UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Cristhian Joel Guanin Mackencie.

Alex Fernando Aguirre Pantoja.

Marco Vinicio Ortiz Barrera.

TUTOR: Alejandro Cortés Msc.

Sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad

QUITO – ECUADOR | 2023

APROBACIÓN DEL TUTOR

Yo, NOMBRE TUTOR, certifico que conozco los autores del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

_____

Nombre Tutor

DIRECTOR DE TESIS

DECLARATORIA DE AUTORÍA

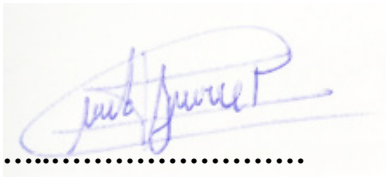
Nosotros, **CRISTHIAN JOEL GUANIN MACKENCIE, ALEX FERNANDO AGUIRRE PANTOJA, MARCO VINICIO ORTIZ BARRERA**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

……

CRISTHIAN JOEL GUANIN MACKENCIE

C.I.: 1206398255



……

ALEX FERNANDO AGUIRRE PANTOJA.

C.I.: 0401180021

……

MARCO VINICIO ORTIZ BARRERA

C.I.: 1720139029

DEDICATORIA

Dedico este trabajo a mis padres Marcelo y Mónica por el apoyo incondicional y sacrificio hicieron posible que hoy culmine esta etapa de mi vida. A mis profesores, por su inspiración y orientación constante a lo largo de este viaje académico. A mis abuelos Segundo y Cumanda, hermanos Pablo y Valentina, que siempre estuvieron ahí para animarme en los momentos difíciles. A todos aquellos que de una u otra manera contribuyeron a la realización de esta tesis, ¡gracias!

Cristhian.

A mis padres Alfonso y Ana María, por cada muestra de amor incondicional y apoyo en mi formación, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

El apoyo incondicional de mi hermana Diana y en especial a mi novia Mary que, durante todo este proceso, por estar conmigo en todo momento de una u otra forma me acompaña en todos mis sueños y metas.

Alex.

Dedico este trabajo de titulación a mis queridos Padres: José y Ligia por su amor, preocupación y apoyo incondicional, son mi ejemplo y admiración en el transcurso de mi vida sobre todo el temple que han tenido conmigo.

A mi amada esposa Marcela por su amor, tiempo, dedicación y por sobre todo la consideración que ha tenido conmigo, a mi querido hijo: Mathias, que con sus travesuras y ocurrencias alegra al más oscuro de los días.

Marco.

AGRADECIMIENTO

Deseamos expresar nuestro agradecimiento a todas las personas que contribuyeron de manera significativa a la realización de este trabajo de titulación. Agradecemos a los profesores, asesores, por sus valiosas contribuciones, críticas constructivas y por brindarnos la oportunidad de aprender y crecer como estudiantes e investigadores. Nuestra gratitud se extiende hacia los compañeros de grupo final, por su colaboración, intercambio de ideas y por hacer que este proceso sea más enriquecedor. Agradecemos a cada una de nuestras familias, en especial a nuestros padres, por su apoyo inquebrantable, comprensión y amor. Sin su respaldo emocional y financiero, esta tesis no habría sido posible y finalmente, agradezco a la UNIVERSIDAD INTERNACIONAL DEL ECUADOR por proporcionar recursos y facilidades que fueron esenciales para llevar a cabo este proyecto.

Cristhian Joel Guanin Mackencie.
Alex Fernando Aguirre Pantoja.
Marco Vinicio Ortiz Barrera.

RESUMEN

La creación de aplicaciones y sitios web con contenido malicioso van en incremento en una sociedad cada vez más globalizada por el uso del internet, sugiere una mayor atención en los dispositivos móviles que emplean menores de edad los mismos que están siendo presa fácil de engaños, amenazas o incluso de pedofilia por parte de personas inescrupulosas.

Encuestas a padres, adolescentes y administradores de redes revelaron que el control de acceso a la red es muy bajo y no puede garantizar la seguridad de los menores en línea, animando así a niños y adolescentes a utilizar la tecnología de forma irresponsable.

El presente proyecto tiene como objetivos: controlar el acceso hacia aplicaciones y sitios web de contenido inapropiado para menores de edad, restringiendo la navegación total en los dispositivos que traten de ingresar en estos sitios por otro lado también busca determinar la relación que existe entre el control parental percibido y el uso de internet por parte de los usuarios, para finalmente evaluar el uso de internet y las restricciones por edades en los usuarios.

Para validar se propone desarrollar una aplicación para dispositivos móviles, esta aplicación tendrá la posibilidad de enviar información en tiempo real hacia un usuario administrador el mismo que podrá restringir o permitir el acceso dependiendo de las edades y sitios web a visitar, finalmente que proporcione una data de los lugares que más acceso solicitan.

Palabras clave: Aplicación, control, internet, desarrollo.

ABSTRACT

The creation of applications and websites with malicious content is increasing in a society that is increasingly globalized using the Internet, suggesting greater attention to mobile devices used by minors who are falling easy prey to deception, threats. or even pedophilia by unscrupulous people.

Through surveys of parents, adolescents, and network administrators, it is identified that the percentage of control over Internet access is minimal and does not guarantee the safety of minors when they are online, thus promoting irresponsible use. of technology in children and adolescents up to 18 years of age.

The objectives of this project are to control access to applications and websites with inappropriate content for minors, restricting total navigation on devices that try to access these sites. On the other hand, it also seeks to determine the relationship that exists between the control perceived parental and internet use by users, to finally evaluate internet use and age restrictions in users.

To validate, an application will be developed for mobile devices. This application will have the possibility of sending information in real time to an administrator user who will be able to restrict or allow access depending on the ages and websites to visit. Finally, you provide us with data. of the places that are most requested for access.

Keywords: Application, control, internet, development.

Tabla de contenidos

Contenido

Lista de tablas

Lista de figuras

1. INTRODUCCIÓN

Las necesidades tecnológicas de la sociedad avanzan desmesuradamente en una carrera por lograr comunicaciones más rápidas y eficientes, el avance de la tecnología y el acceso a internet desde la mayoría de los lugares ha permitido que la humanidad tenga acceso a información de varios ámbitos: informativo, cultural, investigativo, deportivo, entretenimiento y ahora en auge las denominadas redes sociales.

Hoy en día, todo el mundo, especialmente la generación más joven, corre el riesgo de verse expuesto a información inapropiada como pornografía, violencia abierta, terrorismo, etc. También puede generar adicción o dependencia de las tendencias actuales como las redes sociales. Los peligros que representan en línea los niños y adolescentes menores de 18 años han llevado a empresas y organizaciones de todo el mundo a adoptar leyes, políticas, estándares y procedimientos en un esfuerzo por regular y controlar el abuso en línea.

Al revisar el pretérito de nuestros familiares podemos darnos cuenta de que vivimos en una era que era posible únicamente en películas de ciencia ficción, sin embargo, nunca estuvimos preparados para toda la tecnología que hoy en día tenemos al alcance de nuestras manos.

El uso de Internet aporta muchos beneficios a la educación y comunicación de los menores, puede utilizarse como una herramienta de aprendizaje divertida, un enfoque informativo o como una variedad de entretenimiento. Sin embargo, por otro lado, la gestión de las TIC no se gestiona adecuadamente, los padres y educadores no brindan el apoyo educativo adecuado a los menores y el acceso a contenidos nocivos en Internet está aumentando. Las oportunidades de estar expuestos a diversos peligros en la red también han aumentado significativamente.

Por tanto, teniendo en cuenta las necesidades de la sociedad actual y en virtud de precautelar la integridad de niños y menores de 18 de años se decidió proponer el desarrollo de un "Sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad", lo cual hará posible optimizar el uso del servicio de Internet para actividades productivas, educativas, culturales, investigativas y su vez precautelar la integridad de los menores al momento que se conecten desde

sus diferentes dispositivos móviles para que no sean blanco de engaños, extorciones y sobre todo de grooming.

Este proyecto consta de IV capítulos. El Capítulo I introduce el tema y explica: la necesidad para el desarrollo del proyecto, los problemas actuales relacionados con el control parental y el acceso a Internet, los tipos de medios utilizados en los intentos de controlar el acceso a Internet y la terminología general utilizada en la información teórica contenida en el proyecto.

El Capítulo II realiza un estudio de viabilidad y describe los desafíos actuales para acceder a varios sitios web y la falta de control que existe.

El Capítulo III presenta los resultados de la propuesta, desagregando requerimientos por edad, educación y necesidades sociales. Se dan referencias técnicas y selección de unidades a utilizar. Define sitios de libre acceso y sitios con restricciones para usuarios y necesidades existentes.

En el capítulo IV se presentan los resultados de la simulación del Sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad, Se realizaron pruebas de funcionamiento en base a las máquinas virtuales con software de Raspberry PI 4 y con Android Estudio donde se demuestra la conectividad y la restricción de los equipos móviles en la red, para concluir con la propuesta del desarrollo del proyecto se muestran las conclusiones y sugerencias de la averiguación.

1.2 PLANTEAMIENTO DEL PROBLEMA /CASO DE ESTUDIO

Actualmente, las tecnologías de la información y la comunicación abarcan todos los ámbitos de la vida humana: biológico, psicológico y social. Así podemos decir que las tecnologías de la información y la comunicación intervienen e influyen en las relaciones interpersonales. Especialmente los usuarios más jóvenes que pueden acostumbrarse mejor a utilizar diferentes pantallas. Por lo tanto, sería importante que los adultos pudieran aprender todo lo relacionado con esta área de la tecnología para asegurar un adecuado apoyo, seguimiento y control.

En este contexto, sería interesante comprender la relación entre el control parental percibido y el uso de Internet en niños y jóvenes menores de 18 años.

No existen en el país controles para filtrar información de los lugares más vulnerables, como son en el hogar, en las escuelas y en los sitios web públicos, de modo que el acceso a estos sitios está permitido a todas las personas independientemente de su edad y que puedan contener información inapropiada, afectando especialmente a los más jóvenes.

Los padres pueden reducir el riesgo para los niños y adolescentes menores de 18 años utilizando herramientas de filtrado de información que sean fáciles de configurar y monitorear. Actualmente, existen de dos tipos: gratuitas y de pago, y en muchos casos su adquisición es elevada.

El presente proyecto tiene por objetivo apoyar al control parental con la propuesta de un Sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad, de manera moderna y sencilla controlar el acceso a sitios inapropiados o de contenido explicito, actualmente Internet influye mucho en la vida de los niños y adolescentes menores de 18 años, ya que pasan la mayor parte de su tiempo en Internet, lo que influye en su comportamiento y sus relaciones. Quizás porque la interacción entre pares es un factor tan importante en este grupo, varios dispositivos tecnológicos proporcionan los medios para facilitar esta interacción.

1.3 JUSTIFICACIÓN / PROBLEMA DE INVESTIGACIÓN

Este proyecto aborda el problema existente de las amenazas en línea, ya que los niños y adolescentes menores de 18 años corren mayor riesgo al navegar por la web. Los menores de 18 años dependen del acceso irrestricto a Internet porque no existen herramientas informáticas adecuadas para controlar el acceso a sitios web que contienen contenido inapropiado y deben restringirse a menores y sufren de aislamiento social, depresión, ansiedad y en casos extremos el suicidio.

Por lo que se propone un Sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad, de esta manera optimizar el acceso al servicio de Internet y brindar un mayor control de los sitios a los que acceden las personas menores de 18 años, evitando de esta manera que

se produzcan actos propios del ciberbullying que pueden afectar derechos como el honor, la integridad personal, la salud e incluso la libertad sexual.

1.4 OBJETIVO GENERAL

Proponer un sistema de supervisión y vigilancia para dispositivos móviles usados por menores de edad.

1.5 OBJETIVOS ESPECIFICOS

- Definir y evaluar herramientas informáticas de filtrado para equipos móviles.
- Investigar si existe una correlación entre la supervisión parental recibida y el uso de Internet por parte de los padres.
- Evaluar como las actividades y el uso de internet por medio de controles parentales varían de acuerdo con las edades.

1.6 MARCO CONCEPTUAL

1.6.1CONTROL PARENTAL

El control parental es un conjunto de herramientas y configuraciones que las personas adultas utilizan para controlar, bloquear, monitorear y establecer tiempos de acceso y el uso de internet en diferentes sitios como páginas web, redes sociales, juegos en línea que los menores de edad utilizan en sus diferentes dispositivos móviles, como computadores portátiles, Tablet, teléfonos inteligentes. (Agencia de Regulación y control de las telecomunicaciones, 2023)

En la tabla 1 se indica los riesgos del uso sin restricción de internet en dispositivos móviles en los menores de edad.

Tabla 1 Riesgos del uso sin restricción de internet en dispositivos móviles en los menores de edad.

Riesgo	Definición
Ciberbullying	Se refiere al acoso digital que ocurre principalmente entre los menores de edad, es uno de los mayores riesgos. Gracias al anonimato y a las facilidades que ofrece Internet de poder hacerlo desde Detrás de un dispositivo no se sabe la identidad del usuario, el anonimato es el mayor riesgo que existe.
Falta de privacidad	El manejo de las redes sociales para compartir nuestro contenido personal sin tomar en cuenta qué público puede acceder al mismo esto podría conllevar a una suplantación de identidad.
Grooming	Esto refiere prácticas en línea de adultos que buscan hacerse con la confianza de los menores para acosar explotar sexualmente imágenes de carácter sexual. Está relacionado con la pornografía infantil y la pedofilia en Internet.
Sexting	Consiste en enviar desde tu dispositivo móvil contenido sexual (fotografías, textos, audios) como pruebas de afecto o a modo broma. El problema surge cuando se utiliza este contenido para soborno
Contenidos inapropiados	Un niño puede estar buscando juegos en línea y encontrar accidentalmente páginas no aptas para su edad que incluyan contenidos de carácter sexual o violencia o drogas.
Problemas de adicción a los Smartphone e internet	Es un trastorno real que afecta tanto a menores de edad como a personas adultas. Consiste en la creencia de una necesidad constante de estar conectado al móvil o internet
Distorsión de la realidad	Las noticias falsas se pueden encontrar regularmente y son las noticias engañosas que aparecen en internet. Un menor de edad puede encontrarse con información falsa y que el contenido afecte y distorsione su realidad.

Nota: Riesgos del uso sin restricción de internet (CPA PSICOLOGOS, 2023)

Usos que de una aplicación de control parental:

- Su finalidad es evitar que menores y jóvenes sean contactados por desconocidos y prevenir diversos peligros como el Grooming, el ciberbullying y el sexting.

- Restringir el acceso de los jóvenes a sitios web que contengan contenido violento o inapropiado, como pornografía. O la discriminación contra los niños.
- Establece un horario programado para utilizar la aplicación en tu dispositivo móvil.
- Bloquear descargas de aplicaciones no autorizadas.
- Prevenir transacciones fraudulentas en línea.
- Habilitación de la geolocalización en dispositivos móviles para localizar a niños y jóvenes.

Algunas de las actividades incluidas en los controles parentales incluyen controlar a qué contenido acceden sus hijos, monitorear sus actividades en línea y ver con quién interactúan en las redes sociales, y limitar el tiempo frente a la pantalla. (Villanueva, 2021)

1.6.2 PRIVACIDAD EN EL CONTROL PARENTAL

Uno de los principales temas que se discuten cuando se habla de controles parentales es la privacidad de los datos. Esto plantea debates éticos sobre el control de los padres sobre la información personal de sus hijos. Algunos dicen que los padres deberían tener control total sobre el uso de la tecnología por parte de sus hijos. Otros creen que la mejor manera de resolver el problema es educar a los niños sobre los riesgos asociados con Internet y la tecnología y capacitarlos para que aprendan ellos mismos comportamientos seguros.

Los controles parentales administran y procesan datos, información, mensajes y otros datos en las actividades de menores para controlar o limitar el contenido al que los menores pueden acceder en línea. Tal comportamiento sin el permiso del propietario de la información (menor) puede considerarse una violación de su confidencialidad. (Oña, 2020)

Más bien, una de las razones de tales violaciones de datos es que a los tutores les preocupa que los niños puedan estar expuestos a una gran cantidad de contenido inapropiado en línea, como violencia, armas, imágenes y lenguaje pornográfico. drogas o incluso la posibilidad de que su hijo

desarrolle una relación en línea con un extraño que puede ser una persona peligrosa que intenta aprovecharse del niño, es decir, una víctima de abuso sexual. (Oña, 2020)

1.6.3 CIBERNETICA SOCIAL

La cibernética social es un método de conocimiento social, la sociedad se entiende como un sistema similar a un sistema cibernético. Se basa en supuestos como la interconexión y la interdependencia de cada individuo. (PREZI, 2023)

Cabe señalar que la cibernética social es un enfoque práctico que abarca todas las ciencias sociales y formaliza una visión sistemática y tripartita donde la sociedad se mueve en forma de tres partes y tres fuerzas, creando la base para el Juego de las Tres Vías. (Sanguano, 2021)

Estos juegos están representados por tres subgrupos liderados por:

- Inteligencia Legítima
- Inteligencia Emocional
- Inteligencia Operacional

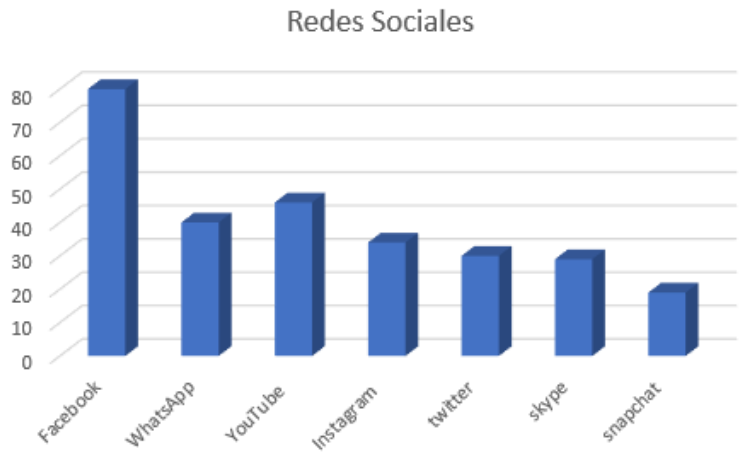
1.6.4 RIESGOS ONLINE

Hoy en día existe una gran cantidad de usuarios de Internet, lo que significa que existen muchos riesgos y desafíos, todos relacionados con la seguridad personal de los usuarios, y la mayoría de los usuarios son menores de edad. El acoso online (cyberbullying), los mensajes de texto pornográficos, el acoso, la violencia, la pornografía y otros fenómenos requieren que la tecnología intervenga en la seguridad de la red para hacer frente a esta situación.

Según la última encuesta de padres de EventTi, las plataformas de redes sociales más utilizadas por los niños son: Facebook 80%, YouTube 46%, WhatsApp 40%, Instagram 34%, Twitter 30%, Skype 29% y Snapchat 19%. (EventosTi.net, 2023)

Figura 1

*R*edes sociales que usan los menores con mayor frecuencia



Nota: Redes sociales usadas con mayor frecuencia por los menores (EventosTi.net, 2023)

Como se señala en la encuesta anterior, el hecho de que hasta el 80% de los menores interactúen con redes sociales como Facebook demuestra lo vulnerables que pueden ser en muchos casos y están expuestos a diversos riesgos informáticos en Internet.

1.6.5 CIBERBULLYING

Este término se utiliza cuando otro niño o joven acosa, amenaza, acosa, humilla, o abusa de un niño o joven utilizando internet u otro medio de comunicación como un teléfono móvil o una tableta.

Se caracteriza por la opresión que se da entre dos iguales, en este caso menores de edad. Esta distinción es importante porque existen otras prácticas que involucran a adultos, denominadas simplemente acoso cibernético, que pueden tener consecuencias legales por el comportamiento de un adulto hacia un menor. (México, 2023)

Algunos tipos de ciberbullying incluyen:

- Además de golpes, empujones y patadas, acoso a través de mensajería instantánea
- Hurto de claves: (WhatsApp, Messenger, Facebook, SMS)
- Publicaciones ofensivas en blogs: foros, sitios web y redes sociales como Facebook,

Twitter u otros.

- Realizar encuestas para humillar o intimidar.

1.6.6 SEXTING

Sexting, derivado de los términos ingleses "sex" y "texting", se refiere al envío de contenidos pornográficos o pornográficos (principalmente fotografías y/o vídeos) a través de medios digitales (casi siempre teléfonos móviles, tabletas y ordenadores). (MARCA, 2023)

Dada la facilidad y velocidad de difusión que permiten las nuevas tecnologías de comunicación, los participantes están escapando del control de los mensajes mediante el robo cibernético o incluso el robo de identidad porque estas herramientas proporcionan un grado de anonimato. (MARCA, 2023)

Además, los cambios en la relación entre los participantes pueden dar lugar a posibles chantajes sexuales o viralización de contenidos eróticos íntimos.

1.6.7 GROOMING

Grooming es el acto por el cual un adulto se gana engañosamente la confianza de un menor con el fin de obtener la oportunidad de establecer contacto sexual con él a través de imágenes o videos que exploten contenido sexual o pornográfico, es una serie de acciones.

Los atacantes suelen operar utilizando perfiles falsos que tienen la misma edad que el menor, comparten los mismos gustos y aficiones e incluso pueden ofrecer regalos físicos o virtuales para ganarse la confianza. Una vez que tengas evidencia sexual (fotos o videos) de un menor, pueden usarla para chantajearlo y obtener lo que quieras de él. (MAPFRE, 2023)

1.6.8 METRICAS

El desarrollo de las TIC abre nuevos escenarios para la realización de investigaciones de datos sobre la información, especialmente la que circula en Internet. La cibermetría se presenta como un sistema dedicado a describir cuantitativamente el contenido y los procesos de comunicación en el ciberespacio. (Oña, 2020)

1.6.9 PROCESAMIENTO DE LENGUAJE NATURAL (NPL)

El procesamiento del lenguaje natural (PNL) se refiere a la subcategoría de la informática (más concretamente, a la inteligencia artificial que otorga a las computadoras la capacidad de comprender texto y habla como los humanos).

La programación neurolingüística (PNL) impulsa programas que traducen de un idioma a otro, responden a comandos de voz y resumen rápidamente grandes cantidades de texto, incluso en tiempo real. Probablemente haya trabajado con la Programación Neurolingüística (PNL) en forma de sistemas GPS de control de voz, asistentes digitales, software de dictado de voz, chatbots de servicio al cliente y otros servicios al consumidor. Pero la PNL también desempeña un papel cada vez más importante en las soluciones empresariales destinadas a mejorar los procesos empresariales, aumentar la productividad de los empleados y optimizar procesos empresariales importantes. (IBM, 2023)

1.6.10 RECUPERACIÓN DE LA INFORMACIÓN

La recuperación de datos es fundamental para la continuidad del negocio en un entorno digital cada vez más dependiente de la información. La subcontratación del respaldo en la nube se ha convertido en una solución importante para garantizar la protección y disponibilidad de los datos en caso de un desastre o falla. Al subcontratar el respaldo en la nube, las empresas pueden brindar mayor seguridad, accesibilidad global, escalabilidad y flexibilidad, además de reducir costos y recursos. Al aprovechar los servicios en la nube, las empresas pueden garantizar una recuperación de datos eficaz y seguir siendo resilientes en un mundo cada vez más digital. (brontobytecloud, 2023)

1.6.11 INGENIERIA DE SOFTWARE

La ingeniería informática se centra en el desarrollo de software. Los desarrolladores de software utilizan técnicas de ingeniería para diseñar, desarrollar, probar y mantener aplicaciones y sistemas de software. Esto incluye el uso de lenguajes de programación, métodos de desarrollo ágiles y una buena gestión de proyectos de software. (POLI VERSO, 2023)

1.6.12 OVERSHARING

Según la Asociación REA, el término se refiere a compartir sin restricciones cualquier cosa relacionada con nuestra vida en Internet y las redes sociales. El problema de este fenómeno es que, si bien es peligroso también para los adultos, este tipo de actividad la realizan niños y jóvenes que son usuarios más vulnerables.

Los principales riesgos de publicar esta información en redes sociales incluyen saber dónde estudia su hijo, cuáles son sus principales actividades durante el día y cómo pueden causar daño los ciberdelincuentes. Además, hacer pública su actividad proporciona su ubicación precisa en tiempo real, lo que lo pone en riesgo de convertirse en víctima de un delito. (EXPANSIÓN, 2023)

1.6.13 VAMPING

El vampirismo es un concepto que hace referencia al uso de las nuevas tecnologías durante la noche. Fue creado a partir de la combinación de las palabras inglesas “vampire” (criatura de la noche) y “text message” (envío de mensajes). Por ello, las personas que caen bajo este término utilizan excesivamente las pantallas y envían mensajes desde sus teléfonos móviles o tabletas, perturbando incluso su sueño nocturno.

En la práctica, el vampirismo hace que los jóvenes se queden despiertos hasta tarde enviando mensajes de texto y es más común entre los adolescentes. Esto crea una dependencia de las nuevas tecnologías que genera miedo a estar desconectado o a las consecuencias de no responder a un mensaje. (Hacer Familia, 2023)

Al utilizar pantallas por la noche, el sueño se ve afectado por el nerviosismo que provoca la atención a estos dispositivos.

1.6.14 RASPBERRY PI 4

Raspberry Pi es un ordenador del tamaño de una tarjeta de crédito con conexión USB, que incluye interfaz LAN, WIFI y Bluetooth.

Es un ordenador pequeño que se puede usar para proyectos de electrónica y muchas tareas realizadas en una computadora de escritorio, como hojas de cálculo, procesamiento de textos, navegación por Internet, juegos en línea y reproducción de videos de alta calidad.

Raspberry PI es una organización con sede en el Reino Unido que se especializa en proporcionar computadoras de alto rendimiento y bajo costo. El modelo elegido para este proyecto es Raspberry PI 4. Los detalles de las características del hardware se explican a continuación:

- MEMORIA RAM: 1 GB.
- Puertos de conexión USB: 4
- Conexiones de salida de Video: HDMI
- Conexiones de puertos de Red: RJ45, Wifi

Imagen 1

Tarjeta Raspberry PI 4

Nota: Tarjeta Raspberry PI 4 Autor: Marco Ortiz

1.6.15 SISTEMA OPERATIVO: LINUX

Linux es un sistema operativo derivado de Unix. Es estable y muy popular entre los administradores de servidores y centros de datos. Este sistema operativo es una de sus primeras opciones al iniciar un proyecto. Una de sus principales características es que es estable, robusto, escalable, no requiere de un hardware extenso para su funcionamiento y es completamente gratuito. Existen varias distribuciones de Linux, las más populares se detallan a continuación:

- Ubuntu Linux.
- OpenSUSE.
- CentOS
- Fedora
- Debian

Existen también otras distribuciones orientadas a empresas más robustas como:

- Red Hat Enterprise Linux
- Ubuntu Server
- CentOS
- SUSE Enterprise Linux

Se eligió la distribución Raspbian para el desarrollo del proyecto ya que es una de las distribuciones que mejor soporta Raspberry PI y además es muy potente como servidor web y proxy transparente.

1.6.16 PROXY

Los servidores proxy permanecen intercalados entre el navegador web de su dispositivo y el mundo. También afecta la velocidad de su servicio de Internet al permitir, denegar o restringir el acceso a Internet y al almacenar en caché las páginas web a las que acceden las computadoras y dispositivos que navegan en la misma red.

Proxy Explicito: Este tipo de proxy requiere que configure el puerto y la dirección IP del servidor proxy en su navegador para forzar todo el tráfico HTTP a través del servidor proxy. Esto es un inconveniente porque si un dispositivo falla por algún motivo, todos los clientes no podrán acceder a Internet.

Proxy transparente: Este tipo de servidor intercepta el tráfico HTTP de la red y lo redirige a un servidor proxy sin ninguna interacción del usuario.

1.6.17 SERVIDOR WEB

Un servidor web pone la información que contiene a disposición de los usuarios a través de un navegador web a través de una red local o Internet. (Solorzano, 2020)

Apache: El más popular y utilizado en el mundo. Además, es no tiene costo, de código abierto y funciona en todas las plataformas. (Solorzano, 2020)

Microsoft IIS: Es una aplicación paga ya que sólo funciona en sistemas Windows.

Ngnix: Es un servidor web muy liviano que se ejecuta en sistemas Unix y Windows. Es el cuarto servidor HTTP más popular de la web.

Lighttp: Este servidor web es uno de los más ligeros del mercado. Está especialmente diseñado para reducir el uso de RAM y CPU y manejar cargas pesadas sin desequilibrio. Los sitios populares que lo utilizan incluyen YouTube y Wikipedia, que admiten grandes cantidades de tráfico diario. También es gratuito y se distribuye bajo licencia BSD. (Solorzano, 2020)

1.6.18 WEB SERVICE

Los desarrolladores pueden incluir un conjunto de soluciones o procedimientos en su sitio web que utilizan servicios web de terceros o sus propios servicios web, como un servicio que proporciona datos meteorológicos para una ubicación particular. Podemos concluir que un servicio web o un servicio web es un programa que se ejecuta en el lado del servidor y espera ser utilizado por otra aplicación interna o externa. Los servicios web utilizan protocolos bien conocidos y ampliamente utilizados, como XML, TCP/IP como protocolo de transporte y HTTP como protocolo de transporte de hipertexto. (Solorzano, 2020)

1.6.19 ANDRIOD

Es esencialmente un sistema operativo con kernel Linux diseñado para dispositivos móviles. Gracias a su innovadora compatibilidad con pantallas táctiles, millones de usuarios en todo el mundo lo adoptaron rápidamente. Este proyecto cuenta con el respaldo de Android, Inc. Comenzó con el soporte de Google y luego fue adquirida por Google. Debido a que este sistema operativo es de código abierto, miles de desarrolladores escriben constantemente aplicaciones para él. (Solorzano, 2020)

El sistema operativo Android es compatible con una amplia gama de dispositivos como teléfonos móviles, tabletas y portátiles.

1.6.20 PHP

Fue desarrollado por Rasmus Lerdorf en 1994 y originalmente se utilizó para rastrear el acceso a su currículum en línea. Llamó a estos scripts "Herramientas de página de inicio personal", pero también se los conoce más comúnmente como "Herramientas PHP". Con el tiempo, su funcionalidad se expandió hasta convertirse en una herramienta PHP y se creó una implementación más grande y rica. (Solorzano, 2020)

Este nuevo modelo PHP puede interactuar con bases de datos y proporciona un entorno de trabajo en el que los usuarios pueden desarrollar aplicaciones web dinámicas simples, como libros de visitas.

Con el transcurso del tiempo se desarrollaron nuevas características de PHP como las siguientes (PHP.net):

- PHP/FI
- PHP 2.0
- PHP 3.0
- PHP 4.0
- PHP 5.0

1.6.21 ANDROID ESTUDIO

Este es el IDE oficial para el desarrollo de aplicaciones de Android.

Android Studio proporciona un amplio conjunto de herramientas de edición, depuración, prueba y creación de perfiles de código que se adaptan a sus necesidades.

Con el tiempo, se crearon nuevas versiones de PHP de la siguiente manera (PHP.net) (ANDROID, 2023)

Característica	Función
Instant Run	Al hacer clic en Ejecutar o Depurar, la función de ejecución inmediata de Android Estudio aplicará los cambios en el código y recursos en la aplicación. Se interpreta de forma inteligente los cambios y, a menudo los entrega sin necesidad de reiniciar la aplicación o volver a compilar el APK, para que pueda ver los efectos inmediatamente.
Editor de código inteligente	El editor de código le ayuda a trabajar más rápido y ser más productivo, ofreciendo finalización avanzada de código, refactorización, y el análisis de código. A medida que el programador escribe, Android Studio proporciona sugerencias en una lista desplegable. Basta con pulsar la tecla Tab para insertar el código.
Emulador rápido y rico en funciones	El emulador de Android instala e inicia sus aplicaciones más rápido que un dispositivo real y le permite probar su aplicación con todas las configuraciones de dispositivos Android: móviles, tabletas, Android Wear y dispositivos Android TV. También puede simular una variedad de características de hardware tales como la localización GPS, la latencia de red, y la entrada multi-touch.

C++ and NDK support	Android Studio le permite utilizar C ++ y el NDK de Android junto con su código de Java. Proporciona resaltado de sintaxis y refactorización para C ++, y un depurador basado en LLDB que permite depurar simultáneamente Java y C ++.
Integración con lanube	Las herramientas integradas de Google Cloud Platform permiten crear e implementar un backend para su aplicación Android empleando servicios como Google Cloud Endpoints y Firebase mensajería en la nube.

1.6.22 SQUIDGUARD

Es una combinación de sistema de filtrado de redireccionamiento web y complemento de control para Squid. "Lista negra" Utilice la lista negra como base de datos para negar o permitir a los usuarios el acceso a sitios web. Su mayor utilidad es bloquear dominios y URL que contengan información innecesaria o no válida durante el horario comercial. (Solorzano, 2020)

1.6.23 LISTA NEGRA

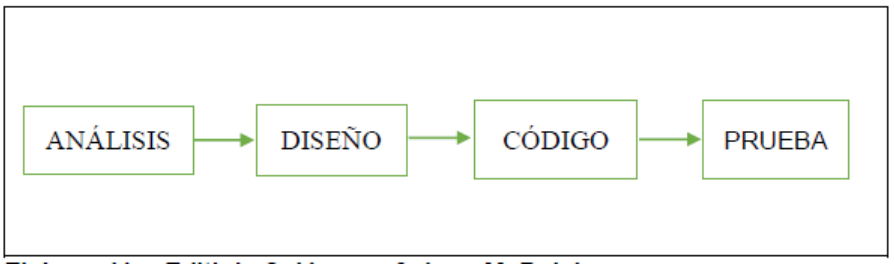
Una lista negra de TI es una lista de dominios, URL o direcciones IP que contienen información inapropiada y deben restringirse. A menudo pueden enviar spam, software espía, piratería informática, pornografía, etc. (Solorzano, 2020)

1.6.24 MODELOS DE PROCESOS DE SOFTWARE

Hay muchos modelos de procesos de software disponibles, cada uno de los cuales describe los pasos y acciones que se deben tomar para entregar el diseño final.

Existe un modelo secuencial lineal, también conocido como modelo de ciclo de vida básico o modelo en cascada. El modelo secuencial lineal ofrece un enfoque de desarrollo de software secuencial y estructurado que comienza en el nivel del sistema y continúa a través del análisis, diseño, codificación, pruebas y mantenimiento.

FIG 2 MODELO LINEAL SECUENCIAL



Nota: Modelo lineal secuencial Autor: Marco Ortiz

El diseño ágil se centra en expresar aspectos del software que son visibles para el usuario/cliente, como el enfoque de entrada y los formatos de salida. Diseñar y prototipar rápidamente.

Los clientes/usuarios evalúan los prototipos para ayudar a refinar los requisitos del software a desarrollar. Las iteraciones implican ajustar el prototipo para satisfacer las necesidades del cliente y, al mismo tiempo, brindar a los desarrolladores una comprensión más profunda de lo que se debe hacer.

1.6.25 CÓDIGO ORGÁNICO PENAL

Delitos contra la seguridad de los activos de los sistemas de información y comunicación.

ARTÍCULO 229: Revelación ilegal de base de datos. La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad, la privacidad de la persona, será sancionada con pena privativa de libertad de uno a tres años. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014).

ARTÍCULO 230: Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

CAP. V. De las Estafas y otras defraudaciones

ARTÍCULO 231: Transferencia electrónica de activo patrimonial. La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma

ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

ARTÍCULO 232: Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

ARTÍCULO 233: Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación

para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

ARTÍCULO 234: Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014)

2.1 GENERALIDADES

Esta propuesta nace de la necesidad de disponer de un control parental en los dispositivos que utilizan frecuentemente los niños y jóvenes menores de 18 años, seguidamente de proporcionar el conocimiento adecuado de los riesgos que existen hoy en día en las conexiones hacia internet, para finalmente poder mitigar tanto en las conexiones a internet como en la vida real fraudes y estafas que pueden tener grandes repercusiones.

2.2 METODOLOGÍA

La investigación es de naturaleza cuantitativa porque tiene como objetivo obtener datos que puedan medirse mediante pruebas estandarizadas. Para ello se trata de un diseño descriptivo y relevante. Su objetivo era, por un lado, determinar el nivel de control parental y de uso de Internet entre menores de 18 años, y por otro, determinar la relación entre estas dos variables. Debido a la naturaleza de la fuente de información, puede ser un estudio de campo ya que los datos se recopilan directamente de los sujetos. Por su carácter temporal, se trata de un estudio transversal en el que se miden variables en un único momento en el tiempo. Se utilizó un diseño no experimental debido a que no se pudieron controlar las variables de estudio.

2.3 FASES DE LA METODOLOGÍA

La primera fase de este proyecto presenta una investigación en profundidad con medios confiables relacionados con la seguridad y los peligros que hay al acceder a diferentes conexiones a internet desde dispositivos móviles que no tienen un sistema de control parental para conocer sus ventajas y características. También se analiza el estado actual de los sistemas de control parental y de los recursos necesarios para satisfacer las necesidades de los padres de familia.

En la fase 2 del proyecto una vez que se conocen los términos e información mínima acerca del control parental se canalizan las características para el diseño del sistema en dispositivos móviles referente a: eficiencia, capacidad, distancia, equipos a utilizar. Se consideran edades, y las necesidades de acceso a internet según la misma.

En la tercera fase, utilice la herramienta de simulación de diseño de aplicaciones Android Studio. Con funciones integrales que incluyen un editor de código inteligente, un emulador de Android y herramientas de depuración avanzadas para aumentar la eficiencia del desarrollo, esta herramienta es imprescindible.

Para la simulación del diseño de una aplicación de control parental su desarrollo se lo puede realizar mediante el entorno Android Studio es un entorno de desarrollo integrado para el sistema operativo Android ofrece nuevas herramientas para el desarrollo de aplicaciones al momento es el IDE (Entorno de Desarrollo Integrado) más utilizado.

2.4 MUESTRA

La muestra para este proyecto de investigación está compuesta por niños y adolescentes de entre 8 y 18 años de la ciudad de Quito. Esta es una muestra no probabilística seleccionada intencionalmente. La unidad de observación estuvo compuesta por niños y adolescentes, y la unidad de análisis fue el control que necesitan los padres de familia, así como también las percepciones sobre el uso de Internet por parte de los adolescentes. En particular, la técnica de la bola de nieve se utiliza para encontrar algunas personas y dirigirlas hacia otras.

Para ser parte de la muestra, se tomaron en cuenta los siguientes criterios:

- Niños y adolescentes varones con una edad entre los 8 y 18 años.
- Niñas y adolescentes mujer con una edad entre los 8 y 18 años
- Menores de 18 años que hagan uso de Internet, posean un teléfono móvil propio y conviva con alguno de sus padres, o tutores.

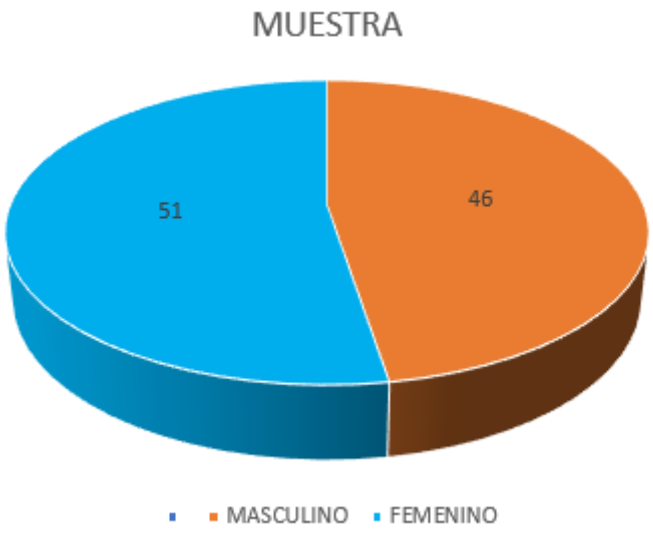
Para no ser parte de la muestra, se tomó en cuenta el siguiente criterio:

- Niños y adolescentes fuera del rango de edad de 8 y 18 años

Se obtuvo un tamaño de muestra de 97 individuos (X = 97). El grupo estuvo integrado por jóvenes de 8 a 18 años de diversas instituciones educativas del área metropolitana de Quito; 51 (52%) mujeres y 46 (47,42%) hombres.

Figura 3

Tamaño y porcentaje de la muestra



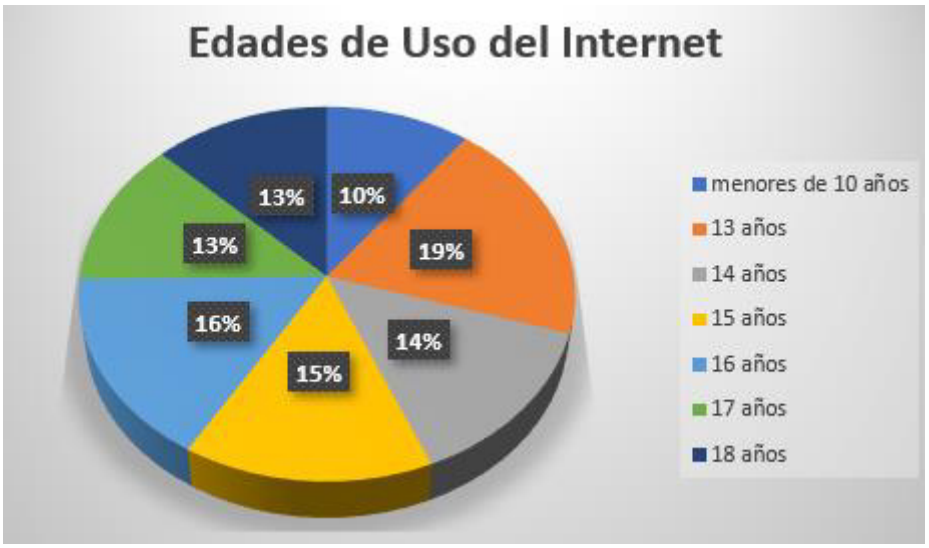
Nota: Tamaño y porcentaje de la muestra Autor: Marco Ortiz

Con la muestra recolectada se pudo observar que la población tiene entre 8 a 18 años (Figura 2), siendo la media de 14,95 años y el desvío estándar de 1,922.

Las personas menores de 12 años representan el 10,3%, 13 años el 19,5%, 14 años el 13,8%, 15 años 14,9%, 16 años el 16,1%, 17 años el 12,6% y 18 años el 12,6%.

Figura 4

Edades de uso de Internet



Nota: Edades de uso de Internet Autor: Marco Ortiz

2.5 TECNICA E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Está especialmente preparado para evaluar datos sobre menstruación, sexo y edad. Falta el formulario en el archivo adjunto.

2.6 CUESTIONARIO DE CONTROL PARENTAL

Mediante la encuesta sobre Control Parental del Uso de Internet en niños y adolescentes de Álvarez-García, cuyo modelo incompleto está disponible en los anexos. Se trata de una prueba de siete ítems dirigida a niños y jóvenes. Cada ítem especifica el comportamiento de los padres que limita o monitorea el uso de Internet en quienes participan de la encuesta. (GONZALES, 2022)

El elemento de monitoreo incluye elementos que se refieren a que los padres monitoreen abierta o encubiertamente las actividades de sus jóvenes en Internet, durante o después de su uso.

Por ejemplo: 1 Cuando navego por Internet en mi tiempo libre, mi familia me mira y mira la pantalla. Este factor incluye los puntos 1, 2, 6 y 7 anteriores. El segundo elemento corresponde a restricciones e incluye elementos relacionados con acciones de los padres para limitar el uso de Internet (tiempo, contenido, actividades) mediante el establecimiento de reglas o el uso de software

especial. Por ejemplo: 2 En casa me dan unas reglas sobre lo que puedo y no puedo hacer online. Además del inciso anterior, se incluyen los incisos 4 y 5.

Se pidió a los informantes que utilizaran una escala de respuesta para indicar en qué medida creían que cada afirmación era cierta se usa una escala tipo Likert, con cuatro alternativas (1=Totalmente falso; 2=Más bien falso; 3=Más bien cierto; 4=Totalmente cierto). Una puntuación alta indica un alto nivel de control parental sobre el uso de Internet. La consistencia interna de los resultados entre escalas es alta (α=.82). (GONZALES, 2022)

2.7 INSTRUMENTOS SOBRE EL USO DE INTERNET

Se utilizó la encuesta de uso de internet modificada de Orellana Marcial (2010), incorporando dos ítems de la encuesta de desarrollo de habilidades TIC de Choque Larrauri (2009). La encuesta, que se puede encontrar en el apéndice, midió varios aspectos del uso de Internet, como el tiempo, la ubicación, la frecuencia de las conexiones, el nivel de conocimiento de Internet, quién enseñó cómo utilizar Internet y el propósito del uso de Internet. ¿Alguna vez has usado Internet? ¿Cuánto tiempo llevas usando Internet? ¿Dónde navegas más por Internet? ¿Qué haces cuando estás en línea? : reviso el correo electrónico, chateo (Messenger) y me conecto a Instagram, Facebook, Twitter u otras redes sociales. Tiene 25 puntos; para las primeras 6 opciones, indique la respuesta que crea adecuada, para las 19 opciones restantes, marque la casilla Siempre, Casi siempre, A veces, Casi nunca en desacuerdo y Nunca, dependiendo de lo que desee considerar. vinculado a. El coche es bastante fiable. (α=0,76). (GONZALES, 2022)

2.8 PROCEDIMIENTO PARA LA RECOLECCIÓN DE DATOS

Se buscaron niños y jóvenes que cumplieran con características relevantes y se les pidió que visitaran a otros niños y jóvenes como parte de una muestra de bola de nieve para reclutar a aquellos interesados en completar la encuesta.

Se dieron a conocer las condiciones de participación y se envió el correspondiente enlace de acceso. En primer lugar, se debía presentar una declaración de consentimiento de un padre o tutor legal o de un estudiante que ya fuera adulto. Se mantuvo el respeto por el individuo, se consideró la

libre participación, se garantizó la confidencialidad y el anonimato de los datos obtenidos y se observaron las normas éticas pertinentes.

De esta manera, las encuestas se administran en línea mediante la creación de un formulario de Google donde todas las encuestas se personalizan para la plataforma. La propuesta está diseñada para permitir a los participantes responder rápidamente a estas preguntas accediendo al enlace a través de su dispositivo móvil. De las encuestas recibidas se seleccionaron las respondidas correctamente y se recuperaron 90 de ellas para su posterior análisis.

2.9 PROCEDIMIENTO PARA EL ANÁLISIS DE DATOS

El procesamiento estadístico y análisis de los datos obtenidos a través del cuestionario se realizó utilizando el software estadístico Statistical Packpage for the Social Sciences (SPSS) versión 23.

Primero se realizó un análisis descriptivo de la muestra para determinar frecuencias, medias y desviaciones estándar.

Realizamos análisis estadísticos descriptivos de diversas medidas de control parental y uso de Internet por parte de los adolescentes.

Finalmente, para determinar la relación entre estas variables se realizó un análisis estadístico de varianza para determinar si existían diferencias entre sexo y edad mediante la prueba de personalidad.

2.10 CONTROL PARENTAL PERCIBIDO

La Tabla 2 muestra los puntajes mínimo y máximo, así como la media y la desviación estándar, de los resultados de protección infantil obtenidos para la muestra de 97niños y adolescentes estudiados.

Tabla 2

Media y desvío del nivel de control parental

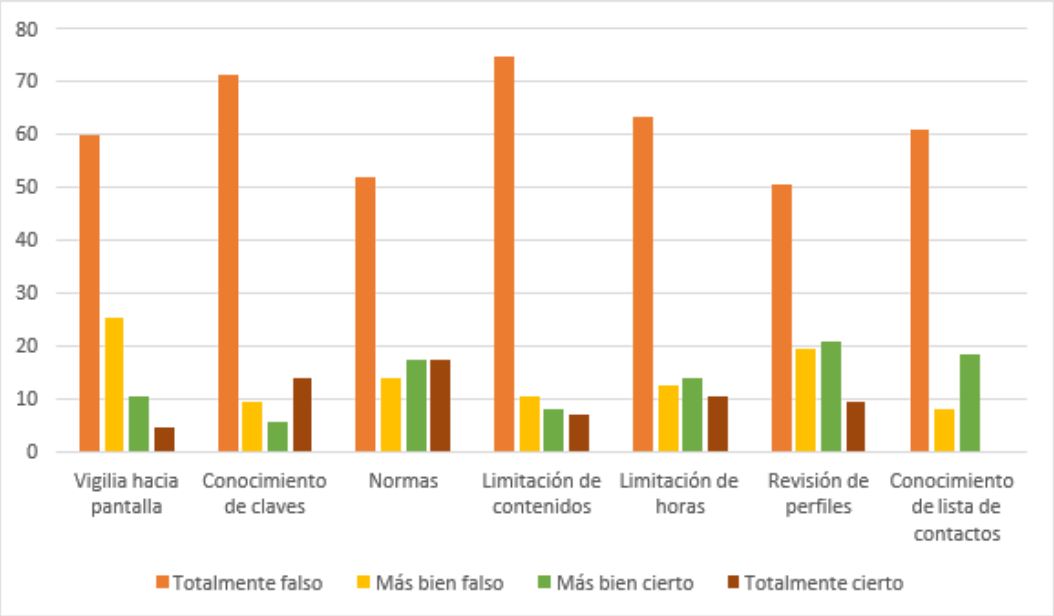
	N	Mínimo	Máximo	Media	Desv. típ.
Control parental	97	7,00	28,00	12,1149	5,46325

Nota: Media y desvío del nivel de control parental

Para obtener una descripción más detallada de las variables de control parental, describimos la frecuencia de respuestas a los distintos ítems evaluados en el cuestionario. Estos resultados se muestran en la siguiente figura;

Figura 3

Frecuencias de respuestas en control parental



Nota: describe las frecuencias de respuestas en control parental, Autor: Marco Ortiz

Para aclarar los dos tipos de control parental evaluados en la encuesta, a continuación, se enumeran las frecuencias de respuesta para las restricciones y la supervisión.

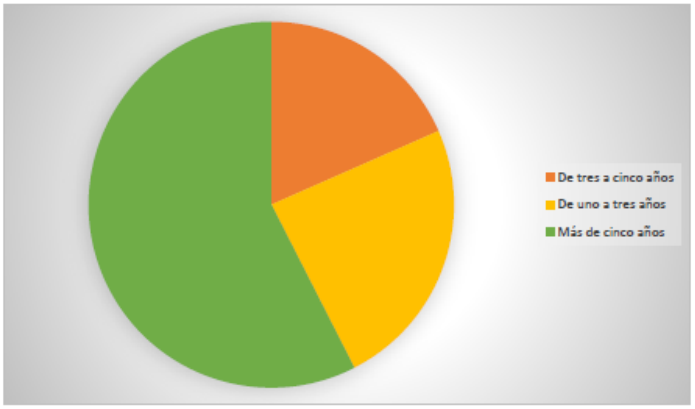
Respecto a los factores limitantes, el 63% de los encuestados respondió que la afirmación aplicable al ítem era completamente falsa, el 12% respondió que era algo falsa, el 13% dijo que era algo cierta y el 12% dijo que la afirmación aplicable al ítem era completamente falso La respuesta es completamente correcta. Respecto al factor cuidado, el 61% de los jóvenes dijo que la afirmación en cuestión era completamente falsa, el 15% dijo que era algo falsa, el 14% dijo que era algo cierta y el 10% dijo que era completamente falsa, respondieron que creían. que sea verdad.

2.11 DESCRIPCIÓN DEL USO DE INTERNET

Para describir con más detalle las variables de uso de Internet, describimos la frecuencia de respuestas a los distintos ítems evaluados en el cuestionario. Estos resultados se muestran en la siguiente figura y tabla. Años de uso de Internet

Figura 4

Años de uso de Internet

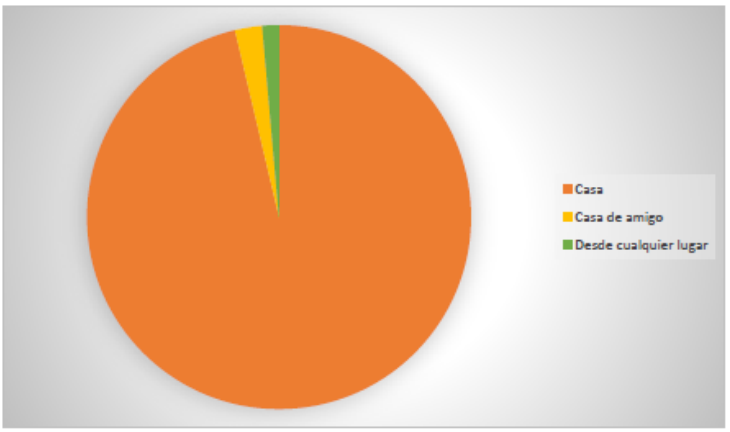


Autor: Marco Ortiz

Nota: Como se puede observar en la Figura 4, el 58% de las personas ha utilizado Internet durante más de 5 años, el 24% ha utilizado Internet durante 1-3 años y el 18% ha utilizado Internet durante 3-5 años.

Figura 2

*L*ugar del uso de internet

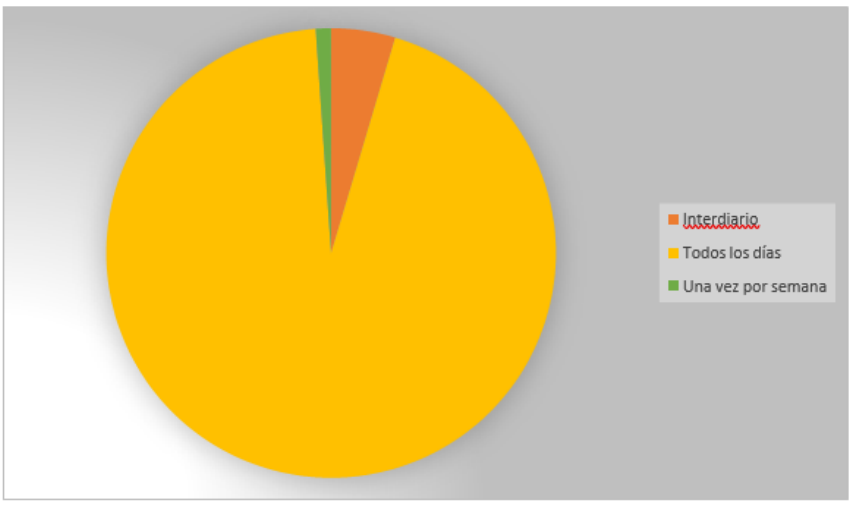


Nota: Lugar de conexión a Internet Autor: Marco Ortiz

La Figura 5 muestra que el 96% de las personas dice que accede a Internet principalmente desde su casa, el 2% accede a Internet desde la casa de un amigo y el 2% accede a Internet desde cualquier lugar.

Figura 3

Frecuencia de conexión a Internet.



Nota: Frecuencia de conexión a Internet Autor: Marco Ortiz

El gráfico 6 muestra que los jóvenes utilizan Internet todos los días (94%), cada dos días (5%) y una vez a la semana (1%).

Tabla 3

Se describe el tiempo que pueden permanecer conectados a Internet

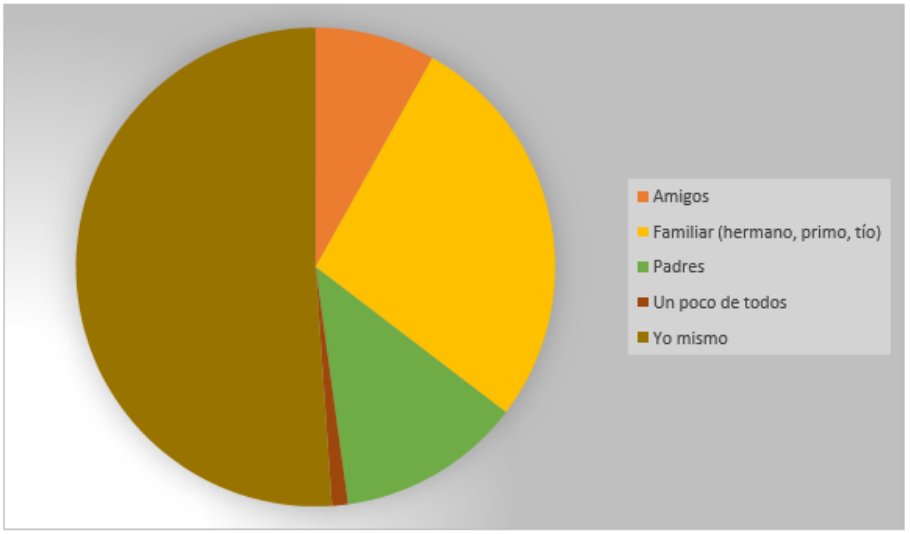
¿Cuánto tiempo permaneces conectado a internet?	
	%
10 horas	1,1
10 minutos	1,1
6 horas	1,1
Dos horas	6,9
Más de dos horas	65,5

Nota: tiempo que pueden permanecer conectados a Internet

Según su nivel de habilidad, los encuestados dijeron que van a Google y buscan información (59%), no hacen nada (27%), crean y publican sitios web y realizan otras actividades como comprar o vender en la web. Internet (6%).

Figura 4

Persona por la que aprendió a usar Internet



Nota: Persona por la que aprendió a usar Internet Autor: Marco Ortiz

En el gráfico 7, los encuestados afirman que aprendieron a utilizar Internet por sí mismos (51 %), gracias a sus familiares (27 %), sus padres (13 %) y sus amigos (8 %) y una pequeña parte (1%).

Tabla 3

Tabla de frecuencia de Uso del Internet

Frecuencia de respuestas en uso de Internet					
Ítems	Siempre	Casi siempre	A veces	Casi nunca	Nunca
Reviso mi correo electrónico	3,4%	9,2%	46,0%	32,2%	9,2%
Chateo (Messenger)	17,2%	13,8%	33,3%	18,4%	17,2%
Ingreso a redes sociales	70,1%	19,5%	9,2%	1,1%	0,0%
Ingreso a redes sociales	70,1%	19,5%	9,2%	1,1%	0,0%
Leo foros virtuales	5,7%	12,6%	33,3%	32,2%	16,1%
Participo en foros virtuales	6,9%	5,7%	31,0%	34,5%	21,8%
Juego en Red	26,4%	18,4%	27,6%	16,1%	11,5%
Veo videos en YouTube	41,4%	28,7%	24,1%	3,4%	2,3%
Escucho radio por Internet	0,0%	3,4%	26,4%	34,5%	35,6%

Nota: Tabla de frecuencia de Uso del Internet Autor: Marco Ortiz

2.12 DESARROLLO

El dispositivo elegido para operar el servidor es Raspberry PI 4; El dispositivo se dejó encendido durante 7 días, tiempo durante el cual permaneció conectado a Internet y se vio obligado

a actualizarse permanentemente. Esto confirma el correcto funcionamiento de las interfaces LAN y WIFI del dispositivo.

El sistema operativo: Para el servidor es Linux Raspbian. La prueba de compatibilidad de hardware es satisfactoria. Inicialmente las pruebas se realizaron con Linux Ubuntu pero esto provocó algunos problemas en el arranque; Se realizaron más pruebas con CentOS 7, pero tuve problemas de compatibilidad con parte del hardware del servidor Raspberry.PI 4.

Servidor web: Inicialmente se utilizó el software Jboss para las pruebas, pero se descubrieron problemas de compatibilidad en la placa base Raspberry PI 4 y luego se instaló Apache 2. Todas las pruebas pasaron.

Aplicación Android: Las aplicaciones desarrolladas para el sistema operativo Android han sido probadas en muchas versiones anteriores y en muchos dispositivos móviles; A partir de la versión 5, los resultados son satisfactorios.

Iptables: Algunas reglas se basan en los requisitos del sistema. Esta regla se ha aplicado con éxito a sitios que utilizan https; especialmente sitios web y aplicaciones como Facebook y WhatsApp.

PHP: El servicio web está desarrollado en PHP. Prueba de funcionalidad inicial utilizada SoapUI 5.2.1. Las pruebas funcionales tienen que ver principalmente con la conectividad. Los permisos de lectura y ejecución deben aplicarse al directorio de Linux donde se encuentra el archivo del servicio web.

2.13 TECNOLOGÍA MÓVIL

En la actualidad la tecnología móvil y el desarrollo de las aplicaciones Android es un mercado en crecimiento, desarrollando, creando aplicaciones atractivas e innovadoras.

Para el desarrollo de las aplicaciones, Androide Studio es una herramienta necesaria por sus amplias características, editor de código inteligente, emulador de androide y herramientas de depuración avanzadas hacen que el desarrollo sea efectivo provechado al máximo.

2.14 FACTIBILIDAD ECONOMICA

Dado que la aplicación se desarrolla utilizando Android Studio (software gratuito), este proyecto no requiere grandes inversiones financieras y no es necesario adquirir licencias. La función de servidor utiliza un componente llamado Raspberry PI 4, que ofrece un rendimiento de costos superior en comparación con los servidores normales. El software que utiliza en su dispositivo también es gratuito.

Esta aplicación se instala en dispositivos con sistema Android. Se eligió este sistema móvil porque, según el Instituto Nacional de Estadística y Censos (INEC), la mayoría de la población ecuatoriana utiliza dispositivos móviles con sistema operativo Android.

La mayoría de los dispositivos móviles disponibles en el mercado funcionan con el sistema operativo Android y utilizan muchas aplicaciones que se pueden descargar desde Play Store.

2.15 COSTO DEL PROYECTO

Los proyectos de control parental utilizan software gratuito para crear aplicaciones e instalar servidores, por lo que requieren muy poco presupuesto para su ejecución, lo que les da una gran ventaja en cuanto a presupuestos. A continuación, se muestra una tabla que muestra el presupuesto del proyecto.

Tabla 4

Tabla PRESUPUESTO DEL PROYECTO

	FUENTES		
RUBROS	ESTUDIANTES	OTROS	**TOTAL**
Recurso Humano	3	-	1000
Recursos Hardware	-	-	250
Recursos Software	-	-	-
Movilización	150	-	150
Servicio de Internet (120 días)	90	-	90
Documentación	39	-	39

Alimentación	320	-	320
TOTAL □	-	-	$ 1849

Nota; PRESUPUESTO DEL PROYECTO Autor: Marco Ortiz

Para la simulación del diseño de una aplicación de control parental, su desarrollo se lo puede realizar mediante el entorno Android Studio es un entorno de desarrollo integrado para el sistema operativo Android ofrece nuevas herramientas para aplicaciones al momento es el IDE (Entorno de Desarrollo Integrado) más utilizado.

Android Studio tiene las siguientes características que ofrece a los desarrolladores

Kotlin es un lenguaje de programación de código libre creado por JetBrains que se ha vuelto popular porque puede usarse para escribir aplicaciones de Android. Java es un lenguaje fácil de aprender si ya sabes programación.

Esta plataforma de trabajo también puede llegar a ser compatible con lenguajes como Kotlin NDK y C++ y en cuestión de compilación de código se utiliza Gradle, que está especializado para funcionalidades Android.

El lenguaje de programación Kotlin, nos permite una interoperabilidad natural con Java, incluso desarrollar código para proyectos utilizando ambos lenguajes a la vez sin ningún problema.

2.16 BASE DE DATOS

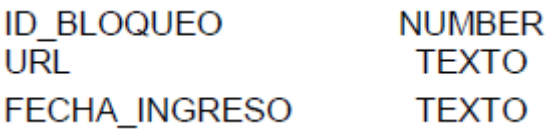
Este proyecto utiliza SQLITE para crear una base de datos. SQLITE es una biblioteca escrita en C que implementa un sistema de gestión de bases de datos transaccionales SQL independiente, sin servidor y sin configuración. El código SQLITE es de dominio público y es gratuito para uso comercial o personal. Actualmente se utiliza en una variedad de aplicaciones, incluidas aquellas desarrolladas como proyectos avanzados. (obviamente no probado)

El programa de control parental se centra en bloquear sitios web, por lo que no contamos con una base de datos grande. Por lo tanto, se ha creado una estructura que le permite guardar todas las

páginas bloqueadas en su dispositivo. Esta base de datos fue creada usando SQLITE Android Studio IDE.

A continuación, se muestra la arquitectura utilizada en el proyecto para almacenar páginas web importadas desde aplicaciones móviles en fragmentos.

IMAGEN ESTRUCTURA DE PÁGINA WEB



Nota: IMAGEN ESTRUCTURA PÁGINA WEB Autor: Marco Ortiz

2.17 APLICACIÓN

Inicialmente, se eligió Eclipse IDE para el desarrollo de aplicaciones. Sin embargo, después de investigar otras opciones de desarrollo de aplicaciones móviles, descubrimos que Android Studio tiene una excelente característica que facilita a los desarrolladores la creación de aplicaciones para Android. Este sitio también proporciona información sobre Eclipse IDE. (academiaandroid, 2021)

Tabla 5

Tabla comparativa entre Android Studio y Eclipse.

Características	AndroidStudio	Eclipse
Creación de nuevos módulos en el mismo proyecto.	SI	NO
Vista en tiempo real de renderizado de layouts.	SI	NO
Más rápido al momento de ejecutarse.	SI	NO
Facilidad de crear Interfaces.	SI	NO
Facilidad en la exportación de .APK.	SI	NO

Nota: tabla comparativa entre Android Studio y Eclipse Autor: Marco Ortiz

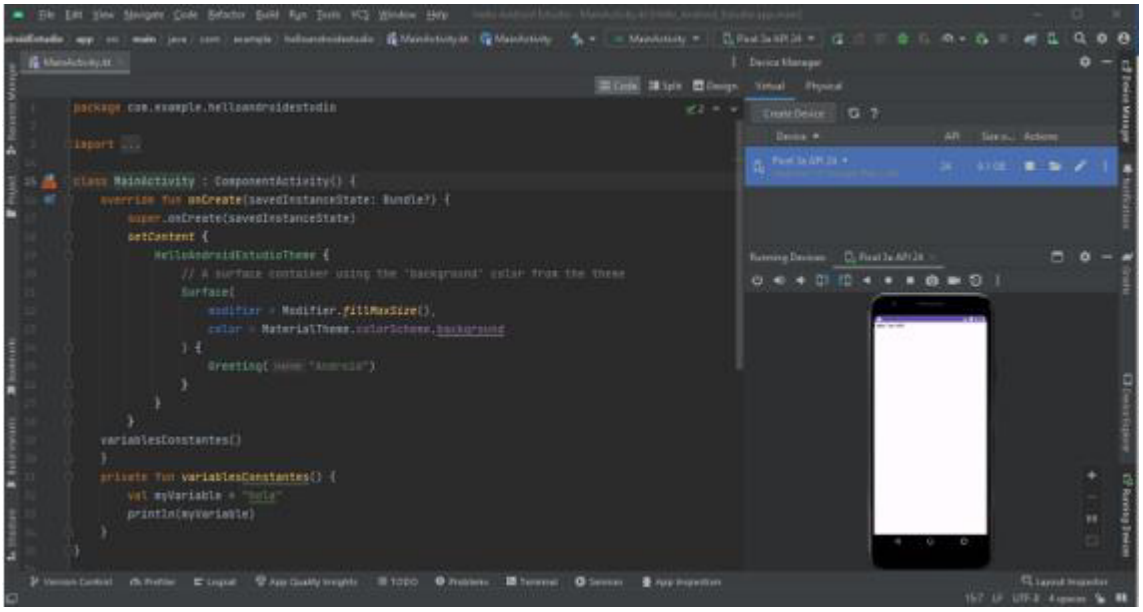
2.18 INTERFAZ DEL USUARIO

Esta sección define la interfaz visual del usuario. Desarrollada con Android Studio IDE, la aplicación es fácil de usar y fácil de usar.

Al comienzo de esta fase, se creó una interfaz de usuario inicial, pero como se muestra en la Figura la imagen no era buena y con el tiempo quedó claro que no era fácil de usar.

Figura 5

INTERFAZ GRÁFICA INICIAL



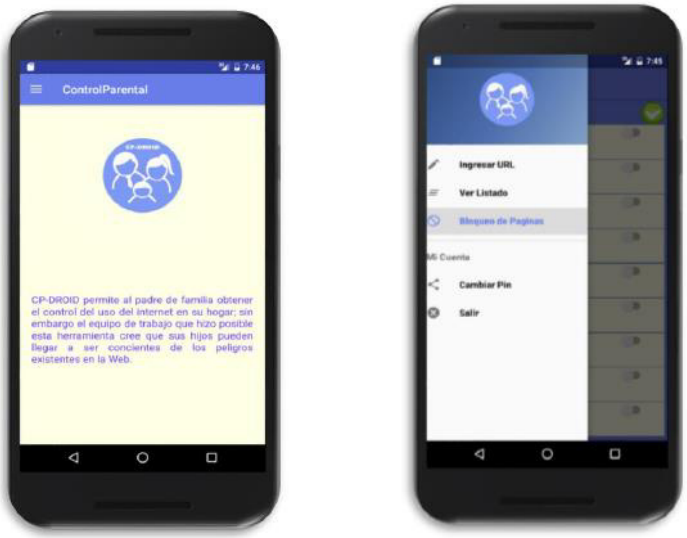
Nota: INTERFAZ GRÁFICA INICIAL Autor: Marco Ortiz

2.19 INTERFAZ DE ACCESO AL USUARIO

Los usuarios pueden registrarse ingresando un PIN de seguridad y una dirección de correo electrónico y, por lo tanto, el PIN de seguridad se puede enviar como respaldo de sus datos de inicio de sesión. La interfaz de la aplicación de control parental se ve así.

La interfaz de la aplicación de control parental tiene este aspecto Autor: Alex Aguirre

La primera GUI le permite registrar un PIN de seguridad para acceder a la aplicación. Se enviará un PIN de seguridad como se muestra en la imagen a la cuenta de correo electrónico que desea registrar.



Nota: primera interfaz gráfica de usuario Autor: Marco Ortiz

La GUI del menú principal se desliza desde el lado izquierdo de la pantalla, brindándole acceso a opciones como ingresar manualmente las URL para bloquear, verificar sitios bloqueados, bloquear por categoría e incluso cambiar su PIN si es necesario.

La opción Mostrar lista proporciona acceso a una lista de páginas de entrada manual. La opción de salida le permite cerrar la aplicación CP-DROID.

Si es necesario, simplemente mueva el cursor desde el lado izquierdo para cargar el menú principal.

Imagen 4

Imagen de reglas predefinidas

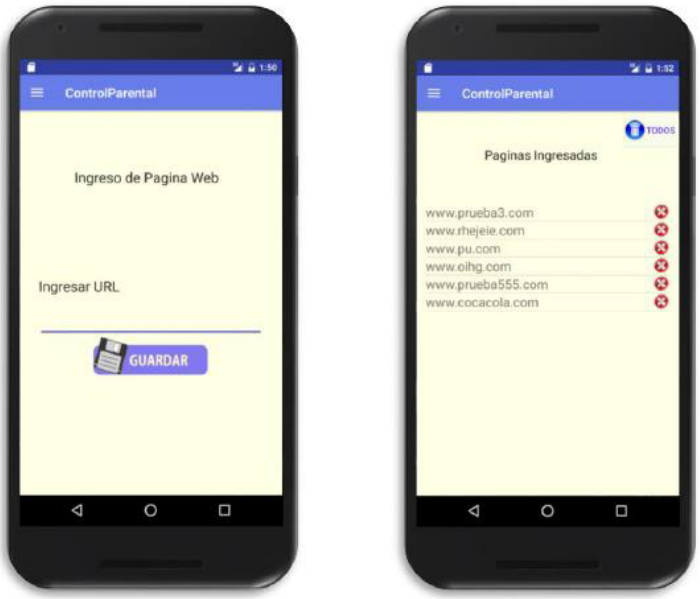
Nota: Imagen de reglas predefinidas Autor: Marco Ortiz

La aplicación cuenta con un menú que contiene reglas predefinidas y categorizadas como son:

- Redes Sociales
- Pornografía.
- Juegos en línea peligrosos
- Salas de Chat públicas.
- Shopping (Paginas de compras consideradas peligrosas).
- Religión (Sitios que contienen violencia basada en religión).
- Violencia (Armas, delitos, etc.)
- Socialnet

Imagen 5

INTERFAZ DE INGRESO DE PÁGINA A BLOQUEAR



Nota: Interfaz de ingreso de página a bloquear Autor: Alex Aguirre

Esta interfaz permite a los usuarios ingresar la URL de un sitio web específico que desean bloquear.

La URL ingresada se almacena en la base de reglas del servidor y se puede habilitar o deshabilitar a través del menú de usuario. Luego puede eliminar las reglas que creó.

2.20 DESARROLLO DEL SERVICIO WEB

Al desarrollar un servicio web, el primer paso fue considerar la compatibilidad del lenguaje del servicio web con el servidor. Una vez confirmada esta compatibilidad, el desarrollo continuó.

Este servicio web fue desarrollado utilizando código fuente PHP para garantizar la compatibilidad con los servidores Apache 2.

PHP (abreviatura recursiva de PHP: preprocesador de hipertexto) es un lenguaje de código abierto muy popular, especialmente adecuado para el desarrollo web y que puede integrarse en HTML. Se ha agregado una nueva biblioteca ksoap para llamar a servicios web desde aplicaciones y traducir servicios en aplicaciones. Utilice la aplicación SOAPUI 5.2.1 para realizar pruebas entre el servicio web y el servidor.

SoapUI es una poderosa herramienta que admite pruebas y desarrollo de aplicaciones. Permite realizar pruebas web con numerosas funciones, incluida una interfaz sencilla, fácil de usar e intuitiva. Esto permite el uso de métodos de captura y repetición y es una herramienta muy útil para realizar potentes pruebas de carga, informes detallados, gráficos y más.

SoapUI incluye el navegador Internet Explorer de Microsoft, que permite monitorear y controlar las acciones realizadas allí. (GONZALES, 2022)

Después de completar cada prueba, se llamaba un servicio web desde la aplicación al servidor. La prueba fue satisfactoria y resultó en el bloqueo de páginas seleccionadas de la aplicación.

2.21 PREPARACIÓN DEL SERVIDOR

Como se mencionó en otras secciones, como servidor se utiliza un dispositivo de baja relación llamado Raspberry PI 4; Este dispositivo utiliza un módulo de memoria microSD como disco duro. La imagen del sistema operativo Raspbian Linux se agrega desde una computadora. Una vez

completada la instalación, la interfaz de red se configurará y conectará a un punto de red con acceso a Internet para actualizar los paquetes de software.

2.22 INSTALACIÓN DE PAQUETES LINUX

Las siguientes líneas fueron ejecutadas para la actualización e instalación de nuevos paquetes de Linux:

Tabla 6

Tabla de instalación de paquetes de Linux

Orden	Línea	Uso
1	sudo apt-get update	Para la actualización de los paquetes pre-instalados
2	sudo apt-get install apache*	Instala el servidor Apache y todas sus Dependencias
3	sudo apt-get install java*	Instala los paquetes de Java y sus Dependencias
4	sudo apt-get install squid3 sudo update-rc. d squid3 enable	Instalación y activación del paquete SQUID3 Proxy
5	sudo apt-get install squidGuard	Instalación del paquete de filtro de contenidos.
6	sudo apt-get install apache2	Instalación de paquete Apache 2 para levantar el servicio Web.

Nota: Tabla de instalación de paquetes de Linux Autor Marco Ortiz

2.23 CONFIGURACIÓN DE UN RASPBERRY PI COMO FILTRO DE CONTENIDOS CON SQUIDGUARD

1. Instalar Squid3 y activarlo al booteo del equipo

```
$ sudo apt-get install squid3
$ sudo update-rc.d squid3 enable
```

Use netstat para validar que Squid escuche por el puerto 3128

```
$ sudo netstat -antp |grep squid
$ sudo ps -aux |grep squid
```

2. Editar el archivo de configuración de Squid3

```
      $ sudo nano -c /etc/squid3/squid.conf

Descomentar las líneas: 1038 to 1040
      acl localnet src 10.0.0.0/8
      acl localnet src 172.16.0.0/12
      acl localnet src 192.168.0.0/16

Descomentar la línea: 1209    #http_access allow localnet

      http_access allow localnet

Descomentar la línea: 1613

      http_port 3128

Grabar y Salir.


$ sudo service squid reload
$ sudo service squid restart
$ sudo service iptables stop
```

3. Si desea monitorear los accesos puede digitar la siguiente línea:

```
$ sudo tail -f /var/log/squid3/access.log
```

4. Instalar SquidGuard una vez que ya se cuenta con Squid3

```
$ sudo apt-get install squidGuard
```

Una vez instalado SquidGuard, es necesario descargar listados de sitios y dominios ya definidos como blacklist y que están disponibles en la Web; por ejemplo, desde: **http://www.shallalist.de**

Sacar una copia de seguridad al archivo de configuración

```
$ cd /etc/squidguard
$ sudo cp squidGuard.conf squidGuard.conf.bak
$ sudo nano -c /etc/squidguard/squidGuard.conf
```

5. Ahora es necesario copiar las listas negras al directorio correspondiente, es necesario copiar todo el directorio BL descargado y copiarlo en la ruta:

```
       /var/lib/squidguard/db

Ahora es necesario dar permisos completos a los siguientes
directorios:

$ sudo chmod -R 755 /var/lib/squidguard/db/BL
$ ls /var/lib/squidguard/db/BL
```

6. Editar el archivo de configuración squidGuard.conf donde se crearán los accesos y las restricciones:

```
$ sudo nano -c /etc/squidguard/squidGuard.conf
```

Archivo de Configuración de SquidGuard:

```
# CONFIG FILE FOR SQUIDGUARD
# Caution: do NOT use comments inside { }
#
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

dest adult {
        domainlist BL/adult/domains
        urllist BL/adult/urls
}

dest azar {
        domainlist BL/azar/domains
        urllist BL/azar/urls
}

dest chat {
        domainlist BL/chat/domains
        urllist BL/chat/urls
}

dest descargas {
        domainlist BL/descargas/domains
        urllist BL/descargas/urls
}

dest hobby {
        domainlist BL/hobby/domains
        urllist BL/hobby/urls
}

dest religion {
        domainlist BL/religion/domains
        urllist BL/religion/urls
}

dest shopping {
        domainlist BL/shopping/domains
        urllist BL/shopping/urls
}

dest socialnet {
        domainlist BL/socialnet/domains
        urllist BL/socialnet/urls
```

```
}

dest spyware {
        domainlist BL/spyware/domains
        urllist BL/spyware/urls
}

dest violence {
        domainlist BL/violence/domains
        urllist BL/violence/urls
}
```

```
}

dest webmail {
        domainlist BL/webmail/domains
        urllist BL/webmail/urls
}

dest webphone {
        domainlist BL/webphone/domains
        urllist BL/webphone/urls
```

```
}
dest webtv {
        domainlist BL/webtv/domains
        urllist BL/webtv/urls
}

dest especificas {
      domainlist BL/especificas/domains
      urllist BL/especificas/urls
}

acl {
        default {
                pass !adult !azar !chat !descargas !hobby
!religion !shopping !spyware !violence !webmail !webphone !webtv
!especificas all
                redirect http://localhost/blocked.html
        }
 }
```

Se graba y se sale para luego:

7. Luego es necesario realizar la instalación de Apache 2 y será necesario crear la página de notificación del bloqueo al sitio que se intenta visitar. La página web de notificación de los bloqueos se debe alojar en la ruta: /var/www/html/

```
$ sudo apt-get install apache2
$ cd /var/www/html/
$ sudo nano blocked.html
```

8. Para casi finalizar se deben cambiar los permisos a las siguientes rutas:

```
$ sudo chown -R proxy:proxy /var/lib/squidguard/db
$ sudo chown -R proxy:proxy /var/log/squidguard
$ sudo chown -R proxy:proxy /usr/bin/squidGuard
```

9. Editar el archivo de configuración de Squid3 “squid.conf” y luego reiniciar los servicios

```
$ sudo nano -c /etc/squid3/squid.conf
```

Bajo la línea 4168 del archivo squid.conf, escribir lo siguiente:

```
url_rewrite_program /usr/bin/squidGuard
```

10. Ahora si es posible realizar pruebas iniciales con el proxy, inicialmente puede configurar en el navegador la dirección y puerto del proxy para efectos de prueba. Si las pruebas iniciales de navegación son satisfactorias puede continuar.

11. Para finalizar digitar las siguientes sentencias:

```
$ sudo squidGuard -C all
$ sudo squidGuard -C all
$ sudo chmod -R 777 /var/lib/squidguard/db/
$ sudo chown -R proxy:proxy /var/lib/squidguard/db
$ sudo service squid3 reload
```

2.24 MONITOREO Y CONTROL

Este proceso de seguimiento y control del proyecto debe realizarse de principio a fin. En cada etapa se debe controlar cada actividad realizada o realizada para determinar acciones correctivas. sin impactar significativamente el proyecto o de manera proactiva.

RESULTADOS

3.1. ANALISIS DE RESULTADOS

Una de las primeras preguntas de la investigación sobre la viabilidad del proyecto se refería al interés de los padres en un software que pudiera controlar el uso de Internet en el hogar. Los padres encuestados expresaron un 100% de interés en esta pregunta. Los padres son conscientes de los riesgos que corren sus hijos al utilizar Internet. Por ello, siempre hubo disposición para compartir experiencias y vivencias que sin duda contribuyeron al correcto desarrollo del proyecto.

El logro exitoso de los objetivos y el alcance del proyecto fue la base para la finalización del trabajo.

Estamos satisfechos con los resultados de nuestra primera prueba. Los probadores de sistemas enfatizan la facilidad de uso y la inversión requerida. El proyecto incluye:

• Un servidor, el hardware es una computadora de la serie Raspberry, esta máquina controla el tráfico de Internet.

• Las aplicaciones desarrolladas en Android pueden interactuar con servidores en la misma LAN. Las pruebas muestran que el software hace lo que está diseñado para hacer y detecta errores de software antes de su uso. Deberá revisar los resultados de las pruebas realizadas y buscar información sobre errores, anomalías o características no funcionales del Software.

Para el proyecto fueron considerados los siguientes parámetros de validación y evaluación:

- Interfaz gráfica del usuario (GUI) amigable y de fácil uso.
- Funcionalidad del servidor, servicios SQUID3 y Apache.
- Categorización de Reglas.
- Operatividad dentro de una red LAN montada en un domicilio.

Tabla 7

TABLA DE CRITERIOS DE MEDICIÓN

TABLA DE CRITERIOS DE MEDICIÓN

Alcances del Proyecto Factibilidad Técnica	Medición y evaluación de Alcances Criterios de Evaluación
La aplicación móvil está diseñada para aplicar el control del uso del internet enel hogar exclusivamente dentro de la misma red LAN	Como parte de los recursos requeridos, se instaló un servidorLinux en un Hardware Raspberry PI 4.Este equipo tiene levantados los servicios SQUID3, Apache 2, Iptables, PHP y SquidGUard para la implementación de reglas de acceso ainternet y la ejecución de Web Serviceque serán el puente entre la aplicaciónmóvil y los servicios Linux
Factibilidad Operacional	Criterios de Evaluación
La interfaz gráfica de usuario permite una fácil interacción entre el padre de familia y el sistema. Desde la aplicación móvil, el usuario podrá activar o desactivar reglas de control de acceso preestablecidas.	Luego de realizar la encuesta de factibilidad del proyecto se pudo identificar la necesidad de los padres de familia en contar con una aplicación que permita controlar el internet en elhogar.
Factibilidad Operacional	Criterios de Evaluación
El sistema permite realizar el control al uso del Internet en el hogar mediante la aplicación de reglas predefinidas	Fueron creados scripts con las reglas de navegación predefinidas dentro delservidor. La aplicación móvil ejecutarádichos scripts utilizando como medio de conexión los Web Service.
Factibilidad Operacional	Criterios de Evaluación
El servidor realizará el control del tráfico de internet y a él se conectará la aplicación móvil desarrollada en Android.	En el servidor fue instalado la distribución Raspbian de Linux y en élse levantaron los servicios SQUID3, Apache 2, Iptables, SquidGuard y PHP; para la implementación de las reglas de internet y ejecución de Web Service respectivamente

Nota: TABLA DE CRITERIOS DE MEDICIÓN

Algunas de estas características pueden medirse objetivamente, pero la mayoría requiere una evaluación subjetiva. Esto significa que aprovechar la experiencia de los empleados de una organización, el llamado juicio experto, es la forma más común, más rápida, más rentable y probablemente mejor refleja la realidad. Sin embargo, esto no permite comparaciones objetivas y, como es un problema de expertos más que de organizaciones, no puede reproducirse sistemáticamente y no contribuye a la maduración de la ingeniería de software.

Los resultados de la tabla de aceptación demuestran que el proyecto es factible y nos permiten concluir que el proyecto será aceptado por el usuario final y cumplirá con los estándares de muchos expertos. Por lo tanto, se consideró adecuado el sistema de seguimiento y control para el seguimiento del uso de dispositivos móviles por parte de menores y se aceptó y aprobó su instalación.

CAPITULO 4

4.1.CONCLUSIONES

En los últimos años el uso de Internet ha aumentado en nuestra sociedad. Usuarios de diferentes grupos de edad utilizan Internet para diferentes tareas. Internet se utiliza principalmente no sólo para navegar sino también para compartir noticias, imágenes y vídeos a través de redes sociales como Facebook, Twitter, Instagram y WhatsApp.

Las herramientas disponibles comercialmente no pueden imponer las restricciones necesarias en toda la red. El proyecto propuesto permitiría a los padres cerrar esta brecha de seguridad al permitirles imponer restricciones en el uso de Internet en casa y, por lo tanto, en cualquier dispositivo que se conecte a la red.

Las distintas etapas del proyecto dieron como resultado una herramienta fácil de usar con funciones adaptadas a las necesidades de los padres.

Finalmente, una vez completadas las pruebas de usuario, se determinó que el proyecto cumplía con las expectativas planteadas en términos de propósito y alcance del proyecto.

4.2 RECOMENDACIONES

- Realizar una campaña de concientización para que los padres ayuden a sus hijos a comprender los riesgos que enfrentan al navegar por Internet.
- Crear un plan de capacitación para cada usuario que utilizará el sistema.
- Supervise el rendimiento del software para obtener comentarios relevantes y mejorar sus proyectos en el futuro.
- Supervise periódicamente el espacio en disco del servidor.
- Cree un plan de recuperación considerando la posibilidad de una corrupción inminente del disco del servidor.
- Los padres deben comunicarse periódicamente con los menores sobre el uso apropiado de Internet y enseñarles las precauciones de seguridad que deben tomar

REFERENCIAS

academiaandroid. (2021). Android Studio v1.0: características y comparativa con Eclipse. ***Android Studio v1.0: características y comparativa con Eclipse*****.**

Agencia de Regulación y control de las telecomunicaciones. (2023). *www.arcotel.gob.ec.* Obtenido de ARCOTEL.

ANDROID. (2023). ANDROID ESTUDIO.

brontobytecloud. (2023). La importancia de la recuperación de datos. *La importancia de la recuperación de datos*.

CÓDIGO ORGÁNICO INTEGRAL PENAL. (2014). CÓDIGO ORGÁNICO INTEGRAL PENAL.

CPA PSICOLOGOS. (2023). *CPA PSICOLOGOS.* Obtenido de https://cpapsicologos.com/riesgos-del-uso-del-movil-en-menores-herramientas-de-control-parental-en-redes-sociales-y-moviles/

EventosTi.net. (2023). Riesgos Cibernéticos en la Era de Microsoft Teams.

EXPANSIÓN. (2023). Oversharing: ¿qué es y por qué puede ser peligroso? *Oversharing: ¿qué es y por qué puede ser peligroso?*

GONZALES, J. (2022). Control parental percibido y uso de Internet en adolescentes de 12 a 18 años en el Departamento Federal, Entre Ríos, Argentina.

Hacer Familia. (2023). Vamping, cuando el uso de internet roba sueño. *Vamping, cuando el uso de internet roba sueño*.

IBM. (2023). ¿Qué es el procesamiento del lenguaje natural (NLP)? *¿Qué es el procesamiento del lenguaje natural (NLP)?*

MAPFRE, F. (2023). Qué es el grooming y cuáles son sus fases? *Qué es el grooming y cuáles son sus fases?*

MARCA. (2023). Sexting: qué es y por qué es un riesgo esta práctica tan extendida. *Sexting: qué es y por qué es un riesgo esta práctica tan extendida*.

México, I. d. (2023). Ciberbullying. *Por Salud Mental ponle un alto al Ciberbullying*.

Oña, D. (2020). IMPLEMENTACIÓN DE UN PROTOTIPO DE CONTROL PARENTAL ENFOCADO EN. *IMPLEMENTACIÓN DE UN PROTOTIPO DE CONTROL PARENTAL ENFOCADO EN*.

POLI VERSO. (2023). INGENIERIA DE SOFTWARE. *INGENIERIA DE SOFTWARE*.

PREZI. (2023). *prezi*. Obtenido de https://prezi.com/zvxrcmrzoovt/cibernetica-social/

Sanguano, E. (2021). Análisis, diseño y evaluación de una propuesta tecnológica que mitigue el acceso a páginas web.

SARMINETO, R., AGUIRRE, A., & GUANIN, C. (2022). *ABUSO INFANTIL.* GUAYAQUIL: UNIVERSIDAD DE GUAYAQUIL , FACULTAD DE CIENCIAS Y FISICA.

Solorzano, E. (2020). PROTOTIPO DE UN CONTROL PARENTAL PARA EL INTERNET. *PROTOTIPO DE UN CONTROL PARENTAL PARA EL INTERNET*.

Tomas, J. (2016). *El gran libreo de Android.* México: Alfaomega .

Villanueva, B. (2021). *Acciones comprendidas sobre el control parental.*

APÈNDICE

SECCIÓN 2: CONTROL PARENTAL PERCIBIDO

Edad: …… Genero:

Cuestionario de Control Parental del Uso de Internet durante la Adolescencia.

Indica en qué medida consideras que es cierta cada una de las siguientes afirmaciones:

1=Totalmente falso; 2=Más bien falso; 3=Más bien cierto; 4=Totalmente cierto

	1	2	3	4
1. Cuando accedo a Internet en mi tiempo libre, mis padres me vigilan y echan un vistazo a la pantalla.				
2. Mis padres conocen las claves de acceso a mis cuentas de correo electrónico, redes sociales o programas de mensajería.				
3. En casa me han puesto algunas normas sobre lo que puedo o no puedo hacer en Internet.				
4. En casa me limitan los contenidos a los que puedo acceder en Internet, mediante filtros en el ordenador				
5. Mis adres me limitan las horas de uso de Internet (ya sea de palabra o configurando el ordenador).				
6. Mis padres revisan mis perfiles en las redes sociales (Tuenti, Facebook, Twitter, Instagram, por ejemplo).				
7. Mis padres conocen mis listas de contactos.				

SECCIÓN 3: ASPECTOS REFERIDOS AL USO DE INTERNET

Cuestionario de Utilización de Internet

Señala o encierra la respuesta que consideres correcta

1 ¿Hace cuánto tiempo vienes usando internet? a) Menos de un año b) De uno a tres años c) De tres a cinco años d) Más de cinco años e) No uso internet
2. ¿Desde dónde te conectas a internet mayormente? a) Casa b) Cabina de internet c) Colegio d) Casa de familiar e) Casa de amigo f) Otros……
3. ¿Con qué frecuencia te conectas a internet?

a) Todos los días b) Interdiario c) Una vez por semana d) Una vez al mes e) Otros……
4. ¿Cuánto tiempo permaneces conectado a internet? a) Media hora b) Una hora c) Dos horas d) Más de dos horas e) Otros……
5. ¿Qué nivel de destreza consideras que tienes en el uso de internet? a) Ingreso a Google y busco información. b) Construyo y público en páginas web. c) Ejecuto acciones como comprar o vender a través de internet. d) Ninguno
6. ¿Quién te enseñó principalmente el uso de internet? a) Padres b) Familiar (hermano, primo, tío) c) Profesor del colegio e) Amigos d) Yo mismo e) Empleado de cabina f) Otros……

Cuestionario de Finalidad de Uso de Internet

Señala con una cruz (X) la respuesta con la que te identifiques:

¿Qué haces cuando estás conectado a internet?					
	SIEMPRE	**CASI SIEMPRE**	**AVECES**	**CASI NUNCA**	**NUNCA**
1. Reviso mi correo electrónico					
2. Chateo (Messenger)					
3. Ingreso a mi Instagram, Facebook, Twitter u otras redes sociales					
4. Leo foros virtuales					
5. Participo en los foros virtuales					
6. Juego en red					
7. Veo videos en YouTube					
8. Escucho radio por internet					
9. Escucho noticias					
10. Bajo música					
11. Reviso blogs					
12. Leo diarios o					

revistas electrónicas para enterarme de las noticias					
13. Veo noticias					
14. Realizo búsquedas sencillas para realizar mis tareas					
15. Uso programas educativos o softwares para aprender un tema					
16. Realizo búsquedas para mis tareas en inglés u otro idioma					
17. Realizo búsquedas avanzadas para mis tareas escolares (por tipo de archivo, año de publicación, lugar)					
18. Uso diccionarios electrónicos					
19. Bajo libros de la biblioteca digital para mis tareas escolares					

Estadísticas obtenidas por encuestas

Edad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	12	9	10,3	10,3	10,3
	13	17	19,5	19,5	29,9
	14	12	13,8	13,8	43,7
	15	13	14,9	14,9	58,6
	16	14	16,1	16,1	74,7
	17	11	12,6	12,6	87,4
	18	11	12,6	12,6	100,0
	Total	97	100,0	100,0	

Genero

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	masculino	35	40,2	40,7	40,7
	femenino	51	58,6	59,3	100,0
	Total	86	98,9	100,0	
Perdidos		1	1,1		
Total		97	100,0		

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. típ.
Edad	97	12	18	14,95	1,922
N válido (según lista)	97				

Cuando accedo a Internet en mi tiempo libre, mis padres me vigilan y echan un vistazo a la pantalla.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	52	59,8	59,8	59,8
	2	22	25,3	25,3	85,1
	3	9	10,3	10,3	95,4
	4	4	4,6	4,6	100,0
	Total	87	100,0	100,0	

Mis padres conocen las claves de acceso a mis cuentas de correo electrónico, redes sociales oprogramas de mensajería.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	62	71,3	71,3	71,3
	2	8	9,2	9,2	80,5
	3	5	5,7	5,7	86,2
	4	12	13,8	13,8	100,0
	Total	87	100,0	100,0	

En casa me han puesto algunas normas sobre lo que puedo o no puedo hacer en Internet.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	45	51,7	51,7	51,7
	2	12	13,8	13,8	65,5
	3	15	17,2	17,2	82,8
	4	15	17,2	17,2	100,0
	Total	87	100,0	100,0	

En casa me limitan los contenidos a los que puedo acceder en Internet, mediante filtros en el ordenador.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	65	74,7	74,7	74,7
	2	9	10,3	10,3	85,1
	3	7	8,0	8,0	93,1
	4	6	6,9	6,9	100,0
	Total	87	100,0	100,0	

Mis padres me limitan las horas de uso de Internet (ya sea de palabra o configurando el ordenador).

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	55	63,2	63,2	63,2
	2	11	12,6	12,6	75,9
	3	12	13,8	13,8	89,7
	4	9	10,3	10,3	100,0
	Total	87	100,0	100,0	

En casa me limitan los contenidos a los que puedo acceder en Internet, mediante filtros en el ordenador.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	65	74,7	74,7	74,7
	2	9	10,3	10,3	85,1
	3	7	8,0	8,0	93,1
	4	6	6,9	6,9	100,0
	Total	87	100,0	100,0	

Mis padres me limitan las horas de uso de Internet (ya sea de palabra o configurando el ordenador).

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	55	63,2	63,2	63,2
	2	11	12,6	12,6	75,9
	3	12	13,8	13,8	89,7
	4	9	10,3	10,3	100,0
	Total	87	100,0	100,0	

¿Hace cuánto tiempo vienes usando internet?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	De tres a cinco años	16	18,4	18,4	18,4
	De uno a tres años	21	24,1	24,1	42,5
	Más de cinco años	50	57,5	57,5	100,0
	Total	87	100,0	100,0	

¿Desde dónde te conectas a internet mayormente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casa	84	96,6	96,6	96,6
	Casa de amigo	2	2,3	2,3	98,9
	Desde cualquier lugar que tenga red de wifi, desde mi celular	1	1,1	1,1	100,0
	Total	87	100,0	100,0	

¿Con qué frecuencia te conectas a internet?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Inter diario	4	4,6	4,6	4,6
	Todos los días	82	94,3	94,3	98,9
	Una vez por semana	1	1,1	1,1	100,0
	Total	87	100,0	100,0	

Cuánto tiempo permaneces conectado a Internet

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	10 horas	1	1,1	1,1	1,1
	10 minutos	1	1,1	1,1	2,3
	6 horas	1	1,1	1,1	3,4
	Dos horas	6	6,9	6,9	10,3
	Más de dos horas	57	65,5	65,5	75,9
	Me puedo llegar a quedar más de 3 horas, dependiendo de los días que tenga que hacer trabajos de la escuela.	1	1,1	1,1	77,0
	Media hora	5	5,7	5,7	82,8
	Todo el tiempo	5	5,7	5,7	88,5
	Una hora	10	11,5	11,5	100,0
	Total	87	100,0	100,0	

¿Qué nivel de destreza consideras que tienes en el uso de internet?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Construyo y público en páginas web	7	8,0	8,0	8,0
	Ejecuto acciones como comprar o vender a través de internet	5	5,7	5,7	13,8
	Ingreso a Google y busco información	51	58,6	58,6	72,4
	Ninguno	24	27,6	27,6	100,0
	Total	87	100,0	100,0	

¿Quién te enseñó principalmente el uso de internet?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Amigos	6	6,9	6,9	6,9
	Familiar (hermano, primo, tío)	24	27,6	27,6	34,5
	Padres	11	12,6	12,6	47,1
	Un poco de todos	1	1,1	1,1	48,3
	Yo mismo	45	51,7	51,7	100,0
	Total	87	100,0	100,0	

Reviso mi correo electrónico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	3	3,4	3,4	3,4
	2	8	9,2	9,2	12,6
	3	40	46,0	46,0	58,6
	4	28	32,2	32,2	90,8
	5	8	9,2	9,2	100,0
	Total	87	100,0	100,0	

Chateo (Messenger)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	15	17,2	17,2	17,2
	2	12	13,8	13,8	31,0
	3	29	33,3	33,3	64,4
	4	16	18,4	18,4	82,8
	5	15	17,2	17,2	100,0
	Total	87	100,0	100,0	

Ingreso a mi Instagram, Facebook, Twitter u otras redes sociales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	61	70,1	70,1	70,1
	2	17	19,5	19,5	89,7
	3	8	9,2	9,2	98,9
	4	1	1,1	1,1	100,0
	Total	87	100,0	100,0	

Leo foros virtuales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	5	5,7	5,7	5,7
	2	11	12,6	12,6	18,4
	3	29	33,3	33,3	51,7
	4	28	32,2	32,2	83,9
	5	14	16,1	16,1	100,0
	Total	87	100,0	100,0	

Participo en los foros virtuales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	6	6,9	6,9	6,9
	2	5	5,7	5,7	12,6
	3	27	31,0	31,0	43,7
	4	30	34,5	34,5	78,2
	5	19	21,8	21,8	100,0
	Total	87	100,0	100,0	

Juego en red

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	23	26,4	26,4	26,4
	2	16	18,4	18,4	44,8
	3	24	27,6	27,6	72,4
	4	14	16,1	16,1	88,5
	5	10	11,5	11,5	100,0
	Total	87	100,0	100,0	

Veo videos en YouTube

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	36	41,4	41,4	41,4
	2	25	28,7	28,7	70,1
	3	21	24,1	24,1	94,3
	4	3	3,4	3,4	97,7
	5	2	2,3	2,3	100,0
	Total	87	100,0	100,0	

Escucho radio por internet

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	2	3	3,4	3,4	3,4
	3	23	26,4	26,4	29,9
	4	30	34,5	34,5	64,4
	5	31	35,6	35,6	100,0
	Total	87	100,0	100,0	

Escucho noticias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	3	3,4	3,4	3,4
	2	11	12,6	12,6	16,1
	3	33	37,9	37,9	54,0
	4	27	31,0	31,0	85,1
	5	13	14,9	14,9	100,0
	Total	87	100,0	100,0	

Bajo música

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	33	37,9	37,9	37,9
	2	22	25,3	25,3	63,2
	3	22	25,3	25,3	88,5
	4	7	8,0	8,0	96,6
	5	3	3,4	3,4	100,0
	Total	87	100,0	100,0	

Reviso blogs

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	9	10,3	10,3	10,3
	2	4	4,6	4,6	14,9
	3	32	36,8	36,8	51,7
	4	27	31,0	31,0	82,8
	5	15	17,2	17,2	100,0
	Total	87	100,0	100,0	

Leo diarios o revistas electrónicas para enterarme de las noticias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	2	2,3	2,3	2,3
	2	9	10,3	10,3	12,6
	3	35	40,2	40,2	52,9
	4	26	29,9	29,9	82,8
	5	15	17,2	17,2	100,0
	Total	87	100,0	100,0	

Veo noticias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	5	5,7	5,7	5,7
	2	16	18,4	18,4	24,1
	3	32	36,8	36,8	60,9
	4	23	26,4	26,4	87,4
	5	11	12,6	12,6	100,0
	Total	87	100,0	100,0	

Realizo búsquedas sencillas para realizar mis tareas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	41	47,1	47,1	47,1
	2	27	31,0	31,0	78,2
	3	17	19,5	19,5	97,7
	4	2	2,3	2,3	100,0
	Total	87	100,0	100,0	

Uso programas educativos o softwares para aprender un tema

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Validos	1	18	20,7	20,7	20,7
	2	20	23,0	23,0	43,7
	3	31	35,6	35,6	79,3
	4	13	14,9	14,9	94,3
	5	5	5,7	5,7	100,0
	Total	87	100,0	100,0	

Realizo búsquedas para mis tareas en inglés u otro idioma

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1	40	46,0	46,0	46,0
	2	18	20,7	20,7	66,7
	3	20	23,0	23,0	89,7
	4	4	4,6	4,6	94,3
	5	5	5,7	5,7	100,0
	Total	87	100,0	100,0	