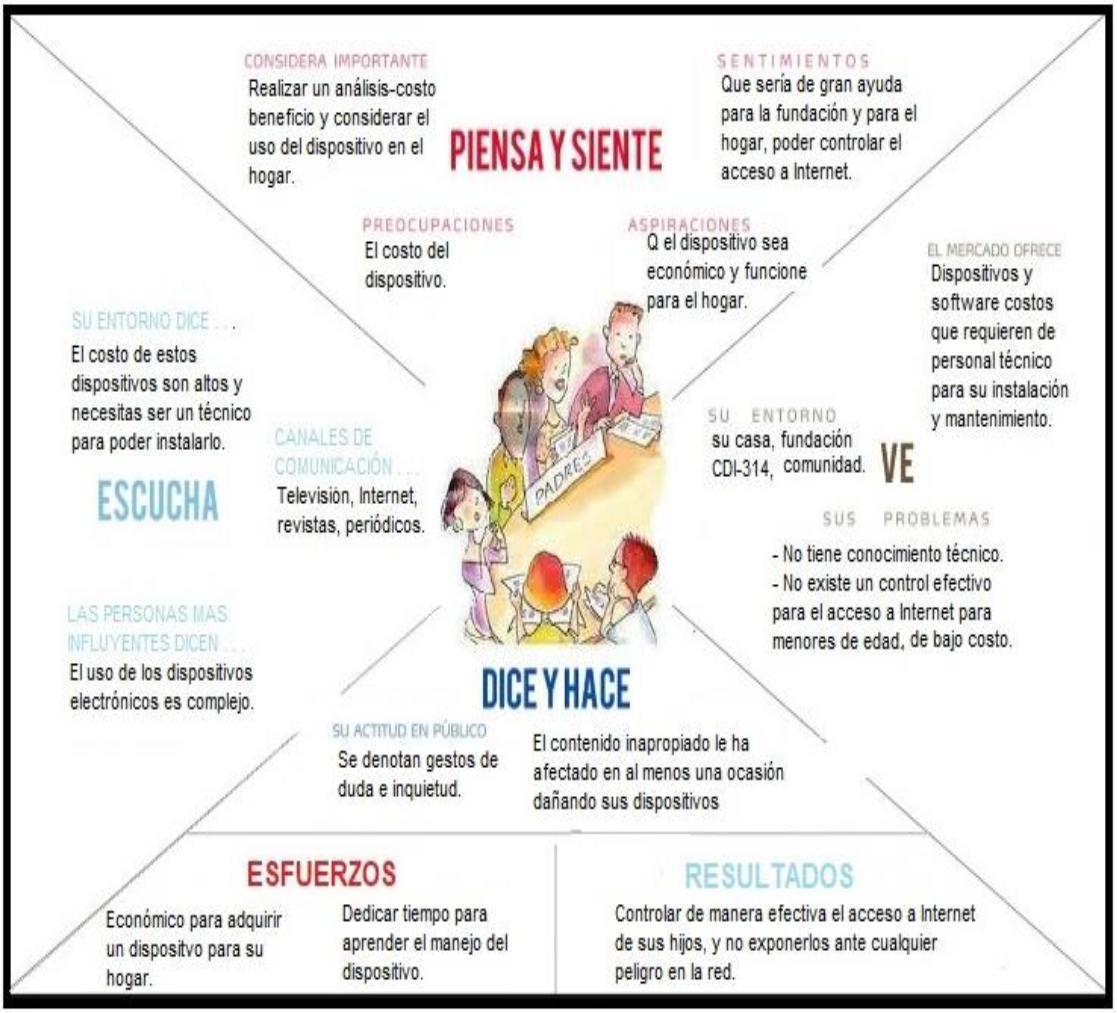

Figura A.5. 2 Mapa de empatía de padres de familia [Autoría Propia].

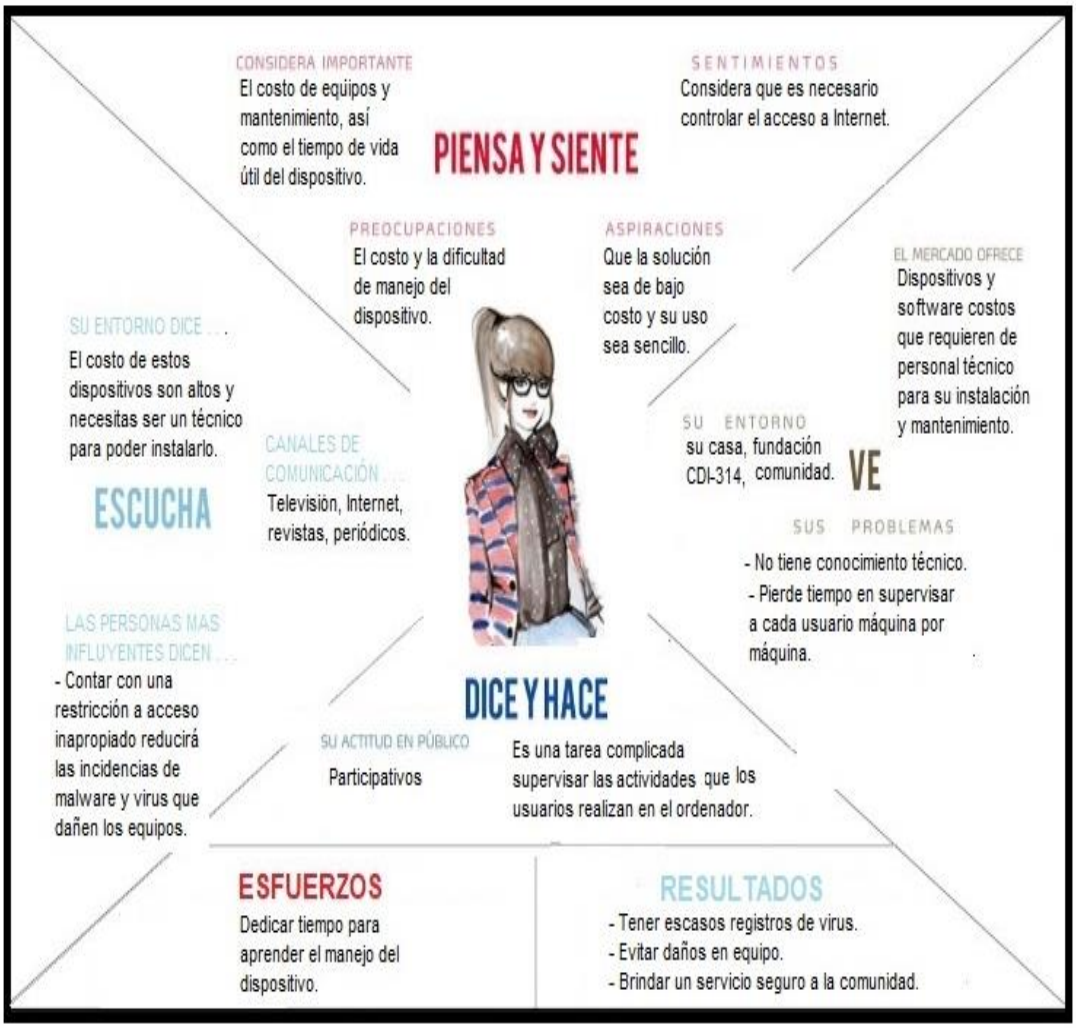

Figura A.5. 3 Mapa de empatía de docentes y tutores [Autoría Propia].

ANEXO 6

LLUVIA DE IDEAS

1. Impartir charlas donde psicólogos expertos en el tema expongan a padres, docentes y tutores lo influyente que puede ser acceder a contenido no apropiado para personas sin criterio formado.
2. Instalar antivirus en los ordenadores del laboratorio.
3. Capacitar a niños, adolescentes y jóvenes sobre cómo actuar en casos de tener acceso a contenido inapropiado de manera involuntaria.
4. Crear una aplicación que genere alertas en un computador central monitorizado por un supervisor cuando los usuarios accedan a contenido inadecuado.
5. Implementación de nuevas políticas al ingresar al laboratorio como por ejemplo el usuario menor de edad solo puede acceder al laboratorio con un adulto responsable de monitorear su navegación web.
6. Organizar la posición física de las computadoras dentro del laboratorio de manera que puedan ser visualizadas por un docente o tutor y los demás usuarios.
7. Restringir el acceso a los usuarios reincidentes en la navegación de sitios web no autorizados.
8. Crear cuentas de usuarios de red, asociarlos a grupos de acceso y filtrado dependiendo de la información de cada persona como: edad, formación, profesión, etc.
9. Elaborar un listado de sitios web de contenido inapropiado y registrarlos como sitios bloqueados en cada computadora del laboratorio.
10. Configurar el bloqueo de pop-ups en los navegadores de Internet.
11. Limitar y/o bloquear la descarga de archivos de extensiones ejecutables.
12. Bloquear la descarga y el uso de los juegos en línea.
13. Elaborar un horario de acceso preferente al laboratorio de acuerdo con las edades de los usuarios.
14. Implementar un único dispositivo centralizado que realice el parental control para toda la red interna.
15. Enviar informe de historial de navegación de los usuarios a los padres de familia.
16. Fomentar mediante charlas el uso seguro, responsable y constructivo de Internet y de sus dispositivos asociados.

17. Crear una base de datos que contenga el historial de navegación web por usuario para ser revisado por los docentes y en caso de existir anomalías estas sean reportadas.

18. Denegar el intercambio de archivos en redes entre pares (P2P).

19. Configurar los buscadores para evitar que muestren contenido para adultos.

20. Colocar carteles promoviendo el buen uso del Internet en lugares de alta concurrencia de personas de la comunidad como tiendas, farmacias, lugares de comida, entro otros.

21. Diseñar un mouse con lector de huellas digitales para poder detectar la edad del usuario antes de iniciar sesión en los ordenadores y a su vez de manera automática se realice el bloqueo de contenido inadecuado según un perfil establecido por su edad.

22. Implementar un lector facial para que al colocarse delante del computador se inicie sesión de manera automática relacione al usuario con un nivel de filtrado correspondiente y previamente configurado.

23. Instalar una herramienta que muestre una ventana emergente con un mensaje de advertencia al acceder a contenido inadecuado sin opción a continuar o retroceder.

24. Crear un dispositivo con una pantalla táctil e interfaz amigable de uso sencillo que físicamente sea pequeño para ser cómodamente manipulado.

25. Crear un blog donde los usuarios nos cuenten sus experiencias con contenido inadecuado para poder emitir recomendaciones.

26. Crear un perfil donde se puedan agregar sitios web específicos según el criterio de un usuario supervisor.

27. Crear un sistema de autenticación en el dispositivo mediante huella dactilar antes de elegir los perfiles mencionados para los niños no puedan acceder.

28. Impartir cursos para los padres de familia, docentes, tutores y adultos donde se garantice el aprendizaje del buen uso del servicio de Internet.

29. Cambiar en los ordenadores el sistema operativo a Linux para reducir el riesgo de los virus y evitar que los usuarios instalen aplicaciones.

30. Crear un canal de YouTube y elaborar documentos tutoriales dirigido a para los padres de familia, docentes y tutores con contenido específico de todo lo que ellos deben saber acerca de seguridad informática y prevención de incidentes.

ANEXO 7

MATRIZ IMPORTANCIA - DIFICULTAD

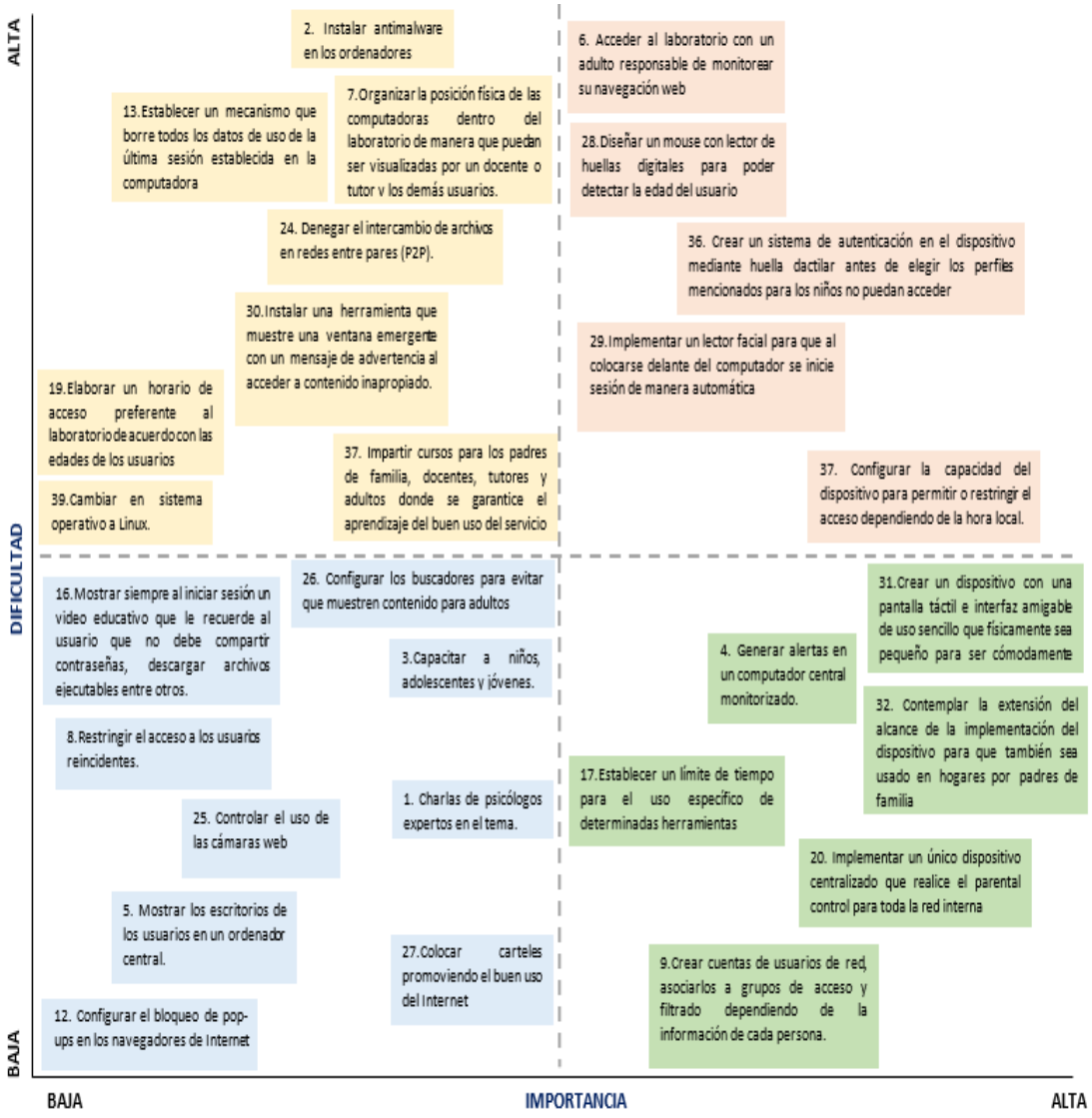

Figura A.7. 1 Matriz Importancia – Dificultad [Autoría Propia].

ANEXO 8

MATRÍZ DE DECISIONES

	SOLUCIONES				
NECESIDADES	Implementación de un servidor Proxy en el laboratorio de la fundación.	Contratación del servicio de Parental Control que ofrecen las licencias de los antimalware u otras aplicaciones.	Implementación de un dispositivo para filtrar la navegación web hardware de bajo costo	Configuración de filtrado en el sistema operativo o en los navegadores web en cada ordenador de manera individual.	Implementación de un sistema de alertas para cuando el usuario ingrese a contenido inapropiado.
Evitar el uso de la infraestructura del laboratorio para acceder a contenido inadecuado.	5	5	5	4	1
Impedir que los ordenadores se infecten con malwares.	4	5	4	3	1
Limitar el tiempo de uso del servicio de Internet dependiendo de las actividades a realizar por el usuario.	3	4	4	1	1
Impartir conocimiento sobre el correcto uso de los navegadores y demás herramientas de acceso a Internet.	1	2	3	1	1
Proporcionar una solución de bajo costo para filtrado de navegación web.	2	3	5	5	2
Brindar la capacidad de realizar el bloqueo de contenido no apto para menores de forma simple y eficiente.	5	5	5	3	2
Permitir a un usuario supervisor personalizar uno de los perfiles según su criterio.	4	2	5	4	4
Monitorear el acceso a contenido inapropiado desde un único dispositivo central	5	2	5	2	4
Bajo Costo	2	2	5	4	4
Portabilidad de la Solución	1	1	4	1	1
TOTAL	32	31	45	28	21

SATISFACE TOTALMENTE	5	SATISFACE LO SUFICIENTE	4	SATISFACE MODERADAMENTE	3	SATISFACE MUY POCO	2	NO SATISFACE	1

Figura A.8. 1 Matriz de decisiones [Autoría Propia].

ANEXO 9

MATRÍZ DE FEEDBACK

Figura A.9. 1 Matriz de Feedback [Autoría Propia].

ANEXO 10

MANUAL DE USUARIO DE MIPIBLOCK

El dispositivo MiPiBlock es de uso intuitivo ya que está diseñado para un usuario final sin mayor conocimiento técnico, a continuación se detallan las diferentes pantallas con su respectiva funcionalidad.

- **Dispositivos.**

  En esta pantalla podemos observar recuadros con la información de red de todos los dispositivos que se encuentran conectados al Router, entre estos estarán tabletas, celulares, ordenadores portátiles, entre otros. Al presionar en el icono del monitor dentro del recuadro, se muestra el historial de los sitios webs que ha visitado ese dispositivo. El botón on/off permite habilitar o deshabilitar el bloqueo esté realizando MiPiBlock, al presionar el botón se mostrará una ventana de advertencia en la cual el usuario podrá confirmar su acción o cancelar.

  En la parte superior izquierda encontramos también el icono “retroceder”, este permite regresar al menú principal.

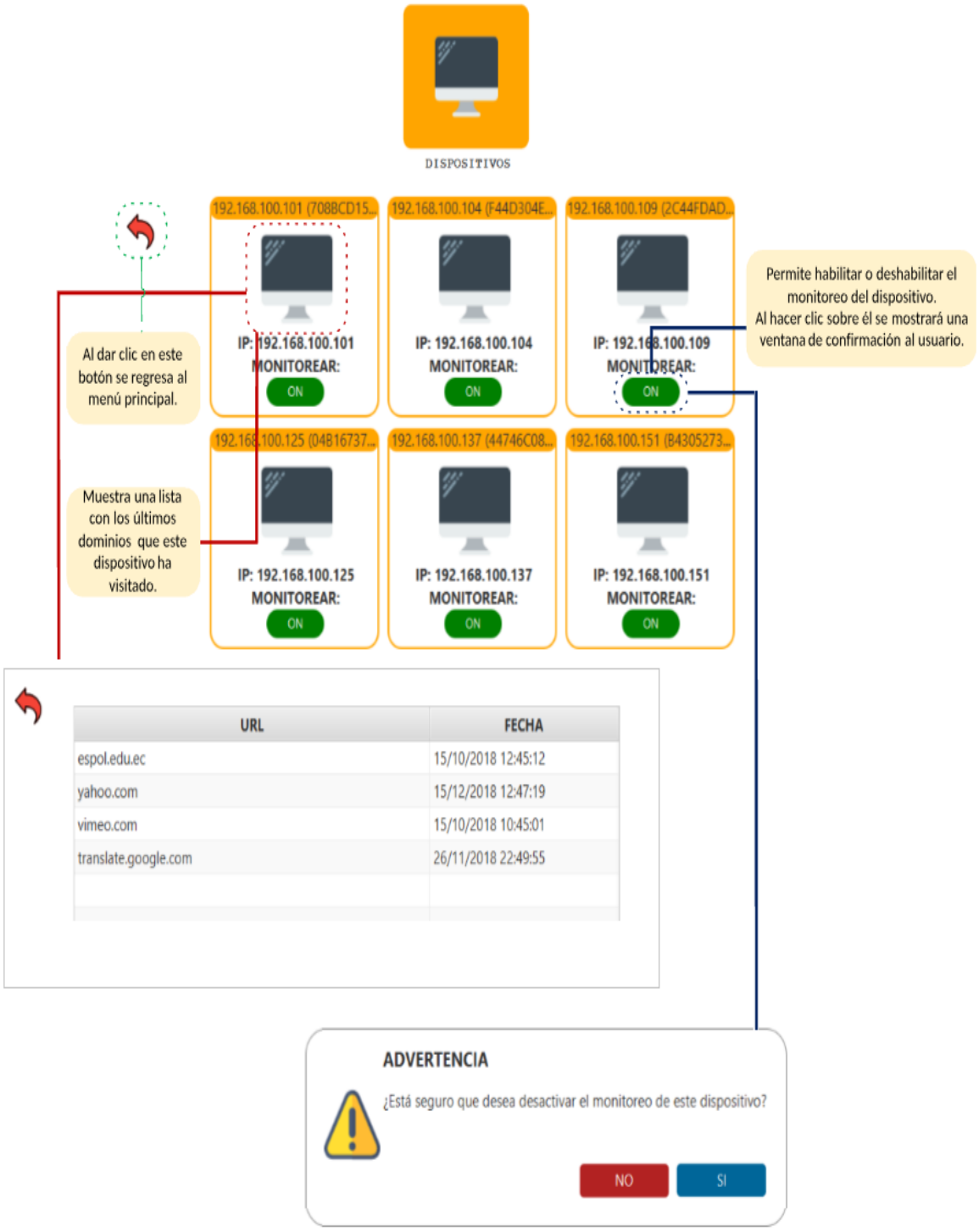

Figura A.10. 1 Módulo de la opción “Dispositivos” de Mipiblock [Autoría Propia].

- **Anuncios.**

Esta opción permite habilitar o deshabilitar los anuncios publicitarios en forma de ventanas emergentes que se muestran al navegar. Para habilitar este filtrado se debe seleccionar el icono “INACTIVO”, luego de esto se muestra una ventana con un mensaje de advertencia el cual nos indica: “¿Está seguro de que desea activar la protección contra anuncios?” Al elegir la opción “SI” se aplica el filtrado, caso contrario no se realiza ninguna acción.

Figura A.10. 2 Módulo Anuncios del MiPiBlock [Autoría Propia].

- **Redes Sociales.**

En esta pantalla podemos encontrar cinco redes sociales predeterminadas para administrar su bloqueo de manera independiente. Para bloquear cualquiera de ellas solo se debe presionar el botón “INACTIVO” junto a la red social que desee bloquear, luego confirmar el bloqueo dando clic en “SI” en la ventana que se abrirá con el mensaje de confirmación. A continuación se muestra cómo se realiza el bloqueo de una red social en el módulo “Redes Sociales” de MiPiBlock.

Figura A.10. 3 Módulo Redes Sociales de MiPiBlock [Autoría Propia].

- **Filtrado por Categoría.**

  El módulo “Filtrado por categorías” permite habilitar o deshabilitar el bloqueo de diferentes categorías de filtrado como: redes sociales, tiendas en línea, sexo, pornografía y violencia. Al hacer clic sobre el botón con el nombre de la categoría elegida, se mostrará un mensaje de confirmación donde el usuario podrá dar clic en “SI” para habilitar o deshabilitar el bloqueo, caso contrario no se realizará ninguna acción.

Figura A.10. 4 Módulo de Filtrado de Categoría [Autoría Propia].

- **Bloqueo por páginas.** En esta pantalla se puede realizar un bloqueo específico, es decir por páginas web. Para poder realizar este bloqueo se coloca la URL en el cuadro de texto, se da clic en agregar. Aparece una venta de advertencia en la cual se puede confirmar o cancelar el bloqueo. En la parte izquierda de la pantalla se cuenta con espacio destinado para que se puedan visualizar los URL de los sitios web que estén bloqueados en ese momento. En la Figura A.10. 5 se pueden apreciar las opciones del módulo de bloqueo por páginas.

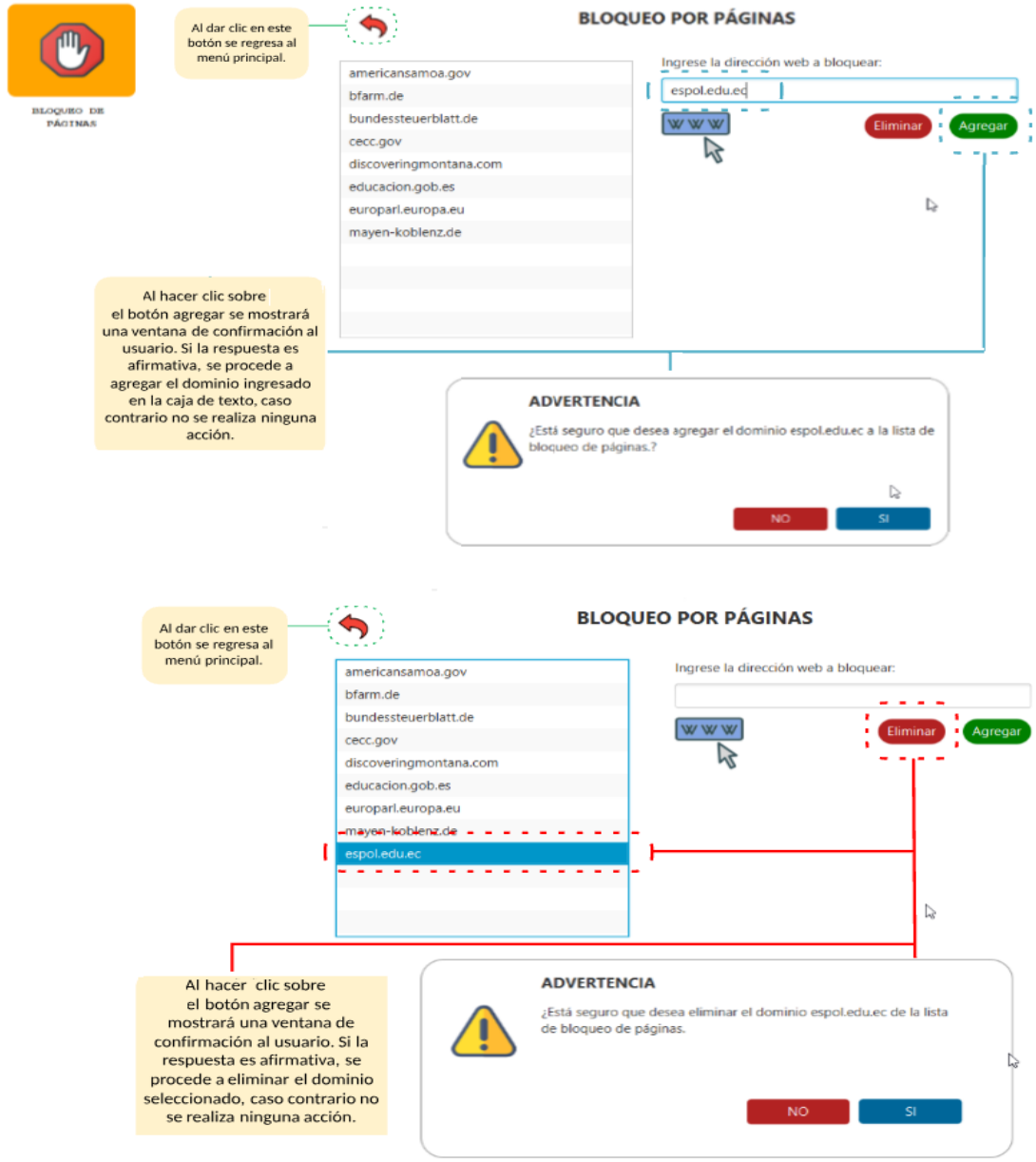

Figura A.10. 5 Módulo Bloqueo de Páginas de Mipiblock [Autoría Propia].

- **Configuración.**

  Esta opción muestra la información de red configurada en MiPiBlock. Además, permite habilitar o deshabilitar el monitoreo de los nuevos dispositivos que se vayan sumando a la red. Para esta última opción se muestra un mensaje de advertencia en donde el usuario puede confirmar o cancelar su acción. También, cuenta con un icono en forma de signo de interrogación el cual muestra la información acerca de los creadores del dispositivo.

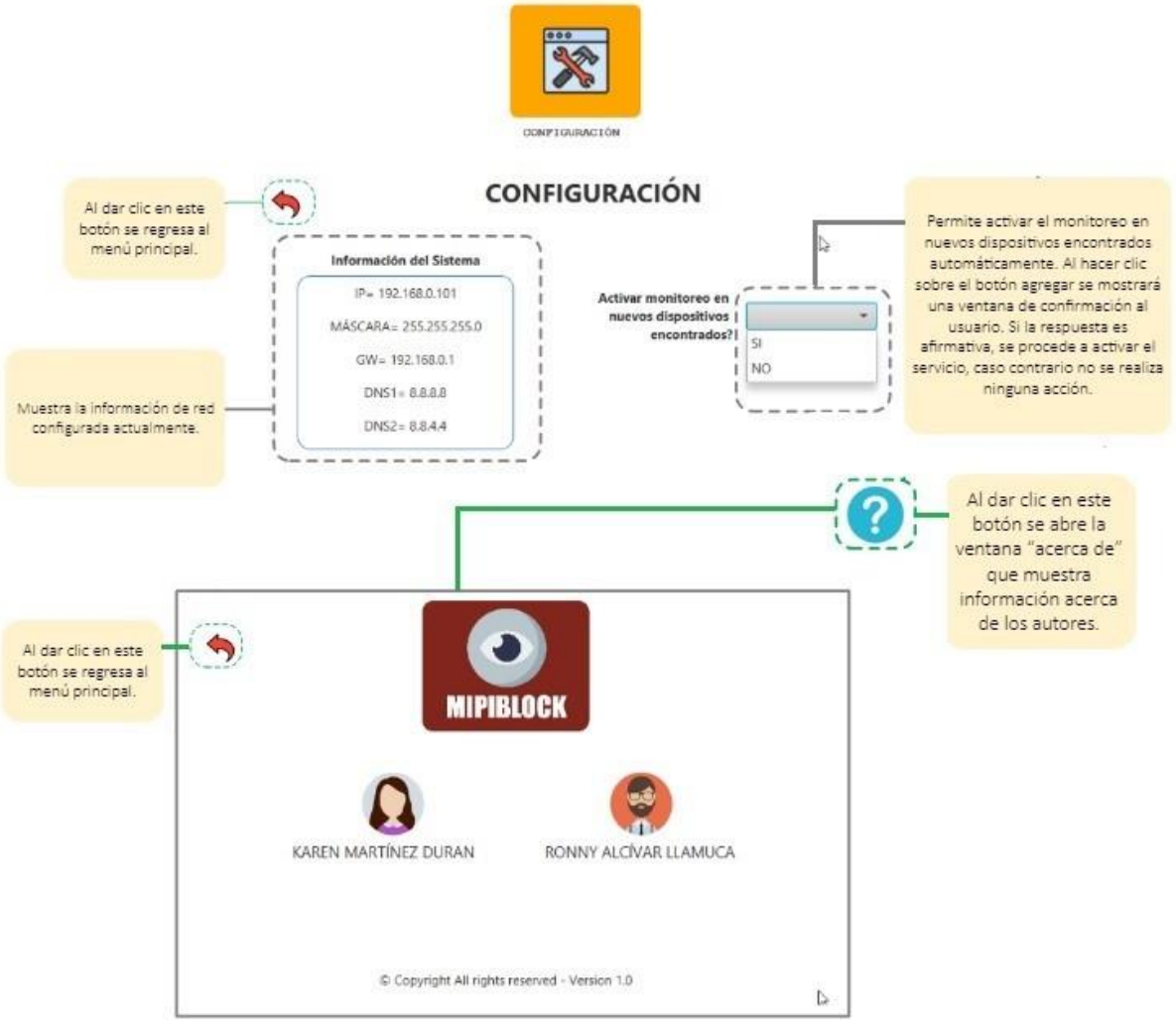

Figura A.10. 6 Módulo Configuración de Mipiblock [Autoría Propia].

ANEXO 11

CAMBIO DE PIN EN DISPOSITIVO MIPIBLOCK

Para poder realizar el cambio de PIN debemos recordar que el PIN por defecto es “123456” y podrá ser reemplazado por un PIN de seis dígitos.

- Paso 1: Tener a mano el código PUK que viene incluido en una tarjeta al momento de adquirir el producto.

- Paso 2: En el menú principal dar clic al icono del candado que se encuentra en la parte superior derecha.

- Paso 3: En la nueva pantalla dar clic donde dice **RECUPERAR PIN**

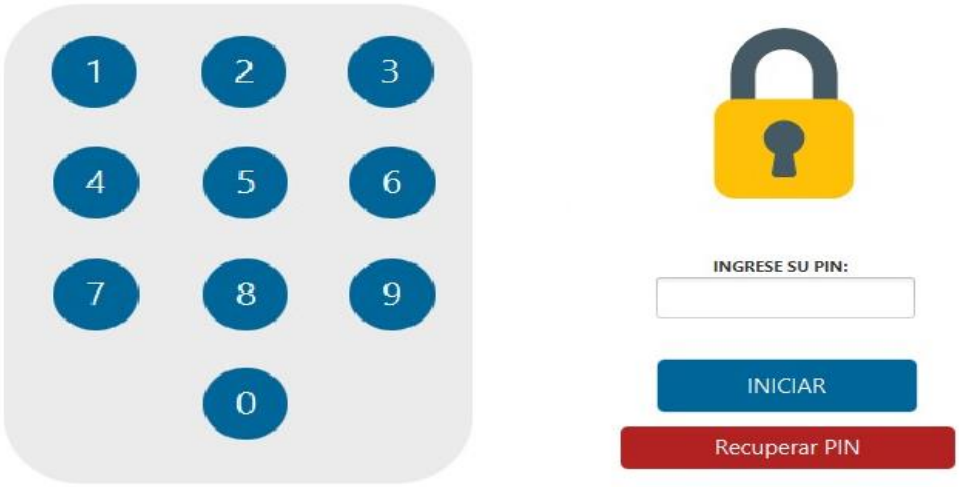

Figura A.11. 1 Pantalla de ingreso o recuperación de PIN [Autoría Propia].

- Paso 4: se mostrará la pantalla a continuación donde debemos ingresar toda la información solicitada y al final dar clic en “CAMBIAR PIN”.

Figura A.11. 2 Pantalla de recuperación de código PIN [Autoría Propia].

- Paso 5: Se mostrará esta pantalla en la cual podrá realizar el cambio, una vez que los datos ingresados sean confirmados.

Figura A.11. 3 Pantalla de cambio de PIN [Autoría Propia].

ANEXO 12

FOTOS DE LAS PRUEBAS REALIZAS CON MIPIBLOCK

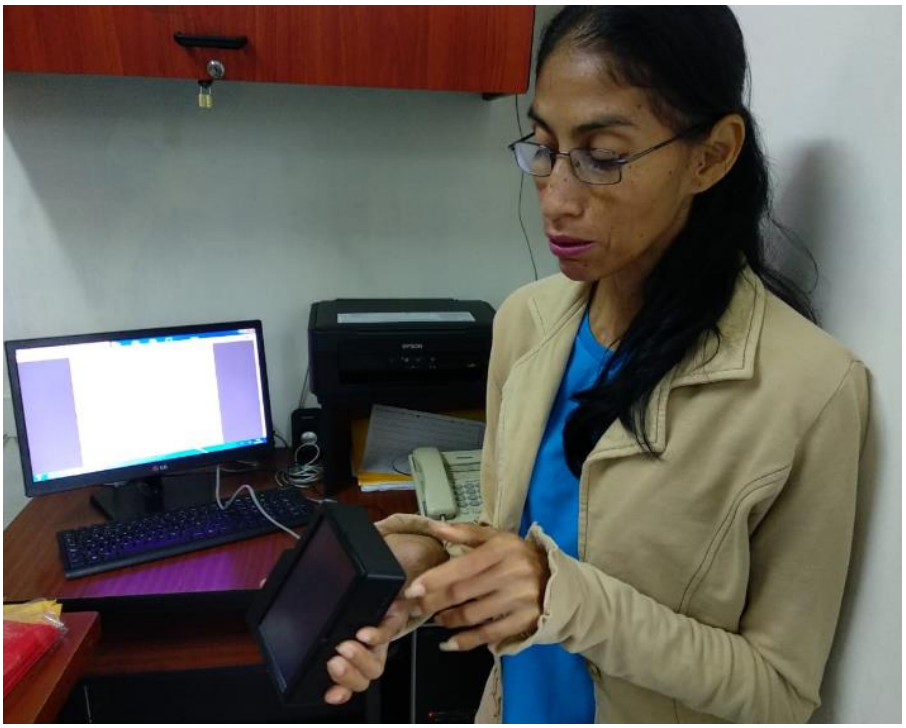

Figura A.12. 1 Visita para pruebas de interacción de los usuarios con MiPiBlock.

Figura A.12. 2 Visita para pruebas de interacción de los usuarios con MiPiBlock.

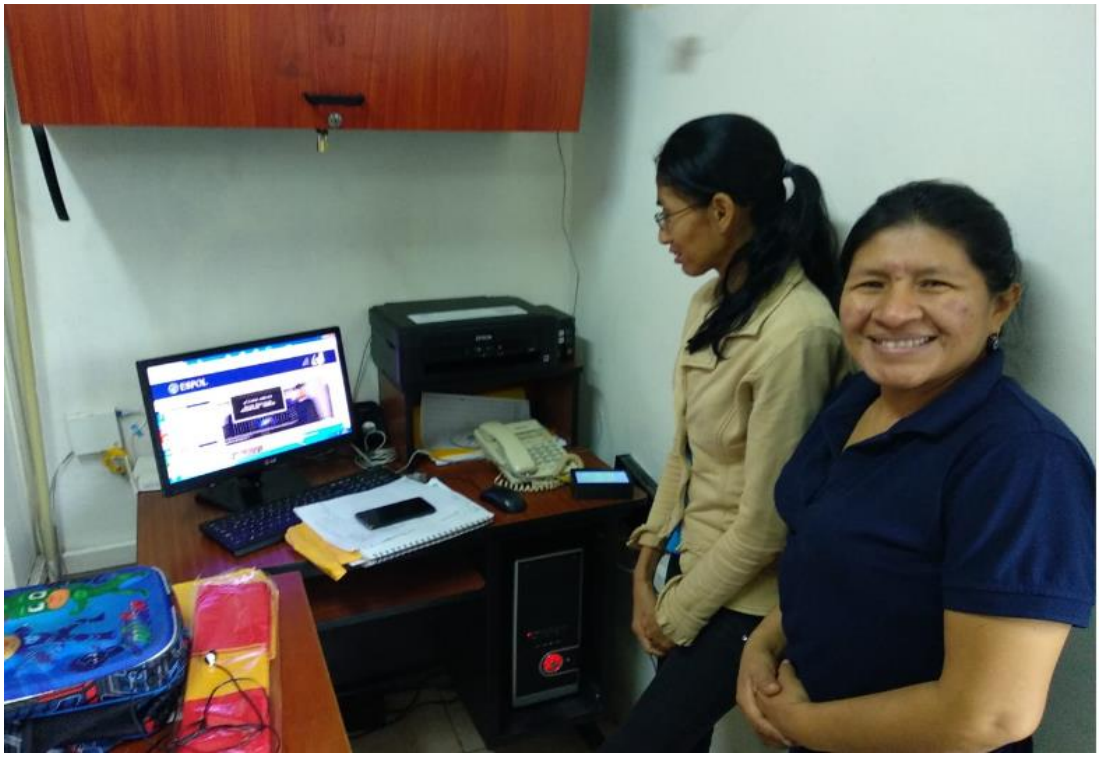

Figura A.12. 3 Visita para pruebas de interacción de los usuarios con MiPiBlock.

Figura A.12. 4 Visita para pruebas de interacción de los usuarios con MiPiBlock.

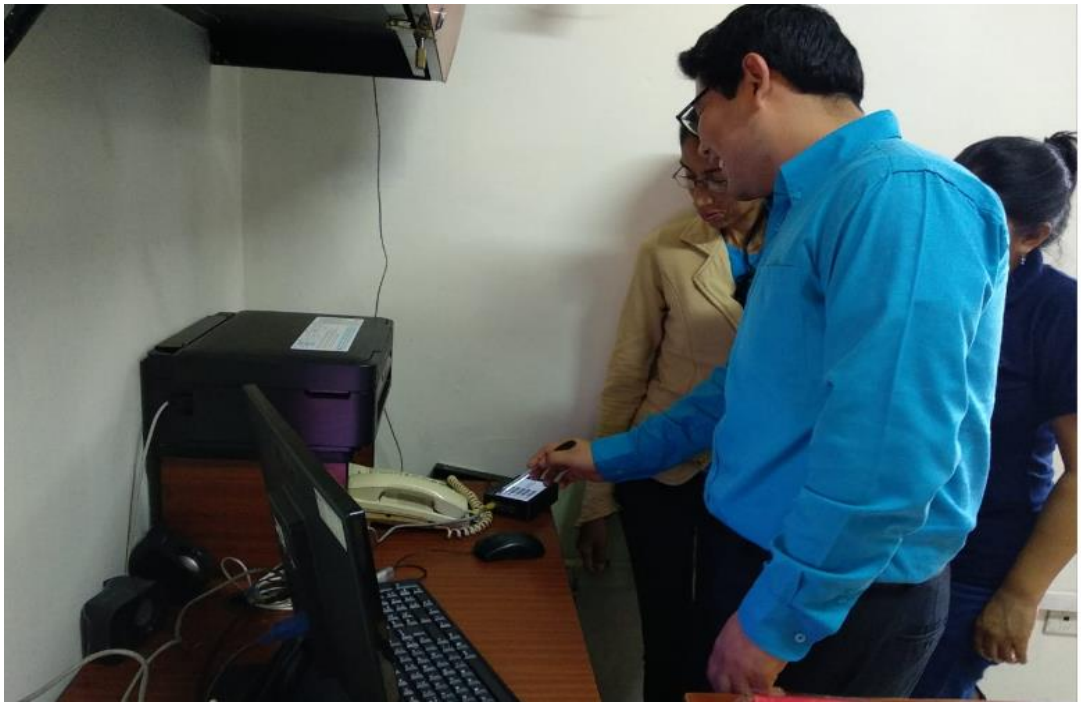

Figura A.12. 5 Visita para pruebas de interacción de los usuarios con MiPiBlock.

Figura A.12. 6 Visita para pruebas de interacción de los usuarios con MiPiBlock.

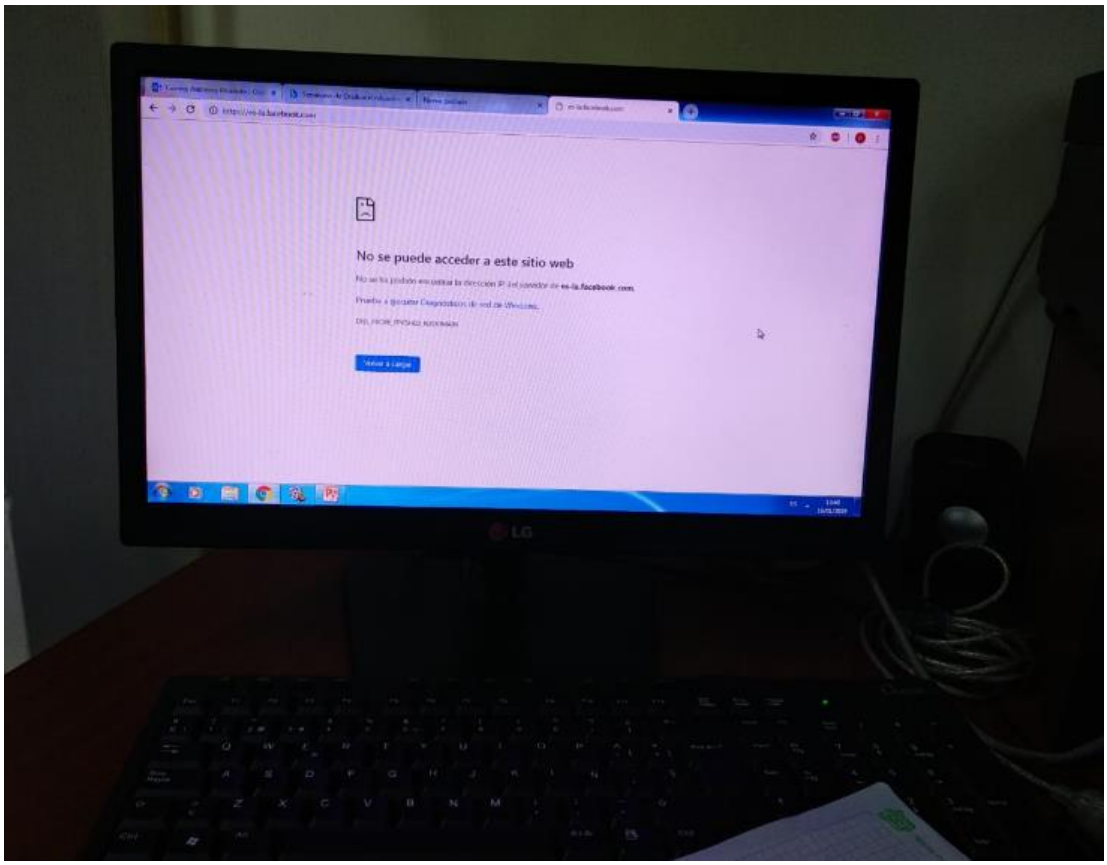

Figura A.12. 7 Visita para pruebas de interacción de los usuarios con MiPiBlock.