ESPECIALIZACIÓN EN CIBERSEGURIDAD

GUÍA PARA LA PREVENCIÓN DEL GROOMING EN NIÑOS, NIÑAS Y ADOLESCENTES EN EDADES ENTRE LOS 11 Y 15 AÑOS EN LAS INSTITUCIONES EDUCATIVAS DE LA CIUDAD DE MANIZALES Y SUS ALREDEDORES.

Erika Gómez Tangarife.

Juan Manuel Guerrero Ramírez.

Jhon Anderson Acevedo Cárdenas.

Ovidio Antonio Guerrero Mosquera.

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

PROPUESTA DE UN PROGRAMA DE CAPACITACIÓN INTEGRAL EN CIBER PROTECCIÓN CONTRA EL GROOMING EN LAS INSTITUCIONES EDUCATIVAS DE LA CIUDAD DE MANIZALES Y MUNICIPIOS ENTRE EDADES DE 11 A 15 AÑOS.

Trabajo de grado presentado como requisito para optar al título de *Especialización en Ciberseguridad*

Modalidad de grado: Proyecto de investigación del estudiante o grupo de estudiantes que se articula a una línea de investigación en coautoría y con acompañamiento de docente investigador

Héctor Roberto Gordon Quinche

Erika Gómez Tangarife.

Juan Manuel Guerrero Ramírez.

Jhon Anderson Acevedo Cárdenas.

Ovidio Antonio Guerrero Mosquera.

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD

ESPECIALIZACIÓN EN CIBERSEGURIDAD

MANIZALES, CALDAS

2023

Nota de aceptación: **4.2**

Dedicatoria

Queremos expresar nuestro profundo agradecimiento a Dios y a nuestros padres por su inmensurable apoyo y amor en la realización de este trabajo de grado de especialización.

En primer lugar, agradecemos a Dios por ser nuestra fortaleza y guía a lo largo de este proceso. Su sabiduría y dirección han iluminado nuestro camino, brindándonos inspiración y motivación para alcanzar nuestros objetivos.

Agradecimientos

Nos gustaría expresar nuestro más sincero agradecimiento a nuestros padres y profesores, quienes merecen una dedicación especial en este trabajo de grado. Su apoyo incondicional y su guía constante fueron fundamentales para culminar con éxito esta especialización que tanto anhelábamos. Estuvieron en nuestro lado, brindándonos su sabiduría, alentándonos en los momentos difíciles y celebrando nuestros logros. Su amor, paciencia y compromiso han dejado una huella imborrable en nuestro camino académico y en nuestras vidas en general. Este trabajo es un tributo a su inquebrantable confianza en nosotros ya la dedicación que han demostrado al impulsar nuestro crecimiento y desarrollo. Estamos profundamente agradecidos por todo lo que han hecho por nosotros y les estamos eternamente agradecidos.

Tabla de Contenido

TABLA DE IMÁGENES

Resumen

Este proyecto es un análisis sobre la situación en que se ven expuestos los niños, niñas y adolescentes entre los 11 y 15 años que hacen parte de instituciones educativas en Manizales y alrededores, por la modalidad de ciberacoso denominado “Grooming”, afecta de manera directa a los estudiantes y entidades educativas donde se encuentran los niños, niñas y adolescentes. Para evaluar la situación actual de los estudiantes, se realizaron encuestas en instituciones educativas aleatorias para estudiantes, profesores y acudientes, con el fin de realizar un análisis integral de esta amenaza latente y que sea una base para generar concienciación, educación y orientación a los niños, niñas y adolescentes expuestos por el uso inadecuado de las redes sociales. A partir de las encuestas realizadas se pudo evidenciar que la mayoría de los profesores conocen el término grooming, mientras que estudiantes y acudientes no conocen bien el término. En conclusión, se deben efectuar más campañas de prevención del grooming con los niños, niñas y adolescentes, profesores y acudientes para que ellos sepan los pasos a seguir si se ven afectados por esta modalidad y, ante todo, inculcar el buen manejo de redes sociales tanto en pequeños y grandes, para evitar el grooming en Manizales y sus alrededores.

***Palabras clave*:** Grooming, redes sociales, concienciación, sexting.

Abstract

This project is an analysis of the situation in which children and adolescents between the ages of 11 and 15 years who are part of educational institutions in Manizales and surrounding municipalities are exposed, by the form of cyberbullying called "Grooming", which directly affects students and educational institutions where children and adolescents are found. To assess the current situation of students, surveys were conducted in random educational institutions for students, teachers and guardians, in order to conduct a comprehensive analysis of this latent threat and to be a basis for generating awareness, education and guidance to children and adolescents exposed by the inappropriate use of social networks. From the surveys conducted, it became evident that most teachers know the term grooming, while students and guardians do not know the term well. In conclusion, more grooming prevention campaigns should be carried out with children and adolescents, teachers and guardians so that they know the steps to follow if they are affected by this modality and above all, instill good management of social networks in both young and old, to avoid grooming in Manizales and surrounding municipalities.

Key words: Grooming, social networks, awareness, sexting.

1. Introducción

Ante el gran aumento que tienen las actividades cibernéticas donde la interacción niño-ciberespacio crece cada día más y estos permanecen más tiempo en línea, lo cual trae consigo también un gran aumento de las situaciones de riesgo en donde ellos y las entidades en las cuales se conectan puedan ser víctimas de ataques, abusos u otra actividad de ciberdelincuencia.

Toda la descripción anterior la podemos resumir en la modalidad Grooming, y para ser más específicos se manifiesta por redes sociales, mensajería instantánea, juegos online etc.… en donde el ciberdelincuente busca ganarse la confianza de los niños haciendo que realicen actividades bajo engaños o en contra de su voluntad.

Para tener datos más reales sobre la situación actual del Grooming en los niños, se realizaron encuestas al azar en instituciones educativas aleatorias con el fin de realizar un análisis parcial de los porcentajes de las amenazas existentes y las nuevas por haber. Además, que los resultados de dichas encuestas serán de utilidad para realizar sensibilización a la población adulta para que orienten a los niños, niñas y adolescentes haciéndoles ver las consecuencias de sus actos si no son correctos, en donde los afectados son tanto ellos como las instituciones educativas, porque una víctima es un puente para que el ciberdelincuente atente con ambas integridades.

La planificación de prevención de riesgos ante estos sucesos pretende tener un alcance más allá de la ciudad capital de Caldas, y con esta planificación se busca que de manera iterativa los padres eduquen a sus hijos de la manera correcta al conocer las amenazas latentes en el ciberespacio o las aplicaciones online.

Por ello la importancia de este proyecto es el de integrar las competencias de educación de los padres en la evolución de las tecnologías mejorando la formación de los preadolescentes y adolescentes (de 11 y 15 años) que se encuentran en las instituciones.

2. Localización

La ciudad de Manizales es la capital del Departamento de Caldas, por lo cual hace parte de la Región Eje Cafetero de acuerdo con lo contemplado en el Plan Nacional de Desarrollo 2014-2018. Se encuentra situada a una altura de 2.153 metros sobre el nivel del mar, está localizada en la región central del occidente colombiano, sobre la prolongación de la Cordillera de los Andes.

Fundada en 1849 por colonos antioqueños, hoy es una ciudad con gran actividad económica, industrial, cultural y turística. Igualmente resalta por su actividad cultural en la que se destacan su Feria anual, el Festival Internacional de Teatro y numerosos espectáculos y convenciones.

De acuerdo con las cifras presentadas por el DANE del censo 2018 Manizales cuenta con una población de 454 077 habitantes. El 47,1 % de la población son hombres y el 52,9 % mujeres. La ciudad cuenta con una tasa de analfabetismo del 5% en la población mayor de 5 años.

3. Objetivos

Objetivo General

Desarrollar una guía de implementación de medidas de ciberseguridad para la prevención del Grooming en niños, niñas y adolescentes en edades entre los 11 y 15 años en las Instituciones Educativas de la ciudad de Manizales y sus alrededores.

Objetivos Específicos

- Realizar una revisión bibliográfica exhaustiva sobre los antecedentes del Grooming, su definición y características, y los factores de riesgo.

- Identificar a través de encuestas dirigidas a los NNA, profesores y padres de familia en la ciudad de Manizales qué aspectos del Grooming conocen y en qué porcentaje son desconocidos.

- Establecer que dispositivo electrónico y cuáles son las cuatro redes sociales más utilizadas por los NNA, a fin de entender mejor los riesgos asociados al Grooming.

- Revisar detalladamente las configuraciones de privacidad y seguridad de las cuatro redes sociales que se establezcan.

- Elaborar una guía práctica que contemple medidas efectivas de ciberprotección para prevenir y mitigar el riesgo de grooming en las redes sociales utilizadas por los NNA, con el fin de fomentar su seguridad en línea y prevenir situaciones de vulnerabilidad.

4. Antecedentes

A nivel de la ciudad de Manizales, podemos rescatar los estudios realizados en años anteriores para determinar que el ciberacoso ha tenido como principal objetivo a la población infantil. En el año 2013 se realizó un estudio de: “Frecuencia de acoso y ciberacoso, y sus formas de presentación en estudiantes de secundaria de colegios públicos de la ciudad de Manizales”, en donde los resultados arrojados nos afirman que la población afectada son estudiantes menores de 14 años y estos son afectados con tendencia a ser víctima de ciberacoso, sexting y pornografía infantil. (Aranzalez Delgado, Castaño Castrillón, Figueroa Salcedo, & Jaramillo Ruiz, 2014)

El Instituto Colombiano de Bienestar Familiar de Colombia en el programa Ser-Padres, tiene un artículo con la clasificación de los principales riesgos digitales y cómo evitarlos, respondiendo a la pregunta ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet?, este recurso, nos permite identificar los riesgos de contenidos, riesgos de conducta y riesgos de contacto a los cuales se encuentran expuestos los niños, niñas y adolescentes objeto de este estudio. (ICBF, 2019)

“El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Apropiación de TIC, presentará "Internet Sano". La iniciativa busca proteger a niñas, niños y adolescentes del país de toda forma de conducta en la red que pueda lesionar su integridad.” (MinTIC Colombia, 2012)

Los hechos que se dieron a conocer por noticia criminal (Denuncia) la fecha 27/04/2021 interpuesta por la abuela de la menor de edad ante las instalaciones de la FGN del municipio de

Riosucio Caldas, en la denuncia se expone que la menor de edad de 11 años ha sido víctima de violencia sexual por parte de un mayor de edad de género masculino.

En la entrevista forense de la fecha 23/06/2021 realizada a la menor víctima, relata que el infractor en múltiples ocasiones la indujo a prácticas sexuales por medio de **sexting,** le exigía que le enviara fotos o contenido multimedia de sus partes íntimas, el sujeto le enviaba fotos suyas de sus partes íntimas.

La red social usada para el delito fue **WhatsApp** por donde se enviaba el contenido sexual, estas conversaciones se sostuvieron en el mes de marzo de 2021.

Los hechos de connotación jurídico penal, ocurrieron en el municipio de Riosucio Caldas, en zona rural conocida como vereda Buenos Aires en el mes de marzo del año 2021.

El denunciado sabía que realizaba conductas prohibidas por la ley con la menor de edad, por lo que utilizaba las redes sociales para “no dejar evidencia” y así aprovechar la poca edad de la joven para inducir a prácticas sexuales.

(fiscalía general de la Nación, Selección Caldas, 2021)

5. Marco teórico

En la elaboración de este trabajo de grado se utilizaron diferentes conceptos y teorías necesarias para el desarrollo de los objetivos específicos planteados y así dar cumplimiento al objetivo general propuesto; dentro de los conceptos y/o teoría revisada, se destacan los siguientes:

Pedofilia

La pedofilia o paidofilia es una parafilia, es decir, un trastorno de la inclinación sexual que se caracteriza por la presencia fantasías recurrentes y productoras de un elevado nivel de excitación sexual en el que el objeto de deseo es un objeto, personas o entes no consintientes o una situación de humillación y sufrimiento propio y ajeno. La experimentación de dichas fantasías puede conllevar su realización y/o sentimientos de intenso malestar para quien las padece.

En el caso concreto de la pedofilia, el objeto de deseo o lo que provoca la atracción sexual son niños o niñas prepúberes. Concretamente se puede considerar una cronofilia, debido a que hay una gran diferencia entre la edad del sujeto y la del objeto de deseo. Para su diagnóstico es necesario que el sujeto sea mayor de dieciséis años de edad y que la víctima u objeto de deseo sea al menos cinco años menor.

Por norma general el pedófilo buscará el contacto con su objeto de deseo, recurriendo con frecuencia a imágenes pornográficas y autoestimulándose en base a sus fantasías, pero no tiene por qué intentar mantener relaciones sexuales.

Pedófilo

Persona que practica la pedofilia, es decir que, siente atracción sexual por niños o niñas, pero no necesariamente realiza actos de agresión sexual.

Pederastia

La pederastia se define como el abuso sexual a menores. Entendiéndose aquí el concepto de "menor" como toda persona que no supere los 18 años de edad, lo que incluye a infantes, prepúberes y adolescentes.

Se considera que existe este abuso cuando hay una relación de desigualdad de edad, madurez o poder significativo entre agresor y víctima y donde se produce la utilización del menor como objeto sexual.

Pederastia es por tanto la implicación de niños o adolescentes en actividades sexuales que todavía no comprenden en su totalidad o no están preparados para asimilar, quedando condicionado su real consentimiento con plena conciencia.

El abuso sexual no tiene por qué implicar contacto sexual directo, hay otras formas de abuso como el exhibicionismo, exposición de menores a material pornográfico, voyeurismo, o comunicación sexual a través de teléfono o Internet, todas ellas igual de graves.

Pederasta

Persona que practica la pederastia, es decir; comete abuso sexual de menores.

Pornografía Infantil

Es toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

Internet

Internet es la red que conecta e interrelaciona dispositivos electrónicos y redes de computadoras entre sí, de todo el mundo. Su nombre proviene del inglés International Network que significa "Red Internacional" y el acrónimo de esas palabras dio origen al nombre Internet.

Identidad Digital

También conocida como identidad 2.0, está la identidad digital por definición engloba todas las acciones que nos identifican en Internet: fotos que publicamos o en las que nos etiquetan, comentarios, likes, retweets, posts y peticiones online que firmamos. Este tipo de acciones online crean una reputación digital, una opinión que los demás se forman acerca de nosotros con lo que ven publicado.

A medida que Internet va creciendo, nuestra identidad digital se ve cada vez más expuesta. Solo observemos la cantidad de actividades que realizamos de forma digital y todos los servicios a los que accedemos con frecuencia: compras, operaciones bancarias, suscripciones, etc. Este avance requiere garantizar la seguridad de nuestra identidad digital y nuestra privacidad.

Huella Digital

Siempre que utilizas Internet, dejas un rastro de información conocido como tu huella digital. Una huella digital crece de muchas maneras: por ejemplo, cuando públicas en redes sociales, te suscribes a un boletín informativo, dejas una reseña en línea o compras en línea.

En ocasiones, no siempre es obvio que estás contribuyendo a tu huella digital. Por ejemplo, los sitios web pueden rastrear tu actividad instalando cookies en tu dispositivo, y las aplicaciones pueden recopilar tus datos sin que lo sepas. Una vez que permites que una organización acceda a tu información, esta podría vender o compartir tus datos con terceros. Y lo que es peor, tu información personal podría verse comprometida como parte de una filtración de datos.

Redes Sociales

Las redes sociales son una herramienta de comunicación que posibilita el intercambio de ideas, e información a través de la web. Están fundamentadas en Internet y brindan a los usuarios la posibilidad de interactuar y compartir contenido como información personal, documentos, videos e imágenes. Los usuarios interactúan con las redes sociales por medio de una PC, tablet o smartphone o por medio de apps o programas basados en la web.

Ingeniería Social

La ingeniería social manipula a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o bien cometan otros errores que comprometan sus activos o seguridad personal o empresarial.

Un correo electrónico que parece proceder de un proveedor fiable en el cual se solicita información actualizada de la tarjeta de crédito, un buzón de voz amenazante que afirma ser del IRS o una oferta jugosa de un potentado extranjero son solo algunos ejemplos de ingeniería social.

Como la ingeniería social explota las debilidades humanas en lugar de las vulnerabilidades técnicas o del sistema digital, a veces se le llama "ataque informático humano".

Phishing

Es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robar información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Seguridad Digital

Es entender a Internet como un escenario real (como el hogar o la calle), donde se viven situaciones reales. Se debe procurar tener cuidado y evitar situaciones de riesgo, como, por ejemplo, la pérdida de información laboral al dañarse o extraviar el computador, el acceso de otras personas a las cuentas en redes sociales o a las transacciones bancarias que se encuentran registradas en el celular, entre otras.

Ciberdelito

Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.

Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.

Ciberacoso

Es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.

Ciberdelincuente

Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

Grooming

El grooming es un fenómeno de engaño en el que un adulto se pone en contacto a través de la red con un menor de edad (normalmente una chica) haciéndose pasar normalmente por un adolescente con el objetivo de abusar sexualmente de él o ella.

A través de la red es fácil inventar un personaje y hacer pensar a un/a adolescente que está comunicándose con alguien de su edad y con unas características determinadas.

Habitualmente contactan con ellas haciéndose pasar por otro adolescente del sexo opuesto. Previamente han estudiado el perfil de la víctima en las redes sociales con lo que les resulta muy fácil entablar una relación. Para ello pueden crear un perfil falso con fotografías y gustos atractivos para las menores. Tras un tiempo ganándose su confianza logran que la víctima le admita como amigo en sus redes sociales. Más tarde tratan de seducirlas intentando obtener alguna imagen íntima o información comprometida. Una vez obtenida el agresor amenaza con mostrar a su grupo de iguales esa imagen o información si no lleva a cabo el comportamiento sexual que él desea… así comienza en muchos casos la extorsión. Este proceso encierra a la víctima en un círculo vicioso de difícil salida.

En estos casos, el adulto establece contacto con el menor y lo hace de manera deliberada y sostenida en el tiempo. Lo hace a través de medios telemáticos (móvil, ordenador, tablet, etc…) con la intención de establecer una relación y un control emocional sobre el menor para así preparar el terreno y abusar sexualmente de él/ella. Una vez más, este tipo de riesgos tienen lugar por el

exceso de confianza que los adolescentes tienen en el manejo de las nuevas tecnologías y la escasa percepción de riesgos.

Características del Grooming

a. SIEMPRE hay una VOLUNTARIEDAD inicial de ENGAÑO de un adulto hacia un menor.

b. La INTENCIÓN del ADULTO que contacta con el menor es de obtener una relación y un control emocional para obtener de él/ella satisfacción sexual.

c. Este tipo de acoso se da mayoritariamente con las CHICAS.

d. Siempre se utilizan DISPOSITIVOS TECNOLÓGICOS para llevarlo a cabo y es posible por la escasa percepción de riesgos en su utilización que tienen los adolescentes.

e. Normalmente el agresor no parece tener prisa y se gana la confianza de su víctima en el tiempo.

f. La relación entre el acosador y el acosado termina en CHANTAJE, cuando el acosador consigue, normalmente a través del acercamiento y engaño, obtener un elemento de fuerza con el que obligar a la víctima a hacer aquello que le solicite. Lo más habitual es que ese elemento sea alguna imagen íntima y/o comprometida de la víctima y el chantaje consista en amenazar a ésta con hacerla pública en el caso de que no haga lo que le pide. Estas peticiones suelen consistir en el envío de imágenes a través de la Webcam o, incluso, un encuentro personal con el riesgo que ello supone.

Riesgos del grooming:

a. ABUSO SEXUAL: El fin último del agresor es la satisfacción sexual con su víctima, que es menor de edad. El abuso sexual puede ocasionar secuelas traumáticas muy graves a la víctima.

b. PÉRDIDA DE PRIVACIDAD: Ver las imágenes compartidas con esta persona difundidas por la Red sin el consentimiento propio.

c. SENTIMIENTO DE ENGAÑO: Al acceder a las peticiones de un desconocido, podemos encontrarnos con que no somos dueños de lo que estamos compartiendo.

d. CHANTAJE: Pueden verse sometidos a chantaje por la persona que les está extorsionando para conseguir sus propios fines.

e. PORNOGRAFÍA: Verse inmersos en el mundo de la pornografía infantil sin tener conocimiento de ello y de las implicaciones legales y psicológicas que conlleva.

f. PÉRDIDA DE AUTOESTIMA: Pueden llegar a sentirse humillados y utilizados y pensar que no han sido capaces de detectar la utilización a la que han sido sometidos.

Ciberbullying o Ciberacoso

Se denomina a todo tipo de intimidación, pero por medio de plataformas digitales (redes sociales, plataformas de mensajería, plataformas de juegos, teléfonos móviles, etc.) Este acto consiste en intimidar, humillar, atemorizar a otras personas. Algunos de estos actos son:

- Difundir mentiras o publicar fotografías o videos vergonzosos de alguien en las redes sociales.

- Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería

- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

El ciberacoso es uno de los delitos más comunes a nivel mundial y ocurre en su mayoría entre los adolescentes. (Juan, Vayá, & García)

4 figura. Ilustración de Ciberbullying. (Siete estrellas, 2021)

Ciber Agresores sexuales

Son denominados a personas aparentemente normales, generalmente hombres y pocas mujeres que saben el manejo del ciberespacio los cuales adoptan una posición de anonimato y seguridad que beneficia su percepción de inmunidad y facilita su actividad mediante la gran demanda que tienen las redes sociales

Los estudios del *Crimes Against Center Research Center (CCRC)* muestran que la mayoría de los ciber agresores son masculinos los cuales la edad media ha disminuido en los últimos años donde hasta el 2009, un 50% tenían menos de 25 años.

Otra tendencia que se afirma al pasar el tiempo respecto a estudios anteriores es que la gran mayoría de los delincuentes eligen víctimas que ya conocen en persona inclusive miembros de sus propias familias.

La posesión de pornografía infantil es otra característica de los ciberagresores y también la tendencia a ser exhibicionistas ya que algunos envían fotos sexualmente explícitas de sí mismos con la intención de reducir sus impedimentos como expone *Krone (2004)* en la siguiente frase.

"Una persona que ha iniciado un contacto en internet con un niño con la intención de establecer una relación sexual que implique sexo virtual o físico. En este caso, las imágenes suelen utilizarse para desensibilizar al niño respecto de la actividad sexual (o "prepararlo"): muestra las imágenes al niño para reducir sus inhibiciones respecto de las actividades sexuales".

(Juan, Vayá, & García)

5 figura. Víctima y victimario. (COLEGIO NUESTRA SEÑORA DEL HUERTO, 2018)

Impacto psicológico del Abuso Sexual Infantil a través de Internet (ASI-I)

Existe la evidencia que el abuso sexual durante la etapa de la infancia crea problemas a largo plazo para quienes han sido víctimas. Los problemas se pueden evidenciar desde graves dificultades en la salud mental de las víctimas, trastornos de conducta y adicciones (CHOO 2009) Pueden sufrir efectos psicológicos comunes al abuso sexual clásico, pero su impacto psicológico puede variar debido a las características específicas del ciberespacio (velocidad de difusión,

simultaneidad de experiencias, interactividad, audiencia mundial, etc.), que influirán más o menos en el proceso de victimización primaria del menor según las características del trauma (duración, violencia, relación con abusador, etc.), del individuo (edad, género, poli victimización, etc.) y los factores contextuales (apoyo familiar, social, recursos disponibles, etc.).

(Juan, Vayá, & García)

Control parental

Es un mecanismo usado especialmente por adultos para tener control y registro de los diferentes sitios web, sistemas operativos y equipos, el acceso y manipulación que los menores de edad les dan a las herramientas tecnológicas.

Las funciones de este control parental son:

-Monitoreo de navegación de los usuarios.

-Restricción de contenido no apto para menores de edad

Es posible establecer límites en el tiempo para el uso del equipo o impedir que ejecuten programas maliciosos.

(Goodwill Community Foundation, Inc.)

6 Figura. Ilustración de navegación segura. (nesterenko.ruslan, s.f.)

Groomer

El termino Groomer hace referencia a un ciberacosador adulto que se sirve del engaño a través del uso de las nuevas tecnologías (fundamentalmente chats, redes sociales o foros) para propiciar un abuso sexual a un menor de edad.

Sexting

Se denomina sexting a la actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación.

Internet sano

"Internet Sano", es una estrategia para proteger la identidad de niños y jóvenes en la red.

El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Apropiación de TIC, presentará "Internet Sano". La iniciativa busca proteger a niñas, niños y adolescentes del país de toda forma de conducta en la red que pueda lesionar su integridad.

La viceministra de TIC, María Carolina Hoyos Turbay, presentará la estrategia "Internet Sano", en acto que se llevará a cabo en el Centro Cultural Gabriel García Márquez, el martes 30 de noviembre a las 2:00 p.m. "Internet Sano", es una propuesta que integra temas de protección a menores en la red como explotación sexual, pornografía y conductas que afectan la integridad de niños y jóvenes en la red. "Internet Sano" es una iniciativa nacional que se desarrolló para darle cumplimiento a las leyes 679 de 2001 y 1336 de 2009.

Para beneficio de los niños, niñas, docentes y padres de familia, se pondrá en funcionamiento a través de redes sociales como Facebook y Twitter, un grupo de profesionales los orientarán para apoyarlos con sus denuncias y promover el buen uso de la red", indicó la viceministra Hoyos Turbay. Prevé la formación virtual de administradores de sitios de acceso social seguros como café internet, tecno centros, portales interactivos y salas de sistemas de las instituciones educativas públicas y privadas de todo el país.

Adicionalmente se ha hecho una invitación a los proveedores de internet, para que hagan parte de esta iniciativa que pretende respaldar la masificación del buen uso de las TIC a través de actividades promocionales, con la entrega de controles parentales en cada activación, con contenidos ilustrativos para niñas, niños y adolescentes. Además, se entregarán premios a los colegios que usen efectivamente las TIC y que adopten esta iniciativa como suya propia. Los objetivos de "Internet Sano", son dictar medidas de protección contra la explotación, la pornografía y el turismo sexual y demás formas de abuso sexual con menores de edad en Internet, a través de disposiciones preventivas y sancionatorias. Busca además prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad en Internet de acuerdo con lo establecido en la Ley 679 de 2001.

Finalmente, "Internet Sano" busca que tanto niñas, niños y jóvenes del país, integren las Brigadas de Voluntarios en Alfabetización para que apoyen a sus padres y vecinos para que puedan convertirse en Ciudadanos Digitales. Este evento será la oportunidad también para el lanzamiento de la nueva imagen de la estrategia, Suzy una adolescente que navega frecuentemente en la web.

(MinTIC Colombia, 2012)

7 Figura. Internet sano es una iniciativa colombiana. (IPcom Sistemas S.A.S, s.f.)

Marco Normativo

En Colombia no se cuenta con una ley explicita para castigar conductas de Grooming, sin embargo, se castiga o imparte justicia sobre los groomer a través de leyes relacionadas con delitos informáticos como lo son la explotación y pornografía infantil que permiten la protección de niños, niñas y adolescentes en los temas y casos de acoso por medio de internet, a continuación, nombramos las leyes y normas más importantes en esta clase de delitos:

Ley 679 de 2001

"por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución" (Función pública, 3 de agosto de 2001)

Ley 1336 de 2009

"Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes." (https://www.icbf.gov.co/, 21 de julio de 2009)

Ley 599 de 2000 del Código penal colombiano

"Artículo 218. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, transmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro."

Artículo 219A. Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años. El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad.

La Ley 1273 de 2009 complementa el Código Penal con la implementación de los siguientes artículos:

"Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro."

Ley 1260 de ciberbullying (ciberacoso) en Colombia

La Ley 1620 de 2103 hace referencia sobre el ciberbullying (artículo 2) como una forma de intimidación con la ayuda de las tecnologías de la información, tales como internet, redes sociales, telefonía móvil, videojuegos en línea, etc., a fin de ejercer maltrato psicológico y continuo.

Al respecto, se creó el Sistema Nacional de Convivencia Escolar y Formación para los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar (artículo 8, numeral 9), cuya función es, entre otras, coordinar la creación de mecanismos de denuncia y seguimiento en internet, redes sociales y demás tecnologías de la información.

(Forjando Ciberseguridad , 2021)

8 Figura. Stop Bullying. (Forjando Ciberseguridad, 2021)

Ley 1581 de 2012 Protección de datos personales

Un dato es una información que puede ser numérica, alfabética, fotográfica, acústica o cualquier otro tipo identificable y pueda ser relativa entre otros a:

-Identidad (Nombres, apellidos, domicilio, fijación, fotografía o video)

-Ocupaciones (Estudios, trabajos, historial de actividades, etc.)

-Patrimonio (Ingresos, egresos, cuentas bancarias, consumos, información fiscal, etc.)

-Salud (Estado de salud, historia clínica, enfermedades físicas o psicológicas)

-Características (Tipo de sangre, ADN, discapacidades, raza, peso)

-Hábitos (Sexuales, políticos, ideológicos, creencias.)

La ley 1581 conocida como la ley de protección de datos fue creada con el propósito de garantizar la seguridad y protección de los datos personales que están almacenados en diversas bases de datos de entidades sean privadas o públicas y que realizan algún tratamiento de datos.

Estos datos son clasificados en tres grupos dependiendo de su alto o bajo grado de aceptabilidad de divulgación o nivel de riesgo que se expone la organización cuando se violan los principios de integridad, confidencialidad y disponibilidad.

-Datos públicos

-Datos semiprivados

- Datos privados o sensibles

El incumplimiento de la Ley de protección de datos lo expone a sanciones de tipo económico y operativo, sin embargo, también se expone a temas reputacionales que pueden ser perjudiciales para su empresa como son:

-Sanciones económicas hasta por 2.000 SMMLV.

-Suspensión de actividades relacionadas al tratamiento hasta por seis (6) meses.

-Cierre temporal de las operaciones relacionadas con tratamiento de datos.

-Cierre definitivo de las operaciones relacionadas con tratamiento de datos sensibles.

(Data Protected)

9 Figura. Datos protegidos. (Lopez & Lopez Abogados)

6. Metodología

Estrategias Metodológicas.

Las estrategias metodológicas que se utilizaron en el desarrollo del presente trabajo de grado serán:

Revisión documental.

Esta estrategia consistirá en la revisión de información acerca del Grooming en Colombia, particularmente en la ciudad de Manizales y sus alrededores vecinos, utilizando como referencia los trabajos de investigación sobre el Grooming previos a este, artículos de estudio, cifras de organizaciones sin ánimo de lucro e instituciones del estado. Por último, se realizará revisión de conceptos y/o metodologías de ciberseguridad relacionadas con la conducta de Grooming cuya utilidad está directamente relacionada con los objetivos propuestos en este proyecto.

Realización de encuestas.

En esta estrategia se recolectará información a través de encuestas en Instituciones educativas aleatorias de la ciudad de Manizales sobre el conocimiento que tienen los NNA, profesores y los padres de familia o tutores de los NNA acerca del Grooming. Adicionalmente, se recolectará información que revele cual es el dispositivo electrónico y las redes sociales que usan con mayor frecuencia.

Análisis de los datos recolectados.

En esta estrategia se analizarán los datos recolectados que permitan generar información de valor y así poder evaluar las necesidades que tiene la comunidad educativa para prevenir que los NNA sean víctimas de Grooming.

Selección de los cuatros redes sociales más utilizadas por los NNA encuestados.

En esta estrategia se seleccionarán las cuatro redes sociales más usadas por los NNA obtenidas en el análisis de los datos recolectados en las encuestas.

Exploración de las configuraciones de seguridad y privacidad del perfil de usuario de las redes sociales elegidas en esta investigación.

En esta estrategia se hará una exploración de las configuraciones de las cuatro redes sociales más utilizadas por los NNA, de acuerdo con el resultado de las encuestas se determinará si se hace en la página web o en la App móvil de la respectiva red social.

Presentación del producto final.

En esta estrategia se realizará un manual para la prevención del Grooming en NNA en la ciudad de Manizales y sus alrededores, pero que también puede ser usado en cualquier parte de Colombia o países de habla hispana. El manual estará compuesto por 3 capítulos, en el primero se sugerirán las configuraciones de seguridad y privacidad que deben tener los perfiles de las cuatro redes sociales que más utilicen los NNA, en el segundo se sugerirán y mostrara la configuración de 4 aplicaciones de control parental, y en el tercero se realizara una guía paso a paso de 2 rutas para la realización denuncia en línea de conductas de Grooming en Colombia. Por ultimo y como valor agregado, se darán una serie de recomendaciones y/o contramedidas que permitan que los NNA

naveguen de manera más segura en Internet, reduciendo el riesgo de ser víctimas de Grooming y/u otros ciberdelitos.

Modalidad del Trabajo de Grado

Tipo de Proyecto.

Este es un proyecto social de enfoque cuantitativo y cualitativo, cuantitativo porque se recogerán y analizarán datos que permitirán medir que porcentaje de NNA, profesores y padres de familia tienen conocimiento acerca del Grooming; y es cualitativo porque permitirá identificar los conocimientos que tienen los NNA, profesores y padres de familia para prevenir el Grooming y las rutas de denuncias disponibles en línea.

Tipo de Trabajo.

Este proyecto es de tipo prospectivo; dado que principalmente se hará un diagnóstico del conocimiento actual que tienen los NNA, profesores y padres de familia sobre el Grooming, y posteriormente se realizara un manual para brindar conocimiento a los miembros de la comunidad educativa y generar concienciación sobre las medidas que se deben implementar para reducir el riesgo de que los NNA sean víctimas de Grooming.

Método de Investigación Aplicado.

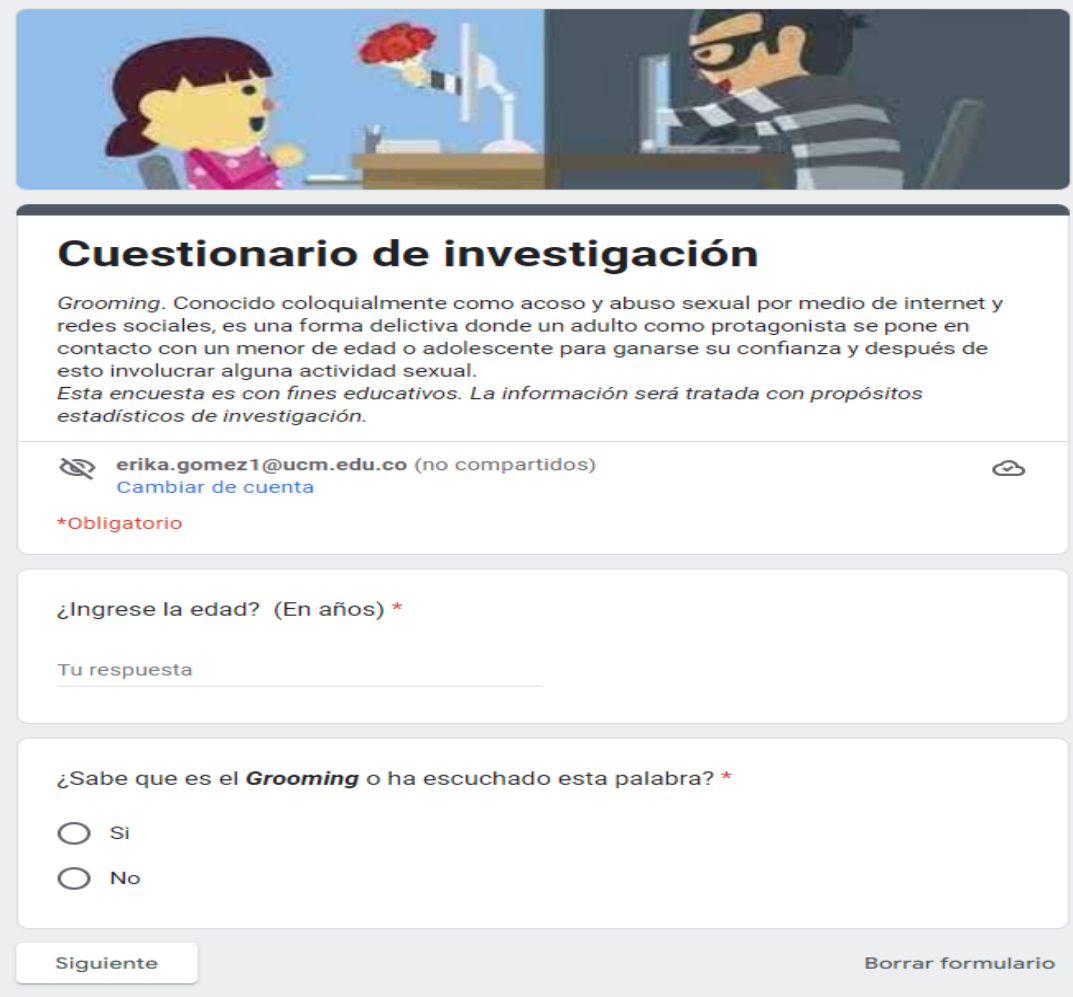
El método de investigación aplicado en el desarrollo del presente proyecto es investigación aplicada tecnológica, ya que se genera conocimiento con aplicación directa a un problema de la sociedad, Grooming, que no solo afecta a los NNA víctimas de este, sino que también puede generar consecuencias negativas en toda una familia.

7. Cuerpo del trabajo

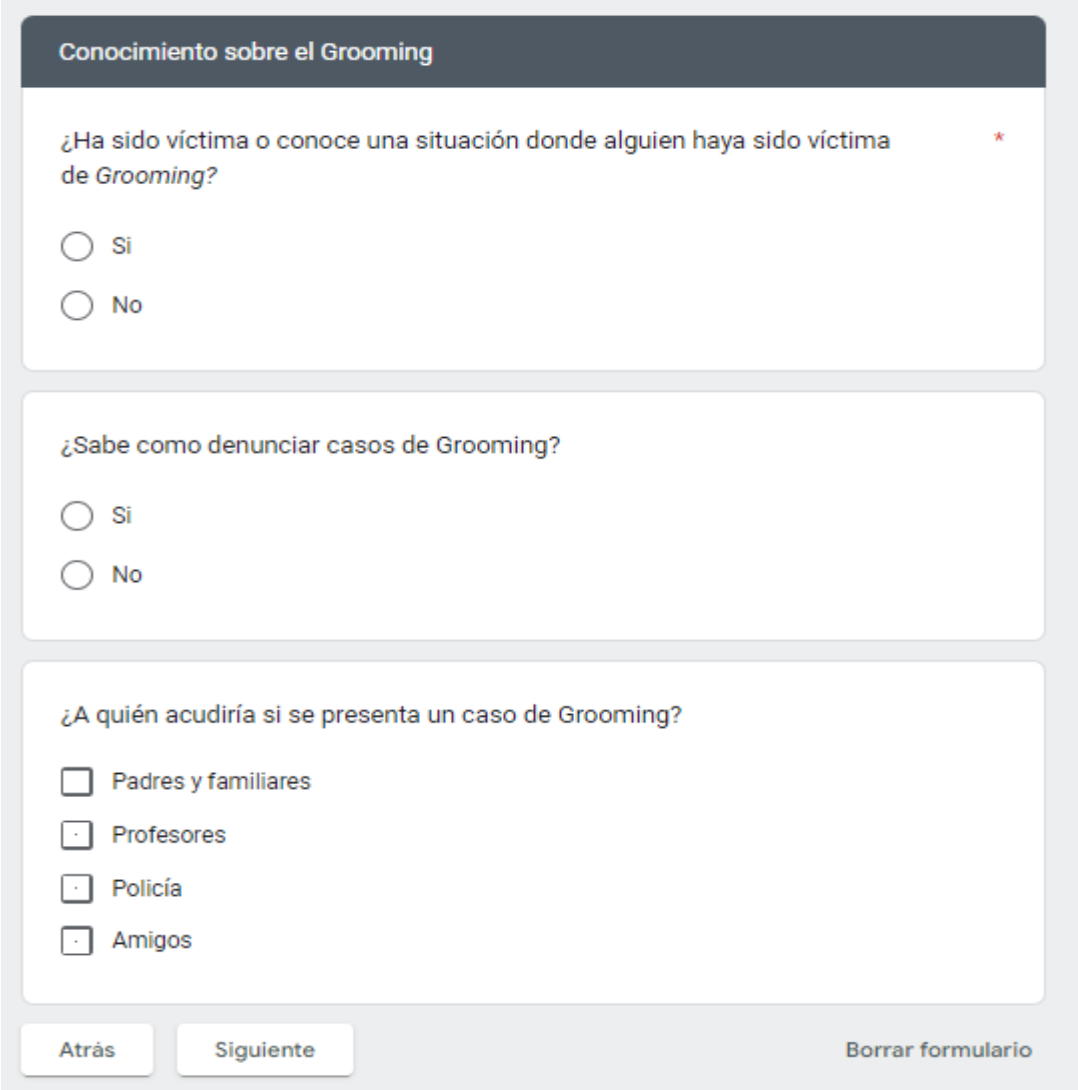
Se realizaron encuestas a los alumnos, profesores y familiares para determinar el conocimiento que tienen acerca del Grooming.

A continuación, se muestran las estructuras de las encuestas realizadas:

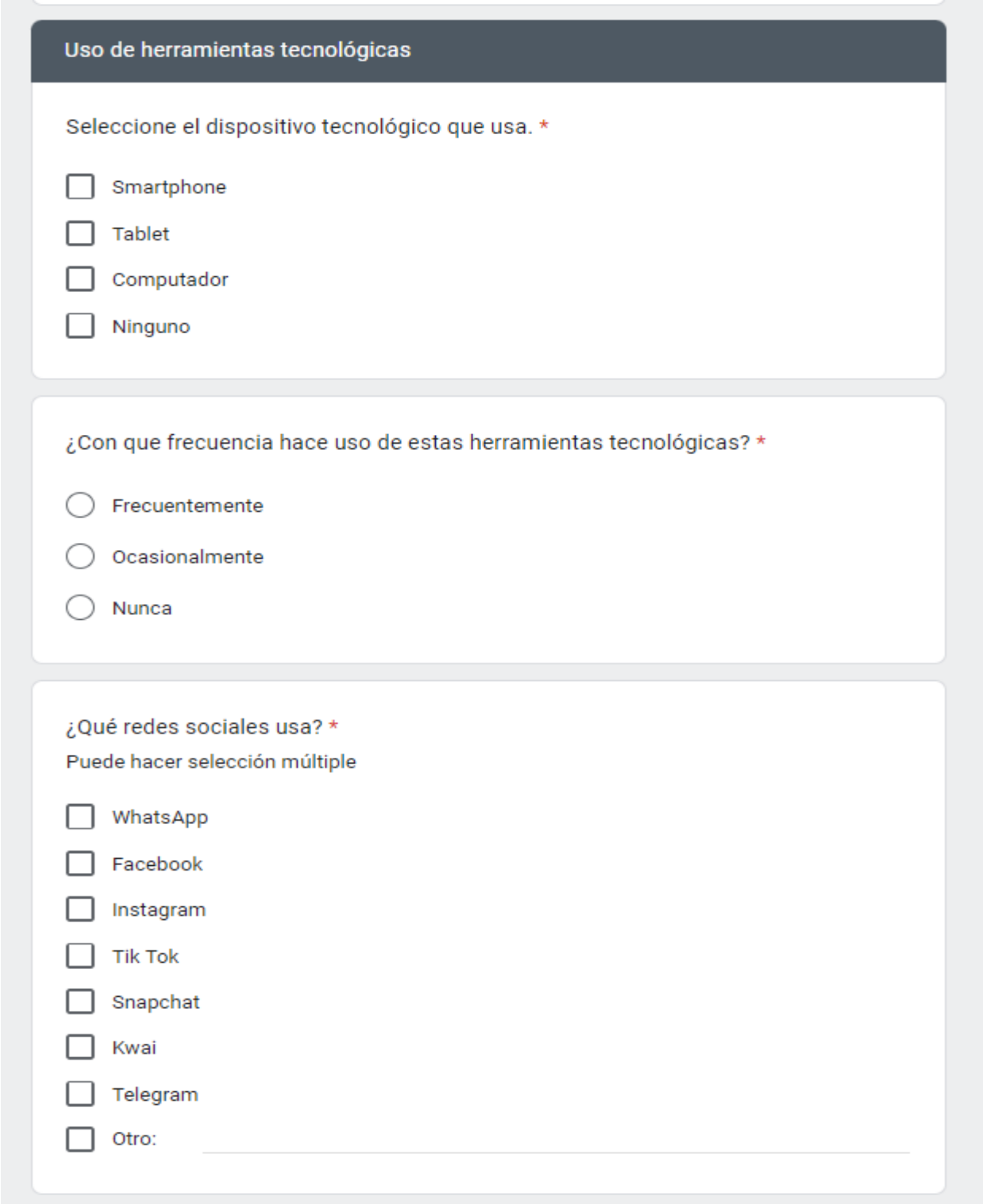
Cuestionario de investigación Alumnos:



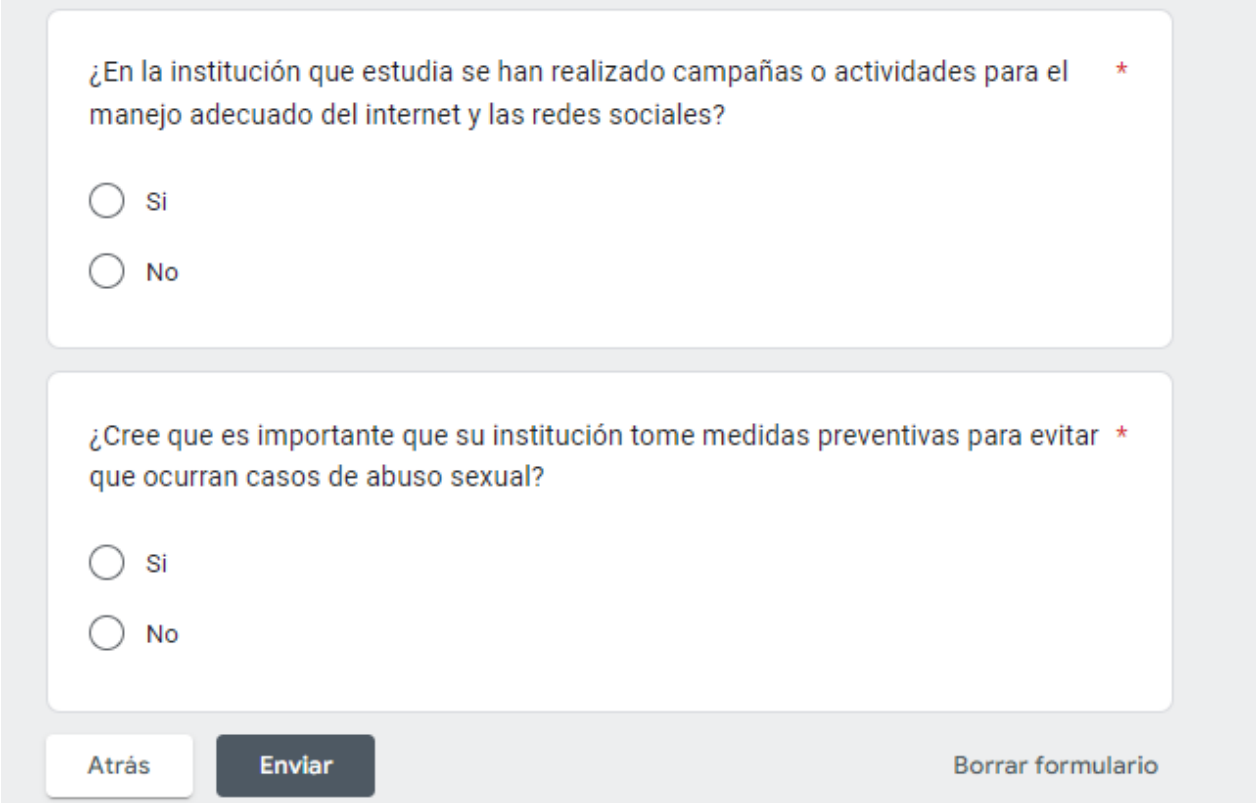
10 Fig. Cuestionario de investigación alumnos (Creación personal 2022) Ilustración (Madera Bojórquez & Armenta, 2020)



11 Fig. Cuestionario de investigación alumnos (Creación personal 2022)



12 Fig. Cuestionario de investigación alumnos (Creación personal 2022)

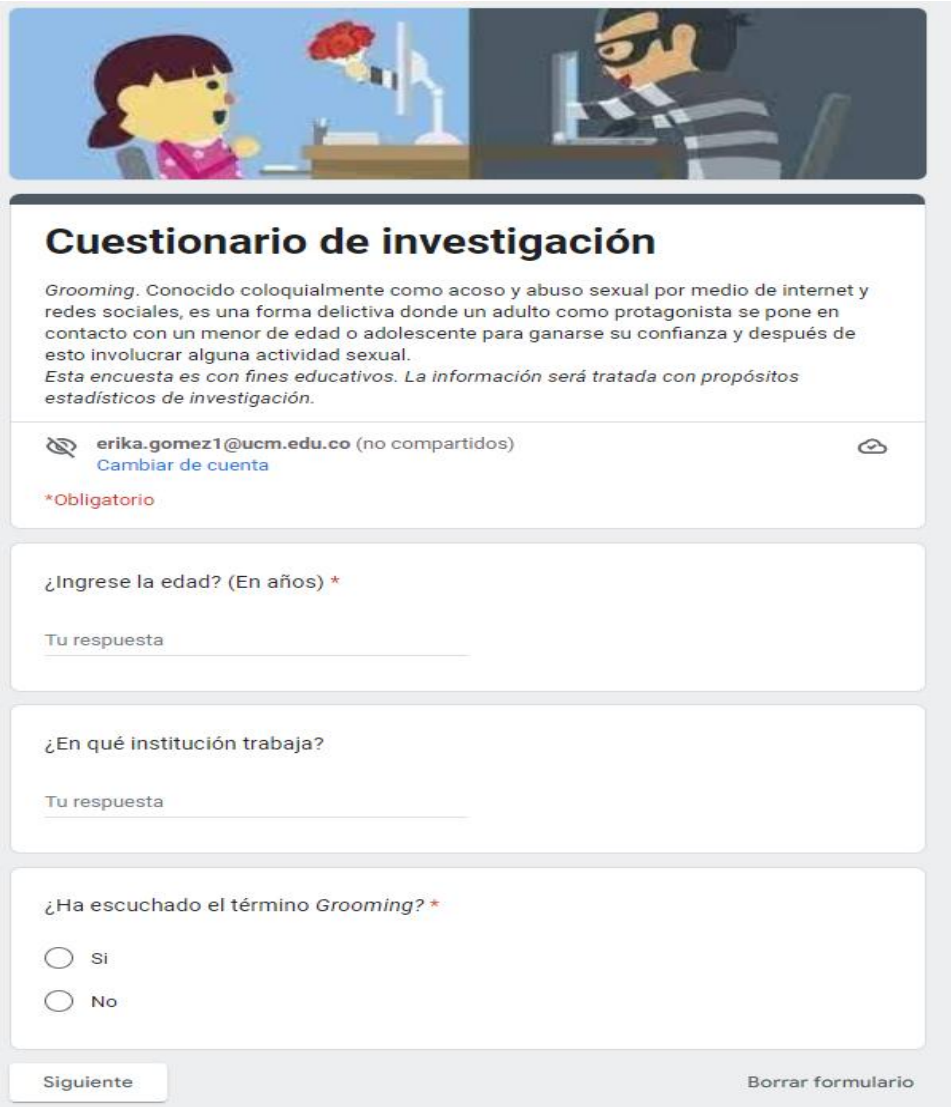


13 Fig. Cuestionario de investigación alumnos (Creación personal 2022)

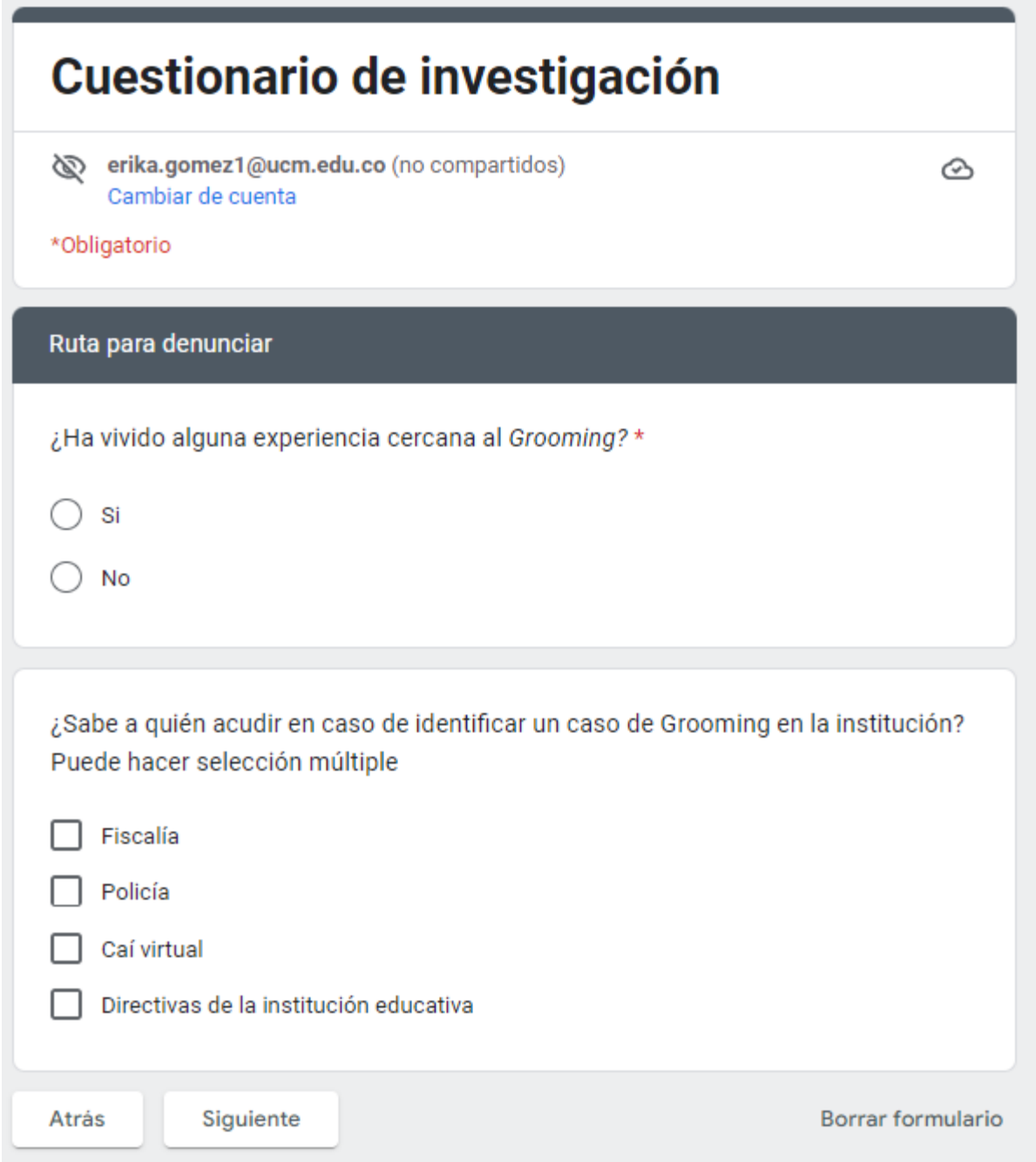
Link del formulario, elaborado en Google forms, herramienta gratuita que brinda el servicio de Google:

https://docs.google.com/forms/d/e/1FAIpQLSf_MhgYTfEy2Z1AIvWKqn3SAPvhAKEZ2j2OavomOd01sKhDnQ/viewform?usp=sf_link

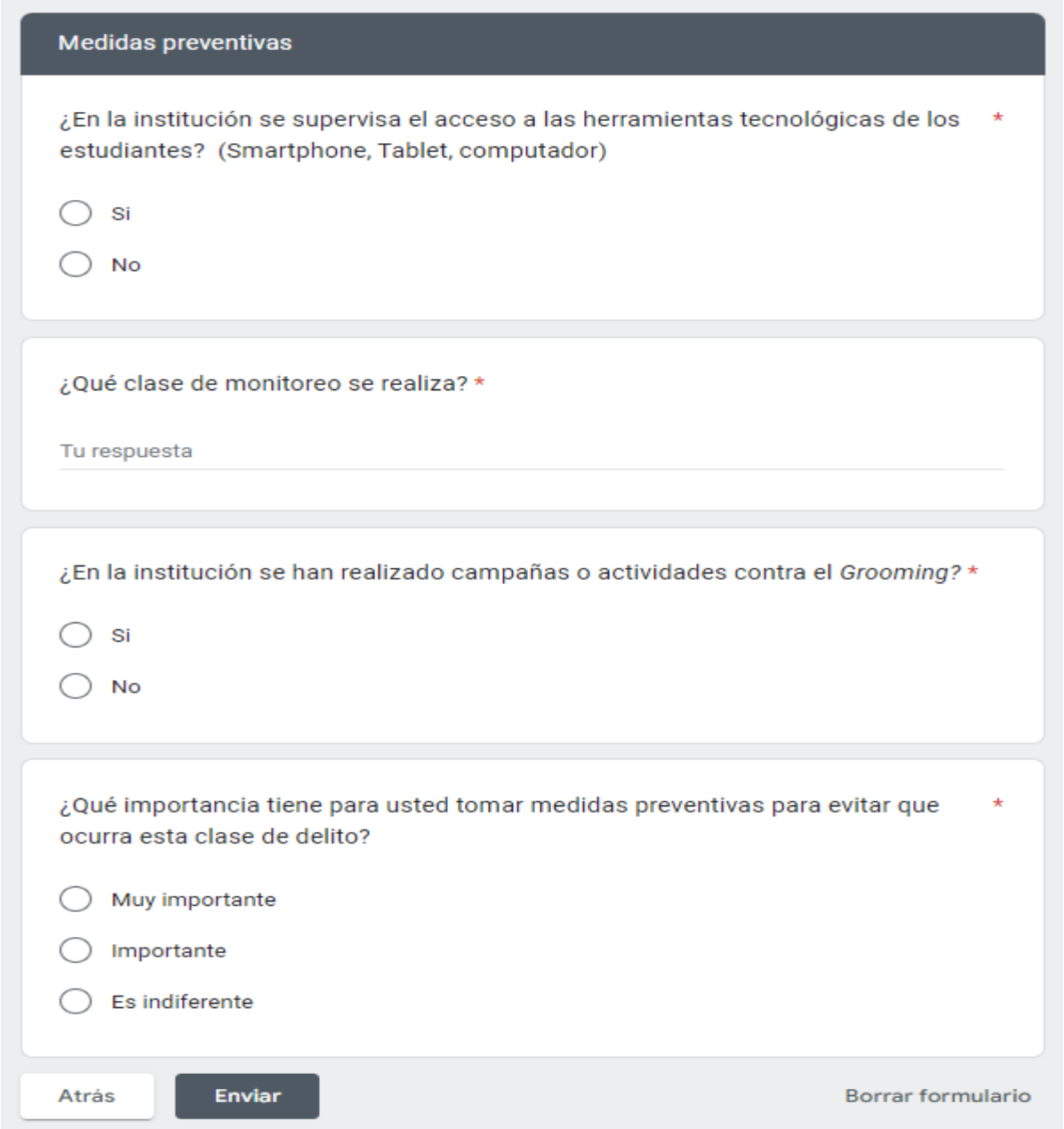
Cuestionario de investigación Profesores



14 Fig. Cuestionario de investigación alumnos (Creación personal 2022) Ilustración (Madera Bojórquez & Armenta, 2020)



15 fig. Cuestionario de investigación alumnos (Creación personal 2022)



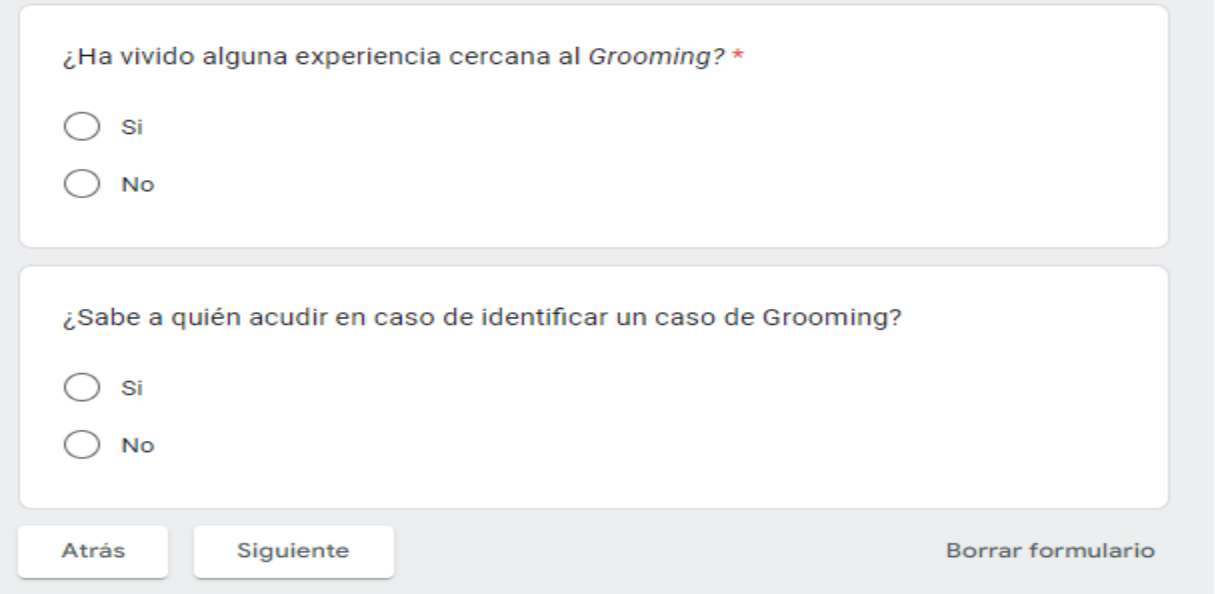
16 Fig. Cuestionario de investigación alumnos (Creación personal 2022)

Link del formulario, elaborado en Google forms, herramienta gratuita que brinda el servicio de Google:

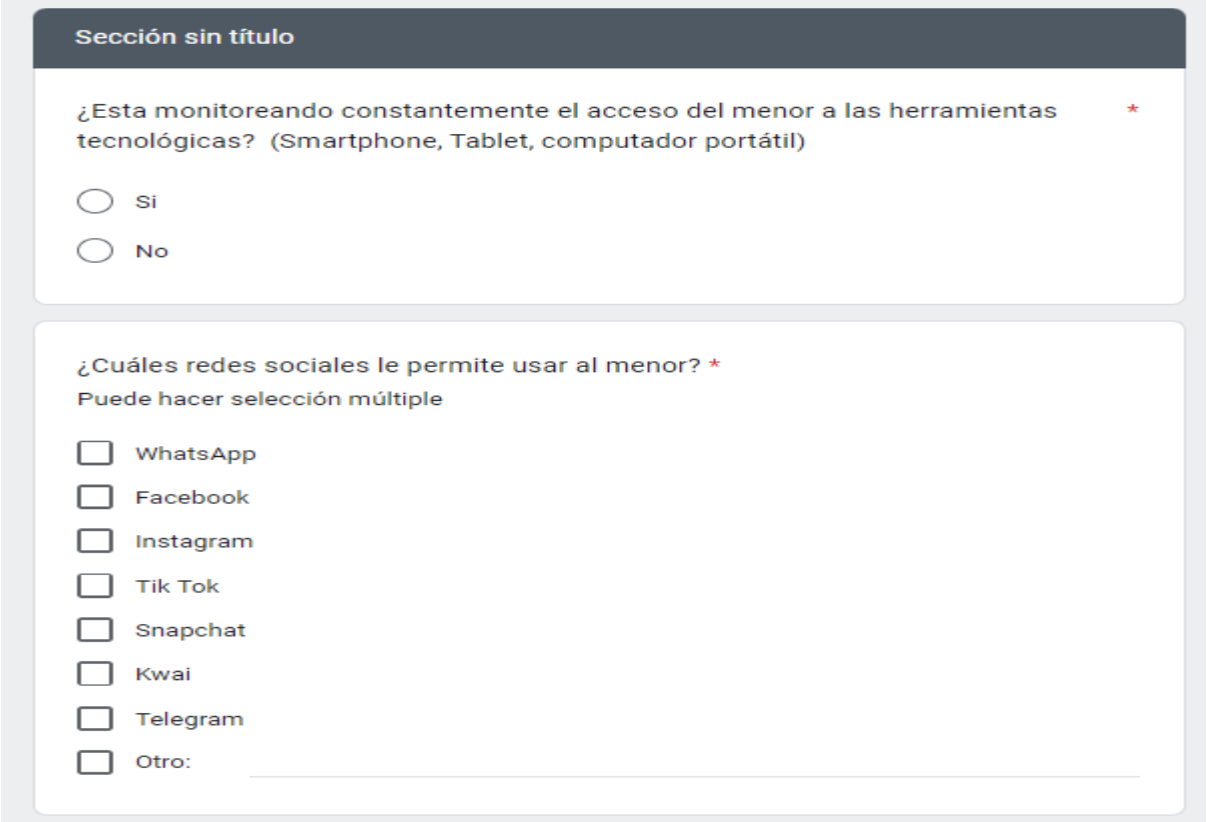
https://docs.google.com/forms/d/e/1FAIpQLSfiDwygxxYgcJyZJr3W88w5-EEyXxc5R2Ef2KzrGWYfLBA_7A/viewform?usp=sf_link

Cuestionario de investigación Familiares

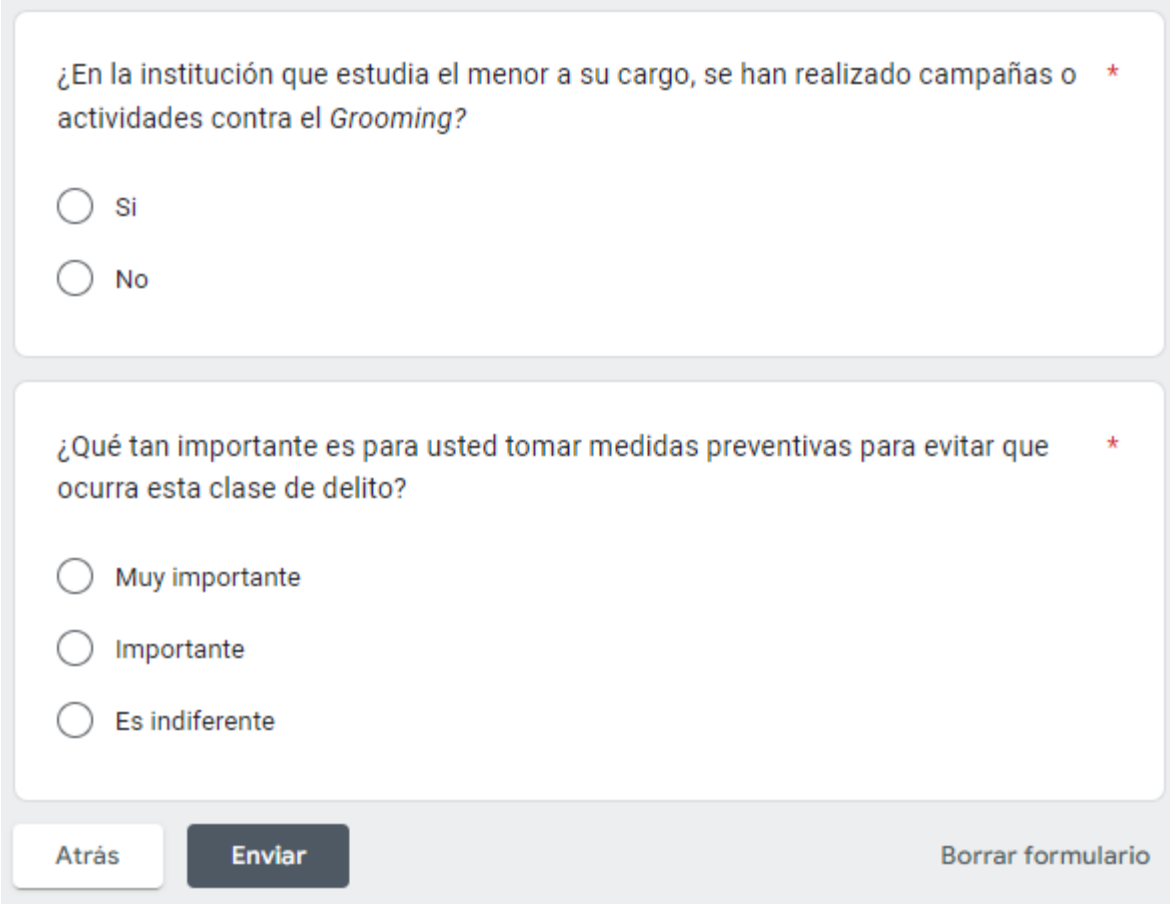
17 *Fig. Cuestionario de investigación alumnos (Creación personal 2022) Ilustración (Madera Bojórquez & Armenta, 2020)*



18 *Fig. Cuestionario de investigación alumnos (Creación personal 2022)*



19 Fig. Cuestionario de investigación alumnos (Creación personal 2022)



20 fig. Cuestionario de investigación alumnos (Creación personal 2022)

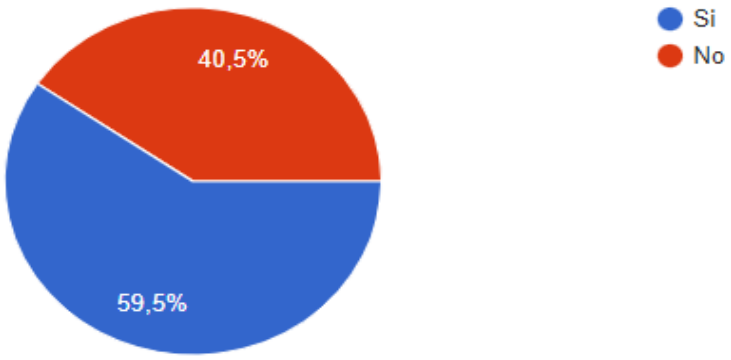
Enlace del formulario, elaborado en Google forms, herramienta gratuita que brinda el servicio de Google:

https://docs.google.com/forms/d/e/1FAIpQLSfsoTj9SNWO-I9cwxW7C7UPf142bWneSTKtxk2sCG-UtzAzvA/viewform?usp=sf_link

8. Análisis de resultados

Encuestas a profesores

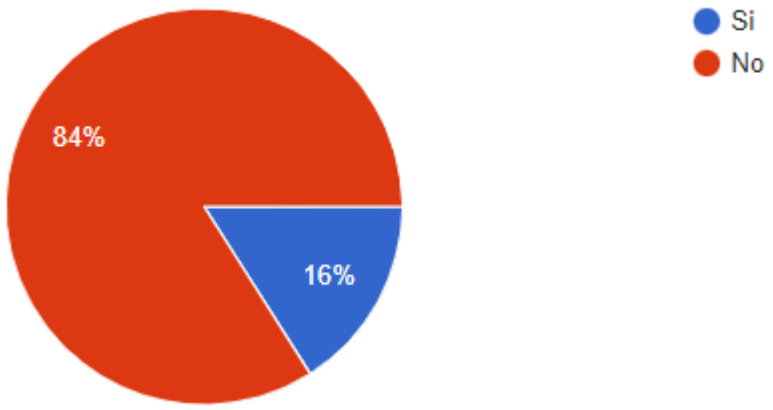
¿Has escuchado el término Grooming?



21 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 42 docentes, de los cuales el 40.5% respondió que no y el 59.5% respondió que sí; es decir que la mayoría de los docentes encuestados ha escuchado el término Grooming.

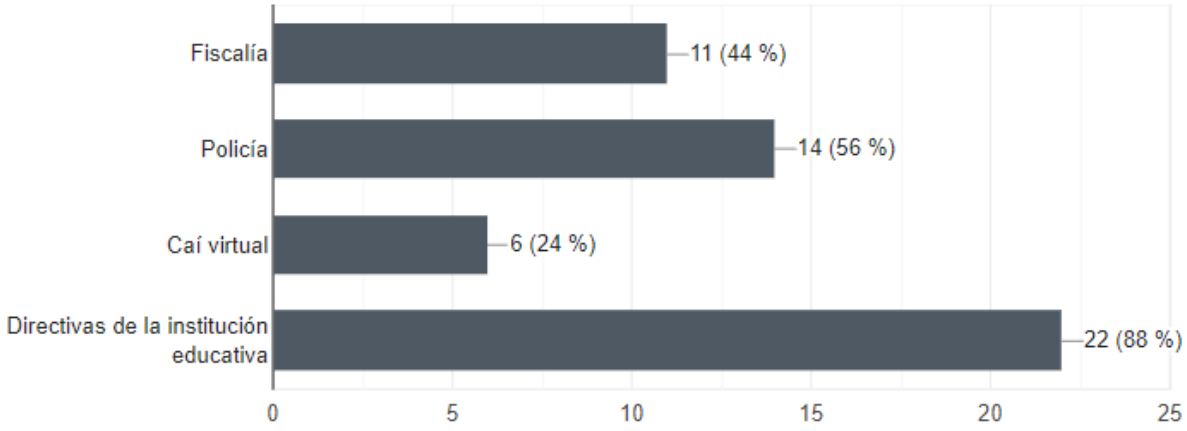
¿Ha vivido alguna experiencia cercana al Grooming?



22 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 25 docentes, de los cuales el 84% respondió que no y el 16% respondió que sí; es decir que la mayoría de los docentes encuestados no han vivido ninguna experiencia cercana al Grooming.

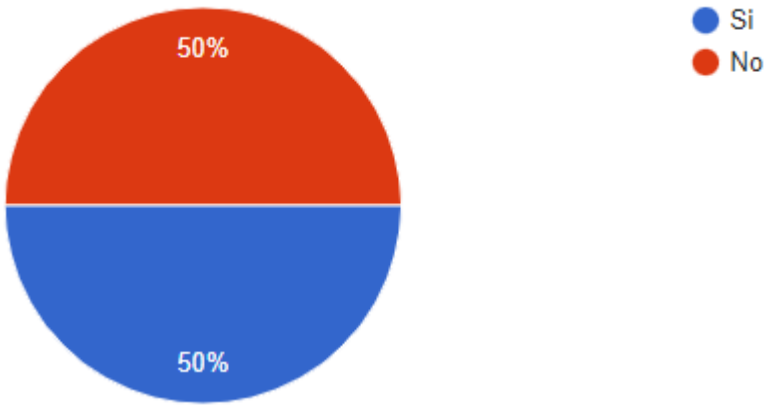
¿A qué institución acudiría en caso de identificar un caso de Grooming en la institución?



23 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 25 docentes, el 88% acudiría a las directivas de institución educativa, el 56% acudiría a la Policía, el 44% acudiría a la Fiscalía y el 24% acudiría al CAI Virtual; es decir que la mayoría de los docentes acudiría a las directivas de la institución educativa.

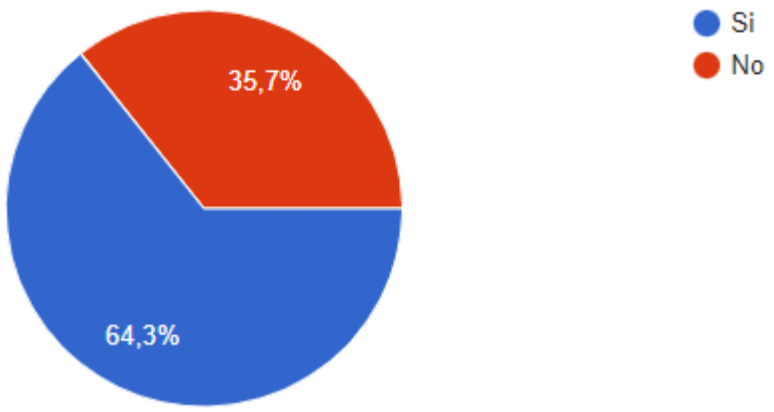
¿En la institución se supervisa el acceso a las herramientas tecnológicas de los estudiantes? (Smartphone, Tablet, computador)



24 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 42 docentes, de los cuales el 50% respondió que no y el 50% restante que sí; es decir que las instituciones deben aumentar la supervisión del acceso a las herramientas tecnológicas de los estudiantes.

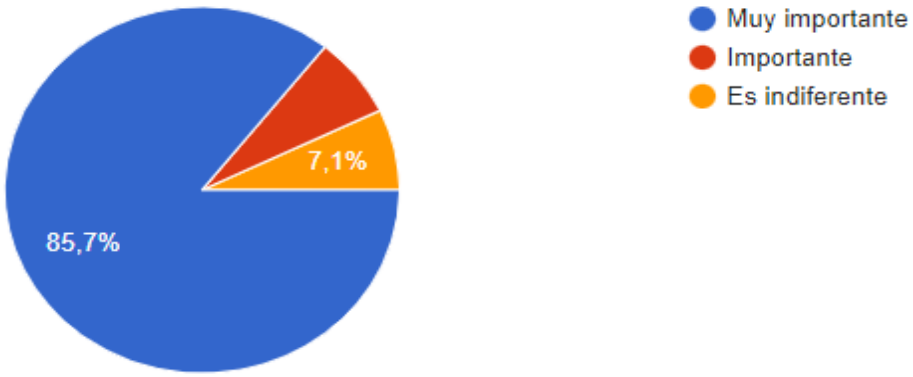
¿En la institución se han realizado campañas o actividades contra el Grooming?



25 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 42 docentes, de los cuales el 64.3% respondió que sí y el 35,7% respondió que no; es decir que en la mayoría de las instituciones han realizado campañas o actividades contra el Grooming.

¿Qué importancia tiene para usted tomar medidas preventivas para evitar que ocurra esta clase de delito?

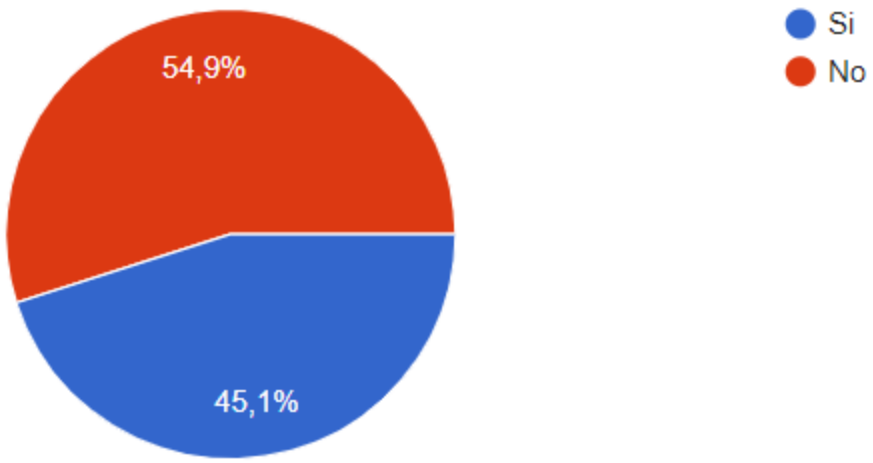


26 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 42 docentes, de los cuales el 85,7% respondió que muy importante, el 7,2% respondió que es importante y el 7,1% restante que es indiferente; es decir que para la mayoría de los docentes es muy importante tomar medidas preventivas para evitar que ocurra esta clase de delito.

Encuestas a familiares

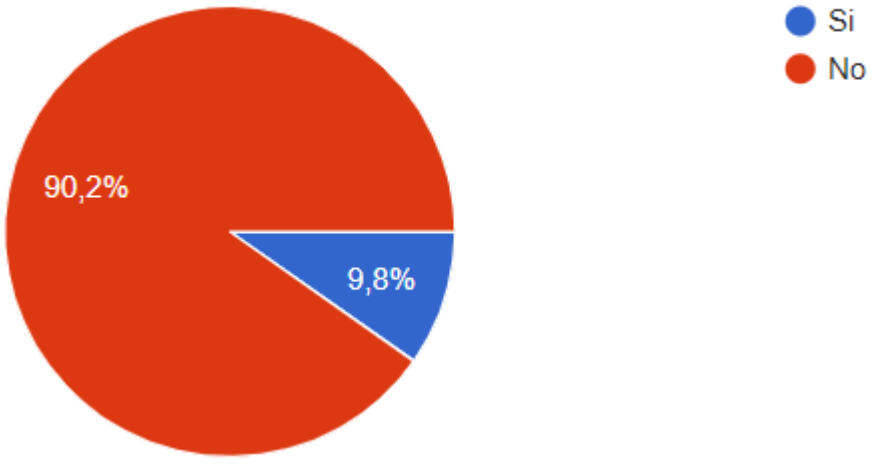
¿Anteriormente ha escuchado el término Grooming?



27 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 91 familiares, de los cuales el 54,9% respondió que no y el 45,1% restante que sí; es decir que la mayoría de los familiares no conocen el término Grooming.

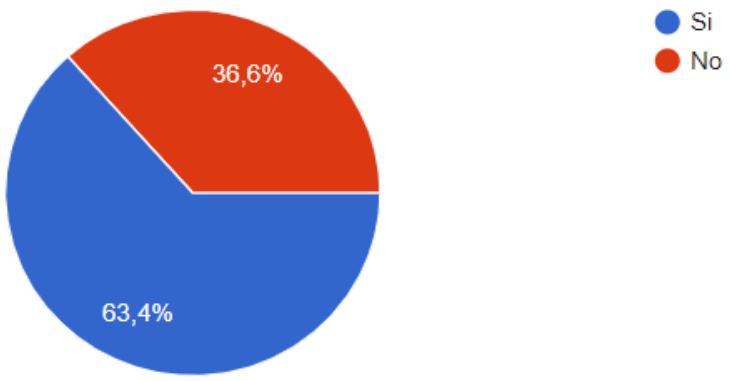
¿Ha vivido alguna experiencia cercana al Grooming?



28 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 41 familiares, de los cuales el 90,2% respondió que no y el 9,8% restante que sí; es decir que la mayoría de los familiares no han tenido una experiencia cercana con el Grooming.

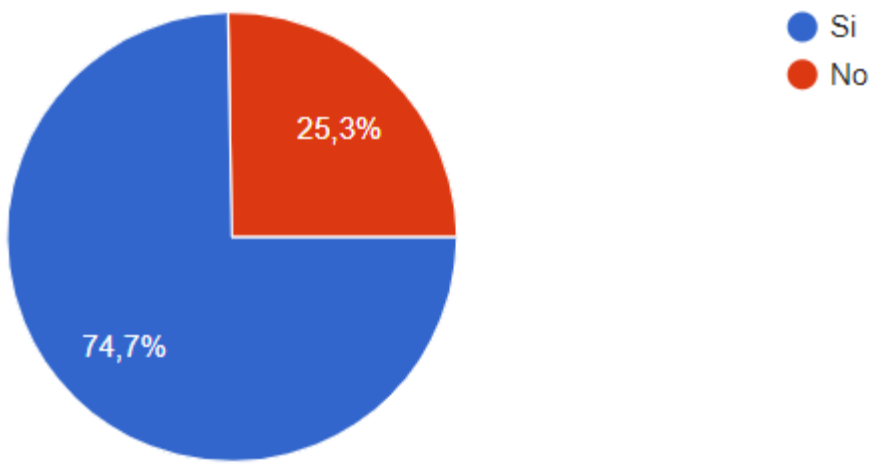
¿Sabe a quién acudir en caso de identificar un caso de Grooming?



29 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 41 familiares, de los cuales el 36,6% respondió que no y el 63,4% restante que sí; es decir que la mayoría de los familiares saben a quién acudir en caso de presentarse una situación de Grooming.

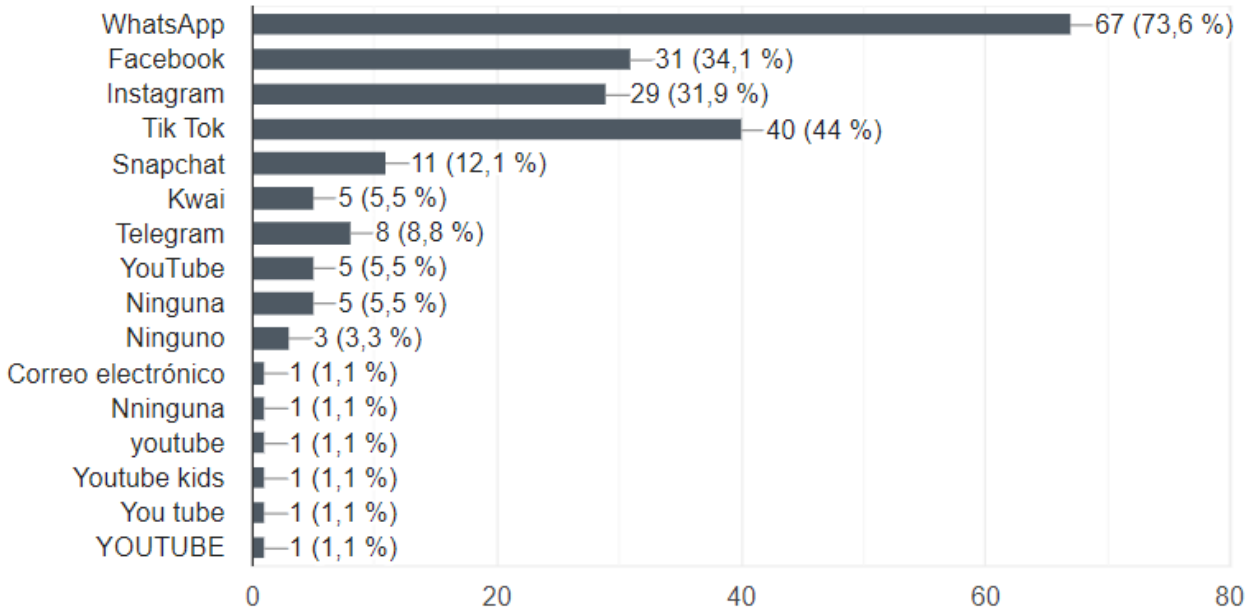
¿Está monitoreando constantemente el acceso del menor a las herramientas tecnológicas? (Smartphone, Tablet, computador portátil)



30 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 91 familiares, de los cuales el 74,7% respondió que sí y el 25,3% restante que no; es decir que la mayoría de los familiares monitorean el acceso de los niños a las herramientas tecnológicas.

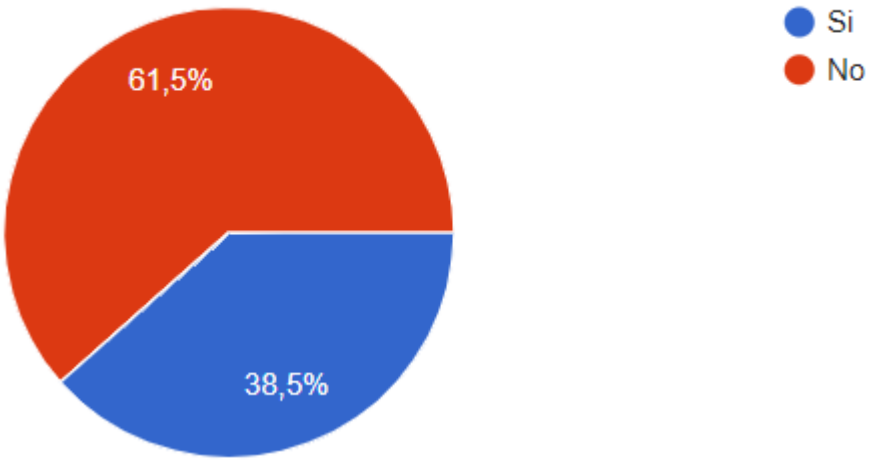
¿Cuáles redes sociales le permite usar al menor?



31 fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 91 familiares, donde los datos más representativos corresponden a lo siguiente: el 73,6% permite el uso de WhatsApp, el 44% permite el uso de Tik Tok, el 34,1% permite el uso de Facebook, el 31,9% permite el uso de Instagram y, el 12,1% permite el uso de Snapchat y el 8,8% permite el uso de Telegram; de acuerdo con este resultado, las 4 redes sociales que más permiten usar los padres de familia al menor son WhatsApp, Tik Tok, Facebook e Instagram.

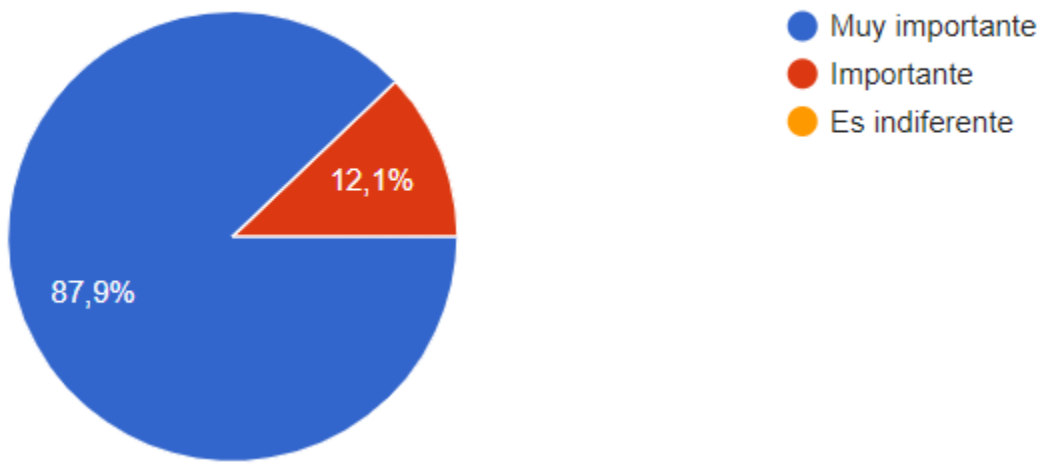
¿En la institución que estudia el menor a su cargo, se han realizado campañas o actividades contra el Grooming?



32 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 91 familiares, de los cuales el 61,5% respondió que no y el 38,5% restante que sí; es decir que la mayoría de los familiares indican que la institución educativa no ha realizado campañas o actividades contra el Grooming.

¿Qué tan importante es para usted tomar medidas preventivas para evitar que ocurra esta clase de delito?

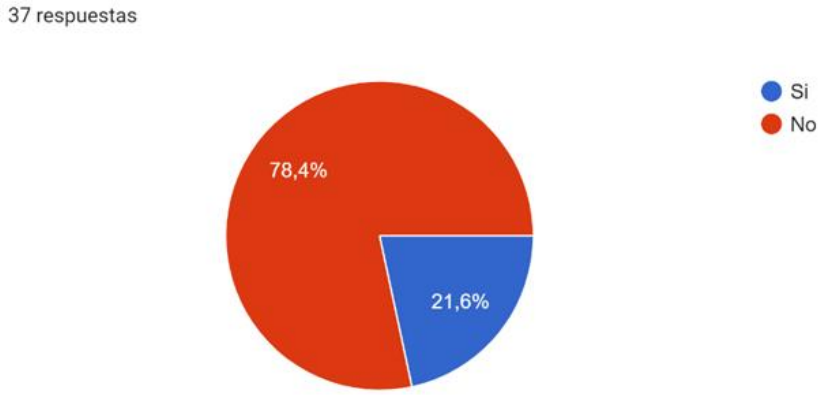


33 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 91 familiares, de los cuales el 87,9% respondió que muy importante y el 12,1% respondió que es importante; es decir que para la mayoría de los familiares es muy importante tomar medidas preventivas para evitar que ocurra esta clase de delito.

Encuestas a estudiantes:

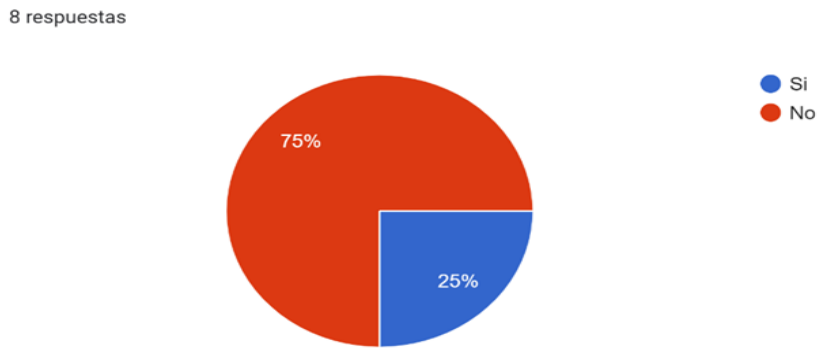
¿Sabe que es el *Grooming* o ha escuchado esta palabra?



***34** Fig. Cuestionario de investigación profesores (Creación personal 2022)*

La pregunta fue respondida por 37 alumnos, de los cuales el 78.4% respondieron que no y el 21.6% responde que sí; es decir que la mayoría de los alumnos encuestados no conocen el término Grooming **0**

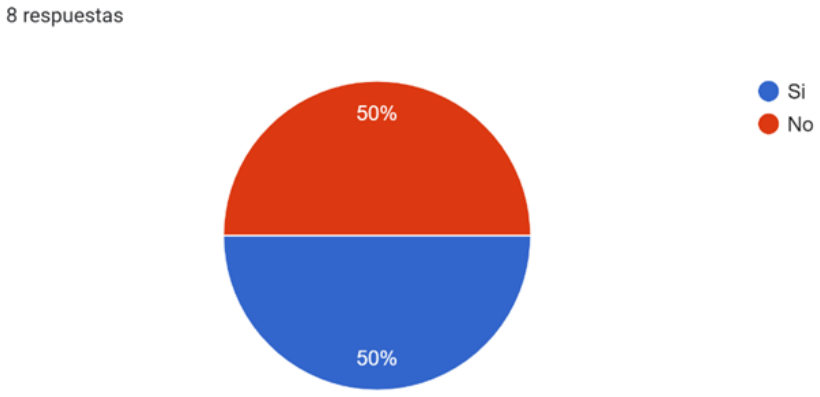
¿Ha sido víctima o conoce una situación donde alguien haya sido víctima de *Grooming*?



35 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 8 alumnos, de los cuales el 75% respondieron que no, mientras que el 25% respondió que sí, es decir que la mayoría de los encuestados no han sido víctimas o no conocen alguna víctima de Grooming.

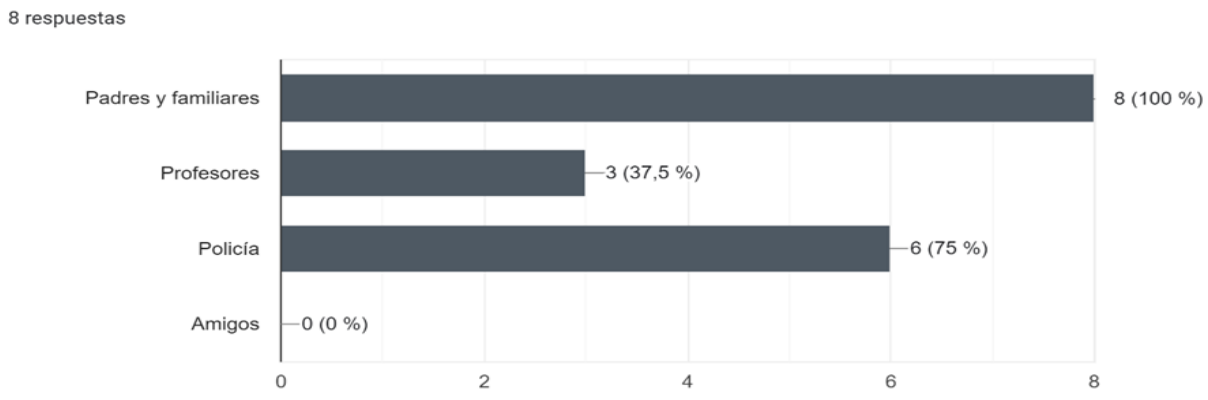
¿Sabe cómo denunciar casos de Grooming?



36 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 8 alumnos, de los cuales el 50% respondieron que sí, mientras el 50% restante respondieron que no.

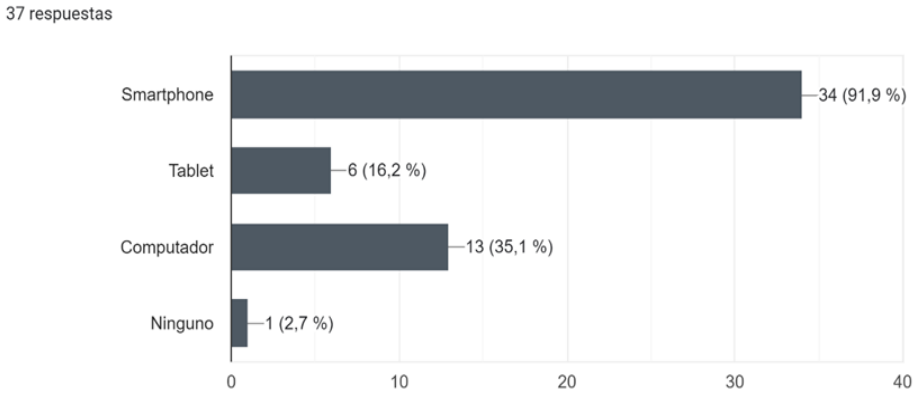
¿A quién acudiría si se presenta un caso de Grooming?



37 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 8 estudiantes de los cuales el 100% acudirían a padres y familiares, el 37,5% acudirían a profesores, el 75% acudirían a la policía y el 0% acudirían a los amigos.

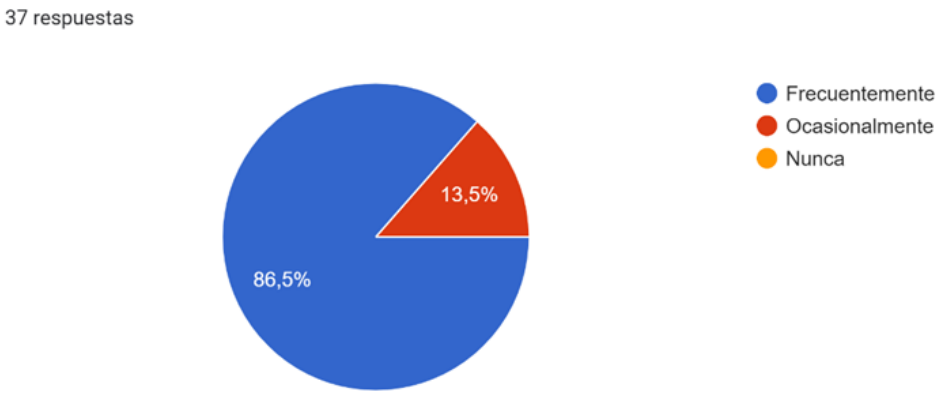
Seleccione el dispositivo tecnológico que usa.



38 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 37 alumnos, el 91,9% usan Smartphone, el 35,1% utilizan computador, el 16,2% usan Tablet y el 2,7% ninguno. El dispositivo más usado fue el Smartphone.

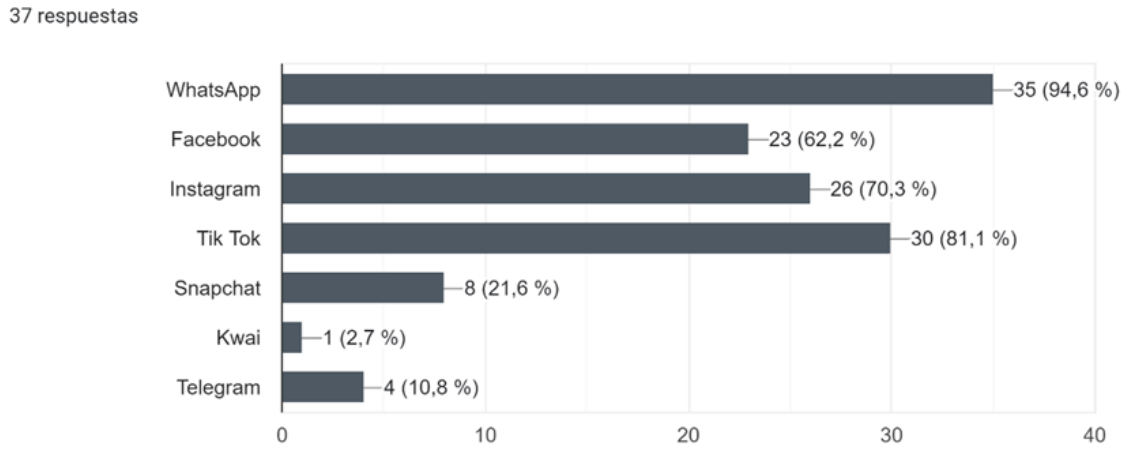
¿Con qué frecuencia hace uso de estas herramientas tecnológicas?



39 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 37 alumnos, de los cuales, el 86,5% usa frecuentemente las herramientas tecnológicas, el 13,5% ocasionalmente.

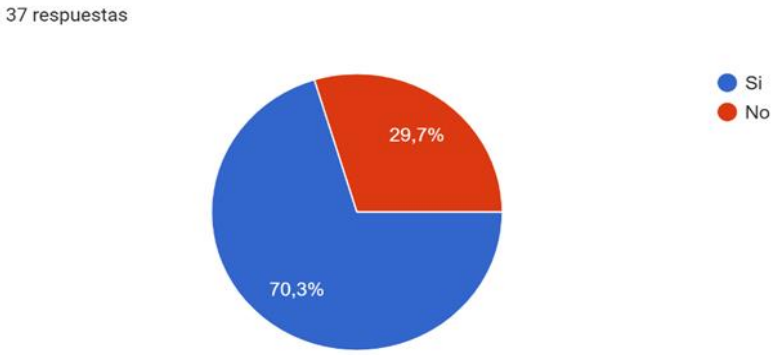
¿Qué redes sociales usa?



40 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 37 alumnos de los cuales el 94,6% usan WhatsApp, el 81,1% usan Tik Tok, el 70,3% usan Instagram, el 62,2% usan Facebook, el 21,6% usan Snapchat, el 10,8% usan Telegram y el 2,7% usan Kwai. WhatsApp, Tik Tok, Instagram y Facebook son las más usadas por los alumnos.

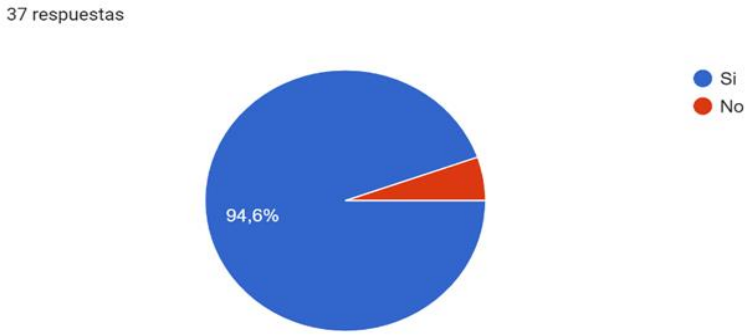
¿En la institución que estudia se han realizado campañas o actividades para el manejo adecuado del internet y las redes sociales?



41 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 37 alumnos, con un 70,3% los alumnos votaron que sí, mientras que el 29,7% votaron que no; es decir que la mayoría de las instituciones realizan campañas o actividades para el manejo adecuado del internet y las redes sociales

¿Cree que es importante que su institución tome medidas preventivas para evitar que ocurran casos de abuso sexual?



42 Fig. Cuestionario de investigación profesores (Creación personal 2022)

La pregunta fue respondida por 37 alumnos, el 94,6% votaron que sí, mientras el 5,4% votaron que no; es decir que la gran mayoría creen que es importante tomar medidas preventivas para evitar casos de abuso sexual.

9. Conclusiones

La falta de conocimiento sobre el grooming y los riesgos asociados a este en la ciudad de Manizales y sus alrededores, evidenciados por los resultados de las encuestas, subrayan la importancia de implementar medidas preventivas efectivas para proteger a los NNA. La guía práctica elaborada puede ser una herramienta útil para tal fin.

La identificación de los factores de riesgo del grooming, como el uso de los smartphones y las redes sociales más populares en la ciudad de Manizales y sus alrededores, es un paso importante en la prevención de este fenómeno. Las medidas preventivas deben tener en cuenta estos factores.

La revisión detallada de las configuraciones de privacidad y seguridad de las redes sociales más utilizadas por los NNA en la ciudad de Manizales y sus alrededores es un trabajo importante para establecer las mejores prácticas de ciberprotección y prevención del grooming. La guía práctica debe ser un recurso útil para ayudar a los padres y tutores a implementar estas configuraciones.

La guía práctica elaborada para prevenir y mitigar el riesgo de grooming en las redes sociales utilizadas por los NNA es una herramienta valiosa para fomentar la seguridad en línea y prevenir situaciones de vulnerabilidad. Es importante que se difunda ampliamente y se utilice en las instituciones educativas y en los hogares.

La concienciación de los preadolescentes, padres y tutores sobre la importancia de aplicar las configuraciones de privacidad y seguridad propuestas en cada una de las redes sociales, especialmente las que tienen que ver con la revelación de información personal y las restricciones

de configuración para evitar que los NNA sean contactados por personas desconocidas, es esencial para proteger a los NNA y prevenir situaciones de grooming.

10. Referencias bibliográficas

Aranzales Delgado, Y. D., Castaño Castrillón, J. J., Figueroa Salcedo, R. A., & Jaramillo Ruiz, S. (Junio de 2014). *Frecuencia de acoso y ciber-acoso, y sus formas de presentación en estudiantes de secundaria de colegios públicos de la ciudad de Manizales, 2013.* Obtenido de researchgate: https://www.researchgate.net/publication/333071867_Frecuencia_de_acoso_y_ciber-acoso_y_sus_formas_de_presentacion_en_estudiantes_de_secundaria_de_colegios_publicos_de_la_ciudad_de_Manizales_2013_Frequency_of_bullying_and_cyberbullying_and_its_ways_of_

Arévalo Moreno, B. Y., Martínez Corredor, Y. A., & Calderón Rodríguez, W. (18 de Junio de 2021). *Campañas de promoción y prevención del grooming en instituciones educativas aplicadas.* Obtenido de Repositorio unilibre: https://repository.unilibre.edu.co/bitstream/handle/10901/19596/Trabajo%20de%20grado.pdf?sequence=2&isAllowed=y

Becerra, B. X. (Sábado de Diciembre de 2021). *Consumo de internet en el mundo aumentó 19,5% durante la pandemia de covid-19.* Obtenido de larepublica.co: https://www.larepublica.co/consumo/consumo-de-internet-en-el-mundo-aumento-195-durante-la-pandemia-de-covid-19-3274945

COLEGIO NUESTRA SEÑORA DEL HUERTO. (11 de Noviembre de 2018). *Concientización y prevención sobre el Grooming a padres Fotografia*. Obtenido de eltribuno: https://us.cdn.eltribuno.com/112018/1541897239569.jpg?&cw=960

Data Protected. (s.f.). *FAQ Protección de Datos.* Obtenido de Log Tec Consulting Group: https://www.dataprotected.com.co/faq-proteccion-datos

Fiscalia General de la Nación, Selección Caldas. (2021). *Denuncia de ciberacoso a menor de edad.* Riosucio Caldas: Caso real Casa de Justicia Riosucio.

Forjando Ciberseguridad . (24 de Enero de 2021). *Ley 1260 de cyberbullying (ciberacoso) en Colombia.* Obtenido de Fundación Forjando Ciberseguridad : https://forjandociberseguridad.org/blog-cyberbullying-ley-1260/

Forjando Ciberseguridad . (24 de Enero de 2021). *Ley 1260 de cyberbullying (ciberacoso) en Colombia.* Obtenido de Fundación Forjando Ciberseguridad : https://forjandociberseguridad.org/wp-content/uploads/2018/04/Imagen-modulo-3-1536x901.jpg

Goodwill Community Foundation, Inc. (s.f.). *¿Qué es el control parental?* Obtenido de GCF Aprende Libre: https://edu.gcfglobal.org/es/seguridad-en-internet/test-seguridad-en-internet-/1/

Hootsuite. (02 de 2021). *Social Media Use Fotografia*. Obtenido de Digital 2021 Colombia (January 2021) v01: https://marketing4ecommerce.co/wp-content/uploads/2021/02/Usuarios-de-redes-sociales.jpg

Hootsuite. (02 de 2021). *Social media: advertising audience profile Fotografia*. Obtenido de Digital 2021 Colombia (January 2021) v01: https://marketing4ecommerce.co/wp-content/uploads/2021/02/Audiencia-por-edad-redes-sociales.jpg

ICBF. (17 de diciembre de 2019). *Riesgos digitales, ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet?Riesgos digitales, ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet?* Obtenido de https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos

IPcom Sistemas S.A.S. (s.f.). *Internet Sano*. Obtenido de https://ipcomsistemas.files.wordpress.com/2017/11/internet_sano_big_thumb-1.gif?w=240&zoom=2

Juan, I. M., Vayá, E. J., & García, M. S. (s.f.). VICTIMIZACIÓN INFANTIL SEXUAL ONLINE: ONLINE GROOMING CIBERABUSO Y CIBERACOSO SEXUAL. *VICTIMIZACIÓN INFANTIL SEXUAL ONLINE: ONLINE GROOMING CIBERABUSO Y CIBERACOSO SEXUAL*, 23.

Lopez & Lopez Abogados. (s.f.). *Protección de datos en Colombia.* Obtenido de https://lopezmoralesabogados.com/wp-content/uploads/2019/12/proteccion-de-datos-en-colombia.jpg

Madera Bojórquez, R., & Armenta, J. D. (28 de abril de 2020). *Grooming: Peligro en las redes Fotografía*. Obtenido de www.senda.edu: https://www.senda.edu.mx/wp-content/uploads/2020/04/grooming.jpg

MinTIC Colombia. (10 de abril de 2012). *"Internet Sano", una estrategia para proteger la identidad de niños y jóvenes en la red*. Obtenido de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/720:Internet-Sano-una-estrategia-para-proteger-la-identidad-de-ninos-y-jovenes-en-la-red

MinTIC Colombia. (10 de abril de 2012). *"Internet Sano", una estrategia para proteger la identidad de niños y jóvenes en la red.* Obtenido de MinTIC: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/720:Internet-Sano-una-estrategia-para-proteger-la-identidad-de-ninos-y-jovenes-en-la-red

nesterenko.ruslan. (s.f.). *Vecteezy*. Obtenido de https://es.vecteezy.com/arte-vectorial/2580126-icono-de-color-rgb-de-control-parental

Save the Children. (1 de Julio de 2019). *Grooming que és. Y cómo detectarlo y prevenirlo.* Obtenido de: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Siete estrellas. (30 de abril de 2021). *Ciberbullying: ¿Qué es y cómo prevenirlo? Fotografia*. Obtenido de Siete Estrellas: https://siete-estrellas.com/wp-content/uploads/elementor/thumbs/cyberbullyng-1170x620-1-p6t8wewfx32we8mbi645buciupso2qyotbujfqadh2.png

UIT. (Diciembre de 2021). *consumo internet fotografía*. Obtenido de larepublica.co: https://img.lalr.co/cms/2021/12/10163849/consumo_internet_p13_sabado.jpg

Función pública - Gestor normativo. (3 de agosto de 2001). *Ley 679 de 2001*. Obtenido de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=18309

ICBF. (21 de julio de 2009). *Ley 1336 de 2009.* Obtenido de: https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

AO Kaspersky Lab. (s.f.). *¿Qué es una huella digital? ¿Cómo podemos protegerla de los hackers?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

Fundación MAPFRE. (s.f.). *Ciberdelincuente*. Obtenido de https://segurosypensionesparatodos.fundacionmapfre.org/glosario/ciberdelincuente/

PantallasAmigas. (2020). *¿Es lo mismo un pederasta que un pedófilo?* Obtenido de https://internet-grooming.net/es-lo-mismo-un-pederasta-que-un-pedofilo/

¿Qué es la ingeniería social? (s.f.). Obtenido de https://www.ibm.com/es-es/topics/social-engineering#:~:text=IBM%20Iniciar%20sesi%C3%B3n-,%C2%BFQu%C3%A9%20es%20la%20ingenier%C3%ADa%20social%3F,la%20seguridad%20personal%20o%20empresarial

1996-2023, A. (s.f.). *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía*. Obtenido de https://www.ohchr.org/es/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

Argentina.gob.ar. (Diciembre de 2022). *¿Qué es el ciberdelito?* Obtenido de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

Ciberseguridad, i. I. (s.f.). *Phishing*. Obtenido de https://www.incibe.es/aprendeciberseguridad/phishing

DÍAZ, C. (26 de Octubre de 2018). *Grooming o cómo aprovecharse de la inocencia de un menor a través de Internet*. Obtenido de https://www.lavanguardia.com/vida/20181026/452537130930/grooming-como-aprovecharse-inocencia-menor-traves-internet.html

Enciclopedia Humanidades. (s.f.). *¿Qué es Internet?* Obtenido de https://humanidades.com/internet/#ixzz7wcZOEuk8

FERNÁNDEZ-PANIAGUA, A. M. (26 de Octubre de 2022). *Las Redes Sociales más utilizadas: cifras y estadísticas*. Obtenido de https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/

Gaptain. (s.f.). *PEDERASTAS online Y PEDÓFILOS: Depredadores sexuales online* . Obtenido de https://gaptain.com/evitar-pederastas-pedofilos-internet/

GCF Global . (s.f.). *¿Qué es el control parental?* Obtenido de https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-control-parental/1/

Grooming: qué es, qué riesgos tiene y cómo pueden prevenirlo los padres. (30 de 06 de 2022). Obtenido de https://www.telefonica.com/es/sala-comunicacion/blog/grooming-que-es-que-riesgos-tiene-y-como-pueden-prevenirlo-los-padres/

Heraldo.es. (07 de 2023 de Marzo). *¿Qué es un 'groomer'?* . Obtenido de https://www.heraldo.es/noticias/nacional/2017/11/14/que-groomer-1207966-305.html

IntraMed. (02 de Noviembre de 2018). *¿Qué es el sexting?* Obtenido de https://www.intramed.net/contenidover.asp?contenidoid=93210

MacAfee. (03 de Junio de 2021). *¿Qué es la identidad digital y todo lo que puedes hacer para protegerla?* Obtenido de https://www.mcafee.com/blogs/es-es/internet-security/que-es-la-identidad-digital-y-todo-lo-que-puedes-hacer-para-protegerla/

Mimeza, O. C. (02 de Febrero de 2017). *Diferencias entre pedofilia y pederastia*. Obtenido de https://psicologiaymente.com/clinica/diferencias-pedofilia-pederastia

Nava, J. A. (10 de Mayo de 2022). *Cómo actúan y cuál es el perfil de los pedófilos que seducen a niños en internet*. Obtenido de https://www.infobae.com/america/tecno/2022/05/10/como-actuan-y-cual-es-el-perfil-de-los-pedofilos-que-enganchan-a-ninos-en-internet/

OEA. (s.f.). *Pornografía Infantil (ICCS 030221)*. Obtenido de http://www.oas.org/ios/glossarydetails.aspx?lang=es&type=0&id=72

Pinilla, A. R. (2016 de Septiembre de 15). *Colnodo Uso estrategico de internet para el desarrollo*. Obtenido de Seguridad digital: tan importante como la seguridad en el hogar o en la calle: https://www.colnodo.apc.org/es/opiniones/seguridad-digital-tan-importante-como-la-seguridad-en-el-hogar-o-en-la-calle-2

UNICEF. (Febrero de 2023). *Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quieren saber acerca del ciberacoso*. Obtenido de https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Ministerio de Hacienda y Crédito Público. (06 de 2019). *Municipio de Manizales (Caldas)*. Obtenido de https://www.minhacienda.gov.co/webcenter/ShowProperty?nodeId=%2FConexionContent%2FWCC_CLUSTER-129383%2F%2FidcPrimaryFile&revision=latestreleased

Wikipedia. (22 de 03 de 2023). *Manizales*. Obtenido de https://es.wikipedia.org/wiki/Manizales#:~:text=La%20ciudad%20de%20Manizales%2C%20situada,una%20altura%20de%205.321%20msnm

11. Anexos

ANEXO 1 MANUAL DE PREVENCIÓN

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co

GUÍA PARA LA PREVENCIÓN DEL GROOMING EN NIÑOS, NIÑAS Y ADOLESCENTES EN EDADES ENTRE LOS 11 Y 15 AÑOS EN LAS INSTITUCIONES EDUCATIVAS DE LA CIUDAD DE MANIZALES Y SUS ALREDEDORES.

Erika Gómez Tangarife - Juan Manuel Guerrero Ramírez - Jhon Anderson Acevedo Cárdenas - Ovidio Antonio Guerrero Mosquera

erika.gomez1@ucm.edu.co - juan.guerrero2@ucm.edu.co - jhon.acevedo2@ucm.edu.co - ovidio.guerrero@ucm.edu.co

Universidad Católica de Manizales
Especialización en Ciberseguridad
Manizales, Colombia
Año 2023

Autores: Erika Gómez Tangarife; Juan Manuel Guerrero Ramírez; Jhon Anderson Acevedo Cárdenas; Ovidio Antonio Guerrero Mosquera. Fecha de publicación: 2023

TABLA DE CONTENIDO

1 INTRODUCCIÓN

Este manual tiene como propósito principal educar y generar concienciación acerca del uso responsable de las redes sociales por parte de los niños, niñas y adolescentes (NNA), que hacen parte de la comunidad educativa de la ciudad de Manizales y sus municipios vecinos. Adicionalmente, se brindan pautas y herramientas a los padres de familia y profesores para que blinden la navegación y/o permanencia de los NNA en Internet, particularmente en las redes sociales.

El manual está compuesto por tres apartados, en el primero se aborda la configuración de seguridad y privacidad de las cuatro redes sociales más usadas por los NNA, en el segundo se aborda la configuración de cuatro aplicaciones de control parental para la supervisión de los NNA por parte de los padres de familia o acudientes, y por último se abordan las diferentes rutas de denuncia que pueden seguir los padres de familia y/o profesores para denunciar conductas de Grooming.

2 REDES SOCIALES

Las redes sociales son plataformas digitales que conectan entre sí a personas con intereses, actividades o relaciones en común (Como amistad, parentesco o trabajo). Estas plataformas permiten el contacto entre los individuos que las componen y funcionan como un medio para intercambiar información. En este cada usuario crea su perfil e interactúa con otras personas compartiendo información; la información publicada por un usuario puede ser pública o privada.

Existen varios tipos de redes sociales, dentro de las cuales se destacan: redes sociales personales, de entretenimiento, profesionales y de nicho. Este manual se enfoca en las redes sociales personales, las cuales están pensadas para conectar a individuos entre sí basándose en sus conexiones personales.

En las redes sociales personales los individuos pueden crear grupos o comunidades, compartir contenido (información, fotos, videos, historias, ubicaciones, etc.) y también pueden comunicarse de manera directa y privada a través de la función de chat que ofrecen estas. Previo a este manual, se realizó una encuesta a los NNA de instituciones aleatorias en la ciudad de Manizales, dentro de los resultados de esta se destaca que las redes sociales más utilizadas por estos son Facebook, Whatsapp, TikTok e Instagram; y que el dispositivo electrónico más utilizado es el smartphone; en consecuencia, este manual se enfoca en la configuración de seguridad y privacidad de estas cuatro redes sociales en un smartphone.

2.1 Configuración de un perfil de Facebook.

Para realizar una correcta configuración de un perfil de Facebook, ***preservando la seguridad digital y la privacidad***, se sugiere ejecutar los siguientes pasos:

2.1.1 Ingresar al menú de Facebook.

Para acceder al menú desde un dispositivo móvil, seleccione el icono resaltado en el recuadro rojo de la siguiente imagen:

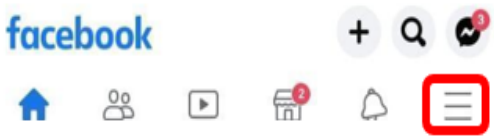


Ilustración 1. Facebook. (2023, 03 de marzo). Menú de configuración [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

2.1.2 Configuración y privacidad.

Seleccione la opción **Configuración y privacidad**, como se muestra en la siguiente imagen, y espere a que se despliegue un nuevo menú:

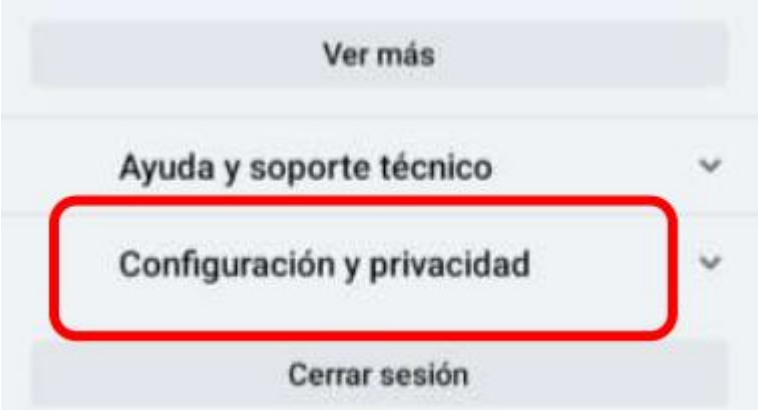


Ilustración 2. Facebook. (2023, 03 de marzo). Menú de configuración [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

En este punto se despliega un nuevo menú, seleccione la opción **Configuración**, como se indica en la imagen:

Ilustración 3. Facebook. (2023, 03 de marzo). Menú de configuración [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

2.1.3 Configuración de la información personal

En el menú que se despliega seleccione la opción **Información personal y de la cuenta**, como se muestra en la imagen:

Ilustración 4. Facebook. (2023, 03 de marzo). Configuración de la cuenta [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

En el menú que se despliega, seleccione la opción **Información de contacto**, resaltada en la imagen:

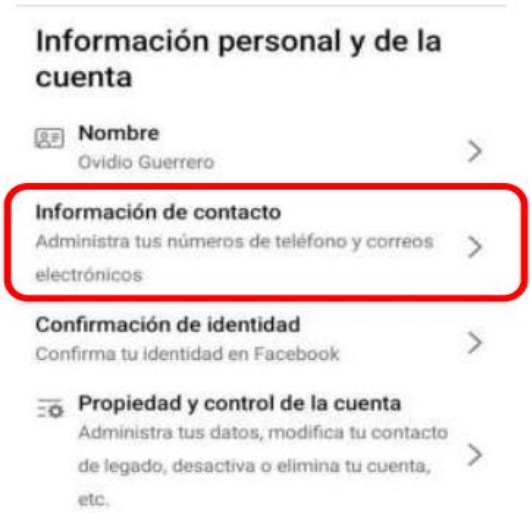


Ilustración 5. Facebook. (2023, 03 de marzo). Configuración de la cuenta [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

En la sección **Administrar información de contacto** valide que en los campos número telefónico y en de la dirección de correo electrónico aparezca la frase **Solo yo**, en caso contrario selecciónela y verifique que quede como se muestra en la imagen:

Ilustración 6. Facebook. (2023, 03 de marzo). Configuración de la cuenta [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

2.1.4 Configuración de las opciones de contraseña y seguridad.

Regrese al menú **Configuración y privacidad**, y estando en este seleccione la opción **Contraseña y seguridad.**

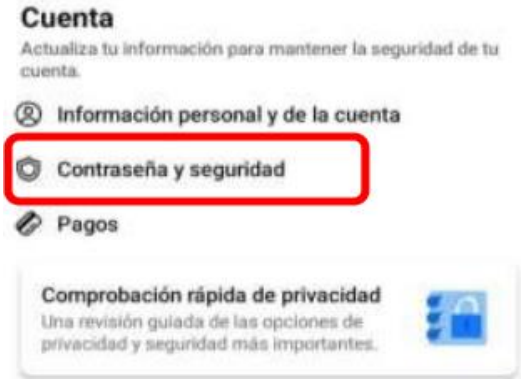


Ilustración 7. Facebook. (2023, 03 de marzo). Configuración de la cuenta [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

En el menú que se despliega, seleccione **Comprobar configuración de seguridad importante:**

Ilustración 8. Facebook. (2023, 03 de marzo). Configuración de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Valide que el resultado de la comprobación muestre el mensaje **No se detectaron problemas** y que las **3 opciones aparezcan verificadas en color verde**, como se muestra en la siguiente imagen:

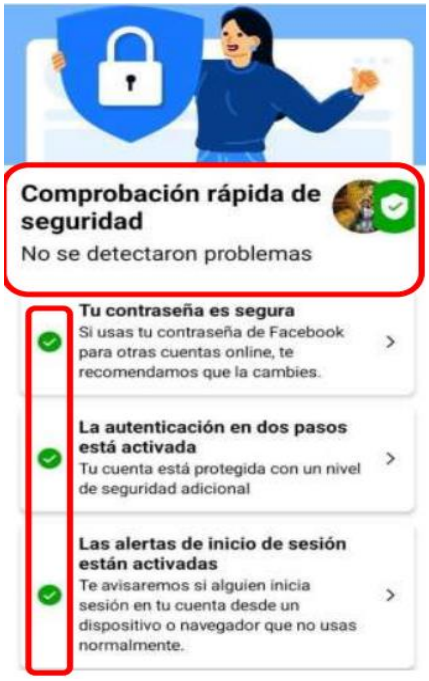


Ilustración 9. Facebook. (2023, 03 de marzo). Comprobación de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Regrese al menú principal de **Contraseña y seguridad**, y en la **sección Autenticación en dos pasos** seleccione la opción **Usar autenticación en dos pasos:**

Ilustración 10. Facebook. (2023, 03 de marzo). Configuración de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Posteriormente, seleccione la opción **App de autenticación:**

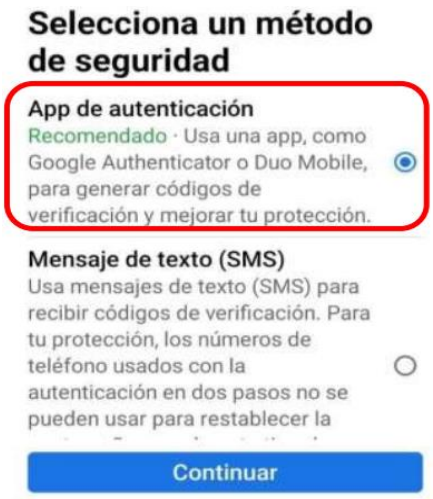


Ilustración 11. Facebook. (2023, 03 de marzo). Configuración de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Nota: antes de ejecutar esta opción, se debe instalar la aplicación **Duo** o **Google Authenticator** en el mismo dispositivo o en un dispositivo distinto si así lo prefiere.

Al seleccionar la opción **App de autenticación**, se abre la siguiente pantalla, en la cual se le dan las indicaciones para aparear la **App de autenticación** con el inicio de sesión de Facebook:

Ilustración 12. Facebook. (2023, 03 de marzo). Configuración de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Después de finalizar el paso anterior, para poder iniciar sesión en Facebook, debe ingresar su contraseña y adicionalmente, debe aprobar el inicio de sesión desde la **App de autenticación** que haya elegido y configurado (Google Authenticator o Duo).

En la sección anterior se sugirieron las configuraciones de seguridad más importantes que debe tener un perfil de Facebook; a partir de aquí se abordarán las configuraciones de privacidad más relevantes, que reducen el riesgo de ser víctima del **Grooming** en esta red social personal**.**

2.1.5 Configuración de las opciones de privacidad

Ubíquese en el menú **Configuración y privacidad**, y desplácese hacia abajo hasta encontrar la sección **Público y visibilidad**, estando en esta, seleccione la opción **Información de perfil**:

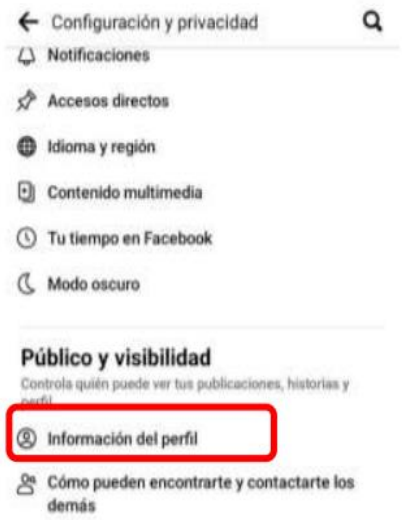


Ilustración 13. Facebook. (2023, 03 de marzo). Configuración de seguridad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Se le recomienda no ingresar información personal en redes sociales, dado que, con esta, le pueden realizar ataques de **Ingeniería social** o **Phishing**; en caso de que alguna información personal sea requerida por Facebook, déjela visible solo para Usted (**Solo yo**):

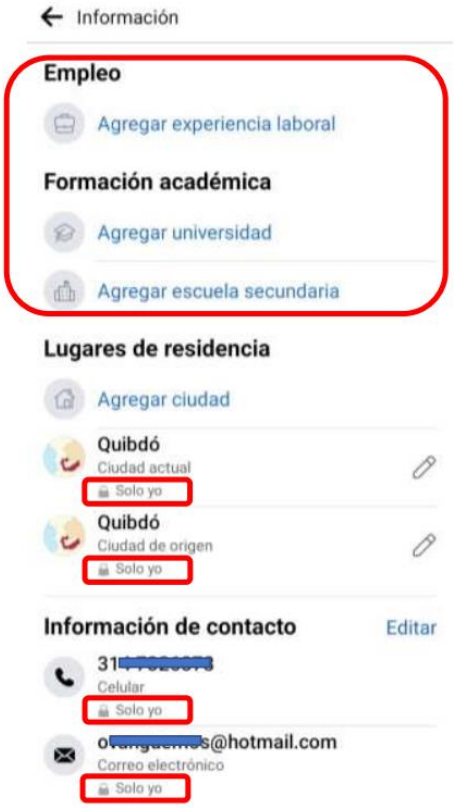


Ilustración 14. Facebook. (2023, 03 de marzo). Configuración de información personal [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

No deje visible su **información personal y de contacto**, eso les facilita el trabajo a los ciberacosadores sexuales y ciberdelincuentes:

Ilustración 15. Facebook. (2023, 03 de marzo). Configuración de información personal [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Se le sugiere **editar** su información de fecha de nacimiento, dejar **visible para sus amigos** la **Fecha de nacimiento** y dejar en modo oculto (**Solo yo)**, el **Año de nacimiento.**

2.1.6 configuración de visibilidad

Regrese a la sección **Público y visibilidad**, y abra la opción **Como pueden encontrarte y contactarte los demás**, se sugiere que la configure así:

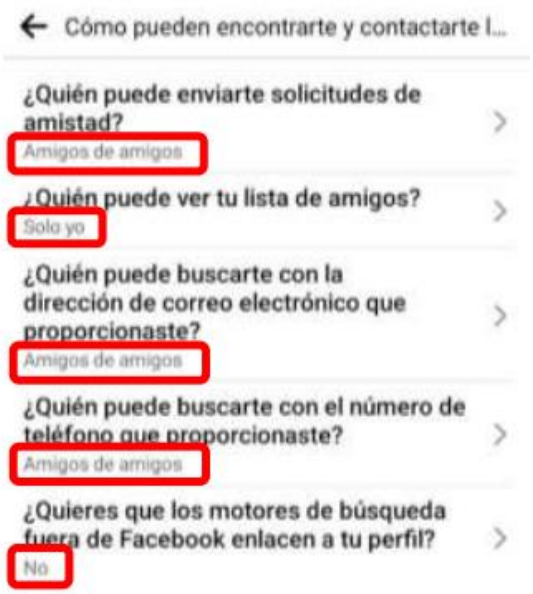


Ilustración 16. Facebook. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

2.1.7 Configuración de publicaciones

Regrese a la sección **Público y visibilidad**, y abra la opción **Publicaciones**, se sugiere que la configure así:

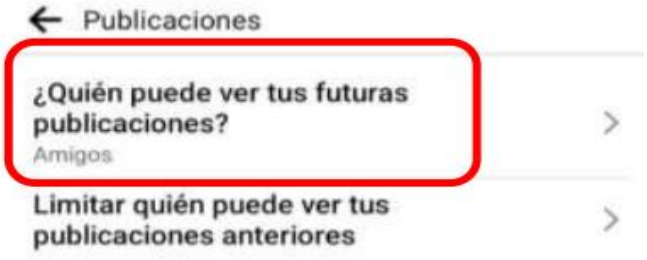


Ilustración 17. Facebook. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Posteriormente, abra la opción **Limitar quién puede ver tus publicaciones anteriores, y seleccione Limitar.**

Regrese a la sección **Público y visibilidad**, y abra la opción **Historias**:

Ilustración 18. Facebook. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

En la opción de Privacidad de la historia, seleccionar amigos y deshabilitar la opción Compartir siempre en Instagram.

Finalmente, regrese a la sección **Público y visibilidad**, y abra la opción **Seguidores y contenido público**, validar que la configuración quede así:

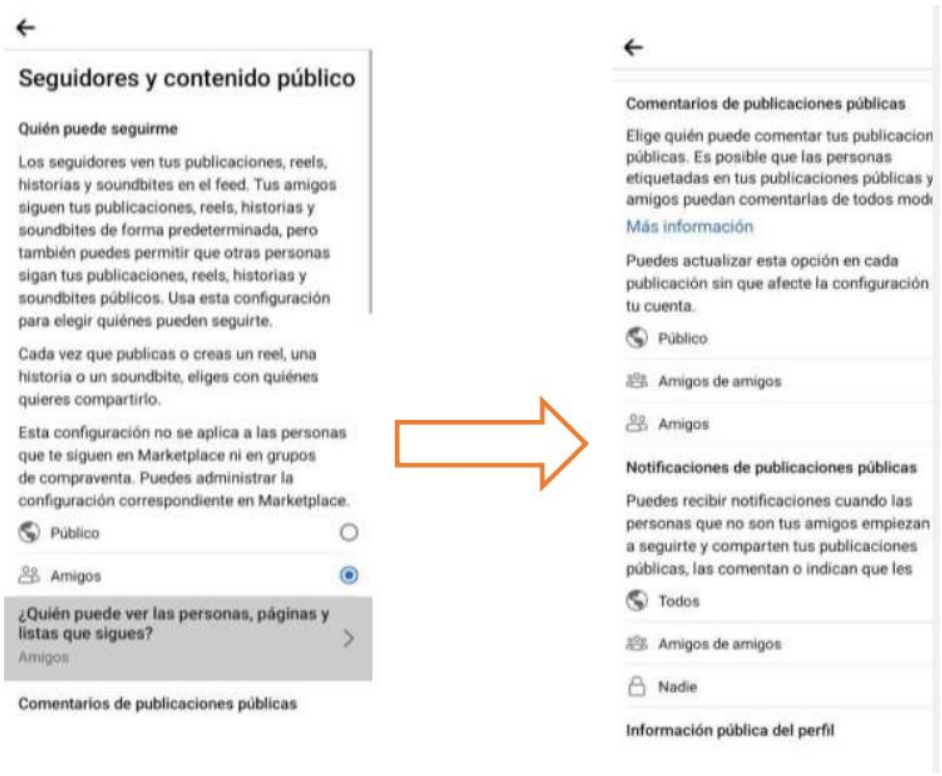


Ilustración 19. Facebook. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

Finalmente, dejar la opción **Información pública del perfil,** así:

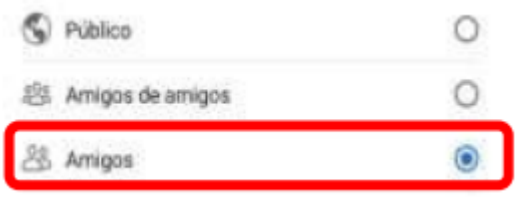


Ilustración 20. Facebook. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver. 411.1.0.29.112

2.2 Configuración de un perfil de WhatsApp.

Para realizar una correcta configuración de un perfil de WhatsApp, **preservando la seguridad digital y la privacidad**, se sugiere ejecutar los siguientes pasos:

2.2.1 Elimina o limita tu foto de perfil.

Los pasos para eliminar la foto de perfil es la siguiente: ir a **Configuración > Seleccione la foto de perfil > Clic 2 veces en editar** y seleccionar la opción **Eliminar foto**

Los pasos para configurar quien quiere que vea la foto de perfil es la siguiente: ir a **Configuración** > **Privacidad** > **Foto del perfil** y seleccionar la opción **Mis contactos.**

Eliminar foto de perfil

Limitar foto de perfil

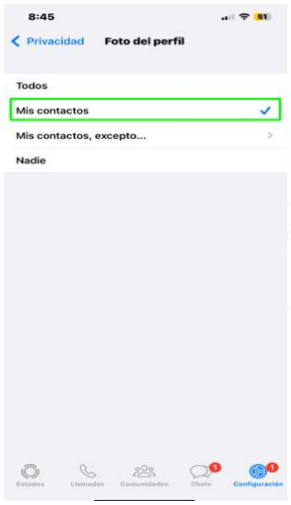


Ilustración 21 WhatsApp. (2023, 04 de marzo). Configuración de perfil [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.2 Editar hora de última conexión y en línea

Para ajustar quién puede ver la hora de última conexión debes ir a **Configuración > Privacidad > Hora de últ. vez y En línea** y seleccionar la opción en quien puede ver mi hora de últ. vez **Mis contactos,** Quién puede ver cuando estoy en línea **Igual que la hora de últ. Vez**

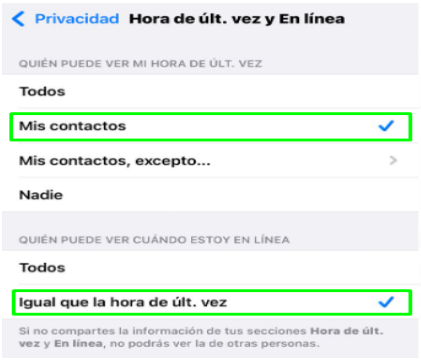


Ilustración 22 WhatsApp. (2023, 04 de marzo). Configuración de privacidad [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.3 Oculta tu nombre en WhatsApp

Los pasos para ocultar el nombre de perfil son los siguientes: ir a **Configuración** > **Seleccione la foto de perfil** > y **edite** el nombre a mostrar.

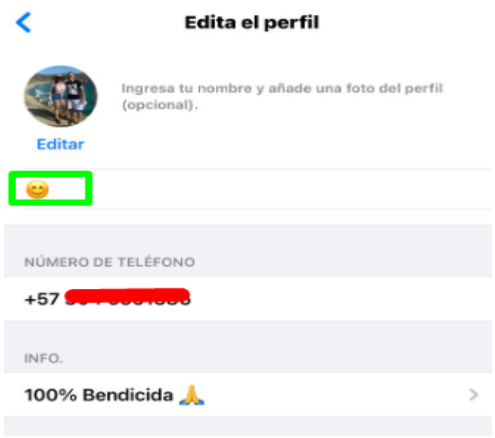


Ilustración 23 WhatsApp. (2023, 04 de marzo). Configuración de perfil [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.4 Que no te metan en grupos sin tu permiso

Los pasos son los siguientes: Ir a **Configuración** > **Privacidad** > **Grupos** > y Seleccionar la opción **Mis contactos**

Ilustración 24 WhatsApp. (2023, 04 de marzo). Configuración de privacidad [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.5 Protege tu WhatsApp con huella dactilar o face ID

Para proteger tu WhatsApp ve a **Configuración** > **Privacidad** > **Bloqueo de pantalla** > **Activa** el interruptor. Podrás elegir si quieres que WhatsApp pida la verificación con huella siempre o al pasar determinado tiempo desde que cambias a otra app.

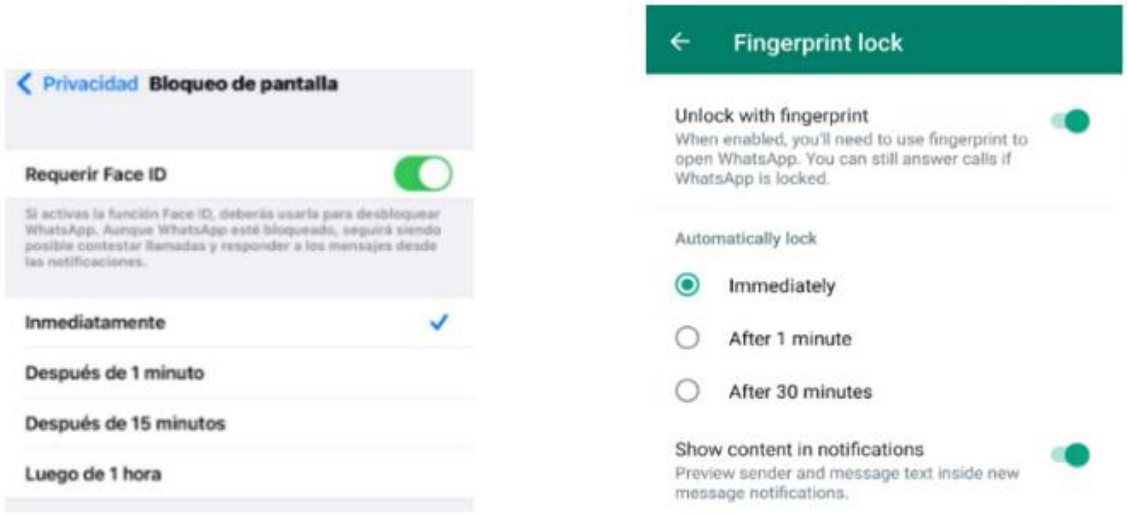


Ilustración 25 WhatsApp. (2023, 04 de marzo). Configuración de seguridad [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.6 Activa la verificación en dos pasos

La verificación en dos pasos de WhatsApp se activa en **Configuración** > **Cuenta** > **Verificación en dos pasos.** Primero deberás i**ntroducir** un **código PIN** y después, opcionalmente, una **dirección de correo**. Necesitarás ese PIN para registrar tu número de teléfono en WhatsApp en otro teléfono.

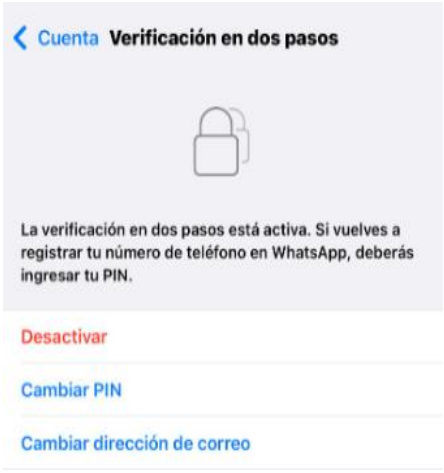


Ilustración 26 WhatsApp. (2023, 04 de marzo). Configuración de seguridad [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.2.7 Cifra tu copia de seguridad

Tienes dos opciones: la más radical es desactivar por completo la copia de seguridad en la nube, lo cual impedirá que puedas llevar tu cuenta a otro terminal. Además, puedes cifrar tu copia de seguridad desde **Configuración** > **Chats** > **Copia de seguridad** > **Copia de seguridad cifrada de extremo a extremo.**

Ilustración 27 WhatsApp. (2023, 04 de marzo). Configuración de seguridad [Captura de pantalla] Recuperado de App móvil ver. 23.7.83

2.3 Configuración de un perfil de Instagram.

Para realizar una correcta configuración de un perfil de Instagram, preservando la seguridad digital y la privacidad, se sugiere ejecutar los siguientes pasos:

2.3.1 Ingresar al Menú de Instagram.

Para acceder al **menú de configuración** desde un dispositivo móvil, se debe ingresar al **perfil** seleccionando el icono resaltado en el recuadro rojo.

Ilustración 28 Instagram. (2023, 03 de marzo). Página principal [Captura de pantalla]. Recuperado de App móvil ver.279.0

En el perfil, se ingresa a las 3 rayas ubicadas en la parte superior derecha de la pantalla.

Ilustración 29 Instagram. (2023, 03 de marzo). Perfil [Captura de pantalla]. Recuperado de App móvil ver.279.0

2.3.2 Ingresar al menú de Configuración

Seleccionar la opción **Configuración**, para que se despliegue un nuevo menú.

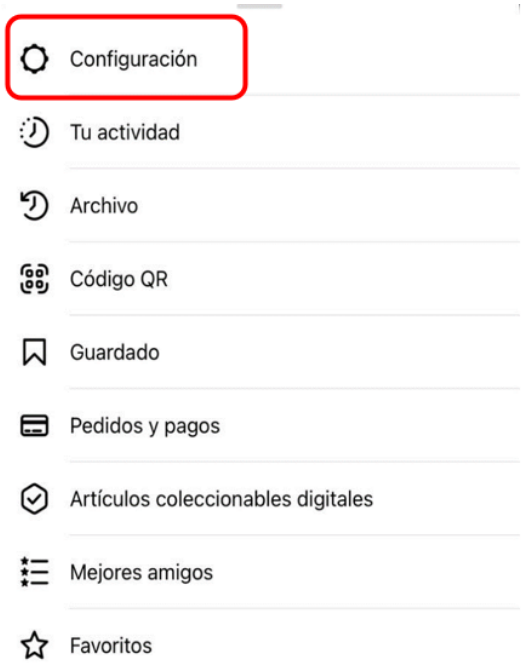


Ilustración 30 Instagram. (2023, 03 de marzo). Configuración [Captura de pantalla]. Recuperado de App móvil ver.279.0

2.3.3 Configurar la privacidad de la cuenta.

Del menú desplegado, seleccionar la opción Privacidad, como se indica en la imagen:

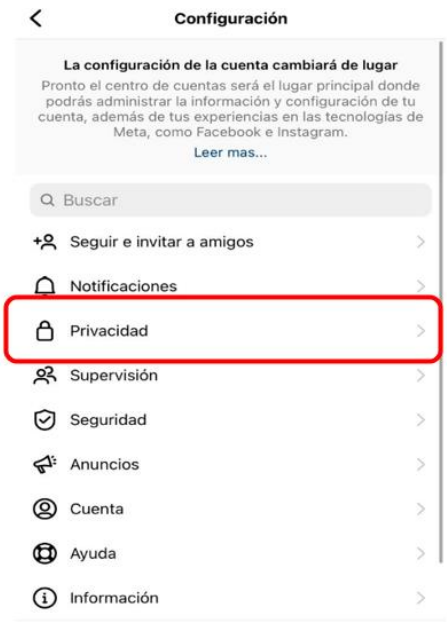


Ilustración 31 Instagram. (2023, 03 de marzo). Menú de configuración [Captura de pantalla]. Recuperado de App móvil ver.279.0

Del menú desplegado, seleccionar la opción Cuenta privada y confirmar en la opción Cambiar a cuenta privada como se muestra a continuación:

Luego se debe confirmar la configuración de la cuenta privada como se muestra a continuación:

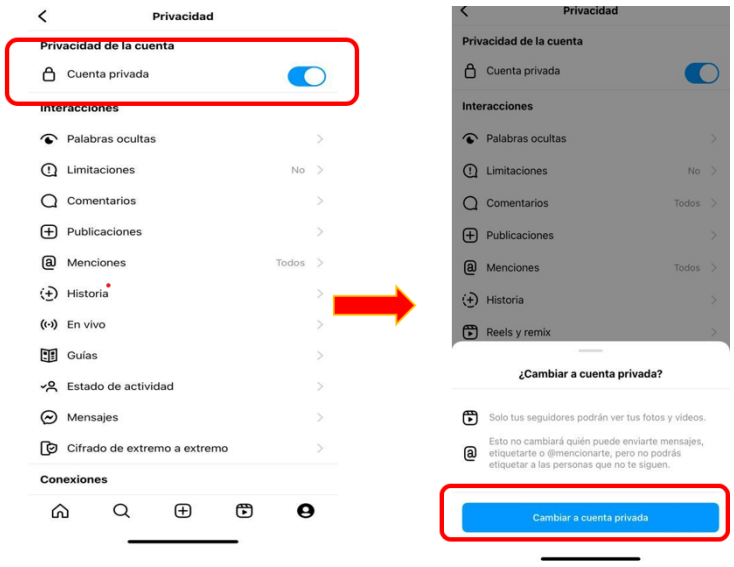


Ilustración 32 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Palabras ocultas** y se puede seleccionar la opción automática o ingresar las palabras manualmente en la casilla **Administrar palabras y frases personalizadas**.

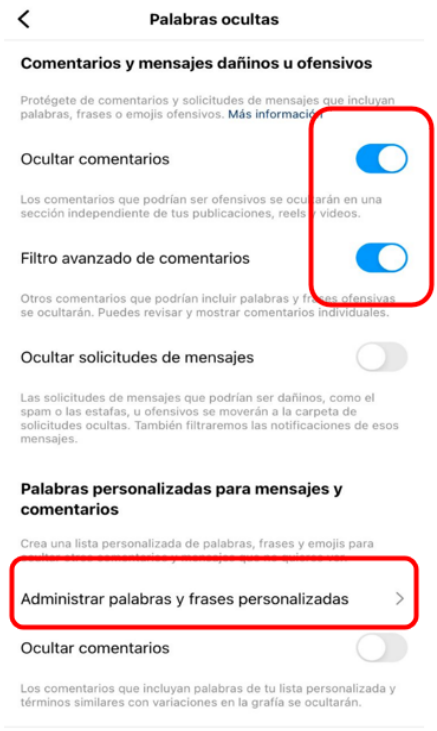


Ilustración 33 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Limitaciones** y limitamos las **cuentas que no te siguen**.

Ilustración 34 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Comentarios** y le permitimos comentarios solo a seguidores.

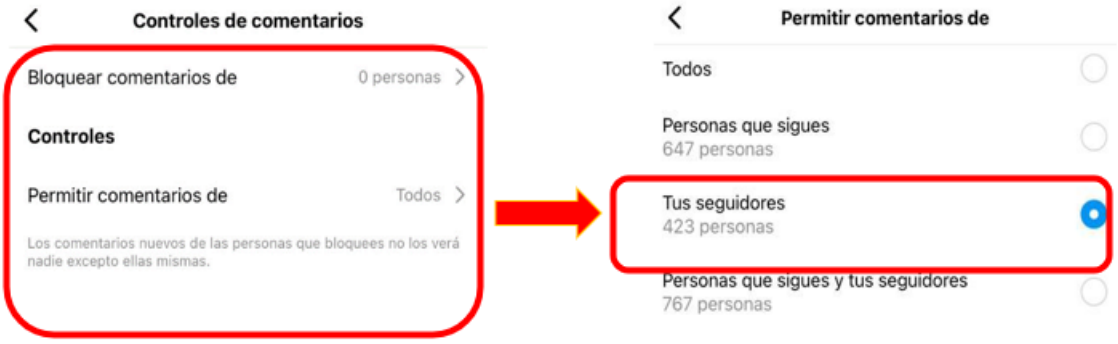


Ilustración 35 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Publicaciones** y seleccionamos las opciones para controlar que las personas que nos escriban deben solicitar el permiso.

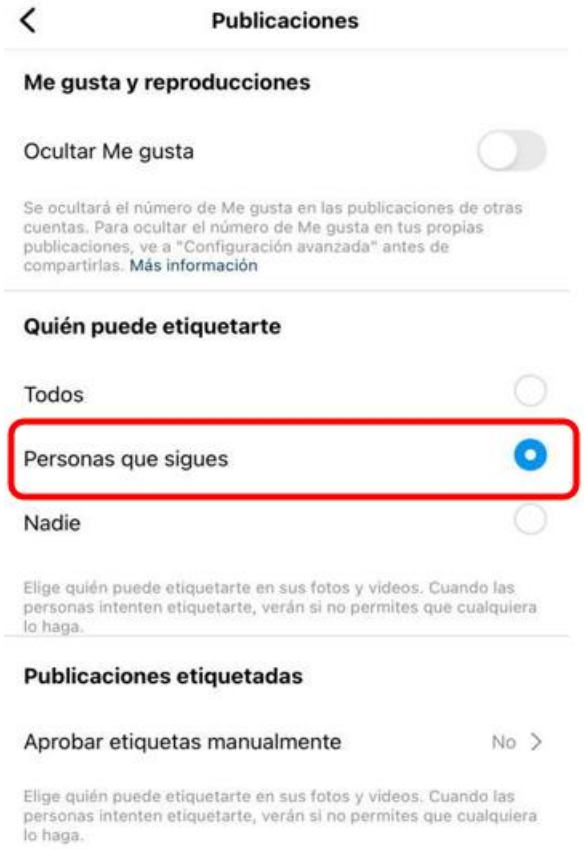


Ilustración 36 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Historias** y seleccionamos las opciones para controlar que las personas que nos escriban deben solicitar el permiso.

Ilustración 37 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

Igualmente, en el menú de **Privacidad**, seguimos a la opción **Mensajes** y seleccionamos las opciones para controlar que las personas que nos escriban deben solicitar el permiso.

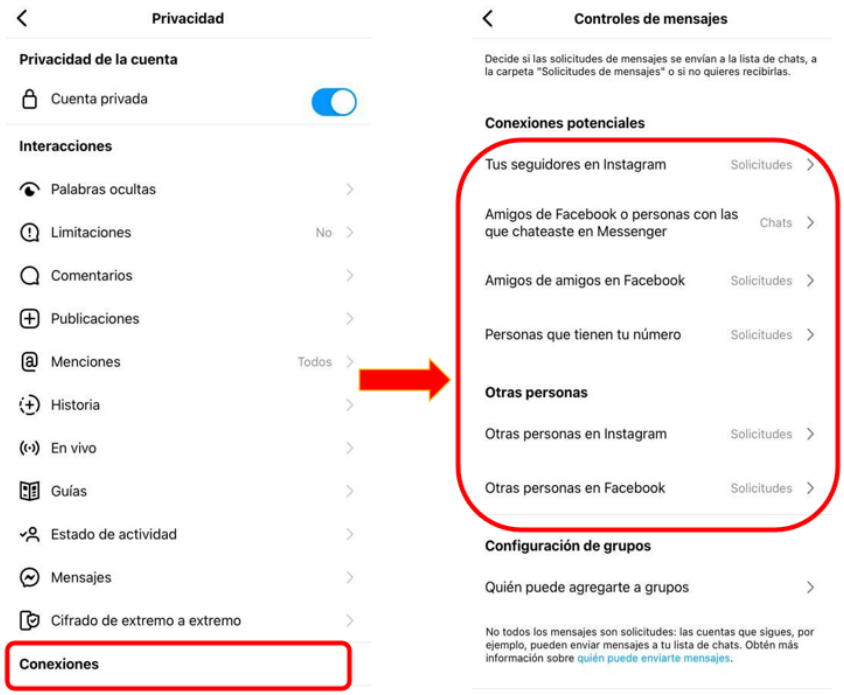


Ilustración 38 Instagram. (2023, 03 de marzo). Configuración de privacidad [Captura de pantalla]. Recuperado de App móvil ver.279.0

2.3.4 Configuración de supervisión

Volvemos al menú Configuración e ingresamos a la opción de Supervisión. Información importante de la supervisión y se selecciona Continuar.

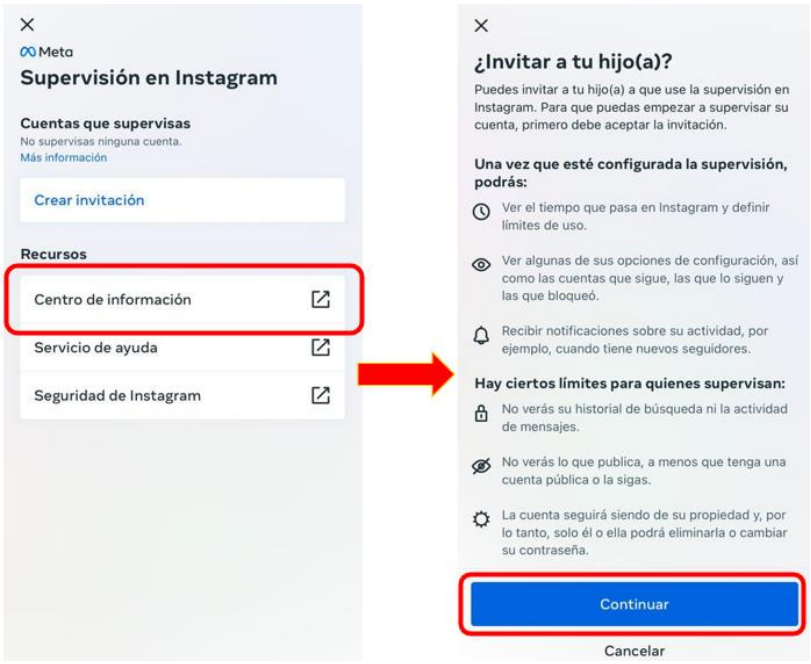


Ilustración 39 Instagram. (2023, 03 de marzo). Configuración supervisión [Captura de pantalla]. Recuperado de App móvil ver.279.0

En este momento se debe escoger el medio por el cual se va a enviar la solicitud de supervisión a su hijo quién debe aceptar para terminar la configuración, puede ser **Buscar a tu hijo en Instagram** o **Enviar un enlace a tu hijo**.

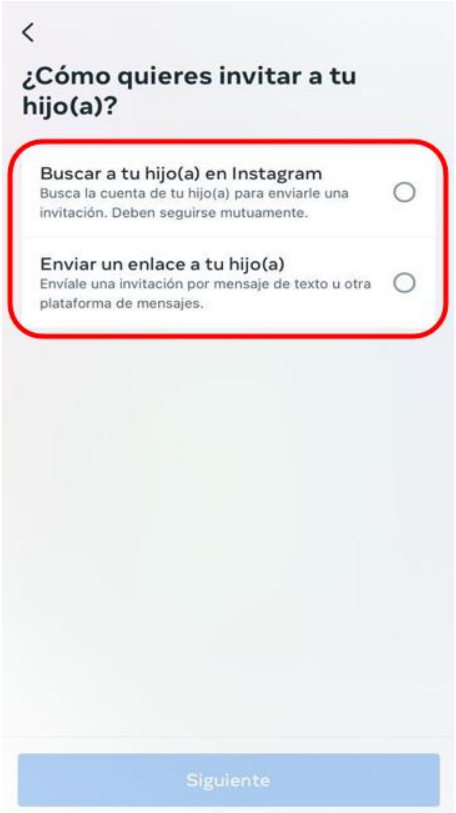


Ilustración 40 Instagram. (2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.279.0

Volviendo al menú de **Configuración**, seguimos a la opción **Cuenta** y seleccionamos **Control de contenido delicado.** Se debe seleccionar la opción **Menos** para disminuir la exposición que tiene el usuario a contenidos de tipo sexual y violento como se muestra a continuación:

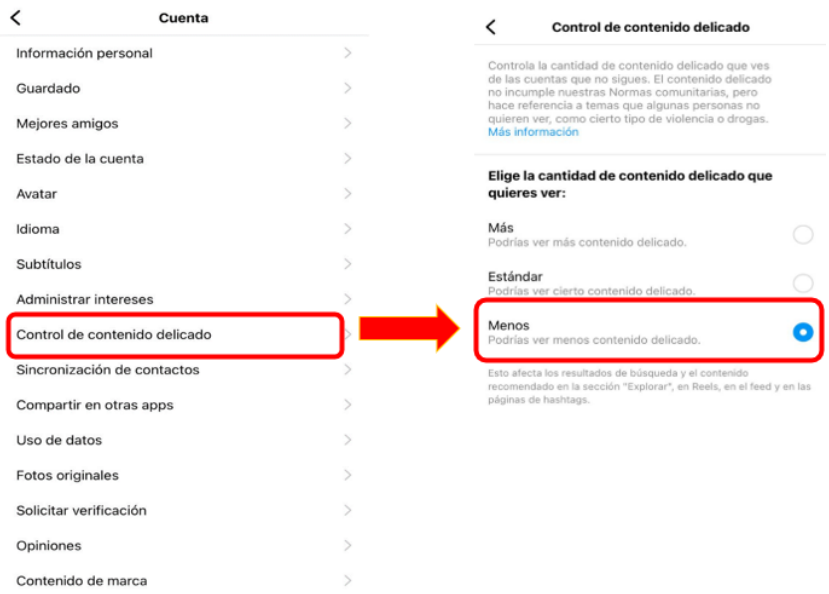


Ilustración 41 Instagram. (2023, 03 de marzo). Configuración de la cuenta [Captura de pantalla]. Recuperado de App móvil ver.279.0

2.3.5 Configurar autenticación en dos pasos

Regrese al menú de **Configuración** y seleccione **Seguridad** y seleccione la opción **Autenticación en dos pasos** y selecciona **Empezar:**

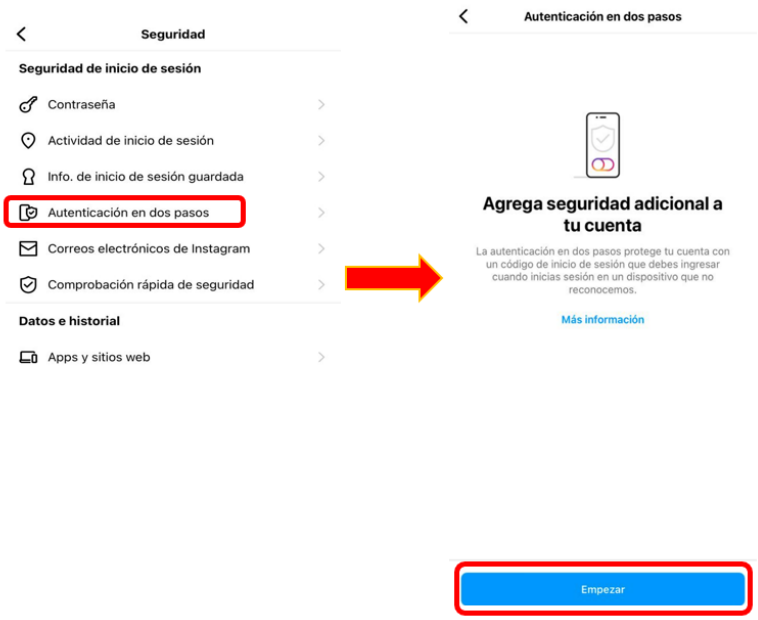


Ilustración 42 Instagram. (2023, 03 de marzo). Configuración de autenticación [Captura de pantalla]. Recuperado de App móvil ver.279.0

Luego del paso anterior, se debe elegir un método de seguridad, seleccionar **WhatsApp**, **App de autenticación** o **Mensaje de texto**:

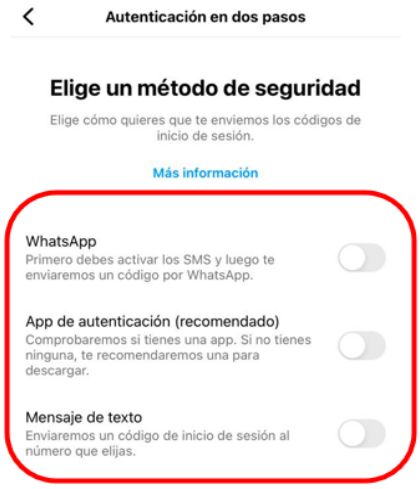


Ilustración 43 Instagram. (2023, 03 de marzo). Configuración de autenticación [Captura de pantalla]. Recuperado de App móvil ver.279.0

Nota: antes de ejecutar esta opción, se debe instalar la aplicación **Duo** o **Google Authenticator** en el mismo dispositivo o en un dispositivo distinto si así lo prefiere.

Al seleccionar la opción **App de autenticación**, se abre la siguiente pantalla, en la cual se dan las indicaciones para aparear la **App de autenticación** con el inicio de sesión de Instagram:

Después de esto, para poder iniciar sesión en Instagram, debe ingresar su contraseña y adicionalmente, debe aprobarlo desde la **App de autenticación** que haya elegido y configurado.

2.4 Configuración de perfil de Tik Tok

Desde un dispositivo móvil accedemos al **perfil** de la cuenta de Tik Tok, señalado en la imagen.

Ilustración 44 v29.1.4(2022901040) Captura de pantalla Perfil de Tik Tok

2.4.1 Opciones de la lista de Perfil

Se despliega un menú con **3 opciones**, seleccionar la opción de **Ajustes y privacidad**, como se indica en la imagen:

Ilustración 45 v29.1.4(2022901040) Captura de pantalla opciones en la sección de configuración de perfil

2.4.2 Ajustes y privacidad

La opción Ajustes y privacidad nos despliega el siguiente menú.

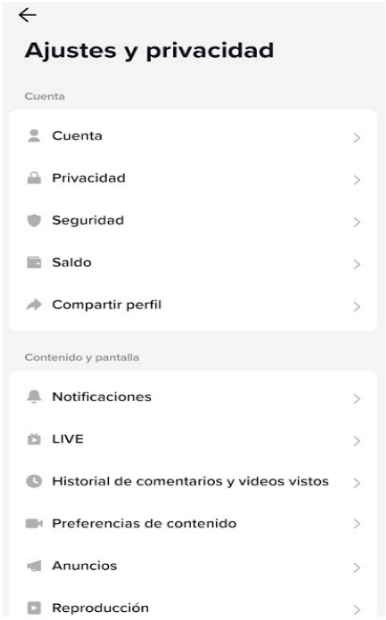


Ilustración 46 v29.1.4(2022901040) Captura de pantalla Ajustes y privacidad

2.4.3 Privacidad

Seleccionamos la opción **Privacidad**

Ilustración 47 v29.1.4(2022901040) Captura de pantalla opción de privacidad de la cuenta

2.4.4 Cuenta privada.

Para evitar exponer el contenido a cualquier público, se recomienda la configuración de **cuenta privada**, con esta configuración solo puede acceder a quien se le otorgue el permiso

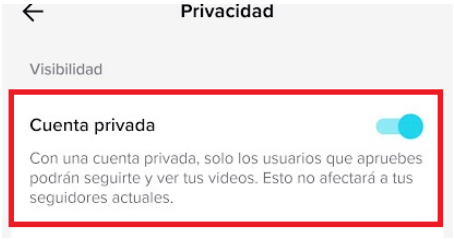


Ilustración 48 v29.1.4(2022901040) Captura de pantalla visibilidad cuenta privada

2.4.5 Sincronización Familiar.

Es una gran alternativa para tener control sobre la navegación de un menor de edad en la aplicación. Tanto el mayor de edad como el menor de edad. **Ambos deben tener la aplicación Tik Tok instalada en sus dispositivos móviles.**

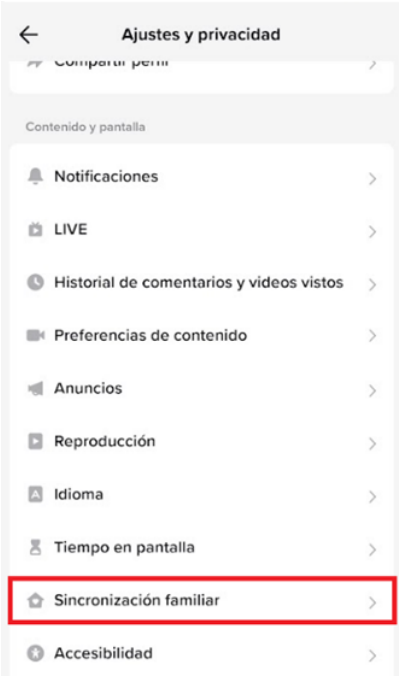


Ilustración 49 v29.1.4(2022901040) Captura de pantalla Sincronización familiar

En la siguiente imagen se puede observar las **opciones** que se aplican cuando se activa esta configuración.

Ilustración 50 v29.1.4(2022901040) Captura de pantalla menú Sincronización familiar

Al pulsar el botón Continuar, aparecen dos opciones: **Tuto/legal y Menor de edad**.

Ilustración 51v29.1.4(2022901040) Captura de pantalla Opciones de control de sincronización familiar

En la siguiente sección se muestra la configuración de Tutor/a legal, **se debe realizar desde el dispositivo del mayor de edad.**

2.4.6 Sincronización como Tutor/legal.

Desde su dispositivo móvil, seleccione la opción de **Tutor/legal**. Al presionar **Siguiente Tik Tok va a generar un código QR.**

Ilustración 52 v29.1.4(2022901040) Captura de pantalla código QR de vinculación

El siguiente paso se hace desde el dispositivo del menor de edad.

2.4.7 Sincronización opción menor de edad.

Ilustración 53 Ilustración 51v29.1.4(2022901040) Captura de pantalla Opciones de control de sincronización familiar

El dispositivo del menor de edad lo que hará es abrir la cámara para **escanear el código QR generado** anteriormente para realizar la sincronización.

Ilustración 54 v29.1.4(2022901040) Captura de pantalla Opción de escaneo de código QR

2.4.8 Preferencias de contenido.

En el **menú de ajustes y privacidad** se encuentra esta configuración**. Permite bloquear vídeos y comentarios que el usuario considere inapropiados.**

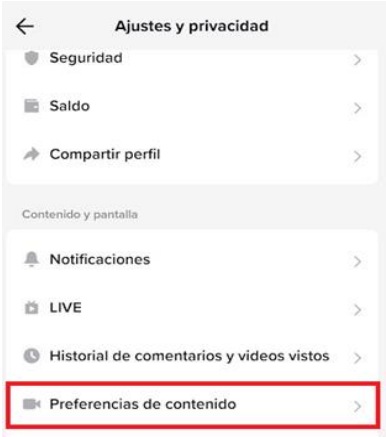


Ilustración 55 v29.1.4(2022901040) Captura de pantalla Configuración de Preferencias de contenido

Al seleccionar esta configuración se despliega un menú con tres opciones.

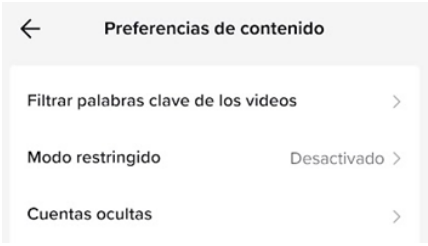


Ilustración 56 v29.1.4(2022901040) Captura de pantalla menú de Preferencias de contenido

Se puede restringir contenido audiovisual y comentarios que los añade a una lista negra, y en la navegación no aparecerán videos que tengan relación con las palabras bloqueadas

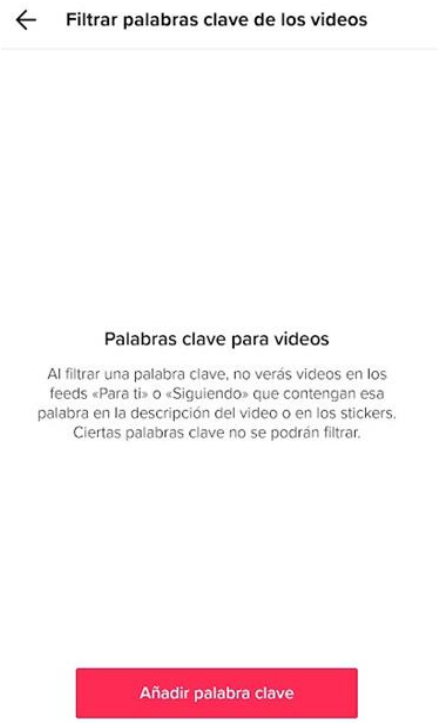


Ilustración 57v29.1.4(2022901040) Captura de pantalla Configuración Filtrar palabras claves

2.4.9 Modo restringido.

Al activar esta configuración, limita videos inapropiados para las personas, al igual que se puede denunciar vídeos de contenido inapropiado.

Ilustración 58 v29.1.4(2022901040) Captura de pantalla información del modo restringido v29.1.4(2022901040)

3 Aplicaciones para el control parental

Es un mecanismo usado especialmente por adultos para tener control y registro de los diferentes sitios web, sistemas operativos y equipos, el acceso y manipulación que los menores de edad les dan a las herramientas tecnológicas.

Las funciones de este control parental son:

-Monitoreo de navegación de los usuarios.

-Restricción de contenido no apto para menores de edad

-Es posible establecer límites en el tiempo para el uso del equipo o impedir que ejecuten programas maliciosos.

(Goodwill Community Foundation, Inc.)

3.1 Configuración de la herramienta control parental Google Family Link.

Ingrese a **Google Play** y descargue la **App Google Family Link**, una vez la aplicación se haya instalado, se recomienda seguir los siguientes pasos para realizar su configuración desde el smartphone del padre o adulto responsable del NNA

Abra la App Family Link:

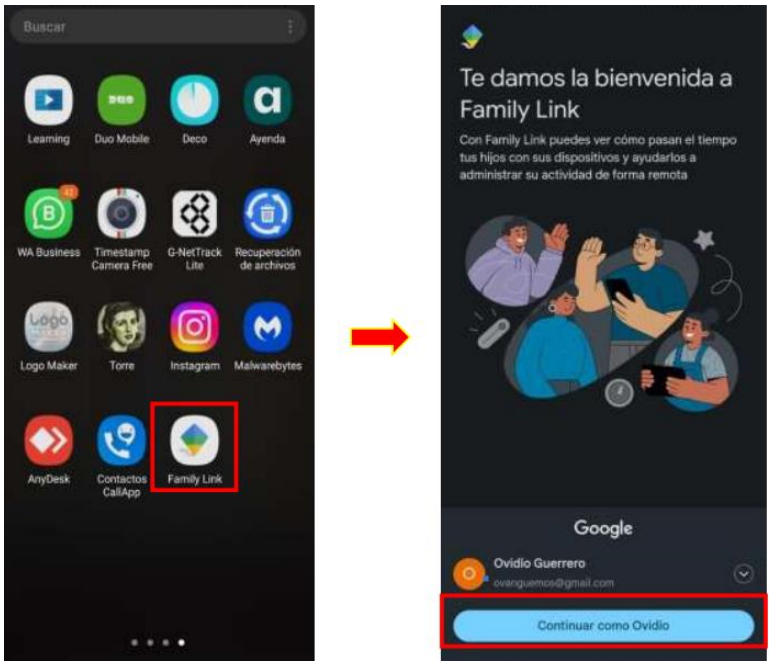


Ilustración 59. Family Link. (2023, 03 de marzo). Pantalla de inicio [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

3.1.1 Agregar un niño al control parental

Al darle en **Continuar como Ovidio,** *donde Ovidio corresponde al nombre del padre o adulto responsable*, le aparece la siguiente imagen, en la cual debe acceder al **menú** ☰ y posteriormente seleccionar la opción **Agregar niño**:

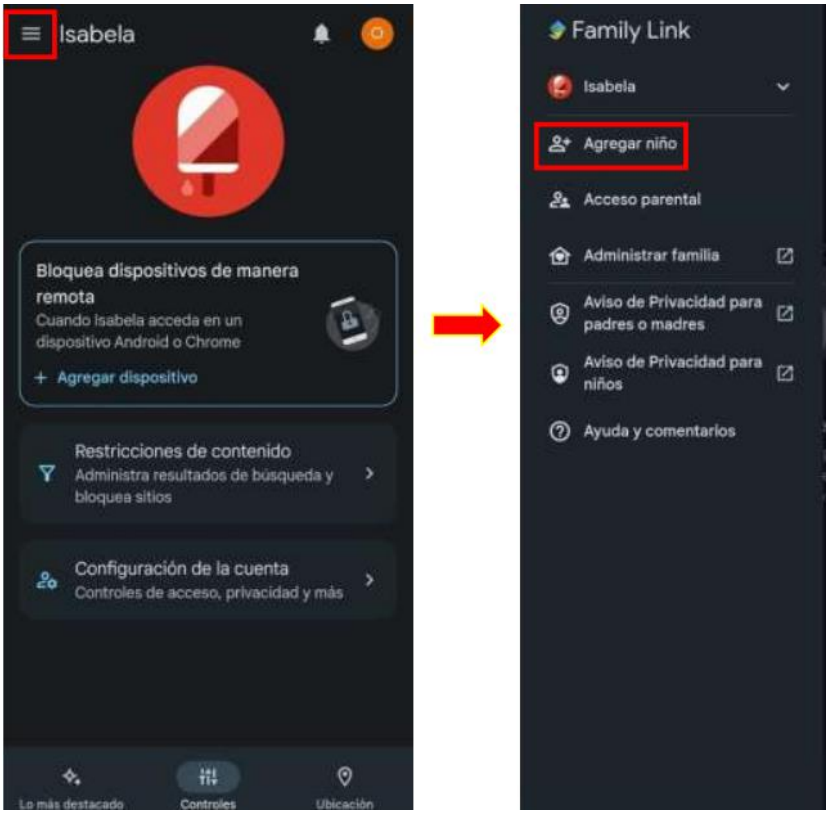


Ilustración 60. Family Link. (2023, 03 de marzo). Agregar dispositivo a controlar [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

Nota: a partir de este momento se le recomienda tener a la mano el smartphone del NNA para que pueda continuar con el proceso de configuración sin inconvenientes.

En la pantalla que se abre, a la pregunta **¿Tu hijo tiene una Cuenta de Google?**, seleccione **No** y posteriormente seleccione **Siguiente**. Después de esto**, será redirigido a Gmail** para que le cree una cuenta a su hij@:

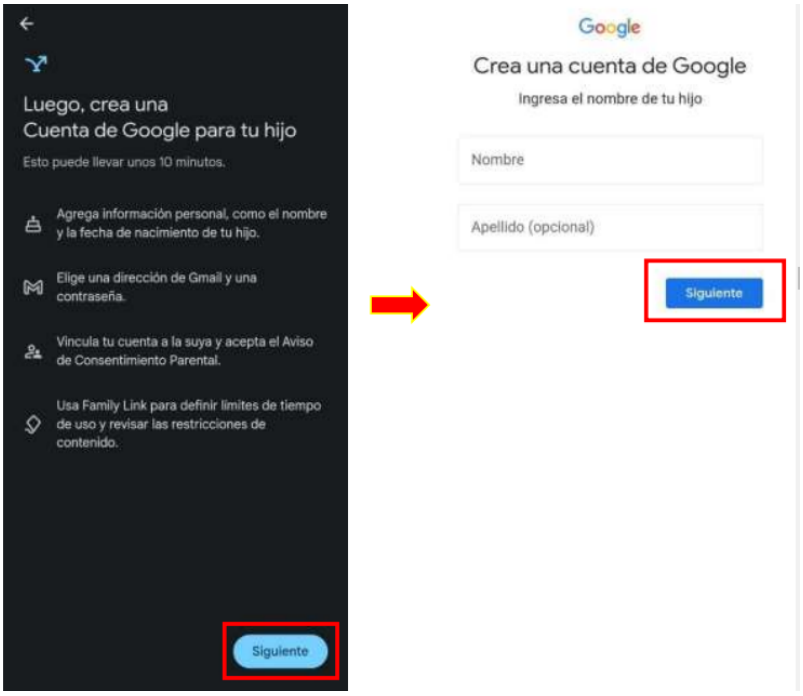


Ilustración 61. Family Link. (2023, 03 de marzo). Crear cuenta al NNA en Gmail [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

En la imagen de la derecha (**Gmail**), ingrese el **Nombre** de su hijo o NNA a cargo y el **Apellido** (opcional), posteriormente seleccione **Siguiente** y siga las instrucciones a medida que avanza (dentro de Gmail).

Una vez, haya finalizado la creación de la cuenta de su hijo, **Gmail** lo retornará a la siguiente pantalla de la **App Family Link** para que continúe el proceso de configuración. En el menú **Controles** seleccione **Agregar dispositivo** y posteriormente siga las indicaciones que se muestran en la nueva pantalla:

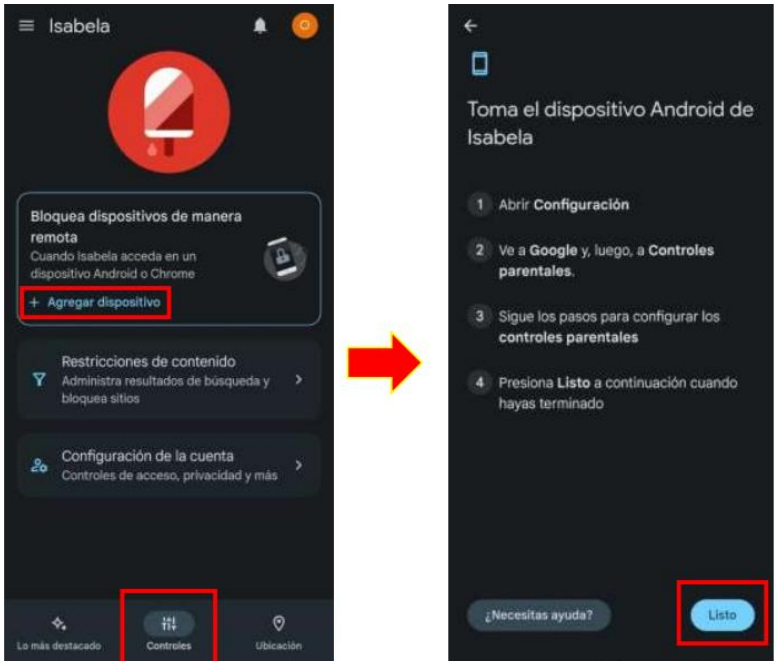


Ilustración 62. Family Link. (2023, 03 de marzo). Sincronizar el dispositivo del menor con la App [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

Después de que haya finalizado la configuración en el dispositivo de su hijo, *(en nuestro caso el de Isabela)*, debe seleccionar la opción **Listo.**

3.1.2 Configuración de restricciones de contenido

Regrese al menú **Controles**, seleccione la opción **Restricciones de contenido** e ingrese a cada una de las aplicaciones y ajuste el nivel de restricción que quiere configurar para su hijo:

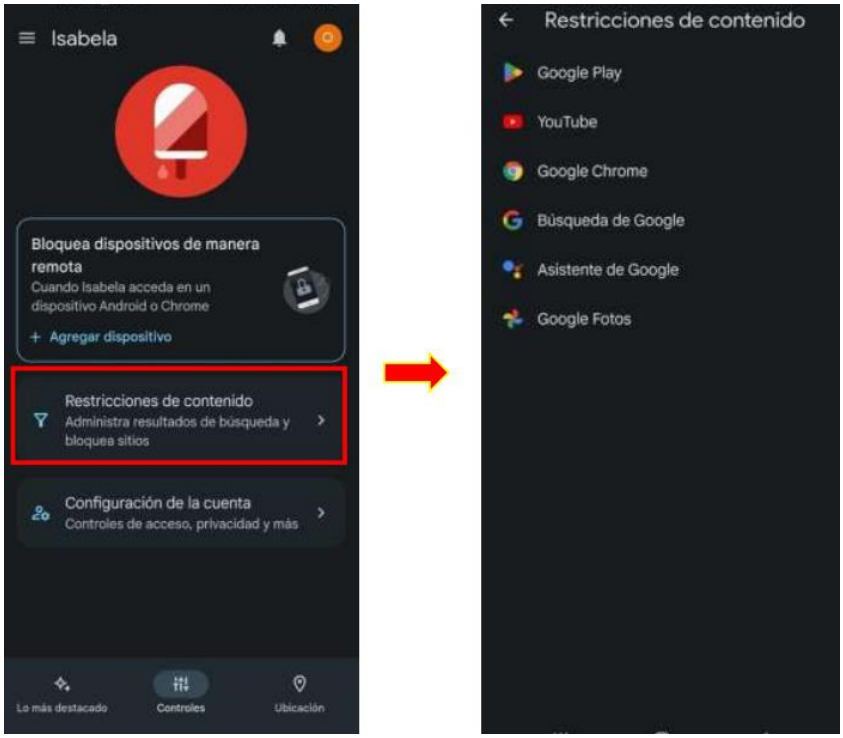


Ilustración 63. Family Link. (2023, 03 de marzo). Configuración de restricciones de contenido [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

Por ejemplo, para las restricciones de contenido de **Google Play**, ubíquese en la sección **Restricciones de contenidos** y seleccione **Apps y juegos**, en la ventana de configuración que se abre, sugerimos que elija la opción que se muestra en la siguiente imagen:

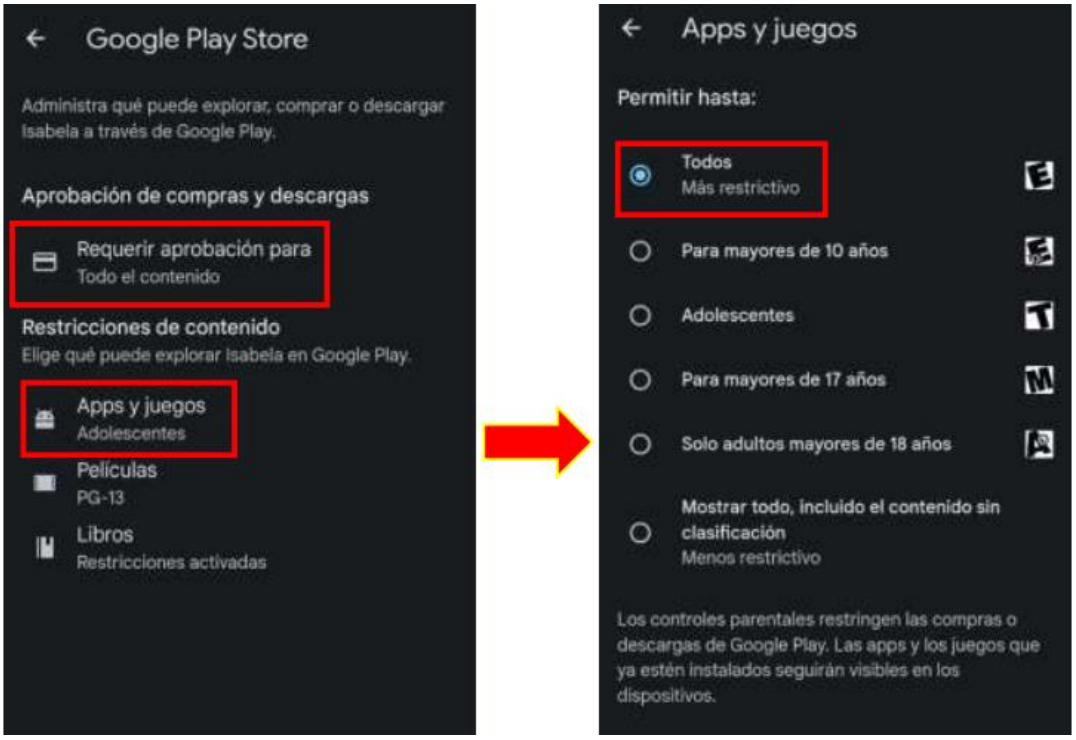


Ilustración 64. Family Link. (2023, 03 de marzo). Configuración de restricciones de contenido [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

El paso anterior, se debe repetir en las opciones **Películas** y **Libros** de la sección de **Restricciones de contenido** de **Google Play Store.**

3.1.3 Configuración de la cuenta

Regrese al menú Controles y seleccione Configuración de la cuenta, y elija Controles para acceder, en la pantalla que se abre seleccione Sí, preguntarme siempre:

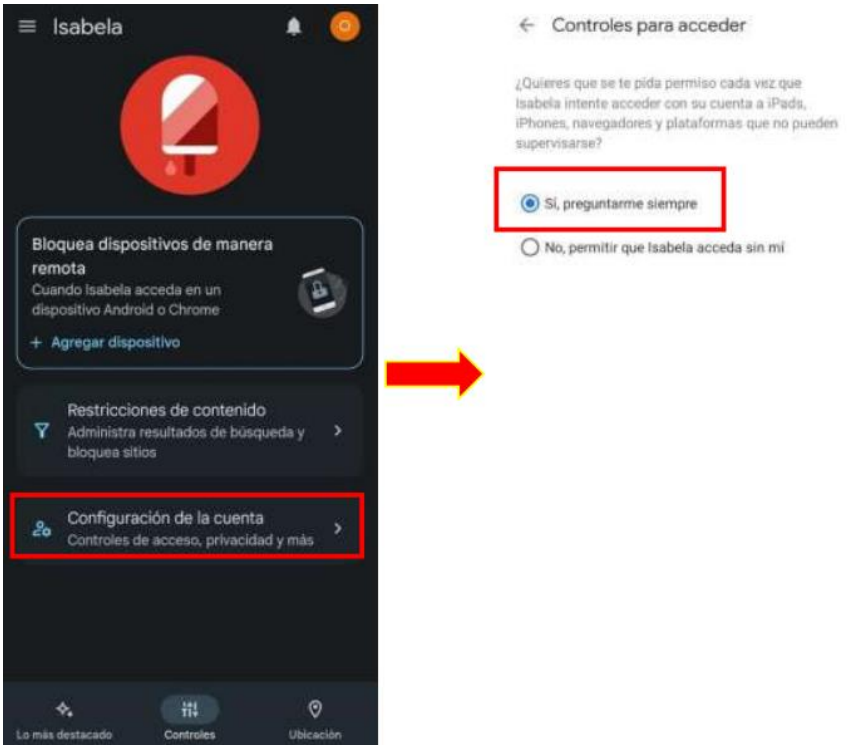
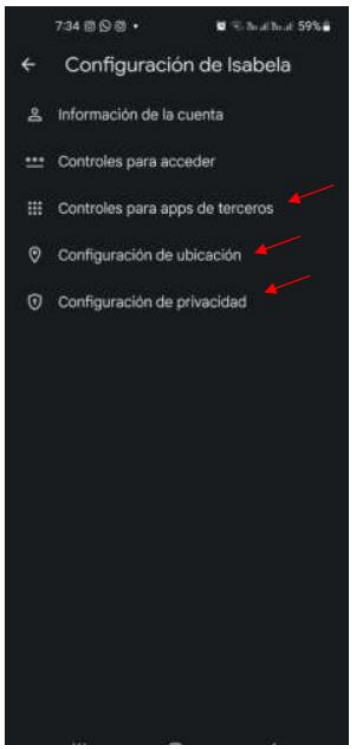


Ilustración 65. Family Link. (2023, 03 de marzo). Configuración de la cuenta del NNA [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

De esta manera, cada que su hijo intente acceder a su cuenta desde un dispositivo o plataforma que no se puede supervisar ***(iPhone, IPad, Navegadores, Plataformas)***, debe solicitarle el permiso al Padre o Tutor.

Abra cada una de las opciones restantes del menú **Configuración de la cuenta** y déjelas, como se muestran en las siguientes imágenes:

Configuración de la cuenta



Controles para Apps de terceros

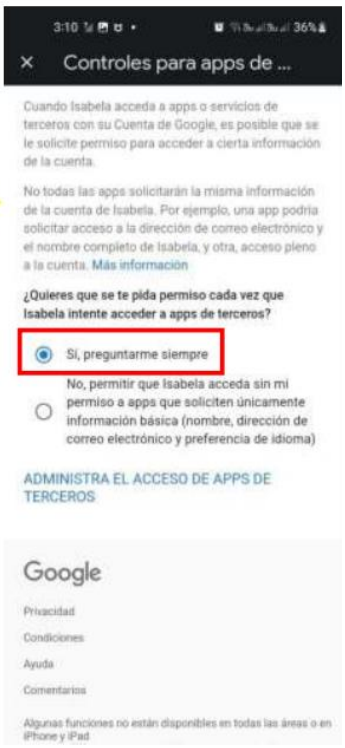
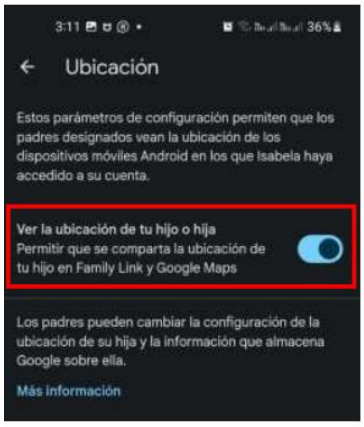


Ilustración 66. Family Link. (2023, 03 de marzo). Configuración de la cuenta del NNA [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

Configuración de ubicación



Configuración de privacidad

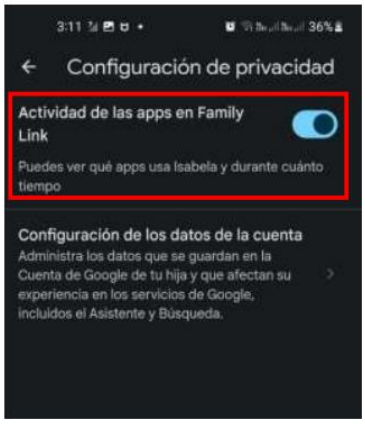


Ilustración 67. Family Link. (2023, 03 de marzo). Configuración de la cuenta del NNA [Captura de pantalla]. Recuperado de App móvil ver. 2.6.0.J.521023119

Después de haber realizado las configuraciones anteriores, puede acceder al menú **Lo más destacado** para ver cuánto tiempo su hijo utiliza el dispositivo y ver las estadísticas de las Apps que utiliza. También puede acceder al menú **Ubicación**, para ver donde se encuentra su hijo y recibir notificación de cuando llegue o se vaya de un sitio, por ejemplo: cuando se va de la escuela y llega a casa. Finalmente, puede complementar esta App con la App de Google **Controles parentales** disponible en Google Play.

3.2 Configuración de la herramienta control parental KASPERSKY SAFE KIDS.

Para realizar una correcta configuración y tener control sobre las actividades y uso de aplicaciones y redes sociales del niño a través de Kaspersky safe kids, se sugiere ejecutar los siguientes pasos:

3.2.1 Descargar la aplicación para control parental Kaspersky Safe Kids

Ingresar a la tienda de aplicaciones de su celular **Play Store** para Android y **App Store** para Iphone y descargar la aplicación Kaspersky safe kids.

Ilustración 68 Descargas. (2023, 03 de marzo). Tienda de descargas [Captura de pantalla]. Recuperado de App móvil

Se debe descargar e instalar la aplicación tanto en el dispositivo del padre como en el dispositivo del hijo.

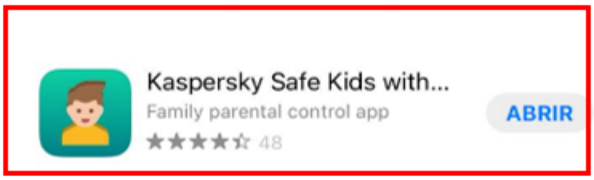


Ilustración 69 Kaspersky Safe Kids.(2023, 03 de marzo). Aplicación [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

3.2.2 Iniciar configuración de Kaspersky Safe Kids

Al abrir la aplicación instalada se pueden ver las siguientes características:

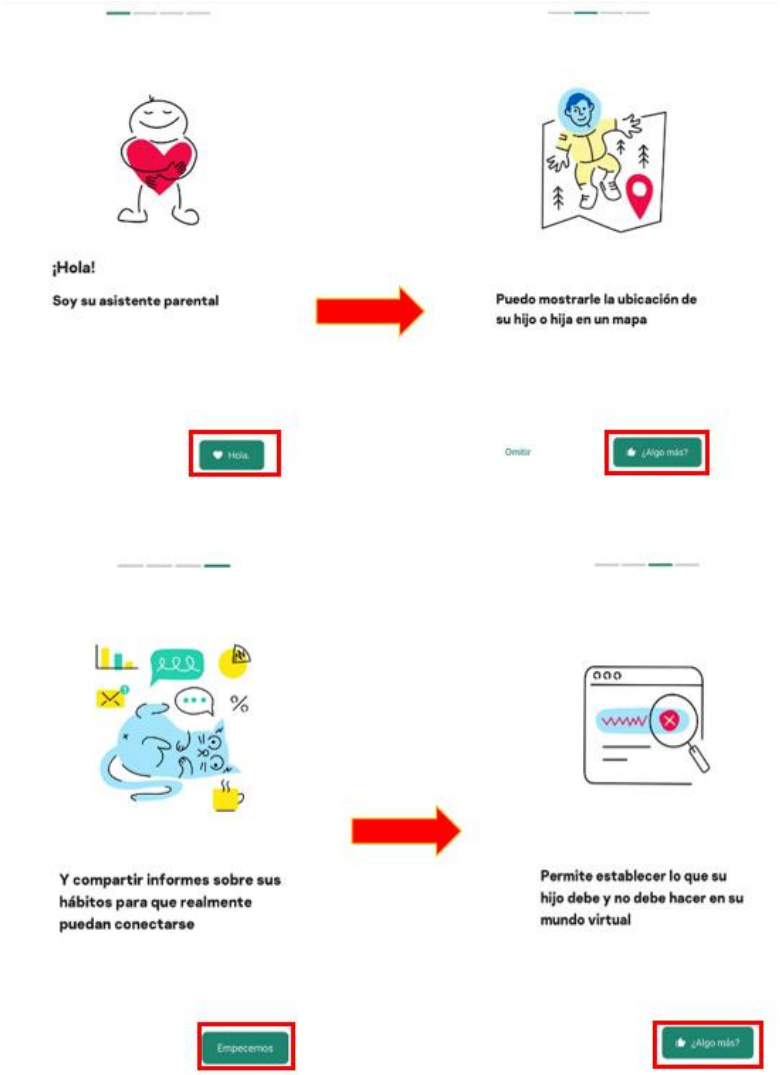


Ilustración 70 Kaspersky Safe Kids.(2023, 03 de marzo). Información de las funciones [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

3.2.3 Creación de una cuenta en Kaspersky Safe Kids

Seleccionar la opción **Padre** o **Niño** dependiendo del dispositivo que se va a configurar como se muestra a continuación:

Ilustración 71 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de dispositivo [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Se debe seleccionar la opción **crear cuenta nueva** como se muestra en la imagen:

Ilustración 72 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de cuenta [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Se debe ingresar el **correo electrónico** y la **contraseña** segura para abrir la aplicación, seleccionar **Acepto** y **Crear una cuenta**:

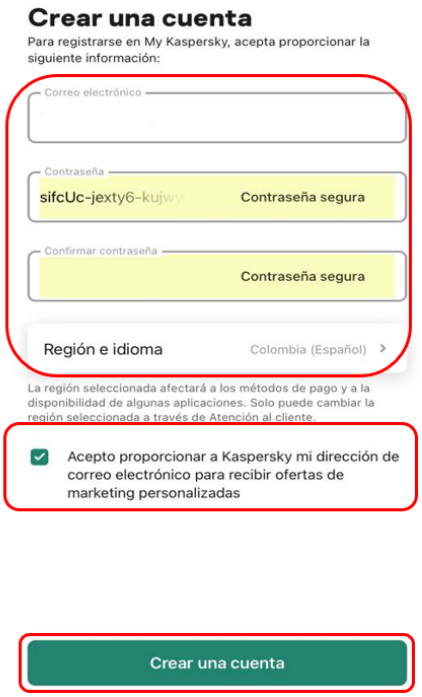


Ilustración 73 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de cuenta [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

3.2.4 Configuración de la aplicación en el dispositivo del niño

Después de crear la cuenta seleccionar la opción **Agregar niño** para realizar la configuración del dispositivo del hijo:

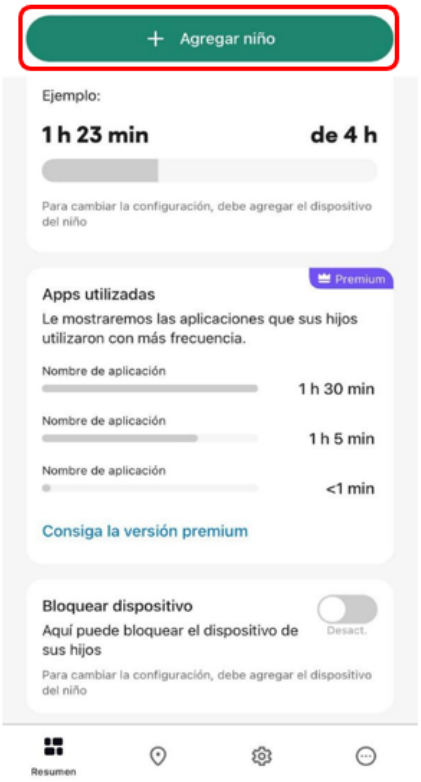


Ilustración 74 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Se deben ingresar los datos **Nombre del niño** y **Año de nacimiento** que permitan identificar el niño y **Guardar**:

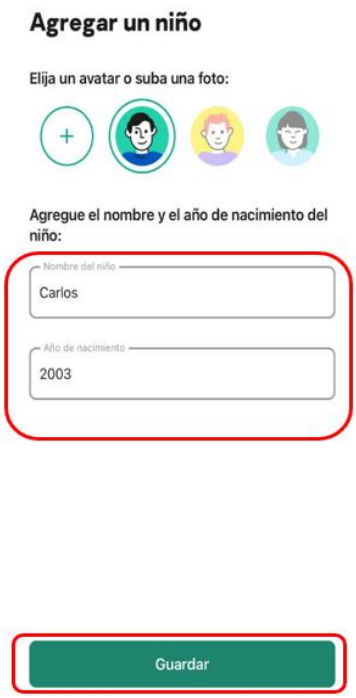


Ilustración 75 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Seguidamente, se debe seleccionar el tipo de sistema que usa el dispositivo que queremos controlar:

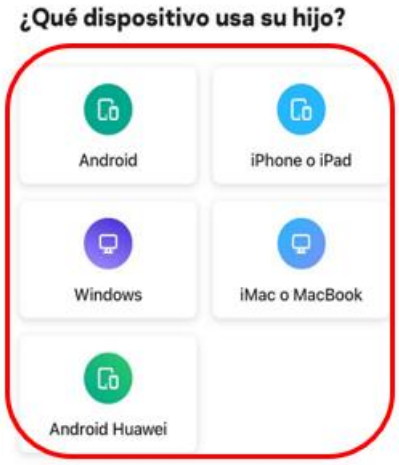


Ilustración 76 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Se debe seleccionar el método con el cual se quiere instalar la aplicación en el dispositivo del hijo puede ser **Por vínculo** o **Por código QR**:

Ilustración 77 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Se debe instalar la aplicación en el dispositivo de su hijo para finalizar con la configuración y seleccionar **Actualizar datos**:

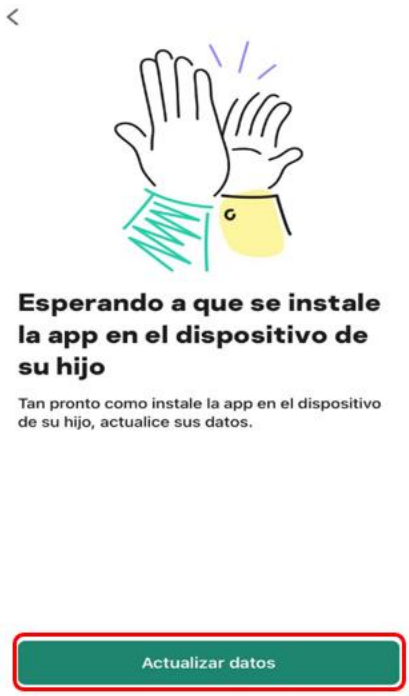


Ilustración 78 Kaspersky Safe Kids.(2023, 03 de marzo). Configuración de supervisión [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

3.3 Configuración de la herramienta control parental FamiSafe.

Para realizar una correcta configuración y tener control sobre las actividades y uso de aplicaciones y redes sociales de su hijo a través de **FamiSafe**, se sugiere ejecutar los siguientes pasos:

3.3.1 Instale y registre FamiSafe en el lado de los padres

Estos son los pasos para registrar una cuenta de FamiSafe en los teléfonos de los padres.

Paso 1: Descargue FamiSafe desde **Google Play** o **App Store** buscando **FamiSafe** directamente

Paso 2: Revise las nuevas características de FamiSafe V6.0.

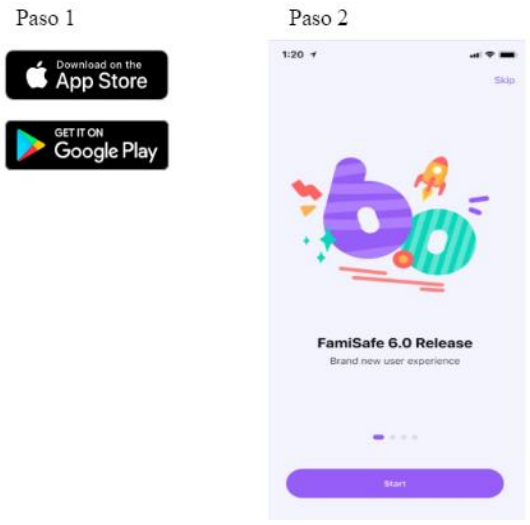


Ilustración 79 Famisafe. (2023, 06 de marzo). Instalar aplicación [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 3: Registre una ID de Wondershare para FamiSafe o **inicie sesión** con una ID de Apple, Google y FaceBook.

Ilustración 80 Famisafe. (2023, 06 de marzo). Registrarse o iniciar sesión [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 4: continúe como padre y conecte el teléfono de los niños con el código QR o el código de emparejamiento.

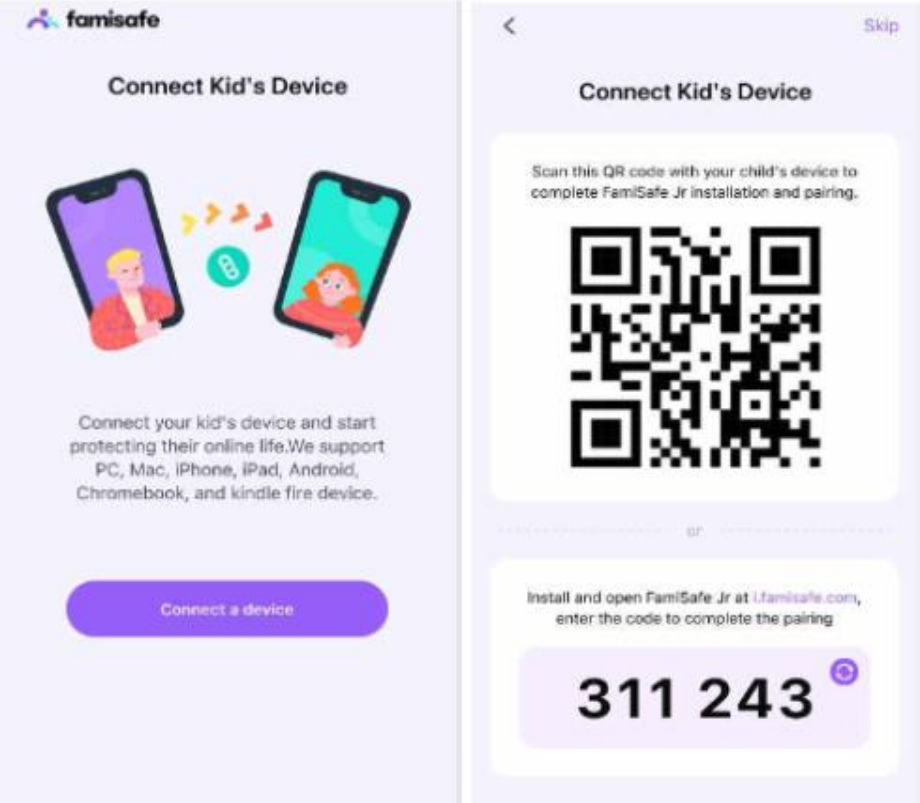


Ilustración 81 Famisafe. (2023, 06 de marzo). Emparejamiento padre niño [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 5: Después del emparejamiento y la autorización por parte de los niños, **configure** el control parental básico con el asistente iniciado y estará listo para comenzar.

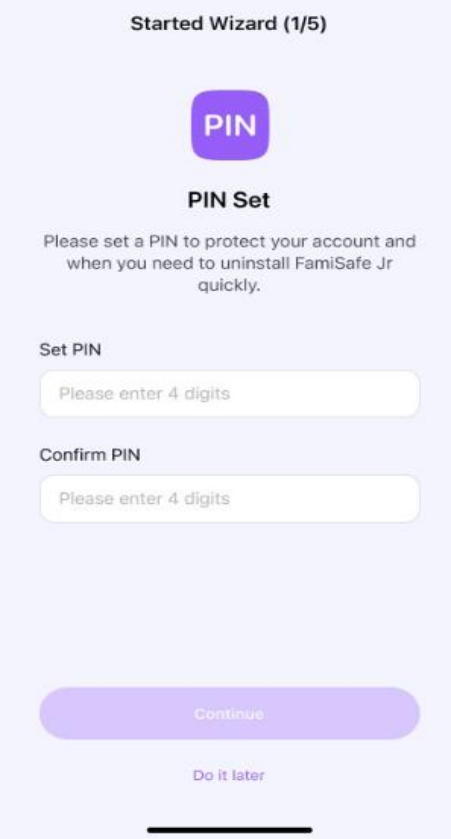


Ilustración 82 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

3.3.2 Configure FamiSafe en el dispositivo Android e iOS de su hijo

Método 1: Emparejar con código QR.

Ahora con **FamiSafe 6.0**, puede **escanear el código QR** en el extremo de los padres con el teléfono de los niños para **instalar FamiSafe Jr** y completar el emparejamiento automáticamente.

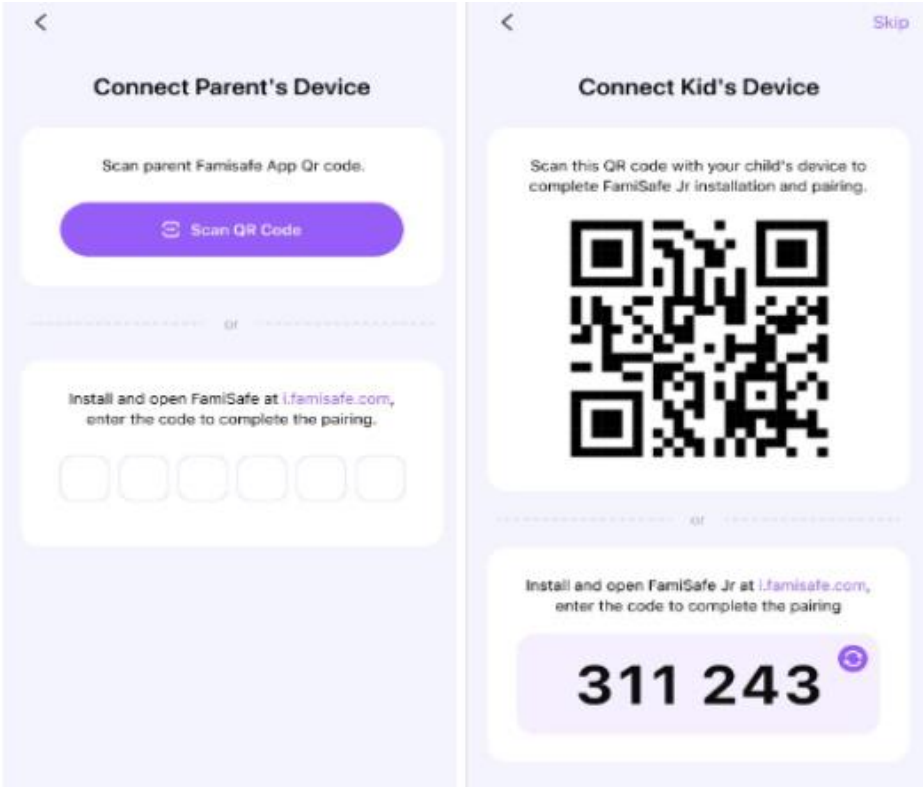


Ilustración 83 Famisafe. (2023, 06 de marzo). Emparejamiento niño - padre [Captura de pantalla] Recuperado de App móvil ver. 6.0

Método 2: Emparejar con código.

Paso 1: Puede buscar **FamiSafe Jr** en **Google Play** o **App Store** del dispositivo Android de su hijo.

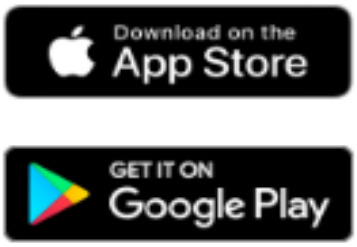


Ilustración 84 Famisafe. (2023, 06 de marzo). Tienda de descargas [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 2: Después de completar la instalación, **inicie FamiSafe** Kids en los dispositivos de sus hijos. Toca **"Iniciar"** y **escribe** el código de emparejamiento que recibes del lado de los padres.

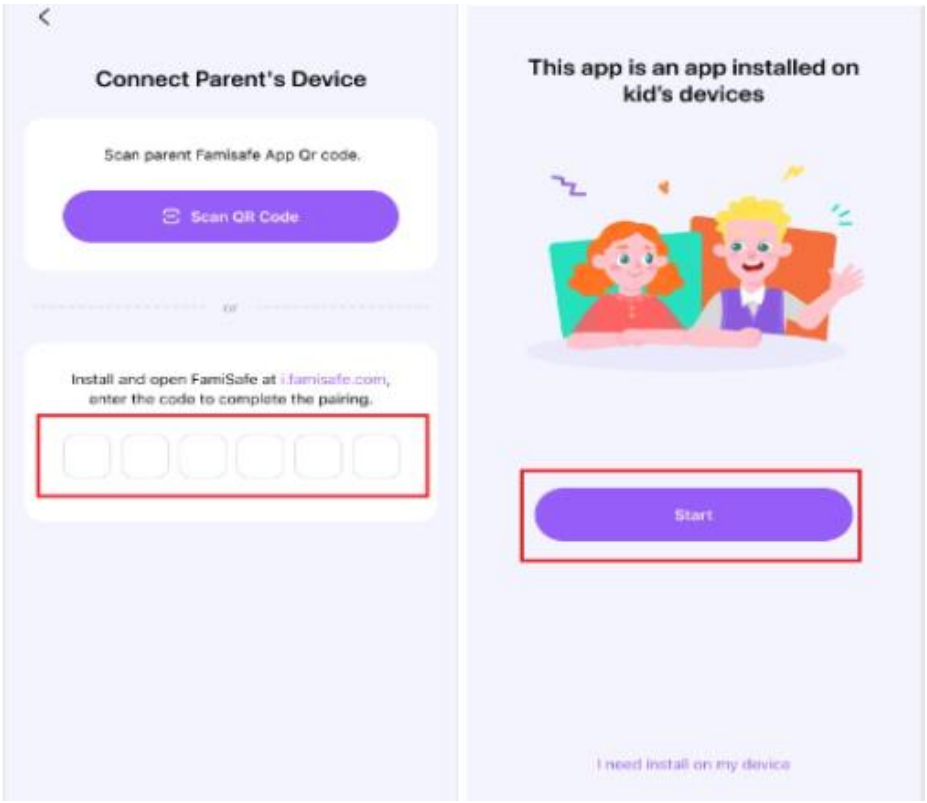


Ilustración 85 Famisafe. (2023, 06 de marzo). Emparejamiento niño - padre [Captura de pantalla] Recuperado de App móvil ver. 6.0

Después del proceso de emparejamiento, **complete la información** sobre sus hijos y otorgue **acceso** a FamiSafe Jr para que pueda **administrar** los teléfonos de los niños.

3.3.3 ¿Cómo otorgar acceso a FamiSafe en el dispositivo Android de su hijo?

Para garantizar el mejor rendimiento de FamiSafe, primero deberá otorgarle cierto acceso.

Paso 1: Active Accesibilidad para permitir que FamiSafe **acceda** a la información necesaria.

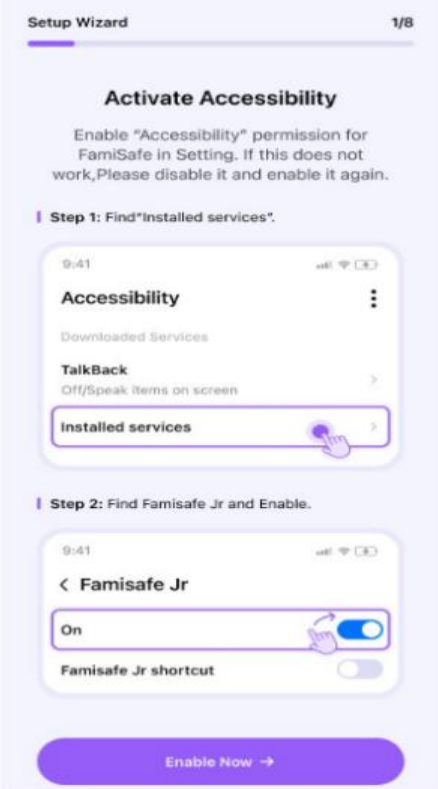


Ilustración 86 Famisafe. (2023, 06 de marzo). Configuración de acceso [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 2: Active el inicio en segundo plano para permitir que FamiSafe bloquee aplicaciones de forma remota.

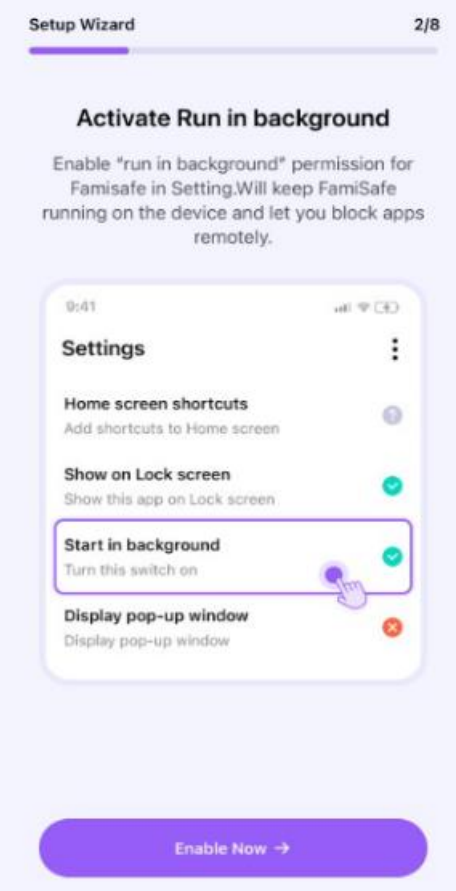


Ilustración 87 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 3: Active la visualización sobre otras aplicaciones para **permitir** que FamiSafe se muestre en otras aplicaciones cuando estén **bloqueadas**.

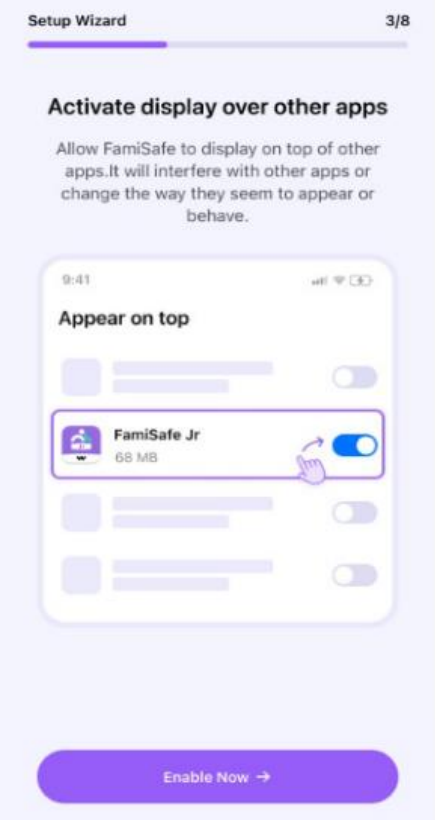


Ilustración 88 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 4: Active la supervisión de la aplicación para permitir que FamiSafe **genere informes de actividad.**

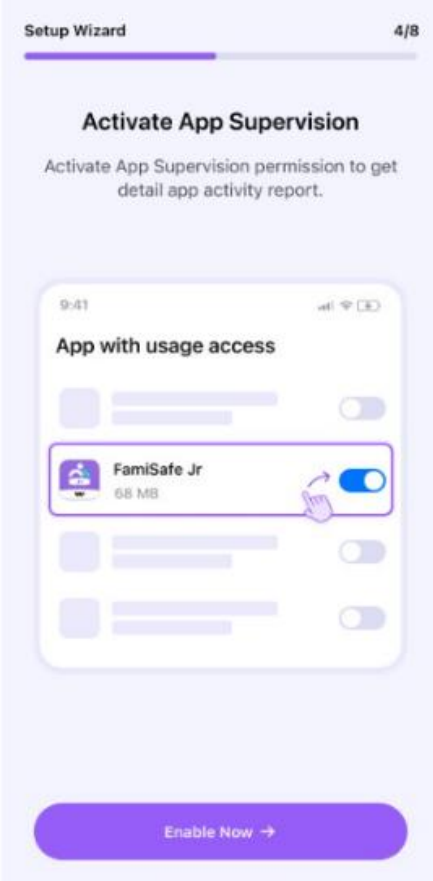


Ilustración 89 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 5: Active el acceso a las notificaciones para permitir que FamiSafe **capture** los mensajes que recibieron los niños.

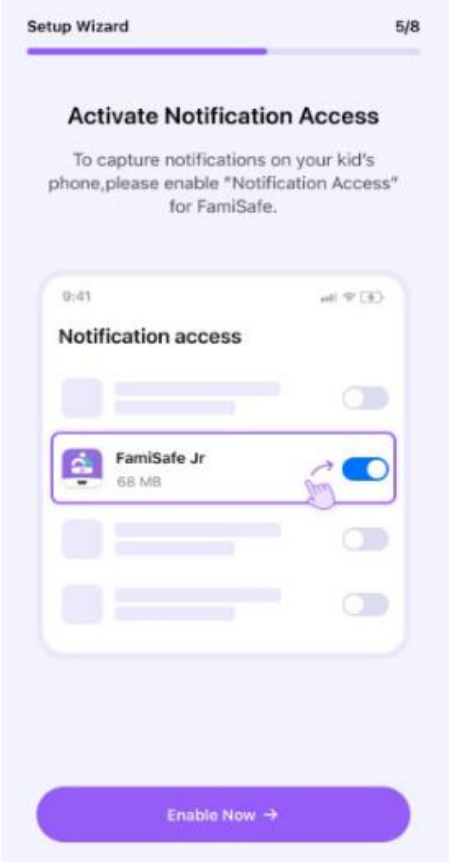


Ilustración 90 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 6: Active el permiso del administrador del dispositivo para permitir que FamiSafe configure el **tiempo de pantalla** y **detenga** el **cierre forzado** o la **desinstalación** por parte de los niños.

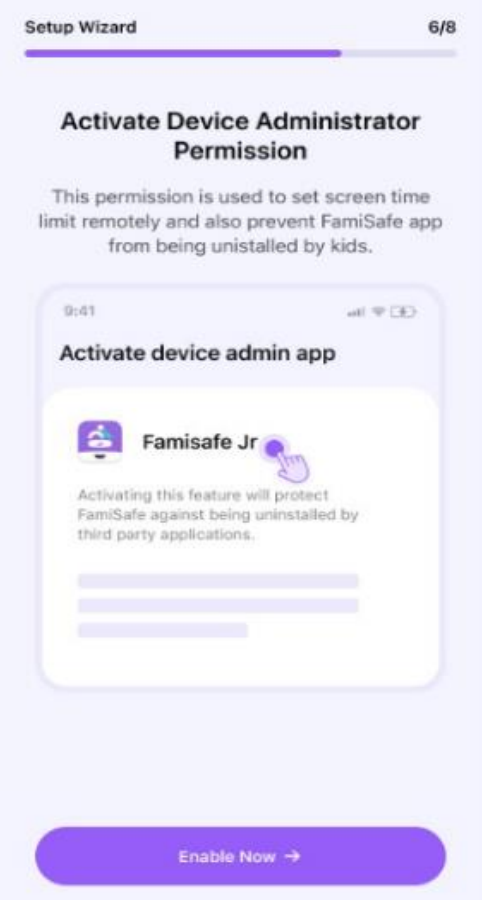


Ilustración 91 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 7: Active la ejecución en segundo plano habilitando "**Inicio automático"** y desactivando **"Ahorro de batería"** para FamiSafe.

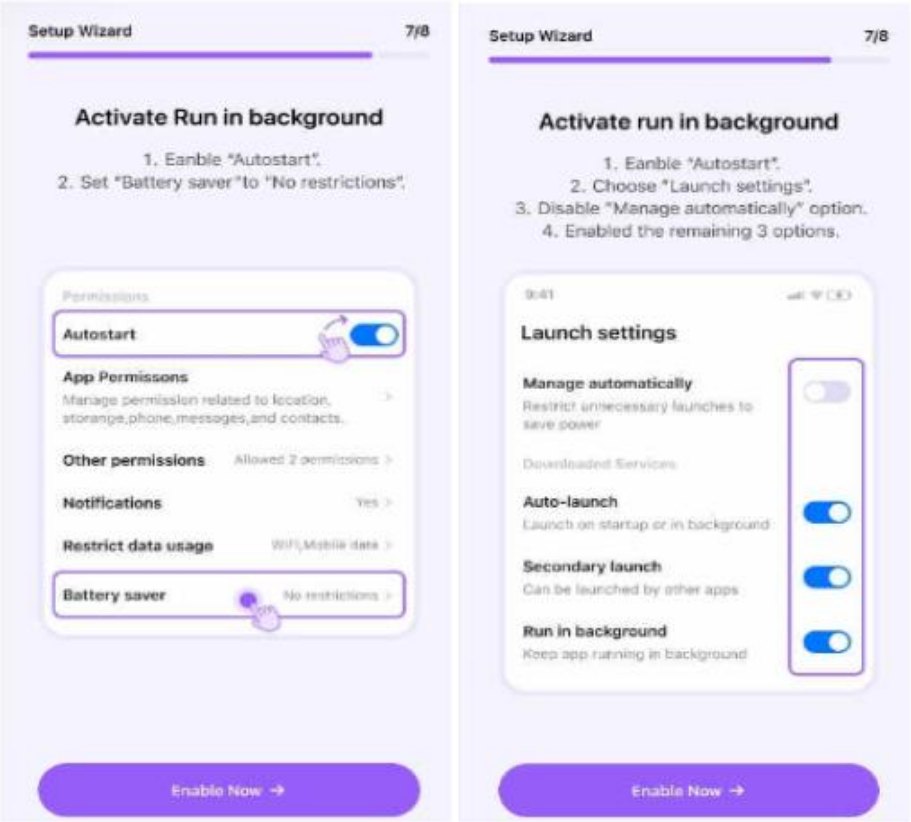


Ilustración 92 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 8: Active la ubicación para permitir que FamiSafe **capture los mensajes** que recibieron los niños.

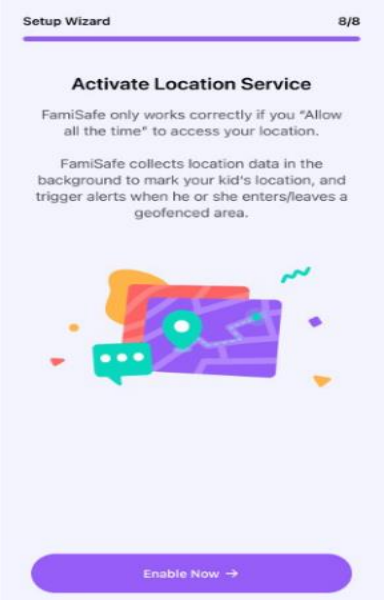


Ilustración 93 Famisafe. (2023, 06 de marzo). Configuración de ubicación [Captura de pantalla] Recuperado de App móvil ver. 6.0

3.3.4 Las funcionalidades de FamiSafe son las siguientes:

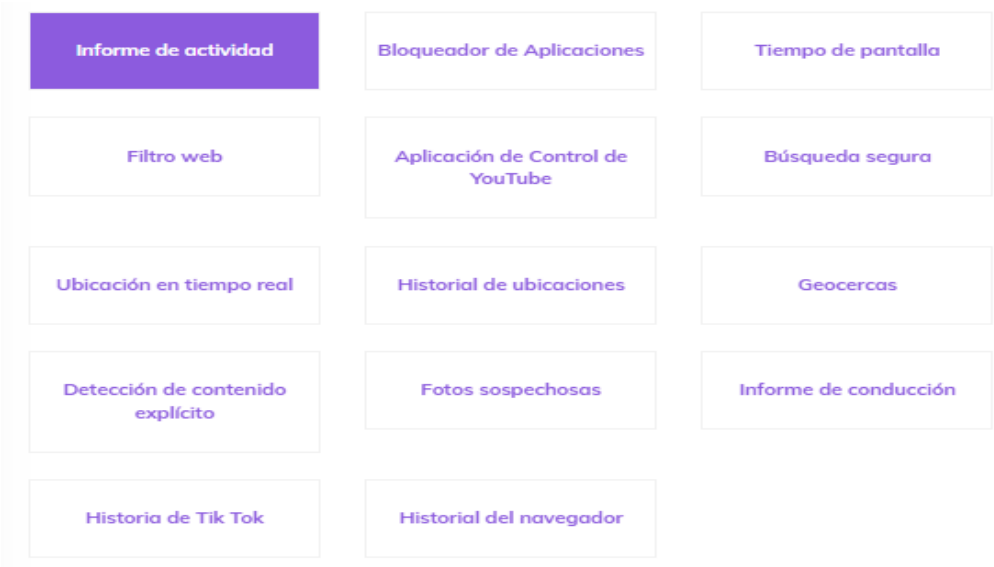


Ilustración 94 Famisafe. (2023, 06 de marzo). Funcionalidades [Captura de pantalla] Recuperado de App móvil ver. 6.0

La configuración adecuada de una de las funcionalidades de FamiSafe es la siguiente:

Detección de contenido explícito

Si se encuentra contenido explícito, los padres pueden revisar los mensajes de la siguiente manera:

Paso 1: Busque la función de contenido explícito

En la interfaz principal de la aplicación **FamiSafe**, toque **"Contenido explícito"** para ver más detalles.

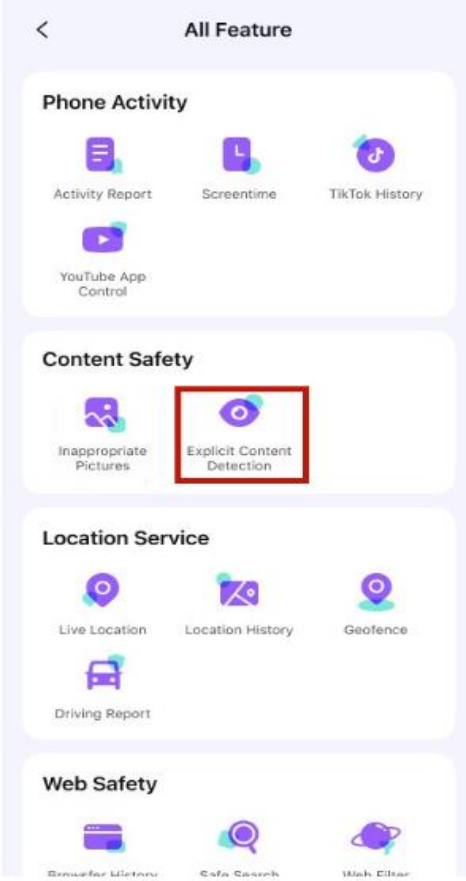


Ilustración 95 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 2: Habilitar la detección

En la interfaz de **contenido explícito**, toque **"Conectando"** y verá una lista de **aplicaciones** que FamiSafe puede detectar. **Active** el interruptor para **habilitar** la detección.

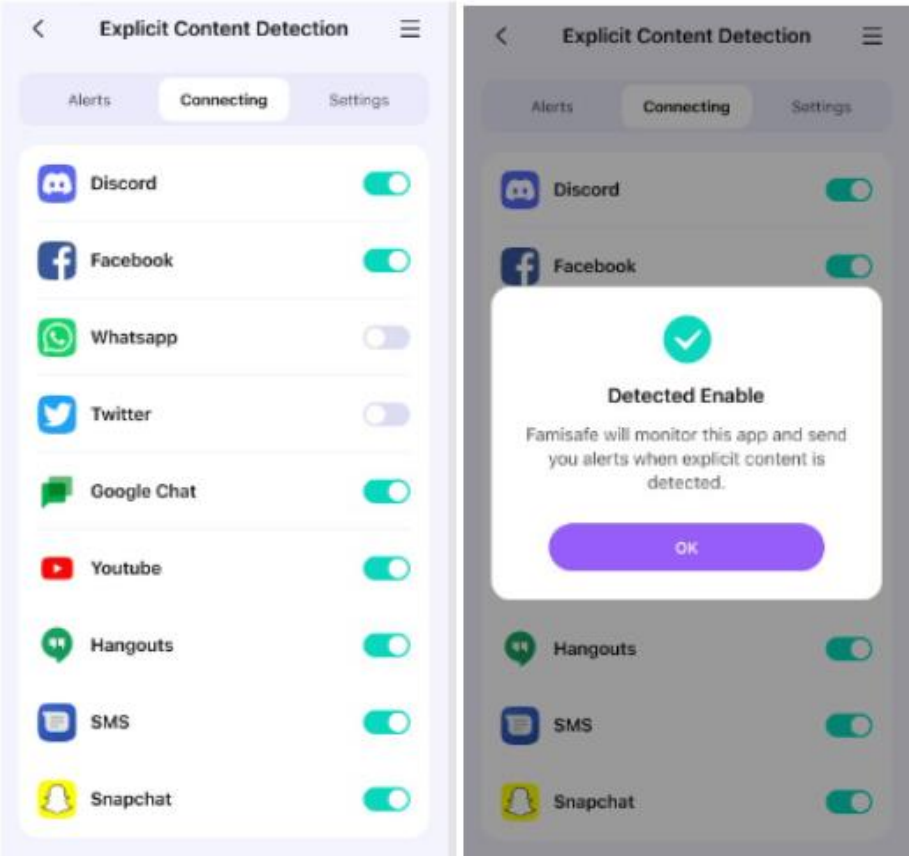


Ilustración 96 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 3: Revisa las **alertas**

En la interfaz de **contenido explícito,** toque **"Alertas"** para verificar las alertas activadas por palabras clave peligrosas relacionadas con drogas, ciberacoso y sexo en el teléfono del niño.

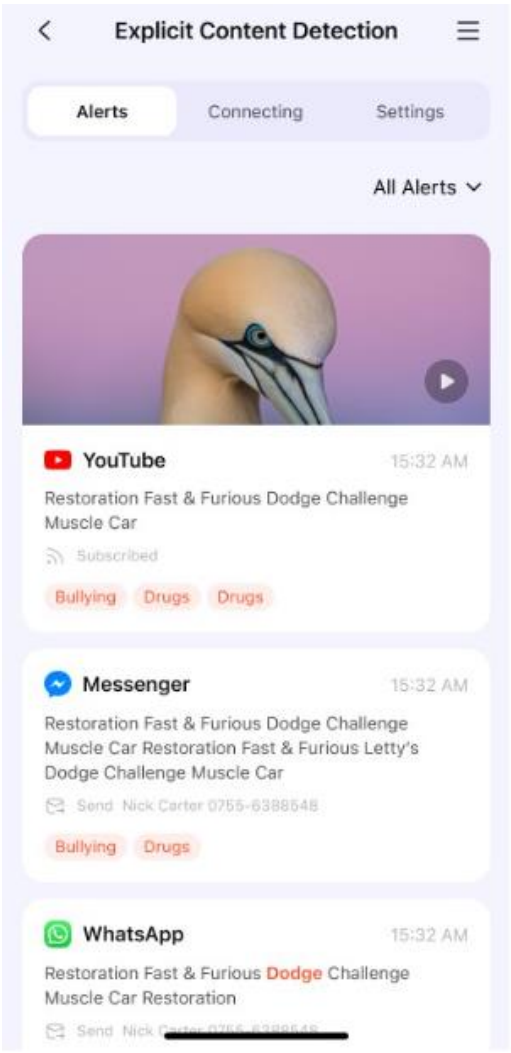


Ilustración 97 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Paso 4: Agregue palabras sospechosas

En la interfaz de contenido explícito, toque "Configuración" para habilitar cualquier categoría de palabras sospechosas.

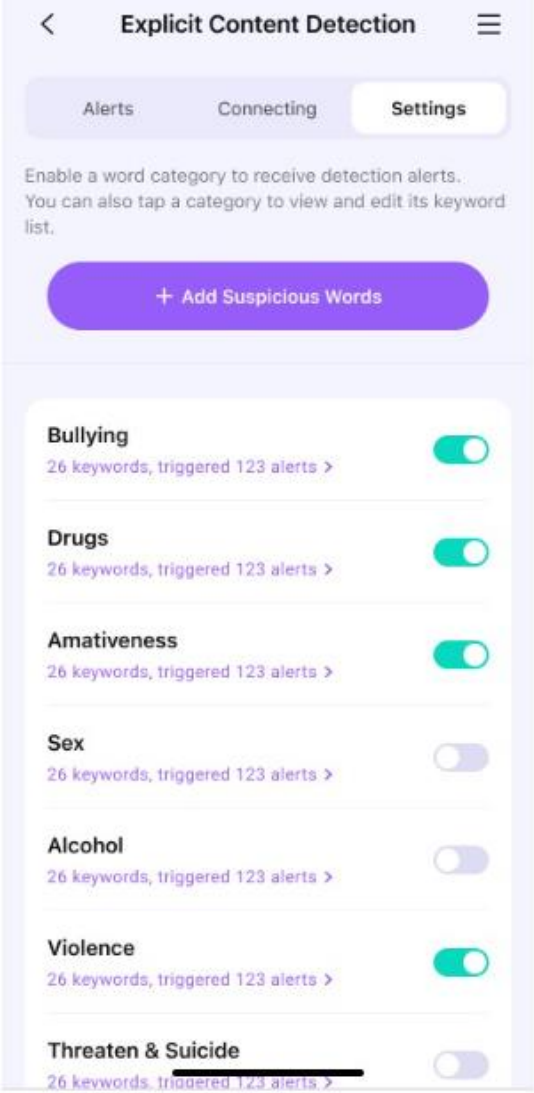


Ilustración 98 Famisafe. (2023, 06 de marzo). Configuración [Captura de pantalla] Recuperado de App móvil ver. 6.0

Después de 3 días de la prueba, puedes seguir utilizando la aplicación de control parental y tiempo de pantalla FamiSafe con una pequeña suscripción mensual.

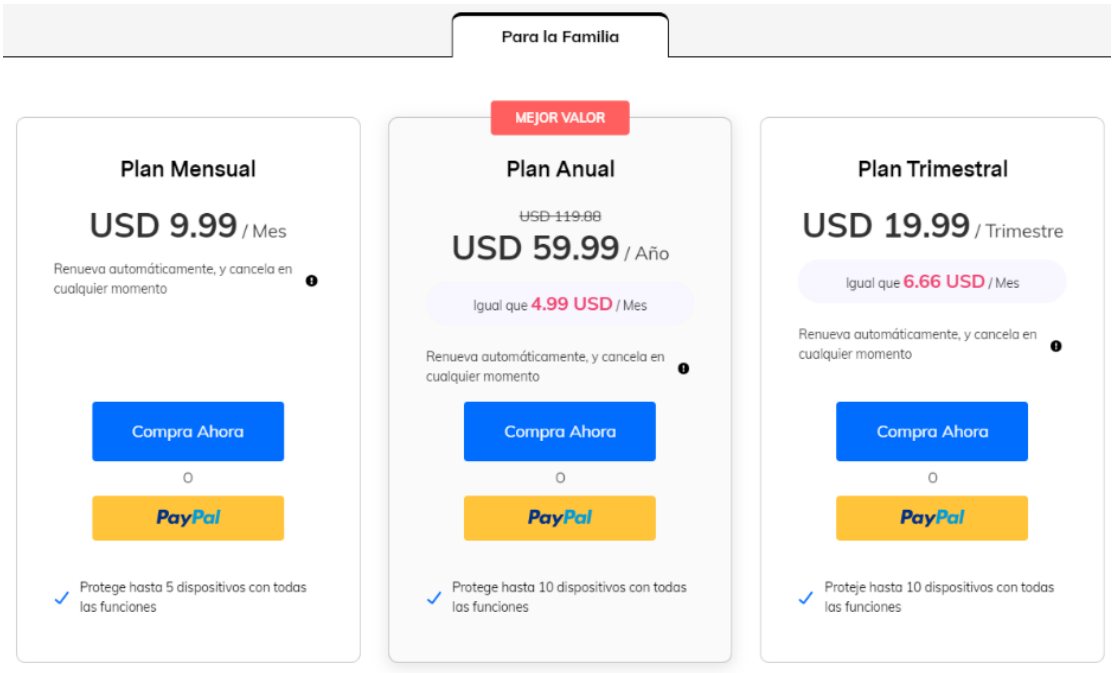


Ilustración 99 Famisafe. (2023, 06 de marzo). Precios suscripción [Captura de pantalla] Recuperado de App móvil ver. 6.0

3.4 Configuración de la herramienta control parental Norton Family

Norton Family tiene como propósito brindar navegación segura y monitoreada para los menores de edad. *Es una aplicación de pago*, y cuenta con una versión gratuita de 30 días. Su instalación se puede hacer en sistemas operativos como Windows, iOS y dispositivos Android.

Antes de iniciar la instalación y configuración, es necesario tener una cuenta en la página de Norton family

3.4.1 Registro en la página de Norton Family

Ilustración 100 V 7.3.1.1 captura de pantalla Inicio de sesión en la página de Norton

3.4.2 Instalación en dispositivo Android.

La aplicación se encuentra en la tienda de Google conocida como Play Store, la buscamos por su nombre para comenzar la instalación

Ilustración 101 V 7.3.1.1 captura de pantalla de Play store, aplicación Norton Family parental

3.4.3 Configuración inicial de la aplicación

Una vez instalada la aplicación, al ejecutar se despliega la siguiente información, leer los términos y pulsar Continuar.

Ilustración 102 V 7.3.1.1 captura de pantalla Aplicación Norton Family, menú de términos

La aplicación debe estar instalada en el dispositivo del mayor de edad y en el dispositivo del menor de edad.

3.4.4 Configuración en el dispositivo móvil del mayor de edad

La siguiente pantalla nos muestra dos opciones, para esta configuración elegir **Inicio de sesión (padre)**

Ilustración 103 V 7.3.1.1 captura de pantalla Aplicación Norton Family menú de configuración

Aparece la interfaz principal donde muestra los dispositivos sincronizados

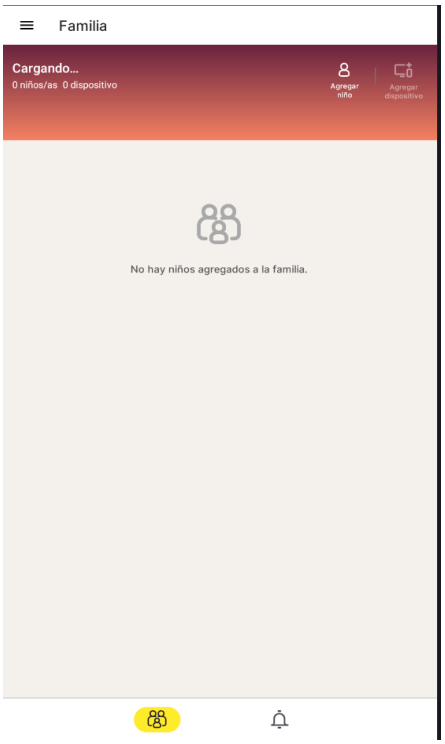


Ilustración 104 V 7.3.1.1 captura de pantalla Menú principal Norton Family

3.4.5 Sincronizar el dispositivo del menor de edad con el dispositivo del mayor de edad.

En el interfaz principal del dispositivo del mayor de edad, seleccionar *agregar niño*.

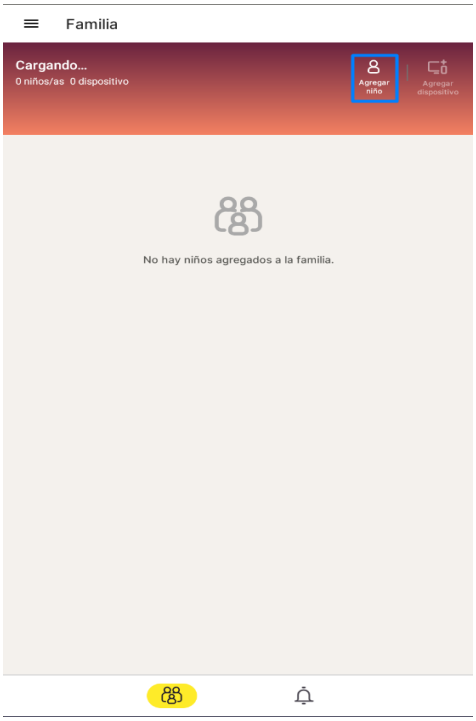


Ilustración 105 Manú principal de Norton Family

Aparece el siguiente menú donde se debe elegir el nombre del menor y el nivel de restricción, al igual que una foto de perfil opcional.

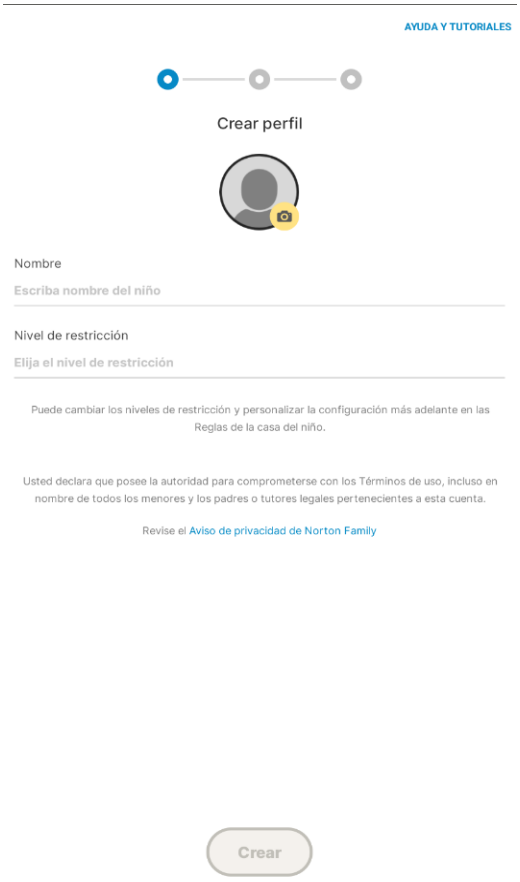


Ilustración 106 V 7.3.1.1 captura de pantalla, crear perfil en Norton Family

Ilustración 107 V 7.3.1.1 captura de pantalla nivel de restricción

Al llenar la información, seleccionar el sistema operativo del dispositivo del menor.

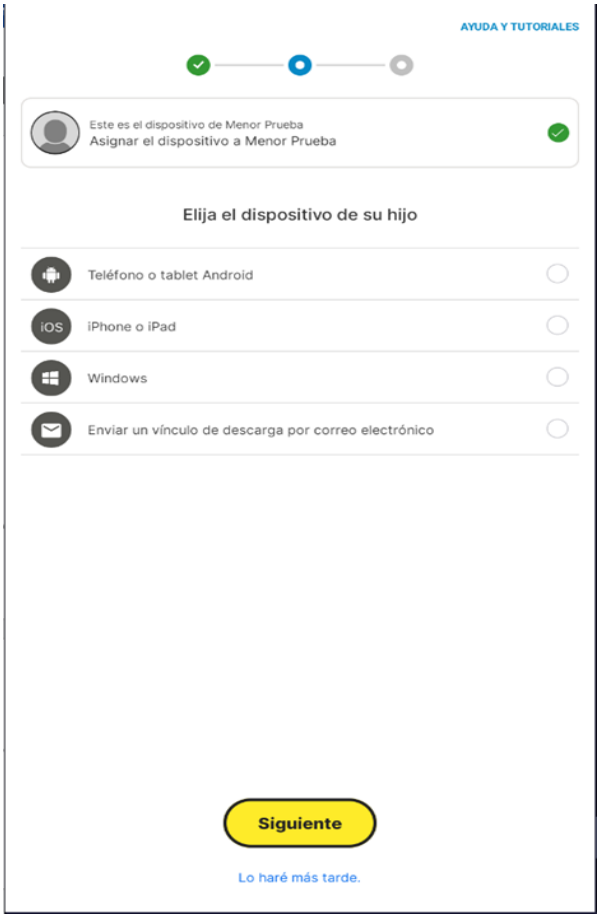


Ilustración 108 V 7.3.1.1 captura de pantalla Configuración de dispositivo móvil

Al pulsar siguiente sale un menú donde hay que ingresar un código que se genera en el dispositivo móvil del menor, al igual que un código QR para descargar la aplicación

Ilustración 109 V 7.3.1.1 captura de pantalla, Menú de sincronización de Norton Family

3.4.6 Configuración desde el dispositivo del menor

Al ingresar a la aplicación instalada en el dispositivo del menor, muestra el código que se va a utilizar para la sincronización

Ilustración 110 V 7.3.1.1 captura de pantalla, generación de código para la sincronización

Cuando ya se ingresó el código al dispositivo del mayor, automáticamente genera el siguiente menú

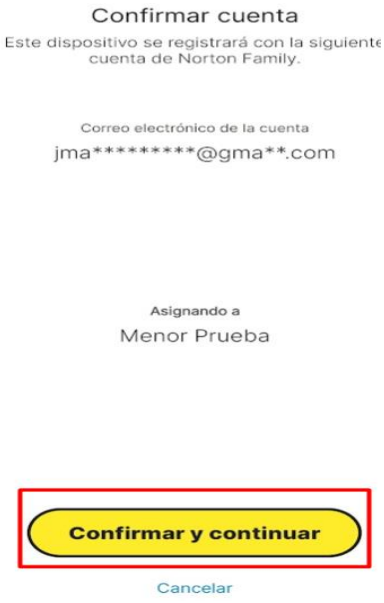


Ilustración 111 V 7.3.1.1 captura de pantalla, confirmación de cuentas sincronizadas

Se despliega el menú de permisos del dispositivo. Activar cada uno de los permisos.

Ilustración 112 V 7.3.1.1 captura de pantalla, permisos de dispositivos

Al terminar de activar los permisos del dispositivo, el mayor de edad ya tendrá el control del dispositivo del menor de edad.

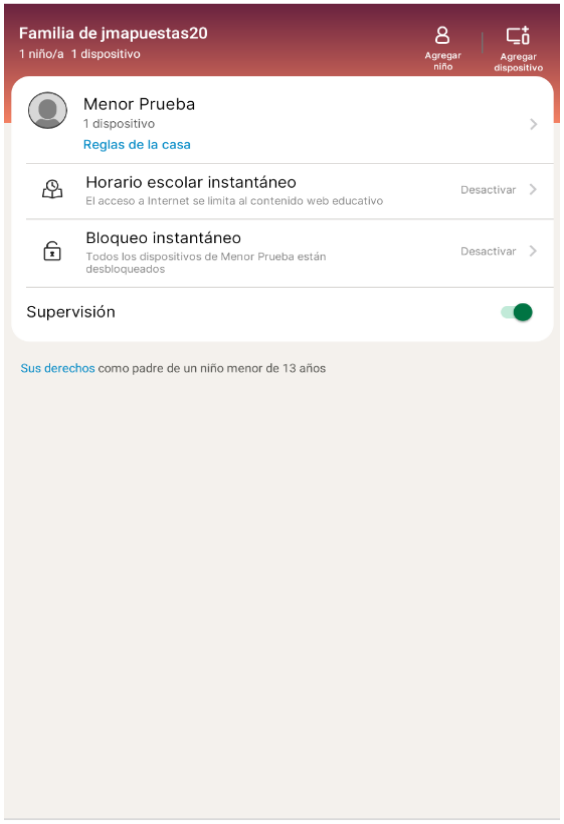


Ilustración 113 V 7.3.1.1 captura de pantalla, Menú principal Norton Family con usuario asignado

4 RUTAS PARA REGISTRAR LAS DENUNCIAS

4.1 Guía para realizar denuncias a través de la página de la Policía Nacional

Paso 1: Ir a la página https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

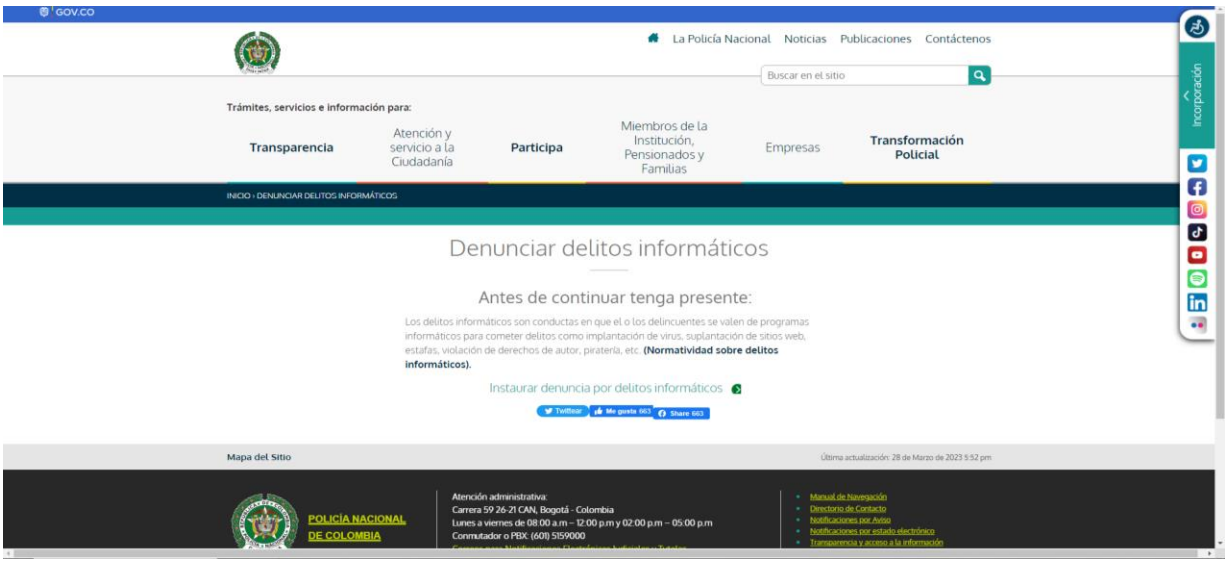


Ilustración 114 CAI Virtual. (2023, 10 de marzo). Página de denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 2: Dar clic en el enlace **Instaurar denuncia por delitos informáticos**

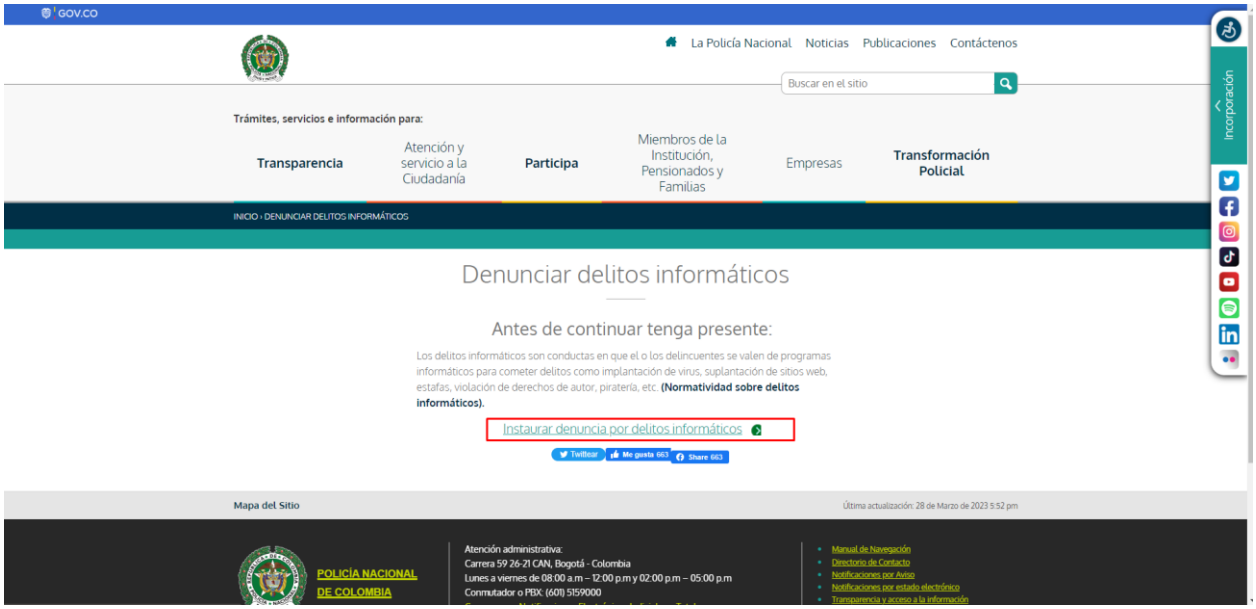


Ilustración 115 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 3: Dar clic en el botón **Denuncia virtual**

Ilustración 116 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 4: Leer y **Aceptar** los términos y condiciones

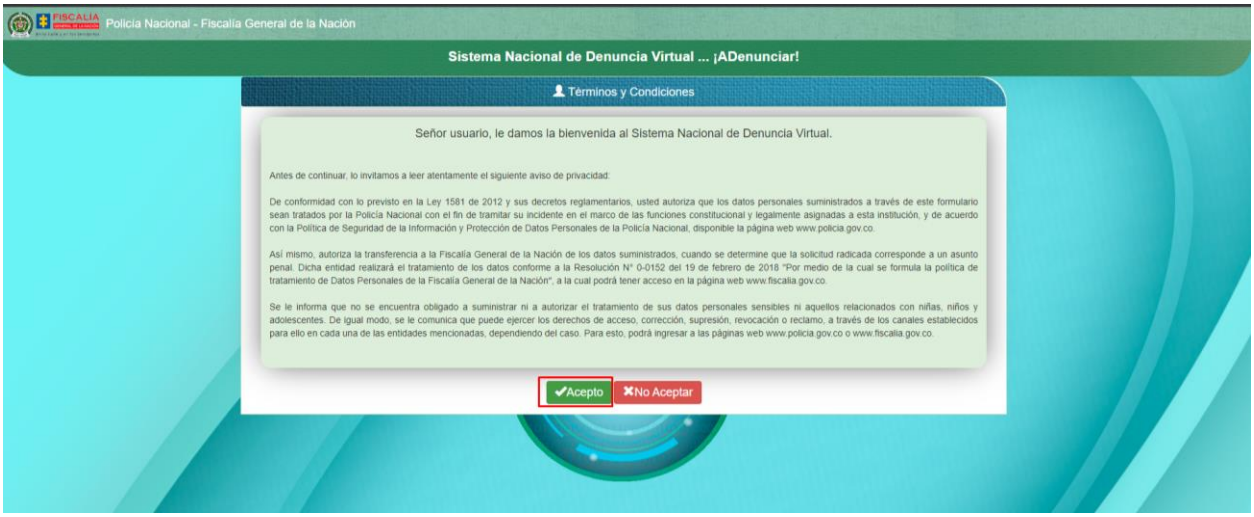


Ilustración 117 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 5: Dar click en el botón **Material con contenido de explotación sexual infantil**

Ilustración 118 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 6: Clic en **consultar normatividad,** leerla y clic **en continuar**

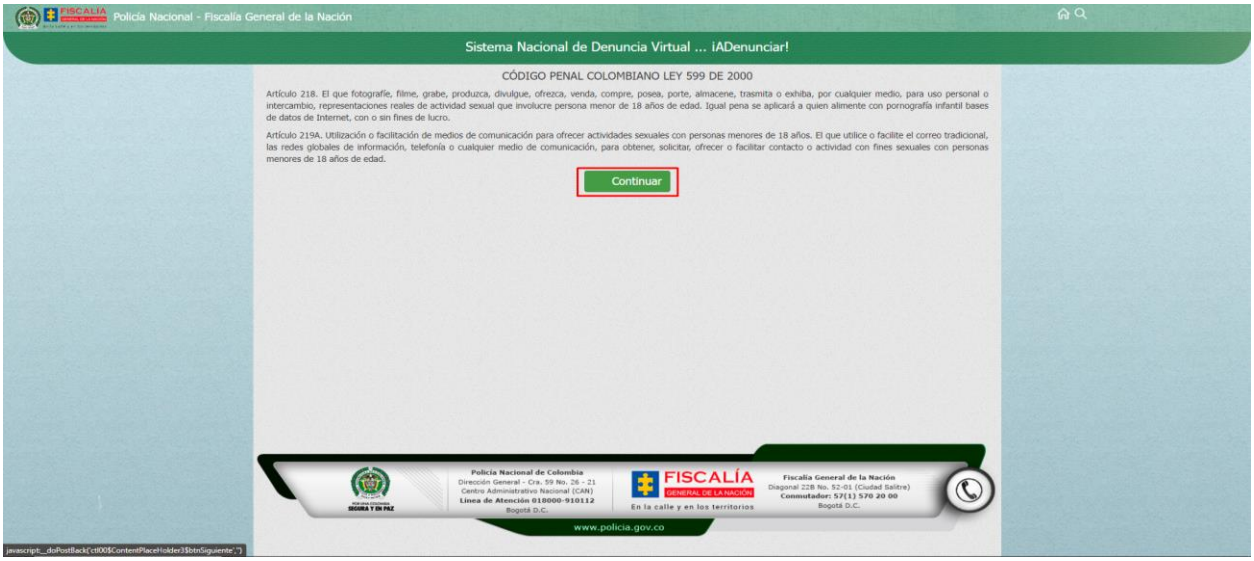


Ilustración 119 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 7: Conocer los **derechos** y **deberes** y dar click en **OK**

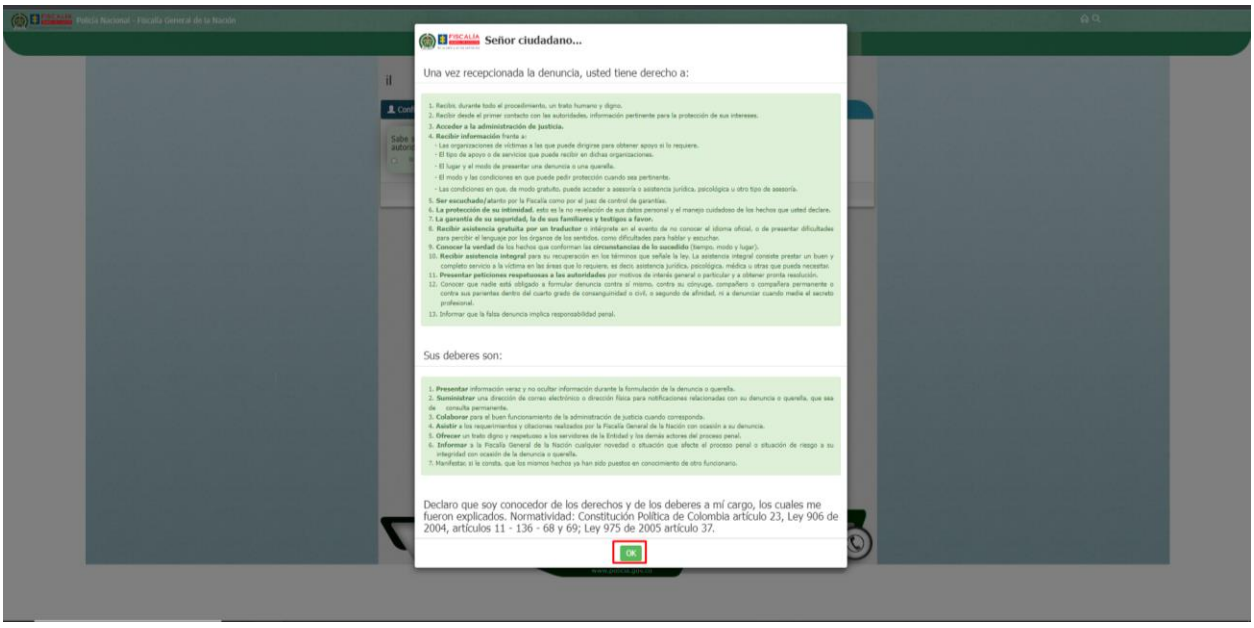


Ilustración 120 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 8: Contestar pregunta de acuerdo con lo sucedido.

Si la respuesta es **SÍ,** diligencie la información requerida y haga clic en **continuar.**

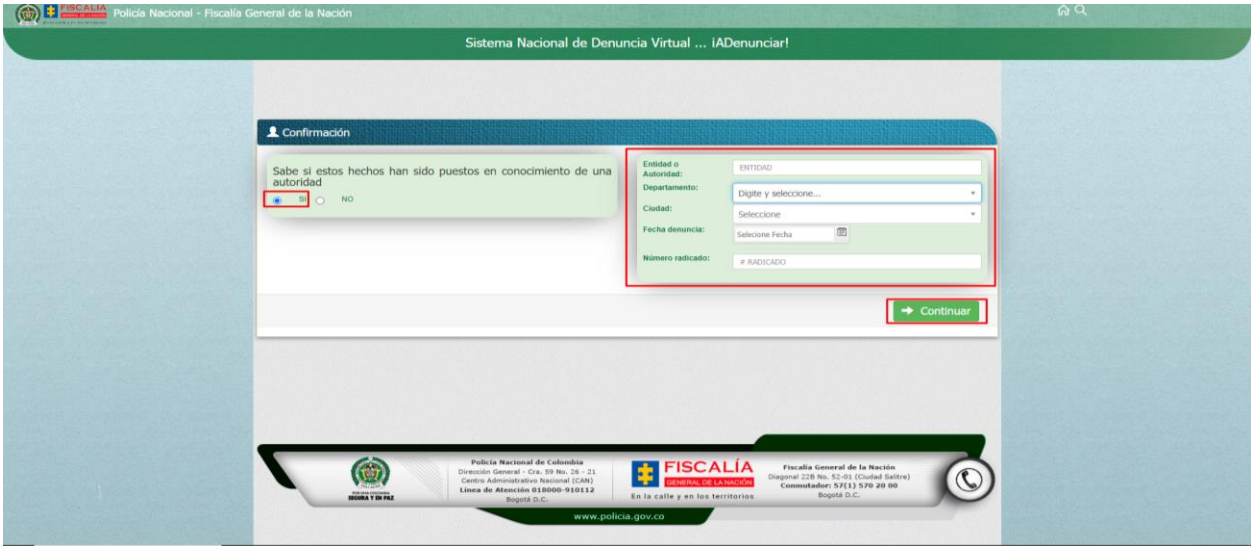


Ilustración 121 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Si la respuesta es **NO,** dar clic en **continuar**

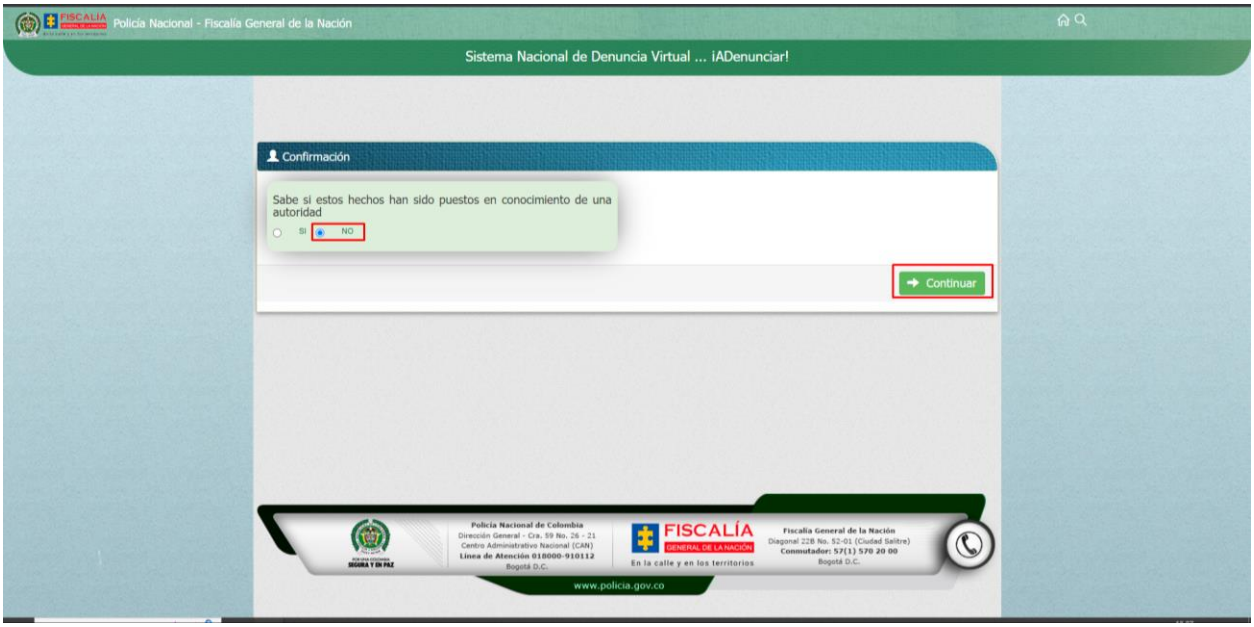


Ilustración 122 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 9: Diligenciar los datos personales del denunciante

Ilustración 123 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Clic en **validar**

Ilustración 124 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Clic en **continuar.**

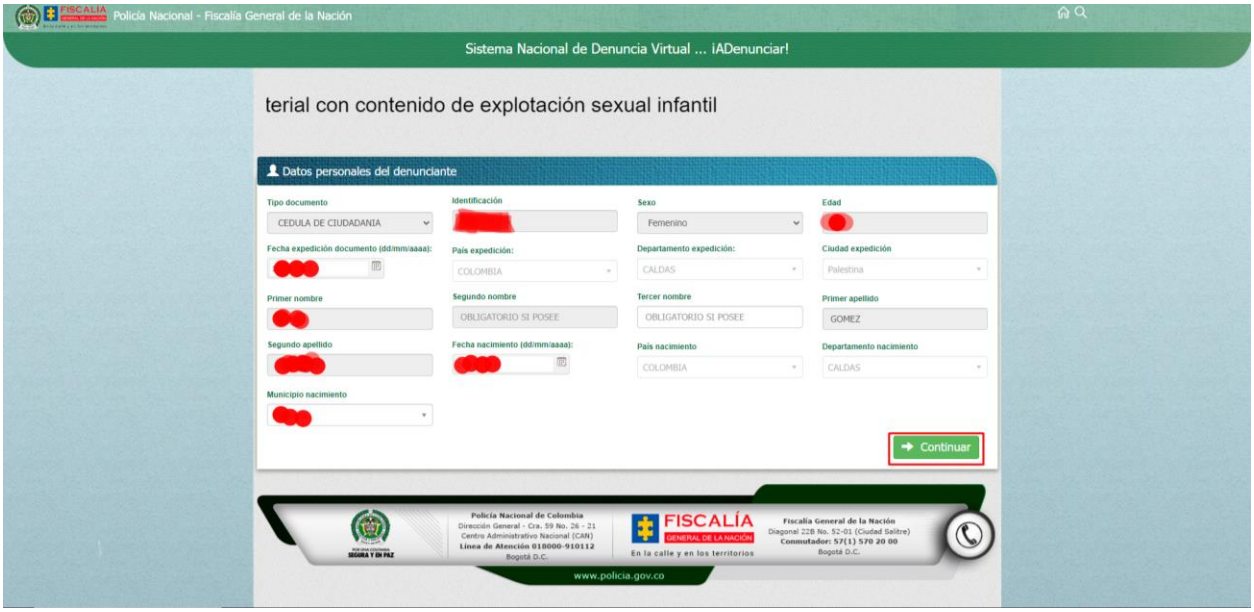


Ilustración 125 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 10: Diligenciar los datos generales y clic en **continuar.**

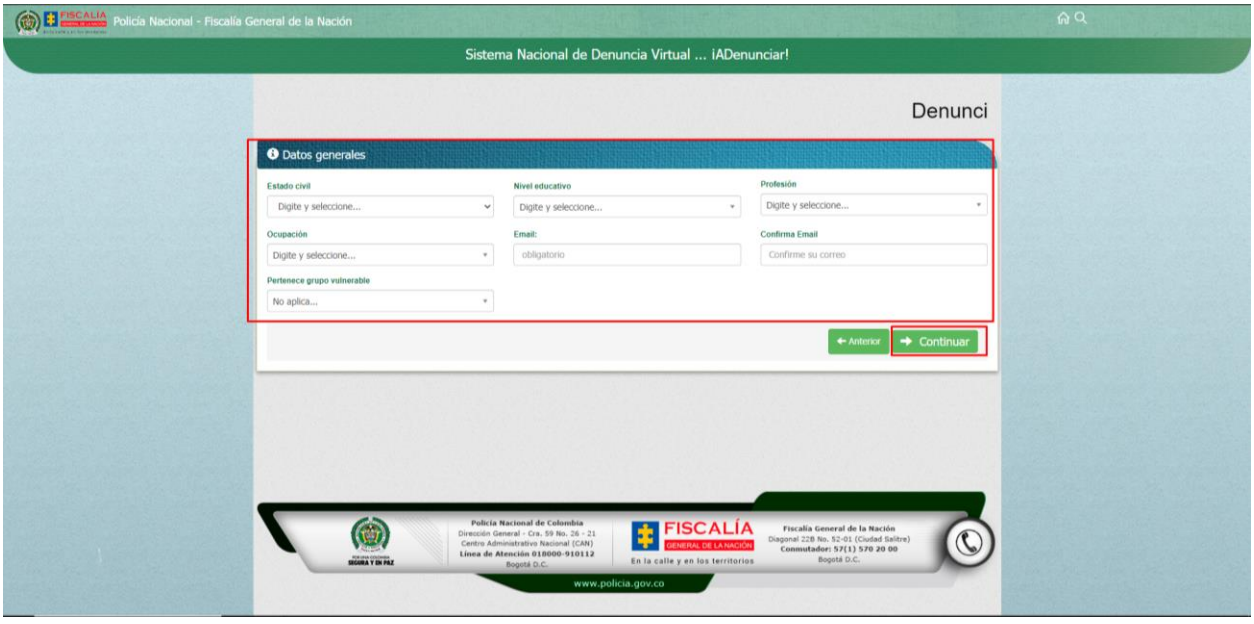


Ilustración 126 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 11: Diligenciar la información del domicilio y clic en **continuar**

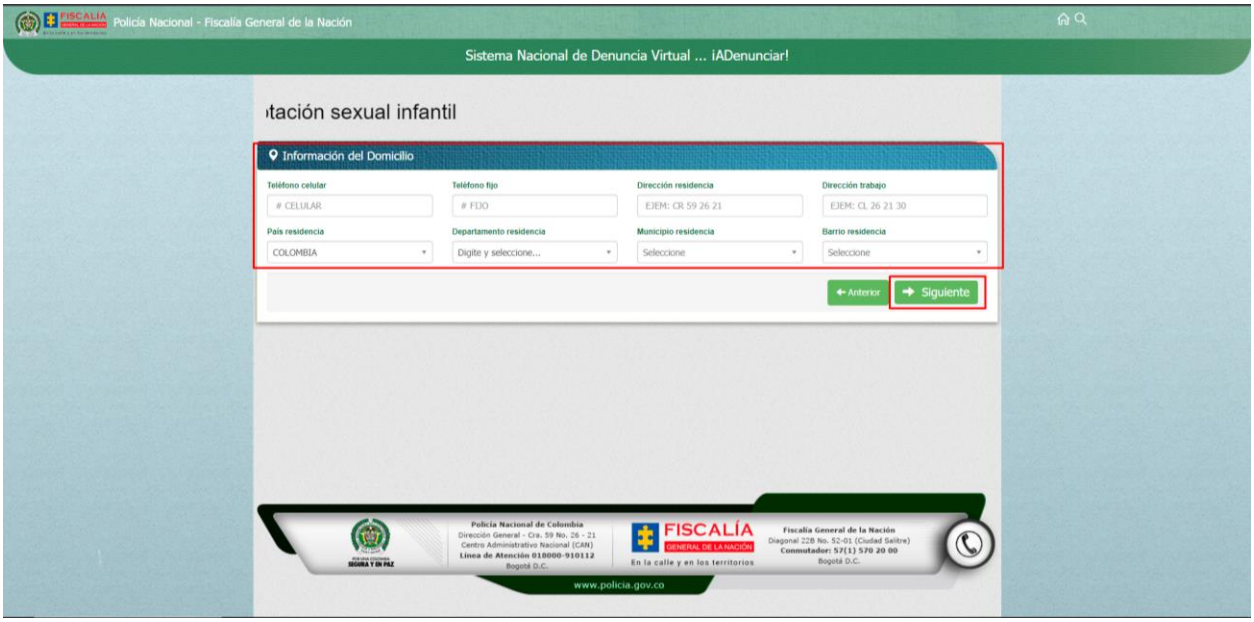


Ilustración 127 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 12: Leer información y clic en **OK**

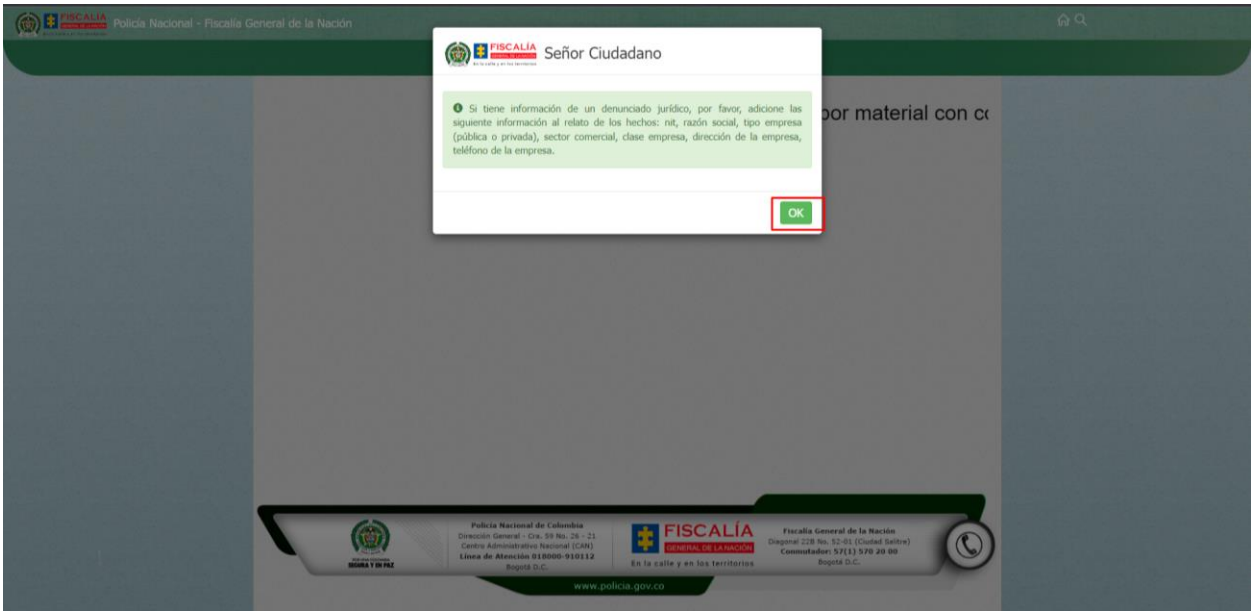


Ilustración 128 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Paso 13: Diligenciar toda la información acerca de los hechos y dar click en el botón **enviar.**

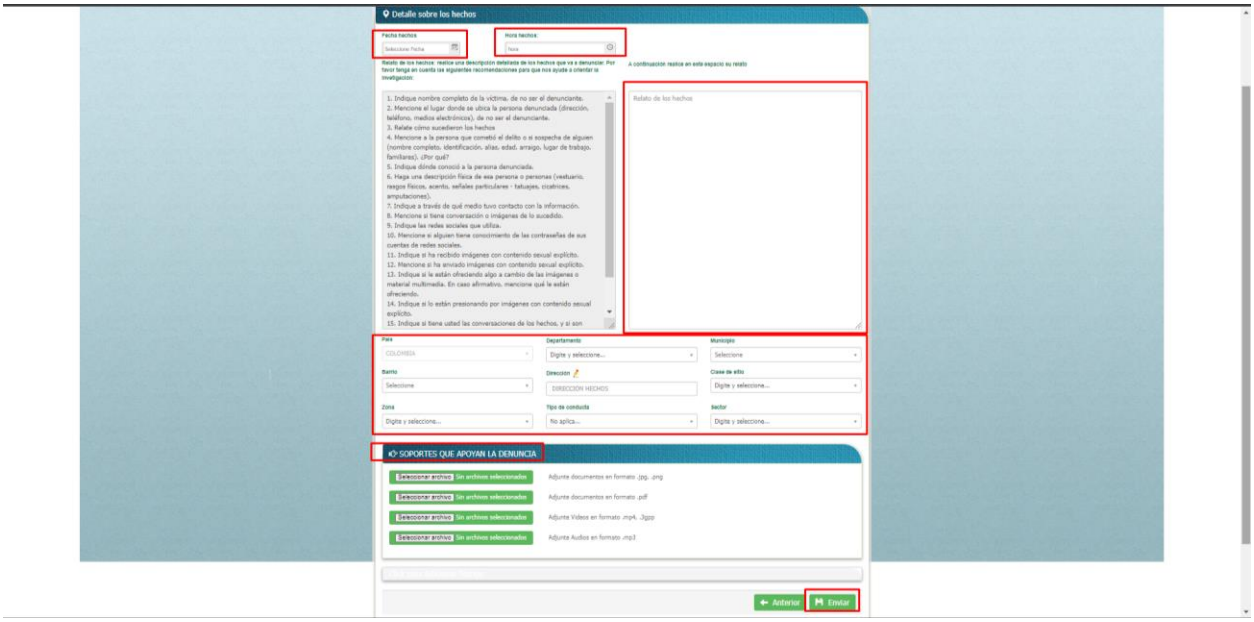


Ilustración 129 CAI Virtual. (2023, 10 de marzo). Denuncia delitos informáticos [Captura de pantalla]. Tomado de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

4.2 Guía para realizar denuncias por la aplicación Te protejo

Descargar la aplicación Te protejo en Google Play o App Store de acuerdo con el sistema del dispositivo que va a utilizar Android o IOS.

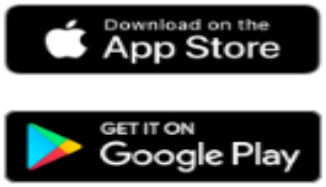


Ilustración 130 Descargas. (2023, 03 de marzo). Tienda de descargas [Captura de pantalla]. Recuperado de App móvil

Seleccionar el país en el que sucede el hecho a denunciar:

Ilustración 131 Te protejo. (2023, 03 de marzo). Configuración de país [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Seleccionar el tipo de delito que desea denunciar:

Ilustración 132 Te protejo. (2023, 03 de marzo). Selección del tipo de delito [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Seleccionar el tipo de delito que desea denunciar:

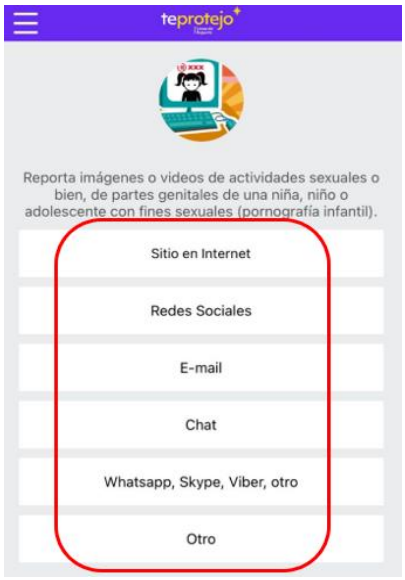


Ilustración 133 Te protejo. (2023, 03 de marzo). Selección de aplicación a reportar [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

Ingresar la información sobre el Sitio web, Red social, etc. de acuerdo con lo seleccionado en el paso anterior y finalmente seleccionar Enviar reporte:

Ilustración 134 Te protejo. (2023, 03 de marzo). Reportar material de explotación sexual [Captura de pantalla]. Recuperado de App móvil ver.1.89.0

5 REFERENCIAS

NortonLifeLock Inc. (s.f.). *Norton Family*. Obtenido de https://co.norton.com/products/norton-family

Webempresa Hosting España. (s.f.). *Control parental: qué aporta y cómo activarlo*. Obtenido de https://ciberprotector.com/blog/que-es-control-parental-como-activar/

AO Kaspersky Lab. (s.f.). *Cuida de tus hijos, incluso cuando no estés cerca*. Obtenido de https://latam.kaspersky.com/safe-kids

Denunciar delitos informáticos. (s.f.). Obtenido de https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Google LLC. (s.f.). *Controles parentales*. Obtenido de https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylinkhelper&hl=es_CO&gl=US

Instagram. (s.f.). Obtenido de https://about.instagram.com/es-la/safety#:~:text=Elige%20una%20contrase%C3%B1a%20%C3%BAnica%20y,el%20servicio%20de%20ayuda%20aqu%C3%AD

Llonch, E. (25 de 05 de 2021). *¿Qué son las redes sociales y cuáles son las más importantes?* Obtenido de https://www.cyberclick.es/numerical-blog/que-son-las-redes-sociales-y-cuales-son-las-mas-importantes

Meta. (s.f.). *Consejos de seguridad para proteger tu cuenta de WhatsApp*. Obtenido de https://faq.whatsapp.com/1095301557782068/

Wondershare. (s.f.). *FamiSafe Guía del usuario*. Obtenido de

https://famisafe.wondershare.com/es/user-guide/