Aplicación móvil inteligente de control parental para la detección temprana de riesgos digitales en menores

LAURA KARINA CAICEDO BORJA
JOHANN DAVID GUZMAN VELOSA
JENNY PATRICIA VARGAS NARANJO

Universidad EAN
Facultad de Ingeniería
Ingeniería de Sistemas
Bogotá, Colombia
2025

Aplicación móvil inteligente de control parental para la detección temprana de riesgos digitales en menores

LAURA KARINA CAICEDO BORJA
JOHANN DAVID GUZMAN VELOSA
JENNY PATRICIA VARGAS NARANJO

Trabajo de grado presentado como requisito para optar al título de
Ingeniería de Sistemas

Director:
MARIE JOSE CHERY LEAL

Universidad EAN
Facultad de Ingeniería
Ingeniería de Sistemas
Bogotá, Colombia
2025

Resumen

La creciente exposición de niños y adolescentes a dispositivos móviles conectados a internet ha incrementado los riesgos digitales, entre ellos la exposición a contenidos inapropiados, el ciberacoso, el grooming, el sexting y el uso excesivo de aplicaciones. Ante estas problemáticas, se identificó la necesidad de fortalecer las herramientas de supervisión parental existentes, las cuales presentan limitaciones en cuanto a efectividad, accesibilidad y detección en tiempo real.

El propósito de este trabajo de grado es desarrollar una aplicación móvil inteligente de control parental, apoyada en técnicas de inteligencia artificial, que permita detectar tempranamente riesgos digitales y generar alertas inmediatas a los padres o tutores sin afectar el rendimiento del dispositivo. La metodología adoptada corresponde a un enfoque aplicado, de tipo exploratorio–descriptivo, organizada en tres etapas: análisis de riesgos y limitaciones de controles existentes; diseño conceptual y técnico de la solución mediante prototipado, desarrollo y verificación de la funcionalidad del prototipo en entorno Android a través de pruebas de funcionamiento y usabilidad.

Los resultados obtenidos evidencian la viabilidad técnica y funcional del prototipo desarrollado, destacando su capacidad para identificar patrones de riesgo digital en tiempo real y emitir alertas inmediatas a los padres o acudientes. Las pruebas de funcionamiento y usabilidad realizadas demostraron un desempeño estable, una interfaz intuitiva y una respuesta eficiente del sistema, sin afectar el rendimiento del dispositivo. Asimismo, el análisis de costos reflejó una estructura financiera sostenible y acorde con la etapa de desarrollo del proyecto. En conjunto, estos hallazgos confirman que la integración de inteligencia artificial no solo fortalece la eficacia

del control parental, sino que también posibilita un monitoreo más preventivo, personalizado y ético, contribuyendo a fomentar entornos digitales más seguros y responsables para los menores.

Palabras clave: control parental, inteligencia artificial, seguridad digital, monitoreo en tiempo real, riesgos digitales, ética digital.

Abstract

The increasing exposure of children and adolescents to internet-connected mobile devices has increased digital risks, including exposure to inappropriate content, cyberbullying, grooming, sexting, and excessive app use. Given these problems, the need to strengthen existing parental monitoring tools was identified, as they present limitations in terms of effectiveness, accessibility, and real-time detection.

The purpose of this thesis is to develop a smart mobile parental control application, supported by artificial intelligence techniques, that allows for the early detection of digital risks and generates immediate alerts for parents or guardians without affecting device performance. The methodology adopted corresponds to an applied, exploratory-descriptive approach, organized into three stages: analysis of risks and limitations of existing controls; conceptual and technical design of the solution through prototyping; and development and verification of the prototype's functionality in an Android environment through performance and usability testing.

The results obtained demonstrate the technical and functional feasibility of the developed prototype, highlighting its ability to identify digital risk patterns in real time and send immediate alerts to parents or guardians. The functionality and usability tests showed stable performance, an intuitive interface, and efficient system response without affecting device performance. Likewise, the cost analysis revealed a sustainable financial structure consistent with the project's development stage. Altogether, these findings confirm that the integration of artificial intelligence not only enhances the effectiveness of parental control but also enables more preventive, personalized, and ethical monitoring, contributing to safer and more responsible digital environments for minors.

Keywords: parental control, artificial intelligence, digital security, real-time monitoring, digital risks, digital ethics.

Contenido

Lista de Figuras

Lista de Tablas

Lista de Anexos

Introducción

En la actualidad, el uso de dispositivos móviles por parte de niños y adolescentes se ha convertido en una parte habitual de su vida cotidiana. Sin embargo, esta creciente interacción con la tecnología también ha traído consigo diversos riesgos, facilitando el acceso a información, entretenimiento y comunicación, esta realidad tecnológica plantea oportunidades, pero también desafíos significativos especialmente para padres que desean proteger a sus hijos de los riesgos inherentes al uso del internet y plataformas digítales (Auxier & Perrin, 2020).

A partir de una revisión empírica y bibliográfica, se identificó que, si bien existen diversas herramientas de monitoreo para menores de edad, muchas carecen de supervisión en tiempo real o de sistemas inteligentes que detecten proactivamente riesgos potenciales, lo que limita la capacidad de los padres o tutores para intervenir de manera oportuna.

El objeto de esta investigación es el desarrollo de una aplicación móvil inteligente, diseñada para instalarse tanto en el dispositivo del menor como en el del padre o tutor, capaz de monitorear de forma continua la pantalla del menor mediante técnicas de inteligencia artificial. Esta permitirá el reconocimiento de textos y la detección automática de palabras clave o patrones asociados a contenidos riesgosos. La necesidad de esta solución surge ante la insuficiencia de los métodos tradicionales de control parental, para garantizar espacios digitales seguros y supervisión constante, y de la importancia de fomentar la interacción familiar para promover un uso responsable de internet, contribuyendo así al desarrollo académico y social de los menores (Delgado-Zambrano, 2022).

La pregunta central que orienta esta investigación es: ¿Cuál es la solución tecnológica, basada en inteligencia artificial, más adecuada para garantizar un control parental efectivo y en tiempo real que permita la detección temprana de riesgos en dispositivos móviles de menores y

que facilite la intervención oportuna de padres o tutores? Esta interrogante guía el desarrollo del sistema propuesto, así como la evaluación de su impacto en la seguridad digital infantil.

El presente documento se organiza en tres secciones principales. La sección introductoria aborda la problemática, los objetivos, la contextualización teórica y el estado del arte relacionado con el control parental y el uso de la inteligencia artificial en la protección digital. La sección metodológica detalla el enfoque adoptado para el diseño y desarrollo del prototipo, describiendo los pasos empleados para alcanzar los objetivos propuestos. La sección de resultados presenta los hallazgos obtenidos en las pruebas de funcionamiento y las conclusiones que expone las reflexiones finales y los aportes derivados de la investigación.

Esta estructura busca ofrecer una comprensión integral del proyecto, desde la identificación de la problemática hasta la propuesta tecnológica, demostrando la viabilidad y relevancia de una aplicación de control parental inteligente que contribuya a garantizar entornos digitales más seguros para los menores, en coherencia con las tendencias actuales en tecnología y protección infantil.

Objetivos

Objetivo General

Desarrollar una aplicación móvil inteligente de control parental apoyada en inteligencia artificial que permita la detección temprana de riesgos digitales y la intervención oportuna de los acudientes de los menores.

Objetivos Específicos

- Analizar los principales riesgos digitales que enfrentan los menores en el uso de dispositivos móviles y las limitaciones de los controles parentales existentes, a partir de encuestas aplicadas a padres y acudientes, complementadas con una revisión de fuentes documentales y tecnológicas.
- Estructurar el modelo funcional y los componentes técnicos del prototipo de la aplicación móvil, incorporando módulos de autenticación, monitoreo de uso de aplicaciones y generación de reportes, así como técnicas de inteligencia artificial para la detección temprana de riesgos digitales en menores, con base en los resultados del diagnóstico obtenido en la fase inicial.
- Verificar la funcionalidad del prototipo mediante pruebas simuladas en dispositivos móviles, para determinar su efectividad en la detección de riesgos digitales y la pertinencia de las notificaciones generadas para los acudientes, garantizando su operatividad, estabilidad y facilidad de uso.

Definición del Problema

En la actualidad el uso cada vez más intensivo de dispositivos móviles con acceso a internet por parte de niños y adolescentes establece uno de los fenómenos tecnológicos más significativos de los últimos tiempos. Según Auxier & Perrin (2020), esta interacción temprana con entornos digitales incrementa las oportunidades de aprendizaje, socialización y entretenimiento, pero aumenta la exposición a contenido inapropiado, el ciberacoso, la suplantación de identidad y la pérdida de privacidad. La supervisión parental tradicional, la cual está basada en la revisión ocasional del dispositivo o en configuraciones básicas de filtrado, resulta insuficiente para responder a la inmediatez y diversidad de las amenazas digitales actuales.

Algunos estudios científicos identifican a la inteligencia artificial como una tecnología con alto potencial para mejorar la efectividad de estas aplicaciones, permitiendo el reconocimiento de patrones, la identificación contextual de contenidos y la generación de alertas oportunas (Alrusaini & Beyari, 2022a). Sin embargo, la adopción de soluciones inteligentes en el ámbito doméstico sigue siendo limitada, en gran medida por la complejidad técnica, la escasa personalización y la falta de integración con mecanismos de comunicación en tiempo real entre dispositivos.

En este contexto, se plantea la necesidad de una solución tecnológica que supere las limitaciones actuales mediante el desarrollo de un sistema de control parental inteligente, capaz de monitorear de forma continua y en tiempo real el contenido que el menor visualiza en su dispositivo, con el fin de detectar de manera proactiva posibles riesgos digitales relacionados con violencia, acoso, contenido sexual o uso de drogas.

Este planteamiento busca responder a una necesidad social y tecnológica urgente, aportando una propuesta innovadora alineada con las mejores prácticas en seguridad digital, usabilidad y ética aplicada al entorno familiar.

Según un balance de la policía nacional sobre ciberseguridad (CAI Virtual CIBERCRIMEN, 2024), en el año 2024 se registraron 77.866 casos relacionados con delitos informáticos en Colombia, reflejando un incremento del 23 % en comparación con el año anterior. Bogotá fue la ciudad con mayor incidencia, concentrando aproximadamente el 33 % de las denuncias reportadas. Al trasladar esta problemática al contexto infantil, se evidencia la alta vulnerabilidad de los menores frente a estas amenazas.

Entre los principales riesgos digitales que enfrentan los menores se encuentran la dependencia excesiva a la tecnología, el acoso en línea, el *grooming* (acercamiento de adultos con fines de abuso) y los desafíos virales, todos con potencial de afectar su integridad y bienestar (Portal ICBF - Instituto Colombiano de Bienestar Familiar ICBF, 2022). Asimismo, el uso de plataformas como las redes sociales representa un mayor nivel de exposición, ya que facilitan el contacto directo con los menores y permiten el acceso no autorizado a su información personal (Trejos-Gil & Vélez, 2023).

Justificación

El uso masivo de dispositivos móviles por parte de niños, niñas y adolescentes ha generado nuevas dinámicas de interacción, pero también ha incrementado los riesgos asociados a la exposición a contenidos inapropiados, ciberacoso, grooming, sexting y conductas adictivas. Aunque en el mercado existen soluciones como Google Family Link, Qustodio o Bark, estas aplicaciones presentan limitaciones significativas: bajo nivel de detección proactiva de riesgos, ausencia de mecanismos avanzados de análisis contextual, y en algunos casos, afectaciones en el rendimiento del dispositivo (Delgado-Zambrano, 2022). A ello se suma que un alto porcentaje de aplicaciones distribuidas fuera de tiendas oficiales presenta deficiencias en cifrado, manejo de datos y transparencia en los permisos solicitados, llegando incluso a ser catalogadas como herramientas de vigilancia intrusiva más que como instrumentos de protección (Madeline et al., 2025).

La conveniencia de este proyecto radica en que se alinea a las tendencias actuales del sector tecnológico, donde el mercado global de aplicaciones de control parental se proyecta a crecer de 1.7 mil millones de USD en 2025 a más de 4.2 mil millones en 2035, con una tasa de crecimiento anual compuesta del 9.8 %, impulsado por la preocupación de los padres frente a la seguridad digital y el bienestar de sus hijos. Sin embargo, la mayoría de estas herramientas aún se sustentan en filtros estáticos o configuraciones poco flexibles, careciendo de sistemas inteligentes capaces de interpretar contextos emergentes y generar alertas tempranas de situaciones de riesgo (Future Market Insights, 2025).

Desde la perspectiva empresarial, el proyecto abre la posibilidad de generar un producto diferenciado en un mercado en expansión, integrando inteligencia artificial aplicada al análisis de

contenido en tiempo real. Este enfoque no solo fortalece el potencial emprendedor y competitivo, sino que también favorece la evolución de procesos organizacionales en empresas de software orientadas a seguridad digital y soluciones educativas.

El valor teórico del estudio reside en la integración de procesamiento de lenguaje natural (NLP) y visión por computadora, áreas de gran relevancia en la investigación contemporánea en inteligencia artificial. La propuesta también tiene alta relevancia social, al contribuir a la protección de los derechos de los menores en entornos digitales, promoviendo la formación de hábitos tecnológicos responsables. En el plano práctico, se traduce en una aplicación funcional que provee a padres y tutores de alertas oportunas, confiables y éticas, sin comprometer la privacidad de los menores, gracias al análisis local de datos y al cifrado de extremo a extremo.

Finalmente, este proyecto se enmarca en el campo de Ciencia, Tecnología e Innovación, dentro del grupo de investigación en Tecnológico Ontare y particularmente en la línea de investigación en tecnología de la información y comunicaciones. Desde esta perspectiva, la propuesta se articula con la filosofía institucional de fomentar proyectos que no solo aporten valor académico y científico, sino que también respondan a problemáticas sociales actuales con impacto real y sostenible.

Marco Teórico

El marco teórico constituye la base conceptual que sustenta el desarrollo del proyecto, permitiendo comprender los elementos tecnológicos, sociales y psicológicos involucrados en el uso de dispositivos móviles por parte de menores de edad. En esta sección se abordan los principales conceptos, teorías y estudios previos relacionados con los riesgos digitales, el control parental, la inteligencia artificial y las herramientas de procesamiento de datos aplicadas a la seguridad infantil. Este análisis proporciona los fundamentos necesarios para el diseño de una solución tecnológica que contribuya a la detección temprana de comportamientos o contenidos de riesgo y a la intervención oportuna de padres o tutores.

Uso De Dispositivos Móviles Por Parte De Menores De Edad

En la última década, el acceso a dispositivos móviles por parte de niños y adolescentes se ha incrementado de manera exponencial. De acuerdo con Beyens et al (2024), más del 70% de los menores entre 8 y 15 años utilizan smartphones de forma cotidiana, con fines de entretenimiento, comunicación y aprendizaje. Este uso temprano favorece la alfabetización digital, pero también implica la exposición a entornos en línea poco regulados.

Los patrones de uso reflejan que más de la mitad de los adolescentes pasan cuatro horas o más frente a pantallas diariamente, con un consumo marcado por la multitarea, la visualización de contenidos breves y el acceso nocturno, lo cual interfiere con el sueño, el rendimiento académico y la salud mental. Sus actividades principales incluyen mensajería instantánea, redes sociales como TikTok, Instagram y Snapchat, y plataformas de video como YouTube, las cuales combinan espacios públicos y privados alimentados por algoritmos de recomendación que pueden exponer rápidamente a contenidos inapropiados o riesgosos (UNICEF, 2021).

Dicho contexto ha potenciado la aparición de problemáticas como ciberacoso, *grooming*, *sexting*, desinformación, exposición a retos extremos y vulneraciones de la privacidad, fenómenos que requieren soluciones más sofisticadas que los filtros tradicionales, pues ocurren en espacios privados y bajo lógicas algorítmicas (Torrecillas-Lacave et al., 2020). Adicionalmente, la existencia de brechas digitales y desigualdades en la alfabetización tecnológica parental incrementan la vulnerabilidad de algunos menores, evidenciando la necesidad de un enfoque integral que combine herramientas de inteligencia artificial con estrategias educativas y de mediación familiar (UNICEF, 2021).

Para este fin, un sistema de control parental efectivo puede incluir detección en tiempo real de riesgos mediante procesamiento de lenguaje natural, visión por computadora y análisis de patrones de uso ajustándose, ajustarse a la edad del menor, garantizando privacidad a través de procesamiento local y ofreciendo, explicabilidad en las alertas y acompañandose de materiales de formación que fortalezcan la intervención de padres y tutores, pues la tecnología, aunque potente, solo alcanza su máxima efectividad cuando se integra con prácticas de acompañamiento y diálogo en el hogar (NIST, 2023).

Principales Riesgos Digitales

El entorno digital representa una fuente de oportunidades para el aprendizaje y la socialización de los menores; sin embargo, también los expone a una amplia variedad de riesgos que pueden afectar su bienestar emocional, social y académico. Entre los más relevantes se encuentran el ciberacoso, que consiste en el uso de medios digitales para hostigar o humillar a otros usuarios; el *grooming*, donde adultos establecen contacto con menores con fines de manipulación o abuso sexual; y el *sexting*, entendido como el envío o recepción de contenidos sexuales que pueden derivar en extorsión o exposición pública (UNICEF, 2023).

Otro riesgo creciente es la adicción a internet y a las redes sociales, caracterizada por un uso compulsivo que interfiere con las actividades cotidianas y el rendimiento escolar. Esta conducta puede generar ansiedad, déficit de atención y dependencia emocional hacia la validación social en línea. Asimismo, la exposición a desinformación o noticias falsas puede influir negativamente en la percepción de la realidad y en la toma de decisiones de los menores, dificultando el desarrollo del pensamiento crítico (Sáiz-Manzanares et al., 2023).

Finalmente, el acceso a contenido violento o sexual explícito sin supervisión adulta puede generar alteraciones en el desarrollo cognitivo y emocional, además de normalizar comportamientos inapropiados o de riesgo. Este tipo de exposición temprana afecta la forma en que los menores interpretan las relaciones sociales y los valores morales asociados al respeto y la privacidad (Torrecillas-Lacave et al., 2020).

El acceso temprano y sin restricciones a redes sociales como Facebook, Instagram o TikTok ha expuesto a los menores a múltiples riesgos digitales Torrecillas-Lacave et al (2020) en su revisión sistemática de literatura sobre ciberdelitos en menores, identificaron que los peligros más comunes incluyen ciberacoso, *grooming, sexting* y exposición a contenido sexual explícito. Estos fenómenos generan consecuencias negativas a nivel emocional, social y académico, evidenciando la vulnerabilidad de los menores frente a entornos digitales poco regulados. En este contexto, un sistema de control parental inteligente con IA puede constituirse en una herramienta clave para identificar y notificar amenazas en tiempo real, reduciendo la exposición de los menores a situaciones de riesgo antes de que escalen en problemas graves (Torrecillas-Lacave et al., 2020).

Control Parental

El control parental constituye una estrategia esencial para guiar el uso responsable de la tecnología en menores. Según P.-C. Muñoz-Carril et al., (2023), los padres que emplean mecanismos de supervisión estructurados logran reducir la exposición a riesgos digitales y fortalecen la alfabetización mediática de sus hijos.

El control parental se entiende como el conjunto de estrategias, prácticas y herramientas diseñadas para supervisar, guiar y proteger la interacción de los menores con dispositivos tecnológicos e internet. Su propósito no se limita únicamente a restringir el acceso a determinados contenidos, sino que busca equilibrar la seguridad con el desarrollo de la autonomía digital infantil. Entre sus objetivos principales destacan la prevención de la exposición a contenidos inadecuados, como la violencia explícita, la pornografía o los discursos de odio; la regulación del tiempo de uso de dispositivos móviles, con el fin de evitar la sobreexposición y promover un uso equilibrado de la tecnología y la promoción de hábitos digitales saludables, incentivando un consumo responsable y educativo de los entornos digitales; y el fomento del diálogo y la corresponsabilidad entre padres e hijos, entendiendo que la supervisión efectiva debe basarse en la confianza mutua y en la construcción de acuerdos familiares en torno al uso de la tecnología. De esta manera, el control parental trasciende la simple restricción, consolidándose como un recurso integral para la protección y la educación digital (Wang et al., 2021).

Tipos De Control Parental

El control parental puede clasificarse en diferentes tipologías según su finalidad y nivel de intervención:

Preventivo: se centra en la definición de reglas antes de que los menores accedan a los dispositivos, tales como establecer horarios de uso, definir espacios libres de tecnología o limitar el tiempo frente a la pantalla (Cheng Yong et al., 2025).

Restrictivo: consiste en la aplicación de mecanismos de bloqueo a aplicaciones, páginas web o categorías de contenido que se consideran inapropiados para la edad del menor, utilizando filtros de navegación o contraseñas de acceso (Cheng Yong et al., 2025).

Monitoreo Activo: implica el análisis constante de las actividades digitales del menor en tiempo real, a través de reportes de navegación, registro de aplicaciones utilizadas o alertas automáticas sobre posibles riesgos (Cheng Yong et al., 2025).

Supervisión Colaborativa: promueve un modelo de acompañamiento basado en el uso conjunto de las tecnologías, el diálogo abierto y la negociación de normas, fortaleciendo así la mediación parental positiva y la alfabetización digital de los niños.

Cada una de estas tipologías aporta un enfoque distinto, y su combinación estratégica permite diseñar un control parental más equilibrado, en el que se integren la seguridad, la confianza y la educación digital como pilares fundamentales (Cheng Yong et al., 2025).

Herramientas Tradicionales De Control Parental

Las herramientas tradicionales de control parental, como Google Family Link, Norton Family, Qustodio o Kaspersky Safe Kids, permiten a los padres establecer límites básicos de uso, como el tiempo de pantalla, el bloqueo de aplicaciones, el filtrado de contenido web o la geolocalización del dispositivo. Estas aplicaciones han sido ampliamente utilizadas como primera medida de supervisión digital, ya que ofrecen funciones de fácil acceso y compatibilidad con múltiples sistemas operativos (Theopilus et al., 2024).

Sin embargo, su efectividad se ve limitada por varios factores. En primer lugar, presentan una configuración compleja para usuarios con bajo nivel de alfabetización digital, lo que dificulta su personalización y mantenimiento. En segundo lugar, los menores tienden a mostrar resistencia o estrategias de evasión, como el uso de cuentas secundarias, el modo incógnito o el cambio de permisos del sistema, lo que reduce la fiabilidad de los reportes (Theopilus et al., 2024).

Control Parental y Supervisión Digital

La complejidad del ecosistema digital actual exige mecanismos eficaces de control parental que permitan a los padres guiar y acompañar a los menores en su interacción con las tecnologías. En su estudio P. C. Muñoz-Carril et al. (2023a), con 885 padres de niños de 6 a 12 años, encontraron que el 93,7% utiliza algún tipo de control parental para regular el uso de smartphones, siendo las medidas más frecuentes la limitación del tiempo de conexión y la restricción mediante contraseñas. Observaron que el nivel educativo de los padres influye directamente en el tipo y número de estrategias aplicadas: aquellos con más información académica tienden a usar más mecanismos de control y supervisión. Asimismo, se evidenció que la edad del menor es un factor determinante, ya que los preadolescentes reciben mayor supervisión que los niños de menor edad P. C. Muñoz-Carril et al. (2023a).

Herramientas de Control Parental en Contextos Educativos

La implementación de aplicaciones de control parental en entornos escolares ha demostrado que estas no solo contribuyen a fortalecer la seguridad digital infantil, sino que también inciden positivamente en el desempeño académico.

Según Torrecillas-Lacave et al., (2020), herramientas como bloqueadores de contenido y filtros de navegación mejoran la concentración, reducen la dispersión durante las clases en línea y apoyan a los padres en la supervisión del estudio en casa. Muchos padres, especialmente aquellos con limitadas competencias digitales, enfrentan dificultades para configurar o interpretar correctamente las aplicaciones, lo cual limita su adopción. Por ello, los autores recomiendan que los sistemas de control parental se diseñen con interfaces intuitivas, acompañadas de recursos educativos y guías prácticas, de manera que no solo funcionen como herramientas restrictivas, sino también como aliados en el proceso de formación académica y digital de los menores (Torrecillas-Lacave et al., 2020).

Tecnologías y Funcionalidades Clave en Aplicaciones de Control Parental

Las aplicaciones modernas de control parental integran diversas funcionalidades que buscan garantizar la seguridad digital de los menores. Entre las más comunes se encuentra el monitoreo en tiempo real de la actividad en pantalla, lo cual permite a los padres conocer qué aplicaciones y contenidos están siendo consumidos. Asimismo, estas herramientas incluyen el filtrado de contenido mediante algoritmos capaces de detectar palabras clave, imágenes y patrones asociados a riesgos potenciales, lo que contribuye a prevenir la exposición temprana a información inapropiada (Alrusaini & Beyari, 2022a).

Otra característica destacada es la geolocalización y el seguimiento de desplazamientos, función que brinda a los tutores la posibilidad de conocer la ubicación del menor en todo momento y reaccionar ante posibles situaciones de peligro. De igual forma, las aplicaciones suelen incorporar notificaciones automáticas que alertan de manera inmediata a los padres sobre eventos sospechosos o actividades consideradas peligrosas (Alrusaini & Beyari, 2022a).

Finalmente, algunas de estas soluciones fomentan la transparencia familiar a través de paneles compartidos, los cuales facilitan la supervisión conjunta, así como la integración de recomendaciones educativas personalizadas que orientan el consumo digital de los niños hacia prácticas responsables y seguras (Alrusaini & Beyari, 2022a).

Ética y Privacidad en el Uso de la Tecnología y el Monitoreo Digital

El uso de la inteligencia artificial (IA) para monitorear a menores plantea dilemas éticos y de privacidad significativos. La tensión entre garantizar la seguridad infantil y respetar el derecho a la privacidad se configura como un eje central de la discusión. El estudio de Madeline et al. (2025) aborda este desafío al examinar las dificultades de recopilar datos objetivos sobre el uso de smartphones. Su propuesta de un enfoque basado en *digital citizen science* (ciencia ciudadana digital), en el que los jóvenes pueden compartir, retirar o eliminar sus propios datos, constituye un modelo relevante para el diseño de aplicaciones de control parental. Este enfoque sugiere que al prototipo debe incorporarse mecanismos transparentes de consentimiento informado, asegurando que tanto padres como hijos comprendan qué datos se recopilan, con qué propósito y cómo se gestionan.

En la misma línea, el artículo de Dutta (2025) sobre IA y privacidad enfatiza que, aunque la inteligencia artificial puede reducir amenazas cibernéticas mediante detección de anomalías en tiempo real y el uso de aprendizaje federado, también introduce riesgos inherentes, como el sesgo algorítmico y la recopilación excesiva de información sensible. Por ello, el diseño de la aplicación debe contemplar un marco de gobernanza ética de la IA, que garantice un manejo responsable de los datos y prevenga sesgos injustos en los algoritmos de detección. Asimismo, principios recogidos en normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y la *Family Educational Rights and Privacy Act* (Ley de Derechos Educativos

y Privacidad Familiar), aún cuando no sean de aplicación directa en todas las jurisdicciones, ofrecen guías universales para el respeto de los derechos de los usuarios (Dutta, 2025).

Por su parte, la investigación de Dedkova et al (2022) sobre las fuentes de información en seguridad digital utilizadas por los padres, complementa esta discusión. Sus hallazgos muestran que las familias recurren a diversas fuentes (internet, expertos, pareja) y que las habilidades digitales parentales influyen en sus prácticas de mediación. Esto evidencia que la aplicación no debe limitarse a ser una herramienta de supervisión tecnológica, sino que también ha de constituirse en una fuente confiable de información y formación para los padres.

El monitoreo de menores mediante IA plantea importantes desafíos éticos y legales. Muñoz-Carril et al. (2023b) resalta que, si bien estas tecnologías permiten detectar riesgos en tiempo real y anticipar amenazas cibernéticas, también pueden derivar en prácticas de vigilancia excesiva, afectando la privacidad y autonomía de los menores. Entre los principales riesgos menciona la recolección desproporcionada de datos sensibles, la posibilidad de sesgos en los algoritmos de detección y la falta de transparencia en el manejo de la información.

El autor propone como solución la incorporación de principios de gobernanza ética de la IA, que incluyan transparencia, consentimiento informado, explicabilidad de los algoritmos y respeto por los derechos digitales de los usuarios. También recomienda que los desarrolladores tomen como referencias normativas internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa o la Family Educational Rights and Privacy Act (FERPA) en Estados Unidos.

Principio de Privacidad por Diseño en Entornos Móviles

El principio de privacidad por diseño enmarca la importancia de la protección de datos, la cual debe estar incorporada en la arquitectura del sistema desde su concepción. En el contexto de

aplicaciones móviles con Reconocimiento Óptico de Caracteres (OCR) y Procesamiento del Lenguaje Natural (PLN), esto garantiza que el análisis se ejecute en el dispositivo del menor y únicamente transmitirá los metadatos mínimos y alertas críticas. Lo anterior garantiza y reduce la exposición de información sensible y mejora la confianza de padres y tutores en el uso de la herramienta (NIST, 2023).

Planes Familiares de Medios y Mediación Parental Positiva

La American Academy of Pediatrics (AAP) aconseja la implementación de planes familiares que permitan fomentar conversaciones y acuerdos sobre el uso responsable de la tecnología. Estos lineamientos destacan la importancia de que las herramientas de control parental funcionen como soporte a la mediación positiva y no como mecanismos de vigilancia intrusiva (Olivero et al., 2025). También deben incluir recomendaciones de este tipo en la aplicación, como recordatorios de diálogo o modos de sensibilidad ajustable, lo que contribuye a un mayor impacto preventivo y educativo.

Inteligencia Artificial Enfocada en el Control Parental

La inteligencia artificial (IA) ha pasado de ser un concepto teórico en la década de 1950 a consolidarse como un elemento esencial en múltiples sectores. Sus primeras aplicaciones se centraron en los sistemas expertos, pero el desarrollo de las redes neuronales y del aprendizaje automático, entre las décadas de 1980 y 1990, marcó un avance significativo al posibilitar el procesamiento de grandes volúmenes de datos y la emulación de ciertos aspectos del razonamiento humano (Antonio et al., 2023).

En la actualidad, la IA se integra de manera transversal en ámbitos como la salud, las finanzas, la educación y la seguridad digital, actuando como un motor de innovación y

optimización de procesos (Antonio et al., 2023). Esta versatilidad y capacidad de adaptación la posicionan como una tecnología estratégica para abordar desafíos complejos, incluyendo aquellos relacionados con la protección y el bienestar digital de los menores.

Inteligencia Artificial Aplicable Al Control Parental y la Ciberseguridad

La inteligencia artificial (IA) aplicada al control parental constituye un recurso estratégico para enfrentar los desafíos que presentan los entornos digitales en los que interactúan los menores. A través de distintas ramas de la IA, es posible anticipar riesgos, identificar comportamientos anómalos y orientar a los usuarios hacia prácticas seguras. En primer lugar, el *Machine Learning* supervisado y no supervisado permite analizar grandes volúmenes de datos y detectar patrones de riesgo vinculados a conductas digitales inusuales, como cambios abruptos en los horarios de conexión, interacciones con desconocidos o descargas de aplicaciones no autorizadas. En segundo lugar, el Procesamiento de Lenguaje Natural (PLN) ofrece herramientas para examinar conversaciones en chats, redes sociales y foros, identificando palabras clave, emociones o contextos que sugieran la presencia de ciberacoso, *sexting* o *grooming*, generando alertas tempranas para la intervención parental.

Asimismo, la visión por computadora posibilita la clasificación automática de imágenes y videos, detectando contenido explícito, violento o inapropiado, lo que contribuye a prevenir la exposición de los menores a material perjudicial. Finalmente, los sistemas de recomendación se constituyen en un componente formativo, ya que, a partir del análisis de preferencias y comportamientos, sugieren alternativas de contenido educativo y saludable, promoviendo hábitos digitales responsables. De este modo, la IA no solo fortalece la protección frente a amenazas, sino que también fomenta la construcción de un entorno digital más seguro y positivo para los niños y adolescentes (Alrusaini & Beyari, 2022b).

En conclusión, la IA en ciberseguridad permite la detección de anomalías y la generación de respuestas automatizadas en tiempo real (Dutta, 2025). En el contexto infantil, esta tecnología es clave para anticipar amenazas digitales y alertar oportunamente a los padres.

Inteligencia Artificial Aplicada a la Protección Digital

El uso de inteligencia artificial (IA) en aplicaciones de control parental constituye un campo emergente que busca no solo detectar riesgos digitales, sino también promover un entorno de aprendizaje seguro. Alsuraini y Beyari (2022) analizaron el efecto de la IA en el comportamiento infantil en el contexto saudí, destacando que las aplicaciones que integran IA no se limitan a restringir accesos, sino que también orientan hacia conductas digitales positivas. Según los autores, este enfoque resulta más sostenible, ya que fomenta hábitos responsables y reduce la dependencia exclusiva de medidas restrictivas. En particular, resaltan que la IA es capaz de aprender de los patrones de uso de cada menor, adaptando las medidas de control según el comportamiento observado. Así, la IA permite generar un control parental dinámico y personalizado, capaz de evolucionar junto con el desarrollo del menor y ajustarse a los riesgos emergentes en entornos digitales.

Inteligencia Artificial Confiable y La Gestión de Riesgos

La incorporación de sistemas que se basan en inteligencia artificial para el control parental debe enmarcase bajo principios de IA confiable, los cuales deben contemplar tanto riesgos técnicos como sociotécnicos. El National Institute of Standards and Technology (NIST) desarrolló el Artificial Intelligence Risk Management Framework (AI RMF), el cual genera lineamientos para identificar, evaluar y mitigar riesgos asociados a sistemas de IA durante todo su ciclo de vida (NIST, 2023).

Políticas Internacionales Sobre Inteligencia Artificial y Niñez

Organismos como UNICEF han resaltado la necesidad de orientar la inteligencia artificial hacia la protección de los derechos de los niños, promoviendo la privacidad, el consentimiento informado y la transparencia. El documento AI for Children (UNICEF, 2021) enfatiza que los sistemas tecnológicos destinados a menores deben priorizar la minimización de datos y la creación de entornos digitales seguros y no invasivos. Integrar estas directrices fortalece la aceptación social y ética de la aplicación.

Antecedentes de Seguridad Digital y Control Parental

La seguridad digital infantil se ha convertido en una prioridad ante el aumento del acceso de niños y adolescentes a internet y redes sociales. Los dispositivos móviles permiten la creación y consumo de contenido sin supervisión constante, exponiendo a los menores a riesgos como el ciberacoso, el *grooming*, el acceso a contenido inapropiado y la pérdida de privacidad (Beyens et al., 2024)

Las herramientas de control parental han evolucionado desde sistemas restrictivos hacia enfoques más equilibrados que promueven la educación digital y la confianza mutua. Estudios recientes, como los de Beyens et al (2024), sugieren que las aplicaciones efectivas son aquellas que combinan funciones de monitoreo con dinámicas colaborativas, gamificación y establecimiento conjunto de metas, en lugar de únicamente aplicar vigilancia (Beyens et al., 2024).

En el ámbito de la seguridad digital, la inteligencia artificial (IA) ofrece posibilidades que trascienden el simple filtrado de contenido. La investigación de Barzilay et al. (2023), aunque centrada en la detección de riesgo de suicidio en adolescentes, presenta un modelo metodológico basado en el uso de *passive sensing* (monitoreo pasivo) de patrones de comunicación y actividad

en dispositivos móviles para identificar correlaciones con conductas de riesgo. Este enfoque demuestra el potencial de la IA para detectar señales tempranas sin depender exclusivamente de la intervención directa del usuario.

El diseño de estas soluciones debe tener en cuenta teorías como la Teoría del Aprendizaje Social y la Teoría del Apego, las cuales resaltan que la supervisión parental es más efectiva cuando se fomenta el diálogo y la participación del menor en la gestión de su vida digital (Hernandez et al., 2024).

El estudio de Theopilus et al. (2024) sobre la adicción a internet en niños indonesios evidencia las limitaciones de las intervenciones digitales existentes, como Google Family Link. Aunque los participantes reconocieron los beneficios de estas herramientas para promover comportamientos digitales saludables, también señalaron barreras significativas. Una de ellas fue la funcionalidad y usabilidad limitadas, que dificultaban el aprovechamiento completo de las aplicaciones disponibles. Asimismo, se identificó la falta de compatibilidad cultural, ya que muchas de estas soluciones no estaban adaptadas a los contextos y prácticas familiares propias de su entorno.

Otro aspecto relevante fueron las preocupaciones sobre la privacidad de los datos, pues existía desconfianza acerca del manejo de la información personal de los menores. Finalmente, se destacaron los desafíos en la relación padre-hijo, dado que, en algunos casos, el uso de estas aplicaciones podía generar tensiones y resistencias en la comunicación familiar.

Estos hallazgos resultan esenciales para el diseño del prototipo, pues sugieren que una aplicación de control parental debe trascender el papel de un mero sistema de monitoreo. Es necesario que funcione como una herramienta que fomente la alfabetización digital en niños y padres, facilite la comunicación y respalde la toma de decisiones informadas, en lugar de

enfocarse únicamente en la restricción de contenidos. El modelo propuesto por Theopilus et al. (2024), basado en actividades sustitutivas y en el desarrollo de competencias en los menores, ofrece una dirección clara: la aplicación no debe limitar, sino también promover un uso positivo y enriquecedor de la tecnología.

En consonancia, la investigación de Cheng Yong et al. (2025) refuerza la idea de que no existe un enfoque único para la "mediación digital". Su metaanálisis evidencia que la mediación positiva, la mediación negativa y el "uso conjunto" (*co-use*) tienen efectos diferenciados en el bienestar digital infantil. Esto implica que un sistema de monitoreo no debe ser intrusivo o punitivo, sino que ha de diseñarse para complementar la comunicación abierta y un estilo de crianza basado en la confianza.

Análisis de Restricciones

Los problemas de ingeniería admiten múltiples soluciones, sin embargo, cada alternativa se ve condicionada por restricciones de diferente índole que pueden impedir, limitar o retrasar la consecución de los objetivos planteados. En el caso del desarrollo de una aplicación móvil inteligente de control parental, basada en inteligencia artificial, dichas restricciones deben analizarse desde un enfoque técnico, normativo, económico, social, ambiental y organizacional.

Ambientales

Si bien el impacto ambiental de un software es bajo en comparación con proyectos industriales, el consumo energético asociado al entrenamiento de modelos de inteligencia artificial y al uso de servidores en la nube puede generar huella de carbono indirecta. Asimismo, la ejecución en tiempo real de modelos de IA en dispositivos móviles implica un mayor consumo de batería y recursos del dispositivo, lo cual limita la viabilidad de soluciones muy pesadas.

Para mitigar esta restricción, se propone optimizar los algoritmos de inteligencia artificial mediante el uso de modelos livianos (lightweight AI), reducir la frecuencia de procesamiento en segundo plano, y aprovechar servicios en la nube con infraestructura sostenible y aprovechar servicios en la nube con infraestructura sostenible, respaldada por certificaciones de eficiencia energética como ISO 50001 (gestión de la energía), Energy Star para centros de datos, o certificaciones de construcción sostenible como LEED. Además, se recomienda implementar técnicas de apagado automático y gestión dinámica de recursos para minimizar el consumo de batería en los dispositivos. Además, se recomienda implementar técnicas de apagado automático y gestión dinámica de recursos para minimizar el consumo de batería en los dispositivos.

Económicas

La disponibilidad de recursos financieros condiciona el alcance del proyecto. El costo de infraestructura en la nube, licencias de software, adquisición de dispositivos para pruebas y servicios especializados de IA puede superar el presupuesto disponible aproximado de 1.000.000 a 1.500.000 COP. Además, factores macroeconómicos como inflación, variaciones en el tipo de cambio o limitaciones de subsidios y apoyos gubernamentales pueden retrasar la implementación o escalamiento del proyecto.

Para mitigar esta restricción, se plantea la utilización de herramientas y servicios de código abierto (open source), la adopción de plataformas en la nube con planes gratuitos o de bajo costo educativo, y la priorización de fases de desarrollo por módulos para distribuir los gastos progresivamente. Asimismo, se buscará la gestión de alianzas con instituciones académicas o programas de apoyo a la innovación que faciliten el acceso a infraestructura tecnológica sin costo adicional.

Legales y Normativas

El proyecto está directamente condicionado por leyes de protección de datos personales y privacidad digital, especialmente tratándose de menores de edad. En Colombia aplican principalmente dos normas:

Ley 1581 de 2012, que regula la protección de datos personales, estableciendo los derechos de los titulares y las obligaciones de quienes recopilan, almacenan o procesan información.

Ley 1266 de 2008, que regula el habeas data financiero y crediticio, así como el manejo responsable de la información contenida en bases de datos con fines comerciales o administrativos.

Adicionalmente, deben considerarse regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa y la Children's Online Privacy Protection Act (COPPA) en Estados Unidos, que establecen directrices específicas sobre la recopilación y tratamiento de información de menores de edad.

También deben atenderse las políticas de las tiendas de aplicaciones (Google Play y App Store), que restringen el tipo de permisos y funcionalidades que puede tener una aplicación de control parental.

Para mitigar esta restricción, el proyecto implementará mecanismos de anonimización y encriptación de datos, formularios de consentimiento informado para padres o tutores, y políticas claras de uso y almacenamiento de información. Además, se realizará una revisión jurídica del cumplimiento normativo antes del despliegue en las tiendas de aplicaciones, garantizando que el producto cumpla con los estándares nacionales e internacionales de protección de datos.

Salud y Seguridad

El uso de la aplicación no debe comprometer la seguridad digital de los menores. Ciberataques o fallas en la protección de datos podrían poner en riesgo la información personal. También es necesario considerar los posibles efectos psicológicos derivados de la percepción de vigilancia excesiva, lo que obliga a diseñar mecanismos de supervisión equilibrados que no generen ansiedad ni dependencia.

Para integrar estos mecanismos de manera más específica, la aplicación puede incorporar estrategias técnicas y pedagógicas orientadas al bienestar digital, tales como:

- Niveles de supervisión progresivos, ajustados según la edad y grado de madurez del menor, que permitan flexibilizar el control a medida que se demuestre responsabilidad en el uso de la tecnología.

- Paneles de transparencia, donde tanto padres como hijos puedan visualizar las actividades monitoreadas y comprender el propósito del seguimiento, promoviendo la confianza mutua.
- Alertas inteligentes basadas en inteligencia artificial, diseñadas para detectar patrones de riesgo como exposición a contenido inapropiado, ciberacoso o contacto con desconocidos, priorizando siempre la privacidad y evitando notificaciones excesivas.
- Opciones de configuración compartida, que posibiliten la participación del menor en la definición de límites de uso y reglas de supervisión, fortaleciendo su autonomía y sentido de corresponsabilidad.
- Notificaciones educativas y preventivas, enfocadas en promover hábitos digitales saludables y la reflexión sobre el uso responsable, en lugar de recurrir a medidas punitivas.
- Controles de tiempo saludables, con recordatorios automáticos para fomentar pausas digitales, descanso visual y desconexión voluntaria.
- Protocolos de seguridad y privacidad por diseño, que incluyan cifrado de extremo a extremo, autenticación reforzada y almacenamiento local de datos, reduciendo los riesgos de filtración o acceso no autorizado.

Estas acciones contribuyen a equilibrar la protección y la autonomía, garantizando un entorno digital seguro, confiable y emocionalmente saludable para los menores.

Socioculturales

La aceptación social es un factor clave para la adopción de la solución. Los padres pueden ver la aplicación como una herramienta útil de protección, mientras que algunos menores

podrían percibirla como invasiva. Los contextos culturales también influyen en el nivel de autonomía que se concede a los niños en el uso de la tecnología, lo que puede generar resistencia en ciertas comunidades o familias.

Para mitigar esta restricción, se propone implementar campañas de sensibilización y educación digital dirigidas tanto a padres como a menores, que destaquen los beneficios de la aplicación en términos de seguridad y bienestar. Asimismo, se promoverá la personalización de las funciones de control, permitiendo adaptar el nivel de supervisión según las preferencias culturales y familiares.

Políticas Gubernamentales

El proyecto depende de las políticas públicas vigentes en Colombia relacionadas con la ciberseguridad, la protección de datos personales y la protección digital de menores. La existencia de estrategias nacionales como la Política de Gobierno Digital y los lineamientos de ciberseguridad impulsados por el Estado favorecen la adopción de soluciones tecnológicas orientadas a la prevención de riesgos en entornos digitales. Asimismo, la priorización de la protección de niños, niñas y adolescentes en la agenda gubernamental, junto con la estabilidad institucional del país, facilita la implementación del sistema, al proporcionar un marco normativo y estratégico que respalda su usabilidad y sostenibilidad.

Para mitigar esta restricción, se propone establecer alianzas con instituciones académicas, organizaciones no gubernamentales y entidades del sector privado que promuevan la educación digital segura, con el fin de asegurar la continuidad del proyecto incluso ante cambios en las políticas públicas. Además, se recomienda adaptar el diseño del sistema a marcos normativos internacionales de protección de datos y seguridad infantil, lo que facilitaría su adopción en diferentes contextos políticos.

Limitaciones del Equipo de Trabajo

Disponibilidad de Capital

- **Limitaciones:**
  - ✓ No se dispone de un presupuesto amplio para la adquisición de equipos de alta gama ni para la compra de licencias de software de pago; en consecuencia, el financiamiento limitado obliga a priorizar el uso de herramientas gratuitas o de código abierto que permitan avanzar en el desarrollo del proyecto sin incurrir en altos costos, esto favorece la implementación futura del proyecto.

Tecnología

- **Limitaciones:**
  - ✓ El acceso para la realización de pruebas se encuentra restringido a los dispositivos personales de los integrantes del proyecto, lo que reduce la variedad de entornos de validación. Asimismo, existe una dependencia de servicios en la nube gratuitos, como Firebase en su versión free o GitHub, que presentan limitaciones en almacenamiento, número de consultas y envío de notificaciones. Finalmente, la ausencia de equipos iOS limita el desarrollo inicial exclusivamente al sistema operativo Android.
- **Impacto:**
  - ✓ El sistema podría no abarcar la totalidad de dispositivos y versiones de Android disponibles en el mercado, lo que restringe su alcance en términos de compatibilidad. Del mismo modo, se presenta una limitación para realizar pruebas de escalabilidad y rendimiento en escenarios de alta

demanda, lo que impide garantizar de manera anticipada su óptimo funcionamiento en condiciones de uso intensivo.

- ✓ Para mitigar este impacto, se propone ampliar gradualmente las pruebas de compatibilidad mediante el uso de emuladores y entornos virtuales que permitan evaluar el comportamiento del sistema en distintas versiones de Android. Asimismo, se implementará el uso de plataformas de prueba en la nube, como Firebase Test Lab, con el fin de reproducir condiciones de carga y rendimiento más exigentes. De igual forma, se realizará una optimización del código y de los procesos internos del sistema para mejorar su eficiencia y estabilidad en escenarios de alta demanda. Finalmente, se establecerá un plan de mantenimiento y actualización continua que garantice la adaptación del aplicativo a nuevas versiones del sistema operativo y a la incorporación de futuras mejoras tecnológicas, asegurando así su correcto manejo y funcionamiento a largo plazo en diversos entornos de uso.

Mano de obra

- **Limitaciones:**
  - ✓ El equipo está conformado por estudiantes en formación que cuentan con experiencia básica en desarrollo Android y en el uso de librerías de reconocimiento de texto (OCR); sin embargo, se requiere capacitación adicional en áreas clave como seguridad de datos, integración con Firebase y optimización del rendimiento. Asimismo, la ausencia de un

equipo especializado en diseño UI/UX puede afectar la experiencia de usuario en las primeras versiones de la aplicación.

- **Impacto:**
  - ✓ La curva de aprendizaje del equipo puede prolongar el cronograma de desarrollo, lo que representa un reto en el cumplimiento de los tiempos establecidos. Además, las primeras versiones del prototipo podrían presentar limitaciones en términos de usabilidad y requerir mejoras posteriores para alcanzar un nivel óptimo de funcionamiento y experiencia de usuario.
  - ✓ Para mitigar este impacto, se implementarán estrategias de fortalecimiento de capacidades técnicas del equipo mediante capacitaciones, tutorías y autoformación en las áreas de desarrollo Android avanzado, integración con servicios en la nube y diseño de interfaces. Se promoverá además un trabajo colaborativo con asesorías de expertos externos en UI/UX, a fin de mejorar la calidad visual y funcional del aplicativo.
    Adicionalmente, se planificarán fases de desarrollo iterativas que permitan realizar ajustes continuos conforme se adquieran nuevas habilidades, asegurando que el aprendizaje del equipo contribuya progresivamente a la mejora del producto y al cumplimiento de los plazos establecidos.

De todas las soluciones posibles, se deben priorizar aquellas que no estén condicionadas por restricciones legales, económicas o técnicas imposibles de superar. En este proyecto, la propuesta tecnológica debe garantizar el cumplimiento de las normas de protección de datos de menores, el uso de modelos de IA optimizados y ligeros que no comprometan la capacidad del

dispositivo móvil, un diseño con enfoque ético y sociocultural que evite percepciones negativas de vigilancia invasiva, y la implementación con tecnologías accesibles y de código abierto que reduzcan los costos de infraestructura. El éxito del proyecto dependerá de minimizar estas restricciones mediante estrategias como el uso de tecnologías de código abierto, modelos de IA ligeros para ejecución en dispositivos móviles, cumplimiento estricto de la normativa de protección de datos, pruebas con información anonimizada y un diseño pedagógico que promueva la aceptación social.

El éxito del proyecto dependerá de minimizar estas restricciones mediante estrategias específicas como:

- **Cumplimiento de la normativa de protección de datos:** Implementar protocolos de anonimización y cifrado de la información recopilada, garantizando que los datos sensibles de los menores no sean almacenados ni compartidos sin consentimiento.
- **Uso de tecnologías de código abierto:** Basar el desarrollo en frameworks y librerías libres como TensorFlow Lite, OpenCV o ML Kit, lo cual facilita la transparencia del código, la reducción de costos de licenciamiento y la adaptabilidad a distintos entornos.
- **Modelos de IA ligeros para ejecución móvil:** Entrenar e integrar modelos optimizados que reduzcan el consumo de recursos del dispositivo, priorizando la eficiencia energética y el rendimiento fluido en equipos de gama media o baja.
- **Diseño ético y sociocultural:** Adoptar un enfoque de diseño centrado en el usuario, que comunique de manera clara la finalidad preventiva de la aplicación y evite interpretaciones relacionadas con vigilancia o control excesivo.

- **Pruebas con información anonimizada:** Realizar simulaciones con datos ficticios o enmascarados para validar la eficacia del sistema sin comprometer la privacidad de los participantes.
- **Diseño pedagógico y social:** Incorporar materiales informativos y funciones educativas dentro del aplicativo que promuevan la comprensión y aceptación de la herramienta por parte de padres, docentes y menores.

Estas estrategias permitirán que la propuesta mantenga su viabilidad técnica, ética y social, garantizando un desarrollo responsable, seguro y sostenible del sistema de control parental.

Metodología Para la Selección y Desarrollo de la Solución

Enfoque, Alcance y Diseño de la Investigación

La investigación adoptó un enfoque mixto, combinando lo cuantitativo y lo cualitativo para obtener una visión integral del problema. Se centró en analizar los principales riesgos digitales que enfrentan los menores en el uso de dispositivos móviles, diseñar una aplicación móvil inteligente de control parental apoyada en inteligencia artificial y verificar que la funcionalidad del prototipo permitiera la detección temprana de riesgos y el envío de alertas en tiempo real a los acudientes. El alcance de la investigación fue de tipo exploratorio-descriptivo y aplicado, ya que buscó caracterizar la problemática existente y, a partir de ello, generar una solución tecnológica práctica y viable.

Fases

Fase 1. Análisis de los Riesgos Digitales y las Limitaciones de los Controles Parentales Existentes

En una primera etapa se aplicó una encuesta estructurada dirigida a padres de familia de estudiantes de tercero y cuarto grado de primaria de un colegio distrital de Bogotá, con el propósito de recopilar información relevante sobre los hábitos de uso de dispositivos móviles por parte de los menores y las prácticas de control parental implementadas en el entorno familiar.

La elección de los estudiantes de tercero y cuarto grado se fundamenta en que, durante esta etapa escolar, los niños atraviesan un período clave de desarrollo cognitivo y socioemocional, comienzan a adquirir mayor autonomía en el uso de dispositivos digitales y acceden con mayor frecuencia a contenidos en línea. Sin embargo, aún no cuentan con los criterios necesarios para identificar riesgos digitales ni para tomar decisiones responsables en

entornos virtuales, lo que hace indispensable el acompañamiento y la orientación parental (UNICEF, 2025).

El diseño del instrumento adoptó un enfoque mixto, combinando el método cuantitativo conformada por preguntas cerradas de opción múltiple y dicotómicas, junto con una pregunta abierta orientada a explorar percepciones cualitativas sobre los riesgos digitales percibidos. Esto permitió obtener una visión integral de las percepciones de los padres, tanto en términos numéricos como interpretativos.

Asimismo, la encuesta fue sometida a un proceso de validación de contenido mediante el Formato de Validación V de Aiken, con la participación de un docente de la facultad, tal como se presenta en el **Anexo 1**. Este procedimiento permitió evaluar la pertinencia, claridad y coherencia de cada ítem del instrumento, garantizando su validez y confiabilidad antes de su aplicación definitiva.

El proceso de recolección de datos se realizó mediante un muestreo no probabilístico, dirigido específicamente a los padres que aceptaron participar de forma voluntaria en el estudio. Los datos recolectados fueron analizados para identificar patrones de riesgo comunes y brechas en las estrategias de mediación parental, sirviendo como base para orientar el desarrollo funcional y pedagógico del aplicativo de control parental propuesto.

Fase 2. Desarrollo del modelo Funcional

En esta segunda fase se llevó a cabo el diseño y construcción del modelo funcional del prototipo, el cual define la estructura técnica, la arquitectura del sistema y la interacción entre los módulos que componen la aplicación móvil inteligente de control parental. Este modelo se desarrolló bajo el enfoque de prototipado incremental, permitiendo validar progresivamente las funciones esenciales de monitoreo, detección de riesgos y envío de notificaciones.

El diseño conceptual del sistema se fundamentó en tres pilares principales:

1. **Monitoreo activo y continuo del dispositivo del menor**, mediante la lectura automatizada de notificaciones y la extracción de texto a través de servicios de accesibilidad.
2. **Análisis inteligente del contenido**, apoyado en técnicas de inteligencia artificial basadas en el procesamiento de lenguaje natural (PLN) para identificar palabras clave o patrones asociados a violencia, acoso, contenido sexual o uso de drogas.
3. **Comunicación en tiempo real entre los dispositivos**, garantizando que los padres reciban alertas inmediatas y reportes consolidados sobre los posibles riesgos detectados.

Arquitectura del Sistema

El sistema se estructuró en dos aplicaciones Android interconectadas y un módulo común de configuración compartida:

- **App Child (Dispositivo del menor):** encargada de capturar y procesar las notificaciones entrantes y el texto visualizado en pantalla mediante servicios de accesibilidad y reconocimiento óptico de caracteres (OCR selectivo). Esta información es evaluada por un modelo de IA local, que clasifica el nivel de riesgo y envía un reporte a la nube.
- **App Parent (Dispositivo del padre o acudiente):** recibe los reportes y alertas generadas por el dispositivo del menor a través de notificaciones *push*, mostrando un resumen de la actividad, la categoría de riesgo y el nivel de severidad.
- **Módulo común:** contiene las dependencias, librerías y configuraciones compartidas por ambas aplicaciones, optimizando la compilación y el mantenimiento del sistema.

Tecnologías Implementadas

Para el desarrollo del prototipo se utilizaron herramientas y tecnologías modernas del ecosistema Android, garantizando eficiencia, compatibilidad y seguridad:

- **Lenguaje de programación:** *Kotlin*, por su sintaxis clara, compatibilidad nativa y eficiencia en el manejo de procesos asíncronos.
- **Entorno de desarrollo:** Android Studio, utilizado para el diseño, compilación y depuración del proyecto.
- **Arquitectura:** *Jetpack* (Room, WorkManager, Lifecycle, Navigation), que permite una estructura modular, segura y escalable. Esta Arquitectura se seleccionó teniendo en cuenta que ofrece una base moderna, sólida y de fácil mantenimiento para desarrollo de aplicaciones en Android. Adicionalmente, sus componentes trabajan en conjunto, lo cual garantiza la integración entre la interfaz de usuario, la lógica de la aplicación y el manejo de los datos.
- **Servicios en la nube:** Firebase (FCM, Firebase, Realtime Database) para la mensajería en tiempo real, almacenamiento sincronizado y control de usuarios. Por otro lado, es la mejor opción para servicios en la nube ya que Firebase posee integración nativa con Android, lo que facilita su implementación y ofrece amplia cobertura de funcionalidades en el caso de la aplicación de control parental.
  El FCM (Firebase Cloud Messaging), permite la mensajería en tiempo real, ya que se necesitan notificaciones instantáneas entre los dispositivos del menor y el tutor.

- **Base de datos:** Firebase Realtime Database, la cual permitió sincronizar la información entre los dispositivos de tutores y menores, manteniendo una actualización constante de los registros de actividad y alertas generadas.
- **Gestión de dependencias:** Gradle, encargado de la compilación y actualización automática de librerías.

Diseño de la Interfaz y Experiencia de Usuario (UI/UX)

La interfaz fue diseñada bajo principios de simplicidad, accesibilidad y usabilidad, priorizando una navegación clara y una experiencia intuitiva tanto para el padre como para el menor. La aplicación del acudiente cuenta con un panel de control central, donde se visualizan las notificaciones recientes, el historial de riesgos detectados y las configuraciones de vinculación.

En el caso de la aplicación del menor, la interfaz es mínima y opera principalmente en segundo plano, reduciendo la interacción directa para evitar alteraciones en el monitoreo. El objetivo principal fue garantizar la discreción y eficiencia, sin afectar el rendimiento ni la batería del dispositivo.

Integración y Sincronización de Datos

La vinculación entre ambas aplicaciones se realizó mediante un *código único de familia* (Family ID), generado durante el registro inicial. Este identificador permitió establecer un canal de comunicación seguro y cifrado entre los dos dispositivos, asegurando la correspondencia de alertas, usuarios y datos monitoreados.

Las pruebas iniciales de sincronización confirmaron la correcta transmisión de alertas en tiempo real y la estabilidad del flujo de datos en la nube, sin pérdida de información ni retrasos

perceptibles. Además, se implementó un mecanismo de encriptación de extremo a extremo, garantizando la confidencialidad de los mensajes y reportes generados.

Fase 3. Pruebas y Verificación del Funcionamiento de Prototipo

En la última etapa, el equipo construyó un prototipo inicial de la aplicación con las funcionalidades básicas de detección y notificación. Dicho prototipo fue sometido a pruebas de usabilidad en un entorno controlado, lo que permitió evaluar su facilidad de uso, la pertinencia de las alertas generadas y la percepción de confianza y seguridad que transmitía. Para ello, se llevó a cabo un ensayo controlado con tres acudientes y sus tres menores, empleando seis dispositivos móviles Android (tres con la App Parent y tres con la App Child). Las pruebas se ejecutaron una única vez, siguiendo un procedimiento estructurado que incluyó la instalación de las aplicaciones, la vinculación padre–hijo mediante el código de 6 dígitos y la ejecución de escenarios de uso en los que los menores interactuaban con sus dispositivos mientras los acudientes verificaban la recepción de alertas en tiempo real. Este proceso permitió obtener evidencia directa sobre el funcionamiento del prototipo en condiciones reales y en un grupo pequeño pero representativo del usuario final.

Finalmente, los resultados obtenidos en cada etapa fueron analizados bajo criterios de validez técnica, pertinencia social, viabilidad económica y cumplimiento normativo, lo cual permitió seleccionar y refinar la solución más adecuada. De esta forma, la metodología asegura que cada objetivo fue alcanzado mediante actividades concretas y medibles, garantizando un proceso sistemático y alineado con la pregunta de investigación.

Desarrollo de la Solución

Análisis de los Riesgos Digitales y las Limitaciones de los Controles Parentales Existentes

En esta primera etapa del proyecto se llevó a cabo la aplicación de una encuesta estructurada dirigida a los padres de familia, específicamente de los grados segundo y tercero de básica primaria. El objetivo principal de este instrumento fue recopilar información relevante sobre los hábitos de uso de dispositivos móviles por parte de los menores, las prácticas de supervisión implementadas en el hogar y el nivel de conocimiento de los padres acerca de los riesgos digitales más comunes.

La muestra se seleccionó de forma intencionada, considerando a padres de los grados tercero y cuarto de un Colegio Distrital con hijos que utilizaban dispositivos móviles o tabletas de manera frecuente para actividades recreativas o académicas.

En esta fase se diseñó y aplicó un instrumento de recolección de información, el cual fue sometido previamente a un proceso de validación de contenido mediante el Formato V de Aiken. Este proceso permitió evaluar la pertinencia, claridad y coherencia de cada ítem, garantizando la validez y confiabilidad del instrumento.

Una vez aprobada la validación, se procedió con la implementación virtual de la encuesta, asegurando que los participantes comprendieran el propósito del estudio, garantizando la confidencialidad de la información suministrada. El proceso de recolección de datos se realizó mediante un muestreo no probabilístico, conformado por los padres que participaron de manera voluntaria.

Los datos obtenidos fueron tabulados y analizados utilizando Microsoft Excel, lo que permitió identificar patrones de riesgo comunes, niveles de conocimiento de los padres, hábitos de uso de los dispositivos y limitaciones en las estrategias de mediación parental.

A partir de la encuesta aplicada a los padres de familia se identificaron los hábitos, percepciones y prácticas asociadas al uso de dispositivos móviles por parte de los menores, así como la percepción de la efectividad de las estrategias de supervisión implementadas en el entorno familiar. Los datos recolectados ofrecen una visión integral sobre el grado de conocimiento de los padres frente a los riesgos digitales más comunes y las medidas de control parental que emplean, constituyéndose en una base fundamental para orientar el diseño del prototipo de la aplicación móvil de control parental propuesta en este proyecto. En la figura 1 se presentan los resultados de la frecuencia de usos de los dispositivos móviles por parte de los hijos de los entrevistados.

Figura 1

Pregunta número uno

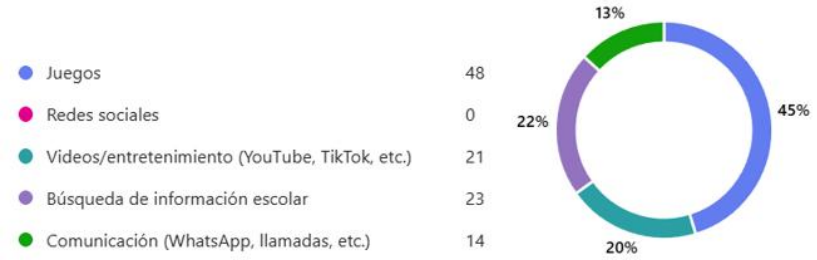
Nota: El gráfico representa la pregunta de con qué frecuencia su hijo(a) utiliza dispositivos móviles (celular / Tablet), Elaboración propia de los autores, 2025.

Los resultados obtenidos en la figura 1 muestran que la mayoría de los padres encuestados (52%) indicó que sus hijos utilizan dispositivos móviles de manera ocasional, es decir, entre una y dos veces por semana. Un 36% manifestó que el uso es frecuente, lo que implica que los menores interactúan con estos dispositivos todos los días, aunque por un tiempo inferior a dos horas. Por su parte, un 11% de los padres reportó un uso muy frecuente, correspondiente a un tiempo de exposición diario entre dos y cinco horas.

En la figura 2 se presentan los resultados de las actividades realizadas por los hijos en los dispositivos móviles.

Figura 2

Pregunta número dos



Nota: El gráfico representa la pregunta de qué actividades realiza principalmente su hijo(a) en los dispositivos móviles, Elaboración propia de los autores, 2025.

Los resultados obtenidos en la figura 2, evidenciaron que la actividad predominante entre los menores fue el uso de juegos, reportada por el 45% de los padres encuestados. En segundo lugar, se encontró la búsqueda de información escolar con un 22%, seguida del consumo de videos o contenido de entretenimiento (como YouTube o TikTok) con un 20%. Finalmente, un 13% indicó que los niños utilizaban los dispositivos principalmente para comunicarse mediante aplicaciones como WhatsApp o llamadas telefónicas.

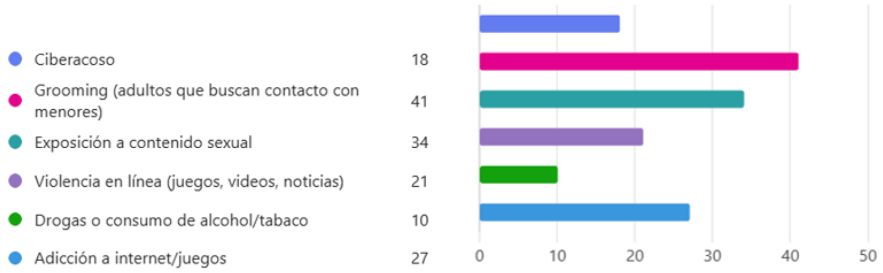
Cabe resaltar que ningún padre manifestó que sus hijos emplearan los dispositivos para el uso de redes sociales, lo cual sugiere una limitación o supervisión activa en cuanto al acceso a plataformas que implican mayor exposición pública o interacción con desconocidos.

Estos resultados reflejaron que el uso de los dispositivos móviles por parte de los menores se concentró en actividades recreativas y educativas, lo que denota un equilibrio entre el entretenimiento y el apoyo académico. Sin embargo, el alto porcentaje de uso para juegos plantea la necesidad de orientar a los padres sobre la importancia de regular el tiempo de ocio digital y promover un uso más formativo y seguro de la tecnología.

En la figura 3 se presentan los resultados de la percepción de los riesgos digitales que los padres consideran más preocupantes.

Figura 3

Pregunta número tres



Nota: El gráfico representa la pregunta de cuales riesgos digitales considera más preocupantes para su hijo(a), Elaboración propia de los autores, 2025.

De acuerdo con los resultados obtenidos en la figura 3, el riesgo digital más preocupante para los padres fue el *grooming* (entendido como el contacto de adultos con menores a través de medios digitales), señalado por el 67% de los encuestados (41 respuestas). En segundo lugar, se destacó la exposición a contenido sexual con un 56% (34 respuestas), seguida de la adicción a internet o juegos con un 44% (27 respuestas).

Otros riesgos mencionados con menor frecuencia fueron la violencia en línea (21 respuestas, 34%), el ciberacoso (18 respuestas, 30%) y el consumo de alcohol o drogas promovido en medios digitales (10 respuestas, 16%).

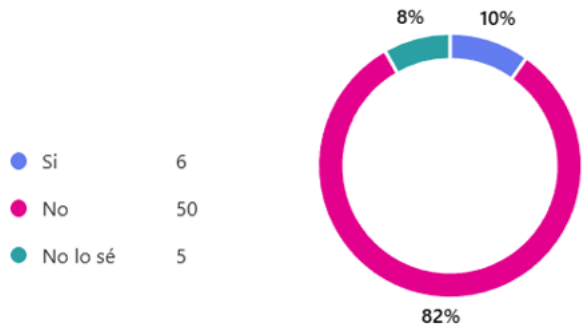
Estos resultados evidenciaron que los padres mostraron una alta preocupación por los riesgos asociados a la interacción directa con desconocidos y la exposición a contenidos inapropiados, lo cual refleja una conciencia creciente sobre los peligros más comunes en el entorno digital infantil. No obstante, la menor percepción del ciberacoso y la violencia en línea

sugiere la necesidad de fortalecer la información y orientación parental respecto a la diversidad de amenazas que pueden afectar el bienestar emocional y psicológico de los menores.

En la figura 4 se presentan los resultados de la percepción de la exposición de los hijos a los riesgos identificados previamente.

Figura 4

Pregunta número cuatro



Nota: El gráfico representa la pregunta de si alguna vez su hijo(a) ha estado expuesto a alguno de estos riesgos, Elaboración propia de los autores, 2025.

Los resultados obtenidos en la figura 4, mostraron que la mayoría de los padres manifestó que sus hijos no habían estado expuestos a riesgos digitales (82%, equivalente a 50 respuestas). Solo un 10% (6 padres) indicó que sí se había presentado algún tipo de exposición, mientras que un 8% (5 padres) afirmó no tener certeza al respecto.

Estos datos evidenciaron que, aunque la percepción general de exposición fue baja, existe un porcentaje significativo de padres que desconoce completamente si sus hijos han enfrentado algún riesgo digital, lo cual puede asociarse a una falta de supervisión o de comunicación abierta sobre las actividades en línea. En consecuencia, se resalta la importancia de fortalecer las estrategias de acompañamiento digital en el hogar y de implementar herramientas tecnológicas que permitan detectar comportamientos o contenidos potencialmente peligrosos de manera temprana.

En la figura 5 se presentan los resultados del uso de métodos de control parental por parte de los padres.

Figura 5

Pregunta número cinco

Nota: El gráfico representa la pregunta de que utiliza actualmente alguna aplicación o método de control parental, Elaboración propia de los autores, 2025.

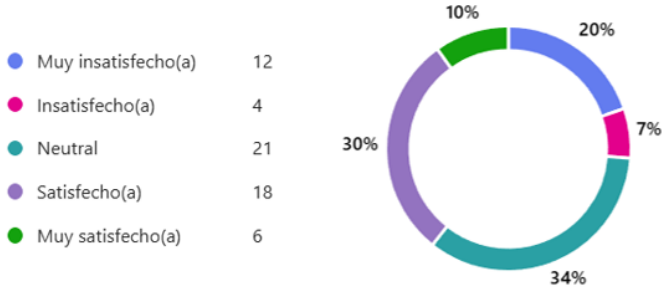
Los resultados obtenidos en la figura 5, indicaron que el 34% de los padres manifestó realizar una supervisión manual sin el uso de aplicaciones (21 participantes), mientras que un 30% afirmó utilizar aplicaciones móviles especializadas como Family Link, Qustodio o Bark (18 participantes). Por otro lado, un 18% señaló emplear los controles integrados en el dispositivo, y un porcentaje igual (18%) reconoció no utilizar ningún tipo de método de control parental.

Estos hallazgos evidenciaron que, si bien una parte importante de los padres implementó algún tipo de control o supervisión, la mayoría optó por estrategias manuales o básicas, lo que sugiere limitaciones en el conocimiento o acceso a herramientas tecnológicas más avanzadas. Además, el hecho de que casi una quinta parte de los padres no empleara ningún método de control reflejó una oportunidad significativa para promover el uso de soluciones digitales más efectivas y automatizadas, que fortalezcan la protección de los menores en entornos virtuales.

En la figura 6 se presentan los resultados de satisfacción respecto a los métodos de control parental empleados actualmente.

Figura 6

Pregunta número seis



Nota: El gráfico representa la pregunta de qué tan satisfecho(a) está con el método que utiliza actualmente, Elaboración propia de los autores, 2025.

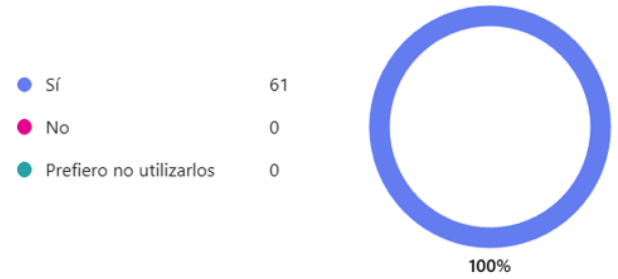
Los resultados obtenidos en la figura 6, mostraron que el 34% de los padres manifestó neutralidad frente al nivel de satisfacción con el método de control parental que utilizaba (21 participantes). Un 30% indicó estar satisfecho, mientras que un 10% se declaró muy satisfecho. Por otro lado, un 20% expresó estar muy insatisfecho y un 7% se mostró insatisfecho.

Estos datos reflejaron que, aunque la mayoría de los padres mantuvo una percepción positiva o neutral, una proporción considerable presentó inconformidad o dudas respecto a la efectividad de los métodos empleados. Esta tendencia sugiere que muchos padres no se sentían completamente respaldados por las herramientas actuales y evidenciaron la necesidad de soluciones más intuitivas, confiables y adaptadas a las dinámicas familiares modernas, lo cual respalda la pertinencia del desarrollo del aplicativo de control parental propuesto en este proyecto.

En la figura 7 se presentan los resultados del interés mostrado por una aplicación de detección de riesgos digitales para los menores.

Figura 7

Pregunta número siete



Nota: El gráfico representa la pregunta de qué le interesaría una aplicación que detecte en tiempo real riesgos en el dispositivo de su hijo(a) y le envíe alertas inmediatas, Elaboración propia de los autores, 2025.

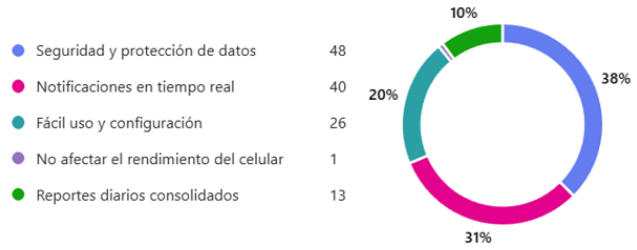
Los resultados obtenidos en la figura 7, mostraron una aceptación unánime por parte de los padres frente a la propuesta de una aplicación capaz de detectar en tiempo real riesgos digitales en los dispositivos de sus hijos y enviar alertas inmediatas, ya que el 100% de los encuestados (61 participantes) respondió afirmativamente.

Este resultado evidenció un alto nivel de interés y necesidad por parte de las familias hacia herramientas tecnológicas que fortalezcan la protección y el acompañamiento digital de los menores. Asimismo, reafirmó la pertinencia y relevancia del desarrollo del prototipo de aplicación de control parental propuesto en el proyecto, al demostrar que los padres reconocieron el valor de soluciones innovadoras que combinen monitoreo activo, alertas preventivas y orientación educativa en la gestión de riesgos digitales.

En la figura 8 se presentan los resultados de la consideraciones importantes para una aplicación de control parental.

Figura 8

Pregunta número ocho



Nota: El grafico representa la pregunta de qué aspectos consideras más importantes en una aplicación de control parental, Elaboración propia de los autores, 2025.

Los resultados obtenidos en la figura 8, evidenciaron que los padres priorizaron principalmente la seguridad y protección de los datos (38%) como el aspecto más relevante al momento de elegir una aplicación de control parental, seguido de las notificaciones en tiempo real (31%) y el fácil uso y configuración (20%). En menor medida, un 10% valoró la generación de reportes diarios consolidados, mientras que solo un 2% consideró importante que la aplicación no afectara el rendimiento del dispositivo móvil.

Estos hallazgos reflejaron que las familias otorgaron una gran importancia a la privacidad y la inmediatez de la información, elementos clave para la confianza y eficacia de una herramienta tecnológica orientada al cuidado digital de los menores. Asimismo, se observó que los padres buscaban soluciones accesibles y prácticas, que no requirieran conocimientos técnicos avanzados, reafirmando la necesidad de un diseño intuitivo y seguro en el desarrollo del prototipo de aplicación propuesto.

En la figura 9 se presentan los resultados de las expectativas y recomendaciones para una aplicación de control parental

Figura 9

Pregunta número nueve

Nota: El gráfico representa la pregunta de qué expectativas, sugerencias o recomendaciones tendría frente a una aplicación de control parental, Elaboración propia de los autores, 2025.

Las respuestas cualitativas obtenidas en la figura 9, reflejaron que los padres tenían altas expectativas respecto a la funcionalidad y efectividad de una aplicación de control parental. Entre las sugerencias más frecuentes se destacó el deseo de contar con alertas inmediatas, la posibilidad de monitorear los movimientos y actividades digitales de los hijos en tiempo real, y la seguridad en el manejo de los datos personales.

Asimismo, los participantes resaltaron la importancia de que la herramienta fuera fácil de usar, transparente en su funcionamiento y confiable en la información que ofrece. Algunas respuestas enfatizaron que la aplicación debía cumplir con lo prometido y no generar falsas alertas o complicaciones técnicas.

En general, el análisis de las percepciones evidenció que los padres buscaban una solución tecnológica eficiente, práctica y segura, que les permitiera proteger a sus hijos sin invadir completamente su privacidad, reforzando así la necesidad de desarrollar un prototipo de aplicación centrado en la confianza, la usabilidad y la detección temprana de riesgos digitales.

Los resultados obtenidos se constituyeron en insumos fundamentales para la definición de los requerimientos funcionales y no funcionales del prototipo de la aplicación móvil de control

parental, orientado a fortalecer la supervisión digital y promover el uso responsable de la tecnología en los menores.

Análisis De Requerimientos

El análisis de requerimientos constituye una etapa fundamental en el desarrollo del sistema, ya que permite definir de manera clara las necesidades funcionales y no funcionales que deberá cumplir la aplicación. En esta fase se establecen los objetivos técnicos y operativos del producto, así como las características que garantizarán su eficacia en la detección temprana de riesgos digitales. El propósito es asegurar que el sistema responda adecuadamente a las expectativas de los padres o tutores y cumpla con los criterios de privacidad, precisión y desempeño necesarios para el control parental inteligente propuesto.

Intención Del Producto: El sistema busca ofrecer a padres/tutores una app móvil de control parental que opere en el dispositivo (Android), capaz de extraer texto desde pantalla/imágenes con reconocimiento óptico de caracteres (OCR selectivo) y analizarlo con procesamientos del lenguaje natural (PLN) para detectar expresiones de riesgo. El sistema genera un reporte diario consolidado y emite alertas inmediatas únicamente ante eventos críticos, minimizando consumo de recursos del dispositivo y preservando la privacidad

Requerimientos Funcionales

Los requerimientos funcionales describen las acciones y procesos esenciales que la aplicación debe realizar para cumplir con su propósito de monitoreo y detección temprana de riesgos digitales. En esta sección se definen las capacidades principales del sistema, como el registro de usuarios, la captura y el análisis del contenido al que el menor se encuentra expuesto y la generación de alertas oportunas. Asimismo, se establecen las funciones necesarias para identificar posibles riesgos relacionados con violencia, acoso, ciberbullying, contenido sexual,

consumo de drogas o interacciones inapropiadas, con el fin de garantizar un acompañamiento efectivo y seguro por parte de los padres o tutores.

1. **Registro y autenticación de usuarios padres/tutores.** Mediante código de vinculación 6 dígitos.
2. **Captura de texto en el dispositivo del menor mediante.**
   - ✓ Servicios de accesibilidad.
   - ✓ Notificaciones entrantes.
   - ✓ OCR selectivo para texto en imágenes/memes.
3. **Análisis semántico y por palabras clave.** El sistema analiza el texto capturado utilizando modelos de inteligencia artificial entrenados para detectar los patrones lingüísticos asociados a posibles situaciones de riesgo. Este proceso se centra en la detección de expresiones relacionadas con violencia, acoso, ciberbullying, contenido sexual, consumo de drogas y solicitudes de contacto inapropiadas, con el fin de alertar al acudiente sobre comportamientos o interacciones que puedan comprometer la seguridad del menor.
4. **Historial de incidentes detectados.** Para seguimiento y acciones correctivas las cuales deben incluir fecha, aplicación, categoría y nivel de riesgo.
5. **Reportes diarios consolidados para los acudientes.** Con métricas de actividad y categorías de riesgo.
6. **Modo de funcionamiento en segundo plano.** Para mantener el monitoreo sin interacción del menor.

Generación de alertas críticas inmediatas mediante notificaciones en tiempo real cuando el sistema de IA detecte un nivel de riesgo alto, permitiendo una intervención oportuna del acudiente. Panel de control para el acudiente, con visualización de reportes y eventos críticos.

Requerimientos No Funcionales

Los requerimientos no funcionales especifican las características de calidad que la aplicación debe cumplir para asegurar un funcionamiento eficiente, seguro y accesible. Estos lineamientos no describen acciones directas del sistema, sino atributos como compatibilidad, desempeño, usabilidad, seguridad y optimización de recursos. Su propósito es garantizar que la aplicación ofrezca una experiencia estable y confiable, se adapte adecuadamente a diferentes dispositivos y proteja la información sensible gestionada durante el proceso de monitoreo.

1. La aplicación debe ser compatible con dispositivos Android versión 8.0 o superior.
2. Debe adaptarse a diferentes resoluciones y tamaños de pantalla (diseño responsivo)
3. La instalación y vinculación deben poder realizarse sin necesidad de rootear el dispositivo.
4. Implementar cifrado de extremo a extremo para la transmisión y almacenamiento de datos.
5. Interfaz simple e intuitiva, pensada para usuarios sin experiencia técnica
6. Optimización de recursos para minimizar el impacto en el rendimiento y batería del dispositivo del menor.

Recursos necesarios para el desarrollo del proyecto

Para llevar a buen término el desarrollo de la aplicación de control parental basada en inteligencia artificial, se requiere la disponibilidad de los siguientes recursos:

Recursos de software

- Android Studio con Kotlin.
- Firebase Cloud Messaging (FCM) o similar para envío de notificaciones en tiempo real.
- OCR: librerías como ML Kit de Google, Tesseract OCR u otra compatible.
- Base de datos en la nube (por ejemplo, Firebase Firestore, Supabase o PostgreSQL en un servidor propio).
- Git/GitHub o GitLab para control de versiones.

Recursos de datos

- Palabras clave y patrones de comportamiento sospechosos (ejemplo: términos de violencia, acoso, drogas, etc.).
- Registros de actividad en el dispositivo del menor (texto escrito, aplicaciones abiertas, páginas visitadas, capturas OCR).
- Información para generar reportes (fecha, hora, aplicación o sitio donde se detectó la actividad).

Recursos financieros

- Presupuesto básico para:
    - Adquisición de dispositivos móviles de prueba.
    - Costos asociados al uso de servicios en la nube para respaldo y pruebas.

Dispositivos de prueba:

- Al menos un dispositivo Android que simule el teléfono del menor.

- Un dispositivo Android (o iOS opcionalmente) que funcione como el teléfono del padre o tutor.
- Computador con Android Studio instalado para el desarrollo.

Desarrollo del modelo Funcional

En esta segunda fase del proyecto se llevó a cabo el desarrollo del modelo funcional de la aplicación móvil inteligente de control parental. Esta etapa tuvo como propósito estructurar los componentes técnicos y la interacción entre los módulos principales del sistema, asegurando que la arquitectura propuesta cumpliera con los requerimientos funcionales definidos en la fase inicial.

El desarrollo del modelo se realizó bajo una metodología progresiva e iterativa, en la que se implementaron versiones parciales del sistema para validar su funcionamiento, evaluar la comunicación entre los dispositivos y garantizar la estabilidad del flujo de datos en tiempo real. El modelo funcional se sustentó en tres pilares fundamentales:

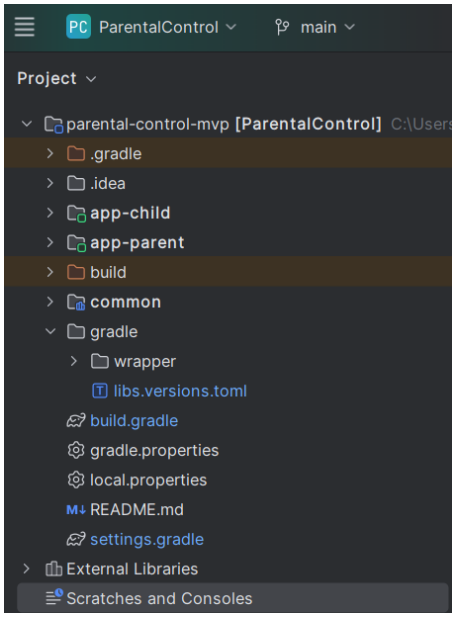
1. **Monitoreo continuo del dispositivo del menor**, permitiendo la captura y análisis del contenido visualizado mediante servicios de accesibilidad.
2. **Análisis inteligente del texto detectado**, empleando técnicas de *procesamiento de lenguaje natural (PLN)* y filtros semánticos que permiten identificar palabras clave asociadas a posibles riesgos digitales como violencia, acoso, contenido sexual o drogas.
3. **Comunicación inmediata entre los dispositivos**, asegurando que los padres o acudientes reciban alertas en tiempo real junto con un resumen de los posibles riesgos detectados.

Modelo lógico y estructura del proyecto

El desarrollo del modelo funcional partió de un árbol de proyecto que representa los módulos, dependencias y flujos de información entre componentes. Este esquema se presenta en la figura10, donde se detallan los módulos principales (captura, preprocesamiento, clasificación, gestión de alertas y reportes). El árbol de proyecto sirvió como guía para distribuir responsabilidades dentro del repositorio y planificar las tareas de desarrollo.

Figura 10

Árbol de Proyecto

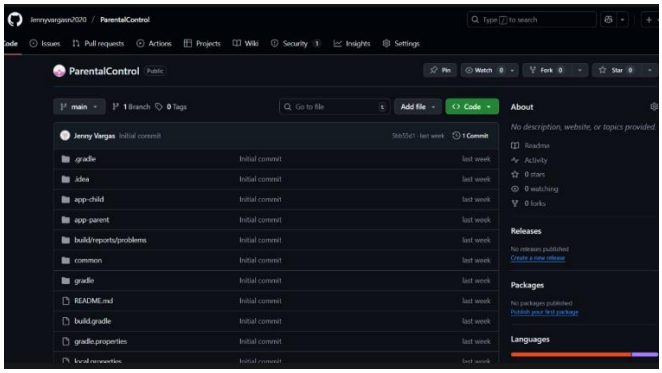


Nota: Elaboración propia de los autores, 2025.

Además, la ubicación del repositorio y la organización del código se definieron desde etapas tempranas para facilitar la integración continua y el control de versiones; la estructura del repositorio y su ubicación se muestran en la figura 11. Esta disposición permitió establecer ramas de trabajo para los módulos (App Child, App Parent y Módulo Común), pruebas automatizadas y registros de versiones.

Figura 11

Ubicación Repositorio proyecto



Nota: Elaboración propia de los autores, 2025.

Arquitectura del Sistema

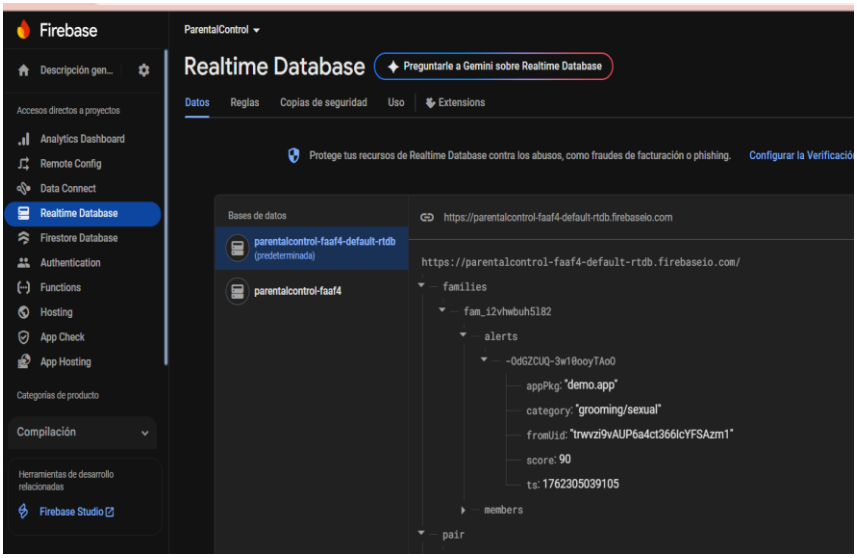
La arquitectura del sistema se diseñó con base en la interoperabilidad de dos aplicaciones Android independientes —**App Child** y **App Parent**— que comparten un módulo común de configuración y servicios.

- **App Child:** se instala en el dispositivo del menor y tiene como función monitorear la actividad del teléfono mediante la lectura de notificaciones y el reconocimiento óptico de caracteres (OCR selectivo). Esta aplicación analiza el texto mediante un modelo de IA local y envía alertas automáticas al servidor en la nube.
- **App Parent:** se instala en el dispositivo del acudiente y permite visualizar los reportes generados por la aplicación del menor. Presenta un panel de control que muestra el historial de notificaciones, la categoría del riesgo identificado y su nivel de severidad.
- **Módulo común:** contiene configuraciones compartidas, dependencias y librerías que permiten la comunicación entre ambos dispositivos, simplificando la gestión de versiones y actualizaciones.

La figura 12 muestra la integración del sistema con la plataforma Firebase, utilizada para el envío de notificaciones en tiempo real, la autenticación de usuarios y el almacenamiento de registros de actividad. Este entorno en la nube permitió una sincronización constante entre los dispositivos y una comunicación bidireccional eficiente entre la App Child y la App Parent.

Figura 12

Firebase Parental Control



Nota: Elaboración propia de los autores, 2025.

Tecnologías Empleadas

Para el desarrollo del prototipo se emplearon tecnologías y herramientas modernas del ecosistema Android. Se utilizó el lenguaje Kotlin debido a su compatibilidad nativa con la plataforma y su seguridad en el manejo de hilos y procesos concurrentes. El entorno de desarrollo Android Studio facilitó las tareas de depuración, compilación y despliegue del código. En cuanto a la arquitectura, se implementaron los Jetpack Components (Room, WorkManager, Lifecycle y Navigation) con el fin de garantizar la modularidad, escalabilidad y mantenimiento del sistema. Además, se integraron servicios en la nube mediante Firebase Cloud Messaging

(FCM) para el envío de notificaciones y Firebase Realtime Database para el registro y sincronización de datos entre dispositivos en tiempo real.

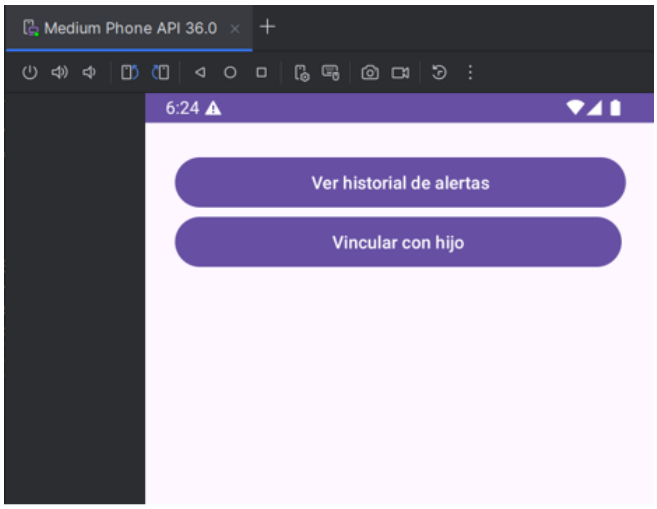
Diseño de Interfaz y Flujo de Navegación

El diseño de la interfaz de usuario se desarrolló priorizando la simplicidad, claridad visual y usabilidad, de manera que los padres pudieran comprender fácilmente la información presentada y los menores no percibieran la aplicación como intrusiva.

La figura 13 presenta la vista principal de la App Parent, donde se visualizan las notificaciones recibidas y el resumen de alertas clasificadas por nivel de riesgo. Esta pantalla integra íconos representativos y elementos visuales que facilitan la lectura rápida y la toma de decisiones.

Figura 13

Visualización pantalla App Parent (inicio)

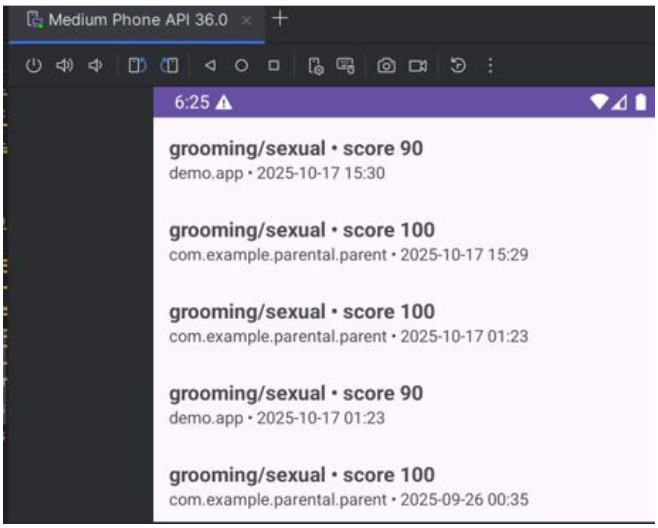


Nota: Elaboración propia de los autores, 2025.

La figura 14 muestra la sección de reportes detallados, en la cual el acudiente puede consultar el historial de eventos y las métricas asociadas (fecha, hora, aplicación de origen y nivel de riesgo), junto con recomendaciones y acciones sugeridas por el sistema.

Figura 14

Visualización pantalla App Parent



Nota: Elaboración propia de los autores, 2025.

Integración y Vinculación entre Dispositivos

La conexión entre la App Parent y la App Child se estableció mediante un identificador único familiar (Family ID) generado durante el registro inicial. Este código permitió vincular los dispositivos de forma segura, posibilitando la recepción inmediata de alertas cada vez que se detectó un riesgo digital en el dispositivo del menor.

El proceso de autenticación y emparejamiento se ejecutó sin necesidad de permisos de *root*, cumpliendo con los estándares de seguridad definidos en Android y respetando los principios de privacidad por diseño. Además, se implementó una capa de cifrado y control de acceso para proteger la información transmitida.

Pruebas de Verificación del Funcionamiento del Prototipo

Las pruebas de funcionamiento y verificación del prototipo se llevaron a cabo mediante un ensayo controlado con tres acudientes y sus tres hijos, utilizando seis dispositivos móviles

Android (tres ejecutando la aplicación App Parent y tres ejecutando la aplicación App Child). Los participantes correspondieron a un grupo cerrado de padres con hijos entre 8 y 14 años, rango de edad seleccionado por su alta exposición e interacción con redes sociales y servicios de internet.

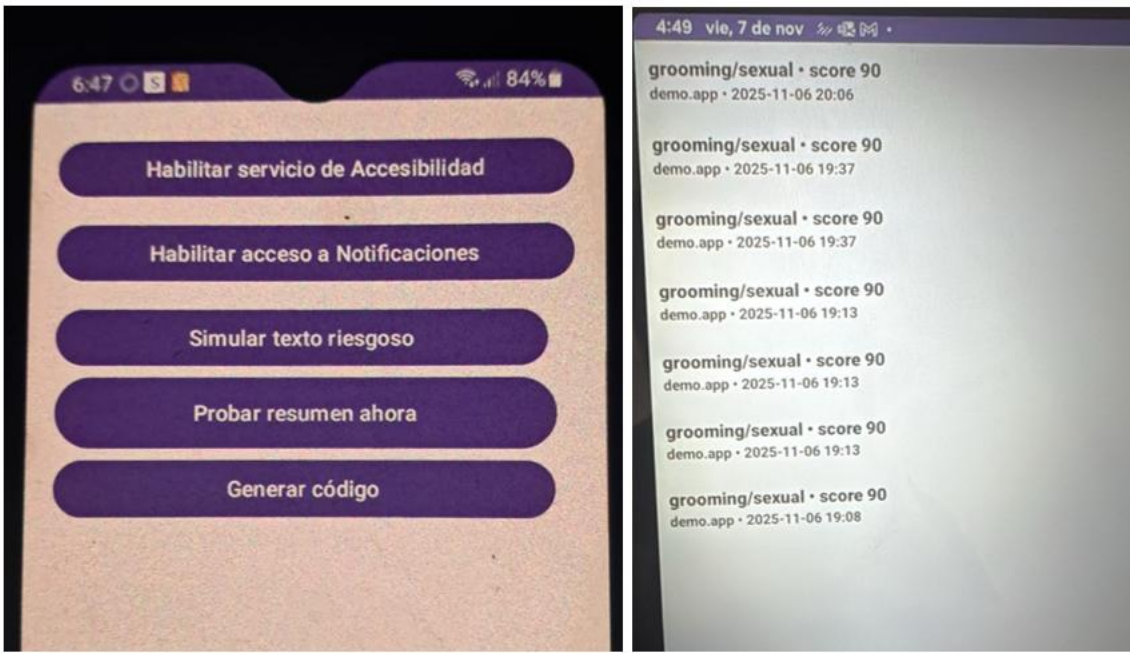
El objetivo del ensayo fue validar los requisitos funcionales y de comunicación definidos para el sistema de control parental, verificando la correcta vinculación de cuentas padre–hijo, la transmisión de eventos de riesgo digital y la generación de notificaciones en tiempo real entre las aplicaciones cliente (App Child) y de monitoreo (App Parent). Para ello se definió un protocolo de pruebas compuesto por las siguientes actividades:

- **Configuración inicial:** Instalación de App Parent y App Child en cada dispositivo, creación de cuentas de acudiente y asociación padre–hijo mediante el código de vinculación de 6 dígitos.
- **Ejecución de escenarios de uso:** Interacción normal de los menores con sus dispositivos mientras el sistema registraba eventos de riesgo digital; de forma paralela, los acudientes monitoreaban en App Parent la recepción de alertas, el resumen de riesgos y el historial de notificaciones.
- **Registro de evidencias:** Recopilación de capturas de pantalla y registros de eventos de la aplicación (logs) para verificar tiempos de respuesta, estabilidad de la conexión y consistencia de los datos sincronizados entre ambas aplicaciones.

Los resultados mostraron que el prototipo cumple el flujo operativo principal: registro y autenticación de usuarios, vinculación padre–hijo, captura de eventos, sincronización de datos y entrega de notificaciones en tiempo casi real entre App Child y App Parent como se muestra en la figura 15. Sin embargo, al tratarse de una prueba preliminar con una muestra reducida y en un

entorno controlado, se plantea como trabajo futuro la ejecución de pruebas formales en un contexto escolar, con un número mayor de participantes y métricas cuantitativas de desempeño y usabilidad que permitan generalizar los resultados.

Figura 15
verificación de funcionalidad



Nota: Elaboración propia de los autores, 2025.

Plan de Implementación

Esta sección presenta los componentes de software desarrollados para el prototipo de la aplicación, especificando su ubicación dentro de la arquitectura (Frontend y Backend) y la función que cumplen dentro del sistema. Los módulos fueron diseñados para garantizar la captura de información en tiempo real, el análisis de riesgos digitales y el envío de alertas al acudiente mediante servicios en la nube.

En la tabla 1 presenta los componentes de software desarrollados para el sistema, organizados según su ubicación en la arquitectura y su funcionalidad principal.

Tabla 1

Componentes de Software

Componente de software	Arquitectura	Funcionalidad
RegisterActivity	Frontend	Registra nuevos usuarios (padres/acudientes) en el sistema con validación básica (Código de vinculación 6 dígitos).
HomeParentActivity	Frontend	Pantalla principal del acudiente: muestra alertas recientes, estadísticas y accesos a reportes.
ChildMonitoringService	Backend (en App Child)	Servicio en segundo plano que lee notificaciones y contenido en pantalla usando accesibilidad.
OCRProcessor	Backend (App Child)	Extrae texto de imágenes y elementos visuales utilizando OCR.
RiskAnalysisModule	Backend (App Child)	Analiza el texto capturado mediante IA; detecta categorías como violencia, acoso, drogas, contenido sexual, grooming.
RiskClassifier	Backend (App Child)	Clasifica el nivel de riesgo (bajo, medio, alto) y desencadena alertas cuando corresponde.
AlertSender	Backend (App Child)	Envía alertas críticas al acudiente por medio de Firebase Cloud Messaging.
ParentAlertsFragment	Frontend	Muestra las alertas recibidas en tiempo real con fecha, categoría y descripción.
FirebaseAuthManager	Backend	Gestiona la autenticación del usuario en Firebase (registro Vinculación).
FirestoreRepository	Backend	Gestiona la lectura y escritura de datos del menor: eventos detectados, configuraciones y reportes.
NotificationManagerParent	Backend	Administra la recepción de notificaciones push en el dispositivo del acudiente.

LocalDatabase (Room)	Backend	Almacena temporalmente eventos y texto capturado para procesarlos antes de enviarlos a la nube.

Nota: Elaboración propia de los autores, 2025.

Pruebas y QA de Software

El proceso de Pruebas y Aseguramiento de la Calidad (QA) se desarrolló con el fin de validar el correcto funcionamiento del prototipo, garantizar la estabilidad del sistema y asegurar que los requerimientos funcionales y no funcionales fueran cumplidos. Este proceso incluyó pruebas en entornos controlados y dispositivos reales, permitiendo identificar comportamientos esperados, inconsistencias y oportunidades de mejora.

Estrategia de Pruebas

Se desarrolló siguiendo un enfoque estructurado que permitió evaluar de forma progresiva la calidad y funcionamiento del prototipo. En primer lugar, se realizaron pruebas unitarias orientadas a validar el correcto comportamiento de las funciones internas desarrolladas en Kotlin, incluyendo los procesos de análisis de contenido, almacenamiento local mediante Room, sincronización con Firebase y ejecución de tareas en segundo plano a través de WorkManager. Posteriormente, se llevaron a cabo las pruebas de integración, en las cuales se verificó que los módulos del sistema interactuaran adecuadamente, garantizando la correcta comunicación entre la captura de contenido, el análisis de riesgos digitales, la generación de alertas y la sincronización con los servicios en la nube. Luego, se ejecutaron las pruebas funcionales para confirmar que todas las características del sistema cumplieran con los requerimientos establecidos, como el inicio de sesión, monitoreo del contenido, detección automática de riesgos y envío de notificaciones al acudiente. Finalmente, se realizó la validación

de datos, verificando la integridad, consistencia y correcta transmisión de la información almacenada localmente y en Firebase.

Despliegue por Etapas

Este se efectuó de manera escalonada para garantizar la estabilidad y confiabilidad del sistema antes de su uso en un entorno real. Primero, el prototipo fue evaluado en un entorno de pruebas (QA), utilizando principalmente el emulador de Android Studio para identificar errores iniciales, validar el flujo de navegación y corregir fallos funcionales. Posteriormente, se pasó a un entorno de *staging*, donde se realizaron pruebas en dispositivos físicos con el fin de simular condiciones reales, validar la conectividad con Firebase, comprobar el envío y recepción de alertas mediante FCM y evaluar el comportamiento del sistema frente a restricciones de batería y permisos del dispositivo. Finalmente, se llevó a cabo la validación en un entorno de producción, donde se comprobó el funcionamiento del sistema en condiciones simuladas, garantizando la sincronización de datos, la estabilidad del monitoreo en segundo plano y la correcta entrega de notificaciones al acudiente.

Análisis de Costos

El presente análisis tiene como propósito identificar y estimar los costos asociados al desarrollo de la aplicación móvil inteligente de control parental para la detección temprana de riesgos digitales en menores, orientada a fortalecer la protección digital de los menores, mediante la supervisión del uso de dispositivos móviles y la detección temprana de comportamientos de riesgo.

Durante esta fase de desarrollo, el proyecto implementó una solución funcional que integra los módulos tutor y menor, con capacidades básicas de monitoreo de texto visible, emisión de alertas locales, gestión de permisos y uso de servicios nativos del sistema Android.

El análisis económico busca determinar los costos del proyecto en su etapa inicial.

Análisis de Resultados

El análisis de costos permite identificar los recursos humanos, técnicos y administrativos necesarios para el desarrollo del proyecto.

A través de esta evaluación se estiman los costos directos e indirectos asociados a la creación del prototipo funcional, con el fin de determinar su viabilidad económica y orientar futuras etapas de implementación y mejora.

En los proyectos de ingeniería de software, los costos se dividen principalmente en tres grupos:

- **Costos Directos:** Gastos directamente relacionados con el desarrollo del producto (mano de obra, herramientas, soporte técnico).

Tabla 2

Costos Directos

Coste de Personal				
Rol	**Cantidad**	**Salario (COP)**	**Duración (horas)**	**Costo Total (COP)**
Desarrollador Backend	1	$ 95.000	48	$ 4.560.000
Desarrollador Frontend (Android)	1	$ 100.000	48	$ 4.800.000
Diseñador UI/UX	1	$ 120.000	24	$ 2.880.000
Tester / QA	1	45000	32	$ 1.440.000
Líder de Proyecto	1	$ 80.000	32	$ 2.560.000
Total Coste de Personal				**$ 16.240.000**

Licencias y Herramientas de Software			
Software / Herramienta	**Costo (COP)**	**Duración**	**Costo Total (COP)**
Android Studio	$ 0	3	$ 0
GitHub	$ 0	3	$ 0
Figma	$ 0	3	$ 0
Firebase (planeado para versión 2)	$ 0	3	$ 0
Total Licencias y Herramientas			$ 0

Resumen de Costos Directos	
Categoría	**Costo Total (COP)**
Costes de Personal	$ 16.240.000
Licencias y Herramientas de Software	$ 0
Total Costos Directos	**$ 16.240.000**

Nota: Elaboración propia de los autores, 2025.

El análisis de costos directos en la tabla 2, evidencia que en este caso la mayor proporción del presupuesto del proyecto se concentra en el recurso humano, con un total estimado de $16.240.000 COP. Este valor corresponde principalmente a los roles técnicos y de gestión necesarios para el desarrollo del prototipo: desarrolladores backend y frontend, diseñador UI/UX, tester y líder de proyecto.

No se contemplan gastos por licencias o herramientas de software, ya que el proyecto hace uso de plataformas gratuitas o con versiones de libre acceso, tales como Android Studio, GitHub, Figma y Firebase (planificado para futuras versiones).

En consecuencia, se puede concluir que el proyecto mantiene una estructura de costos eficiente, centrada en la mano de obra calificada, lo que favorece su viabilidad en la fase inicial de desarrollo. A futuro, se prevé que los costos puedan incrementarse con la integración de servicios pagos, mantenimiento en producción y pruebas a gran escala.

- **Costos Indirectos:** Gastos asociados a la operación general e infraestructura (servicios, licencias, energía, permisos), según se presenta en la tabla 3.

Tabla 3

Costos Indirectos

Costos Administrativos			
Descripción	**Costo (COP)**	**Duración Meses**	**Total (COP)**
Internet	$ 150.000	3	$ 450.000
Energía eléctrica	$ 100.000	3	$ 300.000
Subtotal			**$ 750.000**

Costos de Infraestructura			
Descripción	**Costo Unitario (COP)**	**Duración**	**Total (COP)**
Equipos de desarrollo (PC / Laptop)	$ 0	1	$ 0
Mantenimiento preventivo	$ 300.000	1	$ 300.000
Software de respaldo / almacenamiento en la nube	$ 200.000	1	$ 200.000
Subtotal			**$ 500.000**

Resumen de Costos Indirectos	
Categoría	**Costo Total (COP)**
Costos Administrativos	$ 750.000
Costos de Infraestructura	$ 500.000
Total Costos Indirectos	**$ 1.250.000**

Nota: Elaboración propia de los autores, 2025.

El análisis de costos indirectos en la tabla 3, muestra un valor total estimado de $1.250.000 COP, distribuido entre costos administrativos y costos de infraestructura. Dentro de los costos administrativos, los rubros más representativos corresponden a internet y servicios básicos, energía eléctrica y papelería o consumibles, los cuales son necesarios para el funcionamiento general del equipo de trabajo durante el desarrollo del proyecto.

En cuanto a la infraestructura, se consideraron gastos asociados al mantenimiento preventivo de los equipos y al uso de software de respaldo o almacenamiento en la nube, fundamentales para garantizar la seguridad y continuidad del desarrollo.

Estos valores reflejan un nivel de gasto controlado, acorde con la naturaleza del proyecto y su etapa de prototipo. El uso de recursos tecnológicos ya disponibles y herramientas gratuitas contribuye significativamente a reducir los costos operativos, manteniendo la eficiencia sin comprometer la calidad del producto.

Para complementar el análisis financiero del proyecto, se realizó una estimación consolidada de los costos asociados al desarrollo del prototipo durante la fase del MVP. Este cálculo integra tanto los costos directos como los costos indirectos derivados de las actividades técnicas, operativas y de apoyo necesarias para la construcción y validación de la solución. A continuación, se presenta un resumen general del total de recursos económicos requeridos, con el fin de evidenciar la inversión mínima necesaria para la implementación inicial de la propuesta.

Tabla 4
Resumen General de Costos

Resumen General del Análisis de Costos	
Tipo de Costo	**Valor (COP)**
Costos Directos	$ 16.240.000
Costos Indirectos	$ 1.250.000
Costo Total Estimado del Proyecto (Fase MVP)	**$ 17.490.000**

Nota: Elaboración propia de los autores, 2025.

El análisis general de costos de la tabla 4, refleja un costo total estimado de $17.490.000 COP para la fase MVP (Producto Mínimo Viable) del proyecto.

De este monto, los costos directos representan la mayor proporción con $16.240.000 COP, principalmente asociados al recurso humano involucrado en el desarrollo, diseño y pruebas del sistema. Por su parte, los costos indirectos, equivalentes a $1.250.000 COP, comprenden gastos administrativos y de infraestructura esenciales para garantizar la operatividad del proyecto.

En conjunto, estos resultados muestran una planificación financiera equilibrada y realista, acorde con los requerimientos técnicos y el alcance del prototipo funcional planteado.

Conclusiones

El desarrollo del proyecto permitió evidenciar la necesidad y viabilidad de implementar soluciones tecnológicas basadas en inteligencia artificial para fortalecer la supervisión digital infantil. A partir del análisis realizado, se logró demostrar que una aplicación móvil inteligente puede convertirse en una herramienta efectiva para la detección temprana de riesgos digitales y el acompañamiento parental responsable.

El análisis de los principales riesgos digitales y de las limitaciones de los controles parentales existentes permitió identificar una brecha significativa entre las necesidades de los padres y las herramientas actualmente disponibles. Los resultados de la encuesta aplicada reflejaron una alta preocupación por riesgos como el *grooming*, la exposición a contenido inapropiado y la adicción digital, lo cual reafirma la pertinencia de diseñar una solución con enfoque preventivo y de monitoreo continuo.

La estructuración del modelo funcional posibilitó la definición de una arquitectura modular, escalable y segura, fundamentada en componentes de Jetpack y servicios en la nube de Firebase. El diseño de la interfaz se orientó bajo principios de usabilidad, accesibilidad y eficiencia, garantizando una interacción sencilla para los padres y un funcionamiento discreto en el dispositivo del menor. Esta fase consolidó los fundamentos técnicos necesarios para un sistema confiable de monitoreo y detección de riesgos digitales.

El prototipo desarrollado cumplió con el propósito general del proyecto al demostrar la factibilidad técnica y funcional de una aplicación móvil que, mediante el uso de inteligencia artificial, detecta en tiempo real riesgos digitales en los dispositivos de los menores. Su diseño garantizó la emisión de alertas oportunas sin afectar el rendimiento del dispositivo ni comprometer la privacidad de los usuarios. Este resultado confirma que la integración de

tecnologías inteligentes puede optimizar la efectividad del control parental, promoviendo un entorno digital más seguro y ético.

Las pruebas de verificación realizadas sobre el prototipo validaron su estabilidad, precisión y capacidad de respuesta. Se comprobó que el sistema identifica patrones de riesgo y genera notificaciones en tiempo real de forma efectiva.

En síntesis, el proyecto cumplió con los objetivos propuestos, aportando una solución innovadora, funcional y socialmente pertinente frente a los desafíos de la seguridad digital infantil. La aplicación móvil inteligente de control parental se perfila como una herramienta que no solo protege, sino que también educa y fomenta el diálogo entre padres e hijos sobre el uso responsable de la tecnología. Su desarrollo sienta las bases para futuras versiones con mayores capacidades de personalización y análisis predictivo, fortaleciendo la prevención y el bienestar digital en los entornos familiares.

Referencias

Alrusaini, O., & Beyari, H. (2022a). The Sustainable Effect of Artificial Intelligence and Parental Control on Children's Behavior While Using Smart Devices' Apps: The Case of Saudi Arabia. *Sustainability 2022, Vol. 14, Page 9388*, *14*(15), 9388. https://doi.org/10.3390/SU14159388

Alrusaini, O., & Beyari, H. (2022b). The Sustainable Effect of Artificial Intelligence and Parental Control on Children's Behavior While Using Smart Devices' Apps: The Case of Saudi Arabia. *Sustainability 2022, Vol. 14, Page 9388*, *14*(15), 9388. https://doi.org/10.3390/SU14159388

Antonio, M., Guamán, M., Del Cisne, P., & Guerrero, M. (2023). Revolución educativa: el impacto y futuro de la Inteligencia Artificial. *Killkana Técnica*, *7*(3), 29–36. https://doi.org/10.26871/KILLKANATECNICA.V7I3.1471

Auxier, B., & Perrin, A. & T. E. (2020, July 28). *Children's engagement with digital devices, screen time | Pew Research Center*. https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

Barzilay, S., Fine, S., Akhavan, S., Haruvi-Catalan, L., Apter, A., Brunstein-Klomek, A., Carmi, L., Zohar, M., Kinarty, I., Friedman, T., & Fennig, S. (2023). Real-Time Real-World Digital Monitoring of Adolescent Suicide Risk During the Six Months Following Emergency Department Discharge: Protocol for an Intensive Longitudinal Study. *JMIR Research Protocols*, *12*. https://doi.org/10.2196/46464

Beyens, I., Valkenburg, P. M., & Janssen, L. H. C. (2024). Parental Monitoring in the Digital Age. *The Cambridge Handbook of Parental Monitoring and Information*

Management during Adolescence, 193–214. https://doi.org/10.1017/9781009418652.012

CAI Virtual CIBERCRIMEN. (2024, December). *BALANCES ANUALES DEL CIBERCRIMEN* . https://caivirtual.policia.gov.co/observatorio/analisis-cibercrimen

Cheng Yong, T., Xu, N., Liang, M., & Li, L. (2025). Meta-analysis of associations between digital parenting and children's digital wellbeing. *Educational Research Review*, *48*, 100699. https://doi.org/10.1016/J.EDUREV.2025.100699

Dedkova, L., Smahel, D., & Just, M. (2022). Digital security in families: the sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour and Information Technology*, *41*(5), 1052–1064. https://doi.org/10.1080/0144929X.2020.1851769;WGROUP:STRING:PUBLICATION

Delgado-Zambrano, O. (2022, May 17). *Implementación de aplicativos de control parental en el uso de internet como herramientas tecnológicas de apoyo para el desempeño académico*. https://revistadigital.uce.edu.ec/index.php/CATEDRA/article/view/3383/5174

Dutta, A. C. (2025, June). *ARTIFICIAL INTELLIGENCE IN STUDENT PRIVACY AND DATA SECURITY - ProQuest*. https://www-proquest-com.bdbiblioteca.universidadean.edu.co/docview/3222814875/5ECA172D56344C98PQ/1?accountid=34925&sourcetype=Scholarly%20Journals

Future Market Insights. (2025). *Demanda y perspectivas del mercado de software de control parental 2025-2035*. https://www.futuremarketinsights.com/reports/parental-control-software-market

Hernandez, J. M., Ben-Joseph, E. P., Reich, S., & Charmaraman, L. (2024). Parental Monitoring of Early Adolescent Social Technology Use in the US: A Mixed-Method Study. *Journal of Child and Family Studies*, *33*(3), 759–776. https://doi.org/10.1007/S10826-023-02734-6

Madeline, L., Patel, J., & Katapally, T. R. (2025). Towards ethical surveillance of smartphone use among youth: exploratory digital citizen science approaches shaping the understanding of ubiquitous technology use. *Technology in Society*, *83*, 103012. https://doi.org/10.1016/J.TECHSOC.2025.103012

Muñoz-Carril, P. C., Souto-Seijo, A., Dans-álvarez-de-sotomayor, I., & Fuentes-Abeledo, E. J. (2023a). Parental control measures to regulate smartphones use by children. *Psychology, Society and Education*, *15*(3), 39–47. https://doi.org/10.21071/psye.v15i3.16077

Muñoz-Carril, P. C., Souto-Seijo, A., Dans-álvarez-de-sotomayor, I., & Fuentes-Abeledo, E. J. (2023b). Parental control measures to regulate smartphones use by children. *Psychology, Society and Education*, *15*(3), 39–47. https://doi.org/10.21071/psye.v15i3.16077

Muñoz-Carril, P.-C., Souto-Seijo, A., Dans-Álvarez-de-Sotomayor, I., & Fuentes-Abeledo, E.-J. (2023). Parental control measures to regulate smartphones use by children. *Psychology, Society & Education*, *15*(3), 39–47. https://doi.org/10.21071/PSE.V15I3.16077

NIST. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. https://doi.org/10.6028/NIST.AI.100-1

Olivero, R., Gillespie, S., Rakhmanina, N. Y., Abuogi, L., Gillespie, S., Jao, J., Neilan, A., Olivero, R., Rosebush, J., & Siberry, G. (2025). Increasing Access to Antiretroviral Therapy for the Prevention and Treatment of HIV in Infants, Children, and Youth in the United States: Policy Statement. *Pediatrics*, *156*(2). https://doi.org/10.1542/PEDS.2025-072718

Portal ICBF - Instituto Colombiano de Bienestar Familiar ICBF. (2022, February 17). *Conoce los riesgos cibernéticos a los que se enfrentan los niños y niñas y cómo prevenirlos* . https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-los-riesgos-ciberneticos-los-que-se-enfrentan-los-ninos-y-ninas-y-como

Sáiz-Manzanares, M. C., Marticorena-Sánchez, R., Martín-Antón, L. J., Almeida, L., & Carbonero-Martín, M. Á. (2023). Aplicación y retos de la tecnología de movimiento ocular en Educación Superior. *Oxbridge Publishing House*, *31*(76), 35–46. https://doi.org/10.3916/C76-2023-03

Theopilus, Y., Mahmud, A. Al, Davis, H., & Octavia, J. R. (2024). Digital Interventions for Combating Internet Addiction in Young Children: Qualitative Study of Parent and Therapist Perspectives. *JMIR Pediatrics and Parenting*, *7*. https://doi.org/10.2196/55364

Torrecillas-Lacave, T., Vázquez-Barrio, T., Suárez, R., & Fernández-Martínez, L. M. (2020). The role of parents in the online behavior of hyperconnected minors. *Revista Latina de Comunicacion Social*, *2020*(75), 121–148. https://doi.org/10.4185/RLCS-2020-1419

Trejos-Gil, C. A., & Vélez, Y. P. (2023). Ciberdelitos en menores de edad en la red social Facebook: revisión sistemática de literatura. *Nuevo Derecho*, *19*(32), 1–18. https://doi.org/10.25057/2500672X.1493

UNICEF. (2021). *Policy guidance on AI for children | Innocenti Global Office of Research and Foresight*. https://www.unicef.org/innocenti/reports/policy-guidance-ai-children

UNICEF. (2023). *Los niños y los riesgos digitales: informe sobre protección en línea y alfabetización digital. Fondo de las Naciones Unidas para la Infancia.* https://www.unicef.org/

UNICEF. (2025, June). *Childhood in a Digital World | Innocenti Global Office of Research and Foresight*. https://www.unicef.org/innocenti/reports/childhood-digital-world

Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2021). Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 343. https://doi.org/10.1145/3476084

Anexo

Anexo 1 Formato validación V de Aiken

VALIDACIÓN INSTRUMENTO DE MEDICIÓN - V DE AIKEN

Aplicación móvil inteligente de control parental para la detección temprana de riesgos digitales en menores

Nombre del Evaluador: Leidy Natalia Zapata	Rol del evaluador: Docente	Fecha de aplicación: 22/10/2025

INSTRUCCIONES: Para validar el instrumento de diagnóstico requerido en el presente estudio, se han identificado una serie de variables y un grupo preguntas que las describen. Califique cada una de las preguntas formuladas siendo 1 totalmente de acuerdo y 0 totalmente en desacuerdo, en relación a su grado de claridad, pertinencia y relevancia. Por favor tenga en cuenta las siguientes definiciones:

Claridad: la pregunta está correctamente redactada y es fácil de comprender por el evaluador.
Pertinencia: la pregunta permite medir con precisión la variable identificada.
Relevancia: se evidencia un enfoque teórico adecuado en la redacción de la pregunta.

		A. VARIABLE 1	CLARIDAD	PERTINENCIA	RELEVANCIA	Observaciones
Preguntas	1	De manera voluntaria, explícita, informada e inequívoca, autorizo a la Universidad Ean para tratar mis datos personales (https://universidadean.edu.co/la-universidad/quienes-somos/orientacion-estrategica/reglamentos-universidad-ean/autorizacion-uso-de-datos-personales), de acuerdo con lo dispuesto en los artículos 5, 7 y concordantes del Decreto 1377 de 2013 y las demás disposiciones legales referentes al tema. Para mayor información acerca del manejo de tus datos personales, puedes revisar nuestro aviso de privacidad (https://universidadean.edu.co/la-universidad/quienes-somos/orientacion-estrategica/reglamentos-universidad-ean/aviso-de-privacidad) y nuestra política de privacidad (https://universidadean.edu.co/sites/default/files/institucion/acuerdos/politica-tratamiento-de-datos-personales.pdf) / Si Autorizo / No Autorizo				
	2	¿Con qué frecuencia su hijo(a) utiliza dispositivos móviles (celular/tablet)? / Nunca / Ocasionalmente (1–2 veces por semana) / Con frecuencia (todos los días, menos de 2 horas) / Muy frecuente (todos los días, entre 2 y 5 horas) / Excesivo (más de 5 horas al día)	1	1	1	
	3	¿Qué actividades realiza principalmente su hijo(a) en los dispositivos móviles? (puede marcar varias) Juegos / Redes sociales / Videos/entretenimiento (YouTube, TikTok, etc.) / Búsqueda de información escolar / Comunicación (WhatsApp, llamadas, etc.)	1	1	1	
	4	¿Qué riesgos digitales considera más preocupantes para su hijo(a)? / Ciberacoso / Grooming (adultos que buscan contacto con menores) / Exposición a contenido sexual / Violencia en línea (juegos, videos, noticias) / Drogas o consumo de alcohol/tabaco / Adicción a internet/juegos	1	1	1	
	5	¿Alguna vez su hijo(a) ha estado expuesto a alguno de estos riesgos? / Si / No / No lo se	1	1	1	
	6	¿Utiliza actualmente alguna aplicación o método de control parental? / Sí, aplicaciones móviles (ej. Family Link, Qustodio, Bark) / Sí, controles integrados en el dispositivo / Sí, supervisión manual sin aplicaciones / No utilizo ningún método de control parental	1	1	1	
	7	¿Qué tan satisfecho(a) está con el método que utiliza actualmente? / Muy insatisfecho(a) / Insatisfecho(a) / Neutral / Satisfecho(a) / Muy satisfecho(a)	1	1	1	
	8	¿Le interesaría una aplicación que detecte en tiempo real riesgos en el dispositivo de su hijo(a) y le envíe alertas inmediatas? / si / no / Prefiero no utilizarlos	1	1	1	
	9	¿Qué aspectos considera más importantes en una aplicación de control parental? / Seguridad y protección de datos / Notificaciones en tiempo real / Fácil uso y configuración / No afectar el rendimiento del celular / Reportes diarios consolidados	1	1	1	
	10	¿Qué expectativas, sugerencias o recomendaciones tendría frente a una aplicación de control parental ?	1	1	1	