UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACUTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Proyecto de Investigación, previo a la obtención del título de:

INGENIERO EN SISTEMAS

"Desarrollo e implementación de un navegador web seguro con configuración de vigilancia parental para control y análisis del uso de internet y redes sociales en los adolescentes del Colegio Innova del cantón Salinas, Provincia de Santa Elena."

AUTORES

WASHINGTON HERNÁN NIETO MATAMOROS
GABRIEL ALBERTO BORBOR VERA

PROFESOR TUTOR

ING. LÍDICE VICTORIA HAZ LÓPEZ, MSC.

LA LIBERTAD – ECUADOR
2016

AGRADECIMIENTO

Quiero agradecer a mis padres y a mi querida esposa por todo el apoyo y la confianza que me han brindado durante todos estos años de mi carrera, a mis docentes por ser guías durante todo este periodo de aprendizajes, y a mi tutora académica por todo el apoyo y paciencia que nos ha brindado durante todo este tiempo.

Washington Hernán Nieto.

AGRADECIMIENTO

Quiero agradecer a mis padres por todo el apoyo y la confianza depositada en mí, durante todos estos años de mi carrera, a mis profesores por ser la guía en este largo recorrido de conocimientos, y a mi tutora académica por la paciencia, el soporte y la ayuda que ha mostrado y brindado durante todo el tiempo invertido en este proyecto.

Gabriel Borbor Vera.

APROBACIÓN DEL TUTOR

En mi calidad de tutora del trabajo de titulación denominado: **"Desarrollo e implementación de un navegador web seguro con configuración de vigilancia parental para control y análisis del uso de internet y redes sociales en los adolescentes del Colegio Innova del cantón Salinas, Provincia de Santa Elena",** elaborado por los estudiante **Nieto Matamoros Washington Hernán** y **Borbor Vera Gabriel Alberto,** de la carrera de Informática de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicia los trámites legales correspondientes.

La Libertad, Octubre de 2016

……

Ing. Lídice Victoria Haz López, MSc.

TRIBUNAL DE GRADO

Ing. Walter Orozco Iguasnia, MSc.
DECANO DE FACULTAD

Ing. Mariuxi De La Cruz De La Cruz, MSIG.
DIRECTORA DE CARRERA

Ing. Lídice Haz López, MSc.
PROFESORA TUTORA

Ing. Iván Coronel Suárez, MSIA.
PROFESOR DE ÁREA

Ab. Brenda Reyes Tomalá, Mgt.
SECRETARIA GENERAL

RESUMEN

El presente trabajo tiene como objetivo analizar el comportamiento de los adolescentes con respecto al uso del internet y la redes sociales dentro del aula de clases, además, el diseño e implementación de un navegador web que permita aplicar un control no solo de tipo parental, sino también monitorear y restringir el acceso a redes sociales, servicios de proxys en línea y las descargas de archivos multimedia dentro del laboratorio informático del Colegio Innova. La investigación planteada es de tipo cuantitativa con enfoque descriptivo y correlacional, se plantearon 4 hipótesis en la modalidad lógica que involucran dos variables independientes y cuatro dependientes. Para dar respuesta a las interrogantes planteadas, se utilizaron metodologías de investigación como la observación científica y de campo, también se aplicaron herramientas de control y monitoreo informático, además de una encuesta para la validación y aceptación del navegador desarrollado. El uso del navegador permite controlar de manera eficiente los contenidos a los que acceden los estudiantes en el laboratorio de informática, evitando que éstos puedan navegar a redes sociales o sitios inseguros o con contenidos inapropiados para su edad.

Palabras claves:

Control parental, navegadores, proxys en línea, redes sociales, archivos multimedia.

ABSTRACT

This paper aims to analyze the behavior of adolescents regarding the use of internet and social networks within the classroom, also, the design and implementation of a web browser that can implement control not only parental type but also monitor and restrict access to social networks, online services proxy and downloads of multimedia files in the computer lab of the Innova School. The quantitative research is raised type with descriptive and correlational approach, four hypotheses were raised in logic mode involving two independent variables and four dependents. To answer the above questions, research methodologies as scientific and field observation were used, control tools and computer monitoring were also applied, in addition to a survey for the validation and acceptance browser developed. Using the browser allows efficiently control the content accessed by the students in the computer lab, preventing them to navigate social networking sites or unsafe or inappropriate content for their age.

Keywords:

Parental control, web browsers, online services proxy, social networks, multimedia files.

DECLARACIÓN.

El contenido del presente Trabajo de Graduación es de nuestra responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

_____	_____
Washington Hernán Nieto Matamoros	Gabriel Alberto Borbor Vera.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ITEM DESCRIPCIÓN **PÁGINA**

ÍNDICE DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

Desde su creación, el internet vive en una constante evolución de manera acelerada que lo ha transformado en una herramienta casi indispensable para el desarrollo de todas las actividades que se realizan en la sociedad. Su uso constante ha cambiado la forma de ver y entender las cosas, sus aplicaciones van desde las tareas de educación, industrias, comercio, medicina, etc.; ya que permite agilizar nuestras actividades diarias, como poder interactuar con personas de todo el mundo, realizar transacciones bancarias, comprar artículos de interés las 24 horas del día en tiendas virtuales de todo el mundo, leer revistas y periódicos digitales, cursos y clases en línea, además, de tener a nuestro alcance múltiples aplicativos de utilidad destinados a hacer nuestra vida más fácil.

En la web se puede encontrar todo tipo de información y contenido, tales como, entretenimiento (películas, música, videos), actividades caseras (recetas de limpieza, cocina), contenidos educativos (libros, revistas, documentales). El internet, también ha modificado el comportamiento social, brindando sitios virtuales donde se pueda crear relaciones de amistad con personas en todo el mundo, estas páginas especializadas, son conocidas como redes sociales, y son los sitios de mayor concurrencia. Además, internet es una herramienta globalizada, que a través de un clic, se puede compartir y tener acceso a toda información y conocimientos.

Estas posibilidades de acceso a la comunicación e información que dispone la web, pueden convertir a internet en una herramienta peligrosa a través de la cual se podría vulnerar la seguridad e integridad lógica del computador.

Asimismo, en internet existen personas que se aprovechan del anonimato en la web para acosar, humillar, amenazar y /o desprestigiar a otras por medio de redes sociales, portales de chat o juegos en línea, causando daños psicológicos en las víctimas, entres estos casos se encuentran dos tipos de delitos: el Ciberbullying y el Ciberacoso, estos se diferencian en que el Ciberbullying involucra a dos menores en ambos extremos (el acosador y la víctima), mientras que el Ciberacoso, se refiere

cuando existe acoso tanto psicológico como sexual entre dos adultos; también existe un tercer delito que específica el acoso psicológico y sexual entre adultos y menores, denominado Ciberstalking.

Otro de los delitos informáticos más comunes que ocurren en internet, es el robo de información a través de técnicas de ingeniería social, entre las cuales podemos mencionar: el scam, que consiste en la clonación de páginas de confianza como Facebook o alguna entidad bancaria para engañar y robar a las personas sus datos (usuario, contraseña, claves, cuentas bancarias, entre otros); el phishing, que se basa en engañar a los usuarios por medio del spam (publicidad en internet) en páginas web o correo electrónico, dónde el atacante se hace pasar por una persona o empresa de confianza para obtener los datos del usuario; por último, tenemos las páginas con contenido malicioso que se basan en el uso de ventanas emergentes alojadas en páginas de interés para el usuario y así infectar el equipo con malware, virus, spyware o cualquier otro software dañino.

Del mismo modo, el uso excesivo de internet puede provocar trastornos sociales que afectan nuestra vida y círculo social, como problemas de conducta, aislamiento, dificultad para establecer relaciones sociales y adicción, sin mencionar que, existen muchos portales web con contenido inadecuado al que se tiene acceso libremente, dejando expuestos a los menores de casa.

Por lo antes expuesto, es importante que se tomen medidas de seguridad al momento de acceder a internet como la configuración de los controles parentales disponibles en los navegadores web y en el sistema operativo windows, la instalación y configuración de software, equipos o dispositivos de firewall y proxy que permitan definir políticas de seguridad y permisos de acceso a internet, así como controlar los contenidos a los que acceden los usuarios.

Sin embargo, el desconocimiento, el costo económico o la difícil configuración de las herramientas utilizadas para el control y seguridad en internet, hacen que sea una tarea compleja, dificultando la posibilidad de navegar de forma segura.

Los sistemas operativos y los navegadores web que son herramientas básicas y necesarias para conectarse a la red, cuentan con la opción de establecer un control parental, y firewall básico que permite restringir el acceso a sitios de dudosa procedencia, pero dichos controles únicamente son válidos para dicha herramienta, por tanto, se puede tener un control configurado en Google Chrome, pero éste no es válido para otros navegadores como Mozilla Firefox; es decir, la seguridad que brindan estas herramientas no son suficientes.

Ninguna de estas herramientas permite controlar y configurar horarios de acceso a redes sociales y descargas de archivos, para mejorar los controles de dichos navegadores o de una máquina con sistema operativo windows, es necesario instalar un sinnúmero de herramientas como antivirus, firewalls, aplicaciones, proxys, complementos, entre otros; volviéndolo una tarea tediosa y confusa para el usuario.

Es importante indicar que dichas herramientas (como los proxys), tienen costos altos, que hacen que sea difícil acceder a ellos, en síntesis, internet es un recurso que se ha vuelto indispensable puesto que permite el acceso a múltiples contenidos y sitios web, pero es necesario que sea controlado para garantizar la seguridad del equipo y del usuario.

Así mismo, se puede establecer que, debido a las diferentes aplicaciones e información que facilitan el aprendizaje y la interacción maestro-estudiante dentro del aula, el internet constituye un aliado de gran ayuda dentro del aula de clases de las instituciones educativas tanto públicas como privadas; las cuales deben aplicar controles y políticas de restricción en el acceso a internet para proteger la seguridad informática del alumnado.

Se debe recalcar que, la instalación de software de control pueden afectar al rendimiento de los equipos debido a los recursos de memoria y procesador que consumen, y que al no existir controles, el estudiante podría quedar expuesto a contenidos que no son adecuados para su desempeño académico, pudiendo estos influir en una falta de atención a la clase.

Por tanto, es necesario estudiar y determinar los factores y tendencias de los sitios web más utilizados por los adolescentes durante las horas de uso del laboratorio y las acciones que pueden llegar a cometer estos para vulnerar las medidas de seguridad de la red. Este estudio plantea la propuesta de diseñar e implementar un navegador web que permita controlar de manera eficiente los contenidos a los que tienen acceso los estudiantes, sin el uso de una herramienta o hardware específico.

De esta manera, se crea una alternativa que no solo será de utilidad para la institución educativa y/o empresa, sino que puede ser una medida viable para el control en casa por parte de los padres hacia sus hijos.

El presente documento se encuentra elaborado y estructurado en dos capítulos. El capítulo I, está destinado a describir de manera detallada el objetivo del problema, así como también los antecedentes, las hipótesis planteadas y las metodologías que fueron aplicadas durante el proceso para llegar a la solución del problema y validar las hipótesis.

Dentro del capítulo II, se procede a la descripción del marco conceptual, las herramientas utilizadas para el desarrollo del navegador, el marco legal vinculado al desarrollo del proyecto, los requerimientos de hardware y software, la definición de los procesos, las pruebas de funcionalidad y los resultados obtenidos en la ejecución del proyecto.

CAPÍTULO I

EL PROBLEMA

1.1. Descripción

La presente investigación tiene como objetivo desarrollar e implementar una herramienta (browser) de acceso a internet que permita controlar de manera eficiente los contenidos a los que acceden los adolescentes entre 13 y 17 años durante el uso de los laboratorios de cómputo del Colegio Innova de la ciudad de Salinas. También, se analizó el nivel de dependencia con relación al uso de las redes sociales como principal medio de comunicación e interacción entre los jóvenes y su actitud frente al uso controlado del servicio de internet.

Esta herramienta también optimiza la seguridad lógica de los equipos permitiendo restringir el acceso a páginas web de servicio de proxy en línea, con las cuales se podría vulnerar las políticas de seguridad informática de la Institución. Adicionalmente, permite minimizar los factores que se involucran en la falta de atención en clases por el acceso a redes sociales o contenidos inapropiados durante sesiones realizadas en los laboratorios de cómputo.

El proyecto fue elaborado aplicando la metodología de desarrollo de software incremental y utilizando herramientas Microsoft como Visual Basic y la base de datos SQL Lite. Para la investigación se aplicó un estudio de tipo correlacional y descriptivo, los mismos que fueron desarrollados aplicando las técnicas de la observación directa, encuestas y entrevistas que fueron aplicadas al personal técnico y académico de la Institución. Por último, para el análisis de los datos y validación de hipótesis se utilizó el software Excel de Microsoft Office 2013.

1.2. Antecedentes

El internet se ha convertido en un elemento de vital importancia en todas nuestras actividades de la vida diaria, pasó de ser un lujo para convertirse en una necesidad.

“El servicio de internet es tan indispensable que lo encontramos en los hogares, instituciones públicas, así como también en pequeñas, medianas y grandes empresas, por lo cual, el internet se constituye en un recurso el cuál se debe administrar” (Duart, 2016)

Con el uso de internet a escalas mundiales, los delincuentes aprovechan estas tecnologías y tecnifican sus métodos de búsqueda y captación de sus posibles víctimas mediante el uso de redes sociales, chats, propagación de malware, robo de información y demás delitos que se cometen a través del uso de tecnologías, generando nuevos riesgos y peligros de usarlo al no tener un conocimiento adecuado y no disponer de las herramientas necesarias y seguras para su acceso.

El uso de este servicio se ha vuelto algo tan cotidiano, que ha transformado la forma en que las personas se comunican, realizan sus tareas diarias, y desde luego, ha transformado la educación y los métodos tradicionales de estudio. Actualmente, los adolescentes acceden a la red para descargar músicas, videos, comunicarse con sus amigos por redes sociales, o buscar alguna información de su interés, por lo que, no resulta nada extraño que este servicio también sea utilizado en el ámbito académico permitiendo complementar y facilitar el estudio y aprendizaje de las diferentes asignaturas o tópicos cubiertos en una institución académica.

El poco control y falta de administración del uso del servicio de internet, puede provocar pérdidas económicas como daños en los equipos por la propagación de malware en la infraestructura tecnológica.

El uso inadecuado de este servicio también puede afectar el rendimiento académico de los estudiantes generando un déficit en la atención y participación de los alumnos durante el uso de los laboratorios de informática.

Al no existir controles en la navegación de internet los adolescentes se pueden ver expuestos a ser víctimas del cometimiento de delitos a través del internet, así como también, acceso a páginas no confiables que pueden provocar la descarga de virus,

y software malicioso, poniendo en riesgo información sensible y confidencial.

Asimismo, la alta dependencia de los recursos tecnológicos y de las redes sociales como principal medio de comunicación e interacción entre los jóvenes, puede afectar su normal comportamiento y atención generando patrones de personalidad retraídos y poco sociables.

Por lo antes descrito, y siendo esta una problemática social que nos involucra a todos, es necesario entonces concienciar a la sociedad, a las instituciones educativas y especialmente a los adolescentes, quienes son los más vulnerables en este tipo de delitos y promover mecanismos de prevención y seguridad sobre la información que es publicada y consumida a través de los medios electrónicos.

1.3. Planteamiento de la propuesta

Actualmente el uso de las redes sociales como medios de comunicación de los adolescentes ha promovido nuevos hábitos y comportamientos en relación al uso de estas nuevas tecnologías.

Es así, que los jóvenes se ven cada vez más motivados e inducidos a utilizar diferentes redes sociales sin tener en ocasiones ningún conocimiento de mecanismos de seguridad o herramientas tecnológicas que permitan proteger sus datos y cuentas personales.

En Internet existen un sin número de páginas web a la cuales tienen acceso cualquier tipo de persona, ya sea hombre, mujer o niño. Muchas de estas páginas no tienen o poseen un adecuado control sobre los usuarios que visitan su contenido, un ejemplo son las páginas con contenidos pornográficos o contenidos violentos exclusivos para público adulto.

La gran mayoría de los adolescentes se sienten atraídos por el uso de diferentes redes sociales, ya que encuentran en ellas espacios “idóneos” donde mostrar sus “perfiles” y gustos los cuales suelen contener generalmente información privada tal

como: datos personales, direcciones domiciliarias, teléfonos, e-mails, hobbies, fotografías, videos, entre otros; dicha información es compartida entre sus amigos y miembros de los grupos a los cuales se encuentran asociados.

El intercambio de los datos entre los usuarios de internet sin un debido control y seguridad ha ocasionado que los delincuentes aprovechen la facilidad de acceso que se tiene a estos grupos y a las publicaciones que realizan sus miembros para a través de diferentes técnicas de búsqueda avanzada obtener información que les permita escoger a sus posibles víctimas.

De esta forma se genera un alto riesgo de que cualquier individuo mal intencionado pueda conocer la información personal de alguien y tomar contacto con ellos para el cometimiento de delitos tales como: trata de personas, pornografía infantil, acoso, extorsión o chantaje por el intercambio de fotos íntimas, robo de información, entre otros (Dr. Morduchowicz, Lic. Marcon, Lic. Sylvestre, & Ballestrini, 2010), (Fire, Goldschmidt, & Elovici, 2014).

Para los jóvenes se ha convertido en una necesidad prioritaria el uso del internet y con mayor énfasis en las redes sociales queriendo ser populares a través de estos medios de comunicación.

“En la actualidad existen más de 200 redes sociales, con más de 800 millones de usuarios en todo el mundo. Una tendencia que crece cada mes” (Dr. Morduchowicz, Lic. Marcon, Lic. Sylvestre, & Ballestrini, 2010).

El internet siendo un servicio necesario para el desarrollo económico y social de empresas públicas o privadas, instituciones educativas e inclusive de los hogares, se convierte en un recurso importante parte las tareas del diario convivir de las personas.

El acceso a este servicio es proporcionado a través de un ISP y suele ser administrado por los responsables del área tecnológica de una institución, quienes

utilizan infraestructura de seguridad como equipos proxy o IDS configurables que les permiten establecer reglas de navegación para los usuarios.

Sin embargo, existen servicios de proxy anónimos que facilitan al usuario vulnerar la seguridad implementada por la institución, ya que permiten enmascarar la URL o dirección web solicitada con el fin de que esta no sea detectada e ingresar al sitio web sin ninguna restricción.

La gran mayoría de los hogares tienen contratado el servicio de internet, el cual es mayormente utilizado por los adolescentes para sus tareas escolares y como medio de comunicación entre sus amigos.

Los padres facilitan este servicio a sus hijos muchas veces desconociendo los riesgos a los cuales pueden estar expuestos, así como la falta de control de las actividades o contenidos a los cuales acceden a través de la red.

Para ellos sería costoso y complejo implementar equipos de seguridad que permitan controlar estas acciones, además que podrían ser burlados mediante el uso de proxy en línea.

De acuerdo al panorama antes descrito, es necesario entonces preguntarse:

- ¿Por qué los adolescentes prefieren comunicarse por medio de las redes sociales respecto a otras formas de interacción y comunicación?
- ¿Qué efectos se evidencian en los adolescentes que acceden a internet sin ningún tipo de restricción?
- ¿Qué tipos de contenidos web son mayormente consumidos por los adolescentes?
- ¿Es recomendable utilizar una herramienta administrable que permita controlar el acceso a internet?

Son preguntas necesarias que se deben abordar para establecer criterios acerca de los diferentes mecanismos de seguridad informática que se podrían aplicar a los medios electrónicos que son generalmente usados por los adolescentes.

1.4. Objetivos

1.4.1. Objetivo General

Desarrollar un navegador web administrable para plataformas windows mediante el uso de herramientas de programación Visual Studio que permita realizar un control de acceso a contenidos en la web por parte de adolescentes entre 12 y 17 años del Colegio Innova del cantón Salinas.

1.4.2. Objetivos Específicos

- Evaluar los resultados obtenidos del sistema mediante la aplicación de los diferentes escenarios de prueba que permitan verificar la funcionalidad y eficiencia del aplicativo.

- Diseñar un programa informático que permita bloquear y restringir de manera eficaz el uso de páginas web con contenido inapropiado para menores de edad.

- Elaborar un manual de usuario de la aplicación de tal forma que se especifiquen detalladamente las opciones que este ofrece.

- Analizar el comportamiento de los adolescentes en el uso de internet y redes sociales a través del uso de herramientas de monitoreo de redes de datos.

1.5. Justificación e importancia

Internet es una herramienta tan poderosa que sirve como aliado estratégico dentro de los negocios, es un factor de alta importancia dentro de áreas como las telecomunicaciones y transmisión de datos, facilitando recursos como videoconferencias, transacciones bancarias, vigilancia a través de cámaras, comercio electrónico, e-learning, entre otras actividades, esto permite a las

empresas ahorrar recursos como tiempo y dinero, asimismo, dentro de los hogares favorece el desarrollo de las tareas académicas de los niños y adolescentes, así como el acceso a diversos contenidos de información y/o entretenimiento, entre ellos el uso de las redes sociales como Facebook, Badoo, Instagram, Twitter, entre otras.

Según datos estadísticos donde se planteó el siguiente cuestionamiento ¿A partir de qué edad entran los niños en las redes sociales?, se obtuvieron los siguientes datos. En España, la edad mínima para acceder a una red social, excepto a las específicas para menores, es de 14 años. Actualmente, Tuenti está trabajando con los menores de 14 años que quieren acceder a la red social a través del consentimiento paterno (Guia infantil, s.f.).

Por ello, la red social solicita el permiso paterno antes de permitir que se lleve a cabo el registro del perfil. En el Ecuador, Datos del INEC determinan que niños a partir de los 9 años ya tienen acceso a una red social y al consumo de pornografía por internet (Universo, 2014).

Otro estudio reciente en los Estados Unidos confirma que el 83% de los niños habría mentido sobre su edad para ingresar a una de estas páginas. Además, el 42% de los niños se hace pasar como mayor de edad para poder ingresar a las redes sociales.

En Colombia, la red social Facebook, restringe su uso para los menores de 13 años, y en este mismo país cerca del 7% de los usuarios de Facebook son adolescentes entre 13 y 15 años de edad; sin embargo, la realidad es que muchos de estos jóvenes son niños que han falsificado sus datos personales para poder entrar a esta red social sin ninguna validación de perfil, es decir la cuenta del menor se mantiene activa. (Arcila, s.f.)

Otra pregunta realizada en esa investigación fue ¿A qué edad los niños disponen ya de su propio teléfono móvil? El desarrollo de la telefonía móvil y de los conocidos Smartphone o teléfonos inteligentes permite que los jóvenes puedan tener acceso a internet en cualquier momento desde cualquier lugar.

Según el estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles, elaborado en 2010 por INTECO y Orange, la edad media de inicio en la telefonía móvil por parte de los menores españoles se sitúa entre 10 y 12 años de edad.

Además, la mayoría de los menores accede a internet desde su casa o a través de redes públicas (Guia infantil, s.f.).

Por lo anterior, el presente proyecto propone el diseño y desarrollo de un navegador web seguro que ayude a controlar el uso del servicio de internet mediante paneles de control administrables donde los usuarios puedan establecer horarios, páginas y contenidos admitidos para la navegación web. También, evitará el uso de otros navegadores que se encuentren instalados en el computador de tal manera que el usuario solo utilice Safe Browser.

Otra característica es que previene el salto de las reglas de seguridad establecidas en equipos firewall ya que permite el bloqueo de servicios de proxy online y gestores de descarga según las configuraciones que se establezcan en el programa.

Adicionalmente, esta herramienta presenta un gran ahorro en infraestructura de equipos de seguridad para pequeñas y medianas empresas u organizaciones que lo pueden utilizar como un mecanismo de seguridad y control para sus usuarios.

1.6. Hipótesis y variables

1.6.1. Hipótesis

H1: Controlar el uso del internet no implicará cambios en el acceso de los adolescentes a contenidos en la web.

H2: Existe independencia entre las edades de los adolescentes y el uso de las redes sociales.

H3: A mayor control en el uso de internet mayor es el número de saltos de seguridad que aplicarán los adolescentes.

H4: A más edad de los adolescentes mayor es el acceso a contenidos no aptos para su edad.

1.6.2. Variables

Hipótesis 1:

Variable independiente:

- Control del uso de Internet.

Variable dependiente:

- Contenidos en la web.

Hipótesis 2:

Variable independiente:

- Edad de adolescentes.

Variable dependiente:

- Uso de redes sociales.

Hipótesis 3:

Variable independiente:

- Control del uso de Internet.

Variable dependiente:

- Saltos de seguridad.

Hipótesis 4:

Variable independiente:

- Control del uso de Internet.

Variable dependiente:

- Contenidos no aptos para adolescentes.

1.6.3. Operacionalización de variables

Variable independiente	Conceptualización	Dimensiones	Indicadores	Escala de medición	Técnica e instrumento
Control del uso de Internet.	El control en el uso de Internet corresponde a los mecanismos de seguridad preventivos, los cuales pueden ser configurados en el navegador Safe Browser para evitar el acceso a páginas con contenido para público adulto o que presenten software malicioso	Uso de control parental y de contenidos.	Historial de navegación web y registro de descargas de archivos. Uso de software gestor de descargas.	Porcentaje de navegación mostrado en el historial del navegador.	Observación y recolección de datos mediante las herramientas Chrome History View, Mozilla History View y Safe Browser.
Edad de adolescentes.	Tiempo de vida de una persona u otro ser vivo contando desde su día de nacimiento; por lo general corresponde a la edad en años de los adolescentes.	Rango de edades.	Grupos de estudiantes según las edades.	Edades de los estudiantes.	Informe estadísticos de los paralelos con las respectivas edades de los estudiantes.

Tabla 1 Operacionalización de variables independientes

Tabla 2 Operacionalización de variables dependientes

Variable dependiente	Conceptualización	Dimensiones	Indicadores	Escala de medición	Técnica e instrumento
Contenido en la web.	Todo contenido existente en la web, ya sea imágenes, videos, libros, post, redes sociales, investigaciones científicas y demás temas de interés de la comunidad.	Acceso a Internet desde el equipo.	Historial de navegación web y registro de descargas de archivos.	Porcentaje de navegación mostrado en el historial del navegador.	Observación y recolección de datos mediante las herramientas Chrome History View, Mozilla History View y Safe Browser.
Uso de redes sociales.	Las redes sociales en Internet son comunidades virtuales donde sus usuarios tienen la facilidad de comunicarse entre sí desde cualquier parte del mundo.	Uso de redes sociales.	Historial de navegación web en redes sociales.	Número de accesos e intentos de accesos a las diferentes redes sociales disponibles en Internet.	
Saltos de seguridad.	Son los actos cometidos por uno o varios individuos para violentar la seguridad de una empresa o de un software. Estas personas buscan la manera para no ser detectados ante cualquier acto que realicen.	Uso de proxy anónimos.	Historial de navegación a páginas web con servicios de proxy anónimo.	Número de accesos e intentos de accesos a las distintas páginas web con servicios de proxy anónimo.	
Contenidos no aptos para adolescentes.	Material tanto gráfico como textual de contenido no apto para menores de edad y adolescentes; por lo general se hace referencia a videos o foros los cuales implican material con contenido pornográfico.	Acceso a sitios web con contenido malicioso o para adultos.	Historial de navegación web de páginas con contenido para adultos.	Número de accesos e intentos de accesos a páginas web con contenido pornográficos o software malicioso.	

1.7. Metodología

1.7.1. Diseño de la investigación

Una de las metodologías de investigación que se utilizó para el desarrollo de este proyecto fue la observación científica, que se define como el uso sistemático de los sentidos para resolver un problema de investigación, es decir, observar científicamente se trata de percibir activamente la realidad exterior con el propósito de obtener datos que con anterioridad han sido establecidos como principal interés para la investigación (Sabino, 1984).

La observación que se realiza cotidianamente, como parte de nuestra vida diaria, no puede ser considerada como científica, puesto que no está dirigida ni orientada hacia objetos de estudio. La ventaja de esta técnica consiste en que los hechos son percibidos directamente por el investigador, sin intermediarios, pudiendo observar los resultados tal y como se dan. Una de sus desventajas radica en que el comportamiento de los sujetos observados puede verse alterado y/o modificada por el simple hecho de estar bajo la observación del investigador, razón por la cual puede afectar a los resultados de la investigación (Sabino, 1984).

"También se aplicó la investigación de campo, la cual consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna" (Arias, El Proyecto de Investigación: Guía para su elaboración., 1999).

Estas técnicas en conjunto permitieron trabajar de mejor manera y de forma eficiente en la obtención de datos, previo al estudio y la implementación del software a desarrollar, y a su vez comparar los resultados obtenidos luego de la implementación del proyecto.

Este proceso permitió comprobar y validar las hipótesis planeadas en el estudio.

Modalidad de la investigación

El presente trabajo tiene la modalidad de proyecto factible, pues tuvo como propósito inmediato la ejecución de una propuesta, en tal sentido (Fidias, 2006) señala: "Que se trata de una propuesta de acción para resolver un problema practico o satisfacer una necesidad. Es indispensable que dicha propuesta se acompañe de una investigación, que demuestre su factibilidad o posibilidad de realización". La propuesta que lo puntualiza puede referirse a la formulación de políticas, programas, tecnologías métodos o procesos, que solo tiene sentido en el ámbito de sus necesidades.

Tipo de la investigación

La investigación descriptiva; también llamada investigación científica, se encarga de describir los datos y tiene un impacto en la vida de las personas que le rodean. Según (Tamayo y Tamayo, Tipos de investigación) "Este tipo de estudio busca únicamente describir situaciones o acontecimientos; básicamente no está interesado en comprobar explicaciones, ni en probar determinadas hipótesis, ni en hacer predicciones..."

La investigación descriptiva consiste en conocer las situaciones, costumbres y actitudes predominantes a través de la descripción de las actividades, objetos, procesos y personas.

El principal objetivo es saber el por qué y para qué se está realizando la investigación, la manera más precisa para el cumplimiento de este objetivo y la validación de este tipo de investigación es el uso de su mejor herramienta, la gráfica

La investigación correlacional es un tipo de investigación social que tiene como principal objetivo medir el grado de relación que existe entre dos o más variables; aunque más comúnmente solo se realiza una correlación entre dos variables, frecuentemente también se ubican relaciones entre tres variables.

> La utilidad de este tipo de investigación es saber cómo se puede comportar un concepto o variable conociendo el comportamiento de otra u otras variables relacionadas. En el caso de que dos variables estén correlacionadas, ello significa que una varía cuando la otra también varía y la correlación puede ser positiva o negativa. Si es positiva quiere decir que sujetos con altos valores en una variable tienden a mostrar altos valores en la otra variable. Si es negativa, significa que sujetos con altos valores en una variable tenderán a mostrar bajos valores en la otra variable. (Sampier, 2004)

1.7.2. Población y muestra

El término población se define como una colección o totalidad de elementos principales o posibles sujetos, a los cuales se les realizará un estudio. Según (Tamayo y Tamayo, 1997), "La población se define como la totalidad del fenómeno a estudiar donde las unidades de población posee una característica común la cual se estudia y da origen a los datos de la investigación".

Para la seleccionar los datos de la muestra se utilizó el muestreo estadístico estratificado; que se basa en una técnica de muestreo en donde el investigador divide a toda la población en diferentes subgrupos o estratos, donde posteriormente se selecciona aleatoriamente a los sujetos finales de los diferentes grupos o estratos de forma proporcional.

> Esta técnica, perteneciente a la familia de muestreos probabilísticos, consiste en dividir toda la población objeto de estudio en diferentes subgrupos o estratos disjuntos, de manera que un individuo sólo puede pertenecer a un estrato. Una vez definidos los estratos, para crear la muestra se seleccionan individuos empleando una técnica de muestreo cualquiera a cada uno de los estratos por separado. (Ochoa, 2015)

De esta manera, los posteriores encuestados se eligen con base a las referencias; generando un número suficiente de sujetos necesarios para el estudio.

Población

Nº	Detalle	Cantidad	%
1	Estudiantes entre 11 y 13 años	194	26,25
2	Estudiantes entre 14 y 15 años	246	33,29
3	Estudiantes entre 16 y 18 años	294	39,78
4	Personal administrativo del colegio Innova	5	0,68
Totales		**739**	**100**

Tabla 3 Población de estudiantes de entre básico a bachillerato

Muestra

La muestra es un conjunto de individuos, extraídos de los datos de una población con el fin de obtener datos representativos de la misma. Debido al tamaño de la población, se procede a calcular la muestra mediante la siguiente fórmula.

$$\boldsymbol{n = \frac{P \cdot Q \cdot N}{N - 1 \cdot \frac{E^2}{K^2} + P \cdot Q}}$$

Donde:

N: tamaño de la muestra

P·Q: varianza de la población 0,25

E: margen de error 0,04

K: constante de corrección del error 2

N: Tamaño de la Población 739

Para el análisis se tomó una varianza media de 0,25 lo cual es sugerido en estudios relacionados al ámbito educacional, un margen de error del 4% y el valor de la constante de corrección es 2.

Empleo de la formula

Se procede a realizar las respectivas sustituciones.

$$\boldsymbol{n = \frac{(0,25)\cdot(739)}{(739-1)\cdot\frac{(0,04)^2}{(2)^2}+0,25}}$$

Aplicada la fórmula se determina que la muestra corresponde a 339 personas, a quienes se les aplicará la encuesta.

Aplicar una regla de tres simple se obtienen los siguientes valores:

Fórmula:

$$\mathbf{m= \frac{(\%Población)(Muestra)}{100}}$$

Estudiantes entre 11 y 13 años:

$$\boldsymbol{m = \frac{(26{,}25\%)(339)}{100} = 89}$$

Estudiantes entre 14 y 15 años:

$$\boldsymbol{m = \frac{(33{,}29\%)(339)}{100} = 113}$$

Estudiantes entre 16 y 18 años:

$$\boldsymbol{m = \frac{(39{,}78\%)(339)}{100} = 135}$$

Personal administrativo del Colegio Particular INNOVA:

$$\boldsymbol{m = \frac{(0{,}68\%)(339)}{100} = 2}$$

En el siguiente cuadro se describen los porcentajes y la cantidad de personas a quienes participaran en el experimento.

Nº	Detalle	Cantidad	%
1	Estudiantes entre 11 y 13 años	89	26,25%
2	Estudiantes entre 14 y 15 años	113	33,29%
3	Estudiantes entre 16 y 18 años	135	39,78%
4	Personal administrativo del colegio Innova	2	0,68%
Totales		**339**	**100**

Tabla 4 Muestra obtenida de la población

1.7.3. Instrumentos de la investigación

Encuestas: una encuesta está constituida por una serie de preguntas que están dirigidas a una porción representativa de una población, y tiene como finalidad averiguar estados de opinión, actitudes o comportamientos de las personas ante asuntos específicos.

La encuesta, en este sentido, es preparada por un investigador que determina cuáles son los métodos más pertinentes para otorgarle rigurosidad y confiabilidad, de modo que los datos obtenidos sean representativos de la población estudiada. Los resultados, por su parte, se extraen siguiendo procedimientos matemáticos de medición estadística.

Dependiendo del universo estudiado, se definirá la proporción de la muestra representativa de una población. Aunque cuando se trate de poblaciones muy pequeñas, se podrá proceder a encuestar al cien por ciento de los individuos. Así, una encuesta se designará como parcial cuando se enfoque en una muestra de la población total, y se llamará exhaustiva cuando abarque todas las unidades estadísticas que conforman el universo estudiado. La población, por otro lado, podría estar compuesta por personas, empresas o instituciones.

El proceso de aplicación de las encuestas es llevado a cabo por un encuestador, encargado de la recolección de los datos. Las encuestas pueden ser cara a cara, vía

telefónica, por correo tradicional o por internet.

Se aplican comúnmente para estudios de mercado y para sondeos de opinión de naturaleza política (elecciones, aprobación, popularidad, etc.).

El objetivo de las encuestas es, principalmente, reunir una gran cantidad de información cuantitativa sobre temas específicos que afectan a la sociedad, así como conocer las opiniones, las actitudes, los valores, las creencias o los motivos que caractericen a los ciudadanos de determinado país o región. En este sentido, según autores como Manuel García Ferrado, "todo fenómeno social puede ser estudiado según las encuestas".

Como encuesta, también, puede denominarse el papel impreso donde se encuentra la lista de preguntas que conforma el cuestionario de la que procede.

Observación: La observación forma parte del método científico ya que, junto a la experimentación, permite realizar la verificación empírica de los fenómenos. La mayoría de las ciencias se valen de ambos recursos de manera complementaria.

La astronomía suele ser tomada como ejemplo de las ciencias que se basan en la observación. En este caso, la experimentación no es posible ya que el objeto de estudio no puede trasladarse al laboratorio.

La observación científica consiste en la medición y el registro de los hechos observables. Esta actividad se debe realizar de forma objetiva, sin que las opiniones, los sentimientos y las emociones influyan en la labor técnica.

A grandes rasgos, podemos distinguir tres pasos o etapas que caracterizan el trabajo de observación científica:

- Se elabora una hipótesis, que intenta explicar el fenómeno estudiado; a continuación,

- Se realiza una predicción lógica, basada en resultados anteriores o simplemente en los conocimientos específicos, y se suele experimentar a partir de estas ideas;

- Por último, los profesionales se encuentran en condiciones de llegar a una conclusión y, de esta forma, continuar aportando al saber de la humanidad.

La observación también se realiza en el ámbito del arte y consiste en una mirada detallada para apreciar las características de una obra. Al observar una pieza artística con atención, es posible analizar las cualidades visuales y comprender el significado de aquello que el artista quiso expresar.

1.7.4. Recolección y procesamiento de la información

Recolección de datos

Para la recolección de datos de cada una de las computadoras fue necesario el uso del software **BrowsingHistoryView**, ya que permite tomar los datos tal como se generan en cada computadora; este software permite visualizar el historial de navegación de los diversos navegadores web que se encuentran instalados en los mismos.

A la vez este software permite exportar estos datos obtenidos a un archivo Excel, en el cual los datos serán más manejables y se podrán filtrar según sea la conveniencia de la investigación.

Procesamiento y análisis de datos

Para el procesamiento y análisis de los datos se usó la herramienta Excel que facilita el proceso de datos estadísticos y porcentuales.

Excel es un software desarrollado y distribuido por Microsoft Corp. Este programa informático le permite al usuario realizar tareas como operaciones matemáticas básicas hasta complejos gráficos estadísticos a base de datos en tablas ingresadas en las hojas de cálculo.

Cabe recalcar que este es un software comercial, lo que supone un costo de licencia para su completa instalación; para el presente trabajo se titulación se obtuvo la versión de Office 2013 Home & Student que incluye las aplicaciones básicas como Word, PowerPoint, Excel y One Note.

CAPÍTULO II
EL PROYECTO

2.1. Marco Contextual

2.1.1. Colegio particular INNOVA School

El día 28 de febrero del 2014 se remitió al Rectorado el Oficio N.- 059 CRQ. DDESE. 2014 en el cual se solicitaba aplicar a la brevedad posible el acuerdo 407-12 que establece la obligatoriedad del cambio de Denominación y así también el cambio de Nominación amparado en los artículos 108, 109 y 110 ya que la institución educativa tenía el nombre de una persona viva.

Dando cumplimiento a lo antes expuesto y basados en los acuerdos y Reglamentos de la LOEI, LA UNIDAD EDUCATIVA FRANK VARGAS PAZZOS se presenta hoy como UNIDAD EDUCATIVA SALINAS INNOVA SCHOOL.

Misión

Brindar una educación de calidad con excelencia en los procesos académicos y administrativos, desarrollando programas internacionales con personal capacitado que aplica una formación constructivista desde un enfoque humanista, respondiendo a la filosofía de los colegios del mundo.

Visión

Ser una institución educativa innovadora, formadora de ciudadanos del mundo, capaces de proponer mejoras en el entorno que se desempeñan, manteniendo el respeto de pensamiento e interculturabilidad, destacándose como líderes en los ámbitos académico, tecnológico, científico, ambiental, deportivo y productivo

con enfoque bilingüe e inclusivo, contribuyendo así a crear un mundo mejor y más pacífico.

Metas de enseñanza

Las bases de este Modelo lograrán que el estudiante desarrolle:

- Comunicación efectiva en castellano e inglés.
- Pensamiento Matemático, científico y analítico.
- Competencias digitales.
- Toma de decisiones por sí mismo.
- Desarrollarán conciencia cívica y ciudadana.
- Formación en liderazgo.
- Competencias para trabajar en equipo.
- Éxito universitario, profesional y personal.

Fuente: Colegio INNOVA.

Ubicación

Figura 1 Vista satelital ubicación Colegio INNOVA School

Fuente: Vista satelital Google Earth

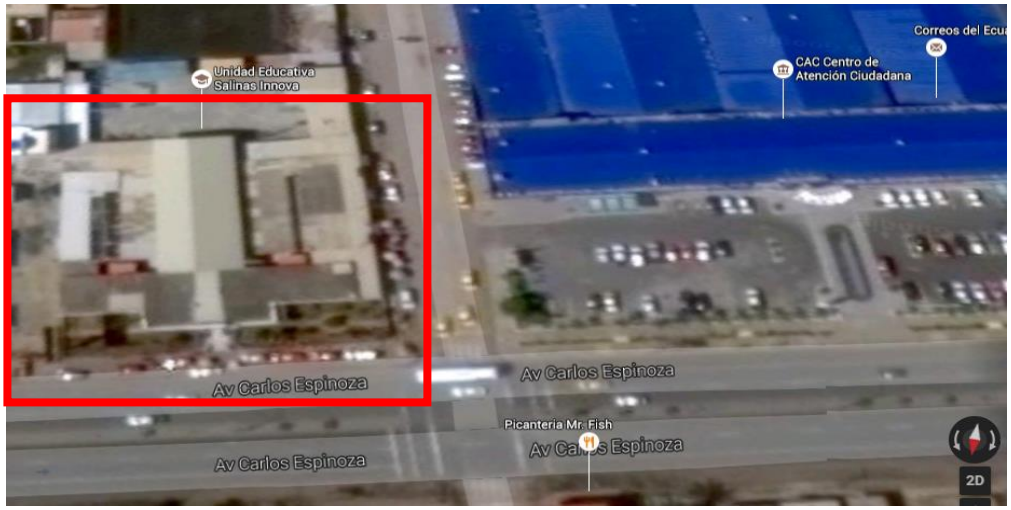

Figura 2 Vista satelital ubicación Colegio INNOVA School

Fuente: Vista satelital Google Earth

Figura 3 Vista StreetView de Colegio INNOVA School

Fuente: Vista StreetView Google Earth

2.1.2. Organigrama Institucional del Colegio INNOVA School

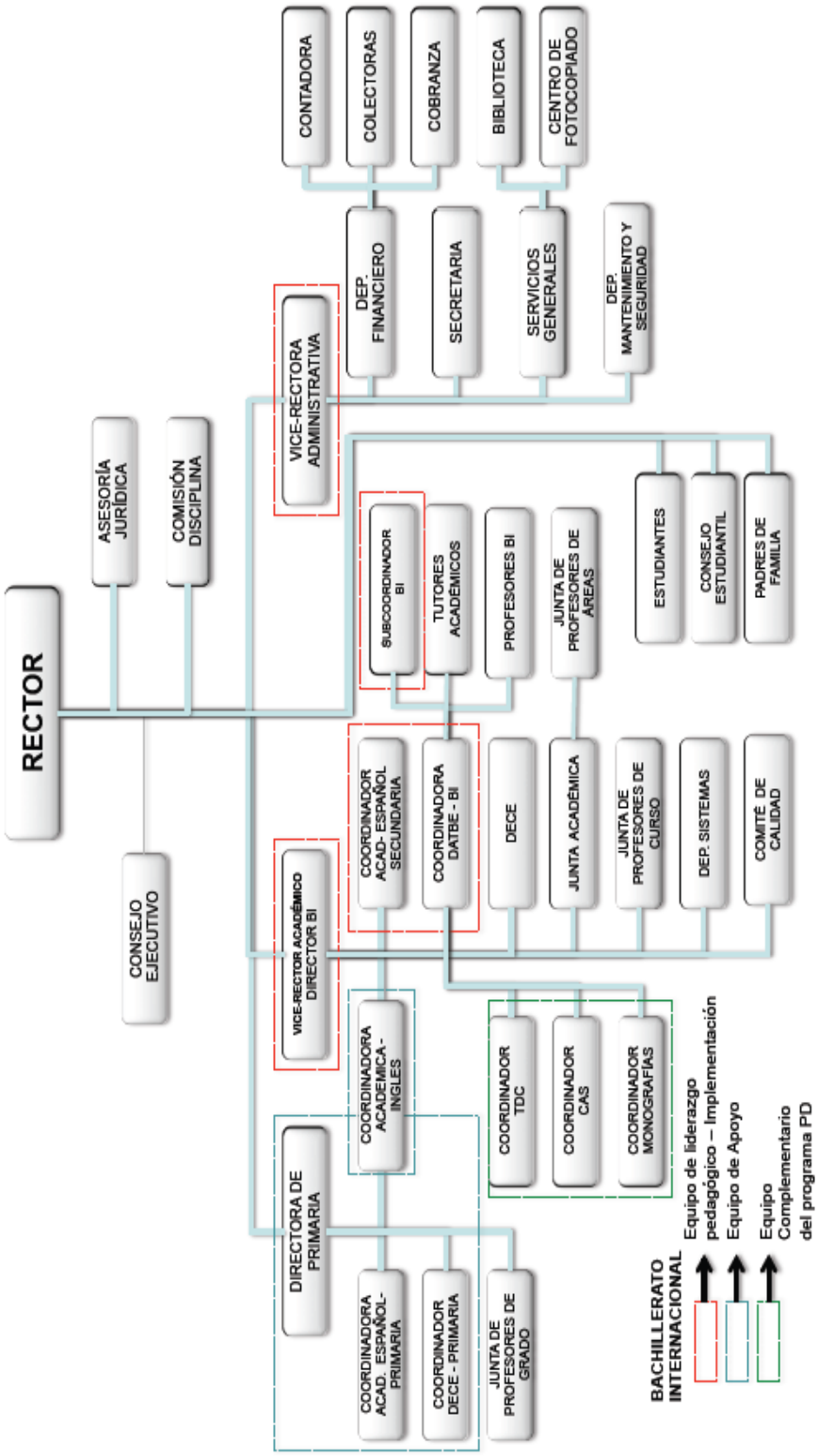

Figura 4 Organigrama estructural del Colegio INNOVA

Fuente: Oficina administrativa, Colegio INNOVA.

1.1. Marco conceptual

1.1.1. Navegador web

Navegador web o browser por sus siglas en inglés. En informática se describe como una aplicación, programa o software que permite acceder a páginas web y navegar por una red informática, principalmente internet ya sea desde computadoras personales o dispositivos móviles. Su nombre proviene de la capacidad de poder "moverse" entre diversas páginas mediante los hipervínculos, que son los que permiten conectar las páginas situadas en distintos lugares del mundo entre sí con solo un clic, a lo que se llama comúnmente navegación.

Navegador web seguro, al usar un navegador web para casi todo, este debe proporcionar una buena seguridad y por esta razón el navegador debe de asegurar al usuario su data personal manteniendo dicha información alejada de aquellos intrusos que harían mal uso de la misma. Al momento de escoger que navegador, se debe de tener en cuenta el nivel de seguridad que brinda para que nuestra información sea transportada de forma segura y confiable por la red.

Navegadores web seguros existentes, en el mercado hay diversos navegadores web que proporcionan seguridad al momento de navegar por la web, tales como: Google Chrome, Mozilla Firefox, Internet Explorer, Safari, Comodo Dragon, Opera, entre otros.

2.2.2. Lenguaje de programación

Visual Basic .NET, es un lenguaje de programación orientado a objetos que cuenta con los beneficios que brinda .NET Framework, el cual es un modelo de programación diseñado para simplificar la programación de aplicaciones en un entorno distribuido como el Internet. Visual Basic .NET (VB.NET) es un lenguaje de programación orientado a objetos que se puede considerar una evolución de Visual Basic implementada sobre el framework .NET. Su introducción resultó muy

controvertida, ya que debido a cambios significativos en el lenguaje VB.NET no es retro compatible con Visual Basic, pero el manejo de las instrucciones es similar a versiones anteriores de Visual Basic, facilitando así el desarrollo de aplicaciones más avanzadas con herramientas moderna, para mantener eficacia en el desarrollo de las aplicaciones. La mayoría de programadores de .NET utilizan el entorno de desarrollo Microsoft Visual Studio, aunque existen otras alternativas para el desarrollo de aplicaciones.

2.2.3. SQLite

Base de datos, un sistema de bases de datos en básicamente un sistema computarizado para llevar registros. Es posible considerar a la propia base de datos como una especie de armario electrónico para archivar; es decir, es un depósito o contenedor de una colección de archivos de datos computarizados. Los usuarios del sistema pueden realizar una variedad de operaciones sobre dichos archivos por ejemplo:

- Agregar nuevos archivos vacíos a la base de datos.
- Insertar datos dentro de los archivos existentes.
- Recuperar datos de los archivos existentes.
- Modificar datos en archivos existentes.
- Eliminar datos en archivos existentes.” (Date, 2001).

SQLite, es una herramienta de software libre que permite almacenar información en dispositivos empotrados de una manera sencilla, eficaz y rápida en equipos con capacidades muy limitadas de hardware, ya sean PDA o un teléfono celular. SQLite implementa el estándar SQL-92, además que implementa las extensiones que facilitan su uso en cualquier ambiente de desarrollo, esto permite que SQLite soporte desde las consultas básicas hasta las más complejas en lenguaje SQL.

Características importantes de SQLite

- La base de datos completa se encuentra en un solo archivo.

- Pueda funcionar enteramente en memoria, lo que hace que funcione con más rapidez.
- Completamente auto contenida, no necesita de dependencias externas.
- Cuenta con librerías de acceso para diversos lenguajes de programación.
- El código fuente es de dominio público.
- Soporta datos numéricos de 64 bits, así como texto en formato UTF-8 y UTF-16.

2.3. Marco Teórico

2.3.1. Herramientas CASE

Son diversas aplicaciones informáticas las cuales dan la facilidad de aumentar la productividad en el desarrollo de software reduciendo así el costo de la misma en términos de tiempo y de dinero. Estas herramientas pueden ayudar en todos los aspectos del ciclo de vida de desarrollo del software, en tareas tales como el proceso de realizar un diseño de un proyecto, cálculo de costos, implementación, compilación automática, documentación o en detección de errores y entre otras.

Tecnología CASE

Supone la automatización del desarrollo del software, contribuyendo a mejorar la calidad y la productividad en el desarrollo de sistemas de información.

Se plantean los siguientes objetivos:

- Permitir a la aplicación la práctica de metodologías estructuradas, las cuales al ser realizadas con una herramienta se consigue agilizar el trabajo.
- Facilitar la realización de prototipos.
- Facilitar el desarrollo conjunto de aplicaciones.
- Simplificar el mantenimiento de programas.
- Mejorar y estandarizar la documentación.
- Facilitar la reutilización de componentes de software.

Software para aplicaciones compatibles:

- NetDynamics.
- PowerBuilder.
- Visual Basic.
- Bases de datos compatibles y entre otros.

2.3.2. Metodología de desarrollo de software

Modelo Incremental: dicho modelo permite dividir el proyecto en varias partes, fase o módulos que pueden desarrollarse de manera independiente, el uno del otro.

Cada fase o módulo está definida dentro de un cronograma de trabajo con un periodo de tiempo determinado, los cuales pueden ser secuenciales o en paralelos, lo cual es una ventaja brindada por este modelo.

Es importante mencionar, que al término de cada periodo los módulos terminados constituirán un producto operacional y funcional, sin la necesidad y la dependencia de los otros módulos que quedan pendientes en el desarrollo, lo que brinda al software un nivel de usabilidad alto, y agiliza los procesos de pruebas, y recolección de datos durante la fase de implementación.

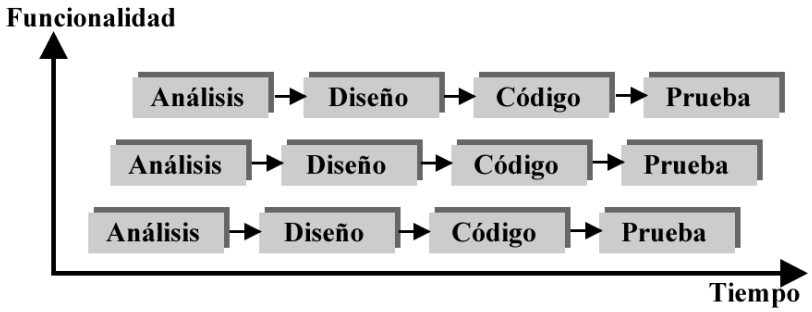

Figura 5 Modelo incremental

En una visión genérica, el proceso de desarrollo del software se divide en 4 partes: el análisis, el diseño, el código y las pruebas. Para la producción del software se usa el principio de trabajo en cadena, utilizado para mantener al cliente en constante

contacto para que tenga un mayor control con los resultados obtenidos en cada incremento.

El mismo cliente es quien se encarga de aceptar o desechar los cambios o mejoras que se apliquen a cada incremento a fin de que se adapten mejor a sus necesidades reales; el proceso se repite hasta que el cliente este satisfecho con el producto final.

De esta manera el tiempo de entrega se reduce considerablemente.

Al igual que los demás métodos de modelado, el Modelo Incremental es de naturaleza interactiva, pero se diferencia de aquellos en que al final de cada incremento se entrega un producto completamente operacional.

2.3.3. Mecanismo de seguridad informática

Cifrado de datos:

SHA: por sus siglas en inglés (**S**ecure **H**ash **A**lgorithm), son funciones hash de cifrado, la primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0.

El mecanismo de seguridad utilizado en el desarrollo del software es SHA1**,** el cual ha sido examinado por la comunidad criptográfica pública, aunque se han divulgado varios ataques significativos sobre funciones criptográficas de hash con una estructura similar a SHA1, no se existe registrado ningún ataque efectivo contra el mismo.

A pesar que SHA1 trabaja en una salida resumen de 160 bits (2^{64}; es decir 20 bytes, en 2004 se encontró una debilidad matemática que permitía encontrar colisiones de hash más rápido. Sin embargo esto resulta poco relevante, pues la complejidad de búsqueda de colisiones pasaría de 2^{80} a 2^{69}, algo que aún es computacionalmente inviable; requiriendo incluso más trabajo que con MD5.

2.3.4. Tipos de investigación

Investigación de campo

Los datos a recolectarse serán las bases de datos de los navegadores de cada una de las maquinas en las que se realizará la investigación. Todos estos datos son extraídos de las bases de datos mediante el software **BrowsingHistoryView,** el cual permite extraer los datos de historial de cada navegador (Internet Explorer, Google Chrome, Mozilla Firefox) de forma ordenada y tabulada.

> La Investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta. (Palella & Martins, 2010)

Investigación descriptiva

Según el autor (Arias, EL proyecto de investigación., 1999), define: "la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento".

Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere.

2.3.5. Glosario de definiciones

E-Learning: permite la interacción del usuario con el material utilizando las diversas herramientas informáticas para el aprendizaje mediante el Internet.

Equipos proxy o IDS: programa de detección de accesos no autorizados a un computador, una red o cuenta de usuario.

Firewall: por motivos de seguridad, es un programa informático dedicado a controlar el acceso de una computadora a la red y de elementos de la red a la computadora.

Framework: entorno o ambiente de trabajo para desarrollo de software; facilitan el desarrollo de aplicaciones y proporcionan soporte para el programa, bibliotecas, plantillas y más.

ISP: por sus siglas en inglés **Internet Service Provider,** compañía que proporciona acceso a Internet.

La red: sinónimo de Internet.

LOEI: Ley Orgánica de Educación Intercultural, reglamento que garantiza el respeto a los derechos y acceso al sistema educativo de todos los estudiantes.

Logueado: termino el cual se refiere a iniciar sesión en una cuenta y mantenerse activo o conectado.

Malware: es la abreviatura de "**Mal**icious soft**ware**", término que engloba a todo tipo de código informático malicioso cuya función sea dañar un sistema, robo de información o causar un mal funcionamiento al equipo.

Operacionalización: proceso que consiste en definir las variables en factores medibles.

PDA: sigla de Personal Digital Assistant (asistente digital personal), agenda electrónica que incluye muchas de las funciones de una computadora personal.

Proxy en línea: página web la cual proporciona un anonimato al usuario que lo usa, enmascarando las direcciones a las que tiene acceso para vulnerar cualquier seguridad de restricción de páginas con la cuente la institución.

2.4. Marco Legal

Para el desarrollo de la investigación se consideraron aspectos legales e importantes que rigen en la toma de datos y la manipulación de equipos tecnológicos, mismos que fueron considerados y aplicados durante el desarrollo de la investigación, y que sustentan la confidencialidad y manejo de la información digital por parte de los investigadores.

A continuación se mencionan artículos de la Ley de comercio Electrónico, Firmas electrónicas y Mensajes de datos de la República del Ecuador, en los cuales se apoya el estudio.

Título V. De las infracciones informáticas. Capítulo I. De las infracciones informáticas.

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.

Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art. ....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.

Art. 62.- A continuación del Art. 553, añádanse los siguientes artículos innumerados:

Art. ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas.

> Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:
>
> Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (Congreso, 2002)

Los estatutos y leyes que rigen las investigaciones científicas en las que se consideren la toma de información digital y el uso de equipos institucionales por parte de terceros protegen a las instituciones tanto privadas como públicas de los robos de equipos y de información por parte del equipo de investigadores.

La información analizada y recopilada en el presente proyecto, son datos a nivel general y no personal, lo cual significa que la información obtenida, fue información generada por grupos de personas sin tomar en consideración ningún nombre en particular.

Toda la información recopilada por los investigadores es información legalmente solicitada y aprobada por los directivos de la institución, e informados a los participantes de la investigación.

2.5. Desarrollo y Resultados

2.5.1. Análisis de la propuesta

Diagrama de casos de uso

Los diagramas de casos de uso describen los procesos; en otras palabas, muestran el uso particular de la aplicación. La imagen de una funcionalidad del sistema es denominada como rol o actor.

A continuación se representan los casos de uso utilizados en la aplicación tanto para el usuario administrador como los usuarios normales (estudiantes).

Figura 6 Caso de uso administrador- Registro en el sistema

Especificaciones de caso de uso	
Nombre	**Registro en el sistema**
Descripción:	Permite el registro del usuario administrador en el sistema.
Precondiciones:	• Se debe de instalar el navegador en la cuenta usuario administrador del equipo en el que se va a trabajar. • La cuenta del usuario administrador debe de tener una clave para mayor seguridad.
Flujo normal:	1. El usuario administrador instala el navegador en la máquina. 2. Completa correctamente todos los campos solicitados. 3. Se mostrará un mensaje de advertencia, si todos los datos son correctos el usuario concluirá con el registro.
Flujo alternativo:	Si el usuario administrador no cumple con los requisitos o algún campo solicitado se encuentra vacío, se mostrará un mensaje de advertencia indicando la falta de datos solicitados. De colocarse un correo electrónico sin el formato de correo, se le solicitará al usuario ingrese una dirección de correo válida.
Poscondiciones:	Los datos del usuario administrador fueron guardados correctamente.

Tabla 5 Caso de uso administrador - Registro en el sistema

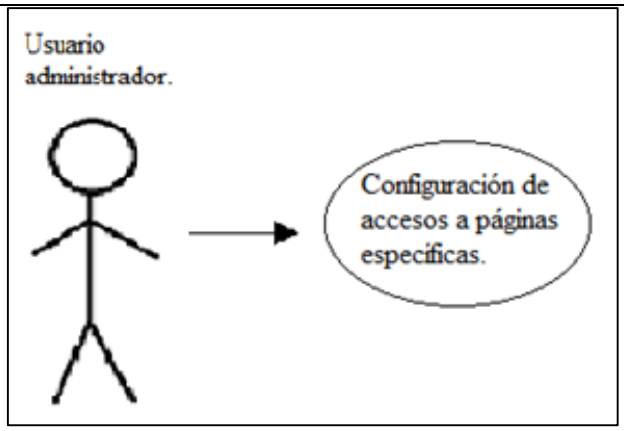

Figura 7 Caso de uso administrador- Configuración a páginas específicas

Especificaciones de caso de uso	
Nombre:	**Configuración de acceso a páginas web específicas.**
Descripción:	El usuario administrador puede configurar las páginas a las cuales los demás usuario no tendrán acceso.
Precondiciones:	El usuario administrador debe de estar logueado.
Flujo normal:	1. El usuario administrador ingresa mediante su usuario y clave a las configuraciones del sistema. 2. Selecciona la opción de registro de páginas bloqueadas. 3. Ingresa las URL´s de las páginas a las cuales desea restringir el acceso a los demás usuarios.
Flujo alternativo:	El usuario administrador debe de escribir una dirección de página web válida, caso contrario se le solicitará que ingrese una URL válida.
Poscondiciones:	La o las direcciones de páginas web registradas en esta sección estarán inhabilitadas para los demás usuarios.

Tabla 6 Caso de uso - Configuración a páginas específicas

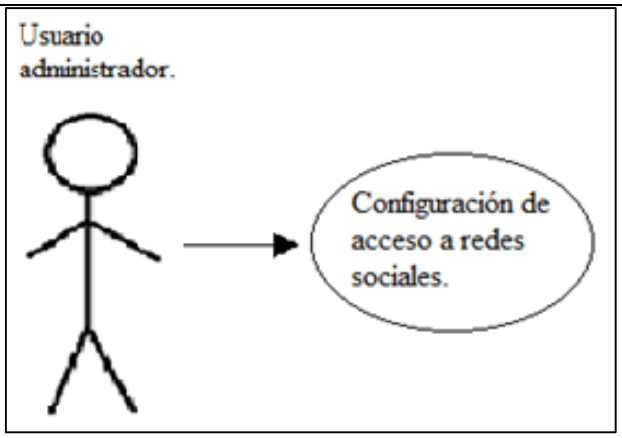

Figura 8 Caso de uso administrador - Configuración a redes sociales

Especificaciones de caso de uso	
Nombre:	**Configuración de acceso a redes sociales.**
Descripción:	El usuario administrador puede configurar los horarios en los que los demás usuarios puedan ingresar a redes sociales tales como Facebook, Twitter, Google + y más.
Precondiciones:	El usuario administrador debe de estar logueado.
Flujo normal:	1. El usuario administrador ingresa mediante su usuario y clave a las configuraciones del sistema. 2. Selecciona la opción de acceso a redes sociales. 3. Determina los horarios en los que los demás usuarios podrán tener acceso a redes sociales.
Flujo alternativo:	El usuario administrador debe de seleccionar horarios válidos; es decir, se deben de seleccionar horas válidas de entre el inicio y fin.
Poscondiciones:	El usuario administrador puede seleccionar entre si deja libre acceso a redes sociales o si establece un horario.

Tabla 7 Caso de uso - Configuración de acceso a redes sociales

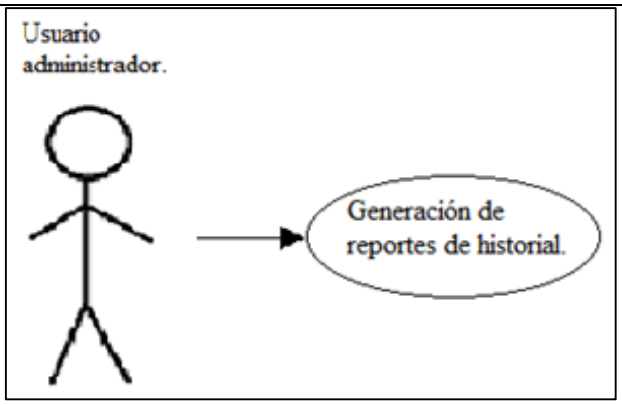

Figura 9 Caso de uso administrador - Generación de reportes de historial

Especificaciones de caso de uso	
Nombre	**Generación de reportes de historial**
Descripción:	El usuario administrador puede generar reportes de historial tanto generales como específicos (redes sociales, búsquedas específicas, etc.)
Precondiciones:	El usuario administrador debe de ingresar desde su propia cuenta administrativa del equipo.
Flujo normal:	1. Selecciona la opción de Historial. 2. Selecciona el usuario al cual desea generar el reporte de historial y selecciona si desea exportarlo como archivo Pdf o Excel.
Flujo alternativo:	Si el usuario administrador desea filtrar los datos por fechas, se debe de seleccionar fechas válidas entre inicio y fin.
Poscondiciones:	El usuario administrador obtiene el archivo Pdf o Excel con el historial de navegación del usuario seleccionado.

Tabla 8 Caso de uso - Generación de reportes de historial

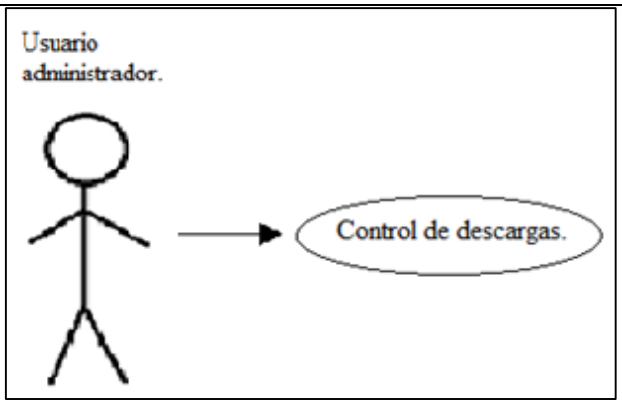

Figura 10 Caso de uso administrador - Control de descargas

Especificaciones de casos de uso	
Nombre:	**Control de descargas.**
Descripción:	El usuario administrador puede configurar si los demás usuarios tendrán acceso a descargas de archivos.
Precondiciones:	El usuario administrador debe de estar logueado.
Flujo normal:	1. El usuario administrador ingresa mediante su usuario y clave a las configuraciones del sistema. 2. Selecciona la opción de Configuración. 3. Define si desea que los demás usuarios tendrán acceso a descargas de archivos libremente o puede configurar un horario para dicha actividad. 4. Además cuenta con la posibilidad de bloquear los gestores de descargas más conocidos como Ares, Internet Donwload Manager, ATubeCatcher y entre otros.
Flujo alternativo:	Si el usuario administrador desea establecer un horario para permitir las descargas a los demás usuarios; se debe de especificar un rango válido de rango de horarios, siendo la hora de inicio menor que la hora de fin.
Poscondiciones:	Las configuraciones establecidas serán guardadas y se establecerán para los demás usuarios.

Tabla 9 Caso de uso - Control de descargas

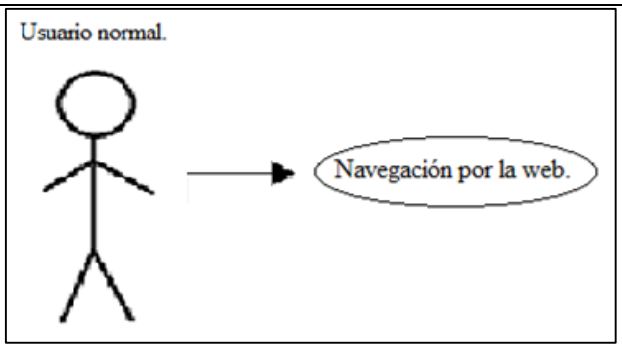

Figura 11 Caso de uso ordinario - Navegación por la web

Especificaciones de casos de uso	
Nombre:	**Navegación por la web.**
Descripción:	Descripción de la acción de acceso a Internet que tiene el usuario.
Precondiciones:	• El usuario debe de ingresar a su cuenta de usuario en el equipo.
Flujo normal:	1. El usuario inicia sesión en su cuenta de usuario del equipo. 2. Inicia la aplicación de Safe Browser.
Flujo alternativo:	De haber restricciones en las configuraciones por parte del administrador, el usuario tendrá acceso a las páginas web según dichas configuraciones.
Poscondiciones:	El usuario tendrá acceso a páginas web según las configuraciones.

Tabla 10 Caso de uso – Navegación por la web

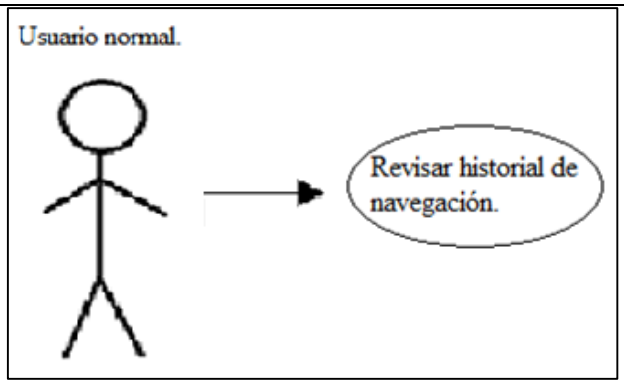

Figura 12 Caso de uso ordinario - Revisar historial de navegación

Especificaciones de casos de uso	
Nombre:	**Revisar historial de navegación.**
Descripción:	Permite que el usuario visualice las direcciones url a las que ha tenido acceso, las opción de eliminación de historial para los usuarios normales esta deshabilitado.
Precondiciones:	• El usuario debe de ingresar a su cuenta de usuario en el equipo.
Flujo normal:	1. El usuario inicia sesión en su cuenta de usuario del equipo. 2. Inicia la aplicación de Safe Browser. 3. Accede al historial mediante el submenú del navegador web; o con la combinación de teclas Ctrl + h.
Flujo alternativo:	El usuario no tendrá acceso a la eliminación del alguna url a la que haya tenido acceso; si el usuario desease filtrar el historial de navegación se lo puede realizar mediante un rango de fechas específicas, tomando en cuenta un rango valido de las mismas.
Poscondiciones:	El usuario podrá visualizar el historial según su criterio de búsqueda.

Tabla 11 Caso de uso - Revisar historial de navegación

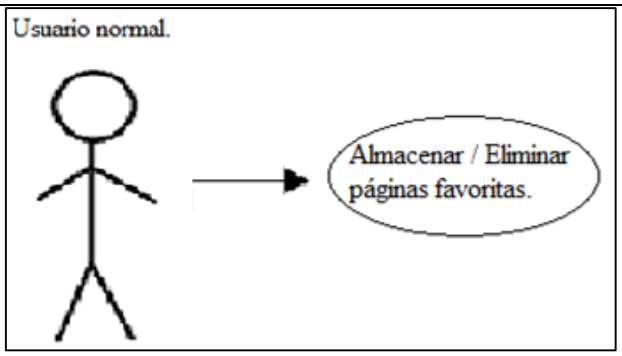

Figura 13 Caso de uso ordinario - Almacenar / Eliminar favoritos

Especificaciones de casos de uso	
Nombre:	**Almacenar / Eliminar páginas favoritas.**
Descripción:	Permite al usuario guardar o eliminar cualquier url para rápido acceso. Las paginas favoritas almacenadas son independiente de cada usuario; esto quiere decir que sin importar la cantidad de usuarios en el equipo, cada uno tiene su propia lista de favoritos
Precondiciones:	• El usuario debe de ingresar a su cuenta de usuario en el equipo.
Flujo normal:	1. El usuario inicia sesión en su cuenta de usuario del equipo. 2. Inicia la aplicación de Safe Browser. 3. Accede a la página web deseada. 4. La añade como favorita mediante el menú del navegador. 5. Si Desease eliminar alguna url, selecciona la pestaña de Favoritos, busca la url deseada y la elimina.
Flujo alternativo:	Solo se podrán almacenar páginas web a las que tenga acceso el usuario, según las configuraciones del administrador.
Poscondiciones:	La página web es agregada / eliminada de la lista de favoritos de dicho usuario.

Tabla 12 Caso de uso - Almacenar / Eliminar páginas favoritas

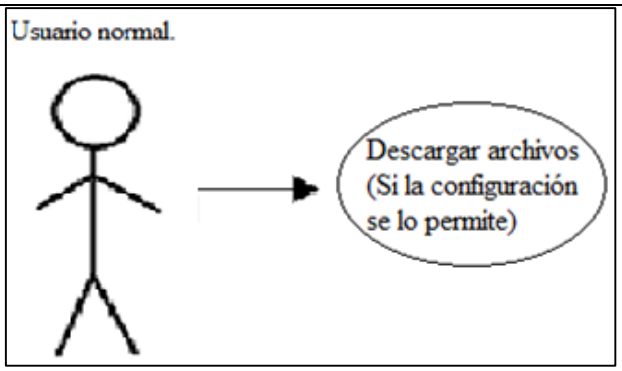

Figura 14 Caso de uso ordinario - Descargas de archivos

Especificaciones de casos de uso	
Nombre:	**Descargas de archivos.**
Descripción:	El usuario tendrá acceso a descargas de archivos si la configuración del administrador la permite.
Precondiciones:	• El usuario debe de ingresar a su cuenta de usuario en el equipo.
Flujo normal:	1. El usuario inicia sesión en su cuenta de usuario del equipo. 2. Inicia la aplicación de Safe Browser. 3. Descarga el archivo que desee, ya sea mediante el navegador o por algún gestor de descargas.
Flujo alternativo:	Si las configuraciones del administrador no permiten las descargas de archivos o no permiten el uso de gestores de descargas, el usuario no tendrá la posibilidad de descargar archivos desde la web.
Poscondiciones:	El usuario descarga el archivo deseado ya sea mediante el navegador o un gestor de descarga.

Tabla 13 Caso de uso - Descarga de archivos

Diseño de la base de datos

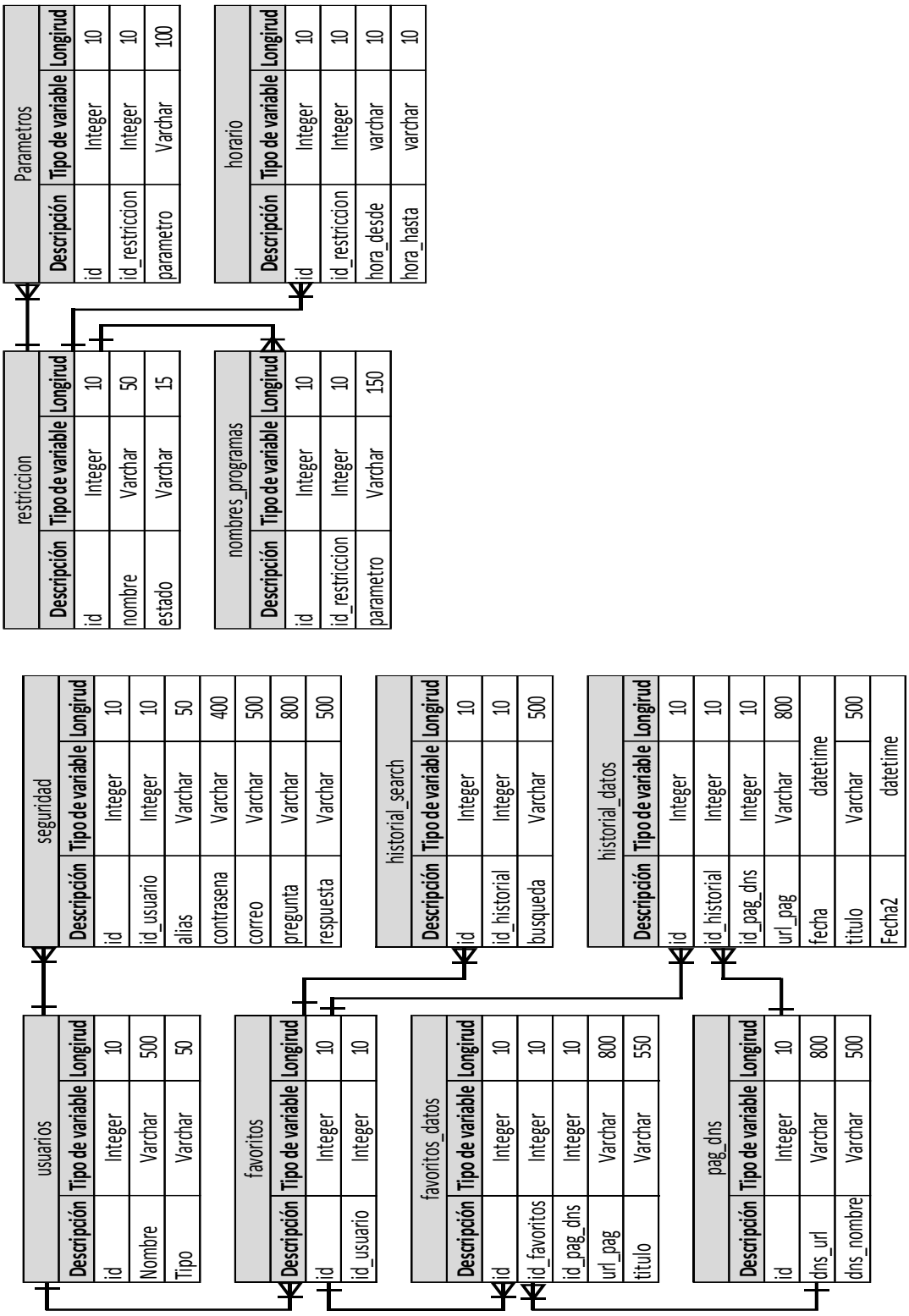

Figura 15 Diseño relacional de la base de datos

2.5.2. Diseño de la propuesta

Arquitectura del navegador web seguro

La arquitectura del navegador web está compuesta por las siguientes especificaciones.

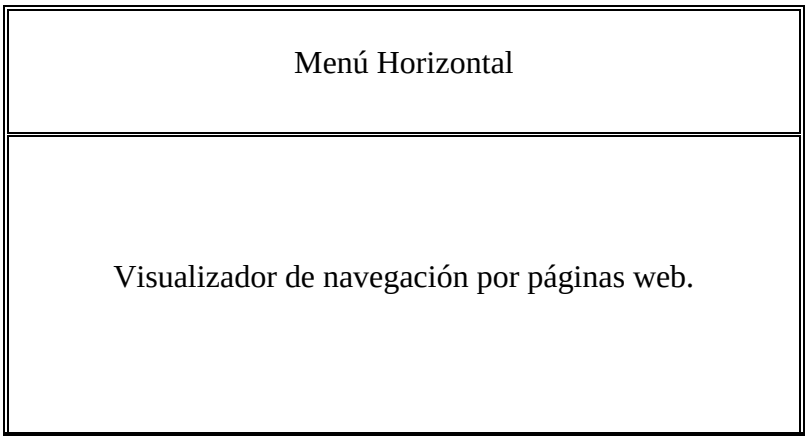

Figura 16 Pantalla de portada principal de navegador web seguro

Componentes de la propuesta

Módulos del navegador web seguro

- **Módulo de registro de administrador:** módulo por el cual se registra los datos del usuario administrador, usuario que tendrá todos los privilegios y accesos a las configuraciones del navegador.

Figura 17 Registro de usuario administrador

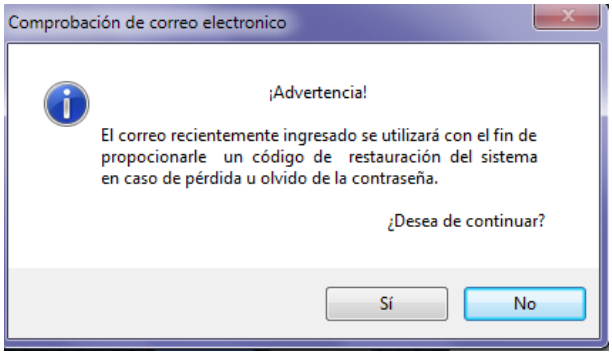

Figura 18 Mensaje de verificación de datos de registro

- **Módulo de configuraciones de accesos:** módulo por el cual el usuario administrador puede configurar los horarios de accesos a redes sociales, bloqueos de páginas específicas, bloqueo de accesos a páginas con contenido para adultos y bloqueo de los gestores de descargas.

Figura 19 Personalización de restricciones.

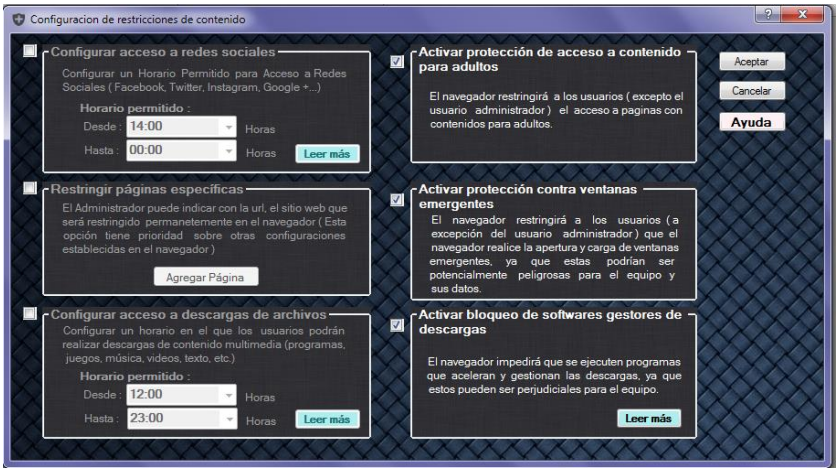

Figura 20 Opciones administrativas de accesos para los demás usuarios

- **Módulo de registro de historial de navegación:** módulo por el cual el usuario administrador y el usuario invitado tienen acceso a la vista del historial de navegación; pero solo el usuario administrador cuenta con privilegios de eliminación, exportación y vista de reportes de todos los historiales de navegación de las otras cuentas de invitado que existan en el equipo.

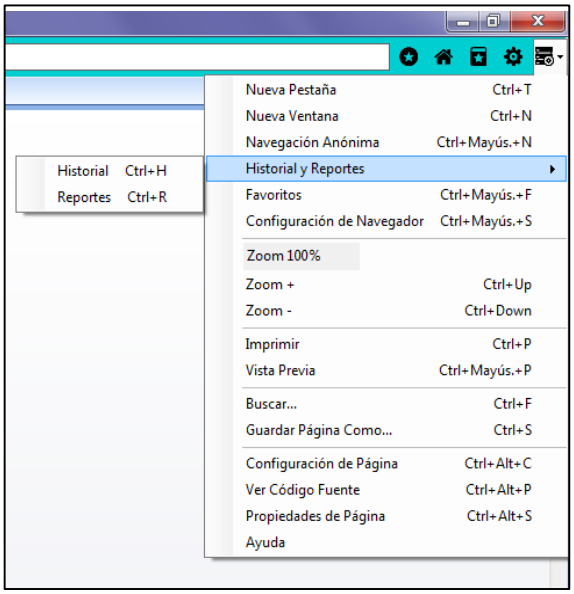

Figura 21 Historial de navegación y reportes.

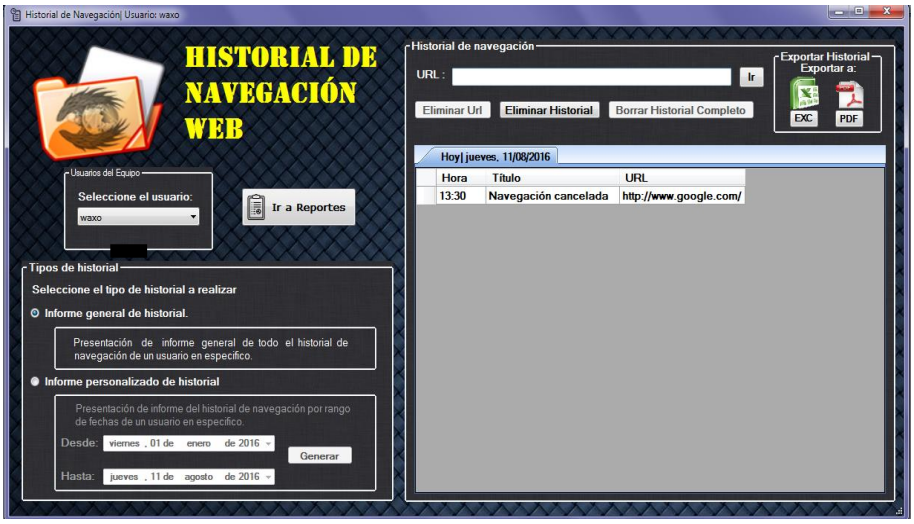

Figura 22 Vista de historial de navegación

- **Módulo de generación de reportes:** módulo en el cual el usuario administrador puede filtrar la información que sea de su interés en relación

a los historiales de navegación de otras cuentas de usuarios; esta información se puede filtrar por búsquedas de: redes sociales, intentos de accesos a proxy en línea, páginas web navegadas e intentos de acceso a contenido adulto.

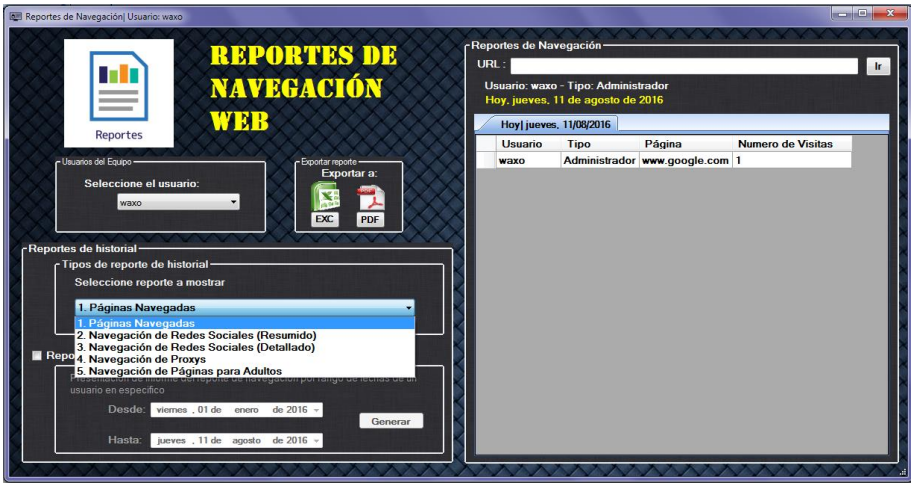

Figura 23 Vista de reportes.

- **Módulo de páginas favoritas:** módulo por el cual los usuarios del navegador pueden guardar y administrar sus páginas favoritas sin afectar los registros de otros usuarios.

Figura 24 Agregado de una página web a favoritos

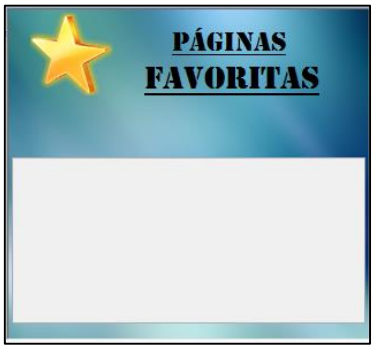

Figura 25 Lista de páginas web favoritas

- **Módulo de acceso administrativo:** módulo por el cual el usuario administrador tiene acceso a las configuraciones del navegador desde cualquier cuenta de usuario del computador.

Figura 26 Formulario para ingreso a configuraciones administrativas

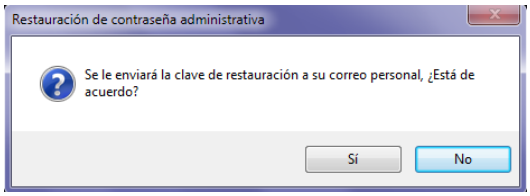

Figura 27 Mensaje de confirmación para recuperación de contraseña

Figura 28 Recuperación de contraseña mediante código electrónico

Figura 29 Recuperación de contraseña mediante pregunta de seguridad

2.5.3. Estudios de factibilidad

Factibilidad técnica

En la factibilidad técnica se detallan los recursos de hardware y software utilizados en el proyecto.

Cantidad	Descripción
1	SQLite
1	NetFramework
1	Office 2013
1	Visual Studio 2013
1	Dr. Explain (versión de prueba)
1	DoNetBar
1	Inno Setup

Tabla 14 Análisis técnico de Software

Cantidad	Descripción
1	Laptop Dell 64 bits
1	Laptop Sony Vaio 64 bits
1	Impresora HP
2	Memoria USB 8 Gb

Tabla 15 Análisis técnico de Hardware

Luego del análisis realizado inicialmente es posible indicar que el desarrollo del proyecto es técnicamente factible, ya que los equipos y herramientas de software usadas en el desarrollo del proyecto las poseen los estudiantes a cargo de la investigación.

Análisis técnico

Al realizar un análisis técnico tanto de hardware como de software se obtuvo lo siguiente: el desarrollo del navegador web es posible ya que la plataforma de

desarrollo de Visual Studio 2013 junto con el lenguaje integrado de NetFramework, ofrece una amplia gama de opciones potentes de desarrollo, también hay la disponibilidad de foros de colaboradores y programadores en la Web, así como una amplia gama de extensiones que se le puede agregar a Visual Studio como lo es DoNetBar, lo que hace más sencillo la programación.

Se utilizó SQLite Maestro como servidor de base de datos, ya que es uno de los más populares sistemas de administración de bases de datos.

El hardware utilizado son dos computadoras de uso personal de los estudiantes a cargo del proyecto, por lo que no se tiene ningún problema en cuanto al acceso y desarrollo de la aplicación, las mismas que cuentan con las herramientas y programas necesarios para el desarrollo del mismo.

Al ser una aplicación de escritorio, se trabajó de tal modo en que no haya limitantes en cuanto a compatibilidad de versiones entre 32 y 64 bits entre los sistemas operativos de los usuarios finales.

Cada computadora cuenta con máquinas virtuales de 32 bits para garantizar el buen funcionamiento de la aplicación en distintas versiones.

Factibilidad económica

A continuación, se detallan los recursos de hardware, software, materiales de oficina, personal y gastos de servicios básicos.

Equipos	Costo	Cantidad	Total
Laptop Dell 64 bits	$ 750.00	1	$ 750.00
Laptop Sony Vaio 64 bits	$ 800.00	1	$ 800.00
Impresora	$ 350.00	1	$ 350.00
Pendrives	$ 12.00	2	$ 24.00
Total			$ 1924.00

Tabla 16 Costo de Hardware

Descripción	Costo	Cantidad	Total
SQLite	$ 0.00	1	$ 0.00
NetFramework	$ 0.00	1	$ 0.00
Office 2013	$ 139.99	1	$ 139.99
Visual Studio 2013	$ 0.00	1	$ 0.00
Dr. Explain	$ 0.00	1	$ 0.00
DoNetBar	$ 0.00	1	$ 0.00
Inno setup	$ 0.00	1	$ 0.00
Total			$ 139.99

Tabla 17 Costo de Software

Descripción	Costo / Mes	Meses	Total
Analista - Programador	$ 1200.00	8	$ 9600.00
Diseñador	$ 1000.00	5	$ 5000.00
Documentador	$ 500.00	3	$ 1500.00
Tester	$ 300.00	3	$ 900.00
Total			$ 17000.00

Tabla 18 Costo de personal

Descripción	Costo	Cantidad	Total
Resma de papel.	$ 5.00	1	$ 5.00
Cartuchos de tinta.	$ 40.00	2	$ 80.00
Total			$ 85.00

Tabla 19 Costo de materiales de oficina

Descripción	Costo	Meses	Total
Internet.	$ 20.00	8	$ 160.00
Energía eléctrica.	$ 17.00	8	$ 136.00
Transporte.	$ 52.00	8	$ 416.00
Total			$ 712.00

Tabla 20 Costo de servicios básicos

Descripción	Costo
Hardware.	$ 1924.00
Software.	$ 139.99
Personal.	$ 17000.00
Materiales de oficina.	$ 85.00
Servicios básicos.	$ 712.00
Total.	$ 19860.99

Tabla 21 Costo del proyecto

El costo de desarrollo del navegador web seguro es de $ 19860.99, los costos de implementación fueron asumidos por el Colegio particular INNOVA.

Como se puede apreciar en la tabla 24 se utilizaron herramientas de software libre, es decir que la institución no tiene que invertir en gastos adicionales por el uso de licencias.

El colegio cuenta actualmente con un Departamento de Tecnología en donde se maneja el funcionamiento de los laboratorios y cuentan con un proxy, el cual se encarga de garantizar el acceso a Internet en toda la institución educativa.

Los costos de hardware, personal, servicios básicos y materiales de oficina serán asumidos por los estudiantes a cargo del proyecto, haciendo que este trabajo no tenga costo alguno y genere un ahorro del 100% de la inversión para el Colegio particular INNOVA.

2.5.4. Resultados

A continuación, se detalla en esta sección las pruebas de seguridad, validación y funcionalidad que se realizaron durante el desarrollo del navegador “Safe Browser”, y los resultados obtenidos. También se describe la comprobación de las hipótesis planteadas para este estudio.

Escenarios de prueba

Se presenta una descripción con detalle de las estrategias utilizadas para el desarrollo de los procesos y de los resultados obtenidos, que sirven para evaluar el desempeño y la funcionabilidad de la aplicación. Las pruebas fueron llevadas a cabo en conjunto con el personal encargado de la administración de la sala de cómputo y el profesor tutor.

Pruebas de Seguridad

El navegador web utiliza la herramienta SQLite, la cual es una base de datos relacional embebida que se integra de manera perfecta a las necesidades del proyecto; Sqlite es utilizado también por otros navegadores como Google Chrome, Mozilla Firefox, Opera, entre otros.

El software, para la configuración y administración del control parental requiere de un usuario y contraseña que garantice la seguridad de acceso al mismo; por tanto, la contraseña, al ser un dato sensible se encuentra cifrada a través del algoritmo SHA-1. Para asegurar la funcionalidad de este módulo se debe ingresar el correo electrónico del usuario y una pregunta de seguridad, en caso de olvido o restauración de la contraseña.

A continuación, se detallan las pruebas de seguridad realizadas:

PRUEBA DE SEGURIDAD	
Descripción	Verificar que el usuario tiene acceso a todas las configuraciones del control parental y de contenidos
Entradas	Usuario y contraseña
Salidas	Formulario de configuración de control parental y de contenidos

Tabla 22 Prueba de seguridad de Usuario

PRUEBA DE SEGURIDAD	
Descripción	Verificar que el usuario tenga acceso a todas las configuraciones del control parental y de contenidos mediante la contraseña encriptada
Entradas	Usuario y contraseña
Salidas	Formulario de configuración de control parental y de contenidos

Tabla 23 Prueba de seguridad de encriptación de contraseña

PRUEBA DE SEGURIDAD	
Descripción	Verificar que el usuario pueda restaurar la contraseña por medio del correo electrónico
Entradas	código de restauración enviada al correo
Salidas	Formulario para volver a ingresar los datos de usuario y contraseña

Tabla 24 Prueba de seguridad de restauración de contraseña (e-mail)

PRUEBA DE SEGURIDAD	
Descripción	Verificar que el usuario pueda restaurar la contraseña por medio de la pregunta de seguridad
Entradas	Respuesta a la pregunta de seguridad
Salidas	Formulario para volver a ingresar los datos de usuario y contraseña

Tabla 25 Prueba de seguridad de restauración de contraseña (pregunta de seguridad)

Análisis: En la pruebas se observa que para realizar las configuraciones en las opciones del control parental y de contenido se debe ingresar el usuario y la contraseña, además, se puede evidenciar que la contraseña está cifrada y su proceso no afecta a la funcionalidad del navegador. Así mismo, en caso de olvido o restauración de la contraseña, hay la posibilidad de recuperar a través de las

opciones disponibles; esto es, a través de un código enviado al correo electrónico del usuario o mediante la pregunta de seguridad establecida por el usuario.

Pruebas de Validación

Las pruebas de validación aplicadas están enfocadas en la información y variables de entrada del navegador Safe Browser y los datos que son obligatorios para los diferentes procesos de la aplicación. A continuación, se describen las pruebas efectuadas:

Usuario de Windows: Se verifica que el usuario de windows del equipo en el cual se instala y configura el navegador Safe Browser debe contar con permisos de administrador.

Contraseña encriptada de usuario de Safe Browser: El password (contraseña) ingresado por el usuario para la configuración del control parental y de contenidos se encuentra cifrado, esto como control de seguridad para evitar que los alumnos no puedan manipular dichos controles. Se verifica que la contraseña proporcionada contenga un mínimo de 8 caracteres, compuesta de números y letras tanto minúsculas y mayúsculas.

Correo electrónico de usuario: Se comprueba que el correo ingresado sea válido y funcional, pues es necesario para la restauración de la contraseña en caso de olvido.

Campos obligatorios (control parental y de contenidos): Todos los formularios con campos obligatorios, se valida su contenido e integridad en la información ingresada.

Restricción de Acceso a Navegadores: El uso de otros navegadores está restringido en los usuarios de windows del equipo, a excepción del usuario en el que se instaló y configuró el navegador web Safe Browser.

Reportes de Historiales y de Navegación: Pueden ser generados solo en la sesión del usuario que tenga permisos de administrador.

Url Específica (control parental y de contenidos): Al restringir el acceso a una url, ésta debe ser válida.

Análisis: El resultado obtenido de las pruebas es satisfactorio, dado, que se determinó que todos los campos se encuentran validados. Todos los campos de la aplicación son obligatorios, ya que son de utilidad en los diferentes procesos que ejecuta el navegador web, principalmente para el control parental y de contenidos.

Pruebas de Funcionalidad

Con estas pruebas se procede a la comprobación de todas las acciones y procesos del navegador Safe Browser.

PRUEBA DE CREACIÓN DE USUARIO DE SAFE BROWSER	
Descripción	Verificar la creación del usuario de Safe Browser para la configuración del control parental y de contenidos
Entradas	Usuario, contraseña, correo, pregunta de seguridad y respuesta
Salidas	Formulario de tipo de configuración del navegador

Tabla 26 Prueba de creación de usuario de Safe Browser

PRUEBA DE SELECCIÓN DE TIPO DE CONFIGURACIÓN	
Descripción	Verificar que el usuario pueda seleccionar el tipo de configuración para el navegador.
Entradas	Tipo de configuración.
Salidas	Ventana Principal de Safe Browser (Configuración por Default) o Formulario de Configuración de Control Parental y de Contenidos (Configuración Personalizada).

Tabla 27 Prueba de selección de tipo de configuración

PRUEBA DE ACCESO A LAS CONFIGURACIONES DE CONTROL PARENTAL Y DE CONTENIDOS	
Descripción	Comprobar que el usuario puede acceder a la ventana de configuración del control parental y de contenidos del navegador.
Entradas	Usuario y contraseña
Salidas	Formulario de Configuración de Control Parental y de Contenidos

Tabla 28 Prueba de acceso a las configuraciones de control

PRUEBA DE CONFIGURACIÓN DEL CONTROL PARENTAL Y DE CONTENIDOS	
Descripción	Comprobar que el usuario pueda configurar de acuerdo a sus necesidades el control parental y de contenidos.
Entradas	Estado de los controles, Horarios de acceso (para aquellos que lo requieran), campos obligatorios.
Salidas	Ventana Principal de Safe Browser.

Tabla 29 Prueba de configuración del control parental y de contenidos

PRUEBA DE RESTAURACIÓN DE CONTRASEÑA (POR CORREO ELECTRÓNICO)	
Descripción	Comprobar que el usuario pueda restaurar la contraseña del usuario de Safe Browser por medio del correo electrónico.
Entradas	Clave de restauración enviada al correo electrónico.
Salidas	Formulario de Ingreso de Datos de Usuario de Safe Browser.

Tabla 30 Prueba de restauración de contraseña (por correo electrónico)

PRUEBA DE RESTAURACIÓN DE CONTRASEÑA (POR PREGUNTA DE SEGURIDAD)	
Descripción	Comprobar que el usuario pueda restaurar la contraseña del usuario de Safe Browser por medio de la pregunta de seguridad.
Entradas	Respuesta de la pregunta de seguridad.
Salidas	Formulario de Ingreso de Datos de Usuario de Safe Browser.

Tabla 31 Prueba de restauración de contraseña (por pregunta de seguridad)

PRUEBA DE NAVEGACIÓN DE PÁGINAS EN INTERNET	
Descripción	Verificar que el usuario pueda navegar en internet mediante el navegador Safe Browser.
Entradas	Dirección URL de la página a navegar.
Salidas	Carga y visualización del sitio web digitado en la ventana principal de Safe Browser

Tabla 32 Prueba de navegación de páginas en internet

PRUEBA DE MANEJO DE LISTA DE PÁGINAS FAVORITAS	
Descripción	Verificar que el usuario agregar, eliminar y modificar un elemento en la lista de páginas favoritas.
Entradas	Dirección URL de la página, Acción a realizar.
Salidas	Listado actualizado de páginas favoritas.

Tabla 33 Prueba de manejo de lista de páginas favoritas

PRUEBA DE EJECUCIÓN DE LAS CONFIGURACIONES DEL CONTROL PARENTAL Y DE CONTENIDOS	
Descripción	Verificar que el control parental y de contenidos se lleve a cabo con éxito durante la navegación.
Entradas	Usuario de Windows, estados y parámetros de los controles.
Salidas	Mensaje de restricción de acceso y navegación

Tabla 34 Prueba de ejecución de las configuraciones del control

PRUEBA DE RESTRICCIÓN DE ACCESO A OTRO NAVEGADORES	
Descripción	Comprobar que la ejecución de otros navegadores está restringidos.
Entradas	Usuario de Windows, Lista de navegadores a restringir
Salidas	Mensaje de error de Windows, Ejecución del Navegador de Safe Browser

Tabla 35 Prueba de restricción de acceso a otros navegadores

PRUEBA DE GENERACIÓN DE HISTORIALES DE NAVEGACIÓN DE USUARIO	
Descripción	Verificar que el usuario pueda visualizar y administrar el historial de navegación
Entradas	Usuario de Windows, rango de fechas para el Historial, acción a realizar.
Salidas	Listado de las páginas Navegadas

Tabla 36 Prueba de generación de historiales de navegación de usuario

PRUEBA DE GENERACIÓN DE REPORTES DE NAVEGACIÓN DE USUARIO	
Descripción	Verificar que el usuario puede generar reportes de navegación que necesite y que el navegador Safe Browser le permite.
Entradas	Usuario de Windows, tipo de reporte a generar, rango de fechas para el reporte de navegación.
Salidas	Reporte de páginas Navegadas

Tabla 37 Prueba de generación de reportes de navegación de usuario

PRUEBA DE EXPORTACIÓN A EXCEL Y PDF DE LOS REPORTES E HISTORIALES DE NAVEGACIÓN DE USUARIO	
Descripción	Verificar que el usuario pueda exportar los reportes e historiales de navegación de los usuarios a Excel y Pdf
Entradas	Usuario de Windows, Tipo de archivo a exportar, Información a exportar
Salidas	Archivos de Excel y/o Pdf con el contenido seleccionado

Tabla 38 Prueba de exportación a extensión Excel y Pdf

Análisis: En estas pruebas no se encontraron deficiencias, puesto que, cada proceso evaluado se ejecutó de manera normal, sin inconveniente alguno.

Pruebas de Aceptación

Estas pruebas tienen como objetivo evaluar el desempeño del navegador Safe Browser basados en el análisis de requerimientos, que permitan conocer los resultados y las ideas generales de las pruebas, estableciendo la aceptación o rechazo de la aplicación. A continuación se detalle las pruebas:

PRUEBAS DE ACEPTACIÓN			
Código:	01	**Nombre:**	Creación de Usuario de Safe Browser.
Descripción:			
El usuario debe crearlas credenciales de acceso (user, password) para configurar el control parental y de contenidos en el navegador.			
Condiciones de Ejecución:			
El usuario de Windows del equipo debe tener permisos de administrador.			

Entradas/Pasos de Ejecución:	
El usuario: Instala el navegador en el equipo y procede a crear el usuario de Safe Browser. Debe ingresar los siguientes datos: Introducir un alias para el usuario. Digitar su correo electrónico. Escribir una contraseña para el usuario. Selecciona y responde la pregunta de seguridad. Clic en Aceptar. Clic en Si, en mensaje de Advertencia.	
Resultado Esperado:	
Mensaje de Confirmación de Creación de Usuario, y apertura de la ventana de Selección de Tipo de Configuración de Restricciones de Usuario.	
Evaluación de la Prueba:	**Satisfactoria**

Tabla 39 Prueba de aceptación - Creación de usuario de Safe Browser

PRUEBAS DE ACEPTACIÓN			
Código:	02	**Nombre:**	Selección de Tipo de Configuración de Safe Browser
Descripción:			
El usuario debe elegir el tipo de configuración para las restricciones del control parental y de contenido del navegador.			
Condiciones de Ejecución:			
El navegador debe contar con el usuario de Safe Browser.			
Entradas/Pasos de Ejecución:			

El usuario: Debe elegir una de las dos opciones de configuración disponibles. <u>Opción 1:</u> Clic en la opción de configuración por defecto. Clic en botón aceptar. <u>Opción 2:</u> Clic en la opción de configuración personalizada. Clic en botón aceptar.
Resultado Esperado:
<u>Opción 1:</u> Mensaje de confirmación, Apertura de la ventana principal de Safe Browser. <u>Opción 2:</u> Apertura de la ventana de configuración del control parental y de contenidos.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 40 Prueba de aceptación - Configuración de Safe Browser

PRUEBAS DE ACEPTACIÓN			
Código:	03	**Nombre:**	Acceso a la configuración de las restricciones de Safe Browser
Descripción:			
El usuario debe acceder a la ventana de configuración del control parental y de contenido por medio del usuario y contraseña de Safe Browser.			
Condiciones de Ejecución:			
La aplicación debe contar con el usuario de Safe Browser.			

Entradas/Pasos de Ejecución:	
El usuario: Puede acceder a configurar las restricciones de Safe Browser a través de las siguientes opciones. 1. Clic en el ícono Administrar Navegador, ubicado en la barra de opciones. 2. Clic en el ícono Menú, y seleccionar la opción "Configuración de Navegador". 3. Digitar simultáneamente las teclas Control, Mayúscula S. Entonces, se da apertura a la ventana de acceso administrativo, el usuario debe introducir su usuario y contraseña. Dar clic en el botón "Login".	
Resultado Esperado:	
Se visualiza la ventana de configuración de las restricciones del control parental y de contenido de Safe Browser.	
Evaluación de la Prueba:	**Satisfactoria**

Tabla 41 Prueba de aceptación - Acceso a control parental y de contenidos

PRUEBAS DE ACEPTACIÓN			
Código:	04	**Nombre:**	Configuración del Control Parental y de Contenidos de Safe Browser
Descripción:			
El usuario puede cambiar las configuraciones del control parental y de contenidos del navegador.			
Condiciones de Ejecución:			
El usuario debe haber accedido por medio del usuario de Safe Browser.			
Entradas/Pasos de Ejecución:			
El usuario:			

Puede acceder configurar cada una de las restricciones del control parental y de contenidos.

Opción 1:

Activar acceso a redes sociales:

Marcar la casilla de acceso a redes sociales

Elegir un horario de inicio y fin para el acceso

Desactivar acceso a redes sociales: Desmarcar casilla

Opción 2:

Activar acceso a páginas específicas: Marcar casilla

Desactivar acceso a páginas específicas: Desmarcar casilla

Opción 3:

Activar acceso a descargas de archivos:

Marcar la casilla de acceso a descargas de archivos

Elegir un horario de inicio y fin para el acceso

Desactivar acceso a descarga de archivos: Desmarcar casilla

Opción 4:

Activar acceso a páginas para adultos: Marcar casilla

Desactivar acceso a páginas para adultos: Desmarcar casilla

Opción 5:

Activar acceso a ventanas emergentes: Marcar casilla

Desactivar acceso a páginas específicas: Desmarcar casilla

Opción 6:

Activar acceso a gestores de descarga: Marcar casilla

Desactivar acceso a gestores de descarga: Desmarcar casilla

Resultado Esperado:

Opción 1:

Acceso a redes sociales:

Activo: Solo pueden navegarse en el horario establecido

Inactivo: Pueden navegarse sin restricciones

Opción 2:

Acceso a páginas específicas:

Activo: Las páginas establecidas no pueden navegarse

Inactivo: No hay restricciones de acceso

Opción 3: Acceso a descargas de archivos: Activo: Descargas permitidas solo en el horario establecido Inactivo: No hay restricciones en las descargas Opción 4: Acceso a páginas para adultos: Activo: Navegación de páginas para adultos restringidas Inactivo: No hay restricciones en páginas para adultos Opción 5: Acceso a ventanas emergentes: Activo: Restricción de acceso a ventanas emergentes Inactivo: Acceso a páginas emergentes sin restricciones. Opción 6: Acceso a gestores de descarga: Activo: Uso de gestores de descargas no permitidas Inactivo: Libre uso de gestores de descargas

Evaluación de la Prueba:	**Satisfactoria**

Tabla 42 Prueba de aceptación - Configuración de control parental

PRUEBAS DE ACEPTACIÓN			
Código:	05	**Nombre:**	Restricción de Páginas específicas
Descripción:			
El usuario puede agregar, editar y eliminar páginas de la lista a restringir.			
Condiciones de Ejecución:			
Tener activado la restricción de páginas específicas, y contar con la url de la página a eliminar, editar o eliminar.			
Entradas/Pasos de Ejecución:			

Opción 1(Agregar Página): Digite la url de la página en el cuadro de texto. Clic en “Agregar URL”. Opción 2(Editar Página): Seleccione una url de la lista de páginas a restringir. Modificar la URL en el cuadro de texto. Clic en “Editar URL”. Opción 3(Eliminar página): Seleccione una url de la lista de páginas a restringir. Clic en “Eliminar URL”. Clic en “Aceptar”
Resultado Esperado:
Opción 1 (Agregar Página): Se verifica en el listado la dirección web añadida y que ésta no pueda ser accedida en la ventana principal. Opción 2 (Editar Página): Se verifica en el listado la dirección web modificada y que ésta no pueda ser accedida en la ventana principal. Opción 3 (Eliminar Página): Se verifica que en el listado no conste la dirección web eliminada y que ésta pueda ser accedida en la ventana principal.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 43 Prueba de aceptación - Páginas restringidas

PRUEBAS DE ACEPTACIÓN			
Código:	06	**Nombre:**	Restauración de contraseña por correo electrónico

Descripción:
El usuario puede restaurar los datos del usuario de Safe Browser a través del correo electrónico en caso de olvido o cambio de contraseña.
Condiciones de Ejecución:
La aplicación debe contar con el usuario de Safe Browser. Acceso a Internet.
Entradas/Pasos de Ejecución:
El usuario: Debe acceder a la ventana de administración de Safe Browser a través de las siguientes opciones. 4. Clic en el ícono Administrar Navegador, ubicado en la barra de opciones. 5. Clic en el ícono Menú, y seleccionar la opción "Configuración de Navegador". 6. Digitar simultáneamente las teclas Control, Mayúsc y S. Una vez abierta la ventana de acceso administrativo, debe: Dar clic en el enlace "¿Olvidó su contraseña?". Clic en "Si", en el mensaje de Advertencia, y esperar el mensaje de confirmación. Revisar su cuenta de correo electrónico y copiar el código de restauración enviado. Digitar o pegar el código en el cuadro de texto. Clic en "Login". Rellenar todos los campos requeridos en la ventana de usuario de Safe Browser y dar clic en "Aceptar".
Resultado Esperado:
Datos del usuario de Safe Browser actualizados y re direccionamiento a la ventana de configuración del control parental y de contenidos.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 44 Prueba de aceptación - Restauración de usuario por e-mail

PRUEBAS DE ACEPTACIÓN			
Código:	07	**Nombre:**	Restauración de contraseña por pregunta de seguridad
Descripción:			
El usuario puede restaurar los datos del usuario de Safe Browser contestando la pregunta de seguridad de Safe Browser en caso de olvido o cambio de contraseña.			
Condiciones de Ejecución:			
La aplicación debe contar con el usuario de Safe Browser. Restauración por correo electrónico fallida.			
Entradas/Pasos de Ejecución:			
El usuario: Una vez abierta la ventana de acceso administrativo y haber intentado restaurar el usuario por correo electrónico, debe: Dar clic en el enlace "Restaurar por pregunta de seguridad". Responder a la pregunta en el cuadro de texto. Clic en "Login". Rellenar todos los campos requeridos en la ventana de usuario de Safe Browser y dar clic en "Aceptar".			
Resultado Esperado:			
Datos del usuario de Safe Browser actualizados y re direccionamiento a la ventana de configuración del control parental y de contenidos.			
Evaluación de la Prueba:		**Satisfactoria**	

Tabla 45 Prueba de aceptación - Restauración de usuario por pregunta de seguridad

PRUEBAS DE ACEPTACIÓN			
Código:	08	**Nombre:**	Navegación de Páginas en Internet.
Descripción:			
El usuario debe poder navegar en internet en la ventana principal de Safe Browser.			
Condiciones de Ejecución:			
La aplicación debe contar con: Usuario de Safe Browser Control parental y de contenidos configurado Acceso a internet.			
Entradas/Pasos de Ejecución:			
El usuario: Ingresa a todas las opciones de navegación de la aplicación. <u>Opción 1 (Ir a una página):</u> Escribir la url de la página a navegar en el cuadro de texto de la barra de opciones y presionar la tecla “Enter”. <u>Opción 2 (Atrás):</u> Clic en el ícono “Atrás” de la barra de opciones. <u>Opción 3 (Adelante):</u> Clic en ícono “Adelante” de la barra de opciones. <u>Opción 4 (Refrescar Página):</u> Clic en el ícono “Actualizar” de la barra de opciones. <u>Opción 5 (Ir a Google):</u> Clic en ícono “Ir a Google” de la barra de opciones. <u>Opción 6 (Nueva Pestaña):</u> Se puede acceder a una nueva ventana de navegación de tres formas: 1. Clic en la pestaña “Nuevo” del panel de Navegación 2. Clic en el ícono “Menú” y seleccionar la opción “Nueva Pestaña”.			

3. Pulsar simultáneamente las teclas “Control” y “T”

Opción 7 (Nueva Ventana):

Se puede acceder a una nueva ventana de navegación de tres formas:

1. Clic en el ícono “Administrar Navegador” y dar clic en “Nueva Ventana”.
2. Clic en el ícono “Menú” y seleccionar la opción “Nueva Ventana”.
3. Pulsar simultáneamente las teclas “Control” y “N”

Opción 8 (Navegación Anónima):

Se puede acceder a una nueva ventana de navegación de dos formas:

1. Clic en el ícono “Menú” y seleccionar la opción “Navegación anónima”.
2. Pulsar simultáneamente las teclas “Control”, “Mayus” y “N”.

Resultado Esperado:

Opción 1 (Ir a una página):

El contenido de la página de la url introducida debe cargarse en la pestaña de navegación actual, siempre y cuando no esté dentro de las restricciones del control parental y de contenidos.

Opción 2 (Atrás):

La página navegada anteriormente debe cargarse en la pestaña de navegación actual.

Opción 3 (Adelante):

La página navegada posteriormente debe cargarse en la pestaña de navegación actual.

Opción 4 (Refrescar Página):

Se vuelven a cargar los contenidos de la página navegada en ese momento.

Opción 5 (Ir a Google): Se debe redirigir a la página de Google en la pestaña de navegación actual. Opción 6 (Nueva Pestaña): Se debe abrir una nueva pestaña de navegación. Opción 7 (Nueva Ventana): Se debe abrir una nueva ventana principal de Safe Browser. Opción 8 (Navegación Anónima): Se debe abrir una ventana de navegación anónima de Safe Browser.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 46 Prueba de aceptación - Navegación en Internet

PRUEBAS DE ACEPTACIÓN			
Código:	09	**Nombre:**	Administración de Lista de Páginas Favoritas
Descripción:			
El usuario puede agregar, editar y eliminar elementos en la lista de páginas favoritas.			
Condiciones de Ejecución:			
La aplicación debe contar con: Usuario de Safe Browser. Control parental y de contenidos configurado.			
Entradas/Pasos de Ejecución:			
El usuario: Ingresa a todas las opciones de la aplicación. Opción 1 (Agregar Favorito): Clic en ícono “Añadir Favorito”. Introducir un nombre de etiqueta para la página. Clic en “Aceptar”.			

Opción 2(Editar Favorito):

Clic en ícono “Añadir Favorito”.

Introducir un nombre de etiqueta para la página.

Clic en “Editar”.

Opción 3 (Eliminar Favorito):

Para eliminar un elemento de la lista, existen 3 métodos:

1. Clic en el ícono “Añadir Favorito” y clic en “Eliminar”.
2. Método 2:

   Clic en el ícono “Administrar Favoritos”.

   Seleccionar un elemento de la lista.

   Clic en el ícono “Eliminar”.
3. Método 3:

   Clic en el ícono “Menú” y seleccionar la opción “Favoritos”

   Seleccionar un elemento de la lista.

   Clic en el ícono “Eliminar”.

Opción 4 (Buscar Favorito):

Para buscar un elemento de la lista, existen 2 métodos:

1. Método 1:

   Clic en el ícono “Administrar Favoritos”.

   Digitar en el cuadro de texto una palabra relacionada a la página a buscar.

   Clic en el botón “Buscar”.
2. Método 3:

   Clic en el ícono “Menú” y seleccionar la opción “Favoritos”

   Digitar en el cuadro de texto una palabra relacionada a la página a buscar.

   Clic en el botón “Buscar”.

Opción 5 (Ir a Favorito)

Para buscar un elemento de la lista, existen 2 métodos:

1. Método 1: Clic en el ícono “Administrar Favoritos”. Seleccionar un elemento de la lista. Clic en el botón “Ir”. 2. Método 3: Clic en el ícono “Menú” y seleccionar la opción “Favoritos” Seleccionar un elemento de la lista. Clic en el botón “Ir”.
Resultado Esperado:
Opción 1 (Agregar Favorito): Se verifica que la página navegada actualmente se encuentre en la lista de páginas favoritas. Opción 2 (Editar Favorito): Se verifica que la etiqueta de la página navegada actualmente se actualice. Opción 3 (Eliminar Favorito): Se verifica que el elemento seleccionado ya no esté en la lista de páginas favoritas. Opción 4 (Buscar Favorito): Se verifica que se muestren aquellos elementos cuya etiqueta coincida con la palabra de búsqueda. Opción 5 (Ir a Favorito) Se verifica que se cargue en la pestaña actual el elemento seleccionado de la lista de páginas favoritas.

Evaluación de la Prueba:	**Satisfactorio**

Tabla 47 Prueba de aceptación - Lista de páginas favoritas

PRUEBAS DE ACEPTACIÓN			
Código:	10	**Nombre:**	Acceso a otro navegadores
Descripción:			
No se puede tener acceso a los navegadores que consten en la lista de			

restricción, a excepción del usuario de Windows en el que fue instalado Safe Browser.
Condiciones de Ejecución:
Usuario de Windows diferente al usuario administrador.
Entradas/Pasos de Ejecución:
El usuario: Da clic sobre los íconos de los navegadores o intenta instalar uno de los navegadores restringidos.
Resultado Esperado:
Mensaje de Error de acceso y apertura de la ventana principal de Safe Browser.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 48 Prueba de aceptación - Acceso a otros navegadores

PRUEBAS DE ACEPTACIÓN			
Código:	11	**Nombre:**	Historiales de Navegación
Descripción:			
El usuario puede administrar y exportar a Excel o Pdf el historial de navegación de los usuarios de la máquina.			
Condiciones de Ejecución:			
El usuario de Windows debe contar con permisos de administrador en el navegador.			
Entradas/Pasos de Ejecución:			
El usuario: Puede ingresar a la ventana de Historial de Safe Browser de 3 maneras: 1. Clic en el ícono “Administrar Navegador” y dar clic en botón “Historial”. 2. Clic en el ícono “Menú”, ir a la opción “Historial y reportes” y seleccionar la opción “Historial” 3. Presionar simultáneamente las teclas “Control” y “H”			

Ingresa a todas las opciones de la aplicación. Opción 1 (Generar historial general): Seleccionar un usuario de la lista en el control. Seleccione la opción “Informe general de historial”. Opción 2 (Generar historial por rango de fechas): Seleccionar un usuario de la lista en el control. Seleccione la opción “Informe personalizado de historial”. Seleccionar una fecha de inicio y una fecha de cierre. Clic en el botón “Generar”. Opción 3 (Eliminar elemento de la lista): Seleccionar una pestaña de historial. Seleccionar un elemento de la lista del historial. Clic en el botón “Eliminar Url”. Opción 4 (Eliminar pestaña): Seleccionar una pestaña de historial. Clic en el botón “Eliminar Historial”. Opción 5 (Eliminar Historial Completo): Clic en el botón “Borrar Historial Completo” Opción 6 (Exportar a Pdf): Seleccionar una pestaña de historial. Clic en el botón “PDF”. Opción 7 (Exportar a Excel): Seleccionar una pestaña de historial. Clic en el botón “EXC”
Resultado Esperado:
Opción 1 (Generar historial general): Se verifica que se muestran en pestañas los historiales de las tres últimas fechas disponibles del usuario seleccionado Opción 2 (Generar historial por rango de fechas): Se verifica que se muestra en una pestaña todas las páginas navegadas del usuario seleccionado que estén dentro del rango de fechas establecido.

Opción 3 (Eliminar elemento de la lista): Se verifica que el elemento eliminado ya no conste en la lista de la pestaña de navegación seleccionada. Opción 4 (Eliminar pestaña): Se verifica que todos los elementos de la pestaña seleccionada no consten en el historial. Opción 5 (Eliminar Historial Completo): Se verifica que no existan datos de historial en el navegador. Opción 6 (Exportar a Pdf): Se verifica que se genere un archivo Pdf con los elementos de la pestaña de navegación seleccionada. Opción 7 (Exportar a Excel): Se verifica que se genere un archivo de Excel con los elementos de la pestaña de navegación seleccionada.

Evaluación de la Prueba:	**Satisfactoria**

Tabla 49 Prueba de aceptación - Historial de navegación

PRUEBAS DE ACEPTACIÓN			
Código:	12	**Nombre:**	Reportes de Navegación
Descripción:			
El usuario puede administrar y exportar a Excel o Pdf los reportes de navegación de los usuarios de la máquina.			
Condiciones de Ejecución:			
El usuario de Windows debe contar con permisos de administrador en el navegador.			
Entradas/Pasos de Ejecución:			
El usuario: Puede ingresar a la ventana de Reportes de Safe Browser de 3 maneras: 1. Clic en el botón “Ir a Reportes” desde la venta de Historial.			

2. Clic en el ícono “Menú”, ir a la opción “Historial y reportes” y seleccionar la opción “Reportes”
3. Presionar simultáneamente las teclas “Control” y “R”

Ingresa a todas las opciones de la aplicación.

Opción 1 (Reporte de Páginas navegadas):

Seleccione un usuario de la lista en el control.

Seleccione la opción 1 en el tipo de reportes a generar.

Opción 2 (Reporte Resumido de Redes Sociales):

Seleccione un usuario de la lista en el control.

Seleccione la opción 2 en el tipo de reportes a generar.

Opción 3 (Reporte Detallado de Redes Sociales):

Seleccione un usuario de la lista en el control.

Seleccione la opción 3 en el tipo de reportes a generar.

Opción 4 (Reporte de Navegación de Proxys):

Seleccione un usuario de la lista en el control.

Seleccione la opción 4 en el tipo de reportes a generar.

Opción 5 (Reporte de Navegación de Página para adultos:

Seleccione un usuario de la lista en el control.

Seleccione la opción 5 en el tipo de reportes a generar.

Opción 6 (Reporte por Rango de Fechas):

Seleccione un usuario de la lista en el control.

Seleccione uno de los tipos de reportes antes mencionados.

Marque la opción “Reporte personalizado de navegación”.

Seleccione una fecha de inicio y de cierre del reporte.

Clic en el botón “Generar”

Opción 7 (Exportar a Pdf):

Seleccione la pestaña de reporte que desea exportar.

Clic en el botón “PDF”

Opción 8 (Exportar a Excel):

Seleccione la pestaña de reporte que desea exportar.

Clic en el botón ”EXC”

Resultado Esperado:

Opción 1 (Reporte de Páginas navegadas):

Se verifica que se muestra un reporte de las páginas navegadas y el número de visitas realizadas en el día; correspondiente al usuario seleccionado de las últimas tres fechas disponibles.

Opción 2 (Reporte Resumido de Redes Sociales):

Se verifica que se muestra un reporte de navegación a redes sociales con: el número de visitas realizadas, y el promedio de horas navegadas en el día; correspondiente al usuario seleccionado de las últimas tres fechas disponibles.

Opción 3 (Reporte Detallado de Redes Sociales):

Se verifica que se muestra un reporte de las de navegación a redes sociales con: la hora en que se inició y finalizó la navegación, y el promedio de horas y minutos que se navegó en ese lapso de tiempo del día; correspondiente al usuario seleccionado de las últimas tres fechas disponibles.

Opción 4 (Reporte de Navegación de Proxys):

Se verifica que se muestra un reporte con la hora y la url del proxy navegado durante el día; correspondiente al usuario seleccionado de las últimas tres fechas disponibles.

Opción 5 (Reporte de Navegación de Página para adultos:

Se verifica que se muestra un reporte con la hora y la url del sitio para adultos navegado durante el día; correspondiente al usuario seleccionado de las últimas tres fechas disponibles

Opción 6 (Reporte por Rango de Fechas):

Se verifica que se muestra un reporte del tipo seleccionado, mostrando todos los elementos que se encuentren dentro del rango de fechas establecido; correspondiente al usuario seleccionado.

Opción 7 (Exportar a Pdf):

Se verifica que se genere un archivo Pdf con los elementos de la pestaña de reporte seleccionada.

Opción 8 (Exportar a Excel):

	Se verifica que se genere un archivo de Excel con los elementos de la pestaña de reporte seleccionada.
Evaluación de la Prueba:	**Satisfactoria**

Tabla 50 Prueba de aceptación - Reportes de navegación

Análisis: Los diferentes escenarios y las pruebas realizadas a la aplicación permiten evidenciar un correcto desempeño del navegador Safe Browser basados en que los resultados obtenidos en este proceso de pruebas de aceptación fueron satisfactorios

Requerimientos para implementación

El objetivo de esta sección es describir todos los recursos y requerimientos identificados que son indispensables para la correcta implementación e instalación del navegador Safe Browser en los equipos del laboratorio informático del Colegio Mixto Particular Innova.

A continuación se procede a describir de manera sencilla y detallada los requisitos de hardware, software y de usuario necesarios previo al proceso de implementación.

Requerimientos de Hardware y Software

Se describen los requerimientos mínimos con los que deben contar los equipos del laboratorio informático para la instalación de Safe Browser:

- Sistema Operativo Windows 7 o superior, de preferencia de 64 bits.
- 2 GB de Memoria RAM
- 500 GB de Disco Duro
- NetFramework 4.5
- Microsoft Visual C++ 2010, 2012, 2013 Redistributable x86 (32 bits)

Estas características garantizan un funcionamiento óptimo del navegador.

Requerimientos de Usuario

Cada equipo en el que se instale el navegador Safe Browser, debe contar con 2 usuarios de windows como mínimo. Uno de estos usuarios debe contar con permisos de administrador protegido con contraseña, mientras que los otros usuarios deben contar con permisos superiores al del usuario invitado, puesto que los usuarios con perfil invitado en el sistema operativo windows impiden la lectura y escritura de los datos de la base SQLite.

La instalación del aplicativo debe realizarse desde la sesión de un usuario administrador protegido con contraseña del equipo.

Resultados de encuesta y validación de hipótesis

En el presente estudio de investigación se utilizó la encuesta como el instrumento por medio del cual se procedió a la recolección de datos e información respecto a la validación y funcionalidad del navegador Safe Browser. Para ello, se elaboró un cuestionario de diez preguntas que van dirigidas a los estudiantes y personal administrativo del Colegio Mixto Particular Innova involucrados en el estudio.

La encuesta se realizó de forma virtual en los laboratorios de la institución bajo el aval y supervisión de los profesores encargados de la clase y la colaboración del personal administrativo. Esta tarea se llevó a cabo durante el periodo de una semana. Para este proceso se utilizó la herramienta de formularios de Google.

Una vez terminado el proceso de la encuesta, se introduce los datos en una hoja de cálculo para tabular los datos y obtener los cuadros estadísticos y porcentajes de las respuestas obtenidas para su posterior análisis e interpretación.

Para determinar los resultados de la encuesta, se elaboraron preguntas estratégicas que permiten determinar la validez y funcionalidad del navegador Safe Browser, luego de su implementación.

Cuadros y gráficos de los resultados de la encuesta.

Cada una de las diez preguntada planteadas se representa por medio de cuadros de datos, donde se registran los resultados, y se obtiene información relevante tal como la frecuencia, el porcentaje que representa y un gráfico estadístico para su comprensión.

1. ¿Le gustaría utilizar otros navegadores que no sean Google Chrome, Internet Explorer o Firefox?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	No	137	40,4	40,4
2	Si	202	59,6	100
	Total	339	100	

Tabla 51 Disponibilidad de uso de otros navegadores

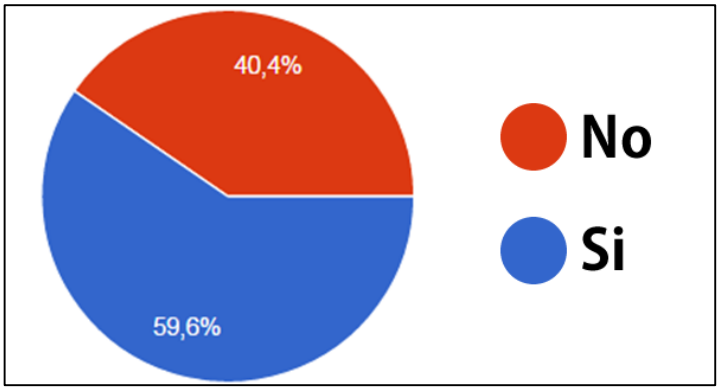

Figura 30 Disponibilidad de uso de otros navegadores

El 59,6% de los encuestados están abiertos a la posibilidad de usar otros navegadores diferentes a Google Chrome, Mozilla Firefox, entre otros. El otro 40,4% no está de acuerdo en utilizar un navegador diferente.

Estos datos permiten conocer la disponibilidad de los usuarios en el uso de herramientas diferentes a las ya conocidas, con ello se estima si una herramienta novedosa tendrá acogida entre los usuarios. Como se puede observar en el resultado,

la mayoría de los encuestados no tienen problema con utilizar un navegador diferente a los que existen en el mercado.

2. ¿Está usted de acuerdo con el uso de una herramienta que restrinja el acceso a sitios en internet con contenido malicioso (spam, virus, etc)?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Muy de acuerdo	184	54,28	54,28
2	De acuerdo	123	36,28	90,56
3	En desacuerdo	23	6,78	97,35
4	Muy en desacuerdo	9	2,65	100
	Total	339	100	

Tabla 52 Uso de herramientas de restricción a Internet

Figura 31 Uso de herramientas de restricción a Internet

El 54,28% de los encuestados indicaron que están de muy de acuerdo con el uso de herramientas que restrinjan el acceso a sitios de internet con contenido malicioso, un 36,28% dice estar de acuerdo, el 6,78% no está de acuerdo, mientras que el 2,65% se rehúsa a esta medida.

El uso de herramientas de control en internet es importante al momento de navegar por la web, ya que garantizan la integridad lógica del equipo y la pérdida de información.

3. ¿Durante el uso del programa Safe Browser, pudo usted utilizar alguno de estos navegadores?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Google Chrome	2	0,59	0,59
2	Mozilla Firefox	0	0,00	0,59
3	Internet Explorer	3	0,88	1,47
4	Opera	0	0,00	1,47
5	Safari	0	0,00	1,47
6	Ninguno de los Anteriores	335	98,53	100
	Total	340	100	

Tabla 53 Uso de otros navegadores

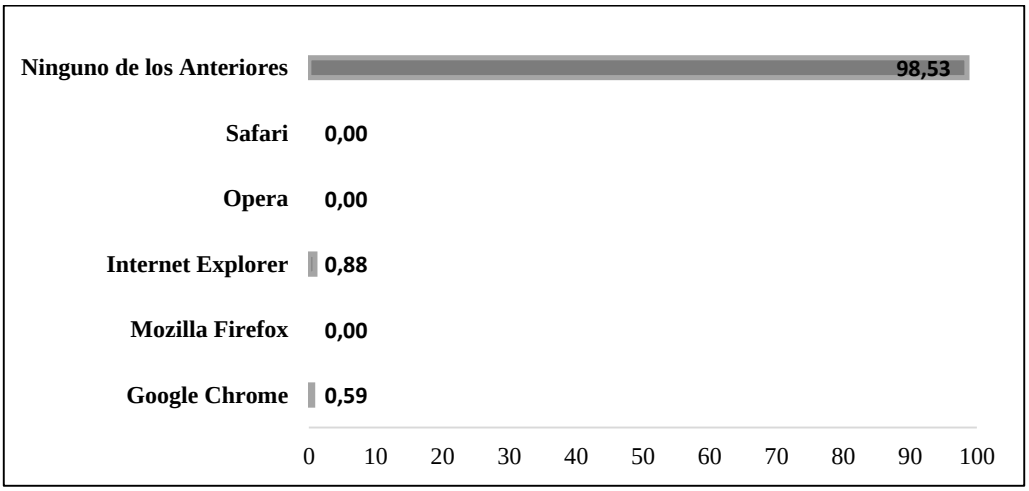

Figura 32 Uso de otros navegadores

El 98,53% de los encuestados manifestó que no tuvo acceso a ninguno de los navegadores mencionados en la pregunta de la encuesta, así mismo el 0,88% dijo tener acceso al navegador Internet Explorer y un 0,59% a Google Chrome.

La restricción de acceso a internet por medio de otros navegadores es un factor que ayuda a determinar la eficiencia del proyecto, puesto que esta restricción garantiza que los controles establecidos en el navegador Safe Browser no sean vulnerados a través del uso de otros navegadores. Los resultados obtenidos muestran que la

funcionalidad de la aplicación en este aspecto es excelente, dado que la mayoría de los encuestados no tuvieron acceso a otros navegadores instalados en el equipo.

4. ¿Durante el uso del navegador Safe Browser pudo usted acceder a alguno de estos sitios de redes sociales?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Facebook	27	7,83	7,83
2	Twitter	4	1,16	8,99
3	Google +	1	0,29	9,28
4	Instagram	1	0,29	9,57
5	No, la aplicación no permitía el acceso	312	90,43	100
	Total	345	100	

Tabla 54 Acceso a redes sociales

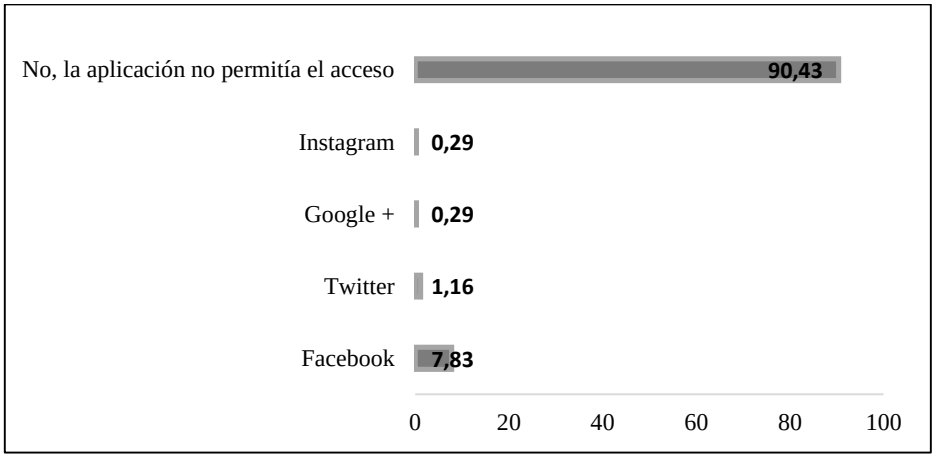

Figura 33 Acceso a redes sociales

El 90,43% de los encuestados manifestaron que no pudieron acceder a ninguna red social, debido a que Safe Browser lo impedía. El control de acceso a redes sociales por parte de los usuarios, es una de las características principales del navegador Safe Browser, por lo tanto conocer si los usuarios tuvieron acceso a internet por medio de los navegadores es un parámetro útil para valorar la funcionalidad de la aplicación.

Los resultados de la encuesta muestran que la aplicación no presenta inconvenientes en el control de acceso a redes sociales, ya que las respuestas obtenidas fueron positivas respecto a la restricción de acceder a redes sociales mediante el navegador Safe Browser. Sin embargo, existe un pequeño porcentaje que indica que los usuarios tuvieron acceso a estos sitios, esto debido a que durante la primera semana de prueba de Safe Browser, el control parental y de contenidos estaba inactivo.

5. Durante el uso del navegador Safe Browser, ¿Se presentaron errores en la aplicación? Indique cuales.

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	La aplicación no se ejecutaba	6	1,69	1,69
2	Algunas páginas no cargaban	30	8,45	10,14
3	La aplicación no respondía	23	6,48	16,62
4	La aplicación se cerraba inesperadamente	14	3,94	20,56
5	La aplicación funcionaba correctamente	282	79,44	100,00
	Total	355	100	

Tabla 55 Errores en la aplicación Safe Browser

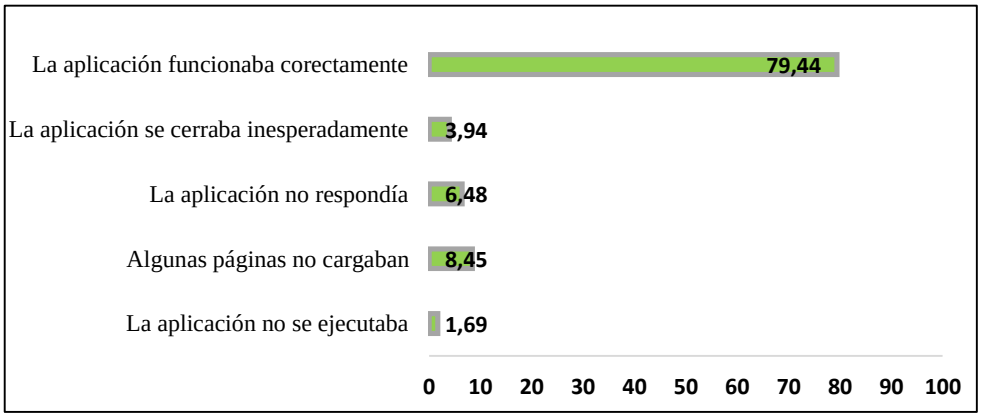

Figura 34 Errores en la aplicación Safe Browser

De los resultados obtenidos en la encuesta, el 1,69% de los encuestados respondieron que uno de los principales inconvenientes del navegador Safe Browser fue que la aplicación no se ejecutaba al momento de dar clic en el ícono del programa, otro 6,48% indicó que la aplicación se colgaba, es decir, había momentos en que esta no respondía, el 3,98% manifestó que Safe Browser se cerraba inesperadamente durante su uso, otro 8,45% expresó que algunas páginas no cargaron durante la navegación en internet, y el 79,44% de los encuestados dijeron que la aplicación funcionaba correctamente.

Conocer los errores de ejecución del proyecto permitió mejorar y optimizar las funcionalidades de los procesos del navegador Safe Browser, aun cuando el proyecto no presente ningún problema durante el período de pruebas previo a la fase de implementación.

El funcionamiento de la aplicación en un ambiente real generó escenarios que no fueron contemplados durante la fase de diseño y desarrollo, lo cual permitió mejorar y corregir estos errores.

6. Durante el uso del navegador Safe Browser, indique cuáles de los siguientes archivos presentaron inconvenientes de acceso o navegación:

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Imágenes	19	4,88	4,88
2	Documentos de Office	7	1,80	6,68
3	Archivos Pdf	22	5,66	12,34
4	Archivos de audio	26	6,68	19,02
5	Video	54	13,88	32,90
6	Ninguno de los Anteriores	261	67,10	100
	Total	389	100	

Tabla 56 Inconvenientes en archivos multimedia

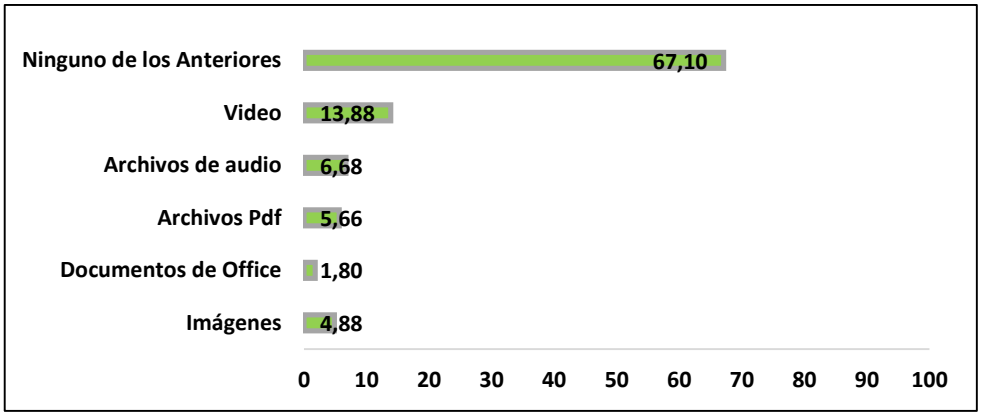

Figura 35 Inconvenientes en archivos multimedia

El 13,88% de los encuestados manifestaron que el navegador Safe Browser presenta problemas al reproducir videos en línea, el 6,68% indicó que hubo problemas con los archivos de audio, el 5,66%, el 4,88% y el 1,80% representan los problemas suscitados con los archivos Pdf, imágenes y documentos de office respectivamente.

Por otro lado, el 67,10% de los encuestados respondieron que el proyecto no presenta inconvenientes al momento de acceder a archivos multimedia en la web.
El acceso y el control de los archivos multimedia son parte de la funcionalidad de todo navegador, por lo que conocer los problemas suscitados con este tipo de archivos, sirvió para determinar su funcionamiento y corregir posibles errores.

7. ¿Qué problemas tuvo usted para manejar el navegador Safe Browser?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	No hay armonía en los colores	13	3,35	3,35
2	Los ícono no son los apropiados	12	3,09	6,44
3	Las opciones del navegador son confusas	35	9,02	15,46
4	Se presentan errores de ortografía	2	0,52	15,98
5	Las funciones de los botones no son claras	23	5,93	21,91
6	La ubicación de los botones y menús no es la adecuada	39	10,05	31,96
7	La aplicación es fácil de manejar	264	68,04	100,00
	Total	388	100	

Tabla 57 Dificultad para manejar la aplicación Safe Browser

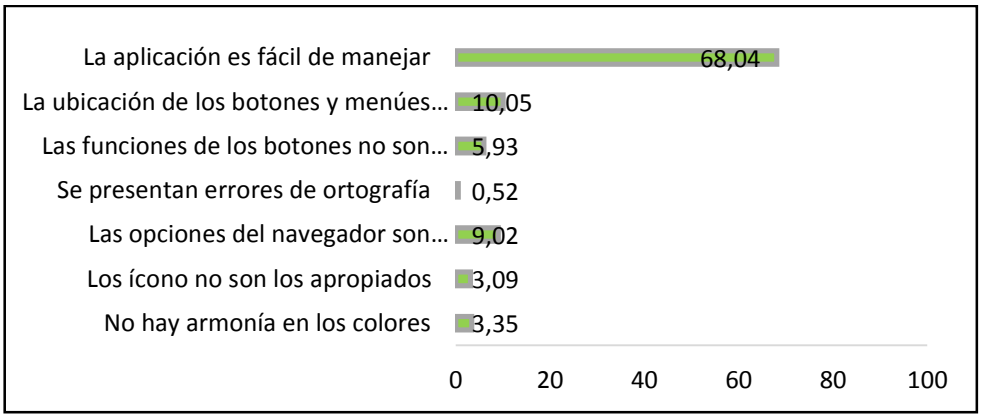

Figura 36 Dificultad para manejar la aplicación Safe Browser

El 10,05% de los encuestados indicaron que la ubicación de los botones y menús no es adecuada dentro de la interfaz de usuario de navegador Safe Browser, el 9,02% puso de manifiesto que las opciones de Safe Browser son confusas, el 3,09 y el 3,35% indicaron que los íconos de la interfaz gráfica no son apropiados y que no hay armonía en los colores, el 5,93% respondió que hay errores de ortografía en la aplicación, y otro 5,93 manifestó que las funciones de los botones de la interfaz del navegador no son claras. Por último, el 68,04% de los usuarios está de acuerdo en que la aplicación es fácil de usar.

Una interfaz intuitiva y fácil de usar es un factor primordial para el éxito del navegador, conocer la satisfacción del usuario permite validar los parámetros de diseño e identificar y corregir los problemas que se presenten. Según los resultados obtenidos, en general, el manejo de la aplicación Safe Browser es fácil e intuitiva para el usuario.

8. ¿El navegador Safe Browser le permite llevar a cabo las tareas que se realizan en clases?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Si	293	86,43	86,43
2	No	46	13,57	100
	Total	339	100	

Tabla 58 Uso de Safe Browser en tareas de clase

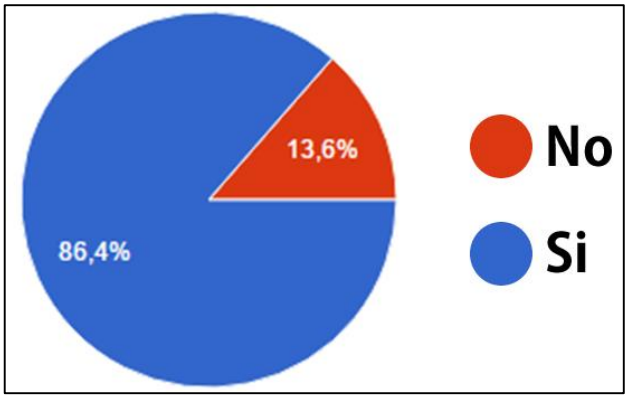

Figura 37 Uso de Safe Browser en tareas de clase

El 86,4% de los encuestados manifestó que no tuvieron problemas para realizar las tareas de clase usando el navegador Safe Browser, mientras que el 13% indicó que si se presentaron problemas durante su uso.

El navegador Safe Browser, es de utilidad para el maestro y el estudiante dentro del aula de clases, conocer si los estudiantes pudieron llevar a cabo con normalidad sus actividades en el laboratorio de informática sirve para validar la funcionalidad de la aplicación.

Los resultados obtenidos de la encuesta son totalmente positivos, ya que la mayoría de los encuestados indicaron no tener problemas con el navegador al momento de realizar sus tareas en la clase, especialmente en la ejecución de código HTML.

9. ¿Cómo calificaría usted la funcionalidad del navegador Safe Browser?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Muy bueno	128	37,76	37,76
2	Bueno	160	47,20	84,96
3	Malo	42	12,39	97,35
4	Muy malo	9	2,65	100
	Total	339	100	

Tabla 59 Funcionalidad del navegador Safe Browser

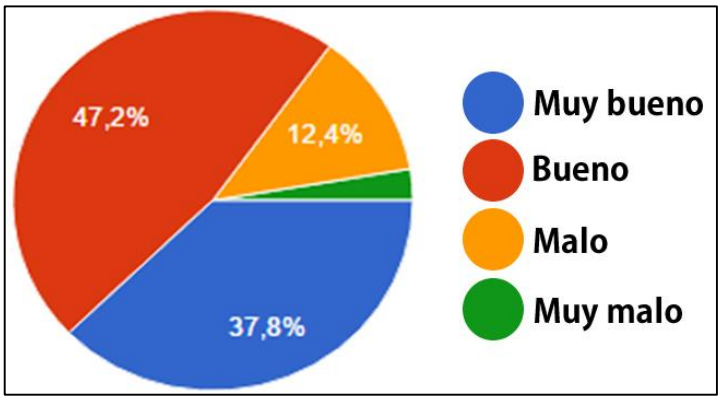

Figura 38 Funcionalidad del navegador Safe Browser

Aproximadamente, el 85% de los encuestados manifestaron que la funcionalidad del navegador Safe Browser es buena, el 12,4% y el 2,65% de los usuarios calificaron como malo y muy malo a la aplicación.

De los resultados obtenidos, se destaca que la mayoría de los usuarios califica como bueno y muy bueno al navegador Safe Browser, es decir, el nivel de aceptación de la aplicación en relación a su desempeño y rendimiento es positivo.

10. ¿Recomendaría el uso del navegador Safe Browser a otras personas?

N°	Detalle	Frecuencia	Porcentaje %	Porcentaje acumulado %
1	Si	253	74,63	74,63
2	No	86	25,37	100
	Total	339	100	

Tabla 60 Recomendación de uso de Safe Browser

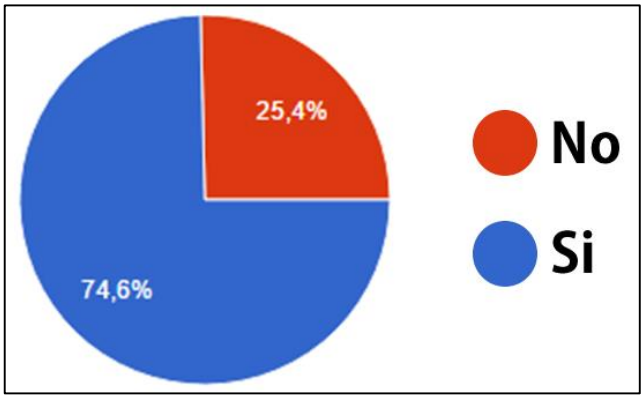

Figura 39 Recomendación de uso de Safe Browser

El 74,63% de los usuarios respondieron que si recomiendan el uso de la herramienta Safe Browser a otras personas, y el 25,4% indicó que no recomendaría el uso del navegador. Conocer si los usuarios recomendarían o no el uso de Safe Browser a otras personas, sirve como parámetro para estimar el grado de aceptación general que tuvo el proyecto con los usuarios.

Validación de Hipótesis

Proceso de recolección de datos.

Para realizar este proceso previo al uso del navegador Safe Browser, se desarrolló un programa informático el cual permitía generar copias de seguridad de las bases de datos de los navegadores web utilizados en las máquinas de la institución donde se realizó el experimento, esto debido a que las computadoras tenían un sistema de seguridad con Deep Freeze el cuál elimina todos los archivos nuevos que se registre en el equipo al momento de apagarlo.

Para almacenar la copia de seguridad de la base de datos de los navegadores fue necesario utilizar la segunda partición lógica del disco duro, las cuales estaban configuradas para salvaguardar toda información que se desee mantener en la máquina, dicha información fue grabada mediante identificadores y clasificada por fechas para un mayor control, y también fueron ocultadas para evitar el acceso y manipulación de los datos por parte de usuarios no autorizados.

Posteriormente, durante el uso del navegador Safe Browser no fue necesario utilizar ningún programa adicional, debido a que la aplicación genera reportes históricos en formato Excel y Pdf de las url de navegación según un rango de fechas y por usuarios.

A continuación se describen los datos obtenidos:

Hipótesis 1

Controlar el uso del Internet no implicará cambios en el acceso de los adolescentes a contenidos en la web.

H_0: Controlar el uso del Internet no implicará cambios en el acceso de los adolescentes a contenidos en la web.

H_1: No controlar el uso del Internet no implicará cambios en el acceso de los adolescentes a contenidos en la web.

Aplicación de control en el uso de internet	**Número de accesos a contenidos en la web**				
	Redes sociales	**Pornografía**	**Proxy en línea**	**Descargas**	
Si (uso Safe Browser)	350	2	55	92	**499**
No (sin uso Safe Browser)	1232	7	0	46	**1285**
	1582	**9**	**55**	**138**	**1784**

Tabla 61 Aplicación de control en el uso de internet

Para la obtención de los valores de diferencia de proporciones entre ambas poblaciones se utilizan las siguientes formulas:

$$p = \frac{X1 + X2}{N1 + N2}$$

Donde:

P= proporción muestral.
X1= número de aciertos en la muestra 1.
X2= número de aciertos en la muestra 2.
N1= número de observaciones de la muestra 1.
N2= número de observaciones de la muestra 2.

Este valor de P se utiliza para calcular el valor estadísticos de prueba.

$$\boldsymbol{Z = \frac{\frac{X1}{N1} - \frac{X2}{N2}}{\sqrt{P(1-P) * (\frac{1}{N1} + \frac{1}{n2})}}}$$

Calculando la proporción muestral se obtiene:

$$P = \frac{X1 + X2}{N1 + N2} = \frac{(1285 + 499)}{1784 + 1784} = 0{,}5$$

Calculando Z se obtiene:

$$Z = \frac{\frac{X1}{N1} - \frac{X2}{N2}}{\sqrt{P(1-P) * (\frac{1}{N1} + \frac{1}{n2})}}$$

$$Z = \frac{\frac{1285}{1784} - \frac{499}{1784}}{\sqrt{0{,}5(1-0{,}5) * \left(\frac{1}{1784} + \frac{1}{1784}\right)}}$$

$$Z = \frac{0{,}72 - 0{,}28}{\sqrt{0{,}5(0{,}5) * (0{,}0005 + 0{,}0005)}}$$

$$Z = \frac{0{,}44}{\sqrt{0{,}25 * 0{,}001}}$$

$$Z = 27{,}5$$

Con un grado de aceptación del 5%, donde hay una aceptación del 1,96

Análisis.

El valor de la aceptación de la hipótesis es de 27,5 con un grado de confianza de 0,05 y una intercepción de grado de libertad de 1,96; donde la hipótesis nula (H_0) es rechazada por la independencia que existe en sus variables, mostrando que al existir un control en el uso de internet y el acceso a contenidos en la web la navegación se ve afectada.

Se concluyó que de los grupos observados se obtuvo un decremento del 78% en

relación al acceso a redes sociales y el acceso a páginas pornográficas durante el uso del navegador Safe Browser. También se evidenció un incremento de intentos por vulnerar la seguridad del navegador mediante el uso de proxys en línea, así como intentos de descargas de archivos multimedia.

Hipótesis 2

Existe independencia entre las edades de los adolescentes y el uso de las redes sociales.

H_0: Existe independencia entre las edades de los adolescentes y el uso de las redes sociales.

H_1: No existe independencia entre las edades de los adolescentes y el uso de las redes sociales.

Estudiantes por grupos de edades	**Número de accesos a redes sociales**				
	Facebook	**YouTube**	**Wattpad**	**Instagram**	
Grupo 1: estudiantes entre 11 y 13 años	36	127	0	0	**163**
Grupo 2: estudiantes entre 14 y 15 años	104	273	45	2	**424**
Grupo 3: estudiantes entre 16 y 18 años	132	133	9	1	**275**
	272	**533**	**54**	**3**	**862**

Tabla 62 Conteo de visitas a redes sociales por rango de edades

Para obtener el cálculo de las frecuencias de cada una de las celdas se las realizó con la siguiente fórmula:

$$e = \frac{(tmr)(tmc)}{tt}$$

Donde:

e= frecuencia esperada para una celda determinada.

Tmr= total marginal del reglón de dicha celda

Tmc= total marginal de la columna de la misma celda

Tt= total de tablas

Desarrollo de la fórmula:

Valores de celdas $\frac{(163)(272)}{862} = 51{,}43$ **Valores de celdas** $\frac{(424)(3)}{862} = 1{,}47$

Valores de celdas $\frac{(163)(533)}{862} = 100{,}78$ **Valores de celdas** $\frac{(275)(272)}{862} = 86{,}77$

Valores de celdas $\frac{(163)(54)}{862} = 10{,}21$ **Valores de celdas** $\frac{(163)(3)}{862} = 0{,}56$

Valores de celdas $\frac{(424)(272)}{862} = 133{,}79$ **Valores de celdas** $\frac{(275)(533)}{862} = 170{,}04$

Valores de celdas $\frac{(424)(533)}{862} = 262{,}17$ **Valores de celdas** $\frac{(275)(54)}{862} = 17{,}22$

Valores de celdas $\frac{(424)(54)}{862} = 26{,}56$ **Valores de celdas** $\frac{(275)(3)}{862} = 0.95$

Tabla de valores de contingencia

A continuación se presenta la siguiente tabla de los valores de contingencia:

51,43387	100,7877	10,21114	0,567285
133,7912	262,1717	26,56148	1,475638
86,77494	170,0406	17,22738	0,957077

Tabla 63 Valor de contingencia

Grados de libertad:

Fórmula: gl = (f.1) (c.1)

Desarrollo de fórmula: gl = (3 – 1) (4 – 1)

gl = (2) (3)

gl = 6

Nivel de confianza = 0,05

Para los valores de grado de libertad se describe la siguiente tabla, donde se puede visualizar el rango de probabilidad con un valor de confianza de 0,05.

Tabla de contingencia de valores de libertad

TABLA DE VALORES DE GRADO DE LIBERTAD					
Grados de libertad	**Probabilidad de un valor superior**				
	0,1	**0,05**	**0,025**	**0,01**	**0,005**
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,6
3	6,25	7,81	9,35	11,34	12,84
4	7,77	9,48	11,14	13,28	14,86
5	9,23	11,07	12,83	15,09	16,74
6	10,64	12,59	14,45	16,81	18,54

Tabla 64 Valores de grado de libertad

Valores de la intersección: 12,59

Fórmula de la chi-cuadrada

$$X^2 = \sum \frac{(0 - e)2}{e}$$

Donde:

$\sum$ = Suma de todas las expresiones.

0 = Valor de frecuencias

e = Frecuencia esperada

Desarrollo de la fórmula:

1.- $\frac{(36-51,43)^2}{51,43} = 4,63$

2.- $\frac{(127-100,78)^2}{100,78} = 6,82$

3.- $\frac{(0-10,21)^2}{10,21} = 10,21$

4.- $\frac{(0-0,56)^2}{0,56} = 0,56$

5.- $\frac{(104-133,79)^2}{133,79} = 6,63$

6.- $\frac{(273-262,17)^2}{262,17} = 0,44$

7.- $\frac{(45-26,56)^2}{26,56} = 12,79$

8.- $\frac{(2-1,47)^2}{1,47} = 0,18$

9.- $\frac{(132-86,77)^2}{86,77} = 23,57$

10.- $\frac{(133-170,04)^2}{170,04} = 8,06$

11.- $\frac{(9-17,22)^2}{17,22} = 3,92$

12.- $\frac{(1-0,95)^2}{0,95} = 0,001$

Suma de todos los valores obtenidos:

$X^2 = (4,63+6,81+10,21+0,56+6,63+0,44+12,79+0,18+23,57+8,06+3,92+0,001)$

$X^2 = 77,86$

Aplicación de chi-cuadrado con grados de libertad.

En la siguiente figura se puede visualizar una progresión lineal, la misma que representa los valores de aceptación de chi-cuadrado para la validación de la hipótesis con sus variables.

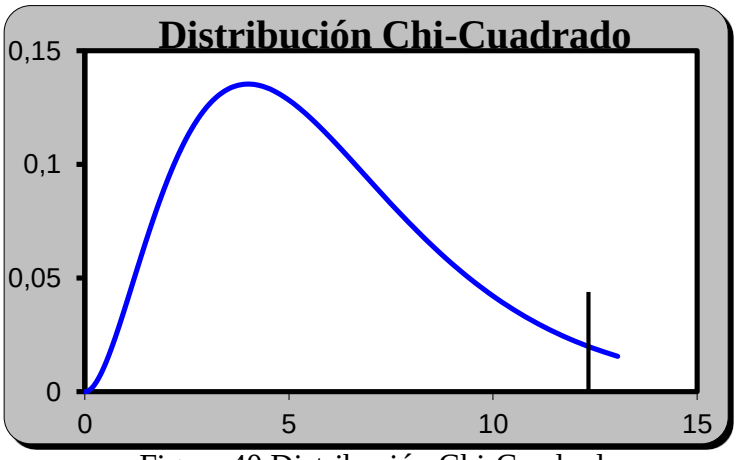

Figura 40 Distribución Chi-Cuadrado

Análisis.

El valor de la aceptación de la hipótesis es de 77,86 con un grado de confianza de 0,05 y una intercepción de grado de libertad de 12,59; donde la hipótesis nula (H0) es rechazada por la independencia que existe en sus variables, mostrando que no existe independencia entre las edades de los adolescentes y el uso de las redes sociales.

Se concluyó que todos los grupos observados indistintamente de su edad utilizan las redes sociales, sin embargo los estudiantes de entre 14 y 15 años son quienes más frecuentemente acceden a las redes sociales de Facebook y YouTube con una frecuencia de 424, seguidos de los estudiantes de entre 16 y 18 años con una frecuencia de 275 y por último los estudiantes de entre 11 y 13 con una frecuencia de 163.

Hipótesis 3

A mayor control en el uso de internet mayor es el número de saltos de seguridad que aplicarán los adolescentes.

H_0: A mayor control en el uso de internet, mayor es el número de saltos de seguridad que aplicarán los adolescentes.

H_1: A mayor control en el uso de internet, menor es el número de saltos de seguridad que aplicarán los adolescentes.

Análisis:

Se considera saltos de seguridad a los intentos de accesos a proxys en línea que efectúan los adolescentes para vulnerar los controles que restringen el ingreso a páginas no aptas para su edad. Como se observa en la tabla 61 el número de intentos de accesos a proxys en línea por parte de los adolescentes fue de 55 intentos durante

el uso del navegador Safe Browser; por lo cual, se acepta la hipótesis nula (H_0) concluyendo que si se aplican controles en el uso del internet, mayor será el número de saltos de seguridad que aplicarán los adolescentes.

Hipótesis 4

A más edad de los adolescentes mayor es el acceso a contenidos no aptos para su edad.

H_0: A más edad de los adolescentes, mayor es el acceso a contenidos no aptos para su edad.

H_1: A más edad de los adolescentes, menor es el acceso a contenidos no aptos

Estudiantes por grupos de edades	**Número de accesos a redes pornográficas sin parámetros de seguridad**	**Número de intentos de accesos a redes pornográficas bajo parámetros de seguridad**
Grupo 1: estudiantes entre 11 y 13 años	0	0
Grupo 2: estudiantes entre 14 y 15 años	2	0
Grupo 3: estudiantes entre 16 y 18 años	5	2
	7	**2**

Tabla 65 Número de accesos a redes pornográficas

Análisis:

Como se observa en la tabla anterior; el grupo 3 que corresponde a adolescentes con más edad son quienes acceden con más frecuencia a este tipo de contenidos, por lo que, se acepta la hipótesis nula.

CONCLUSIONES

- Safe Browser implementa seis controles de seguridad, los cuales permiten establecer horarios de navegación a redes sociales o descargas de archivos, restringir acceso a páginas específicas, deshabilitar la apertura de ventanas emergentes, bloquear software gestores de descargas y restringir acceso a páginas o búsqueda de información con contenido pornográfico.

- Mientras más controles de seguridad se habilitan en Safe Browser, mayor es el número de saltos de seguridad que intentan ejecutar los adolescentes para vulnerar dichas seguridades.

- Durante el estudio se pudo observar que cuando no existen controles de seguridad en los contenidos que son accedidos a través de internet, los adolescentes a partir de los 15 años, son quienes consumen más información con contenido pornográfico.

- En general, todos los adolescentes prefieren utilizar la red social YouTube que Facebook, siendo los estudiantes entre 14 y 15 años quienes la utilizan con más frecuencia.

- De acuerdo a los resultados obtenidos en el estudio, el 91% de los usuarios dijeron que estaban de acuerdo en utilizar una herramienta que restringa el acceso a sitios en internet con contenido malicioso.

- El 98,53% de los usuarios encuestados confirmaron que durante el uso del navegador Safe Browser no tuvieron accesos a otros navegadores web instalados en el computador, validando la efectividad de los controles de seguridad que implementa el navegador en relación a otros navegadores convencionales.

- Tener un manual de instalación es una ayuda para los diversos usuarios u entidades ya que permite entender y conocer las diversas herramientas que proporciona Safe Browser.

RECOMENDACIONES

- Para futuras versiones de Safe Browser se debe migrar el proyecto para que sea soportado en diversos sistemas operativos y dispositivos electrónicos.

- Habilitar el mayor número de controles posibles en Safe Browser para disminuir los riesgos a los cuales podrían estar expuestos los adolescentes durante el uso de internet.

- Agregar nuevos controles de seguridad en el navegador Safe Browser, que permitan bloquear o deshabilitar el uso de hardware del equipo, tales como, cámaras web, micrófonos, y altavoces.

- Identificar nuevos sitios webs que ofrezcan proxys en línea para que sean agregados a la base de datos de Safe Browser y evitar su uso.

- La Institución debe generar campañas informativas que concientice a los estudiantes y padres de familia sobre los riesgos que existen en internet y a los cuales podrían estar expuestos los adolescentes.

- Para mejores resultados de aprendizaje y entendimiento de la herramienta Safe Browser, a futuro realizar videos tutoriales sobre las diversas opciones que proporciona el navegador.

BIBLIOGRAFÍA

- Arcila, J. C. (s.f.). Precaucion: niños y redes sociales. Obtenido de Sura: http://www.sura.com/blogs/calidad-de-vida/ninos-redes-sociales.aspx
- Arias, F. (1999). EL proyecto de investigación. Caracas: Episteme.
- Arias, F. (1999). El Proyecto de Investigación: Guía para su elaboración. Caracas, Venezuela: Episteme.
- Congreso, N. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
- Date, C. (2001). Introducción a los Sistemas de base de datos. 7th Edición. México.: Pearson Educación.
- Dr. Morduchowicz, R., Lic. Marcon, A., Lic. Sylvestre, V., & Ballestrini, F. (Septiembre de 2010). Me. (Los adolescentes y las redes sociales) Recuperado el 10 de Mayo de 2016, http://www.me.gov.ar/escuelaymedios/material/redes.Pdf
- Duart, J. M. (11 de Mayo de 2016). Internet y aprendizaje: Una estrecha relacion. Obtenido de Revista de Universidad y Sociedad del Conocimiento.: http://www.uoc.edu/rusc/3/2/esp/editorial.html
- Fidias, A. (2006). El proyecto de investigación: Introducción a la metodología científica. En A. Fidias, El proyecto de investigación: Introducción a la metodología científica. (pág. 134). Caracas, Venezuela: Episteme.
- Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Network: Threats and Solutions. Obtenido de IEEE Xplore: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6809839
- Guia infantil. (s.f.). (Los riesgos de Internet y las redes sociales para los niños) Recuperado el 10 de Mayo de 2016, de http://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/internet-y-las-redes-sociales-riesgos-para-los-ninos/
- Ochoa, C. (16 de Abril de 2015). Muestreo probabilistico: muestreo estratificado. http://www.netquest.com/blog/es/muestreo-probabilistico-muestreo-estratificado/

- Palella, S., & Martins, F. (2010). Metodología de Ingestigación cuantitativa. Caracas.: Fedupel.
- Sabino, C. (1984). El proceso de Investigación . Buenos Aires, Argentina: Panapo.
- Sampier, R. H. (2004). Metodologia de la investigación. La Habana: Editorial Felix Varela.
- Tamayo y Tamayo, M. (1997). El proceso de la investigación científica. Mexico: Editorial Limusa S.A.
- Tamayo y Tamayo, M. (s.f.). Tipos de investigación.
- Universo, D. E. (18 de Diciembre de 2014). El Universo. (Mal uso de las redes sociales afecta a niños y adolescentes) Recuperado el 10 de Mayo de 2016, http://www.eluniverso.com/noticias/2014/12/18/nota/4354351/mal-uso-redes-sociales-afecta-ninos-adolescentes