UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

ESTUDIO COMPARATIVO DE APLICACIONES LIBRES PARA CONTROL PARENTAL, AÑO 2023.

AUTOR:

JAIRO LENIN UCHUBANDA GUAMARICA

DIRECTORA:

ING. MÓNICA BONILLA

GUARANDA – ECUADOR

2023

TEMA DEL PROYECTO DE INVESTIGACIÓN

ESTUDIO COMPARATIVO DE APLICACIONES LIBRES PARA CONTROL PARENTAL, AÑO 2023.

AGRADECIMIENTO

Agradezco a la “Universidad Estatal de Bolívar”, a los docentes de la carrera de Ingeniería en Software por haberme compartido sus conocimientos a lo largo de mi preparación profesional, de manera especial, a la Ing. Mónica Bonilla directora de mi proyecto de investigación por la entrega y el apoyo que me ha brindado para la realización de este trabajo, también agradecer a mis pares académicos Lic. Edgar Rivadeneira y Dra. Edelmira Guevara, agradezco infinitamente a mis padres quienes han sido muy importantes en mi formación académica por su comprensión, apoyo incondicional que cada día me motivan a cumplir con mis metas.

Jairo Lenin Uchubanda Guamarica

DEDICATORIA

El presente trabajo de titulación está dedicado a mis queridos padres Bolívar Uchubanda y Rosa Guamarica por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy, a mis hermanos, Kevin y Bryan por estar siempre presentes y brindarme su apoyo moral a lo largo de mi formación académica.

Jairo Lenin Uchubanda Guamarica

CERTIFICADO DE VALIDACIÓN

Ing. Mónica Bonilla, Lic. Edgar Rivadeneira y Dra. Edelmira Guevara, en su orden Directora y Pares Académicos del Trabajo de Integración Curricular "ESTUDIO COMPARATIVO DE APLICACIONES LIBRES PARA CONTROL PARENTAL, AÑO 2023" desarrollado por el señor Uchubanda Guamarica Jairo Lenin.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 09 de junio del 2023

Firmado electrónicamente por:
MONICA ELIZABETH BONILLA MANOBANDA

Ing. Mónica Bonilla
Directora

Firmado electrónicamente por:
EDGAR PATRICIO RIVADENEIRA RAMOS

Lic. Edgar Rivadeneira
Par Académico

Firmado electrónicamente por:
EDELMIRA LILA GUEVARA INIGUEZ

Dra. Edelmira Guevara
Par Académico

DERECHOS DE AUTOR

Yo, **Jairo Lenin Uchubanda Guamarica** portador de las cédulas de identidad **N° 0250350659** respectivamente**,** en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación: "**ESTUDIO COMPARATIVO DE APLICACIONES LIBRES PARA CONTROL PARENTAL, AÑO 2023",** modalidad Trabajo de Integración Curricular, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedo a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de titulación el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Firmado electrónicamente por:
JAIRO LENIN
UCHUBANDA GUAMARICA

Jairo Lenin Uchubanda Guamarica
CI. 0250350659

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Las aplicaciones de control parental están diseñadas tradicionalmente para bloquear y filtrar el acceso a determinados sitios de Internet o monitorear la actividad a través de dispositivos tecnológicos, hoy, sin embargo, ofrecen más flexibilidad y más funcionalidades para adaptar mejor estas herramientas a los distintos entornos y necesidades que los padres encuentran a sus hijos e hijas en su cada vez más frenética vida digital.

Es importante controlar el acceso a internet para evitar que los menores de edad accedan a contenidos que no son adecuados para ellos, además de la protección frente a los depredadores en línea, el ciberacoso o el ciberacoso y el troleo son muy comunes, los menores de edad suelen ser las principales víctimas, los delincuentes usan aplicaciones y sitios web para contactar a menores y fingir ser amigos para aprovecharse de ellos, pedirles que proporcionen información personal como nombres, direcciones y números de teléfono.

Lo que se desea lograr en la investigación es conocer mediante pruebas usabilidad la eficiencia que tienen algunas aplicaciones libres para control parental, para ello, se investigaron aplicaciones existentes en el mercado y a elegirlas para de esta manera identificar sus funciones, analizando de manera profunda ciertos criterios específicos de los controles como el filtrado del contenido y localización, el presente proyecto se encuentra estructurado en cinco capítulos.

En el capítulo I, este capítulo detalla la descripción del problema, formulación del problema, preguntas de investigación, justificación, objetivos, hipótesis y variables.

En el capítulo II, contiene los antecedentes, fundamentación científica, fundamentación conceptual y fundamentación legal

En el capítulo III, contiene la metodología, tipo de investigación, enfoque de investigación, métodos de investigación, técnicas e instrumentos de recopilación de datos, universo, población, muestra y el procesamiento de la información.

En el capítulo IV: Presenta el resultado de la investigación.

RESUMEN

Actualmente existen diferentes riesgos en internet a los que se enfrenta los niños y adolescentes desde el ciberacoso hasta el sexting y los padres no pueden estar siempre controlando lo que visualizan sus hijos la falta de este control puede llegar a ser muy perjudicial con el tiempo. El objetivo del presente estudio es realizar un estudio comparativo de aplicaciones libres para el control parental para lo cual se determinó diferentes aplicaciones tanto para dispositivos Android como para PC y se estableció los parámetros que serían probados para verificar sus funcionalidades, además se revisó casos del uso de dichas aplicaciones que fueron desarrolladas en el Ecuador. Para el desarrollo del mismo se realizó un estudio descriptivo, bibliográfico con un enfoque cualitativo, se establecieron las características a ser probadas en cada aplicación y mediante un cuadro de valoración se estableció la mejor aplicación con base en sus características. Los resultados obtenidos de la investigación de los casos de uso muestran que es necesario una aplicación que ayude a los padres en el control parental, además las pruebas realizadas a las aplicaciones muestran que la mejor aplicación de control parental con licencia gratuita para dispositivos Android sería SecureKids y para PC la mejor aplicación que cumple con la mayoría de características sería Microsoft Family Safety, por lo tanto, se concluye que la aplicación SecuriKids dispone de las mejores características para realizar de manera eficiente el control parental de los niños y adolescentes

Palabras Clave: aplicaciones parentales, ciberdelitos, dispositivos inteligentes, ciberseguridad

ABSTRACT

Currently, there are different risks on the Internet that children and adolescents face, from cyberbullying to sexting, and parents cannot always control what their children view. The lack of this control can be very harmful over time. The objective of this study is to carry out a comparative study of free applications for parental control, for which different applications for both Android and PC devices were determined and the parameters that would be tested to verify their functionalities were established, in addition use cases were reviewed. of said applications that were developed in Ecuador. For its development, a descriptive, bibliographical study was carried out with a qualitative approach, the characteristics to be tested in each application were established and the best application based on its characteristics was established through an evaluation table. The results obtained from the investigation of the use cases show that an application that helps parents in parental control is necessary, in addition, the tests carried out on the applications show that the best parental control application with a free license for Android devices would be SecureKids. and for PC the best application that meets the majority of features would be Microsoft Family Safety, therefore, it is concluded that the SecuriKids application has the best features to efficiently perform parental control of children and adolescents

Keywords: parental apps, cybercrime, smart devices, cybersecurity

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1 Descripción del Problema

Con la pandemia del COVID-19 que inició en el año 2019 todas las personas se debieron adaptar a los nuevos cambios, incluidos los estudiantes de los diferentes centros educativos de nuestro país Ecuador, donde se empezó a ejecutar la actividad de enseñanza-aprendizaje en línea por lo que las familias compraron computadoras e instalaron internet, pero al tener tanta libertad sin ningún tipo de control.

Se usaron los recursos tecnológicos no solo para apoyar el proceso educativo, sino también para ingresar a contenidos inapropiados para adolescentes como espacios visuales como violencia, pornográficas, apuestas, mal uso de redes sociales, u otra información no apta para su edad, generando algunos inconvenientes como déficit de atención, depresión, aislamiento, entre otros.

Sobre las prácticas de riesgo en la red, el estudio de Gómez et al. (2017) revela que contactar con desconocidos es el comportamiento más frecuente entre los adolescentes, y hay un aumento en el número de usuarios que tienen menos control sobre su uso de Internet.

Algunos de los riesgos que suponen un mal uso de Internet es que hay personas que buscan aprovecharse de los demás, hay contenidos no aptos para niños y jóvenes, no todo lo que se dice en Internet es verdad, no todo el mundo es quien dice ser, de hecho, no suele serlo ciberbullying, grooming, sexting.

Además, los niños, niñas y adolescentes enfrentan otros riesgos al navegar libremente en Internet, como el acceso a sitios web de contenido para adultos con contenidos sexuales, así como contenidos de apuestas, loterías y esquemas piramidales o cualquier otra forma sencilla de ganar dinero pueden ser adictivos, otro riesgo es comunicarse con personas que no conocen, que pueden engañar, seducir, abusar o incluso cometer actos ilegales al solicitar información personal como nombre, dirección, número de teléfono, etc. (García Piña, 2008)

Con base en lo anterior, podemos decir que, es evidente que existen muchos riesgos en internet y es necesario una aplicación de control parental que ayude a los padres a monitorizar lo que sus hijos ven mientras están conectados a internet.

1.2 Formulación del Problema

¿Cuáles son las características más relevantes de las aplicaciones informáticas de control parental de acceso libre en entornos web y móvil para el control de seguridad de adolescentes?

1.3 Preguntas de Investigación

- ¿Cuáles son las aplicaciones informáticas de control parental de licencia gratuita para el control de la seguridad integral de adolescentes en ambientes digitales?
- ¿Cuáles son los parámetros a tener en cuenta para realizar la comparación de las aplicaciones informáticas para control parental de licencia gratuita?
- ¿Cuáles fueron los resultados obtenidos de los casos del uso de las aplicaciones libres para control parental desarrollados en el Ecuador?

1.4 Justificación

Este proyecto nace de la necesidad de los padres de familia de conocer sobre la existencia y funcionamiento de las aplicaciones de control parental, que evitan que sus hijos queden expuestos a los diversos riesgos que existen en internet.

Algunos riesgos son los siguientes: ciberbullying, adicción a Internet, sexting, publicar datos privados, compras online sin permiso, contenido inadecuado en internet, grooming.

Para evitar este tipo de riesgos, se revisarán las aplicaciones de control parental con licencia gratuita más utilizadas y se realizará una comparación de sus características junto a una valoración por cada una, destacando la mejor, basándonos en su funcionalidad.

Las aplicaciones parentales permiten a los padres supervisar y adecuar el tiempo de uso y el contenido al que tienen acceso sus hijos mientras están conectados a internet, son muy útiles para llevar un control de uso que le dan los estudiantes al internet permitiendo monitorizar, evitar el contacto con desconocidos, limitar el tiempo de uso de la computadora y el móvil, reduce la posibilidad de acceder a sitios inapropiados.

Los beneficiarios de esta investigación son los padres de familia quienes podrán comprender cuáles son los riesgos digitales a los que están expuestos sus hijos cada vez que se conectan a internet y, a su vez, podrán supervisar lo que pueden hacer de esta manera podrán conocer las páginas web que visitan sus hijos y determinar los posibles peligros que enfrentan, otros beneficiarios son los niños que evitaran estar expuestos a contenidos que puedan perjudicar a su a los mismos.

La siguiente propuesta aportará a la línea de investigación de la carrera de Software: Ingeniería De Software, Redes y Telecomunicaciones en la sub línea de Pruebas y aseguramiento de la calidad del software, redes y telecomunicaciones.

1.5 Objetivos:

1.5.1 Objetivo General

Realizar un estudio comparativo de aplicaciones libres para el control parental, año 2023

1.5.2 Objetivos Específicos

- Conocer las aplicaciones libres para control parental más utilizadas en la seguridad de los adolescentes
- Establecer los parámetros o indicadores de comparación de las aplicaciones libres para control parental considerando sus funcionalidades
- Analizar casos del uso de las aplicaciones libres para control parental desarrollados en el Ecuador

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes Nacionales

La tesis de Delgado (2021) “Herramienta tecnológica de control parental sobre los contenidos de Internet y su aplicación como apoyo en el desempeño académico de los estudiantes de la UEF “Tarqui” de Manta el objetivo es diagnosticar el control parental sobre los contenidos tratados en Internet por cuenta de los menores de edad, determinar la información necesaria para la aplicación de este control y determinar la viabilidad de implementar medios técnicos de control parental, el método utilizado es un análisis cualitativo y enfoque cuantitativo. perteneciente al tipo investigativo y propositivo; la encuesta se aplicó a 160 delegados y 160 estudiantes, con una muestra de 140 delegados y 140 estudiantes respectivamente; También se examinaron 40 docentes del nivel de licenciatura y los resultados obtenidos permitieron establecer que, a pesar de las acciones realizadas por los representantes para controlar las actividades de los menores en Internet, aún se necesita una herramienta adecuada para implementarlo en tiempo real. control para dar respuesta a los tiempos que vivimos a través de programas o aplicaciones informáticas.

En el trabajo de Benetazzo & Sotomayor (2021) “Implementación de una aplicación para control parental en dispositivos inteligentes” donde el objetivo fue desarrollar un sistema que permite a los padres controlar el uso de dispositivos inteligentes Android de sus hijos para lo cual se comenzó con un estudio para averiguar cómo los padres controlan actualmente el uso de dispositivos por parte de sus hijos, para lograr este objetivo primero se efectuó una encuesta para determinar cómo los padres de familia controlan actualmente el uso de los dispositivos de sus hijos así como su utilidad una vez puesto a prueba el sistema y en la evaluación comparativa con otros sistemas similares, se concluyó que la aplicación desarrollada puede administrar y controlar de manera efectiva el uso de dispositivos inteligentes Android.

En la tesis de Coello & Saltos (2022) “Análisis práctico comparativo de herramientas de control parental con licencias gratuitas y pagadas para la seguridad integral a menores de edad en ambientes digitales en la ciudad de Guayaquil” se identificaron diferentes herramientas de control parental para encontrar aquellas que ofrecen más seguridad en términos de funcionalidad y costo para ayudar a reducir ciertos tipos de riesgo cibernético, se evaluaron varias herramientas de control parental, tanto gratuitas como pagas, de las cuales Qustodio, Norton Family, Secure Kids y FamiSafe seleccionaron dos para cada licencia, y luego pusieron estas herramientas a disposición de las familias de padres para experimentar los beneficios de usarlas y lo que hacen, y finalmente, cuando los resultados del análisis muestran que estas herramientas cumplen con cada una de sus funciones, se utilizó de encuesta para demostrar la factibilidad del control parental frente a los padres, para que cuando reciban la herramienta, conozcan todos los beneficios. ellos proveen. la oferta

2.1.2 Antecedentes Internacionales

Sánchez (2020) desarrolló el trabajo de investigación denominado “Herramienta de control parental basada en software libre”, Trabajo Fin de Grado. El objetivo del presente estudio fue la creación de una herramienta de control parental, dicha aplicación solo será accesible por los usuarios registrados en ella desde la misma, Los usuarios pueden bloquear, desbloquear y listar sus páginas web bloqueadas para facilitar la tarea, la propia aplicación recomienda algunas páginas web que se consideran inapropiadas para menores de edad, los usuarios también pueden agregarlas a su lista de bloqueo, como resultado de dicha aplicación ha sido encapsulada y desplegada también en su distribución gracias a los servicios que ofrece Docker y su nube.

Coronel (2018) desarrolló el trabajo de investigación denominado “Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de internet “, Informe de Proyecto de Maestría El propósito del estudio fue ofrecer educación que ayudará a aumentar el conocimiento sobre el control parental que pudiera ser utilizado para reducir los riesgos que enfrentan los niños del Colegio Internacional Fundación Liceo en el año 2018, para desarrollar un estudio descriptivo utilizando métodos cuantitativos, el cual también se llevó a

cabo . La muestra estuvo conformada por 20 padres de familia de los estudiantes quienes utilizaron una herramienta de encuesta que diagnosticó conocimiento de tecnología y conocimiento de herramientas de control parental, luego se les presentó un video sobre los riesgos y las herramientas de control parental como resultados el 70% consideró que representa un alto riesgo, el 100% manifestaron interés en conocer sobre las herramientas de control parental y el 75% tuvo como preferencia el uso de este control parental.

Moyano et al. (2017) desarrollaron el trabajo de investigación denominado "Análisis de herramientas usadas para el control parental en dispositivos móviles con acceso a internet", el enfoque del proyecto de investigación está basado en el análisis de las aplicaciones de control parental como herramientas de protección frente a las numerosas amenazas a las que se exponen niños, niñas y adolescentes que usan redes sociales, juegos e internet como resultados de acuerdo al análisis realizado a las herramientas de control parental como resultado se determina que la herramienta Qustodio es la mejor aplicación para realizar un control parental.

Villanueva & Serrano (2019) desarrollaron el tema de investigación denominado "Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género". Es un estado descriptivo relacional de tipo transversal. La muestra se compone de 163 alumnos de 12 a 16 años, se empleó Cuestionario sociodemográfico en el presente estudio, se ha encontrado que en torno al 32% de los adolescentes muestran una frecuencia de conexión a internet elevada y un porcentaje igualmente destacable lo hace en horas nocturnas

2.2 Marco Científico

2.2.1 Metodología site-centric

Esta metodología se basa en el registro de las actividades de los usuarios en el sitio web mediante herramientas diseñadas para recopilar y analizar dichas actividades, los principales métodos orientados al sitio se basan en el análisis de archivos LOG de servidores web o instalaciones modificadas. (Alonso Conde, s.f.)

Entre las funcionalidades permite:

- Monitorear online el comportamiento de las vistas a un sitio de sus contenidos en particular

- Identificar qué porcentaje del total está compuesto por nuevas Visitas
- Identificar el origen de las visitas, segmentación entre tráfico directo (visitantes que llegan directamente al sitio introduciendo la dirección en la barra del navegador o desde marcadores guardados), referencias
- Controle la velocidad de carga del contenido de su sitio web.
- Seguimiento de la conversión del sitio web (objetivos alcanzados en función del contenido configurado, visitas, formularios de contacto, compras, etc.)
- Determine el tipo de dispositivo que genera el tráfico.
- Administrar el sitio web para mejorar su rendimiento de acuerdo con los objetivos del sitio web. (IAB Chile, 2012)

2.2.2 Metodología OSSTMM (Open Source Security Testing Methodology Manual)

Es un estándar reconocido y extendido en las auditorías de seguridad para evaluar la seguridad de los sistemas informáticos, esta guía proporciona un marco que describe las fases a seguir al realizar una auditoría o sello de seguridad, y ha sido desarrollado gracias al consenso un gran grupo de expertos internacionales en seguridad informática que colaboran para crear y mantener esta metodología. (Ciberseguridad, s.f.)

- Esto también lo hace ideal para probar computación en la nube, infraestructura virtual, middleware de mensajería, infraestructura y dispositivos móviles.
- Y también, sitios de alta seguridad, recursos humanos, procesamiento de datos confiable y cualquier proceso lógico que cubra todos los canales y requiere varios tipos de controles de seguridad.
- Un conjunto de métricas de superficie de ataque denominada ámbar que proporciona una herramienta poderosa y altamente flexible que puede proporcionar una representación gráfica del estado
- Se integra bien con el "tablero" para beneficiar a la gerencia y a los empleados internos
- La gestión de riesgos de informes cuantitativos se puede realizar en función de los resultados de la auditoría OSSTMM, lo que da como resultado mejores resultados a través de resultados más precisos y sin errores.

2.3 Marco Conceptual

Aplicación de Control Parental

Un sistema de control parental es una herramienta que permite a los padres controlar y/o limitar el contenido a los que sus hijos puedan acceder en internet desde sus dispositivos, ya sean ordenadores, móviles o tabletas. (Securekids, 2015)

La tecnología digital es parte fundamental en la educación de niños, niñas y adolescentes en los colegios y hogares, es cada vez más habitual el uso de dispositivos tecnológicos desde edades tempranas y el acceso a recursos formativos a través de internet. Por todo ello, es importante que desde pequeños aprendan a utilizar la tecnología de forma responsable, que les ayude a sentirse intrépidos y les permita aprovechar al máximo las posibilidades del mundo digital.

Además de ayudar a promover hábitos responsables, las familias cuentan con herramientas útiles para ayudar a mantener a sus hijos e hijas seguros en Internet. Por ejemplo, aplicaciones de control parental.

Diseñadas para ayudar a los padres a monitorear la actividad en Internet de sus hijos adolescentes, estas aplicaciones ofrecen muchos beneficios, desde la capacidad de filtrar contenido inapropiado hasta la capacidad de limitar el tiempo de pantalla.

A continuación, se presentan las mejores aplicaciones para control parental con licencia gratuita:

1) G*oogle Family Link.*

Family Link es una aplicación de control parental creada por Google, y sirve para que los padres puedan controlar de forma remota el dispositivo Android de sus hijos, funciona a través de la cuenta de Google. (Fernández, 2019)

Características

- Restringir el contenido
- Ver el tiempo de uso y establecer límites
- Bloquear aplicaciones o permisos
- Poner límites diarios del uso del dispositivo
- Ver las aplicaciones instaladas recientemente
- Protección de la configuración
- Ver la última ubicación del dispositivo del hijo

Sistemas operativos compatibles: Android

2) SecureKids

SecureKids es un control parental para Android con el que los padres y madres pueden gestionar y controlar los dispositivos de sus hijos e hijas de forma remota, con el control parental puedes bloquear aplicaciones, páginas web, o incluso bloquear temporalmente todo el dispositivo de tu hijo/a de una forma simple y clara. (Grupo Deidev, 2023)

Características

- Filtrado de Páginas Web.
- Bloqueo de Aplicaciones.
- Bloquear llamadas.
- Protección de la configuración
- Geolocalización.
- Crear alarmas
- Crear descansos
- Emergencias
- Configuración remota

Sistemas operativos compatibles: Android

3) Microsoft Family Safety

Microsoft Family Safety es un servicio gratuito de control parental y supervisión desarrollado por Microsoft, permite a los padres estar al tanto de lo que hacen los menores en su ordenador. (PcHardwarePro, 2023)

Características

- Límites de tiempo de pantalla
- Límites de aplicaciones y juegos
- Límites de dispositivos (Windows y Xbox)
- Solicitudes de tiempo de pantalla
- Resúmenes de actividades
- Filtros de aplicaciones y juegos
- Protección de la configuración
- Filtros web y de búsqueda
- Compartir ubicación
- Lugares guardados

Sistemas operativos compatibles: Windows y Xbox

4) KidsGuard.

Kidsguard es una herramienta de monitoreo de teléfonos inteligentes, está diseñado para ayudar a los padres a realizar un seguimiento de las actividades de sus hijos en sus teléfonos inteligentes, por lo tanto, ofrece numerosas formas de rastrear un teléfono inteligente desde el seguimiento de redes sociales, incluso ubicación GPS en tiempo real. (Hamed , 2022)

Características

- Aviso de nueva versión
- Ubicación en tiempo real
- Historial de ubicaciones
- Protección de la configuración
- Bloqueo web
- Uso de aplicaciones
- Bloquear pantalla
- Bloqueo de aplicaciones

Sistemas operativos compatibles: iOS, Android.

5) Kidlogger.

Es un software de control parental compatible con el sistema operativo más utilizado en el mundo sirve para obtener toda la información sobre la actividad de PC, móvil o tableta de sus hijos. (kidlogger, 2023)

Características

- Monitoreo de actividades
- Los agentes de monitoreo están protegidos con contraseña
- Soporte de monitoreo de múltiples usuarios
- Capturas de pantalla
- Bloqueo de aplicaciones
- Limitador de tiempo en pantalla

Sistemas operativos compatibles: Windows, MacOS y BlackBerry

6) Norton Family.

Norton Family es un servicio estadounidense de control parental basado en la nube, Norton Family tiene como objetivo "fomentar la comunicación" entre los padres y

las actividades en línea de sus hijos, las actividades de la computadora son monitoreadas por el cliente de software y los informes se publican en línea. (Hmong, s.f.)

Características

- Filtro web
- Bloquear aplicaciones
- Configuración de pin de seguridad
- Contactos de emergencia

Sistemas operativos compatibles: Android

7) Kaspersky Safe Kids.

Kaspersky Safe Kids es un sistema de control parental completo y rentable, para ordenadores y dispositivos móviles, que no limita el número de dispositivos que se pueden supervisar. (kaspersky, 2023)

Características

- Filtrar contenido web inapropiado
- Establecer límites de tiempo de uso para el dispositivo del hijo
- Bloqueo de aplicaciones
- Búsqueda segura en YouTube
- Protección de la configuración
- Informes

Sistemas operativos compatibles: iOS, Android.

8) Locategy.

Es un programa que combina funciones de control parental con integraciones de GPS, es por ello que se trata de una de las aplicaciones más versátiles para controlar el uso de dispositivos electrónicos por parte de niños y adolescentes. (Parentalia, 2023)

Características

- Localización
- Informes de uso
- Histórico de ubicación
- Bloquear sitios web
- Botón de emergencia

- Limitar uso de aplicaciones y de tiempo en pantalla

Sistemas operativos compatibles: iOS, Android.

Ciberbullying

Se trata de emplear cualquiera de las posibilidades de uso de las nuevas tecnologías de la información y de la comunicación para hostigar con ensañamiento a su víctima. (Prados & Fernández, 2007)

Control parental

Los controles parentales, mejor conocidos como controles parentales, generalmente se refieren a sistemas que restringen o impiden que los menores accedan a un dispositivo o su contenido, para ello, se utilizan varios sistemas de pulsación de teclas, ya sea alfanuméricos o combinaciones de teclas por parte del tutor legal del menor, suelen ser los padres y adultos los que se encargan de utilizar el equipo en cuestión. El objetivo es evitar que los menores accedan a contenidos inadecuados, o realice acciones como comprar contenido o suscribirse a servicios, compartir información personal o confidencial públicamente los sistemas de control parental varían según la computadora, la tableta, el teléfono inteligente, la consola, el televisor y el formato de la aplicación, red social, también del tipo de información que se desea controlar. (ElisaYuste, 2019)

Clasificación de las aplicaciones de control parental

De acuerdo con Sipbench (2017) las aplicaciones de control Parental se pueden clasificar según sea el uso específico que se le dé:

- Instale en su computadora o descargue la aplicación en su teléfono o tableta.
- Suscripción a un servicio de filtrado web
- La combinación de ambas soluciones".

Dispositivos inteligentes con acceso a internet

Un dispositivo inteligente es un dispositivo electrónico que normalmente utiliza varios protocolos inalámbricos como Bluetooth, NFC, Wifi, 3G, LoRa, NB-IoT, Zigbee, etc. para conectarse con otros dispositivos o redes, y tiene cierta interactividad y autonomía. Varios dispositivos inteligentes conocidos, phablets y tabletas, relojes inteligentes, pulseras inteligentes y llaveros inteligentes (Kuan, 2017)

Un dispositivo inteligente habilitado para Internet consiste en un objeto al que se le proporciona una conexión a Internet y cierta inteligencia de software que permite medir o manipular sus parámetros físicos de forma remota para que se pueda generar un ecosistema de servicios a su alrededor, un ecosistema diseñado para crear valor transformando la experiencia del cliente. (Ashton, s.f.)

Funcionamiento de una herramienta de control parental.

El funcionamiento de las herramientas de control parental se basa en la prevención y protección de los menores en el uso de dispositivos conectados a Internet, las características principales de las aplicaciones de control parental son:

- Control de navegación: Es probable que este sea el principal plus de una herramienta de control parental y la funcionalidad está dada por técnicas de prevenciones con los usos de un listado de páginas web permitido y no permitido, los métodos de filtrado también se utilizan para palabras cuya estructura gramatical indica sexo, pornografía, crimen, tabloide u origen de drogas, etc.
- Bloqueo de aplicaciones: Esta característica se basa en las restricciones de los programas que pueden acceder a Internet, chat, mensajería instantánea y correo electrónico (Segu-kids, s.f.)
- Herramientas para bloquear información saliente del ordenador: Como se mencionó anteriormente Son aplicaciones que evitan la fuga de información personal. Esto es especialmente útil para llenar formularios y formularios de registro en línea o realizar compras con crédito, tarjeta, se puede utilizar para web, correo electrónico, chat, etc.
- Monitorización: seguimiento del sistema, por ejemplo, registrar todas las páginas de Internet visitadas para poder realizar un seguimiento posterior de los hábitos de navegación de los menores, no son las mejores herramientas porque se asocian a una mayor vulneración de la privacidad de los menores y al mismo tiempo no son preventivas, sino solo de vigilancia. (Segu-kids, s.f.)

Grooming

En sí, no está relacionado con la actividad sexual, sino solo una táctica de "domesticación" utilizada por el perpetrador para acercarse al menor, llamar su

atención e interés, seducirlo, reducir su autocontrol y aumentar las posibilidades de éxito.

Lo mismo que ocurre con el abuso sexual infantil tradicional. esta solicitud puede incluir cualquier cantidad de actividades sexuales, desde hablar sobre sexo usando pornografía autogenerada o imágenes pornográficas, hasta sexo virtual usando una cámara web o una reunión en persona (Montiel et al., 2014).

Riesgos del internet

Diversos autores (De la Villa Moral & Suárez, 2016), coinciden que los usuarios más frecuentes de las TIC son los jóvenes, ya que están muy familiarizados con las TIC y, por lo tanto, son un grupo de riesgo ante un posible abuso de Internet, ya que están constantemente buscando nuevas experiencias en su uso.

Según el informe EU Kids Online (Garmendia et al., 2015) puede ser difícil determinar qué actividades en línea son beneficiosas y cuáles son dañinas. Sin embargo, las preocupaciones de los padres sobre el uso de Internet de los niños y las actividades relacionadas con Internet han aumentado recientemente.

Los riesgos más evidentes en las redes sociales son el ciberacoso, el sexting, el troleo o la promoción de ideas o mensajes inapropiados que puedan perjudicar a los adolescentes que se encuentran en una etapa de desarrollo personal y priorizando nuevos sentimientos y situaciones.

Seguridad

En términos informáticos es la protección de la información y de los sistemas de información del acceso, uso, divulgación y destrucción no autorizada a través de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos. (Avenía Delgado, 2017)

Sexting

La palabra "sexting" originalmente se refiere a una combinación de sexo y mensajes de texto con teléfonos celulares, pero a medida que la tecnología ha evolucionado, ya no se puede clasificar como uso de teléfonos celulares, pero se incluye en estas publicaciones. Imágenes filtradas, como fotos sexualmente sugerentes o vídeos enviados a través de determinados espacios virtuales (Lounsbury et al., 2011). Sin embargo, a la fecha no existe un consenso sobre qué características debe tener un

mensaje para ser considerado sexting, y hasta la fecha no se ha realizado ningún metanálisis sobre el tema. (Mercado et al., 2016).

Sextorsión

Acuñado para una de las nuevas formas de chantaje sexual a través de la red donde bajo amenaza la victima publica o envía imágenes de contenido sexual o semidesnudos donde se muestra una actitud erótica o de lo más clásico manteniendo relaciones sexuales que exhiben y ponen en circulación en las redes y el internet bajo amenaza. (Supo Mendoza, 2022)

2.4 Marco Legal

CÓDIGO DE LA NIÑEZ Y ADOLESCENCIA

Título III

Derechos, garantías y deberes

Capítulo I

Disposiciones generales

Art. 15.- Titularidad de derechos. - Los niños, niñas y adolescentes son sujetos de derechos y garantías y, como tales, gozan de todos aquellos que las leyes contemplan en favor de las personas, además de aquellos específicos de su edad. (Código de la Niñez y Adolescencia, 2022, pág. 3)

Título IV

De la protección contra el maltrato, abuso, explotación sexual, tráfico y pérdida de niños, niñas y adolescentes

Art. 69.- Concepto de explotación sexual. - Constituyen explotación sexual la prostitución y la pornografía infantil. Prostitución infantil es la utilización de un niño, niña o adolescente en actividades sexuales a cambio de remuneración o de cualquier otra atribución. Pornografía infantil es toda representación, por cualquier medio, ¡de un niño, niña y adolescente en actividades sexuales explicitas, reales o simuladas; o de sus órganos genitales, con la finalidad de promover, sugerir o evocar la actividad sexual. (Código de la Niñez y Adolescencia, 2022, pág. 17)

CÓDIGO ORGÁNICO INTEGRAL PENAL

TÍTULO IV

Infracciones en particular

CAPÍTULO SEGUNDO

Delitos contra los derechos de libertad

SECCIÓN CUARTA

Delitos contra la integridad sexual y reproductiva

Art. 172.- Utilización de personas para exhibición pública con fines de naturaleza sexual. - La persona que utilice a niñas, niños o adolescentes, a personas mayores de sesenta y cinco años o personas con discapacidad para obligarlas a exhibir su cuerpo total o parcialmente con fines de naturaleza sexual, será sancionada con pena privativa de libertad de siete a diez años. (Código Orgánico Integral Penal, 2022, pág. 54)

Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal, 2022, pág. 54)

SECCIÓN SEXTA

Delitos contra el derecho a la intimidad personal y familiar Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal, 2022, pág. 56)

Legislación Ecuatoriana sobre los delitos informáticos

Los delitos informáticos se refieren a las actividades ilícitas que se realizan utilizando la tecnología y los medios y equipos de comunicación para destruir, causar daños o impedir el uso de los sistemas informáticos. Hoy en día, la pornografía infantil, el fraude informático e incluso el terrorismo se consideran nuevos delitos informáticos. Está prohibido incluir grabaciones y fotografías sin consentimiento o autorización legal, robo de claves electrónicas, destrucción o pérdida intencional de información e invasión o violación de la privacidad de otros.

Actualmente, las leyes ecuatorianas sancionan delitos como la privación de la libertad, las mismas leyes reconocidas como el (Código Orgánico Integral Penal, 2022).

Tabla 1

Delitos Informáticos

Tabla 1: Delitos informáticos

DELITOS	**SANCIÓN**
Pornografía infantil	De 13 a 16 años de prisión.
Violación del derecho a la intimidad	De 1 a 3 años de prisión
Revelación ilegal de información de bases de datos	De 1 a 3 años de prisión
Interceptación de comunicaciones	De 3 a 5 años de prisión
Pharming y Phishing	De 3 a 5 años de prisión
Fraude informático	De 3 a 5 años de prisión
Ataque a la integridad de sistemas informáticos	De 3 a 5 años de prisión
Delitos contra la información pública reservada legalmente	De 3 a 5 años de prisión
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	De 3 a 5 años de prisión

Elaborado por: Jairo Uchubanda

En Ecuador, a través del Código Orgánico Integral Penal (COIP), la tercera parte, de los artículos 178 al 234 del COIP, sanciona los delitos cibernéticos que atentan contra la seguridad de la información confidencial, revelación ilegal de datos, daños financieros, accesos no autorizados, entre otros (Código Orgánico Integral Penal, 2022, págs. 56-71).

En la siguiente tabla Nro. 2 se muestra de forma detallada los artículos, la actividad que sanciona y la pena que se impone a los culpables.

Tabla 2

Legislación nacional sobre ciberdelito

Artículo en el COIP	Se comete cuando	Sanción
Artículo 178.- Violación a la intimidad	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos.	Pena privativa de libertad de uno a tres años.
Artículo 190.- Apropiación fraudulenta por medios electrónicos	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona.	Pena privativa de libertad de uno a tres años.
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	Sancionada con pena privativa de libertad de uno a tres años.
Artículo 230.- Interceptación ilegal de datos	La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u	Pena privativa de libertad de

	observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, 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 La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior. 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. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o	tres a cinco años

	sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.	
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. 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.	Pena privativa de libertad de tres a cinco años.
Artículo 232.- Ataque a la integridad de sistemas informáticos	La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave,	Pena privativa de libertad de tres a cinco años.

	deliberada e ilegítima el funcionamiento de un sistema informático.	
	La persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana.	
Artículo 233.- Delitos contra la información pública reservada legalmente	La persona que destruya o inutilice información clasificada de conformidad con la Ley Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado	Pena privativa de libertad de cinco a siete años.
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 sobre dicho sistema	Pena privativa de libertad de tres a cinco años.

	Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos	

Elaborado por: Jairo Uchubanda

Legislación en otros países sobre ciberdelito

Debido a que los delitos informáticos tienen alcance internacional, otros países en Latinoamérica ya han tomado conciencia y han desarrollado e implementado leyes con funcionalidades similares a las leyes del Ecuador por medio del Ecuador adopta el Código Orgánico Integral Penal (COIP) en la Parte III del COIP Artículos 178 al 234 del COIP

En la tabla Nro. 3 se describen las leyes de otros países que mantienen el mismo rol de protección contra delitos informáticos.

Tabla 3

Legislación internacional sobre ciberdelito

País	Artículo	Se comete cuando	Sanción
Perú Ley de Delitos Informáticos. tomado de (Ley N.º 30096, 2013)	**Artículo 2.-** Acceso ilícito	El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo	Reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa

	Artículo 3.- Atentado contra la integridad de datos informáticos	El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos	Reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa
	Artículo 4.- Atentado contra la integridad de sistemas informáticos	El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios	Reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.
	Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él	Reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal

	Artículo 6.- Tráfico ilegal de datos.	El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio	Reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años
	Artículo 7.- Interceptación de datos informáticos**.**	El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo	Reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
	Artículo 8. Fraude informático.	El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un	Reprimido con una pena privativa de libertad no menor de tres ni

		provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia de un sistema informático	mayor de ocho años y con sesenta a ciento veinte días multa.
	Artículo 9.- Suplantación de identidad.	El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral	Reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.
	Artículo 10.- Abuso de mecanismos y dispositivos informáticos**.**	El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley	Reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Venezuela Ley especial contra los delitos informáticos. tomado de (Ley Especial Contra Los Delitos Informáticos, 2001)	**Artículo 6**. Acceso indebido	Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información	Penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias
	Artículo 21. Violación de la privacidad de las comunicaciones.	Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos	Sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias
	Artículo 14. Fraude.	Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes	Penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.
	Artículo 20. Violación de la privacidad de la data o información de carácter personal.	Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales	Penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

	tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información	
Artículo 12. Falsificación de documentos	Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información	Penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias
Artículo 24. Exhibición pornográfica de niños o adolescentes.	Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos	Penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.
Artículo 23. Difusión o exhibición de material pornográfico.	Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico	Sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
Artículo 22. Revelación	Quien revele, difunda o ceda, en todo o en parte, los	Sancionado con prisión de dos a

	indebida de data o información de carácter Persona.	hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21	seis años y multa de doscientas a seiscientas unidades tributarias.
Argentina Ley 26.388 tomado de (Ley 26.388, 2008)	**Artículo 153 bis**	Si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.	Reprimido con prisión de quince días a seis (meses
	Artículo 197	El que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.	Reprimido con prisión de seis meses a dos años
	Artículo 155	El que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra	Reprimido con multa de pesos un mil quinientos a cien mil pesos

	naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.	
Artículo 255	El que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público.	Reprimido con prisión de un mes a cuatro años
Artículo 128	El que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales,	Reprimido con prisión de seis meses a cuatro años

Elaborado por: Jairo Uchubanda

Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador

En la actualidad la policía nacional del Ecuador cuenta con una dependencia llamada Unidad Nacional de Ciberdelito de la Policía Nacional del Ecuador enfocados en su lucha contra el crimen organizado que amenaza las redes del mundo digital, esta unidad forma parte de una de las 12 Unidades investigativas que se articulan de manera transversal en la Dirección General de Investigación Para tal efecto, la Policía Estatal, de conformidad con la resolución No. 002 del 16 de febrero de 2011, el Consejo de Generales de la Policía Nacional, da inicio a la creación de la Unidad de Investigación de Delitos Tecnológicos, siendo esta su primera denominación en este tipo de delitos; con la implementación del Acuerdo Ministerial N. 080 de 2029, pasó a denominarse Unidad Nacional de Ciberdelito. (Gonzalez, 2023)

En base a su misión de detectar, identificar y prevenir el uso ilegal de las tecnologías de la información y la comunicación de diversas formas, utilizando métodos de investigación digital y herramientas científicas, han tomado medidas claras y detenido a 10 ciudadanos en los últimos meses. Existe una variedad de delitos digitales que se refieren a la pornografía con fines de lucro dirigida a niñas, niños y jóvenes, y la apropiación fraudulenta por medios electrónicos.

Para realizar la denuncia toca acercarse a denunciar en los Servicios de Atención Ciudadana de la Fiscalía más cercana a su lugar de residencia. En Quito existen siete Unidades de Servicio de Atención al Integral (SAI) Fiscalía de Pichincha, Carcelén, Mena 2, Tres Manuelas, Tumbaco, Quitumbe, Los Chillos donde receptan las denuncias.

CAPITULO III

METODOLOGÍA

3.1 Tipo de Investigación

3.1.1 Investigación bibliográfica

El presente trabajo es de carácter investigativo para su desarrollo se utilizará la investigación bibliográfica que "es un proceso mediante el cual recopilamos conceptos con el propósito de obtener un conocimiento sistematizado, el objetivo es procesar los escritos principales de un tema particular" (Salas Ocampo, 2019).

Será muy necesaria para la recolección de información de diferentes fuentes como libros, buscadores académicos, revistas, artículos entre otros sobre las aplicaciones para control parental.

3.1.2 Investigación descriptiva

Así también se empleará la investigación descriptiva que "se define como un método de investigación que describe las características de la población o fenómeno estudiado. Esta metodología se centra más en el «qué» del sujeto de investigación que en el «por qué» del sujeto de investigación" (Tiposdeinvestigacion, 2020)

Será útil para describir y explicar si las aplicaciones cumplen o no con las diferentes características establecidas que son necesarias para un correcto control parental

3.1.3 Investigación histórica

Se trabajará con la Investigación histórica, puesto que "implica estudiar, comprender e interpretar eventos pasados, el propósito de la investigación histórica es llegar a ideas o conclusiones sobre personas u ocurrencias pasadas. La investigación histórica implica más que simplemente compilar y presentar información objetiva" (Tiposdeinvestigacion, 2020)

Será de gran utilidad para la revisión de los casos del uso de las aplicaciones libres para control parental que fueron desarrollados en el Ecuador.

3.1.4 Investigación analítica

Es un tipo particular de investigación que requiere el uso de la capacidad de pensamiento crítico y la evaluación de los datos y la información pertinentes para el proyecto en cuestión. (Ortega, 2023)

Este tipo de investigación será necesario para explicar la comparación de las aplicaciones realizadas frente a una valoración.

3.2 Enfoque de la investigación

El presente trabajo será diseñado bajo el planteamiento metodológico del enfoque cualitativo, ya que es el "procedimiento metodológico que utiliza palabras, textos, discursos dibujos, gráficos e imágenes la investigación cualitativa estudia diferentes objetos para comprender la vida social del sujeto a través de los significados desarrollados por éste" (Sánchez Flores, 2019)

Este enfoque nos servirá para poder responder las preguntas de investigación y es el que mejor se adapta a las características y necesidades de la investigación.

3.3 Métodos de Investigación

En el presente trabajo de investigación se emplearán los siguientes métodos de investigación:

3.3.1 Método bibliográfico

Consiste en la revisión de material bibliográfico existente con respecto al tema a estudiar. Se trata de uno de los principales pasos para cualquier investigación e incluye la selección de fuentes de información (Ayala, 2021)

Este método es importante porque se basa en el análisis de tesis, artículos, revistas y será necesario para la recolección de la información relacionada con el tema de investigación propuesto.

3.3.2 Método analítico

Se va a utilizar el método analítico que "es aquel método de investigación que consiste en la desmembración de un todo descomponiéndolo en sus partes o elementos para observar las causas, naturaleza y los efectos" (Hernandez Coca, 2017).

Será importante en la delimitación del tema, redacción del planteamiento del problema, preguntas de investigación, objetivos, justificación, marco teórico y resultados.

3.3.3 Método deductivo

El método deductivo se enfoca en estudiar la realidad y en verificar o refutar la premisa por comprobar (Muguira, s.f.).

Será de utilidad para la elaboración del planteamiento del problema, para la redacción y comprobación de la hipótesis, así como de las conclusiones

3.3.4 Método inductivo

Este método consiste en la obtención de conclusiones generales a través de premisas particulares. En otras palabras, el método inductivo parte de hipótesis específicas para obtener una información más general del objeto de estudio. (TUTFG, 2023).

Será útil en la recolección de datos sobre las aplicaciones de control parental y realizar su respectivo análisis.

3.4 Técnicas e Instrumentos de Recopilación de Datos

Para la recolección de datos se utilizó las siguientes técnicas: análisis de documentos, informes de investigación, entrevista, los cuales sirvieron para encontrar información útil para el estudio del problema.

3.4.1 Análisis de documentos.

El análisis de los documentos fue realizado con fichas bibliográficas para registrar información de los diferentes repositorios de internet resultado de los procedimientos y poder usarlo cuando sea necesario.

3.4.2 Informes de investigación

El informe de investigación intenta reflejar de forma clara y objetiva los objetivos de la investigación, el método de ejecución, los principales resultados obtenidos, las principales conclusiones y recomendaciones realizadas tras la realización de la investigación.

Esta técnica es utilizada para detallar la investigación realizada detallando cómo se cumplieron los objetivos y preguntas de investigación del tema planteado.

3.4.3 Entrevista

Una entrevista es un intercambio interpersonal entre un investigador y un sujeto de investigación para obtener respuestas verbales a las preguntas sobre un problema propuesto.

Para la presente investigación se entrevistó al Sargento Quinso de la policía judicial con el fin de recopilar información sobre los ciberdelitos y conocer acerca de cómo se realiza el proceso en caso de que una persona esté siendo víctima de un ciberdelito.

3.5 Universo, Población y Muestra

Al tratarse de un estudio comparativo, con el cual se busca determinar cuál de las aplicaciones seleccionadas es la mejor para garantizar un control parental eficiente, y considerando que las aplicaciones no serán sometidas a una valoración de los posibles usuarios, esta investigación no tiene un universo ni muestra, la población se tiene como objeto de investigación las ocho aplicaciones de control parental con las que se trabajara.

3.6 Procesamiento de la Información

Para el procesamiento de la información se utilizó un procesador de datos y una hoja de cálculo, una vez determinado las aplicaciones libres para control parental más utilizadas, se procede a tabular los resultados en una tabla que confrontara características y una valoración para cada una de ellas.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

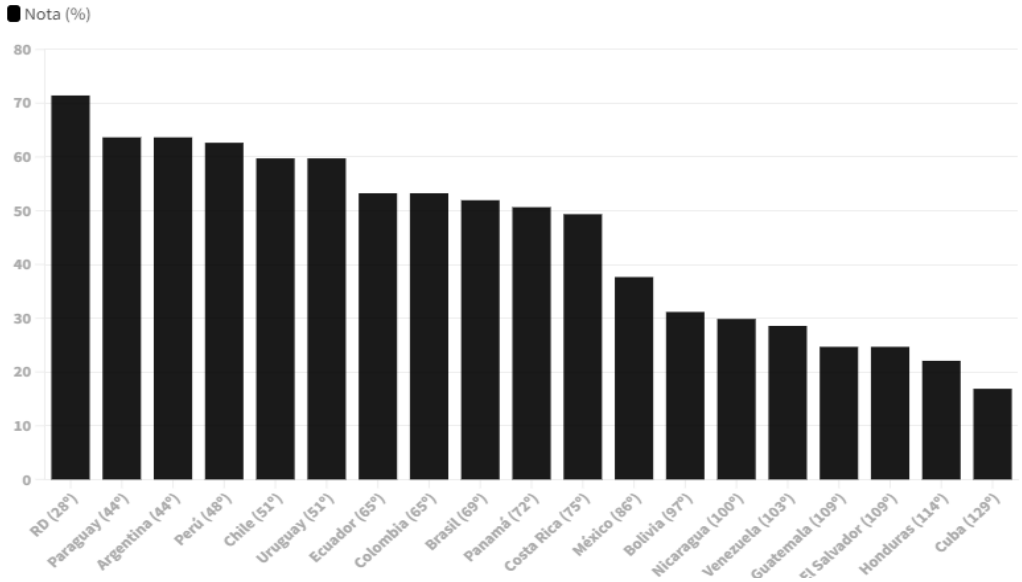
4.1 Análisis, Interpretación y Discusión de Resultados

4.1.1 Ranking en América Latina de uso de estas herramientas de ciberseguridad

En la Imagen Nro. 1 se destacan los países en su compromiso en la ciberseguridad global y en la cual República Dominicana es el líder de la región en materia de ciberseguridad. Para encontrar al próximo país latinoamericano hay que bajar casi 20 puestos hasta el 44, con Paraguay y Argentina empatados.

Ilustración 1

Ranking latinoamericano en ciberseguridad



Fuente: (e-Governance Academy, 2023)

En cuanto a nuestro país Ecuador se encuentra en el puesto 7 esto demuestra que el país ha tomado medidas efectivas para proteger sus sistemas y datos de ataques cibernéticos y está bien preparado para enfrentar posibles incidentes de seguridad cibernética, pero aún falta mucho por mejorar comparado con República Dominicana que está actualmente dominando en materia de la ciberseguridad.

4.1.2 Estadística delitos cibernéticos en Ecuador

En el Ecuador, los ciberdelitos están tipificados en el Código Orgánico Integral Penal (COIP) como una medida para perseguirlos y fijar sanciones. De acuerdo con el Sistema Integrado de Actuaciones Fiscales (SIAF) de la fiscalía general del Estado, los delitos cibernéticos que se han denunciado con mayor frecuencia a escala nacional, son:

Ilustración 2

Estadística delitos cibernéticos

ART. COIP	TIPO PENAL /ARTICULO	2017	2018	2019	2020	2021[1]	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	103	104	81	113	95	**496**
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	**85**
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	158	202	165	152	152	**829**
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	12	14	16	7	7	**56**
178	Violación a la intimidad	1.660	2.062	2.038	1.985	1.346	**9.091**
186	Estafa	13.911	14.268	16.918	18.415	16.272	**79.784**
188	Aprovechamiento ilícito de servicios públicos	102	130	194	99	72	**597**
190	Apropiación fraudulenta por medios electrónicos	959	1.448	1.744	2.280	3.962	**10.393**
192	Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	1	1	**2**
193	Reemplazo de identificación de terminales móviles	4	2	-	3	-	**9**
194	Comercialización ilícita de terminales móviles	24	14	7	285	10	**340**
195	Infraestructura ilícita	-	5	7	-	-	**12**
211	Supresión, alteración o suposición de la identidad y estado civil	52	81	54	23	28	**238**
229	Revelación ilegal de base de datos	22	44	34	30	23	**153**
230	Interceptación ilegal de datos	63	41	86	73	35	**298**
231	Transferencia electrónica de activo patrimonial	54	37	50	76	170	**387**
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	86	**463**
233	Delitos contra la información pública reservada legalmente.	14	12	5	5	4	**40**
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	274	**1.265**
366	Terrorismo	12	120	65	13	17	**227**
Total general por años		**17.480**	**18.914**	**21.834**	**23.968**	**22.569**	**104.765**

Fuente: (Fiscalía General del Estado, 2021)

En la figura Nro.2 observamos las diferentes modalidades de delitos que se reportaron del año 2017 a 2021, el aumento, disminución y acumulado de la mayoría de estos delitos. (Fiscalía General del Estado, 2021)

4.1.3 Principales actividades de uso de los dispositivos móviles

En Ecuador las principales actividades de uso de los dispositivos móviles se tienen:

Ilustración 3

Tráfico web según el sistema operativo usado

Fuente: (Branch, 2022)

En el ecuador el 87% del tráfico web proviene de dispositivos con tecnología y el 13% del tráfico proviene de dispositivos Apple

El,

Ilustración 4

Sitios web más visitados

Fuente: (Branch, 2022)

Los sitios más buscados por los ecuatorianos son Google, YouTube, el Comercio y Facebook. Por otro lado, el 97% del tráfico web en Internet proviene de las páginas más buscadas en Google: WhatsApp, WhatsApp Web, traductor y Facebook.

Ilustración 5

Uso de redes sociales

Fuente: (Branch, 2022)

Las redes sociales son utilizadas por el 81% de la población, o 14,6 millones de ecuatorianos. De estos, el 49 por ciento eran mujeres y el 51 por ciento eran hombres. En el 2022, el número de usuarios ha crecido +4.3%, lo cual representa 600.000 nuevas personas.

En una década, el número de usuarios de redes sociales ha crecido +57%

Quito. - Facebook, Twitter o Instagram es una de las redes sociales más reconocibles del planeta, reuniendo a millones de usuarios. En Ecuador, su uso es un mecanismo común de comunicación y aprendizaje para muchas personas. En el marco de la disponibilidad de las tecnologías de la información y la comunicación (TIC), el Ministerio de Telecomunicaciones y Sociedad de la Información actúa como ente rector del sector e implementa la política de Estado que asegure la democratización de estos servicios. (telecomunicaciones, s.f.)

A nivel urbano se registra que el 92,4% de ciudadanos acceden a redes sociales, por medio de sus teléfonos móviles; mientras que en la zona rural el 82,88% de personas con celular accede a las redes sociales.

4.1.4 Casos del uso de las aplicaciones libres para control parental desarrollados en el Ecuador

Caso 1

En la investigación de Delgado (2021) se analizó la necesidad de la implementación de una herramienta tecnológica de control parental sobre el uso que los menores le dan al internet la Unidad Educativa Fiscal Tarqui en la Ciudad de Manta

Con la finalidad de conocer si es necesario aplicar el control parental desde el punto de vista del público respecto a los contenidos de Internet y el control parental, se consideraron entrevistas a diversos representantes de la comunidad educativa: administradores, docentes y representantes.

La encuesta se aplicó a 140 representantes, a través de un cuestionario de preguntas diseñado en la aplicación Formularios de Google.

A continuación, los resultados:

Tabla 4

¿En cuál de las siguientes opciones, considera usted que los estudiantes emplean la mayor parte del tiempo en internet?

Opciones de Respuestas	Frecuencia	Porcentaje
Actividades académicas	71	50,70 %
Redes sociales	35	25,00 %
Ver videos	11	7,90 %
Juegos online	12	8,60 %
Actividades de emprendimiento y promoción de productos	3	2,10 %
Otros	8	5,70 %
Totales	**140**	**100,00 %**

Fuente: (Delgado , 2021)

Un 49,30% contestó que los estudiantes emplean la mayor parte del tiempo en actividades distintas.

Es razonable interpretar estos resultados como una indicación de que los recursos o contenidos en Internet pueden ser un factor perturbador que afecte el rendimiento académico de los estudiantes.

Tabla 5

¿Creé usted que la implementación de una herramienta de control parental sobre los contenidos que los menores manejan en internet puede influir en un mejor desempeño académico de los estudiantes?

Opciones de Respuestas	Frecuencia	Porcentaje
De acuerdo	90	64,30 %
Parcialmente de acuerdo	33	24,60 %
En desacuerdo	17	12,10 %
Totales	**140**	**100,00 %**

Fuente: (Delgado , 2021)

El 90 % contestó que se necesita una herramienta de control parental.

Tabla 6

En caso de estar dispuesto a utilizar una herramienta de control parental: ¿Qué tipo de reportes le gustaría que esta herramienta le brinde?

Opciones de Respuestas	Frecuencia	Porcentaje
Reporte de páginas navegadas	39	27,86 %
Tiempo de navegación	31	22,14 %
Ubicación	2	1,43 %
Todas las anteriores	68	48,57 %
Totales	**140**	**100,00 %**

Fuente: (Delgado , 2021)

Los resultados de esta pregunta muestran que los padres no están seguros acerca de la interacción de sus hijos con el contenido de Internet y, sorprendentemente, menos del 50 % dijo que quiere herramientas de control tecnológico. le dé un reporte de todas las opciones planteadas lo que nuevamente refuerza los pensamientos iniciales de los investigadores acerca de que el contenido de Internet es propiedad de agentes de control parental. El diagnóstico permitió justificar la necesidad de

implantar una herramienta tecnológica proactiva para el control parental, que permita representantes de un mismo espacio virtual en el que se encuentran los estudiantes, para obtener una información detallada y en tiempo real de lo que realizan los menores en internet la aplicación de control parental que fue seleccionada fue Family Link.

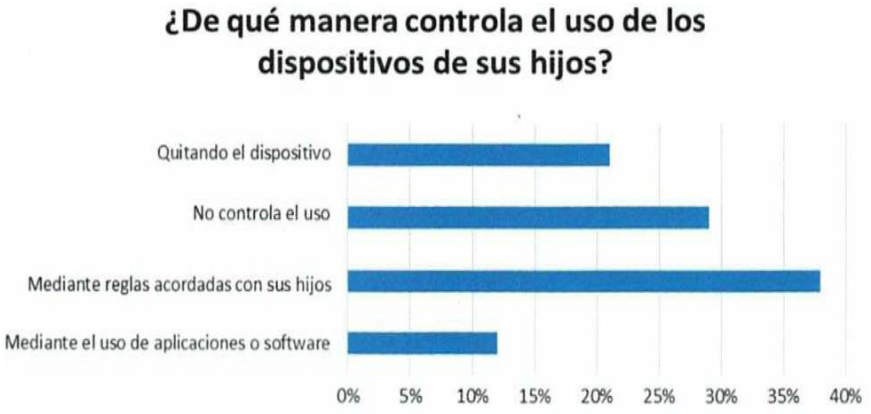
Caso 2

En la investigación realizada por Benetazzo & Sotomayor (2021) se enfocó en conocer si una aplicación de control parental era necesario en la ciudad de Guayaquil para lo cual se realizó una encuesta la cual se cumplirá con un muestreo no probabilístico, se seleccionará 150 padres o madres de familia de ciudadelas ubicadas en la ciudad de Guayaquil y sus alrededores, se obtuvo los correos electrónicos de los padres seleccionados y la encuesta se realizará a través de internet, utilizando las herramientas de Documentos de Google, las preguntas en la encuesta serán de tipo cerrada, ya que lo que se desea es cuantificar si existe la necesidad del software.

Los datos de las encuestas realizadas fueron:

Ilustración 6

Formas en las que controlan el uso de los dispositivos inteligentes de los hijos



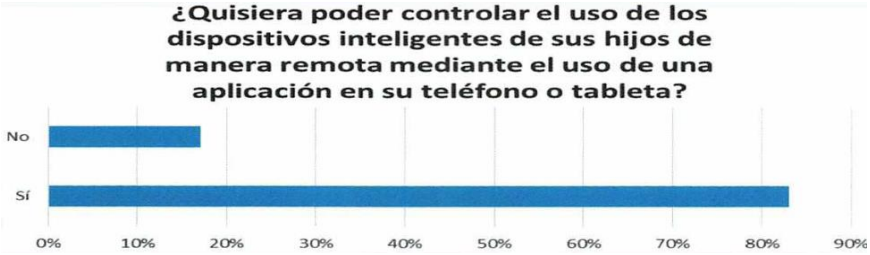
Fuente: (Benetazzo & Sotomayor, 2021)

Se puede ver cómo los padres pueden controlar los dispositivos inteligentes de sus hijos. Solo el 12% de los padres de familia indican que utilizan algún tipo de software para controlar los dispositivos de sus hijos. El 21% indica que recurre a quitar los dispositivos a sus hijos para poder controlar el uso, esto es poco práctico ya que administrados correctamente son útiles para los padres de familia,

especialmente en casos de emergencia para poder establecer comunicación inmediata con sus hijos. Al quitar los teléfonos o tabletas los padres de familia pierden esta funcionalidad importante. El 38% dijo que controlan acordando reglas verbalmente con sus hijos.

Ilustración 7

Los dispositivos inteligentes causan distracciones de las obligaciones de los hijos



Fuente: (Benetazzo & Sotomayor, 2021)

En la figura se puede observar que el 83% de los padres de familia indican que quisieran poder controlar el uso de los dispositivos de sus hijos de manera remota. Con base en la encuesta se optó por crear el aplicativo de control parental, finalizado el desarrollo se procedió a entregar el piloto a una de las madres de familia encuestadas por dos semanas para que probara todas las funciones del aplicativo

Una vez finalizado el piloto se procedió a realizar una entrevista a la madre de familia para conocer su experiencia, utilizando la aplicación y si en su opinión ayudó a disminuir las distracciones de su hija, de acuerdo a lo expresado por la madre en la entrevista el sistema cumplió con el objetivo de permitirle gestionar el uso del dispositivo de su hija y fue útil para eliminarlo como distracción durante las horas de estudio, adicionalmente la madre de familia expresó que fue de gran ayuda para que su hija evite el uso del dispositivo durante momentos familiares, como las horas de comer o salidas familiares.

Caso 3

En la investigación realizada por Coello & Saltos (2022) en la ciudad de Guayaquil con el objetivo de conocer si el uso de herramientas de control parental ayudaría a detectar los riesgos que podrían sufrir los menores de edad al acceder algún contenido no autorizados a través de los dispositivos electrónicos, dónde el universo establecido son los padres de familia que tienen hijos de un rango de edad de 5 a 15 años, que son los que se encuentran en edades más vulneradas y son más fáciles de

manipular, la muestra seleccionada serán familias de sectores norte y el sur de la ciudad de Guayaquil, siendo los encuestados elegidos al azar para dar su punto de vista sobre las herramientas de control parental, para calcular el tamaño de la muestra se consideró una población de tamaño desconocido.

Se establece las aplicaciones que serán entregadas a los padres se realizó pruebas de usabilidad para comprobar que cumplan con las características establecidas, finalizados las pruebas se entregó a los padres para que puedan utilizar en sus familias en total fueron cuatro aplicaciones las herramientas seleccionadas fueron: Con licencia de paga Qustodio y Norton Family y con licencia gratuita FamiSafe, Secure Kids.

Para La recolección de información se utilizó un cuestionario utilizado fue el electrónico obtenido de Microsoft Forms, ya que permite a los usuarios puedan responder los cuestionarios accediendo desde algún dispositivo digital, y a su vez muestra en tiempo real los análisis de los resultados que han sido enviados, también brinda la facilidad de exportar los resultados a Excel para proceder hacer los análisis correspondientes.

Una vez recolectada la información del uso de las aplicaciones por parte de los padres se concluyó que de acuerdo a la licencia gratuita Secure Kids queda como mejor herramienta y de licencia paga Norton Family.

Tabla 7

Nivel de satisfacción en los padres de familia

Herramienta	Totalmente satisfecho	Muy satisfecho	Neutral	Poco satisfecho	Nada satisfecho
FamiSafe	8	13	3	0	0
Secure Kids	6	15	3	0	0
Qustodio	14	9	1	0	0
Norton Family	9	10	3	1	1

Fuente: (Coello & Saltos, 2022)

4.1.5 Evaluación de las características de las aplicaciones de control parental

Para poder probar las aplicaciones y realizar la evaluación de las características de control parental de las aplicaciones se utilizó dos dispositivos Android para las cinco aplicaciones de versión Android y una laptop con Windows 10 para poder probar las dos aplicaciones para PC

Filtrar contenido Web

Permite restringir páginas web de forma individual o por categorías, configurar la opción de búsqueda segura, bloquea el acceso del menor o adolescente a ciertos contenidos inapropiados y emite alertas cuando se intenta acceder a páginas web no permitidas.

Ilustración 8

Página web bloqueada

Elaborado por: Jairo Uchubanda

Tabla 8

Aplicaciones que permiten filtrar contenido Web

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids	✓	
KidsGuard	✓	
Norton Family	✓	
Kaspersky Safe Kids	✓	
Locategy	✓	
PC		
Microsoft Family Safety	✓	
Kidlogger		✓

Elaborado por: Jairo Uchubanda

Todas las aplicaciones para dispositivos Android cuentan con la característica para filtrar contenido web, además Norton Family, Kaspersky Safe Kids permiten el filtrado en diferentes navegadores web instalados en el dispositivo mientras que Google Family Link, SecureKids, KidsGuard permiten el filtrado web solo con el navegador Google Chrome,

La aplicación Microsoft Family Safety permite bloquear filtrar contenido web de una manera precisa sin embargo el filtrado solo funciona con el navegador Microsoft Edge, por otro lado, la aplicación Kidlogger no cuenta con la característica de filtrado

Bloqueo de aplicaciones

Esta característica permitirá al padre bloquear el acceso a determinadas aplicaciones instaladas en el dispositivo, emite alertas o interrumpe la navegación al alcanzar determinada hora o límite de tiempo.

Ilustración 9

Aplicación bloqueada

Elaborado por: Jairo Uchubanda

Tabla 9

Aplicaciones que permiten bloquear aplicaciones

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids	✓	
KidsGuard	✓	
Norton Family	✓	
Kaspersky Safe Kids	✓	
Locategy	✓	
PC		
Microsoft Family Safety	✓	
Kidlogger		✓

Elaborado por: Jairo Uchubanda

Todas las aplicaciones para dispositivos Android cuentan con la característica para bloquear cualquier aplicación instalada en el dispositivo, sin embargo, al ser aplicaciones con licencia gratuita tienen sus limitaciones por lo que la aplicación KidsGuard no permite bloquear cualquier aplicación instalada en el dispositivo sólo permite bloquear aplicaciones básicas del dispositivo como galería, Play Store, la aplicación Norton Family no permite elegir que aplicación bloquear sino que bloquea todas las aplicaciones y la aplicación Locategy permite bloquear solo 1 aplicación.

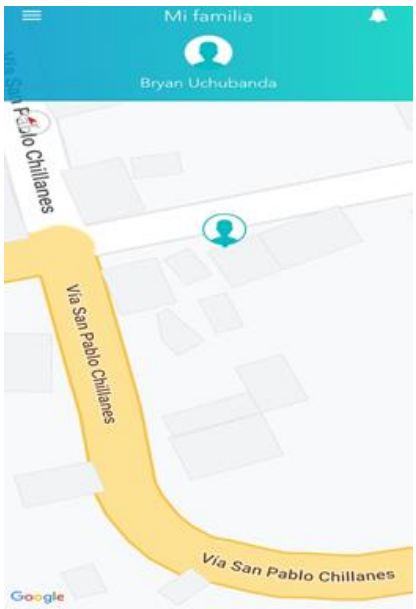
La aplicación Microsoft Family Safety permite bloquear cualquier aplicación instalada en el dispositivo ya sea por tiempo indefinido o establecido por el padre, por otro lado, la aplicación Kidlogger no cuenta con la función para poder bloquear aplicaciones.

Ubicación

Con esta característica el padre puede seguir la posición actual del dispositivo y ubicar exactamente donde se encuentra en tiempo real.

Ilustración 10

Ubicación del dispositivo



Elaborado por: Jairo Uchubanda

Tabla 10

Aplicaciones que permiten revisar la ubicación

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids	✓	
KidsGuard	✓	
Norton Family	✓	
Kaspersky Safe Kids	✓	
Locategy	✓	
PC		
Microsoft Family Safety		✓
Kidlogger		✓

Elaborado por: Jairo Uchubanda

Todas las aplicaciones para dispositivos Android cuentan con la característica para poder revisar la ubicación actual del dispositivo

Para las aplicaciones de PC la característica de ubicación no se encuentra disponible.

Limitador de tiempo en pantalla

Permite controlar el tiempo que los menores podrán hacer uso del equipo, es posible definir durante cuánto tiempo se puede utilizar el dispositivo al día una vez cumplido el tiempo el dispositivo se bloquee y es imposible usar sin el consentimiento del padre.

Ilustración 11

Dispositivo bloqueado

Elaborado por: Jairo Uchubanda

Tabla 11

Aplicaciones que permiten limitar tiempo en pantalla

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids		✓
KidsGuard	✓	
Norton Family	✓	
Kaspersky Safe Kids	✓	
Locategy	✓	
PC		
Microsoft Family Safety	✓	
Kidlogger		✓

Elaborado por: Jairo Uchubanda

La aplicación SecureKids no cuentan con la característica para poder establecer un límite del tiempo en pantalla del dispositivo además KidsGuard al ser la versión gratuita solo cuenta con la característica de limitar el tiempo en pantalla con la opción premium.

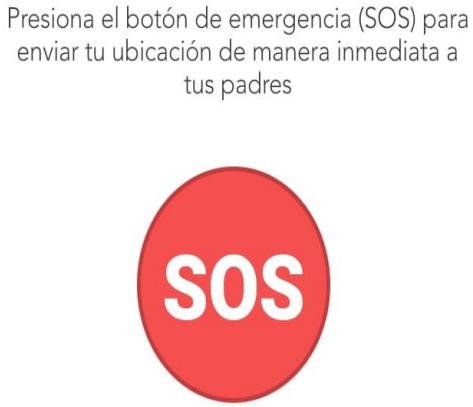
La aplicación Microsoft Family Safety permite establecer un horario en el cual el dispositivo se va a poder usar una vez finalizado el tiempo se bloquee y no puede acceder, la aplicación Kidlogger no cuenta con esta característica

Botón de emergencia

En caso de emergencia el dispositivo hijo puede enviar una alerta instantánea que incluye la ubicación del dispositivo.

Ilustración 12

Botón de emergencia



Elaborado por: Jairo Uchubanda

Tabla 12

Aplicaciones que permiten enviar una emergencia

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link		✓
SecureKids	✓	
KidsGuard		✓
Norton Family		✓
Kaspersky Safe Kids		✓
Locategy	✓	
PC		
Microsoft Family Safety		✓
Kidlogger		✓

Elaborado por: Jairo Uchubanda

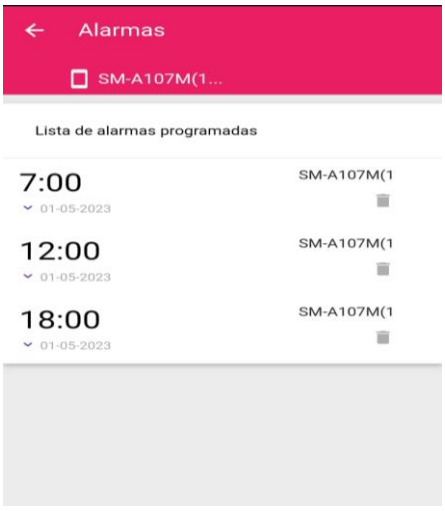
Las únicas aplicaciones que cuenta con la característica para poder enviar una señal de emergencia al dispositivo del padre son Locategy y SecureKids que al presionar el botón le llegará una alerta al dispositivo padre con la ubicación desde donde fue enviada, además SecureKids toma una foto con la cámara del dispositivo al momento de presionar el botón que será enviada junto con la ubicación.

Crear alarmas

Mediante esta característica se pueden establecer alarmas programadas ya sea para un día específico o para una semana con un recordatorio de lo que debe realizar en cierto momento.

Ilustración 13

Alarmas



Elaborado por: Jairo Uchubanda

Tabla 13

Aplicaciones que permiten crear alarmas

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link		✓
SecureKids	✓	
KidsGuard		✓
Norton Family		✓
Kaspersky Safe Kids		✓
Locategy		✓
PC		
Microsoft Family Safety		✓
Kidlogger		✓

Elaborado por: Jairo Uchubanda

La única aplicación que permite programar alarmas es SecureKids que permite configurar un horario y un mensaje que será recibido por el dispositivo hijo.

Protección de la configuración

Sirve para evitar que los niños o adolescentes puedan desinstalar las aplicaciones de control parental sin el permiso del padre.

Ilustración 14

Bloqueo de configuración para desinstalar

Elaborado por: Jairo Uchubanda

Tabla 14

Aplicaciones que evitan ser desinstaladas por los hijos.

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids	✓	
KidsGuard	✓	
Norton Family		✓
Kaspersky Safe Kids	✓	
Locategy		✓
PC		
Microsoft Family Safety	✓	
Kidlogger		✓

Elaborado por: Jairo Uchubanda

Norton Family y Locategy no cuentan con la característica para poder evitar que los hijos desinstalen las aplicaciones de control parental.

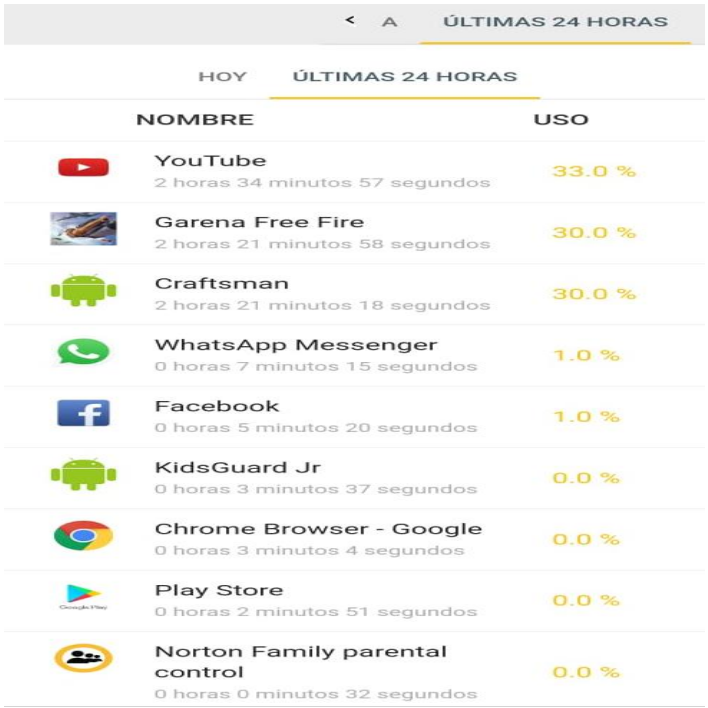
Kidlogger no evita que los hijos puedan desinstalar la aplicación y evadan la protección establecida.

Reporte de actividad

Permite revisar un reporte diario de todas las aplicaciones que se utilizaron en el dispositivo y cuánto tiempo se le dedicó a cada una.

Ilustración 15

Reporte de uso



Elaborado por: Jairo Uchubanda

Tabla 15

Aplicaciones que permiten revisar un reporte de uso

Aplicaciones	Cumple	No cumple
Dispositivos Android		
Google Family Link	✓	
SecureKids	✓	
KidsGuard	✓	
Norton Family		✓
Kaspersky Safe Kids	✓	
Locategy	✓	
PC		
Microsoft Family Safety	✓	
Kidlogger	✓	

Elaborado por: Jairo Uchubanda

Casi todas las aplicaciones Android permiten revisar un reporte diario del uso del dispositivo, la única aplicación que no permite revisar un reporte de la actividad del dispositivo es Norton Family, además Locategy permite revisar un reporte de las búsquedas realizadas en internet.

La aplicación Microsoft Family Safety permite revisar cuanto tiempo uso el dispositivo y cuánto tiempo uso cada aplicación, la aplicación Kidlogger permite revisar un reporte de todo lo que hizo el adolescente en el dispositivo desde ingresar a una aplicación hasta revisar que búsquedas realizó en internet además de poder configurar un tiempo para sacar una captura discreta que será almacenada para posteriormente revisar.

4.1.6 Valoración de las características de las aplicaciones libres para control parental

Tabla 16

Valoración de las características de las aplicaciones

	Filtrar contenido	Bloqueo de aplicaciones	Localizador	Limitador de tiempo en pantalla	Botón de emergencia	Crear alarmas	Protección de la configuración	Reporte de actividad
Excelente (3)	La aplicación permite filtrar páginas web por categorías, restringiendo determinados tipos de sitios web, desde cualquier navegador	La aplicación permite bloquear cualquier aplicación instalada en el dispositivo	La aplicación tiene la capacidad de saber la ubicación geográfica real de donde se encuentran los adolescentes.	La aplicación permite programar un horario en el cual se bloqueará el dispositivo	La aplicación cuenta con la opción de botón de emergencia, envía una emergencia con la ubicación exacta.	La aplicación permite programar alarmas en remoto con un mensaje de información	La aplicación solo permite ser desactivada o desinstalada con la autorización del padre.	La aplicación permite monitorear los teléfonos para conocer sus actividades diarias, comprueba las aplicaciones que más utilizan y las aplicaciones que instalan o desinstalan.
Bueno (2)	La aplicación permite restringir páginas web solo con un navegador en específico	La aplicación permite bloquear solo aplicaciones esenciales del dispositivo	La aplicación solo presenta un aproximado de la ubicación real	La aplicación permite establecer un tiempo máximo de uso de dispositivo o en un intervalo horario determinado.	La aplicación cuenta con la opción de botón de emergencia, envía una emergencia y se conoce la ubicación aproximada en el mapa,	La aplicación permite programar solo alarmas en remoto sin mensajes	La aplicación puede ser desinstalada con conocimientos básicos en Android	La aplicación muestra un reporte de actividades, pero solo el tiempo de uso no con detalles

Regular (1)	La aplicación solo permite filtrar contenido con una función premium.	La aplicación permite bloquear aplicaciones solo con una función premium.	La aplicación tiene la capacidad de saber la ubicación geográfica solo con una función premium.	La aplicación permite bloquear el dispositivo o una solo con una función premium.	La aplicación cuenta con la opción de botón de emergencia, solo con una función premium.	La aplicación permite programar alarmas en remoto, con difícil configuración	La aplicación evita ser desinstalada solo con una función premium	Se nos presenta un reporte de actividades solo con una función premium.
Deficiente (0)	La aplicación no cuenta con la función de filtrar contenido	La aplicación no cuenta con la función para bloquear aplicaciones.	La aplicación no cuenta con la función de localizar	La aplicación no cuenta con la función de limitar el tiempo de pantalla	La aplicación no cuenta con la función de botón de emergencia	La aplicación no cuenta con la función de programar alarmas	La aplicación no tiene una opción para evitar ser desinstalada	La aplicación no cuenta con la función de reporte de actividad

4.1.7 Comparación de características y una valoración para cada una de las aplicaciones libres para control parental

Tabla 17

Comparación de aplicaciones Android y sus características

Aplicaciones Android	Google Family Link	SecureKids	KidsGuard	Norton Family	Kaspersky Safe Kids	Locategy
Filtrar contenido Web	2	2	2	3	3	1
Bloqueo de aplicaciones	3	3	2	2	3	1
Ubicación	3	3	3	3	1	3
Limitador de tiempo en pantalla	3	0	1	2	3	3
Botón de emergencia	0	3	0	0	0	3
Crear alarmas	0	3	0	0	0	0
Protección de la configuración	3	3	3	0	3	0
Reporte de actividad	3	3	3	0	2	3
Total	17	20	14	10	15	14

Tabla 18

Comparación de aplicaciones PC y sus características

Aplicaciones PC	**Microsoft Family Safety**	**Kidlogger**
Filtrar contenido Web	2	0
Bloqueo de aplicaciones	3	0
Ubicación	0	0
Limitador de tiempo en pantalla	3	0
Botón de emergencia	0	0
Crear alarmas	0	0
Protección de la configuración	3	0
Reporte de actividad	3	3
Total	14	3

Después de la comparación realizada tanto para dispositivos Android como para PC se obtiene que:

Para los dispositivos Android de la comparación de las aplicaciones de control parental presentadas en la tabla N.17 se puede observar que la mejor aplicación es SecureKids dado que presenta una valoración superior a las demás dando a conocer que cumple con la mayoría de las características necesarias para lograr un correcto control parental

Para la PC de las aplicaciones de control parental presentadas en la tabla N.18 se tiene que la mejor es Microsoft Family Safety, ya que cumple con la mayoría de las características de control parental y presenta la mayor valoración en comparación con la segunda aplicación que solo permite revisar un reporte de las actividades realizadas en el equipo.

CONCLUSIONES

- Consultando varios sitios web (EPE, SSOO, Xatakandroid, Softzone) en donde se trata del tema de las aplicaciones de control parental, se logró sistematizar que las más utilizadas son: Google Family Link, SecureKids, KidsGuard, Norton Family, Kaspersky Safe Kids, Locategy, Microsoft Family Safety, Kidlogger teniendo en cuenta que son las que se encuentran en cada sitio.
- Los parámetros utilizados para la comparación de las aplicaciones libres son las siguientes: filtrar contenido Web, bloqueo de aplicaciones, ubicación, limitador de tiempo en pantalla, botón de emergencia, crear alarmas, protección de la configuración, reporte de actividad.
- La aplicación SecureKids es una herramienta informática que permite a los padres de familia realizar el control y monitoreo del uso adecuado de los dispositivos tecnológicos, el mismo que dispone de las mejores características para realizar de manera eficiente el control parental de los niños y adolescentes.
- En base a los casos analizados en las ciudades de Guayaquil y Manta se puede observar que los padres de familias están de acuerdo en la utilización de aplicaciones para el control parental

RECOMENDACIONES

- Las herramientas libres para control parental pueden ser utilizadas por los padres de familia para el control y monitoreo del uso de los dispositivos tecnológicos por los adolescentes.
- Utilizar la aplicación SecureKids por ser la herramienta más adecuada para realizar de manera eficiente el control parental de los niños y adolescentes por parte de los padres de familia.
- Considerando los casos analizados en el Ecuador es necesario que los padres de familia se capaciten en el uso de las herramientas de control parental y la legislación existente para el efecto.

BIBLIOGRAFÍA

Alonso Conde, A. B. (s.f.). *Herramientas y sistemas de medida*. Obtenido de vlex: https://vlex.es/vid/herramientas-sistemas-medida-247143#:~:text=%C2%B7%20M%C3%A9todos%20site%2Dcentric%20(centrados,y%20an%C3%A1lisis%20de%20esta%20actividad.

Asamblea Nacional de Venezuela. (2001, 30 de octubre). *Ley Especial Contra Los Delitos Informáticos.* Gaceta Oficial de Venezuela. Obtenido de https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Ashton, K. (s.f.). *Caminar con éxito hacia la Industria 4.0: Capítulo 14 – Dispositivos (I) Internet de las cosas (IoT)*. Obtenido de ticnegocios: https://ticnegocios.camaravalencia.com/servicios/tendencias/caminar-con-exito-hacia-la-industria-4-0-capitulo-14-dispositivos-i-internet-de-las-cosas-iot/#:~:text=Un%20dispositivo%20IoT%20consiste%20en,de%20servicios%20alrededor%20del%20mismo.

Avenía Delgado, C. A. (2017). Fundamentos de seguridad. *Core*, 98. Obtenido de https://core.ac.uk/download/pdf/326424171.pdf

Ayala, A. (2021). *Investigación Bibliográfica: Definición, Tipos, Técnicas.* Obtenido de https://docplayer.es/204971617-Investigacion-bibliografica-definicion-tipos-tecnicas.html

Benetazzo, G., & Sotomayor, M. (2021). *Implementación de una aplicación para control parental en dispositivos inteligentes.* Universidad Espíritu Santo, Guayas. Obtenido de https://revistas.uees.edu.ec/index.php/IRR/article/view/42

BetanCourt, D., & Andrade, P. (2011). Control Parental y Problemas Emocionales y de Conducta en Adolescentes*. *redalyc*. Obtenido de https://www.redalyc.org/pdf/804/80419035006.pdf

Branch. (2022). *Estadísticas de la situación Digital en Ecuador 2021-2022*. Obtenido de Branch: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-en-ecuador-2021-

2022/#:~:text=El%20crecimiento%20digital%3A%20enero%202021,en%20redes%20sociales%20%2B4.3%25.

Cámara de Diputados de la Nación Argentina. (24 de Junio de 2008, 04 de Junio). *Ley 26.388.* El Boletín Oficial de la República Argentina. Obtenido de https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

Ciberseguridad. (s.f.). *¿QUÉ ES OSSTMM? DEFINICIÓN, HISTORIA Y CARACTERÍSTICAS*. Obtenido de Ciberseguridad: https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/

Coello, A., & Saltos, M. (2022). *Análisis práctico comparativo de herramientas de control parental con licencias gratuitas y pagadas para la seguridad integral a menores de edad en ambientes digitales en la ciudad de Guayaquil.* Universidad de Guayaquil, Guayaquil. Obtenido de http://repositorio.ug.edu.ec/handle/redug/59774

Coronel, C. (2018). Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de internet. *Instituto Politécnico de leiria*, 103. Obtenido de https://iconline.ipleiria.pt/handle/10400.8/3745

De la Villa Moral, M., & Suárez, C. (2016). Factores de riesgo en el uso problemático de Internet y del teléfono móvil en adolescentes españoles. *redalyc*, 11. Obtenido de https://www.redalyc.org/articulo.oa?id=245145815004

Defensoría Pública del Ecuador. (2022). *Código de la Niñez y Adolescencia.* Quito: Registro Oficial. Obtenido de https://biblioteca.defensoria.gob.ec/handle/37000/3365#:~:text=Este%20C%C3%B3digo%20dispone%20sobre%20la,de%20libertad%2C%20dignidad%20y%20equidad.

Defensoría Pública del Ecuador. (2022). *Código Orgánico Integral Penal.* Quito: Asamblea Nacional del Ecuador. Obtenido de https://biblioteca.defensoria.gob.ec/handle/37000/3427#:~:text=Este%20C

%C3%B3digo%20tiene%20como%20finalidad,reparaci%C3%B3n%20integral%20de%20las%20v%C3%ADctimas.

Delgado , O. (2021). *Herramienta tecnológica de control parental sobre los contenidos de.* Investigación presentada como requisito para la obtención del título de Magister en Educación, mención Educación y Creatividad, UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO, Manta. Obtenido de http://repositorio.sangregorio.edu.ec/bitstream/123456789/1918/1/Herramienta%20tecnol%C3%B3gica%20de%20control%20parental%20sobre%20los%20contenidos%20de%20Internet%20y%20su%20aplicaci%C3%B3n%20como%20apoyo%20en%20el%20desempe%C3%B1o%20acad%C3%A9mico%20de

e-Governance Academy. (31 de Enero de 2023). *Ranking internacional de ciberseguridad: RD, a la cabeza de América Latina*. Obtenido de revistamercado: https://www.revistamercado.do/tecnologia/ranking-ciberseguridad-rd-avanza

El Congreso de la República. (2013, 21 de octubre). *Ley Nº 30096.* Gaceta oficial. Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

ElisaYuste. (2019). *CONTROL PARENTAL: QUÉ ES Y CÓMO APLICARLO*. Obtenido de elisayuste: https://www.elisayuste.com/control-parental-que-es-y-como-aplicarlo/

EPE. (19 de septiembre de 2022). *Las 10 mejores apps de control parental ¡Y gratis!* Obtenido de epe: https://www.epe.es/es/sociedad/20220919/10-mejores-apps-control-parental-75637206

Fernández, Y. (2019). *Google Family Link: qué es y cómo configurarlo para usar el control parental de Android*. Obtenido de xataka: https://www.xataka.com/basics/google-family-link-que-como-configurarlo-para-usar-control-parental-android

Fiscalía General del Estado. (Diciembre de 2021). *Criminologico*. Obtenido de Fiscalia General del Estado: https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

García Piña, C. A. (2008). Riesgos del uso de internet por niños y adolescentes. Estrategias de seguridad. *redalic*, 8. Obtenido de https://www.redalyc.org/articulo.oa?id=423640313006

García, K. (2023). *Aplicaciones que facilitan el Control Parental*. Obtenido de tipsorientadores: https://tipsorientadores.com/blog/tecnologia/aplicaciones-que-facilitan-el-control-parental/

Garmendia, M., Jiménez, E., Casado, M., & Mascheroni, G. (2015). *Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles.* Obtenido de Netchildrengomobile: https://netchildrengomobile.eu/ncgm/wp-content/uploads/2013/07/Net-Children-Go-Mobile-Spain.pdf

Gómez, P., Rial, A., Braña, T., Golpe, S., & Varela, J. (2017). Detección del uso problemático de Internet entre adolescentes españoles: prevalencia y variables relacionadas. *Cyberpsychology, Behavior y Social Networking*. Obtenido de https://www.liebertpub.com/doi/10.1089/cyber.2016.0262

Gonzalez, C. (Febrero de 2023). *La Unidad Nacional de Ciberdelito conmemora su doceavo aniversario al servicio de la ciudadanía*. Obtenido de Policia Nacional del Ecuador: https://www.policia.gob.ec/la-unidad-nacional-de-ciberdelito-conmemora-su-doceavo-aniversario-al-servicio-de-la-ciudadania/#:~:text=La%20Unidad%20Nacional%20de%20Ciberdelito%20de%20la%20Polic%C3%ADa%20Nacional%20del,las%20redes%20del%20mundo%20digital.

GR, R. (28 de julio de 2021). *Control parental: Protege y controla a tus hijos en Internet*. Obtenido de adslzone: Mejores Apps

Grupo Deidev. (2023). *SecureKids Control Parental*. Obtenido de Grupo Deidev: https://www.google.com/search?q=que+es+SecureKids&rlz=1C1UEAD_e

nEC1049EC1049&oq=que+es+SecureKids&aqs=chrome..69i57j69i60l2.6533j0j4&sourceid=chrome&ie=UTF-8

Hamed , M. (24 de Octubre de 2022). *La mejor aplicación de control parental para niños: seguimiento de actividades, conversaciones, llamadas y más*. Obtenido de review-plus: https://review-plus.com/es/how-to-monitor-everything-on-childs-phone/

Hernandez Coca, G. (Julio de Diciembre de 2017). *Metodo Analitico*. Obtenido de https://www.uaeh.edu.mx/docencia/P_Presentaciones/b_huejutla/2017/Metodo_Analitico.pdf

Hmong. (s.f.). *Familia Norton*. Obtenido de hmong: https://hmong.es/wiki/OnlineFamily.Norton

IAB Chile. (2012). Libro Blanco de las Mediciones. *silo*, 51. Obtenido de https://silo.tips/download/libro-blanco-de-las-mediciones-sistemas-de-medicion-de-la-industria-on-line-indi#

kaspersky. (2023). *KasperskySafe Kids*. Obtenido de kaspersky: https://www.kaspersky.es/safe-kids

kidlogger. (2023). *¿SABES LO QUE ESTÁN HACIENDO TUS HIJOS EN LÍNEA?* Obtenido de kidlogger: https://kidlogger.net/

Kuan, F. (18 de Agosto de 2017). *¿Qué es un dispositivo inteligente?* Obtenido de mokosmart: https://www.mokosmart.com/es/what-is-a-smart-device/

Lounsbury, K., Mitchell, K. J., & Finkelhor , D. (2011). La Verdadera Prevalencia del “Sexting”. *Centro de Investigación de Delitos contra Niños*, 5. Obtenido de https://scholars.unh.edu/ccrc/64/

Mercado, C., Pedraza, F., & Martínez, K. (2016). SEXTING: SU DEFINICIÓN, FACTORES DE RIESGO Y CONSECUENCIAS. *riunet*, 18. Obtenido de https://riunet.upv.es/handle/10251/73303

Montiel, I. J., Carbonell Vayá, E. J., & Salom García, M. (2014). VICTIMIZACIÓN INFANTIL SEXUAL ONLINE: ONLINE

GROOMING, CIBERABUSO Y CIBERACOSO SEXUAL. *researchgate*, 23. Obtenido de https://www.researchgate.net/publication/275273999_Victimizacion_Infantil_Sexual_Online_Online_Grooming_Ciberabuso_y_Ciberacoso_sexual

Moyano, A., Barahona, D., Forero, J., & Miller, A. (2017). Análisis de herramientas usadas para el control parental en dispositivos móviles con acceso a internet. *Repositorio Fundación Universitaria Compensar*. Obtenido de https://repositoriocrai.ucompensar.edu.co/handle/compensar/3334

Muguira, A. (s.f.). *Tipos de estudio de investigación y sus características*. Obtenido de Questionpro: https://www.questionpro.com/blog/es/tipos-de-investigacion-2/

Ortega, C. (s.f.). *Investigación cuantitativa. Qué es y cómo realizarla*. Obtenido de Questionpro: https://www.questionpro.com/blog/es/que-es-la-investigacion-cuantitativa/

Ortega. (2023). *Investigación analítica: Qué es, importancia y ejemplos*. Obtenido de questionpro: https://www.questionpro.com/blog/es/investigacion-analitica/

Parentalia. (2023). *Review Locategy: Características, beneficios y funciones*. Obtenido de Parentalia: https://parentalia.info/review-locategy-opiniones-y-funciones

PcHardwarePro. (2023). *Microsoft Family Safety for Windows 10: Características, Cómo configurar y usar*. Obtenido de pchardwarepro: https://www.pchardwarepro.com/microsoft-family-safety-for-windows-10-caracteristicas-como-configurar-y-usar/

Prados, H., & Fernández, S. (2007). Ciberbullyng, un problema de acoso escolar. *redalyc*, 21. Obtenido de redalyc: CIBERBULLYING, UN PROBLEMA DE ACOSO ESCOLAR

Salas Ocampo, D. (3 de diciembre de 2019). *Investigación bibliográfica*. Obtenido de investigaliacr: https://investigaliacr.com/investigacion/investigacion-bibliografica/

Sánchez Flores, F. A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. *Scielo*, 21. Obtenido de http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2223-25162019000100008#:~:text=Por%20enfoque%20cualitativo%20se%20entiende,Mej%C3%ADa%2C%20como%20se%20cit%C3%B3%20en

Sánchez, N. (2020). Herramienta de control parental basada en software libre. *Universidad de Sevilla*, 86. Obtenido de https://idus.us.es/handle/11441/106088

Securekids. (25 de Agosto de 2015). *¿Qué es el control parental y para qué sirve?* Obtenido de securekids: https://securekids.es/que-es-el-control-parental-y-para-que-sirve/

Segu-kids. (s.f.). *Control Parental*. Obtenido de segu-kids: https://www.segu-kids.org/padres/control-parental.html

Sinnaps. (2023). *INVESTIGACIÓN CUANTITATIVA. CARACTERÍSTICAS DEL MÉTODO CUANTITATIVO*. Obtenido de Sinnaps: https://www.sinnaps.com/blog-gestion-proyectos/metodo-cuantitativo#:~:text=El%20m%C3%A9todo%20cuantitativo%20est%C3%A1%20basado,la%20poblaci%C3%B3n%20a%20preguntas%20espec%C3%ADficas.

Sipbench. (2017). *Benchmarking de herramientas de control parental para la protección online de menores SIP-Bench III*. Obtenido de Sipbench: https://sipbench.eu/transfer/SIP_BENCH_III_4th_cycle_report.pdf

Softzone. (24 de marzo de 2023). *Protege a tus hijos de Internet con estos programas*. Obtenido de softzone: https://www.softzone.es/programas/utilidades/mejores-programas-control-parental-windows/

SSOO. (s.f.). *Control parental en Whatsapp: Mejores aplicaciones*. Obtenido de todosobretusistemaoperativo: https://www.todosobretusistemaoperativo.com/control-parental-en-whatsapp/

Supo Mendoza, J. A. (2022). *CIBEREXTORSIÓN Y SEXTORSIÓN EN EL CÓDIGO PENAL.* Obtenido de http://181.176.219.234/bitstream/handle/UPRIT/708/TESIS%20-%20SUPO%20MENDOZA.pdf?sequence=1&isAllowed=y

telecomunicaciones. (s.f.). *91% de ecuatorianos utiliza las redes sociales en su teléfono inteligente*. Obtenido de telecomunicaciones: https://www.telecomunicaciones.gob.ec/91-de-ecuatorianos-utiliza-las-redes-sociales-en-su-telefono-inteligente/#:~:text=A%20nivel%20urbano%20se%20registra,accede%20a%20las%20redes%20sociales.

Tiposdeinvestigacion. (13 de Octubre de 2020). *¿Qué es la investigación descriptiva?* Obtenido de tiposdeinvestigacion: https://tiposdeinvestigacion.review/que-es-la-investigacion-descriptiva/

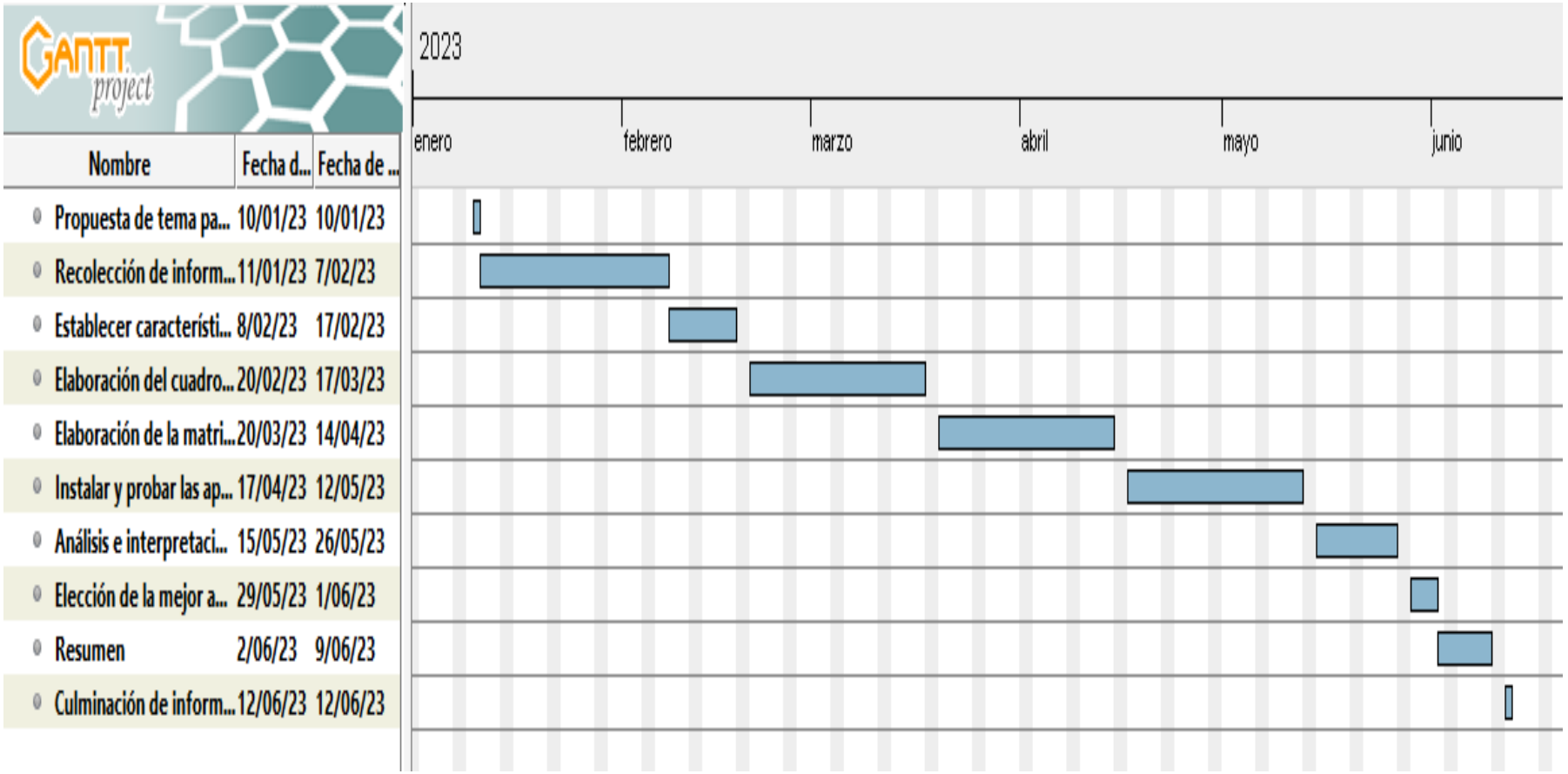
TUTFG. (2023). *¿Qué diferencias existen entre el método deductivo e inductivo?* Obtenido de tutfg: https://tutfg.es/metodo-inductivo-y-deductivo/

Villanueva , V., & Serrano, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes : una perspectiva de género. *Revista de psicología y educación*, 11. Obtenido de https://redined.educacion.gob.es/xmlui/handle/11162/220154

Xatakandroid. (06 de Septiembre de 2018). *Nueve apps Android de control parental para instalar en el móvil de tus hijos*. Obtenido de xatakandroid: https://www.xatakandroid.com/aplicaciones-android/nueve-apps-android-control-parental-para-instalar-movil-tus-hijos

ANEXOS

- **Cronograma (Gantt)**



- **Presupuesto Ejecutado**

Tabla 19

Presupuesto

RECURSO	CANTIDAD	PRECIO UNITARIO	TOTAL
Personal (Humano)	1	$0.00	$0.00
Carpetas	2	$0.75	$1.50
Pc Portátil	1	$0.00	$0.00
Smartphone	2	$0.00	$0.00
Esferos	2	$0.35	$0.70
Internet	Mensual (Por 6 Meses)	$25	$150
Electricidad	Mensual (Por 6 Meses)	$25.00	$150
Transporte	20	3.50	$70
		PRESUPUESTO TOTAL	$372.2

Elaborado por: Jairo Uchubanda

- **Instrumento de recopilación de datos**

  Modelo de entrevista

Tema:	Estudio comparativo de aplicaciones libres para control parental, año 2023
Objetivo:	Recopilar información sobre los ciberdelitos y conocer cómo se realiza el proceso en caso de que una persona esté siendo víctima de un ciberdelito.
Entrevistador:	Jairo Uchubanda
Entrevistado:	Sargento Quinso de la policía judicial

Cuestionario

1. **¿Qué son los ciberdelitos?**
2. **¿Cuáles son las características principales de los delitos informáticos?**
3. **¿Cuáles son las clases de delitos informáticos?**
4. **¿Existe alguna dependencia encargada del ciberdelito en Ecuador?**
5. **¿Qué hacer ante un ciberdelito?**
6. **¿Dónde se deja la denuncia?**
7. **¿Cómo procede la dependencia de ciberdelito en caso en caso de una denuncia?**
8. **¿Cuál es la sanción para una persona que comete ciberdelitos?**
9. **¿Existen casos de ciberdelitos en la ciudad de Guaranda?**
10. **¿Cómo prevenir un ciberdelito?**

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

ING. MÓNICA ELIZABETH BONILLA MANOBANDA EN CALIDAD DE DIRECTORA DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**ESTUDIO COMPARATIVO DE APLICACIONES LIBRES PARA CONTROL PARENTAL, AÑO 2023**", presentado por JAIRO LENIN UCHUBANDA GUAMARICA estudiante de la **Carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta URKUND, reflejando un **porcentaje de similitud del 7%**, como se puede evidenciar en el documento adjunto.

Guaranda, 16 de mayo del 2023

Atentamente,

Ing. Mónica Bonilla M.
Directora

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

Ouriginal
by Turnitin

Document Information

Analyzed document	Trabajo de investigación Jairo Uchubanda.docx (D167090289)
Submitted	5/16/2023 1:22:00 AM
Submitted by	
Submitter email	juchubanba@mailes.ueb.edu.ec
Similarity	7%
Analysis address	mbonilla.ueb@analysis.urkund.com

Sources included in the report

Entire Document

Hit and source - focused comparison, Side by Side

- Submitted text
  As student entered the text in the submitted document.
- Matching text
  As the text appears in the source.