HERRAMIENTAS Y/O MÉTODOS PARA PROTEGER A LA COMUNIDAD INFANTIL DE ATAQUES DE INGENIERÍA SOCIAL EN REDES SOCIALES.

KARINA SANDOVAL CAMELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

HERRAMIENTAS Y/O MÉTODOS PARA PROTEGER A LA COMUNIDAD INFANTIL DE ATAQUES DE INGENIERÍA SOCIAL EN REDES SOCIALES.

KARINA SANDOVAL CAMELO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Daniel Palomo
Director de trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
202

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mi familia, la cual me ha apoyado en todos los proyectos que he emprendido y gracias a ellos y a los valores que me enseñaron desde pequeña, es que hoy en día soy una persona capaz de asumir retos y responsabilizarme por mis acciones, buscando ser siempre un miembro útil de la sociedad.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, por darme la oportunidad de ser parte de su comunidad, y brindarme oportunidades para retarme a mí misma y conocer hasta donde puedo llegar; así mismo agradezco a mis asesores por todo su apoyo y comprensión a lo largo de la elaboración de este trabajo, quienes, con paciencia y cariño guiaron mis pasos para ayudarme a alcanzar los objetivos propuestos en este.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

AMENAZA: situación que puede desencadenar un daño y/o pérdida. En el presente trabajo van relacionadas con los peligros a los que se puede exponer la comunidad infantil

***BULLYING*:** se trata de un acoso reiterado a otra persona, una intimidación emocional y a veces física. Se pueden crear testimonios falsos o discriminar y mofarse de algunas características del individuo.

***CATFISHING*:** creación de cuentas o identidades falsas en redes sociales para que las personas compartan información con estos usuarios.

CIBERACOSO: consiste en intimidar a otra persona a través de plataforma virtuales y tecnologías de la información, con la intensión de dañar, humillar o difamar a la víctima mediante mensajes, rumores, vídeos entre otros.

CIBERDELINCUENTE: delincuente que comete sus delitos en entornos digitales.

CIBERCRIMEN: o ciberdelito en un concepto amplio son delitos que se presentan en el entorno digital y/o informático, son actividades que van en contra de la ley y tiene como objetivo causar daño, robar información, provocar pérdidas o impedir el correcto funcionamiento de sistemas informáticos.

CONTENIDO ILÍCITO: contenido que no está permitido de manera legal como la pornografía infantil.

CONTENIDO NOCIVO: contenido que puede ser legal, pero aun así puede ser dañino para el desarrollo de un menor, como el contenido violento.

ENTORNO DIGITAL: conjunto de plataformas y aplicación que permiten interactuar a la sociedad a través de la tecnología de la información en ambientes virtuales.

ESTUPRO: acceso carnal con menores entre 12 y 16 años, conseguido con engaños.

***FACEBOOK*:** es una red social que fue creada para poder mantener en contacto a personas, compartiendo información, noticias y contenidos audiovisuales con amigos y familiares.

***GROOMER*:** cibercriminal que practica el *grooming*

***GROOMING*:** tácticas de engaño que realizan los adultos para con fines de satisfacción sexual contra niñas, niños y adolescentes en el entorno digital

ICBF: Instituto Colombiano De Bienestar Familiar, entidad del gobierno que vela por la seguridad y derechos de los niños y adolescentes en Colombia.

INGENIERÍA SOCIAL: conjunto de métodos que usan los ciberdelincuentes con el fin de engañar a sus víctimas y lograr que den información personal de forma voluntaria.

***INSTAGRAM*:** "es una red social de compartir fotos y vídeos entre usuarios, con la posibilidad de aplicación de filtros"

***MACHINE LEARNING*:** definida por BBVA como: “euna rama de la inteligencia artificial que permite que las máquinas aprendan sin ser expresamente programadas para ello.”1

PEDERASTA: adulto que comete abuso sexual contra menores de edad (niños y niñas)

PEDÓFILO: persona que siente atracción sexual por menores de edad, puede tener o no contacto sexual con el menor, el cual puede ser o no mediante el abuso.

***PHISHING*:** delito de ingeniería social relacionado con suplantación de identidad, o hacerse pasar por una persona o entidad, con el fin de engañar a su víctima y obtener información personal de forma voluntaria.

PHONBIE: relacionados con riesgos de contenido, se refiere a la posible dependencia de dispositivos móviles.

PORNOGRAFÍA INFANTIL: representación visual de menores de edad en conductas sexuales implícitas, ya sea acciones individuales o con otros menores y/o adultos.

RECONOCIMIENTO DE PATRONES: es una disciplina que busca clasificar los elementos en categorías o clases. Esos reconocimientos pueden ser a través de aprendizaje supervisado, donde el sistema tiene un conjunto de referencia para clasificar la nueva información, o semi supervisado, que busca definir relaciones entre los elementos para definir categorías.

[1] BBVA. 'Machine learning': ¿qué es y cómo funciona? [En línea]. BBVA - Tecnología - Inteligencia Artificial 08 de noviembre de 2019 (Recuperado en marzo de 2023) Disponible en https://www.bbva.com/es/innovacion/machine-learning-que-es-y-como-funciona/

REDE SOCIALES: estructuras sociales formadas en internet, donde las personas se conectan a partir de intereses comunes, donde se crean relaciones y se comparten contenidos.

RETO VIRAL: videos o acciones que se hacen populares por internet e invitan a los usuarios a hacer lo mismo y compartirlo por redes sociales.

RIESGO: posibilidad que una amenaza se materialice.

RIESGOS DE CONDUCTA: riesgos a los que se ven expuestos los niños y que pueden alterar su comportamiento de forma negativa.

RIESGOS DE CONTACTO: riesgo a los que los niños se ven expuestos por la conexión con personas que pueden engañarlos y abusar de ellos.

RIESGOS DE CONTENIDO: riesgo de que un niño sea expuesto a contenidos no apropiados, como aquellos de alto contenido sexual o violencia.

SEXTING: envío de mensajes de contenido sexual, generalmente imágenes, producidas por el mismo remitente y enviados a través de teléfonos inteligentes.

SEXTORSIÓN: chantaje a una persona, para conseguir una acción o dinero de esta, a través de la amenaza publicar fotos intimas de la víctima en diversas plataformas virtuales, o envío a personas conocidas.

***SUGGAR DADDY /MOMMY*:** persona mayor que busca jóvenes y complace sus caprichos con dinero, regalos u otros, a cambio generalmente de favores de carácter sexual.

TIC O TECNOLOGÍAS DE LA INFORMACIÓN: definidas como todos aquellos recursos y herramientas utilizados en el proceso, análisis, administración, distribución de la información a través de elementos tecnológicos.

TRATA DE PERSONAS: delito que viola los derechos humanos, se trata cuando una persona captura o secuestra a otra para posteriormente ser explotada en distintos trabajos y así el atacante obtiene ganancias.

UNICEF: *United Nations International Children's Emergency Fund*, organización internacional que busca la seguridad y la protección de los derechos de la infancia y adolescencia.

***VAMPING*:** relacionado con los riesgos de conducta, se define como la incapacidad de desconectarse de internet a través del teléfono móvil, en horarios nocturnos.

***WHATSAPP*:** "es una aplicación descargable que utiliza la conexión a Internet (Wi-Fi) de su teléfono para enviar mensajes, fotos, vídeos o archivos. También permite a los usuarios hacer videollamadas en tiempo real (como FaceTime en iOS)"

WEB 1.0: donde los dueños de los sitios web tienen pleno control sobre ellas, tanto de la información que exponen como del acceso y nivel de interactividad que quieren fomentar.

WEB 2.0: una tendencia en el uso de las páginas web, donde el usuario es el centro de la información y generador de contenidos.

RESUMEN

Hoy en día tras la situación presentada por la pandemia, las tecnologías de la información sufrieron un crecimiento exponencial y acelerado, así mismo lo hizo la ciberdelincuencia; la comunidad infantil al igual que otras comunidades, también están expuestos a riesgos y amenazas digitales, identificarlas y tomar medidas necesarias para proteger a los niños se hace necesario en una realidad en que las redes sociales se han vuelto esenciales en la cotidianidad de la sociedad. El presente proyecto pretende abordar tres aspectos importantes acerca de la ciberseguridad infantil en el uso de las redes sociales, la primera es la identificación de las amenazas a los que se ven expuestos los niños en el entorno digital, la segunda, examinar la eficacia de los métodos actuales para protegerlos contra estos, para finalmente, proponer estrategias tecnológicas que ayuden a mejorar esta seguridad. Dado que el termino herramientas tecnológicas aborda una gran cantidad soluciones, se describirán la implementación de medidas de control en aquellos elementos que hacen parte de la conexión al mundo digital y que permiten el ingreso a redes sociales y otros contenidos, como navegadores, aplicaciones y otros.

ABSTRACT

Today, after the situation presented by the pandemic, information technologies suffered exponential and accelerated growth, as did cybercrime; The children's community, like other communities, are also exposed to risks and digital threats, identifying them, and taking the necessary measures to protect children is necessary in a reality in which social networks have become essential in the daily life of society. The present project aims to address three important aspects about child cybersecurity in the use of social networks, the first is the identification of the threats to which children are exposed in the digital environment, the second is to examine the effectiveness of current methods to protect them against them, and finally, to propose technological strategies that help improve this security. Since the term technological tools addresses many solutions, the implementation of control measures will be described in those elements that are part of the connection to the digital world and that allow access to social networks and other content, such as browsers, applications and others.

INTRODUCCIÓN

La comunidad infantil siempre ha tenido que enfrentar riesgos de acoso, abuso y explotación sexual, dichas amenazas a su integridad han evolucionado a la par de las tecnologías y hoy se encuentran en entornos digitales como las redes sociales, volviéndose aún más agresivas y llegando con más facilidad a ellos. El número de denuncias durante la reciente cuarentena ha superado los umbrales normales en más del 100%, lo cual pone en evidencia una realidad en la que los niños están expuestos a diferentes riesgos en los entornos digitales y para los cuales, al parecer no se cuentan con métodos o herramientas eficaces para protegerlos. El reconocimiento de vectores, la forma en que se manifiestan estos ataques y la identificación de las amenazas más recurrentes, es la primera etapa para la elaboración de una estrategia que permita mitigar el riesgo de estos, así mismo la identificación de las herramientas y métodos actuales permite evaluar cuales son las deficiencias y fortalezas de la forma en que se ha buscado hacer frente a estas amenazas, esto con el fin de proponer nuevas estrategias que permitan mitigar los riesgos que corren los niños en los entornos virtuales donde interactúan. El siguiente trabajo se enfoca en aquellas amenazas que afectan la comunidad infantil, para desde nuestro campo de estudio de la seguridad informática, poder aportar para el reconocimiento del problema y generar propuestas que puedan ayudar a mejorar la seguridad de la comunidad infantil en las redes sociales.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Gracias a la pandemia hubo un aumento significativo en el uso de las tecnologías de la información y por consecuencia de las redes sociales, así mismo la ciberdelincuencia creció con estas y aunque poco a poco se ha ido normalizando la situación, las redes sociales y el internet ya se convirtieron en un aspecto elemental en la vida de las personas. Según Machado [2], entre el año 2020 y 2021 años de pandemia, los menores de edad tuvieron mayor acceso a internet y a dispositivos electrónicos, cambio social que también se evidenció en un aumento en casos de explotación sexual en niños y adolescentes en entornos digitales; En Colombia durante el 2021 se registraron 28.000 casos de explotación sexual en menores de edad mientras que en 2020 según la línea Te Protejo fue de 21.864 denuncias; hasta febrero de 2022 ya se habían registrado 2.282 casos, de los cuales el 97.6% fueron identificados en los entornos digitales.

La comunidad infantil una de las más vulnerables, aunque no era ajena al mundo digital, encontró en las redes sociales una oportunidad para mantener conexión con el mundo, y por consecuencia, el tiempo que pasaron conectados a internet aumento; esta comunidad no es ajena a los riesgos y amenazas que habitan en internet, y ha sido una de los más afectados por ciberdelincuentes que además los ataques ya conocidos de ingeniería social para el robo de información, también se ven expuestos a predadores sexuales que usan estos medios para llegar a sus

[2] MACHADO AMAURY. Casos de abuso sexual infantil en entornos digitales aumentó en pandemia. [En línea] Diario del Huila. 21 de febrero de 2022. (Recuperado en: 20 de noviembre de 2022) Disponible en: https://diariodelhuila.com/casos-de-abuso-sexual-infantil-en-entornos-digitales-aumento-en-pandemia/

víctimas. En Argentina, por ejemplo, según un artículo de Micucci Mario[3] comenta que el abogado especializado en delitos informáticos Daniel Monastersky, público en su cuenta de Twitter que durante la cuarentena los ciberdelitos crecieron un 500% durante la cuarentena, encabezando las denuncias de *grooming*, seguido por la explotación sexual infantil y la difusión de imágenes íntimas; en España la guardia civil también se encontró con un crecimiento del 507% en el tráfico de vídeos pedófilos, en este mismo país un artículo del portal ABC[4] registra que el *grooming* ha aumentado en un 410% en el AÑO 2019. En un artículo la FM indica que "En el año 2022 en Colombia, el Centro Cibernético de la Policía Nacional, registró más de 14.500 sitios de internet con perfiles en redes sociales dedicados a la venta de imágenes de abuso sexual." 5 Un vergonzoso lugar ocupa Colombia según la Red Contra el abuso Sexual[6] que coloca al país como uno de los que más produce pornografía infantil en América Latina.

Se puede decir que este incremento de casos, que puede ser aún mayor ya que muchos delitos no se denuncian, demuestran que los métodos que están siendo usados para prevenir estos ataques no han sido lo suficientemente eficaces para proteger a los niños; se observa que las medidas para contrarrestar estas amenazas van más dirigidas a la educación, y la responsabilidad de proteger a los niños se ha delegado casi en un 100% a sus padres, sin evaluar posibles soluciones que puedan ofrecer desde las misma tecnologías de la información. Las redes sociales buscan más soluciones para riesgos de contenido, por lo que se puede observar en un

3 MICUCCI MARIO. Grooming: una problemática que crece durante la cuarentena. [En línea] Portal Welivesecurity. 20 de mayo de 2020. (Recuperado en agosto de 2021) Disponible en: https://www.welivesecurity.com/la-es/2020/05/20/grooming-crece-durante-cuarentena/

4 ABC. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años. [En línea] Sección Padres e Hijos. 10 de marzo de 2019. (Recuperado en agosto de 2021) Disponible en: https://www.abc.es/familia/padres-hijos/abci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ffamilia%2Fpadres-hijos%2Fabci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html

5 CEBALLOS PAULA. Grooming, el peligro que acecha a los menores de edad en internet [En línea] LA FM. (Recuperado en abril de 2023) Disponible en https://www.lafm.com.co/tecnologia/grooming-el-peligro-que-asecha-a-los-menores-de-edad-en-internet

6 RED CONTRA EL ABUSO SEXUAL Los peligros de la era digital. [En línea] 2020. (Recuperado en agosto de 2021) Disponible en: https://redcontraelabusosexual.org/los-peligros-de-la-era-digital/

artículo de Camargo[7] las redes sociales solicitan ayuda a los mismos usuarios para reportar contenidos inadecuados que incumplan las normas de convivencia de la comunidad, así mismo *Facebook* según se evidencia en un artículo en el Perfil[8] cuenta con algoritmos que permiten identificar contenidos inapropiados para posteriormente bloquearlos. Sin embargo, estos son controles generales para riesgos de contenido, más no se evidencian medidas específicas para la comunidad infantil o los delitos de ingeniería social asociados a ellos.

1.2 FORMULACIÓN DEL PROBLEMA

Pregunta: ¿Cuáles son los métodos o herramientas que existen actualmente en las redes sociales para proteger a la comunidad infantil de los ataques de ingeniería social a los que se exponen?

[7] CAMARGO MARIA DEL PILAR. Reportar contenidos inapropiados en redes sociales. ¿Para qué sirve? [En línea] El colombiano 19 de marzo de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.elcolombiano.com/tendencias/reportar-contenidos-inapropiados-en-facebook-instagram-y-twitter-DD14717444

[8] PERFIL. Cómo Es El Algoritmo Que Usa Facebook Para Controlar Contenido Inapropiados. [En línea] 20 de mayo de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.perfil.com/noticias/tecnologia/como-es-el-algoritmo-que-usa-facebook-para-controlar-contenidos-inapropiados.phtml

2 JUSTIFICACIÓN

Las tecnologías de la información, además de ser herramientas para mejorar el trabajo, la educación y la interacción social, también están siendo explotadas por ciberdelincuentes para cometer todo tipo de crímenes. La comunidad infantil, también se ve expuesta a riesgos y amenazas cada vez que hacen uso de las redes sociales, los niños no son ajenos a ataques de ingeniería social que buscan robar su información o dañar su integridad física y/o mental. Según el portal ACIS Asociación colombiana de ingenieros de sistemas[9] luego de la pandemia, hubo un aumento en el tiempo promedio en que niños y adolescentes entre 9 y 16 años pasan al frente de una pantalla, pasando de 3 horas 31 minutos a 5 horas, acompañada de un aumento en el uso de redes sociales, que encabeza Facebook, seguida de youtube y luego Instagram, e indicando que la mayoría de estos usuarios menores de edad no conoce como hacer los ajustes de privacidad de estas plataformas; pero este aumento en el uso de redes sociales por parte de la comunidad infantil también está acompañado de un aumento de ciberacoso y discurso de odio. Se considera que los jóvenes son el grupo de edad más conectado actualmente a la red, siendo casi el 71% en comparación con el 48% de la población total. La mayoría de los niños aún no son cocientes de los riesgos a los que se exponen en los entornos digitales, convirtiéndose en potenciales víctimas para ser explotadas por ciberdelincuentes. Pasar más tiempo en plataformas virtuales los expone al uso indebido de su información privada, acceso a contenido perjudicial y acoso cibernético. Aunque Internet ha sido una herramienta para compartir conocimiento, desarrollar la creatividad y compartir experiencias con grupos afines también ha expuesto a los niños a material sexual implícito, cuestiones de

[9] ACIS. ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. Internet por la pandemia [En línea]. Enero 20 de 2021. (Recuperado en abril de 2023) Disponible en: https://www.acis.org.co/portal/content/noticiasdelsector/en-promedio-los-ni%C3%B1os-y-ni%C3%B1as-aumentaron-tres-horas-su-tiempo-conectados-internet-por-la

dependencia y adicción a las pantallas, mensajes de odio, y se ha convertido en una nueva línea para el acoso contra los niños.

La protección de la comunidad infantil en el entorno digital, debe ser un esfuerzo coordinado, de la sociedad civil, las autoridades y los responsables de la ciberseguridad. La identificación de los riesgos a los que se ven expuestos, la perfilación de los ciberdelincuentes y la forma en que implementan sus ataques hace parte de las necesidades actuales para identificar formas de contrarrestar estos ataques, esto permite evaluar las herramientas para prevenir las amenazas y las políticas de seguridad actuales de las redes sociales para identificar los puntos fuertes y las falencias de estas en la detección y prevención de amenazas, para proponer métodos que puedan mejorar seguridad de la comunidad infantil.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar los métodos y/o herramientas que existen en las redes sociales para proteger la comunidad infantil de los ataques presentes en el entorno digital, mediante la revisión sistemática de literatura especializada para identificar falencias que puedan ser minimizadas con la implementación de soluciones tecnológicas existentes.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer los tipos de ataque de ingeniera social a los que se expone la comunidad infantil al usar redes sociales, a través de una revisión sistemática de informes realizados por diversas organizaciones que protegen el bienestar infantil con el fin de identificar cuáles son los más recurrentes y cómo es su modus operandi.
- Examinar los métodos actuales que se utilizan las redes sociales para garantizar la seguridad de sus usuarios mediante la revisión de las guías políticas de seguridad y controles para la comunidad infantil publicadas en sus portales para identificar los puntos fuertes y falencias de estas.
- Justificar la necesidad de proteger en el ciberespacio a la población infantil, a partir de estadísticas y casos registrados en plataformas digitales de gobierno.
- Proponer medidas o estrategias de contingencia que permitan mejorar la seguridad infantil en entornos digitales, mediante el uso y apropiación de herramientas y/o métodos existentes en el mercado.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Los riesgos que corre la comunidad infantil en el mundo digital se pueden clasificar en tres categorías, tal como lo indica un artículo del ICBF:

Riesgos de contenido: en lo referente a contenido inapropiado al que puede ser expuesto como imágenes pornográficas o violentas, mensajes de discriminación, odio o racismo o sitios que promuevan conductas que afectan su integridad física o mental como que susciten a autolesionarse, al suicidio o conductas como la bulimia o la anorexia.

Riesgos de conducta: cuando el niño interactúa con otras personas terminando involucrado en comportamientos peligrosos como el ciberacoso, definido como acciones delibradas y repetitivas para provocar daño a otra persona mediante contenido negativo o falso; el *sexting* relacionado con el envío de material erótico y sexual a través de recursos tecnológicos y redes sociales; y la ciberdelincuencia como el uso desmedido de dispositivos electrónicos.

Riesgos de contacto: los que se producen cuando un niño tiene una interacción peligrosa con un adulto.
Este último riesgo de contacto es el que más se relaciona con el concepto de ataque de ingeniera social, que implica engañar a una persona con el fin de robar información personal o persuadirlo para realizar alguna acción que vaya en contra de su propio beneficio.
Entre los riesgos de contacto se tiene el *phishing* o suplantación de identidad, el cual consiste en pasarse por otra persona o entidad para engañar a su víctima y robar su información y el *grooming* en la cual el ciberdelincuente crea también

perfiles falsos para ganarse la confianza de un menor para manipularlo y así involucrarlo en actividades sexuales.

Estos riesgos pueden desembocar en daños más allá del daño de reputación del menor, sino que también puede afectarlos psicológicamente, hacerlos víctimas de abuso sexual, explotación comercial, chantaje y en casos extremos trata de personas y homicidio.

4.2 MARCO CONCEPTUAL

4.2.1 **Revolución digital.** Los grandes avances tecnológicos van más allá de la continuidad de la tercera revolución: la revolución industrial, sino el inicio de la cuarta; una revolución que según Schwab Kalus[10] transformará la forma en que vivimos, nos relacionamos y trabajamos; cambios que deben involucrar no solo al sector privado o político, sino al sector público, el académico y el civil; esta revolución es una sinergia de tecnologías que desdibujan las fronteras entre lo físico y lo digital. Una revolución que a nivel de cada individuo afecta su identidad, su sentido de privacidad, sus hábitos de consumo, la forma en que se desarrolla la educación, las habilidades, el tiempo dedicado al trabajo y al descanso, la forma en que se conoce a la gente y así mismo como se cultivan las relacione entre ellas.
Una era en la que el ser humano puede con ayuda de la tecnología ir más allá de sus capacidades actuales y mejorar su calidad de vida, pero que, así como ofrece ventajas, también presenta un abanico de amenazas y peligros para los cuales se deben desarrollar estrategias y herramientas para contenerlos.

[10] SCHWAB, KLAUS. La Cuarta Revolución Industrial. [En línea] 2020. Futuro Hoy, 1(1), 06–10. DOI: https://doi.org/10.52749/fh.v1i1.1 (Recuperado en marzo de 2023) Disponible en: http://ojs.ssh.org.pe/index.php/Futuro-Hoy/article/view/1/118

4.2.2 **El motor de la era digital.** Aunque el internet y los dispositivos digitales son los medios utilizados en esta era, es en realidad “la información” el eje en el cual gira la revolución digital. La información se ha convertido en el bien más preciado tanto de las empresas y entidades como del individuo común. Mientras las empresas deben proteger bases de datos con información sensible, las personas del común deben resguardar sus datos personales como datos de contacto, números de tarjetas, imágenes, entre otros. Los niños a su vez pueden carecer de cuentas bancarias o datos que puedan ser atractivas para el ciberdelincuente común, sin embargo, comparten su propia información personal, sus gustos, sus imágenes, permitiendo que personas malintencionadas utilicen esta información para acercarse a ellos y manipularlos para sus intereses personales.

4.2.3 **Los peligros de la era digital para la comunidad infantil.** Así como la revolución digital ha permitido un gran avance en cuanto a tecnología y comunicación, también han surgido amenazas y riesgos relacionados al uso de internet y la tecnología de la información. Las empresas se enfrentan en reiteradas ocasiones a ataques que pretenden afectar sus sistemas informáticos y al robo y/o secuestro de su información y bases de datos; los adultos son víctimas de ataques de ingeniería social y virus para el robo de su información personal y a partir de esta ser víctimas de estafas y robos; los niños por su parte encontraron el equivalente digital de las amenazas que encontraban en su vida diaria, sin embargo esta equivalencia resulto ser inclusive más peligrosa.

El acoso por parte de sus pares y las agresiones sexuales por parte de adultos también evolucionaron en este nuevo mundo. Según un artículo del portal Heather R. Hayes[11] “Los estudios muestran que las víctimas del acoso cibernético suelen ser las mismas personas que sufren el acoso tradicional. Sin embargo, tal vez dado que no hay respiro en el hogar, el acoso cibernético parece más peligroso psicológica y emocionalmente que otras formas”, el *ciberbullying* cuenta ahora con

[11] HAYES HEATHER. The Evolution of Cyberbullying in a Digital era. [En línea] 18 de marzo de 2020. (Recuperado en 21 de noviembre de 2022) Disponible en: https://www.heatherhayes.com/cyberbullying/

una plataforma que le permite llegar a más personas para hacer público contenido y con características que le permiten al atacante permanecer en el anonimato, provocando mayores tasas de depresión, ansiedad e inclusive suicidios que el acoso tradicional.

Por su lado, los agresores sexuales y pedófilos encontraron una forma más eficaz de llegar a sus víctimas, formas más elaboradas de engañarlas e inclusive una forma más sencilla de compartir su contenido con otros agresores y con un gran mercado de demanda de pornografía infantil.

En los últimos años se ve un aumento alarmante en el delito denominado *child grooming* o *grooming,* en su trabajo de investigación Pillajo Diego indica que "ha venido evolucionando y configurándose en diferentes tipos de conductas contra los menores de edad y adolescentes por medio del uso de redes sociales para la comisión de delitos como son la suplantación de identidad, extorción, pornografía infantil, abuso sexual y violación."12

El *grooming* como tal hace referencia a un adulto que busca abusar sexualmente de un menor y que fue utilizado inicialmente para indicar que dicho abuso venia por parte de personas de su entorno familiar; posteriormente este término se usó en aquellos casos donde el agresor se gana el afecto mediante manipulación emocional buscando ganarse la confianza y aceptación del menor para luego abusar de él.

El *child grooming* es definido como "el proceso a través del cual un adulto consigue victimizar sexualmente a un menor valiéndose de Internet"13; proceso por el cual

[12] PILLAJO PEREZ DIEGO XAVIER. Propuesta de política pública para la protección de niños, niñas y adolescentes frente a la figura delictiva sexual-informática "CHILD GROOMING" en la Legislación Ecuatoriana. [En línea] 2022. Tesis de Licenciatura. (Recuperado en: marzo de 2023) Disponible en: https://dspace.uniandes.edu.ec/bitstream/123456789/15283/1/UI-DER-PDI026-2022.pdf

[13] GÁMEZ-GUADIX MANUEL, et al. Creencias Erróneas Sobre El Abuso Sexual Online De Menores (" Child Grooming") Y Evaluación De Un Programa De Prevención. Psicología Conductual [En línea]

un adulto consigue engañar a un menor para obtener material sexual como imágenes o vídeos y en algunos casos llega a materializarse como abuso sexual físico.

SKÓRZEWSKA-AMBERG ofrece otro concepto, indicando que “El *grooming* en línea, que es uno de los muchos tipos de *grooming*, se define en la literatura como un proceso en el que un adulto que está sexualmente interesado en un niño construye una relación con el niño en el mundo virtual para cometer delitos sexuales que requieren contacto físico o no” 14.

En cuanto al *sexting* que es un terminó relativamente más reciente que sale de la unión entre sex and texting y se define como[15]. enviar, recibir o reenviar mensajes, fotografías o imágenes sexualmente explícitos a través de internet y teléfonos celulares. Este contenido puede ser usado para chantajear al menor para que cometa otras acciones peligrosas o para ser comercializada y/o compartida como pornografía infantil.

Lo anterior en cuanto a las amenazas más comunes, sin desmeritar los riesgos de contenido y otros tipos de riesgos de conducta.

2021, vol. 29, no 2, p. 283-296. (Recuperado en marzo de 2023) Disponible en: https://www.researchgate.net/publication/354856627_Creencias_erroneas_sobre_el_abuso_sexual_online_de_menores_child_grooming_y_evaluacion_de_un_programa_de_prevencion

[14] SKÓRZEWSKA-AMBERG MAŁGORZATA. Online Child Grooming–Some Remarks Against the Background of the Pandemic. Krytyka Prawa. Niezależne studia nad prawem [En línea]] 2021, vol. 13, no 4, p. 72-87. (Recuperado en noviembre de 2022) Disponible en: https://www.ceeol.com/search/article-detail?id=1062176

[15] GASSÓ AINA, BIANCA KLETTKE, JOSÉ AGUSTINA AND IRENE MONTIEL. "Sexting, Mental Health, and Victimization Among Adolescents: A Literature Review" [On line] 2019 International Journal of Environmental Research and Public Health 16, no. 13: 2364. https://doi.org/10.3390/ijerph16132364
(Recuperado en abril 2023) Disponible en: https://www.mdpi.com/1660-4601/16/13/2364

4.2.4 **La pandemia y el aumento de los riesgos para la comunidad infantil.** El covid-19 es una enfermedad infecciosa provocada por el virus SARS-CoV2. Es un tipo de virus respiratorio cuyos síntomas van desde leve a letal, y que cobró muchas vidas a nivel mundial. Entre los años 2019 cuando empezó la pandemia y el 2020, los gobiernos tuvieron que tomar medidas extremas para evitar su propagación, siendo el confinamiento una de ellas, obligando a los habitantes a no salir de casa y a volcarse en la tecnología existente para continuar con sus actividades.

Según SKÓRZEWSKA-AMBERG[16] "La pandemia de COVID-19, o más precisamente, las medidas tomadas para frenar su propagación, influyó significativamente en el aumento de los delitos relacionados con la sexualidad infantil. Lo que se observó durante la pandemia no fue solo un aumento de tráfico relacionado con la distribución de pornografía infantil, sino también un aumento definitivo en comportamientos que pueden ser clasificados como grooming." Esto se evidencia en el aumento de las denuncias de los distintos países como se indicará más adelante.

4.2.5 **Las medidas para castigar a los agresores infantiles en internet.** De los tres tipos de riesgos, los de conducta, contenido y contacto, solo este último está siendo castigado por la ley.

Para los riesgos de contenido, hay un enfrentamiento entre lo que puede o no puede publicar una persona y la libre expresión y los riesgos de conducta no constituyen como tal un delito.

En cuanto a los riesgos de contacto, los delincuentes han estado aprovechando vacíos legales para salir impunes, sin embargo, los gobiernos ya están tomando medidas para evitarlo. En Europa, por ejemplo, según SKÓRZEWSKA-AMBERG[17] "el artículo 23 del Convenio del Consejo de Europa para la Protección de los Niños

[16] SKÓRZEWSKA-AMBERG, Małgorzata. Online Child Grooming–Some Remarks Against the Background of the Pandemic. Krytyka Prawa. Niezależne studia nad prawem [Online] 2021, vol. 13, no 4, p. 72-87. [Consultado en: noviembre de 2022] Disponible en: https://www.ceeol.com/search/article-detail?id=1062176.

[17] Ibíd

contra la Explotación y el Abuso Sexual (Convenio de Lanzarote), la incitación a un niño con fines sexuales se definió como la propuesta de un adulto, a través de las TIC, de encontrarse con un niño con el propósito de explotar sexualmente al niño – si la propuesta va seguida de acciones que se supone deben conducir a la reunión. De conformidad con el artículo 23 del Convenio, tal conducta debe ser sancionada."

En Colombia por su parte, la Corte Suprema de Justicio, definió algunos puntos clave para evitar los grises y vacíos que aprovechan los delincuentes, en un artículo de El Tiempo[18], aclara que: "Cuando una persona obliga a otra a grabar videos con contenido sexual, y a enviárselos bajo amenazas, no está cometiendo un constreñimiento (que implica doblegar la voluntad de otro para que haga o tolere una cosa), o una extorsión (que tiene de por medio la exigencia de dinero), sino que constituye un acto sexual violento", estos actos son diferentes al acceso carnal o violación, pero la corte indica que sin necesidad de tener contacto físico con la víctima, este acto se materializa a través de las amenazas en los entornos digitales como redes sociales.

En cuanto al *grooming* lo define cuando un adulto a través de internet crea una conexión con un niño para abusarlo o explotarlo sexualmente. Si el menor tiene menos de 14 años se tipifica como abuso sexual, pero si es mayor cae en la categoría de acto sexual violento. Si se prueba acoso sexual a través de redes o *WhatsApp* puede incurrir hasta en tres años de cárcel.

En cuanto a pedir sexo por internet, si es solicitado a un menor de 14 años, el solicitante puede ser castigado por 14 años de prisión.

[18] SARRALDE MILENA. ¿Hay delitos en el 'sexting'? Estas son las aclaraciones de la Corte [En línea] 03 de noviembre de 2019 El tiempo (Recuperado en 23 de noviembre de 2022) Disponible en: https://www.eltiempo.com/justicia/cortes/cuales-son-los-delitos-sexuales-en-internet-segun-la-corte-suprema-429966

Para la pornografía infantil, una persona que fotografíe venda y/o distribuya imágenes sexuales de niños, o las guarde en su celular o computador puede ser condenado por hasta 20 años de cárcel.

Cuando se trata de explotación y prostitución, si un menor de 14 años es contactado a través de internet para tales fines, la pena puede ser hasta de 33 años de prisión.

En cuanto al sexting, más recientemente, se aprobó en primer debate un proyecto de ley que tipifica el *sexting* como Violencia Sexual Cibernética. Esta iniciativa busca proteger la vida íntima sexual de las personas, en especial mujeres y niños. Según un artículo de la Cámara de Representantes[19] "El proyecto sanciona la violencia sexual que se ejerce contra una persona mediante la divulgación de documentos, en cualquier formato, de la vida íntima o sexual, sin el consentimiento de ella, a través de cualquier medio."

4.2.6 **Medidas de prevención.** Las medidas para proteger a los niños en los entornos digitales se basan en la educación, con campañas que intentan difundir información sobre los peligros actuales en las redes sociales y cómo comportarse en línea; en las redes sociales existen opciones de privacidad y seguridad configurables por los usuarios y además algunos controles basados en los datos de registro como la edad del usuario, sin embargo, han tomado fuerza los controles parentales definidos por la Cámara de Comercio de Bogotá[20] "como una serie de filtros que permiten a los padres controlar el uso de internet de los niños."

[19] CAMARA DE REPRESENTANTES. Aprobado proyecto que tipifica el #Sexting como delito en primer debate. [En línea] 11 de junio 2021 (Recuperado en 23 de noviembre de 2022) Disponible en: https://www.camara.gov.co/aprobado-proyecto-que-tipifica-el-sexting-como-delito-en-primer-debate#:~:text=El%20proyecto%20sanciona%20la%20violencia,a%20trav%C3%A9s%20de%20cualquier%20medio.

[20] DE BOGOTÁ, Cámara de Comercio, et al. ¿Qué son las medidas de protección parental? [En línea] 2022. PDF (Recuperado en noviembre de 2022) Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/27720/Mecanismos%20de%20cotrol%20parental%20prevencion.pdf?sequence=1

Dichas medidas parecen no ser suficientes ante el aumento de casos descritos en este documento, posiblemente porque los controles actuales están de cierta forma relacionados con la tecnología, y actualmente existe una brecha de conocimiento entre las nuevas generaciones que ya nacen en una era digital llamados también nativos digitales y sus progenitores que podemos llamar inmigrantes digitales. Definidos por Cusicanqui José Luis[21] como aquellas personas que se han tenido que ir adaptando al uso de los medios digitales ya en una edad adulta o aquellas que por algún motivo viven en lugares donde el uso de internet no es común, ya sea por factores como educación, acceso a la tecnología u otros, y que se ven aprietos para poder "hablar el mismo idioma que las nuevas generaciones".

Muchos padres no se involucran en la vida digital de sus hijos, no usan los controles de privacidad de las redes sociales y/o desconocen los diferentes controles parentales que ya vienen incluidas en aplicaciones o los mismos dispositivos y que pueden ayudar a mejorar la seguridad de sus hijos, haciendo que estas medidas sean ineficaces al no usarlas de forma adecuada.

4.3 ANTECEDENTES O ESTADO ACTUAL

Los delitos tradicionales como el *bullying,* el maltrato y el acoso sexual contra menores, han ido evolucionando, y hoy en día tienen su equivalencia en el mundo digital.

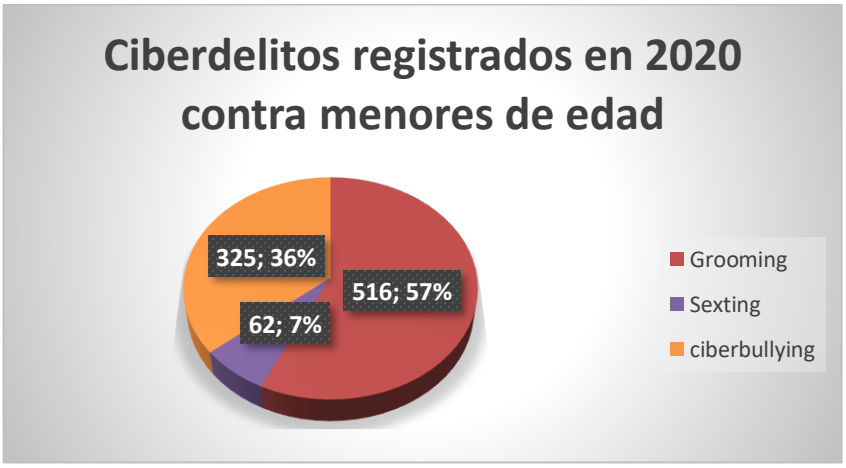
El *bullying*, por ejemplo, tiene su evolución en el *ciberbullying* o ciberacoso, sin embargo, en un artículo del psicólogo Sanches Mauricio indica que "el ciberbullying intensifica la violencia ejercida sobre las víctimas del abuso escolar sumando

[21]CUSICANQUI JOSÉ LUIS. Nativos Digitales Vs. Inmigrantes Digitales ¿Brecha Generacional, Brecha Cognitiva?¡ Una Mirada Psicopedagógica! Digital Natives Vs. Digital Immigrants [En línea] 2019. Generational Gap, Cognitive Gap? A Psychopedagogical Look!. Edición Revista Editora, vol. 2, no 1, p. 89 (Recuperado en marzo 2023) Disponible en: https://www.redalyc.org/pdf/140/14002809.pdf

nuevos agresores”22; el acoso cibernético puede ser aún más intenso que el tradicional, y que, a diferencia de este, el cibernético sigue al niño fuera de la escuela gracias al uso generalizado de las redes sociales. Así mismo muchos pedófilos han modificado sus ataques para adecuarse a las nuevas tecnologías, utilizando las tecnologías de información como medios para encontrar a sus víctimas; mientras que bajo la “libertad de expresión” y el masivo contenido que muchas personas suben a la red, los menores se ven expuestos a contenidos inadecuados.

Según la periodista Suesca Lizeth “Durante 2021 los delitos cibernéticos en Colombia ascendieron a 33.465, lo que significa un aumento de 17 % en comparación con 2020, cuando fueron 28.524 casos.”[23]
En la figura 1, podemos ver las cifras relacionadas con delitos contra menores de edad y su porcentaje de participación según el tipo de delito.

Figura 1 Ciberdelitos contra menores de edad en 2020



[22] SÁNCHEZ MAURICIO. Identificar el ciberbullying o ciberacoso El ciberbullying suele ser una 'extensión' del *bullying* tradicional, por lo que identificar sus manifestaciones puede ser clave en la detección del acoso 'cara a cara'. [En línea] 2020. Fuentes, no 26. (Recuperado en marzo de 2023) Disponible en: https://www.menteyciencia.com/identificar-el-ciberbullying-o-ciberacoso/
[23] SUESCA LIZETH, Delitos cibernéticos en Colombia ascendieron un 17 % en 2022. [En línea] 2022. Caracol radio. (Recuperado en abril 2023) Disponible en: https://caracol.com.co/radio/2021/12/26/politica/1640514049_007856.html

Fuente: Elaboración propia

El portal del Gran Santo Domingo[24] indica que: “Según un estudio de la UNICEF, si bien internet ha descubierto a los niños todo un mundo para explorar, también ha facilitado a los acosadores, agresores sexuales, traficantes y abusadores la tarea de encontrarlos.”

El *groomer* así mismo también ha ido evolucionando con el tiempo, Martinez[25] identificaba al *groomer* como un hombre entre 20 y 40 años, con problemas para relacionarse en su vida diaria, que optaba por cafés internet para lograr anonimato, que creaban perfiles falsos para engañar a sus víctimas y que contactaban a los menores entre las 3 de la tarde y las 7 de la noche, que generalmente eran tiempo de descanso; sin embargo, hoy en día se reconocen distintos perfiles de acosadores, en un artículo de Heinze Elena e Hidalgo Irene[26] indican que hay casos donde los *groomers* tienen entre 15 y 17 años, además muchos de estos delincuentes no tienen problemas al entablar relaciones sociales y algunos acosadores no usan perfiles falsos, indicando su edad real cuando hablan con el menor, siendo cada vez más veloces y en cierta forma agresivos.

Se puede observar que los riesgos asociados a las redes sociales son la evolución digital de las amenazas tradicionales, además de un aumento significativo en las denuncias que durante la pandemia llego a ser de hasta el 500%[27] y una constante

[24] EL GRAN SANTO DOMINGO. Los *millennials* ante retos del mundo tecnológico. [En línea] 29 de noviembre de 2018. (Recuperado en agosto de 2021) Disponible en: http://www.elgransantodomingo.com/los-millennials-ante-retos-de-un-mundo-tecnologico/

[25] MARTINEZ JOSÉ. Conozca cómo actúan los acosadores en las redes para que proteja a sus hijos. [En línea]] 18 de octubre de 2018. Bogotá.gov (Recuperado en: agosto de 2021) Disponible en: https://bogota.gov.co/mi-ciudad/gestion-publica/riesgos-de-los-ninos-en-internet

[26] GARAYZÁBAL HEINZE ELENA, HIDALGO DE LA GUÍA IRENE. Detección De Depredadores Sexuales En Los Chats Y La Captación De Menores. El Papel De La Lingüística Forense. [En línea] 2020 Tonos Digital, 2020, vol. 39, no 0. (Recuperado en abril de 2023) Disponible en: https://digitum.um.es/digitum/bitstream/10201/96042/1/2549-6933-1-PB.pdf

[27] FALESTCHI DEMIAN. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. [En línea] 11 de noviembre de 2020. IABCOLOMBIA. (Recuperado en agosto de

mutación entre los métodos que utilizan los agresores, así como en el comportamiento de estos.

4.4 MARCO LEGAL

Entre las leyes que protegen a la infancia se encuentran:

La ley 1098 de 2006 “Este código tiene por finalidad garantizar a los niños, a las niñas y a los adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad, en un ambiente de felicidad, amor y comprensión. Prevalecerá el reconocimiento a la igualdad y la dignidad humana, sin discriminación alguna.”

La ley 1878 de 2018 “Por medio de la cual se modifican algunos artículos de la Ley 1098 de 2006, por la cual se expide el Código de la Infancia y la Adolescencia, y se dictan otras disposiciones.”

Pero Colombia cuenta también con leyes orientadas a los riesgos encontrados en las redes sociales, más allá de los que ya existen relacionados con la protección infantil, como se puede evidenciar en un artículo de Redalyc

En Colombia, el ciberacoso en los colegios es castigado con la ley 1620 de 2013 "Por la cual se crea el sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar" (Ley 1620 de 2013 de Colombia, 2013), y abarca redes sociales como *Facebook*, *Twitter,* entre otros.

2021) Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-y-el-avance-del-grooming-en-america-latina/

La sextorsión se castiga en el código penal colombiano capitulo segundo "De la extorsión" articulo 244 el cual fue modificado por la ley 733 de 2002 " Por medio de la cual se dictan medidas tendientes a erradicar los delitos de secuestro, terrorismo y extorsión, y se expiden otras disposiciones" en el artículo cinco, donde la pena por este delito es de doce (12) a dieciséis (16) años y multa de seiscientos (600) a mil doscientos (1.200) salarios mínimos legales mensuales vigentes (Ley 733 de 2002 de Colombia, 2002).

El *child grooming* y la pornografía infantil se castiga en el código penal colombiano capítulo cuarto "Del proxenetismo" modificado por la 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" En el artículo 218 "pornografía con personas menores de 18 años" la pena por estos delitos es de diez (10) a veinte (20) años y multa de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (Ley 1336 de 2009 de Colombia, 2009).

En portal Red Contra el Abuso Sexual, también identifica otras leyes relacionadas:

“La Ley 599 de 2000 del Código Penal Colombiano, establece que quienes fotografíen, graben, filmen, produzcan, divulguen o vendan, compren, posean, porten, almacenen, transmitan o exhiban por cualquier medio, representaciones de actividad sexual que involucren a menores de dieciocho años, incurrirá en prisión de 10 a 20 años y se les impondrá una multa de 1.500 salarios mínimos mensuales legales vigentes.

La Convención de Budapest, el cual es el primer tratado internacional, que busca armonizar las leyes y la colaboración entre naciones para hacer frente a los delitos informáticos, y los delitos en internet. La Ley 1928 de 2018, aprueba este convenio sobre ciberdelincuencia adoptado el 23 de noviembre de 2001. El convenio del

concejo europeo, que busca proteger a los niños contra la explotación y el abuso sexual, mediante el cual los estados se ponen de acuerdo para criminalizar formas de abuso sexual contra los niños, siendo el primer tratado internacional en penalizar el abuso sexual ocurrido dentro del hogar.

Más recientemente se encuentra una referencia en noticias UNAD sobre la ley 679 de 2010 aplicada contra el *grooming* que tiene como objetivo dictar medidas de protección contra distintas formas de abuso sexual con menores de edad.
Se encuentra un proyecto de ley en 2017 que busca “formular los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes; se modifica el código penal y se dictan otras disposiciones”, pero de la cual no se encuentra información de su aprobación.

5 RIESGOS DE INGENIERÍA SOCIAL QUE ENFRENTAN LOS NIÑOS EN LAS REDES SOCIALES

Uno de los principales pasos para formular métodos eficaces para proteger a la comunidad de los riesgos que albergan las redes sociales no es solo identificarlos de manera general, sino ir un paso más allá y entender cuáles son las fases que sigue el agresor para llegar a su víctima y al igual que en cualquier otro delito hacer un perfil del atacante. Este capítulo busca identificar cuáles son los ataques relacionados con ingeniería social que atacan a los niños, así como recopilar las fases y los perfiles en común identificados por distintos investigadores en el tema.

El Principal Ataque De Ingeniería Social Que Afecta La Comunidad Infantil. Según Chevalier[28], se realizó un estudio en 30 países, entre los años 2017 y 2019 (antes de la pandemia) dirigido a menores entre los 8 y 12 años por el *think tank internacional DQ Institute*, que arrojó como resultado que más del 60% de ellos se expuso a un riesgo cibernético cuando tuvo acceso a internet.

[28] CHEVALIER NARANJO Stephani ¿Qué riesgo corren los niños al conectarse a internet? [En línea] 8 de febrero de 2021 Portal Statista.com (Recuperado en 2 de noviembre de 2021) Disponible en: https://es.statista.com/grafico/24110/los-ninos-y-la-seguridad-en-linea/

En la figura número dos podemos observar el porcentaje los riesgos que enfrentaban a los menores antes de pandemia

Figura 2 Estadísticas Riesgos antes de 2019

Fuente: CHEVALIER NARANJO Stephani ¿Qué riesgo corren los niños al conectarse a internet? [En línea] 8 de febrero de 2021 Portal Statista.com (Recuperado en 2 de noviembre de 2021) Disponible en: https://es.statista.com/grafico/24110/los-ninos-y-la-seguridad-en-linea/

Sin embargo, debido a la pandemia, el tráfico en internet y por ende los ciberataques tuvieron un aumento significativo en el entorno social, situación de la cual no escapo la comunidad infantil. Según el portal welivesecurity [29] en países como Argentina México y España, el tráfico de red aumento entre un 25% y hasta un 90% en época

[29] MICUCCI MARIO. Grooming: una problemática que crece durante la cuarentena. 2020

de cuarentena, así mismo los ciberdelitos crecieron exponencialmente, en especial los que tiene que ver con *grooming* y explotación sexual infantil.

Como se mencionó anteriormente según el ICBF[30], los riesgos a los que se ven expuestos los niños y adolescentes en las redes se pueden clasificar en riesgos de contenido, como imágenes violentas o sexuales, mensajes de odio o racismo, entre otros; de conducta como el ciberacoso, el *sexting*, o la dependencia; o de contacto como el *phishing* y el *grooming*. Estos últimos, los riesgos de contacto por su forma de proceder son equiparables a los ataques de ingeniería social del mundo adulto. En un riesgo de contacto un delincuente, generalmente mayor de edad, engaña a su víctima para obtener algo de la misma. Entre el *phishing* y el *grooming* encabeza el *grooming* como el delito más frecuente, concluyendo de forma personal que el primero (*phishing* o suplantación de identidad) es solo uno de los pasos de un ataque de *grooming*.

Según Serra[31], con respecto al ciberacoso y al *grooming*, se evidenció un crecimiento de denuncias hasta del 133% durante la pandemia entre los meses de marzo y octubre en comparación con el año anterior.

Además, en el mismo artículo de Serra[32] se puede observar que los ataques están distribuidos entre niños de 12 y 17 años con un 65% y entre 6 y 11 años el otro 35%, siendo las niñas y mujeres adolescentes más afectadas con un 79% en contraste con el 21% de la comunidad infantil masculina.

---

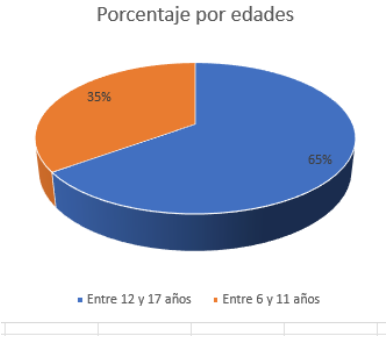
[30] ICBF. Riesgos digitales, ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet? [En línea] 17 de diciembre de 2019 (Recuperado en agosto 2021) Disponible en: https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos

[31] SERRA KARINA. Radiografía del grooming y ciberacoso en pandemia. [En línea] 29 de enero de 2021 Diario El Perfil. (Recuperado en agosto 2021) Disponible en: https://www.perfil.com/noticias/opinion/karina-serra-radiografia-del-grooming-y-ciberacoso-en-pandemia.phtml

[32] Ibíd

En la figura número 3 podemos ver los porcentajes de distribución según los rangos de edad de los menores que han sido víctimas de algún tipo de ataque en internet, observando que la mayor cantidad de ataques están dirigidos a preadolescentes entre los 12 y 17 años.

Figura 3 Porcentaje de ataques por rango de edad



Fuente: Propia

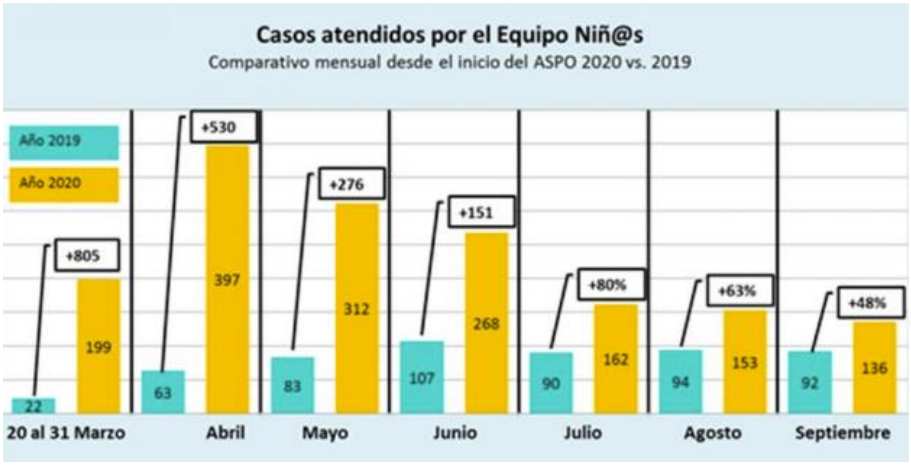
En la figura número 4 vemos una distribución de porcentajes según el género del menor, identificando que, aunque el género femenino es el más atacado, también hay un porcentaje masculino, lo que indica que los ataques no son exclusivos de la comunidad femenina.

Figura 4 Porcentaje de ataques por género

Fuente: Propia

La figura número 5 muestra una comparación entre las denuncias registradas cada mes entre el año 2019 contra el año 2020, observando un aumento significativo de estas

Figura 5 Aumento de *Grooming* durante la pandemia en comparación con el año anterior



Fuente: SERRA KARINA. Radiografía del grooming y ciberacoso en pandemia. [En línea] 29 de enero de 2021 Diario El Perfil. (Recuperado en agosto 2021) Disponible en: https://www.perfil.com/noticias/opinion/karina-serra-radiografia-del-grooming-y-ciberacoso-en-pandemia.phtml

En América latina en general, la situación es similar, Falestchi [33] CEO de *Kids Corp*, advierte que la conectividad a internet de la comunidad infantil creció hasta en un 100%, debido al cambio de presencialidad al uso masivo de plataformas digitales, así mismo las denuncias de *grooming* en este escenario tuvieron un aumento del 500%.

[33] FALESTCHI DEMIAN. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. 2020.

Más específicamente en Colombia, un artículo de la Radio Nacional de Colombia[34] índica que hasta julio del año 2021 ya se habían reportado 177 denuncias de *grooming*, sin embargo, esta cifra puede ser el doble o el triple, ya que muchas de estas situaciones no son denunciadas, y que esta cifra al igual que la importancia y peligro del delito no debe desconocerse o subestimarse.

Como se observa uno de los delitos que más ha crecido junto con el ciberacoso (riesgo de conducta), es el *grooming* que corresponde a ataques de ingeniería social y en el cual se va a enfocar los siguientes temas de este capítulo.

5.1 ESCENARIOS DE ATAQUE DE INGENIERÍA SOCIAL.

Como se menciona en el título de este trabajo, está enfocado en las redes sociales, sin embargo, es importante evidenciar cuales de ellas son las más usadas por lo ciberdelincuentes y así mismo no desestimar otros entornos digitales en los cuales se puede presentar.

Según un artículo de Sacristán Francisco “Ya en la actualidad las redes sociales y las plataformas de mensajería instantánea se consolidaron como nuevas formas de planificar y realizar actividades ilícitas, afirmación que se sostiene prácticamente para todas las figuras delictivas imaginables, pero especialmente cierta en el ámbito de la criminalidad sexual.”35

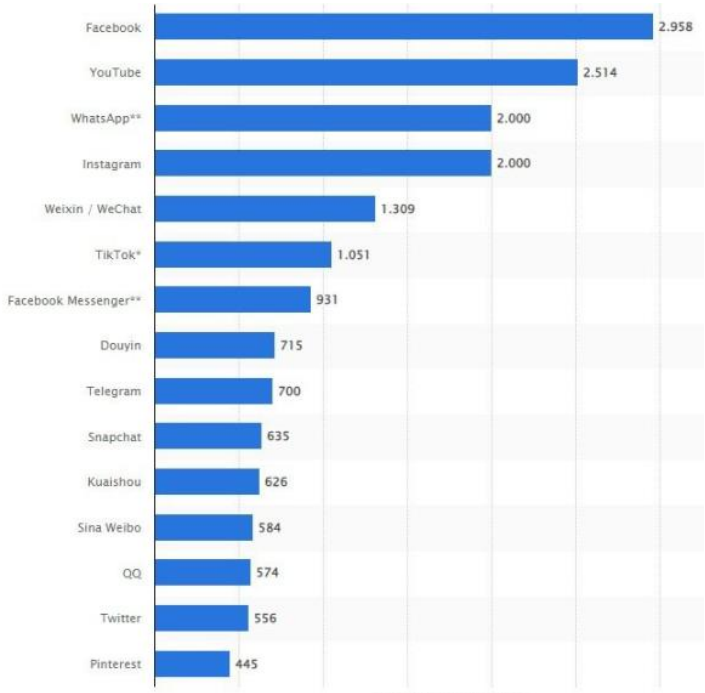
[34] RADIO NACIONAL DE COLOMBIA. En 2021 se han reportado 177 denuncias de acoso sexual en internet a menores. [En línea] 02 de julio de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.radionacional.co/actualidad/judicial/en-2021-se-han-reportado-177-denuncias-de-acoso-sexual-en-internet-menores

35 ROMERO FRANCISCO SACRISTÁN. Escenarios actuales de agresiones al derecho a la intimidad personal del menor. [En línea] 2021. Revista DH/ED: derechos humanos y educación, no 4, p. 137-155. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8126366

En los últimos años con el auge de las tecnologías de la información, las redes sociales se han convertido en los escenarios más usados por *groomers* para acercarse a sus víctimas;

En la figura número 6 podemos ver el top de las redes sociales más usadas, según su número de usuarios, en un estudio realizado por statista en enero de 2023, donde lidera Facebook

Figura 6 Ranking De Redes Sociales Líderes A Nivel Mundial Por Número De Usuarios Activos En Enero De 2023 (En Millones) STATISTA



Fuente: STATISTA. ¿CUÁLES SON LAS REDES SOCIALES MÁS UTILIZADAS? [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://2immarketing.com/cuales-son-las-redes-sociales-mas-usadas/

De las redes sociales a diferencia de que se podría interpretar con la figura anterior y aunque cibercrimen[36] reitera que *Facebook* fue la red más usada por la mayoría de la comunidad en 2020, no significa que sea la red más usada para estos tipos de delito. Los porcentajes de estas redes varían de un país a otro, por ejemplo, según SINEMBARGO[37] en Argentina es *Instagram* quien encabeza estos ataques con un 54%, de segundo se tiene a *WhatsApp* con un 31%, *Facebook* con un 11% y finalmente *Tik Tok* con un 2%. Mientras en países como Perú según Portal Andino[38] aunque no indica cifras específicas, si identifican a *Facebook* y *WhatsApp* como las plataformas más usadas, siendo en este el responsable del 80% de denuncias relacionadas por *grooming*. En Colombia por estadísticas de uso, más que de estadísticas de denuncia, según un artículo en la revista digital de Semana[39] Indica un aumento de usuarios de *Facebook* del 87% y de *Instagram* en un 54%, mientras que posteriormente *WebFinfYou*[40] identifican que las redes más usadas en Colombia son *Facebook* con cifras de 93,6%, *WhatsApp* con 90,7% e *Instagram* con un 82%.

[36] CIBERCRIMEN. Facebook, La Red Social Mas Usada En La Pandemia. [En línea] 09 de junio de 2020. (Analisis&Tendencias). (Recuperado en agosto de 2021) Disponible en: https://www.cibercrimen.org.ar/2020/06/09/facebook-la-red-social-mas-usada-en-la-pandemia-analisistendencias/

[37] SIN EMBARGO. "Instagram, WhatsApp, Facebook y TikTok, redes usadas para 'cazar' niños en Argentina". [En línea]. 02 de junio de 2021 (Recuperado en septiembre de 2022) Disponible en: https://www.noroeste.com.mx/internacional/instagram-whatsapp-facebook-y-tiktok-redes-usadas-para-cazar-ninos-en-argentina-NBNO1222708

[38] MORENO HAROLD, PILLACA MARYORIE. Redes peligrosas. [En línea] 2019 Portal Andina. (Recuperado en septiembre de 2022) Disponible en: https://portal.andina.pe/edpespeciales/2019/redes-peligrosas/index.html

[39] SEMANA. ¿Cuánto aumentó el uso de internet en niños por la pandemia? [En línea] 22 de enero de 2021 (Recuperado en septiembre de 2022) Disponible en:https://www.semana.com/educacion/articulo/cuanto-aumento-el-uso-de-internet-en-ninos-por-la-pandemia/202104/

[40] WEBFINDYOU. El uso de las redes sociales en Colombia. [En línea] 09 de septiembre de 2021 (Recuperado en setiembre de 2021) Disponible en: https://www.webfindyou.com.co/blog/uso-redes-sociales-colombia/

5.2 FASES DE ATAQUE DEL *GROOMING*.

Se pueden identificar de 3 a 4 etapas en un ataque de *grooming*, las cuales se resumen de la siguiente manera:

- La primera es la amistad, en este caso busca establecer comunicación con su víctima, haciéndose pasar generalmente por otro menor de edad, buscando establecer lazos de amistad y empezar el seguimiento del menor. Según un artículo del canal 13[41] en esta etapa se buscan factores de vulnerabilidad como necesidades emocionales, soledad o poca autoestima, además de recaudar toda la información posible del menor como gustos, información familiar, miedos, los cuales serán usados para manipularlo en la siguiente etapa.

- La segunda etapa puede ser llamada engaño, enganche o vinculo de confianza; independiente del nombre, las actividades a las que se refiere esta etapa son las mismas; aquí el abusador intenta ganarse la confianza de la víctima, ya sea fingiendo estar enamorado de ella, o haciendo que la víctima se identifique con él, al compartir gustos, intereses o inclusive problemas. El lapso de esta etapa puede ser de semanas e inclusive años, dependiendo de la motivación del acosador. Se incluye en esta etapa unos pasos adicionales identificados por la organización *Save the Children*[42] donde intenta aislar a la víctima de sus redes de apoyo ya sea familiares, amistades y/o docentes, manipulándolo para que guarde todo en secreto, evaluando a su vez si el menor a compartido los detalles de su relación con otras personas e iniciando conversaciones de tipo sexual para que la víctima se valla relacionando con el tema, el lenguaje y las solicitudes que vendrán.

[41] Canal 13. ¿Qué es el grooming? [En línea] 13 de marzo de 2023. (Recuperado en abril de 2023) Disponible en: https://canaltrece.com.co/noticias/grooming-que-es-etapas-y-caracteristicas/
[42] SAVE THE CHILDREN. Grooming. Qué es, Cómo detectarlo y Prevenirlo. [En línea] 01 de julio de 2019 (Recuperado en: septiembre de 2021) Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

- La tercera etapa es el acoso y la extorsión o chantaje. En esta etapa ya se ha conseguido la confianza de la víctima y el ciberdelincuente ha logrado obtener de esta, imágenes de carácter sexual frente a la cámara o por medio del envío de fotografías, en algunos casos hasta le indica que poses o comportamientos debe hacer el niño o niña. En este caso según el perfil del cibercriminal puede detenerse una vez que cumplió su objetivo, o utilizar este mismo material para chantajear al menor para que siga enviando contenido de esta índole, muchas veces solicitar que le contacte con nuevas víctimas o acosándolo para la última y más peligro fase, la de contacto físico.

- La cuarta y última etapa, se añadió considerando un artículo del gobierno de Argentina[43], es el contacto o encuentro físico, en esta el ciberdelincuente puede tener contacto físico con su víctima, permitiendo abusar sexualmente de él o ella, inclusive en situaciones más extremas su reclutamiento para trata de blancas o el mismo homicidio de la víctima, según su motivación, como se ve en la próxima sección.

Se identifican entonces 4 etapas: amistad, engaño y confianza, acoso y extorsión y contacto físico.

5.3 PERFIL DEL CIBERDELINCUENTE.

Ahora intentar crear un perfil de ciberdelincuente, de ahora en adelante llamado *groomer*, no es tan simple como se creería. Pues pensar que solo se trata de un hombre mayor que busca a menores de edad para satisfacer sus deseos, es desestimar el daño que puede causar y el peligro de este tipo de ataque. Se pueden diferenciar tipos de *groomer* ya sea por su motivación o por la forma de acercarse a su víctima.

[43] ARGENTINA.GOB. ¿Cómo actúan los acosadores? [En línea]. 2021 (Recuperado en septiembre de 2021) Disponible en: https://www.argentina.gob.ar/grooming/como-actuan-los-acosadores

Según Vanesa García Carbone, Perfiladora Criminal y directora de la División de Criminología, Criminalística y Análisis de la Conducta Criminal, de la Sociedad Argentina de Trastornos de la Personalidad y Psicopatías (SATP), en una entrevista que dio para USECIM[44], indica que no todos los *groomer* tiene el mismo comportamiento, patrones de conducta y/o motivaciones, pero conocer a profundidad todos estos perfiles permite mejorar las estrategias para defender a la comunidad infantil. Así mismo ella identifica seis categorías de acosadores:

- Pederasta Digital, este acosador, nunca pasara a una fase física, no le interesa conocer a la víctima.
- *Groomer* pederasta, quien si busca conocer a su víctima.
- *Groomer* cazador, estos son delincuentes organizados, que utilizan las redes sociales para captar objetivos para la trata de personas.
- *Groomer* depredador, estos ya son criminales violentos que pueden llegar al homicidio de la víctima.
- *Groomer sugar daddy/mommi,* aunque estos términos no son nuevos, y hoy en día hasta se publicitan por redes sociales sin ningún control, cuando un *suggar daddy* va tras un menor de edad, sus acciones se enmarcan en los métodos que utilizan individuos con un interés sexual en los niños para "prepararlos" para el abuso sexual, engañándolos a través de “mimos”, regalos y dinero y ganando así su confianza para poder manipularlos posteriormente. Un artículo en el portal san Luis noticias[45], indica que un hombre mayor que busca menores de edad bajo esta modalidad puede encubrir posibles abusos, además va un poco más allá indicando que este fenómeno tiene como epicentro la pedofilia, y que un fenómeno social que busca infantilizar la sexualidad y acudir a la filiación

[44] USECIM El perfil criminal del Groomer. [En línea] 31 de julio de 2021 (Recuperado en septiembre de 2021) Disponible en: https://canalnoticias.usecim.es/el-perfil-criminal-del-groomer/

[45] SAN LUIS NOTICIAS "My Sugar Daddy": Un peligroso juego, entre menores y adultos, que encubre posibles abusos o riesgo de trata. [En línea] 5 de diciembre de 2022. (Recuperado en marzo de 2023) Disponible en: https://sanluisnoticias.com/post/mi-sugar-daddy-advierten-sobre-peligroso-juego-sexual-entre-adolescentes-y-adultos#:~:text=Adolescentes%20entre%2011%20y%2016,fantas%C3%ADas%20y%20deseos%20generalmente%20sexuales.

paterna para hablar de sexo sienta la base que sustenta la cultura del abuso sexual infantil.

- Productores de MASI (Material de abuso sexual contra la infancia), relacionados con pornografía infantil.

Por otro lado, en la página del hospital de *Sant Joan de Deu* - Barcelona[46] ofrece otro tipo de clasificación:

- Directo: quien participa activamente en redes sociales para buscar menores y entablar una comunicación con ellos, luego realiza propuestas de tipo sexual pidiendo imágenes o ejerciendo presión y manipulación al menor para que active la cámara.
- Oportunista: quien busca imágenes con contenido sexual que hayan sido filtradas o subidas a la red y con esta información planea chantajear al menor.
- Específico: Este no solo busca obtener imágenes de tipo sexual, sino también establecer un contacto físico. Es el más peligroso ya que se dedica con esmero a la fase de amistad para lograr ganarse la confianza del menor y concretar un encuentro.

Trabajos similares a este, han clasificado los engaños a los que se ven expuestos los menores como técnicas de ingeniería social, por ejemplo, Triana Carlos y Andres Oliva indican que estos cibercriminales “suelen emplear técnicas para engañarlos a través de conductas sociales o técnicas llamadas Ingeniería Social, que consisten en la manipulación psicológica y persuasión, para que voluntariamente la víctima brinde información o realice algún acto que lo ponga en riesgo.”47

[46] SJD. Cómo evitar que los menores sufran grooming (acoso sexual por Internet) [En línea] 06 de febrero de 2021 (Recuperado en marzo de 2023) Disponible en: https://faros.hsjdbcn.org/es/articulo/como-evitar-menores-sufran-grooming-acoso-sexual-internet

[47] TRIANA CARLOS, OLIVA EDGAR. Esquema para la prevención del grooming en niños, niñas y adolescentes desde los 7 a 14 años en Bogotá a través de un análisis de riesgos basados en la norma ISO 27005. [En línea] 2021. Bogotá: Universidad Católica de Colombia, 202261 páginas (Recuperado en marzo 2023) Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/35315784-6fd2-41e9-baf1-c75910b5e537/content

Sin embargo. en este punto se quiere resaltar que el *grooming* no es solo un ataque de ingeniería social de suplantación de identidad, sino que es comparable con un *phishing* especializado, ya que el acosador debe invertir tiempo en conocer a su víctima para ganar su confianza. No es una campaña que se lance masivamente para ver quien cae, un *groomer* basa su comportamiento con base a lo que sabe de su víctima, camparte material y entabla conversaciones de temas que sabe el menor sigue y/o le gustan, simulan ser sus amigos, y ganan su confianza ya sea con manipulación u ofreciendo regalos para obtener material sexual del menor que posteriormente puede ser usado para chantajearlo.

Según García V[48], aunque la mayoría de los depredadores usan perfiles falsos, se han encontrado algunos que usan su perfil verdadero; pueden ser desconocidos o conocidos, hasta familiares; pueden utilizar a la víctima para conseguir más víctimas en las etapas de extorsión y/o chantaje, puede ser un solo agresor o “una manada”, agresores que trabajan en grupo para atacar a su víctima.

Uno de los principales problemas para dar frente a estos ataques es que los engaños usados por los delincuentes pueden ser infinitos, varían de país en país, o de víctima a víctima, dependen también de la motivación del victimario y de la forma en que se acerca a su víctima.

5.4 SÍMBOLOS DE ALERTA DE *GROOMING* Y PORNOGRAFÍA INFANTIL.

Algunos estudios han permitido identificar acrónimos, figuras, y lenguajes, utilizados en ataques de *grooming* y pornografía infantil.

[48] USECIM El perfil criminal del Groomer. 2021

Según Zagalsky[49] hoy en día se han introducido abreviaturas procedentes generalmente del inglés, que esconden comportamientos de riesgo, relacionados con estos dos delitos.

De los cuales se citan algunos de ellos a continuación:

- PAW o PAN: *parents are watching o parents are near* / mis padres están observando o mis padres están cerca, en otros casos para la misma situación se coloca el número “99”
- GNOC: *Get naked on camera* / Desnúdate frente a la cámara
- GYPO: *Take your pants off* / Sácate los pantalones
- SUGARPIC: Pedido de una imagen sugerente, con “*sugar*” como término relacionado con sexo y “pic” con relación a “*picture*”/foto.
- 53X ó CU46: See (escrito con “c”) you (u) for (4) sex (6) / Nos vemos para tener sexo
- 1174: Meet in person at / Nos vemos en persona para
- 420: Weed / Marihuana
- CID: Acid & drugs / Ácido y drogas
- THOT, HOE, BOSH SBW y SLUB: Bitch / Zorra, perra o puta

Estudios lingüísticos también han intentado identificar patrones en las conversaciones entre abusador y menor, indicando que los temas de contenido sexual siempre son introducidos por el *groomer* con preguntas como “¿qué llevas puesto?, ¿cuáles son tus preferencias sexuales?, ¿cómo te gusta la ropa interior?, ¿cuáles son tus fantasías?50, también indican que el tipo de dinámica es tipo pregunta/ofrecimiento por parte del abusador y respuesta por parte del menor.

[49] ZAGALSKY ALEJO Los acrónimos sexuales y las palabras que pueden indicar ciberacoso en las redes sociales. [En línea] 18 de julio 2021 (Recuperado en septiembre de 2021) Disponible en: https://tn.com.ar/tecno/redes-sociales/2021/07/18/los-acronimos-sexuales-y-las-palabras-que-pueden-indicar-ciberacoso-en-las-redes-sociales/

[50] GARAIZABAL ELENA, HIDALGO IRENE. Detección De Depredadores Sexuales En Los Chats Y La Captación De Menores. El Papel De La Lingüística Forense. [En línea] 2020 (Recuperado en abril de 2023) Disponible en: https://digitum.um.es/digitum/bitstream/10201/96042/1/2549-6933-1-PB.pdf

Así mismo, investigadores de la policía[51] en Colombia han identificado acrónimos y figuras relacionadas con la publicación de pornografía infantil. Bajo las iniciales CP (*child pornography*), se esconden términos como “caldo de pollo”, “*club penguin*”, “código postal” u otras, aparentemente inofensivos, pero que les sirve a los delincuentes para identificar los contenidos publicados en internet relacionado con estos delitos.

En la figura número 8 se pueden ver algunos de los símbolos que ha identificado la policía y que identifican sitios de pornografía infantil, los azules indicando que son niños y los rosas para niñas.

Figura 7 Símbolos usados por delincuentes para identificar contenido pornográfico infantil

Fuente: EL TIEMPO. Autoridades siguen la pista a delincuentes que comparten esos contenidos en Google y redes sociales. [En línea] 23 de septiembre de 2019 (Recuperado en septiembre de 2021) Disponible en: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

[51] EL TIEMPO. Autoridades siguen la pista a delincuentes que comparten esos contenidos en Google y redes sociales. [En línea] 23 de septiembre de 2019 (Recuperado en septiembre de 2021) Disponible en: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

Como conclusión de este capítulo, se resalta que hay formas diferentes en las que un *groomer* puede acercarse a su víctima y diferentes perfiles de este tipo de delincuentes, por lo tanto, una solución integral para esta amenaza no se debe dejar en manos de los padres o los proveedores de redes sociales, y que al igual que la ciberseguridad como tal, debe ser une esfuerzo de todos los campos de la sociedad, tanto gobierno, sociedad, familia, ONGs, sectores privados, e invitar a los profesionales de distintos campos, como desde su área de experiencia pueden ayudar a proponer métodos de prevención para este tipo de ataques.

6 HERRAMIENTAS Y MÉTODOS ACTUALES PARA COMBATIR LOS ATAQUES DE INGENIERÍA SOCIAL CONTRA LA COMUNIDAD INFANTIL EXISTENTES EN LAS REDES SOCIALES.

En este capítulo se hablará sobre los métodos actuales que ofrecen las redes sociales para combatir esta amenaza, empezando por los recursos dados a los padres y niños para prevenir esta amenaza y siguiendo con los controles de las principales plataformas identificadas como son *Facebook, Instagram* y *WhatsApp.* Se aclara que estas medidas son servicios o funcionalidades que ofrecen cada una de las redes sociales.

6.1 APOYO A PADRES Y NIÑOS.

El primer frente de batalla será siempre la educación y los valores en casa. Teniendo esto en cuenta las principales herramientas que hoy en día se cuentan contra esta amenaza están enfocadas en la capacitación tanto de padres como de niños para prevenir el *grooming*.

Según el portal *save the children*[52] es importante una educación afectivo-sexual, para formar a la comunidad infantil y adolescente en materia de sexualidad, al tiempo que se forma en el uso seguro y responsable de las herramientas digitales.

En un artículo de Chauvan S[53] (S.F) se recopilan los concejos que se han visto durante esta investigación en distintos portales, en cuanto a lo que deben hacer los padres.

[52] SAVE THE CHILDREN. Grooming Qué Es, Cómo Detectarlo Y Prevenirlo 2019.
[53] CHAUVIN SILVIA. 12 Consejos Para Proteger A Los Chicos del Grooming. [En línea] (Recuperado en octubre de 2021) Disponible en: http://www.mujeresdeempresa.com/12-consejos-para-proteger-a-los-chicos-del-grooming/

- Establecer vínculos de confianza con sus hijos. Se debe recordar que un ataque de *grooming* es un engaño al menor, por lo tanto, él no es responsable de lo que pasa, es importante no hacerlo sentir culpable.
- Establecer horarios para el uso del dispositivo, en qué lugares puede usarlo y por cuanto tiempo.
- Dar ejemplo, no tener malos comportamientos en la red que los hijos puedan imitar, recordar que se debe dar ejemplo en cuanto temas de privacidad, lo que se debe y no se debe publicar.
- Al igual que en mundo real, se debe recordar a los hijos la importancia de no hablar con desconocidos.
- Acompañar a los hijos, en espacial los más pequeños, cuando hagan uso de los dispositivos.
- Contar con programas antimalware y antivirus en los equipos y dispositivos con los cuales se conecta a internet.
- Usar controles parentales para limitar las acciones que su hijo pueda hacer en la red.
- Concientizar a los hijos sobre los peligros que existen en la red.

En cuanto a los niños, hay campañas que les informa como prevenir estos ataques, como por ejemplo los que se encuentran en páginas de en TI confío, páginas del gobierno, de ONGs relacionadas con la protección infantil, entre otros, algunos de estos concejos como los publicados en la página del hospital *Sant Joan de Deu*[54] son:

- Rechazar mensajes que tengan contenido sexual y/o pornográfico.
- No publicar fotos en sitios públicos.
- Usar perfiles privados en *Facebook*, donde solo invite a sus amigos.
- Cuando suba una foto, piense si se siente bien con que todo el mundo la vea.

[54] SJD. Cómo evitar que los menores sufran grooming (acoso sexual por Internet) 2021

- Evitar compartir datos personales en redes sociales y/o con personas que no conozca.
- Bloquear aquellos contactos que no conozca personalmente
- Confiar en los padres, mantener comunicación con ellos de las cosas que observa en la red.
- No tenga contraseñas que se puedan descifrar fácilmente.

6.2 RECONOCIMIENTO DE PERFILES FALSOS.

Dado que muchos cibercriminales utilizan perfiles falsos para llegar a sus víctimas es importante tener ciertas pautas para reconocerlos.

Según el portal del gobierno de Argentina[55] reconocer un perfil falso es muy fácil, se puede identificar revisando las siguientes características:

- Identifique la primera fotografía que subió, si es reciente significa que el perfil fue creado hace poco, aunque no todos los perfiles nuevos son realizados con estos fines, es importante desconfiar de estos como primera medida.
- Las fotos que tiene no son de autoría propia, pueden ser encontradas en otros perfiles o en un banco de imágenes
- Revisar los *likes* de las fotos, en un perfil real los amigos del dueño de perfil comentarán y darán *likes* a sus fotos, la ausencia de ellos puede indicar un falso perfil, en el que probablemente publique fotos ajenas.
- Si hay comentarios, todos se refieren a resaltar la belleza física y no del momentos o situación en que se hizo la foto. Además, estas fotos tienden a ser de personas muy atractivas.
- Tiene muy poca información personal

[55] ARGENTINA.GOB ¿Cómo me doy cuenta si un perfil es falso en Facebook? [En línea] 2022. (Recuperado en marzo de 2023) Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-detecto-un-perfil-falso

- No participa en grupos y/o no tiene muchos posteos.

Certgov[56] dan otras pistas:

- Generalmente no tiene fotos de perfil, optan por frases, caricaturas, dibujos, entre otros.
- No comparte fotos de situaciones familiares o con amigos.
- No actualiza su perfil de forma frecuente
- Estos perfiles casi no interactúan en conversaciones ajenas, pero cuando interactúa con alguien, busca acceder a información personal.

6.3 *FACEBOOK* E *INSTAGRAM*.

Se reúnen estas dos plataformas ya que provienen de la misma empresa. El reconocimiento de perfiles infantiles generalmente se basa en la solicitud de ingreso de edad al crear el perfil, que como es evidente, depende de la buena fe de las personas.

Otras medidas de protección van dirigidas a la comunidad en general, y se relacionan más con riesgos de contenido. Se tiene por ejemplo la denuncia e identificación de material inadecuado; en la primera se hace un llamado a la comunidad para que denuncie imágenes o mensajes con contenidos inapropiados, en la segunda se usan algoritmos que permiten identificar estos contenidos y bloquearlos; aunque la segunda opción es bastante relevante ha tenido bastantes críticas, indicando que así como bloquea contenido inadecuado, también puede bloquear contenidos específicos atacando la libertad de expresión y manipulando la

[56] CERT.GOV.PY Perfiles falsos, grooming, extorsión – cómo cuidarse [En línea] 2021 (Recuperado en octubre de 2021) Disponible en: https://www.cert.gov.py/noticias/perfiles-falsos-grooming-extorsion-como-cuidarse

información, como lo indica un artículo en el portal IONOS[57], mientras que otras fuentes como PERFIL[58] dan indicadores de su eficacia, como por ejemplo que durante el cuarto trimestre de 2020, *Facebook* intervino en 34,3 millones de contenidos violentos o sensibles en el cuarto trimestre del 2020.

En la actualidad dados los recientes escándalos sobre el manejo de información y la protección de usuarios por parte de esta empresa, referentes al caso "*Facebook Files*", que se puede encontrar en ESQUIRE[59] donde indica que una ex empleada de la compañía reveló que "Mark Zuckerberg es consciente del efecto negativo que sus servicios provocan en la sociedad, y no hace nada al respecto" ha debido cambiar y crear nuevas políticas de protección.

En el caso de *Instagram*, por ejemplo, ya cuenta con nuevas propuestas encaminadas a la comunidad infantil como lo indica su portal *About Instagram*[60] es importante proteger a los miembros más jóvenes de la comunidad, para esto ha diseñado las siguientes funciones:

Recursos para ayudar a padres y adolescente: en colaboración con el *Child Mind Institute* y *ConnectSafely*, se han implementado nuevas configuraciones de seguridad, listas de concejos, puntos de partida para la comunicación. Estas

[57] IONOS. El filtro burbuja: la realidad a tu imagen y semejanza. [En línea] 23 de enero de 2020 (Recuperado en octubre de 2021) Disponible en: https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-filtro-burbuja/

[58] PERFIL. Cómo es el algoritmo que usa Facebook para controlar contenidos inapropiados. [En línea] 20 de mayo de 2021 (Recuperado en octubre de 2021) Disponible en: https://www.perfil.com/noticias/tecnologia/como-es-el-algoritmo-que-usa-facebook-para-controlar-contenidos-inapropiados.phtml

[59] GALAN RAFAEL. Facebook Files: El nuevo escándalo de la red social. [En línea] 05 de octubre de 2021 (Recuperado en octubre de 2021) Disponible en: https://www.esquire.com/es/tecnologia/a37862809/facebook-frances-haugen-archivos-escandalo/

[60] ABOUT INSTAGRAM. Seguimos haciendo de Instagram un lugar más seguro para los miembros más jóvenes de la comunidad. [En línea] 17 de marzo de 2021 (Recuperado en octubre de 2021) Disponible en: https://about.instagram.com/es-la/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community

relacionadas con ayuda a padres y jóvenes como los revisados al comienzo del capítulo.

Comprender la verdadera edad de las personas: Una política de *Instagram*, es que se debe tener una edad mínima de 13 años para usarlo. *Instagram* es consciente que no siempre se dice la edad verdad, ya sea por un menor que indique tener más, o un mayor que indique tener menos edad. Ya que identificar la edad de una persona a través del perfil es una tarea difícil, se están desarrollando tecnologías de inteligencia artificial y aprendizaje automático que permitan aplicar funciones de acuerdo con su edad, como, por ejemplo:

- Restringir los mensajes entre adolescentes y adultos a los que no siguen. Esta protección bloquea a los adultos enviar mensajes a menores de 18 años, si estos menores no lo siguen.
- Envío de mensajes que promuevan la cautela y prevengan a los adolescentes. También busca identificar si un adulto tiene comportamientos sospechosos advirtiendo al menor si este intenta interactuar con él. Por ejemplo, un perfil adulto que envía solicitudes de amistad a una gran cantidad de perfiles jóvenes, la aplicación avisará a estos jóvenes y les permitirá bloquearlo o reportarlo.
- También se busca que las cuentas de menores de edad se establezcan como privadas.

Como se puede observar por ahora, los esfuerzos de *Facebook* están relacionados con los riesgos de contenido en general, mientras que *Instagram* ya está tomando acciones para la comunidad adolescente. Sin embargo, la apreciación del filtro de *Facebook* es que probablemente está siendo utilizado para el escaneo de patrones con fines comerciales y la manipulación de contenido en la red; mientras que, en el caso de *Instagram*, aunque ya está tomando medidas más consientes con la comunidad adolescente, cabe resaltar que están ligadas a la identificación de la

edad indicada en el registro, por lo que puede haber una gran brecha de seguridad si el atacante se registra como menor.

6.4 *WHATSAPP*.

Aunque esta aplicación es más de mensajería que una red social, se incluirá en este trabajo, al ser reportada como un vector de *grooming*.

Esta aplicación es una de las menos seguras, no tiene controles sobre la edad, contenido u otros, por lo que la protección depende directamente del buen uso que se le dé.

El portal SanCristobal[61] informa sobre el uso responsable de la aplicación y los concejos que ya se han compartido antes para evitar riesgos en la red, también indica que las opciones de privacidad también son escasas: puede optar por “todo el mundo”, “contactos” o “nadie”, por lo que se concluye depende únicamente del cuidado y uso responsable de niños y adultos.

El portal *MacAfee*, Birdsong Toni[62] advierte de algunos riesgos a los que se pueden enfrentar los menores al usar esta aplicación:

- Están expuestos a contenido inapropiado que puedan recibir de otros contactos.
- Cualquier persona puede enviar un mensaje o unirse a un grupo si tiene el enlace de este

[61] SANCRISTOBAL. El uso responsable de WhatsApp por menores. [En línea] (Recuperado en octubre de 2021) Disponible en: https://www.sancristobalsl.com/blog/el-uso-responsable-del-whatsapp-en-menores/

[62] BIRDSONG TONI. ¿Es WhatsApp seguro para los niños? Lo que deben saber los padres. [En línea] 09 de marzo de 2020. Portal McAfee (recuperado en junio 2022) Disponible en: https://www.mcafee.com/blogs/es-es/family-safety/es-whatsapp-seguro-para-los-ninos-lo-que-deben-saber-los-padres/

- Se puede prestar para el ciberacoso por ejemplo con la función “Eliminar para todos”, esta función permite eliminar mensajes que se ha enviado por equivocación en un plazo de 60minutos, eliminándolo de ambos dispositivos (emisor y receptor), lo que puede ser usado para mandar mensajes amenazantes y dañinos, esperar que el receptor los lea y luego bórralos sin dejar rastro.
- También pueden estar expuestos a otros riesgos como: estafas, *malware* y propagación de noticias falsas.

Como se puede evidenciar el mayor esfuerzo en la prevención de estos ataques está en capacitar a padres y niños, dejando prácticamente toda la responsabilidad sobre sus hombros, y aunque las redes sociales ya están tomando conciencia de la importancia de proteger a sus usuarios sobre los riesgos digitales, en especial la comunidad infantil, hasta ahora están explorando soluciones y/o herramientas tecnológicas para implementar controles que permitan reducir estos riesgos. El análisis de puntos débiles de estas soluciones, así como la propuesta de mejores soluciones, son temas del próximo capitulo.

6.5 UNICEF Y EL ICBF

UNICEF es El Fondo de las Naciones Unidas para la Infancia, esta agencia con ayuda de la organización de las Naciones Unidas busca dar ayuda humanitaria a niños y madres, buscando garantizar la seguridad de los niños y defendiendo sus derechos de cuidado, participación y protección. Esta agencia vela por los derechos de la niñez a nivel mundial. Por otro lado, El ICBF o Instituto colombiano de Bienestar familiar, es “la entidad del Estado Colombiano que trabaja por la prevención y protección integral de la primera infancia, infancia y adolescencia, el fortalecimiento de los jóvenes y las familias en Colombia, brindando atención

especialmente a aquellos en condiciones de amenaza, inobservancia o vulneración de sus derechos"[63].

Según un documento publicado por el gobierno de México "La presencia de dispositivos móviles ha hecho que el acceso en línea para muchos niños esté menos supervisado y sea potencialmente más peligroso, son muy escasas las medidas que se toman para protegerlos de los peligros del mundo digital y para aumentar su acceso a un contenido seguro en línea." 64. Este documento publicado en 2020 hace referencia a informes creados por UNICEF sobre la seguridad de los niños en línea antes de la pandemia, lo que indica que estas organizaciones ya habían anunciado los peligros existentes en el mundo digital para los niños y la poca seguridad existente en él, y desde años anteriores a esta crisis quería llamar la atención del mundo para que entendiera que un entrono digital seguro, solo se puede crear desde un esfuerzo colectivo que incluya al gobierno, los sectores públicos y privados, la entidades académicas, las organizaciones de protección infantil, las familias e inclusive los mismos niños.

Sobre los riesgos en el mundo digital que afectan a los niños, el portal del ICBF ofrece información sobre su clasificación y cuáles son, parte de este trabajo toma información de este sitio; sobre su prevención ofrece pautas y concejos que se basan en la educación y acompañamiento por parte de padres y adultos responsables. Sin embargo, es importante anotar que ha adoptado y de hecho, promueve las 6 acciones indicadas por UNICEF que buscan favorecer los derechos digitales de la infancia, con las cuales como lo dice el ICBF en su portal "busca

[63] ICBF. El Instituto. [En línea] 2022 (Recuperado en 20 de septiembre de 2022) Disponible en: https://www.icbf.gov.co/instituto

[64] PUENTE DE LA MORA XIMENA. Que Adiciona El Artículo 4o. De La Ley General De Los Derechos De Niñas, Niños Y Adolescentes, En Materia De Alfabetización Digital Y Protección De La Niñez En El Uso De Internet, A Cargo De La Diputada Ximena Puente De La Mora, Del Grupo Parlamentario Del Pri. 2020 (Recuperado en abril de 2023) Disponible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4071722_20200915_1600122822.pdf

promover la mediación y participación entre los gobiernos internacionales, nacionales y locales, como también el de las empresas, los colegios y las familias para mitigar el riesgo, potencializar las oportunidades y defender los derechos de los menores de edad en Colombia y en el mundo" 65 entre los cuales se encuentran:

- Proporcionar a todos los niños acceso de alta calidad a recursos en línea, en busca de la igualdad de oportunidades en cuanto a uso, acceso, conocimiento y participación social.
- Proteger a los niños de los daños en línea, incluido el abuso, la trata, la explotación, el acoso cibernético y la exposición a materiales inadecuados. Donde se busca con el sector privado, en especial empresas de tecnología la realización de actividades centradas en la protección infantil.
- Proteger la privacidad y la identidad de los niños en línea, Donde se promueve la educación por parte de padres y docentes para guiar a los niños en que información es pertinente compartir y cómo comportarse en la red; y con las empresas para no explotar la información de los niños con fines comerciales y la utilización de lenguaje sencillo y claro para que ellos entiendan sus políticas de privacidad, así como la garantía de la protección de la información que manejan.
- Impartir alfabetización digital para mantener a los niños informados, comprometidos y seguros en línea, campañas de uso responsable de las TICs más allá del salón de clases.
- Aprovechar el poder del sector privado y promover normas o prácticas éticas que protejan y beneficien a los niños en línea, aquí se trabajan tres puntos, el primero ofrecer a los padres herramientas fáciles para mejorar la seguridad de sus hijos, por otro evitar que las redes y otros servicios difundan material de abuso infantil, y la tercera proporcionar acceso a internet a aquellos menos favorecidos.

[65] ICBF. Conoce las acciones prioritarias que favorecen los derechos digitales de la infancia. [En línea] 24 se marzo de 2021. (Recuperado en junio 2022) Disponible en: https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-las-acciones-prioritarias-que-favorecen-los-derechos-digitales-de-la

- Poner a los niños en el centro de la política digital, ya que actualmente las políticas de las TICs se centran es en los adultos, desconociendo que prácticamente 1/3 de la población digital es infantil, y que se deben crear políticas en pro de sus derechos y necesidades.

Esas acciones buscan un mundo digital más seguro y responsable para los menores de edad.

En la figura número 8 podemos ver un top de los peligros a los que se enfrentan los jóvenes en las redes sociales. Se aclara que el ícono solo hace referencia a una red social, pero no significa que este ligado directamente a la descripción del peligro.

Figura 8 Top de los riesgos en las redes sociales

Fuente: ATICO 34. Peligros de las redes sociales para niños y adolescentes. [En línea] 2022. (Recuperado en abril 2023) Disponible en: https://protecciondatos-lopd.com/empresas/peligros-redes-sociales/

En cuanto a las denuncias, el ICBF pone a disposición de las familias colombianas dos canales de atención para reportar cualquier situación que vulnere los derechos d ellos menores de edad en el entorno digital, uno es el CAI virtual de la policía nacional, y otra es la línea 141; esta línea es gratuita y busca dar una respuesta oportuna a los casos que se presenten, cuenta con un equipo calificado de especialistas entre los cuales existen psicólogos, abogados y trabajadores sociales, además de trabajar en red con otras entidades como la policía de infancia y adolescencia y la Red Mundial de Líneas de Asistencia para Niños, a través de la Fundación *Child Helpline International* que busca apoyar el fortalecimiento de canales de comunicación para la protección infantil.

7 ¿PORQUÉ SE DEBE MEJORAR LA SEGURIDAD INFANTIL EN EL CIBERESPACIO?

Actualmente no hay normas robustas o medidas que en este momento ofrezcan un espacio digital seguro a un menor de edad; la seguridad del entorno depende más que todo del comportamiento del menor en él y del acompañamiento y control de los padres. Los niños son una de las comunidades más vulnerables de la sociedad y están en un momento de sus vidas: la infancia, donde están desarrollando su personalidad, su autoestima y sus valores, los cuales se pueden ver afectadas por los riesgos que enfrentan en entornos digitales.

En cuanto a los riesgos de contenido un artículo de El mundo indica que “Daños psicológicos, adicciones o manipulación son algunas de las conductas que experimentan los menores tras una exposición prolongada a contenidos inadecuados para su edad” 66

Un contenido inadecuado puede ser de tipo ilícito, como terrorismo, fabricación de bombas, drogas, armas; o de tipo nocivo, peligroso o poco saludable que también puede ser ilícito pero que demás puede interferir con el desarrollo intelectual y emocional del menor.

Un menor de edad, esta apenas aprendiendo, creciendo y desarrollando su autoestima, es una edad en la que es vulnerable a nivel emocional y está construyendo su sistema de valores y su personalidad; cuando un niño es expuesto a contenidos que no es capaz de entender puede causar fobias y/o trastornos; cuando aún no tiene la capacidad de discernir conductas positivas o negativas, puede adoptar comportamientos dañinos y agresivos, tanto para otros como para el mismo; por eso es importante que los padres además de tener una comunicación

[66] EL MUNDO. Las consecuencias de que tus hijos naveguen por páginas inapropiadas. [En línea] 12 de octubre de 2020 (Recuperado en agosto de 2022) Disponible en: https://porunusolove.elmundo.es/contenido-inapropiado/las-consecuencias-de-que-tus-hijos-naveguen-por-paginas-inapropiadas

abierta con sus hijos, tengas a la mano herramientas que les permitan supervisar y controlar las actividades y búsquedas que tienen sus hijos en internet.

Entre los riesgos de conducta, se pueden citar los retos virales peligrosos, que muchas veces ponen el peligro la vida de los menores y que no son visibles hasta que ya han cobrado alguna víctima.

Algunos de estos retos son:

- 48 horas desaparecido: como su nombre lo indica, consiste en desaparecer sin dejar rastro durante 48 horas.
- El cascarón, se trata de consumir distintos alimentos en su envoltorio, en este caso huevos con cáscara, o dulces con sus empaques.
- Caza al pijo: En este reto se deben buscar en la calle adolescentes que lleven ropa de marca y/o artículos lujosos, para luego agredirlos de manera brutal mientras graban dicha acción para posteriormente subirle a sus redes.
- *Cha Cha Slide*: Consiste en subir a un coche en marcha al ritmo de la canción del mismo nombre.
- Rompecráneos: Para este se necesitan tres personas que salten al mismo tiempo en línea, los que están a los lados deben hacer que el del medio caiga de espalda, entre más duro suene el golpe mejor; este reto ya cuenta con una víctima de 16 años que murió tras un fuerte golpe en el cabeza ocasionado en la caída.
- El desmayo: Este busca atarse algo al cuello para cortar la respiración hasta desmayarse.

No se debe olvidar retos pasados como “Momo” o “la ballena azul”, que imponía a los jóvenes tareas para autolesionarse y en muchos casos incitar al suicidio. Una nueva variante es el caso de “Jonathan Galindo”, o también conocido como el “Goofy humano”, que contacta a los jóvenes a través de diferentes redes sociales, buscando ser sus amigos, una vez logra este propósito, les envía tareas agresivas, peligrosas y que incitan a lastimarse a sí mismos.

Por otro lado, los riesgos de contacto que en este trabajo se equiparan a ataques de ingeniería social en línea pueden llegar a desembocar en alteraciones del comportamiento del menor, así como en casos de explotación sexual en internet, acoso en línea y en los peores casos cuando el engaño pasa al plano físico en abuso sexual y graves agresiones físicas al menor.

Según el portal contigo conectados[67], algunas de las consecuencias que se pueden observar en los niños que han sufrido estos ataques son:

- Depresión infantil
- Pérdida de la autoestima
- Desconfianza
- Cambios de humor
- Bajo rendimiento académico
- Aislamiento
- Alteraciones del sueño y de la alimentación
- Pensamientos y comportamientos suicidas
- Heridas
- Traumatismos o lesiones derivadas de los actos sexuales
- Falta o mala relación de comunicación en la familia
- Chantaje a la propia familia por parte del atacante
- Modificación de su lenguaje corporal ante adultos
- Miedo a salir de casa
- Dolores de cabeza, náuseas, mareos, ataques de ansiedad, lesiones físicas sin justificación o diarreas frecuentes

[67] CONTIGOCONECTADOS. Grooming, la amenaza disfrazada de confianza que engaña a los niños en internet [En línea] (Recuperado en marzo de 2022) Disponible en: https://contigoconectados.com/sexualidad/grooming-la-amenaza-disfrazada-de-confianza-que-engana-a-los-ninos-en-internet/

A nivel de acoso en línea, la palabra *grooming* en Colombia aún no ha sido bien tipificado como tal en una ley que permita penalizaciones para acosadores por internet, sin embargo, se cuenta con herramientas para la denuncia de estos como el portal www.teprotejo.org. Se aclara que si bien hay formas que facilitan el denuncio de estas amenazas lo ideal es no denunciar sino prevenir.

En cuanto a la explotación sexual por internet, comparando entre el año 2019 contra el 2020, en este último las cifras de denuncias subieron en un 31%. Según un artículo de RCN Radio "La Red Nacional de Padres de Familia (Red PaPaz) reportó un aumento superior al 31% en los casos de menores de edad que han sido víctimas de explotación sexual en internet, durante el año 2020, en comparación al 2019, cifra que en lo corrido del 2021 ya supera el balance anterior a la pandemia" 68. A nivel mundial se han detectado hasta 252.000 páginas web con material de explotación sexual de niños, niñas y adolescente. En Colombia hasta febrero de 2022, ya se habían denunciado 2.280 casos de abuso sexual infantil de los cuales el 96.7% se trata de material de explotación sexual.

Según Unicef "La violencia es un acto deliberado que comete una tercera persona y, en esa medida, se debe y se puede prevenir." El *grooming*, el ciberacoso y las amenazas en internet se pueden interpretar como una forma de violencia contra la comunidad infantil, el mismo artículo reconoce que el uso del entorno digital "amplía el espectro de potenciales agresores fuera del núcleo familiar con quienes pueden interactuar desde el entorno digital, como pares o personas desconocidas" 69

[68] GUERRERO VALERIA. Se dispararon reportes de explotación sexual infantil por internet en 2020 [En línea] 24 de septiembre de 2021. Red PaPaz, RCN Radio (recuperado en marzo de 2022) Disponible en: https://www.rcnradio.com/colombia/se-dispararon-reportes-de-explotacion-sexual-infantil-por-internet-en-2020-red-papaz#:~:text=La%20Red%20Nacional%20de%20Padres,balance%20anterior%20a%20la%20pandemia.

[69] UNICEF Violencia contra niñas, niños y adolescentes en tiempos de COVID-191 [En línea] noviembre 2020 (Recuperado en marzo de 2022) Disponible en: https://www.unicef.org/lac/media/19611/file/violencia-contra-nna-en-tiempos-de-covid19.pdf

El uso de internet viene asociado a unos riesgos latentes que esperan a los niños en el entorno digital como los contenidos inapropiados, el *ciberbullying* y los depredadores; los depredadores están utilizando aplicaciones y creando estrategias para acercarse a los menores y hacerse pasar por sus amigos para obtener de ellos todo tipo de información y contenido.

Según un artículo publicado en diciembre de 2021 por infobae "Se detalló que entre los principales delitos informáticos está el grooming, nombre que recibe la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital. Se registraron 516 incidentes de este crimen. En segundo y tercer lugar está la sextorsión con 62, y el ciberbullying con 325." 70

Las cifras registradas no parecen disminuir, por lo que es importante evaluar cómo se pueden mejorar las estrategias de seguridad y como ayudar a los padres a hacer de internet un sitio más seguro que permita la recreación y el conocimiento para los menores.

[70] INFOBAE. Delitos informáticos en Colombia subieron un 17 % en el 2021: sepa cómo prevenirlos. [En línea] 26 de diciembre de 2021. (Recuperado en 14 de mayo de 2022) Disponible en: https://www.infobae.com/america/colombia/2021/12/27/delitos-informaticos-en-colombia-subieron-un-17-en-el-2021-sepa-como-prevenirlos/#:~:text=Se%20registraron%20516%20incidentes%20de,en%20esta%20%C3%A9poca%20de%20vacaciones.

8 ESTRATEGIAS PARA MEJORAR LA SEGURIDAD DE LA COMUNIDAD INFANTIL EN REDES SOCIALES

En este capítulo se evaluarán distintos elementos utilizados para la conexión al entorno digital y cómo estos pueden ayudar a los padres a crear un ambiente más seguro; así mismo, se hace una reflexión de cómo las tecnologías aplicadas hoy en día para mejorar las experiencias del cliente pueden ser usadas para mejorar la seguridad de la comunidad infantil en las redes sociales.

8.1 ENFOCADOS EN PADRES.

Como se ha dicho antes, la mayoría de las medidas para proteger a la comunidad infantil se basa en la educación de padres e hijos en el buen uso de los entornos digitales, y la creación de lazos de confianza entre ellos, sin embargo, la tecnología actual ofrece muchas características para ayudar a los padres a mitigar situaciones de riesgo y llevar a cabo las recomendaciones hechas por los expertos en cuanto al control que deben tener sobre sus hijos en el mundo digital.

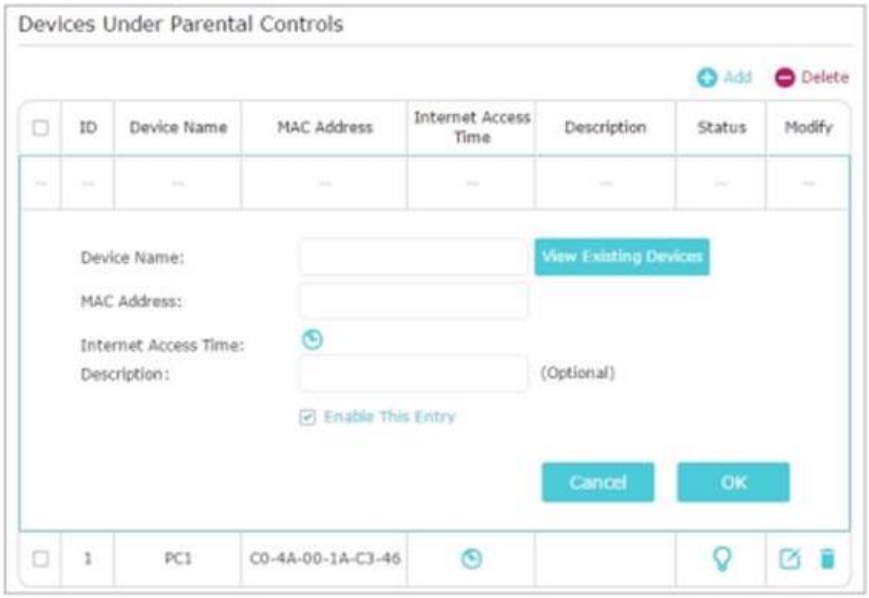
Bajo el nombre de controles parentales, se encuentran una serie de características que ayudan a controlar no sola las actividades del menor, sino a denunciar y evitar situaciones de riesgo. La mayoría de estos controles son externos a las plataformas de redes sociales, pero en el ejercicio del uso del entorno digital ayuda a mitigar las situaciones de riesgos que se encuentran en estas. Una combinación de estos controles que abarque desde el sistema operativo, navegadores y aplicaciones especializadas pueden ayudar a mitigar los riesgos que el menor corre, no solo en las redes sino en todo el mundo virtual.

8.1.1 ***Router.*** es el dispositivo que se usa para la conexión a internet, muchos de ellos ofrecen servicios que permiten la creación de reglas para limitar el acceso al uso de internet, esto es muy útil para establecer de manera eficaz los tiempos en que el menor puede estar conectado.

Se puede ingresar a través del navegador de internet a la interfaz de configuración del *router*, para esto se debe contar con la IP de administración, se ingresa a esta con un usuario y contraseña, si no lo conoce podría comunicarse con el operador de internet y preguntar por esta consola de administración. Esta interfaz permite cambiar la contraseña de la red, mirar los dispositivos conectados a ella y muchas veces establecer tiempos en los que se permite o no el servicio, estos también son conocidos como controles parentales que ofrece el propio enrutador.

En la figura número 9 se puede observar el servicio de restricciones que ofrece un *router* inalámbrico Tp_Link

Figura 9. Pantalla principal Control Parental *Router* TP -LINK



Fuente: TPLINK. How to configure Parental Controls on the Wi-Fi Routers (case 1)? [En línea] 18 de marzo de 2022. (Recuperado en 12 de abril de 2022) Disponible en: https://www.tp-link.com/co/support/faq/1531/

En la anterior interfaz se ingresan los dispositivos que tenga en casa, en este ejemplo en particular la dirección MAC privada de los dispositivos debe estar deshabilitada en sus clientes o el control parental no tendrá efecto. Una vez ingresado el dispositivo en la consola usted puede crear reglas para que los dispositivos no tengas internet en horas de la noche, o para que accedan o no accedan a ciertos tipos de páginas durante determinadas horas del día. Un ejemplo del proveedor es bloquear la página de Facebook durante el horario que el menor realice sus tareas, o bloquear todo el contenido y solo permitirle el acceso a páginas como Wikipedia.

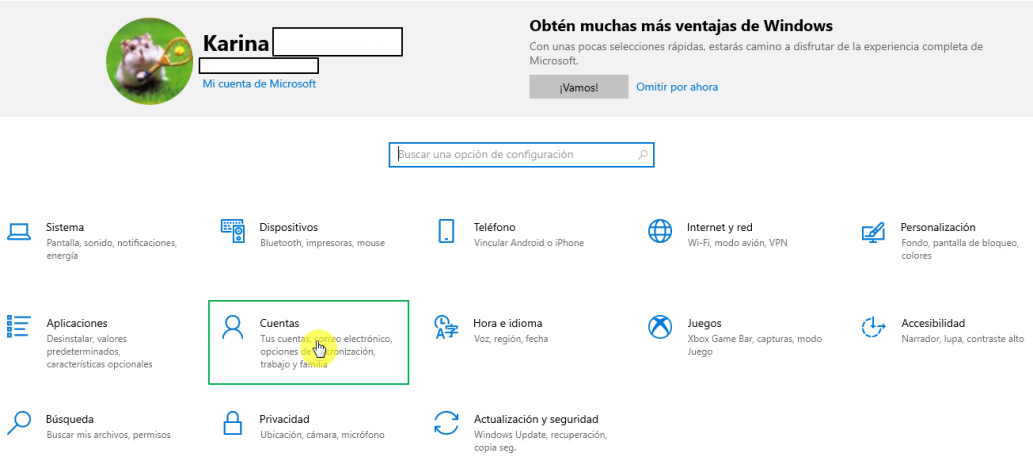
Las características de la interfaz y las funcionalidades pueden variar entre marcas y modelos, pero esta información es publicada por cada proveedor para ser consultada por el público en general.

8.1.2 **Sistemas Operativos**. Uno de los sistemas operativos más usados es Windows; con Windows 10 se puede crear una cuenta para el menor y adicionarla a un grupo familiar que permite a la familia controlar la actividad y configurar restricciones de edad, contenido, aplicaciones y tiempo de actividad. Esta información que muchos desconocen se puede encontrar en el siguiente enlace: ControlesParentalesWindows

Lo primero es crear una cuenta para el menor, en este caso se debe dirigir a configuración de Windows – cuentas

En la figura número 10 podemos ver la interfaz de configuración de Windows 10 y el apartado de cuentas que se debe seleccionar.

Figura 10 Configuración de Windows

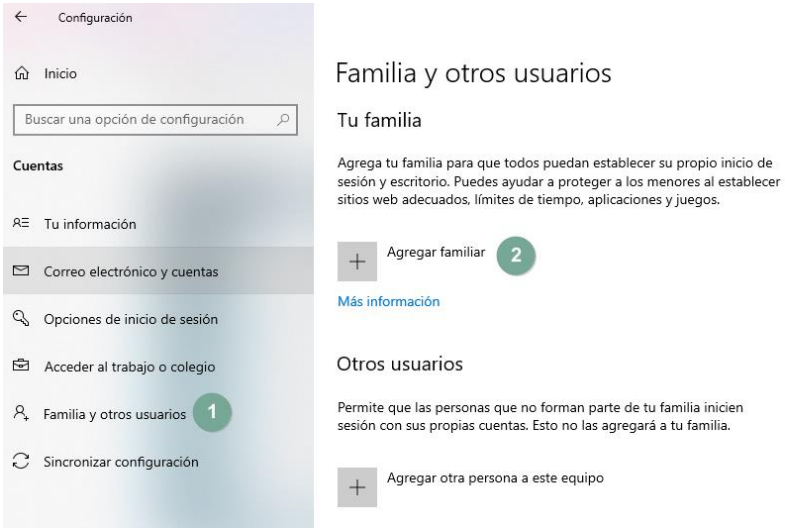


Fuente: Elaboración propia

Una vez aquí, en el menú del lado izquierdo escoja Familia y otros usuarios y luego agregar familiar.

En la figura 11 podemos ver las opciones indicadas para agregar un familiar

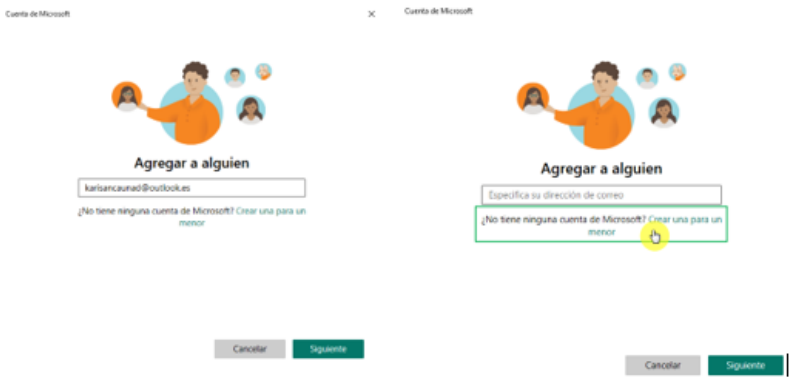
Figura 11 Opción agregar Familiar



Fuente: Elaboración propia

Ahora se puede agregar una cuenta de correo existente o crear una nueva desde cero. En la figura 12 podemos ver las opciones para agregar la cuenta.

Figura 12 Opciones para agregar una cuenta al grupo familiar



Fuente: Propia

En este ejercicio se trabaja con una cuenta ya creada y se agrega como miembro de la familia.

En la figura 13 se pueden observar los roles que se pueden asignar, en este caso debe ser miembro

Figura 13 Roles que se pueden asignar al usuario

Fuente: Elaboración propia

Se procede a invitar al usuario al grupo familiar.

En la figura número 14 se muestra cómo confirmar la invitación del menor

Figura 14 Finalizar invitación

Fuente: Propia

En estos momentos, se agrega la cuenta, pero queda en estado pendiente.

En la figura 15 se puede observar el estado pendiente de la cuenta

Figura 15 Estado de cuenta pendiente

Fuente: Propia

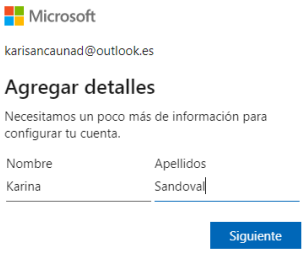
Se debe ir a la cuenta del menor para que acepte la invitación.
En la figura 16 se ve cómo es el correo que le llega al menor para que acepte la invitación.

Figura 16 Invitación

Fuente: Elaboración propia

En este paso el menor debe aceptar la invitación, haciendo clic en el botón que se ve en la imagen. Luego pedirá confirmar el nombre.
En la figura 17 muestra el sistema pidiendo el nombre del menor que se va a unir al grupo familiar.

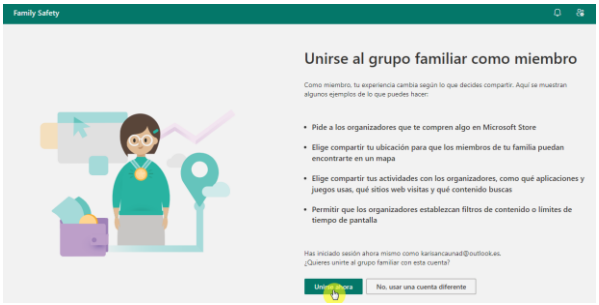
Figura 17 Solicitud Nombre



Fuente: Elaboración Propia

En la figura 18 podemos ver que el sistema confirma nuevamente si el menor quiere unirse al grupo.

Figura 18 Confirmación para unirse al grupo familiar

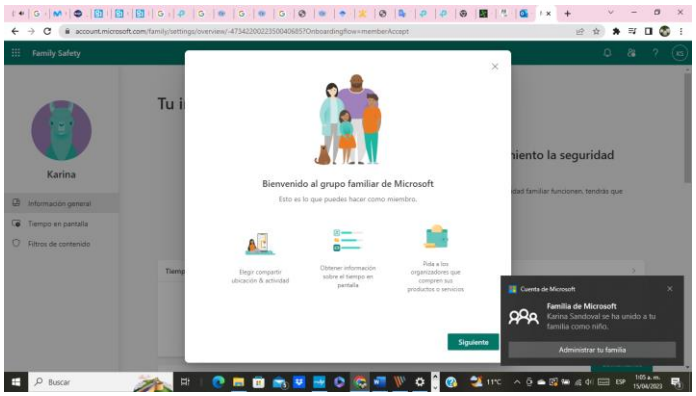


Fuente Propia

Finalmente, el sistema da la bienvenida al nuevo miembro del grupo familiar, al mismo tiempo que envía un mensaje al usuario administrador (padre) que se ha unido un nuevo miembro a la familia.

En la figura 19 podemos ver tanto la pantalla de bienvenida que verá el menor al unirse al grupo, como el mensaje que recibe el padre por correo cuando su hijo a aceptado la invitación.

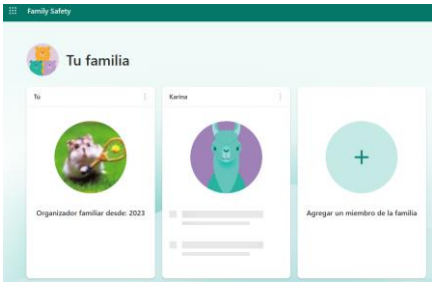
Figura 19 Pantalla de bienvenida y mensaje de confirmación



Fuente: Elaboración propia

En la figura 20 se puede observar la interfaz web que tiene el padre para administrar los distintos miembros del grupo

Figura 20 Interfaz web de *Family Safety*

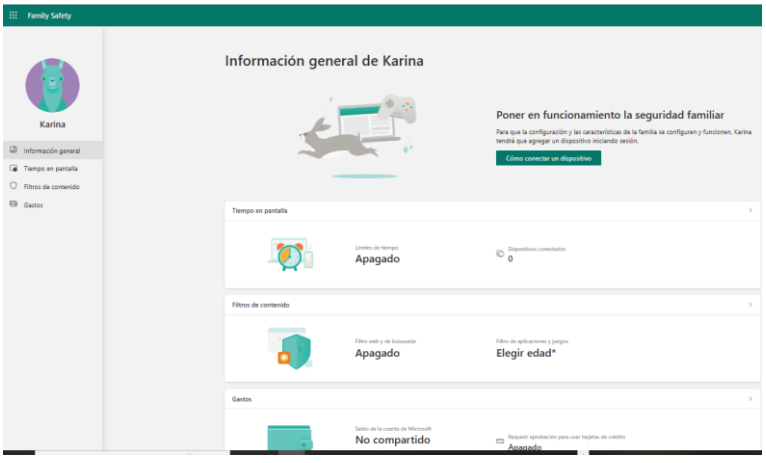


Fuente: Elaboración propia

Si ingresa al perfil del menor puede observar las opciones que tiene de control parental, entre las cuales está la funcionalidad de limitar el tiempo del menor para usar el dispositivo, el filtrado web para contenido malicioso, y una tercera opción que permite al padre dar un presupuesto para compras en la tienda de Microsoft.

En la figura 21 se puede observar las tres opciones de control parental que ofrece el portal web

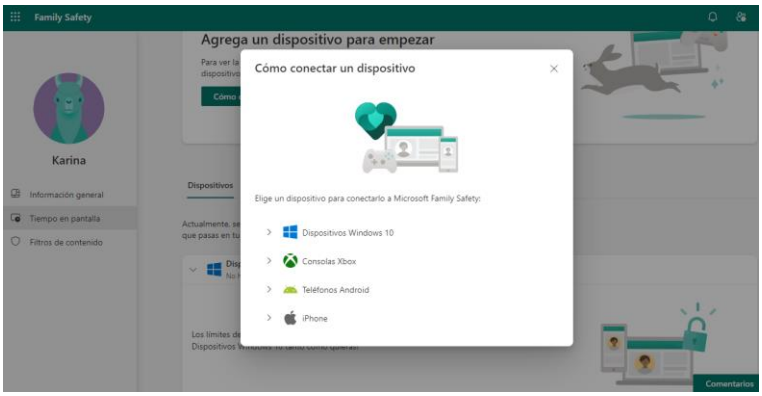
Figura 21 Interfaz del perfil del menor



Fuente: Elaboración propia

Es importante aclarar que para que estos controles sean efectivos, el menor debe ingresar al dispositivo con la cuenta que se agregó al grupo familiar.
En la figura 22 se observa la ventana de ayuda para dar las instrucciones de como conectar distintos dispositivos.

Figura 22 Ventana de ayuda para conexión a distintos dispositivos.



Fuente: Elaboración propia

En la figura 23 vemos las instrucciones para un equipo Windows 10 como lo podría ser un pc.

Figura 23 Instrucciones para dispositivo Microsoft.

Fuente: Elaboración propia

Una vez se empiezan a vincular los dispositivos, se habilitan las opciones para configurar las herramientas de control parental.

En la figura 24 vemos más detalles acerca del filtrado web.

Figura 24 Interfaz del Control Web

Fuente: Elaboración propia

En la figura 25 vemos la interfaz para el control de tiempo, discriminado por días y horarios.

Figura 25 Interfaz Control de Tiempo

Fuente: Elaboración propia

Windows 11 es la versión más reciente de sistema operativo de Microsoft, este sigue teniendo las mismas características que su antecesor.

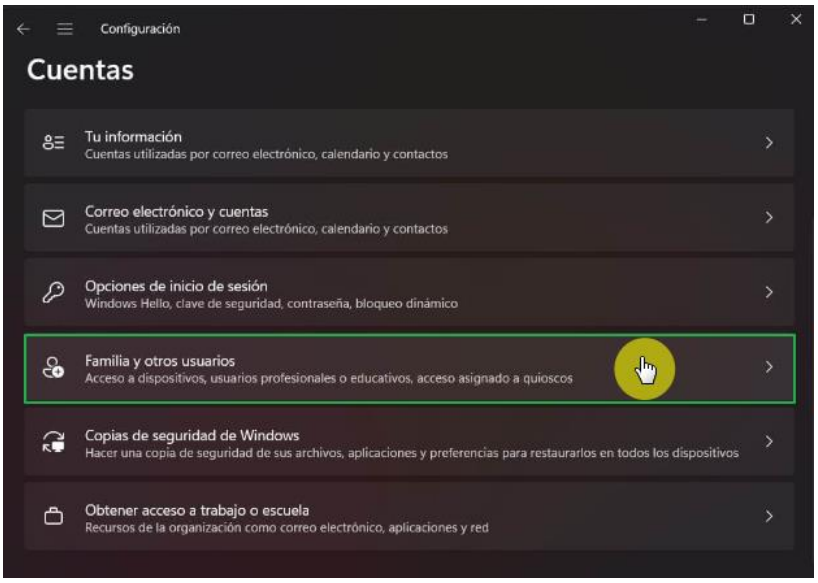
Es importante aclarar como ya se vio en el apartado anterior que para que el control parental funcione el menor debe tener una cuenta de correo activa conectada al portal de Microsoft y esta debe ser incluida dentro de un grupo familiar; la mayoría de estas características se gestionan desde un navegador.

El primer paso crear una cuenta de usuario para el menor, para esto siga estos pasos:

- Ir a configuración de Windows
- Abrir el apartado de cuentas
- Escoger Familia y otros usuarios

En la figura 26 se ve como crear la cuenta desde un sistema operativo Windows 11.

Figura 26 Configuración cuentas windows 11



Fuente: Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

En la figura 27 se observa la opción de agregar un familiar

Figura 27 Opción agregar Familiar

Fuente: Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

En la figura 28 se observa las opciones para conectar la cuenta, como se puede observar la interfaz no cambia con respecto a su antecesor Windows 10.

Figura 28 Opciones para conectar la cuenta de correo

Fuente: Elaboración propia

En este caso se va a mostrar el proceso si el menor no cuenta con una dirección de correo, en este caso en el paso anterior se escogió “Crear una cuenta para un menor”

En la figura 29 se puede observar la solicitud del nombre para la nueva cuenta de correo

Figura 29 Creación de cuenta

Fuente: Elaboración propia

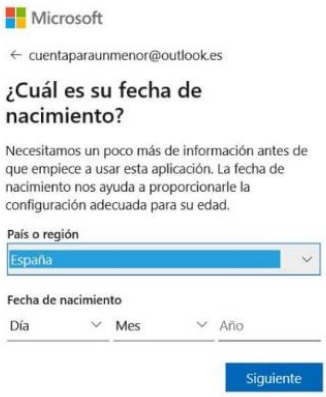
En la figura 30 se ve la solicitud de la contraseña, coloque una contraseña segura así sea para un menor, que contenga combinación de letras (mayúsculas, minúsculas), números y caracteres especiales.

Figura 30 Solicitud contraseña

Fuente: Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

En la figura 31 se ve algunos otros datos solicitados para terminar de configurar la cuenta del menor.

Figura 31 Otros datos de configuración



Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

En este caso como se creo la cuenta directamente la confirmación de la unión al grupo familiar llega directamente.

Figura 32 Confirmación vinculación cuenta menor

Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

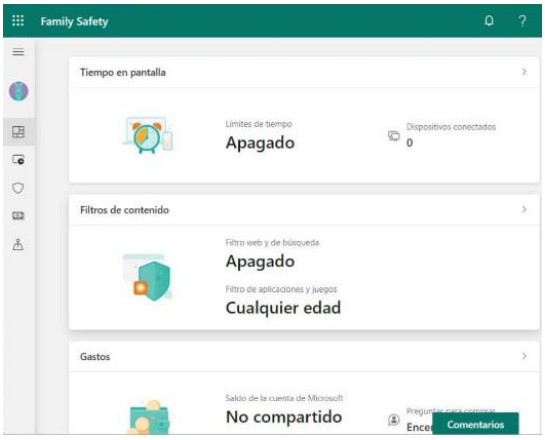
En la figura 33 se puede ver ya como queda habilitada la cuenta y el enlace para el portal de control parental.

Figura 33 Cuenta de menor agregada

Fuente: OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

En la figura 34 se puede observar el portal de control parental, el cual no ha sufrido cambios desde su versión anterior.

Figura 34 Portal de control parental Microsoft

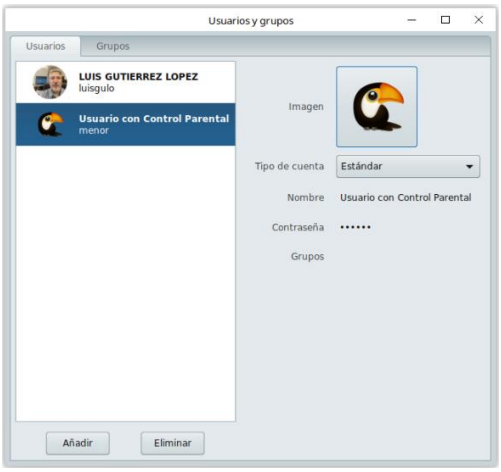


Fuente: Elaboración propia

En el caso de los sistemas operativos Linux, los controles parentales vienen como paquetes para ser instalados y configurados.
Al igual que con Windows, lo primero es crear una cuenta de usuario para el menor, lo cual lo podemos hacer desde la interfaz gráfica, en configuración – usuarios y grupos.

En la figura 35 podemos ver la interfaz gráfica para crear cuentas en un sistema Ubuntu – Linux.

Figura 35 Creación de cuenta para menor en Linux

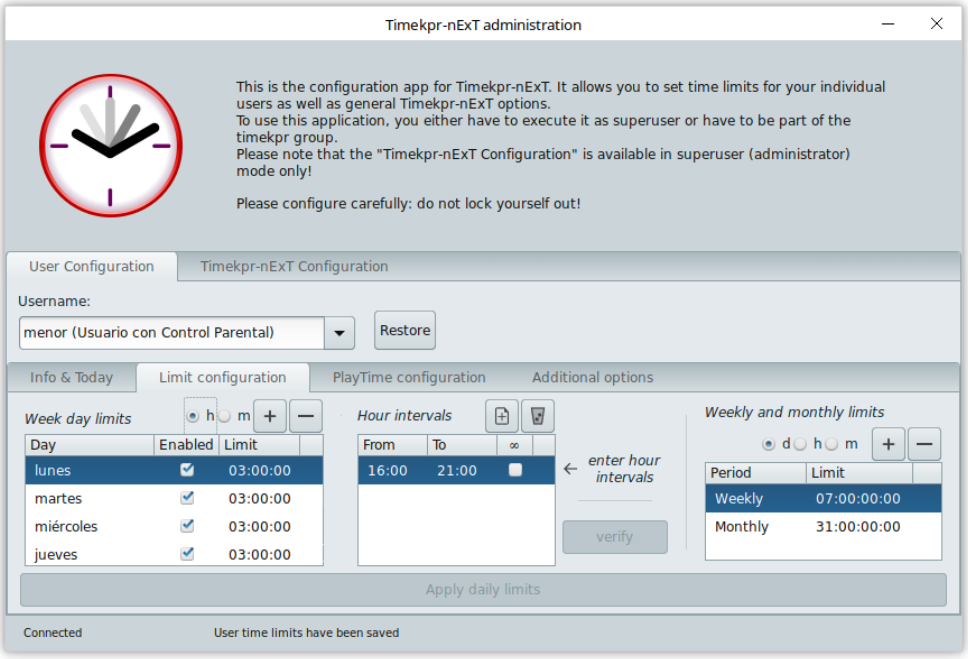


Fuente: GULO LUIS. Control Parental en Linux. [En línea] 19 de enero de 2023. (Recuperado den marzo de 2023) Disponible en: https://soloconlinux.org.es/control-parental-en-linux/

Luego procedemos a instalar los paquetes de control parental:
Para poder controlar el tiempo de uso y/o la franja de tiempo permitida se puede usar la herramienta timekpr-next
apt-get -y install timekpr-next
Esta aplicación permite indicar a que horas se puede hacer uso del equipo, o limitar el número de uso de horas diarias, actualmente soporta todos los directorios disponibles.

En la figura 36 se puede observar la interfaz gráfica de timekpr-next

Figura 36 Timerkpr-next



Fuente: GULO LUIS. Control Parental en Linux. [En línea] 19 de enero de 2023. (Recuperado den marzo de 2023) Disponible en: https://soloconlinux.org.es/control-parental-en-linux/

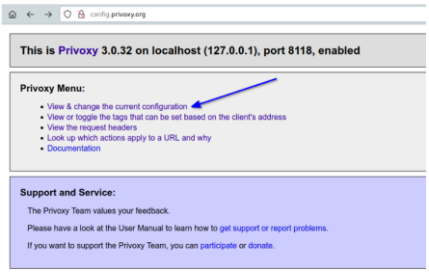
Para filtrar el contenido web se puede usar la herramienta Privoxi. Se instala con el siguiente comando

apt-get -y install privoxy

Esta herramienta es tan confiable, que algunas oficinas la utilizan como contrafuegos, incluso permite eliminar algunos tipos de anuncios que salen al navegar en internet.

Como se observa en la figura 37 se administra desde una interfaz web local

Figura 37 Interfaz Privoxy



Fuente: GULO LUIS. Control Parental en Linux. [En línea] 19 de enero de 2023. (Recuperado den marzo de 2023) Disponible en: https://soloconlinux.org.es/control-parental-en-linux/

La herramienta malcontent ayuda a controlar que aplicaciones puede ejecutar el menor. Se instala con la siguiente línea de comandos.

sudo apt -y install malcontent malcontent-gui

En la figura 38 podemos ver la interfaz de la herramienta malcontent

Figura 38 Malcontent

Fuente: GULO LUIS. Control Parental en Linux. [En línea] 19 de enero de 2023. (Recuperado den marzo de 2023) Disponible en: https://soloconlinux.org.es/control-parental-en-linux/

Otras herramientas útiles para el filtrado web pueden ser:

- Gnome nanny
- E2guardian
- WebContentControl
- SquidGuard
- MintNanny
- DansGuardian
- PeerGuardian

Otro aspecto por resaltar de Linux es que, así como tiene distintas distribuciones especializadas para adultos, también las tiene para niños. Estas distribuciones están enfocadas en la educación mediante el juego y el entretenimiento.

- Debian Edu / Skolelinux (3-18 años)
- Kano OS (7-14 años)
- Leeenux Kids (3-12 años)
- Qimo for kids (<3 años)
- PuppyLinux (2-15 años)
- Dodudolinux (> 2 años)
- UberMix (estudiantes de todas las edades)

En la figura 39 podemos observar algunos de los escrotirios de distribuciones linux para niños.

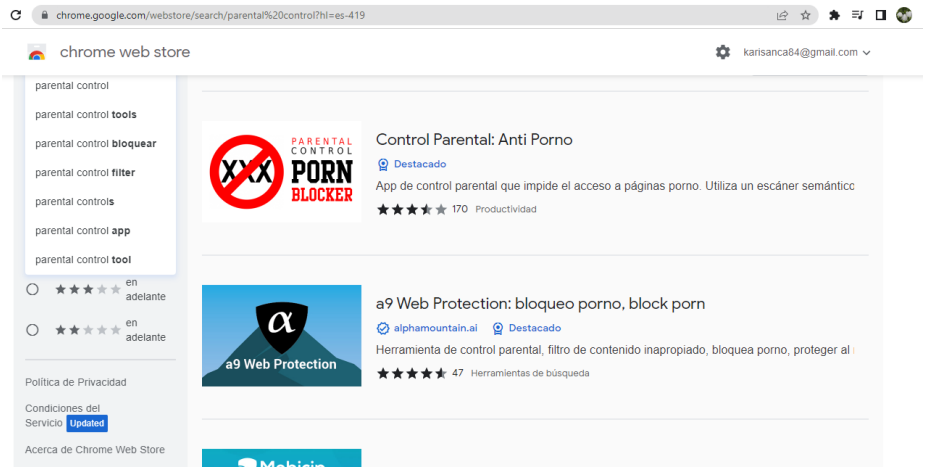
Figura 39 Distribuciones infantiles

Fuente: Elaboración propia

8.1.3 **Navegadores.** Por el lado de los navegadores, Chrome, Opera y Mozilla no tienen herramientas de control parental, pero si admiten extensiones que permiten el filtrado de contenido.

En la figura 40 se muestran algunas extensiones de control parental disponibles en Google Chrome.

Figura 40 Controles Parentales en Chrome

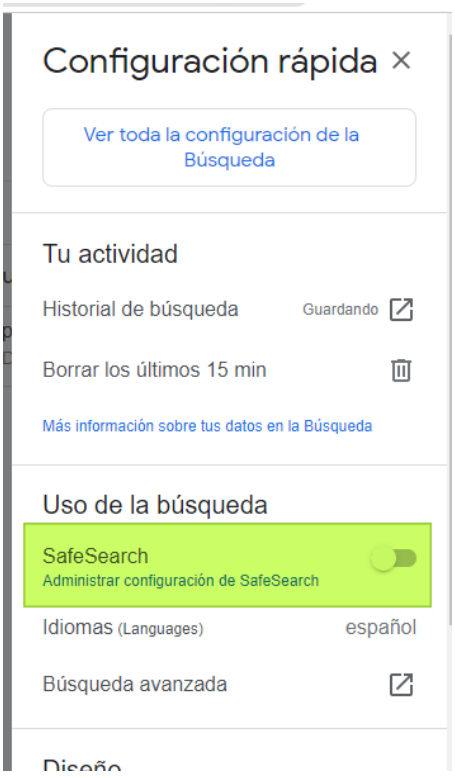


Fuente: Elaboración propia

Google posee una característica llamada *SafeSearch*, que se puede activar y desactivar desde el navegador, y esta alienada con las políticas de contenido de Google, busca bloquear contenido explicitó de sexo, drogas, violencia y/o odio. Para activarla basta con hacer una búsqueda, hacer clic en el engranaje y activar la característica.

En la figura 41 se puede ver la configuración rápida que se habilita el engranaje de la parte superior derecha cuando se hace una búsqueda y la forma de habilitar *Safe Search.*

Figura 41 *Safe Search*



Fuente: Elaboración propia

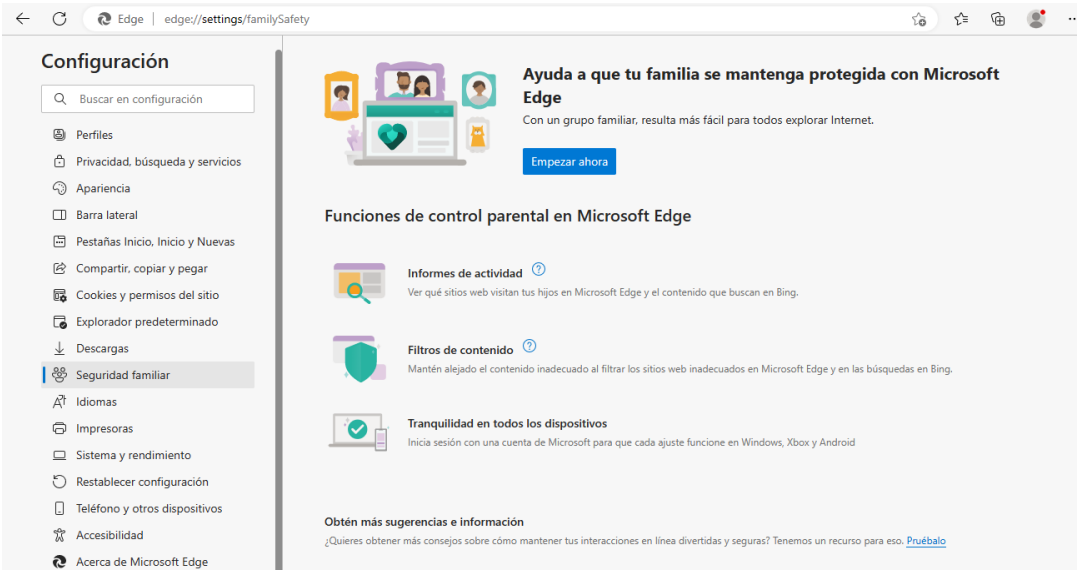
Firefox por su lado permite la integración con los controles parentales instalados en el equipo y habilita un modo de preferencia seguro para la navegación de los hijos; también cuenta con extensiones que permiten el filtrado web.

Así mismo en los distintos navegadores se puede bloquear el acceso a ciertas páginas que el padre halla identificado como sospechosas creando listas blancas y/o negras de sitios para el acceso o bloqueo de navegación; también es importante revisar el historial, para saber dónde ha estado navegando el menor.

En el paso de Edge se puede ir a configuración – seguridad familiar. Estas características esta relacionadas con los controles parentales del sistema operativo, por lo tanto, son administradas desde portal de *Microsoft Family Safety.*

En la figura 42 se ve como desde la configuración del navegador Edge se puede encontrar la opción de seguridad familiar.

Figura 42 Configuración de Edge - Seguridad Familiar



Fuente: Elaboración propia

En la figura 43 se muestra la ventana informativa que básicamente llevará al usuario al portal de seguridad familiar.

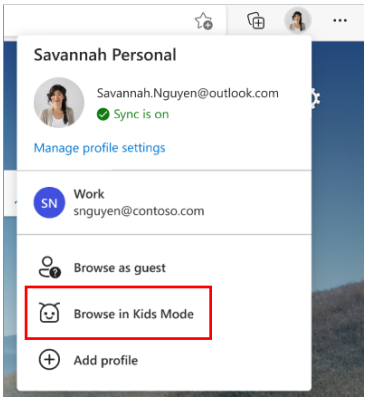
Figura 43 Redirección al portal de control parental

Fuente: Elaboración propia

Sin embargo, dado que hoy en día ya se tiene más conciencia sobre la importancia de la protección infantil en internet, Edge está mejorando de forma escalonada sus controles, actualmente existe un modo de navegador para niños, sin embargo, esta limitado a la versión en inglés. El modo para niños cambia totalmente el aspecto del navegador. Se puede configurar para niños de 5 a 8 años, o de 9 a 12. En ambos rangos se pueden crear filtros para texto, imágenes y videos.
Para activarlo debe ir al globo de la imagen de su perfil en la parte superior derecha y escoger la opción, navegar en modo niño

En la figura 44 se observa cómo se habilita la opción de navegar en modo niño.

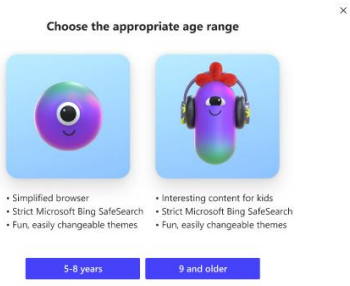
Figura 44 Navegación en modo niño



Fuente: MICROSOFT. Más información sobre el modo Niños en Microsoft Edge. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

En la figura 45 se pueden ver los rangos de edades que se pueden escoger para el menor.

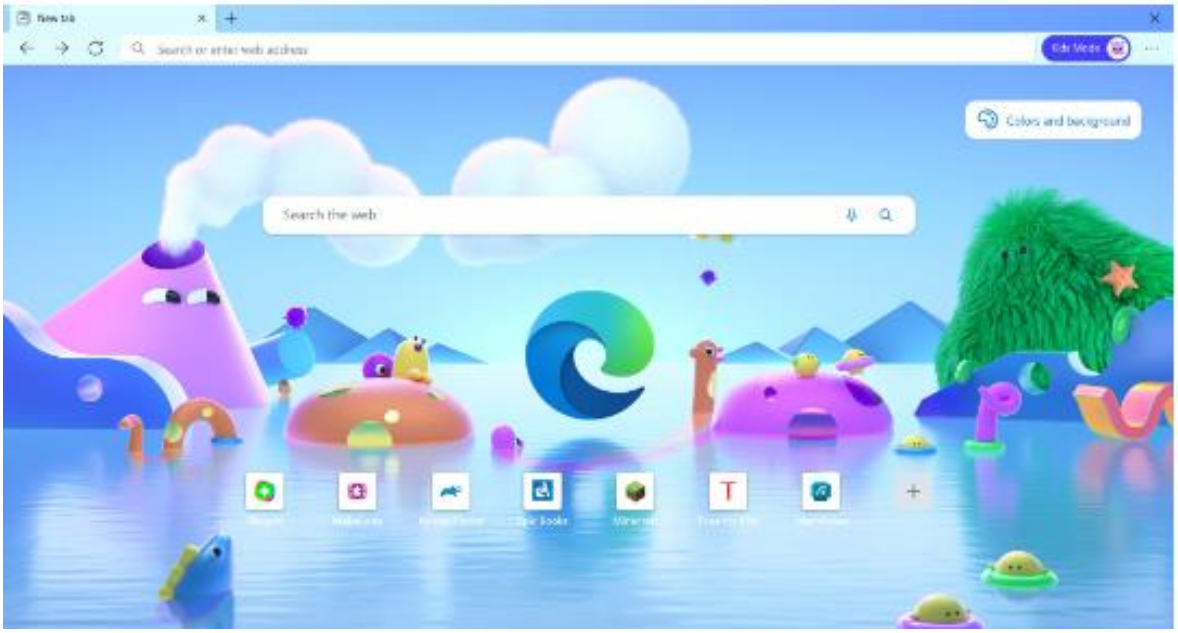
Figura 45 Rangos de edad navegación modo niño



Fuente: MICROSOFT. Más información sobre el modo Niños en Microsoft Edge. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

Una vez seleccionada la opción se guardará esta configuración, se cerrará la ventana actual y se abrirá una nueva ventana en modo infantil en pantalla completa. En la figura 46 se observa la interfaz del navegador en modo niño

Figura 46 Modo Niño

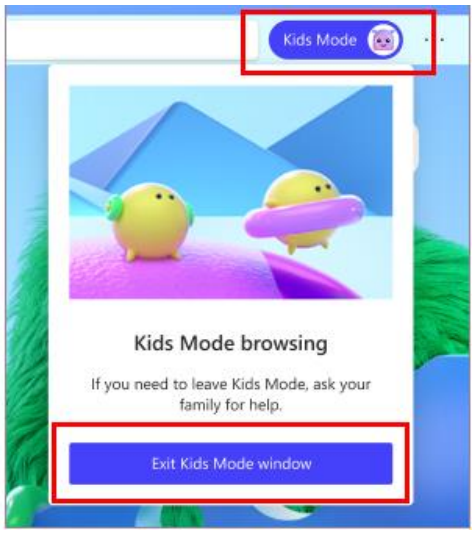


Fuente: MICROSOFT. Más información sobre el modo Niños en Microsoft Edge. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

El sistema le pedirá credenciales para salir, que son las mismas con las que desbloquea el equipo. De lo contrario empezara en este modo de forma predeterminada.

En la figura 47 se observa como desactivar la navegación modo niño.

Figura 47 Salir del modo niño de navegación



Fuente: MICROSOFT. Más información sobre el modo Niños en Microsoft Edge. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

8.1.4 **Antivirus.** Los antivirus poseen características que, así como los navegadores permiten crear listas blancas o negras, además que pueden escanear las páginas para saber si son seguras o no, sin embargo, empresas como karspesky y Norton van un paso más allá y ofrecen servicios de antivirus un poco más especializados en los menores de edad.

Kaspersky *safe kids*, es una de ellas; esta permite bloquear el acceso a contenido inapropiado, se pueden crear listas blancas de acceso, además protege el acceso a sitios de contenido para adultos, y permite bloquear búsquedas de temas inapropiados, establecer límites de tiempo y rastrear su ubicación; en este caso va más allá de saber dónde está, sino que permite establecer zonas seguras y avisar al padre en caso de que el niño salga de esta.

En la figura 48 vemos dos opciones de karspesky, resaltando las características que tiene la versión gratuita.

Figura 48 Opciones Karspesky

Fuente: Karspesky. *KasperskySafe* Kids. [En línea] 2023. (Recuperado en marzo de 2023) Disponible en: https://latam.kaspersky.com/safe-kids

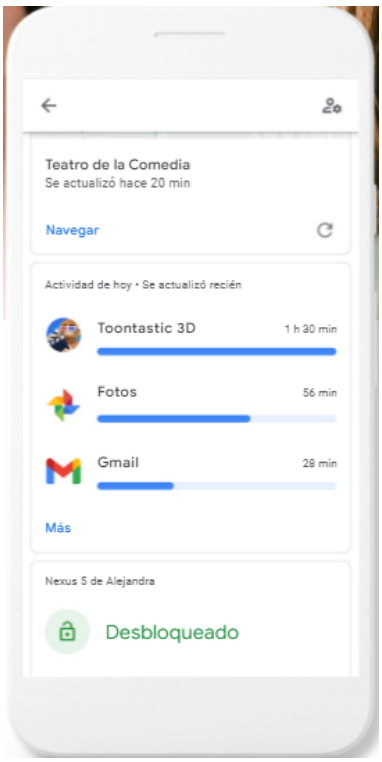
Norton family, ofrece servicios de seguridad en navegación, creación de informes relacionada con las búsquedas de sus hijos, bloqueos de páginas, limitación de tiempos, alertas por correo por ejemplo cuando al menor insista en el ingreso de una página bloqueada por contenido inapropiado.

McAfee no cuanta con un producto especializado, pero tiene un control parental que está disponible solo para los clientes de McAfee que hayan recibido McAfee Security a través de Telstra.(La principal empresa de telecomunicaciones y tecnología de Australia)

8.1.5 **Aplicaciones de monitoreo.** Para reforzar estos controles se pueden descargar aplicaciones más especializadas en controles; para el control en dispositivos Android se puede evaluar la *Family Link* de Google “Familia de Google” Esta aplicación permite consultar informes de actividad de tiempo y navegación del menor.

En la figura 49 se puede observar la interfaz de Familia de Google para el monitoreo de tiempo de actividad en línea

Figura 49 Informes actividad para dispositivos android

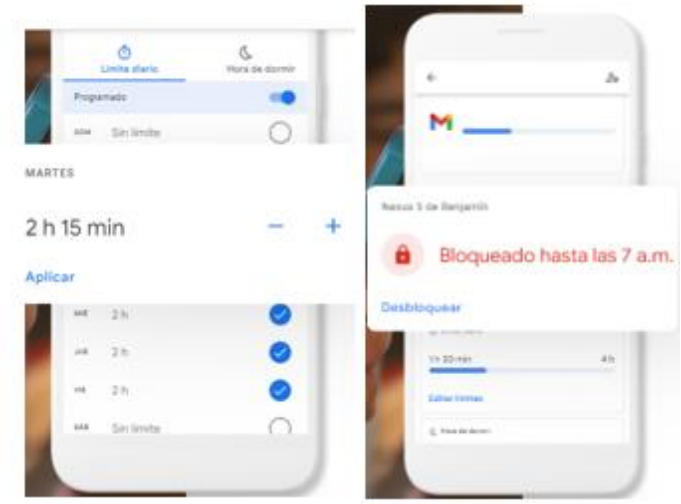


Fuente: FAMILIES GOOGLE. Ayuda a tu familia a adoptar hábitos digitales saludables. [En línea] (Recuperado en marzo de 2022) Disponible en: https://families.google.com/intl/es-419/familylink/

También permite fijar límites de tiempo del uso del dispositivo, logrando que se bloquee después del límite establecido, establecer una hora para ir a dormir o bloquearlo de manera remota.

En la figura 50 se puede observar la funcionalidad para limitar el tiempo conectado.

Figura 50 Tiempo de actividad en dispositivos



Fuente: FAMILIES GOOGLE. Ayuda a tu familia a adoptar hábitos digitales saludables. [En línea] (Recuperado en marzo de 2022) Disponible en: https://families.google.com/intl/es-419/familylink/

BARK o ladrido en español es una aplicación que permite monitorear las redes sociales del menor. Envía alertas si intenta acceder a algo inapropiado, monitorea más de 30 redes sociales, correo, actividades de texto, permite también la configuración de tiempos y el filtrado web. *Bark*

UMobix al igual que *Web Watcher* es ideal para el teléfono inteligente, monitorea más de 30 aplicaciones, incluidas redes sociales, puede ver y leer mensajes enviados o recibidos desde plataformas de redes sociales incluidas *WhatsApp*, ver llamadas entrantes, saliente, la duración de estas y obtener información del contacto. También puede revisar el historial de ubicación y navegación del menor

Qustodio, esta aplicación es de pago, permite el bloqueo a sitios no adecuados a su edad y ofrece características más avanzadas como la revisión de actividad en

tiempo real, historial de reproducciones de YouTube, publicaciones en *Facebook* (característica importante del tema de la monografía), tiempo de pantalla, entre otros. También permite la generación de alertas ante situaciones especifica, y generación de informes, diarios, semanales y mensuales.

ClevGuard, esta aplicación también para teléfonos ayuda a revisar las actividades en línea, archivos, y chats. Está disponible para Android, iPhone, iCloud y actúa también sobre *WhatsApp*.

Otras aplicaciones que se pueden buscar son: *Panda Dome Family* o *Norton Family*, que permiten filtrar contenido, bloquear páginas, monitorizar actividades y establecer límites de tiempo. También se recomienda para los más pequeños utilizar navegadores especiales para ellos como *Kidoz* o *Kiddle.*
En conjunto, todas estas medidas pueden ayudar a los padres a mejorar la seguridad de sus hijos no solo en las redes sociales, sino también en los demás servicios que ofrece internet.

8.1.6 **Controles parentales en las propias aplicaciones.** Muchas de las aplicaciones a las que acceden los menores tiene controles parentales, es cuestión de conocerlas y activarlas.
Por ejemplo, YouTube, cuenta con la creación de cuentas supervisadas o creación de perfiles para menores que permiten mantener el control sobre las navegaciones del menor y el contenido que se le presenta.
Tiktok, permite marcar la cuenta como privada, gestionar alarmas para controlar el tiempo en pantalla y realizar un modo restringido para evitar que se visualice contenido inapropiado.
Google play permite controles parentales para el acceso a juegos y/o aplicaciones con restricción de edad, así como el bloqueo de descargar y/o compras.

Lo importante es conocer a que tipo de aplicaciones y/o redes accede el menor y como combinar las medidas de seguridad que ofrecen con herramientas externas como las mencionadas anteriormente.

8.2 ENFOCADOS EN LAS PLATAFORMAS DE REDES SOCIALES.

A nivel mundial el departamento de justicia y seguridad nacional de estados unidos y gobiernos como el de Canadá, Australia, Nueva Zelanda y Reino Unido, han reconocido la importancia de tomar acciones contra el *grooming* y han hecho un llamado a compañías tecnológicas en las que se encuentran las redes sociales a luchar contra el abuso infantil en internet. Según el artículo de caracol radio: "Esperamos que los Principios Voluntarios estimulen la acción colectiva por parte de la industria para detener uno de los crímenes más horrendos que afecta a algunos de los miembros más vulnerables de la sociedad"71

Estos principios invitan a las compañías a prevenir el material de abuso sexual infantil en sus plataformas, a incentivar formas de búsqueda para identificar el abuso infantil centrado en el *grooming*, y a instaurar métodos de ayuda para víctimas y respuesta a amenazas.

A partir de lo anterior, se propone una estrategia de cómo mejorar la seguridad en las plataformas de redes sociales para la comunidad infantil, con un cambio de objetivo o un nuevo uso de tecnologías que ya son usadas en estas.

Una tecnología muy utilizada para fines de marketing es la llamada minería de datos.

Los datos recopilados de las redes sociales suelen ser utilizados por empresas de mercadeo e investigación. El objetivo principal de estos análisis es descubrir patrones y tendencias. Estos datos van desde los datos de registro hasta

[71] CARACOL RADIO. Grandes tecnológicos toman medidas contra el abuso infantil. [En línea] 06 de marzo de 2020 (Recuperado en marzo de 2022) Disponible en: https://caracol.com.co/radio/2020/03/06/tecnologia/1583508810_702576.html

comentarios, *likes* y todo lo que se genere en estas plataformas, identificando así actitudes, comportamientos y sentimientos de las personas. Esta información es luego utilizada para mejorar campañas de marketing.

Ahora bien, ¿qué pasa si se utiliza esta minería no para mejorar las campañas de marketing, sino la seguridad infantil?; La minería de datos implica combinaciones de técnicas de estadística, matemáticas y aprendizaje automático para identificar patrones comunes; algunas de estas técnicas son la clasificación, asociación, patrones de seguimiento, análisis predictivo y extracción de palabras clave.

En cuanto al aprendizaje automático, este puede usar modelos de aprendizaje por refuerzo, supervisado o no supervisado. Para el tema que se trata en esta monografía, se toma el modelo supervisado, ya que los algoritmos de aprendizaje se basan en alimentar el sistema con datos ya establecidos y lograr que asocie el ingreso de nuevos datos con etiquetas ya establecidas para identificarlas.

Como se apreció en el objetivo uno, se han hecho estudios que permiten identificar palabras claves y comportamientos con los cuales se pueden alimentar estos sistemas y que permitan identificar conductas sospechosas relacionadas con el *grooming*.

La intención es cambiar el objetivo de la minería de datos de una meta comercial hacia una meta de seguridad.

En cuanto a las técnicas, se basarían en asociación, la cual busca relaciones entre elementos para identificar patrones y los patrones secuenciales que permiten identificar tendencias. Las empresas de marketing utilizan estas técnicas para en primera medida seguir qué compran los usuarios y en segunda que pueden llegar a comprar.

Estas técnicas de aprendizaje automático de forma independiente han sido también utilizadas por departamentos de policía en estados Unidos para predecir tendencias criminales, entre los que se tienen zonas con más alto riesgo de crímenes y posibles reincidencias; otro ejemplo de este aprendizaje es la predicción de propagación de enfermedades, lo que puede indicar que modificando el objetivo de la minería y

alimentándolo con la información correcta se puede predecir posibles comportamientos que terminen en *grooming*.

La segunda tecnología por analizar es la identificación de imágenes, en este caso se va a hablar de una tecnología llamada *Automatic Alternative Text*. Esta tecnología de reconocimiento de imágenes busca analizar el contenido de la imagen y etiquetarla, permitiendo una descripción de esta. El objetivo es ayudar a personas ciegas a entender lo que se muestra en las imágenes permitiendo ofrecerles una descripción hablada de la misma. Es una tecnología más avanzada que la que generalmente se utiliza para detectar y clasificar imágenes; de nuevo estas tecnologías se basan en modelos de aprendizaje, a modo general de ejemplo, se puede pensar que el sistema se alimenta con suficientes fotos de camisetas de color rojo, de forma que cuando detecte una imagen pueda reconocer si en ella hay o no una camiseta roja. De esta forma tan simple, sin entrar en detalles técnicos se puede inferir que con el nivel de detalle que tiene esta tecnología para poder describir una imagen, es posible que detecte imágenes de contenido sexual enfocado en perfiles infantiles y que permita bloquearlas, eliminarlas o enviar algún tipo de notificación.

8.3 ENFOCADO EN PROFESIONALES DE SISTEMAS, SEGURIDAD Y TICS

El Internet y las redes sociales son entornos que hoy en día hacen parte de la vida diaria de miles de jóvenes; la pandemia probablemente solo aceleró la adopción de estas tecnologías, sin embargo, la urgencia y velocidad con la que la sociedad se tuvo que adaptar a este sistema, provocó que la respuesta ante los delitos y las nuevas situaciones que aquí se presentan se haga de manera reactiva, teniendo primero que conocer la infracción y sus consecuencias para luego evaluarlo y buscar como contenerla. La cooperativa Abacus ya indicaba que “El salto generacional entre padres e hijos y la rápida evolución de los dispositivos electrónicos ha ocasionado que hoy en día exista una generación de menores considerados huérfanos digitales. Una situación que ha expuesto a estos jóvenes a

riesgos que desconocen y para los que no están preparados. Y que ha pillado de imprevisto y sin saber cómo afrontarlo a padres y educadores.” 72

Es posible que, a futuro, las herramientas de filtrado de contenido y los controles parentales sean lo suficientemente robustos para no tener que ser supervisados y lo suficientemente intuitivos para que puedan ser utilizados fácilmente, pero hoy en día, los padres se enfrentan a una realidad, en la que deben cuidar a sus hijos en un entorno muchas veces desconocidos para ellos y en la que sus propios hijos tienen más conocimiento de su funcionalidad. Pensando en esto, a nivel de las tecnologías de la información se debe buscar una manera de apoyar a los padres para mejorar la supervisión de sus hijos. Para las generaciones actuales y para las venideras, el internet es más que una herramienta de comunicación y/o aprendizaje, sino que se ha convertido en un elemento vital de sus vidas.

Los profesionales de distintas áreas de sistemas pueden ser un gran apoyo en la capacitación de las distintas herramientas que existen para limitar, controlar y/o supervisar el comportamiento de los menores en la red; las alcaldías actualmente dictan capacitaciones en sistemas para personas adultas, pero van enfocadas en el uso básico y manejo de redes propias; capacitaciones como estas pero enfocadas en conocer los distintos controles que existen en redes sociales y como pueden ser reforzadas con otras aplicaciones y funcionalidades de los mismos dispositivos que se usan para acceder al entorno digital, pueden ser de gran utilidad para padres que no tienen suficientes conocimientos sobre la supervisión de sus hijos en la era digital.

Por lo tanto, se invita a los profesionales en sistemas, TICs y seguridad, a que desde sus competencias busquen una forma de responder al llamado a la acción del ICBF y UNICEF, ya sea compartiendo sus conocimientos de cómo mejorar la seguridad

[72] ABACUS CORPORATIVA. ¿Qué son los contenidos inadecuados en internet y cómo afectan a los menores? [En línea] 10 de enero de 2019 (Recuperado en septiembre de 2022) Disponible en: https://cooperativa.abacus.coop/es/comunidades/comunidad-de-ocio/conocimiento-compartido-ocio/que-son-los-contenidos-inadecuados-en-internet-y-como-afectan-a-los-menores/

en casa enfocados en los más pequeños, mediante capacitaciones a padres sobre aplicaciones o controles, o mediante el diseño de una estrategia de seguridad enfocada en controles parentales.

9 CONCLUSIONES

Se establecieron los tipos de amenazas a los que se expone la comunidad infantil al usar redes sociales, a través de una revisión sistemática de informes realizados por organizaciones que protegen el bienestar infantil, como son los distintos informes de UNICEF, el ICBF Instituto colombiano de bienestar familiar, y diferentes portales de apoyo para la denuncia de delitos contra la comunidad infantil a través de las redes sociales, Identificando el ciberacoso y el *grooming* como las amenazas más recurrentes, y comparando el *grooming* con los ataques de ingeniera social del mundo adulto.

Se examinaron los métodos actuales que utilizan las redes sociales para garantizar la seguridad de sus usuarios mediante la revisión de las políticas de seguridad y la exploración de los controles que ofrecen estas aplicaciones para mejorar la seguridad de los menores de edad, identificando falencias en estos e identificando que se centran más que todo en controles de contenido y educación del correcto uso de las redes sociales.

Se justificó la necesidad de proteger en el ciberespacio a la población infantil a partir de estadísticas y casos registrados en plataforma digitales del gobierno, que exponen las consecuencias tanto físicas como mentales que se pueden presentar en los niños a raíz de haber sido víctimas de estos ataques.

Se propusieron medidas y estrategias de contingencia que permitan mejorar la seguridad infantil en entornos digitales, mediante el uso y apropiación de herramientas y/o métodos existentes en el mercado e investigando controles parentales de otras herramientas usadas en el entorno digital como sistema operativos y navegadores que mejoran la seguridad de la comunidad infantil.

10 RECOMENDACIONES

La comunidad infantil se ve expuesta a distintos riesgos en los entornos digitales y las redes sociales, se ha visto un aumento en la denuncia de amenazas tanto de conducta, contenido y contacto, por lo que se recomienda mantener constante acompañamiento y monitoreo por parte de padres cuando los menores naveguen por la red.

A diferencia de lo que se cree, la perfilación de un *groomer* es una tarea compleja, ya que no solo se trata de un adulto que busca engañar niño para su satisfacción sexual, sino que hay todo un universo, en el cual se puede clasificar dependiendo de la motivación del atacante, y cuyas formas de contactar al menor también están evolucionando haciendo aún más difícil dar una respuesta eficaz para la reducción de riesgos, por esta razón es importante que las autoridades mantengan constante monitoreo de las denuncias y las formas en que los ciberdelincuentes llegan a los niños para conocer la evolución de estos delitos.

Los controles parentales en las redes sociales no son lo suficientemente eficaces para proteger a la comunidad infantil, se recomienda por lo tanto reforzar los lazos de confianza entre los miembros de la familia, y mejorar la educación de padres e hijos en el correcto comportamiento en las redes sociales y los peligros a los que se pueden enfrentar.

Debido a que la mayoría de los controles por parte de las redes sociales están asociadas a controles de contenido, se recomienda a los padres hacer seguimiento de los contactos de sus hijos y en lo posible establecer sus cuentas como privadas, así como ser parte integral de la vida digital de los hijos.

Ya que muchos los niños no comunican este tipo de situaciones en casa, es importante que los padres estén atentos a cambios en el comportamiento de sus

hijos, como ansiedad o depresión, estos pueden ser pistas silenciosas de que necesitan ayuda.

Debido a que se establece una relación entre el contenido obtenido por un *groomer* y los sitios de pornografía infantil, se recomienda a los padres reforzar la educación sobre los contenidos a compartir en redes sociales y con nuevos contactos y supervisar lo que los menores comparten en las redes.

Se recomienda a los padres investigar un poco más acerca de los controles parentales no enfocados solo en redes sociales, sino en distintos aspectos que se relacionan con la conexión de estas y la navegación segura; esto puede ayudar a crear una estrategia más elaborada y a mejorar a seguridad digital en casa.

Se recomienda la instalación de aplicaciones de monitoreo en especial aquellas que permiten ver mensajes y contactos intercambiados para los más pequeños, ya que estas permiten un mejor control sobre riesgos de contenido y contacto.

Se recomienda a las plataformas, reflexionar que, así como están innovando para ofrecer una mejor experiencia a sus usuarios, también evaluar el potencial que tiene estas tecnologías para ayudar a ofrecer una respuesta más proactiva a las amenazas existentes en la red que afectan a la comunidad infantil.

11 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de XXXXX, puedan acceder al documento.

BIBLIOGRAFÍA

ABACUS CORPORATIVA. ¿Qué son los contenidos inadecuados en internet y cómo afectan a los menores? [En línea] 10 de enero de 2019 (Recuperado en septiembre de 2022) Disponible en: https://cooperativa.abacus.coop/es/comunidades/comunidad-de-ocio/conocimiento-compartido-ocio/que-son-los-contenidos-inadecuados-en-internet-y-como-afectan-a-los-menores/

ABC. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años. [En línea] Sección Padres e Hijos. 10 de marzo de 2019. (Recuperado en agosto de 2021) Disponible en: https://www.abc.es/familia/padres-hijos/abci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ffamilia%2Fpadres-hijos%2Fabci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html

ABOUT INSTAGRAM. Seguimos haciendo de Instagram un lugar más seguro para los miembros más jóvenes de la comunidad. [En línea] 17 de marzo de 2021 (Recuperado en octubre de 2021) Disponible en: https://about.instagram.com/es-la/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community

ACER. Cómo usar el modo para niños en Microsoft Edge. [En línea] 15 de febrero de 2023. ACER answers. (Recuperado en abril 2023) Disponible en: https://community.acer.com/es/kb/articles/15733-como-usar-el-modo-para-ninos-en-microsoft-edge

ACIS. ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS. Internet por la pandemia [En línea]. Enero 20 de 2021. (Recuperado en abril de 2023) Disponible en: https://www.acis.org.co/portal/content/noticiasdelsector/en-promedio-los-ni%C3%B1os-y-ni%C3%B1as-aumentaron-tres-horas-su-tiempo-conectados-internet-por-la

ARGENTINA.GOB. ¿Cómo actúan los acosadores? [En línea]. 2021 (Recuperado en septiembre de 2021) Disponible en: https://www.argentina.gob.ar/grooming/como-actuan-los-acosadores

_____ ¿Cómo me doy cuenta si un perfil es falso en Facebook? [En línea] 2022. (Recuperado en marzo de 2023) Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-detecto-un-perfil-falso

ASTORGA CRISTEL, FONSECA Ileana. Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. [en línea] 30 de octubre de 2019 Revista Electrónica Educare. versión ISSN 1409-4258. (Recuperado en septiembre de 2021) Disponible en: https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-42582019000300339

ATICO 34. Peligros de las redes sociales para niños y adolescentes. [En línea] 2022. (Recuperado en abril 2023) Disponible en: https://protecciondatos-lopd.com/empresas/peligros-redes-sociales/

BBVA. 'Machine learning': ¿qué es y cómo funciona? [En línea]. BBVA - Tecnología - Inteligencia Artificial 08 de noviembre de 2019 (Recuperado en marzo de 2023) Disponible en https://www.bbva.com/es/innovacion/machine-learning-que-es-y-como-funciona/

BIRDSONG TONI. ¿Es WhatsApp seguro para los niños? Lo que deben saber los padres. [En línea] 09 de marzo de 2020. Portal McAfee (recuperado en junio 2022) Disponible en: https://www.mcafee.com/blogs/es-es/family-safety/es-whatsapp-seguro-para-los-ninos-lo-que-deben-saber-los-padres/

BROADHURST RODERIC. Child Sex Abuse Images and Exploitation Materials [On line]May 8, 2019. Roger Leukfeldt & Thomas Holt, Eds. Cybercrime: the human factor, Routledge, Forthcoming , (Recuperado en abril de 2023) Disponible en SSRN: https://ssrn.com/abstract=3384499

CAMARA DE REPRESENTANTES. Aprobado proyecto que tipifica el #Sexting como delito en primer debate. [En línea] 11 de junio 2021 (Recuperado en 23 de noviembre de 2022) Disponible en: https://www.camara.gov.co/aprobado-proyecto-que-tipifica-el-sexting-como-delito-en-primer-debate#:~:text=El%20proyecto%20sanciona%20la%20violencia,a%20trav%C3%A9s%20de%20cualquier%20medio

CAMARGO MARIA DEL PILAR. Reportar contenidos inapropiados en redes sociales. ¿Para qué sirve? [En línea] El colombiano 19 de marzo de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.elcolombiano.com/tendencias/reportar-contenidos-inapropiados-en-facebook-instagram-y-twitter-DD14717444

Canal 13. ¿Qué es el grooming? [En línea] 13 de marzo de 2023. (Recuperado en abril de 2023) Disponible en: https://canaltrece.com.co/noticias/grooming-que-es-etapas-y-caracteristicas/

CARACOL RADIO. Grandes tecnológicos toman medidas contra el abuso infantil. [En línea] 06 de marzo de 2020 (Recuperado en marzo de 2022) Disponible en: https://caracol.com.co/radio/2020/03/06/tecnologia/1583508810_702576.html

CEBALLOS PAULA. Grooming, el peligro que acecha a los menores de edad en internet [En línea] LA FM. (Recuperado en abril de 2023) Disponible en https://www.lafm.com.co/tecnologia/grooming-el-peligro-que-asecha-a-los-menores-de-edad-en-internet

CERT.GOV.PY Perfiles falsos, grooming, extorsión – cómo cuidarse [En línea] 2021 (Recuperado en octubre de 2021) Disponible en: https://www.cert.gov.py/noticias/perfiles-falsos-grooming-extorsion-como-cuidarse

CHAUVIN SILVIA. 12 Consejos Para Proteger A Los Chicos del Grooming. [En línea] (Recuperado en octubre de 2021) Disponible en: http://www.mujeresdeempresa.com/12-consejos-para-proteger-a-los-chicos-del-grooming/

CHEVALIER NARANJO Stephani ¿Qué riesgo corren los niños al conectarse a internet? [En línea] 8 de febrero de 2021 Portal Statista.com (Recuperado en 2 de noviembre de 2021) Disponible en: https://es.statista.com/grafico/24110/los-ninos-y-la-seguridad-en-linea/

CIBERCRIMEN. Facebook, La Red Social Mas Usada En La Pandemia (Analisis&Tendencias). [En línea]] 09 de junio de 2020. (Recuperada en agosto de 2021) Disponible en: https://www.cibercrimen.org.ar/2020/06/09/facebook-la-red-social-mas-usada-en-la-pandemia-analisistendencias/

CONTIGOCONECTADOS. Grooming, la amenaza disfrazada de confianza que engaña a los niños en internet [En línea] (Recuperado en marzo de 2022) Disponible en: https://contigoconectados.com/sexualidad/grooming-la-amenaza-disfrazada-de-confianza-que-engana-a-los-ninos-en-internet/

CUSICANQUI JOSÉ LUIS. Nativos Digitales Vs. Inmigrantes Digitales ¿Brecha Generacional, Brecha Cognitiva? Una Mirada Psicopedagógica! Digital Natives Vs. Digital Immigrants [En línea] 2019. Generational Gap, Cognitive Gap? A Psychopedagogical Look!. Edición Revista Editora, vol. 2, no 1, p. 89 (Recuperado en marzo 2023) Disponible en: https://www.redalyc.org/pdf/140/14002809.pdf

DE BOGOTÁ, Cámara de Comercio, et al. ¿Qué son las medidas de protección parental? [En línea] 2022. PDF (Recuperado en noviembre de 2022) Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/27720/Mecanismos%20de%20cotrol%20parental%20prevencion.pdf?sequence=1

EL GRAN SANTO DOMINGO. Los *millennials* ante retos del mundo tecnológico. [En línea] 29 de noviembre de 2018. (Recuperado en agosto de 2021) Disponible en: http://www.elgransantodomingo.com/los-millennials-ante-retos-de-un-mundo-tecnologico/

EL MUNDO. Las consecuencias de que tus hijos naveguen por páginas inapropiadas. [En línea] 12 de octubre de 2020 (Recuperado en agosto de 2022) Disponible en: https://porunusolove.elmundo.es/contenido-inapropiado/las-consecuencias-de-que-tus-hijos-naveguen-por-paginas-inapropiadas

EL TIEMPO. Autoridades siguen la pista a delincuentes que comparten esos contenidos en Google y redes sociales. [En línea] 23 de septiembre de 2019 (Recuperado en septiembre de 2021) Disponible en:

https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

FALESTCHI DEMIAN. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. [En línea] 11 de noviembre de 2020. IABCOLOMBIA. (Recuperado en agosto de 2021) Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-y-el-avance-del-grooming-en-america-latina/

FAMILIES GOOGLE. Ayuda a tu familia a adoptar hábitos digitales saludables. [En línea] (Recuperado en marzo de 2022) Disponible en: https://families.google.com/intl/es-419/familylink/

FAROS. Cómo evitar que los menores sufran grooming (acoso sexual por Internet) [En línea] 06 de febrero de 2021. Sant Joan de Déu. Barcelona Hospital. (Recuperado en marzo de 2023) Disponible en: https://faros.hsjdbcn.org/es/articulo/como-evitar-menores-sufran-grooming-acoso-sexual-internet

FERNANDEZ YUBAL. Control parental de Windows 10: cómo configurar sus límites y el tiempo que tus hijos pasan en el PC. [En línea] 2 de mayo de 2022. Xataca. (Recuperado en abril de 2023) Disponible en: https://www.xataka.com/basics/control-parental-windows-como-configurar-sus-limites-tiempo-que-tu-hijo-puede-pasar-pc

GALAN RAFAEL. Facebook Files: El nuevo escándalo de la red social. [En línea] 05 de octubre de 2021. (Recuperado en octubre de 2021) Disponible en: https://www.esquire.com/es/tecnologia/a37862809/facebook-frances-haugen-archivos-escandalo/

GÁMEZ-GUADIX MANUEL, et al. Creencias Erróneas Sobre El Abuso Sexual Online De Menores (" Child Grooming") Y Evaluación De Un Programa De Prevención. Psicología Conductual, 2021, vol. 29, no 2, p. 283-296. (Recuperado en marzo de 2023) Disponible en: https://www.researchgate.net/publication/354856627_Creencias_erroneas_sobre_el_abuso_sexual_online_de_menores_child_grooming_y_evaluacion_de_un_programa_de_prevencion

GARAYZÁBAL HEINZE ELENA, HIDALGO DE LA GUÍA IRENE. Detección De Depredadores Sexuales En Los Chats Y La Captación De Menores. El Papel De La Lingüística Forense. [En línea] 2020 Tonos Digital, 2020, vol. 39, no 0. (Recuperado en abril de 2023) Disponible en: https://digitum.um.es/digitum/bitstream/10201/96042/1/2549-6933-1-PB.pdf

GASSÓ AINA, BIANCA KLETTKE, JOSÉ AGUSTINA AND IRENE MONTIEL. "Sexting, Mental Health, and Victimization Among Adolescents: A Literature Review" [On line] 2019 International Journal of Environmental Research and Public Health 16, no. 13: 2364. https://doi.org/10.3390/ijerph16132364
(Recuperado en abril 2023) Disponible en: https://www.mdpi.com/1660-4601/16/13/2364

GUERRERO VALERIA. Se dispararon reportes de explotación sexual infantil por internet en 2020 [En línea] 24 de septiembre de 2021. Red PaPaz, RCN Radio (recuperado en marzo de 2022) Disponible en: https://www.rcnradio.com/colombia/se-dispararon-reportes-de-explotacion-sexual-infantil-por-internet-en-2020-red-papaz#:~:text=La%20Red%20Nacional%20de%20Padres,balance%20anterior%20a%20la%20pandemia.

GULO LUIS. Control Parental en Linux. [En línea] 19 de enero de 2023. (Recuperado den marzo de 2023) Disponible en: https://soloconlinux.org.es/control-parental-en-linux/

GUPTA Ashima. Las 12 mejores aplicaciones de control parental para una mejor seguridad. [En línea] 24 de febrero de 2022. Geekflare. (Recuperado en 15 de abril de 2022) Disponible en: Las 12 mejores aplicaciones de control parental para una mejor seguridad (geekflare.com)

HAYES HEATHER. The Evolution of Cyberbullying in a Digital era. [En línea] 18 de marzo de 2020. (Recuperado en 21 de noviembre de 2022) Disponible en: https://www.heatherhayes.com/cyberbullying/

ICBF. Conoce las acciones prioritarias que favorecen los derechos digitales de la infancia. [En línea] 24 se marzo de 2021. (Recuperado en junio 2022) Disponible en: https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-las-acciones-prioritarias-que-favorecen-los-derechos-digitales-de-la

_____ El Instituto. [En línea] 2022 (Recuperado en 20 de septiembre de 2022) Disponible en: https://www.icbf.gov.co/instituto

_____ Riesgos digitales, ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet? [En línea] 17 de diciembre de 2019 (Recuperado en agosto 2021) Disponible en: https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos

INCIBE. IS4K Contenido inapropiado. [En línea] SF (Recuperado en septiembre de 2022) Disponible en: https://www.is4k.es/necesitas-saber/contenido-inapropiado#:~:text=El%20acceso%20a%20contenidos%20inapropiados,a%20este%20tipo%20de%20actividades.

INFOBAE. Delitos informáticos en Colombia subieron un 17 % en el 2021: sepa cómo prevenirlos. [En línea] 26 de diciembre de 2021. (Recuperado en 14 de mayo de 2022) Disponible en: https://www.infobae.com/america/colombia/2021/12/27/delitos-informaticos-en-colombia-subieron-un-17-en-el-2021-sepa-como-prevenirlos/#:~:text=Se%20registraron%20516%20incidentes%20de,en%20esta%20%C3%A9poca%20de%20vacaciones.

IONOS. El filtro burbuja: la realidad a tu imagen y semejanza. [En línea] 23 de enero de 2020 (Recuperado en octubre de 2021) Disponible en: https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-filtro-burbuja/

JIMENEZ JAVIER. Configura el control parental en Chrome, Firefox y Opera. [En línea] 05 de julio de 2022. Redes Zone. (Recuperado en abril de 2023) Disponible en: https://www.redeszone.net/tutoriales/internet/configurar-control-parental-chrome-firefox-opera/

KASPERSKY. Karspersky Safe Kids, Cuida de tus hijos, incluso cuando no estés cerca. [Sitio web] [Consultado el 13 de marzo de 2022] Disponible en: Kaspersky Safe Kids 2022 | Control Parental para Android y iPhone | Kaspersky

MACHADO AMAURY. Casos de abuso sexual infantil en entornos digitales aumentó en pandemia. [En línea] Diario del Huila. 21 de febrero de 2022. (Recuperado en: 20 de noviembre de 2022) Disponible en: https://diariodelhuila.com/casos-de-abuso-sexual-infantil-en-entornos-digitales-aumento-en-pandemia/

MARTINEZ JOSÉ. Conozca cómo actúan los acosadores en las redes para que proteja a sus hijos. [En línea]] 18 de octubre de 2018. Bogotá.gov (Recuperado en: agosto de 2021) Disponible en: https://bogota.gov.co/mi-ciudad/gestion-publica/riesgos-de-los-ninos-en-internet

MCAFEE. Preguntas frecuentes sobre el control parental en McAfee Security. [En línea] 2023 (Recuperado en abril de 2023) Disponible en: https://www.mcafee.com/support/?locale=es-ES&articleId=TS103321&page=shell&shell=article-view

MICROSOFT. Más información sobre el modo Niños en Microsoft Edge. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

MICUCCI MARIO. Grooming: una problemática que crece durante la cuarentena. [En línea] 20 de mayo 2020 WELIVESECURITY (Recuperado en agosto 2021) Disponible en: https://www.welivesecurity.com/la-es/2020/05/20/grooming-crece-durante-cuarentena/

MORENO HAROLD, PILLACA MARYORIE. Redes peligrosas. [En línea] 2019 Portal Andina. (Recuperado en septiembre de 2022) Disponible en: https://portal.andina.pe/edpespeciales/2019/redes-peligrosas/index.html

Norton. Norton Family. [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://co.norton.com/products/norton-family

MORILLO TAMARA. Los retos virales más peligrosos que circulan por Internet. Sucesos [En línea] 23 de febrero de 2022 (Recuperado en agosto de 2022) Disponible en: https://www.epe.es/es/sucesos/20220223/retos-virales-peligrosos-circulan-internet-13281423

MOZILLA. Bloquea o desbloquea las páginas web con el control parental. [En línea] SF (Recuperado en 13 de abril de 2022) Disponible en: https://support.mozilla.org/es/kb/bloquea-o-desbloquea-las-paginas-web-con-el-contro#:~:text=Firefox%20comprueba%20los%20controles%20parentales,parentales%20activos%20en%20tu%20equipo

OTERO EDGAR. Cómo configurar el control parental en Windows 11. [En línea] 20 de noviembre de 2021. (Recuperado en marzo de 2023) Disponible en: https://www.profesionalreview.com/2021/11/20/como-configurar-el-control-parental-en-windows-11/

PERFIL. Cómo Es El Algoritmo Que Usa Facebook Para Controlar Contenido Inapropiados. [En línea] 20 de mayo de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.perfil.com/noticias/tecnologia/como-es-el-algoritmo-que-usa-facebook-para-controlar-contenidos-inapropiados.phtml

PILLAJO PEREZ DIEGO XAVIER. Propuesta de política pública para la protección de niños, niñas y adolescentes frente a la figura delictiva sexual-informática “CHILD GROOMING” en la Legislación Ecuatoriana. [En línea] 2022. Tesis de Licenciatura. (Recuperado en: marzo de 2023) Disponible en: https://dspace.uniandes.edu.ec/bitstream/123456789/15283/1/UI-DER-PDI026-2022.pdf

PUENTE DE LA MORA XIMENA. Que Adiciona El Artículo 4o. De La Ley General De Los Derechos De Niñas, Niños Y Adolescentes, En Materia De Alfabetización Digital Y Protección De La Niñez En El Uso De Internet, A Cargo De La Diputada Ximena Puente De La Mora, Del Grupo Parlamentario Del Pri. 2020 (Recuperado en abril de 2023) Disponible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4071722_20200915_1600122822.pdf

RADIO NACIONAL DE COLOMBIA. En 2021 se han reportado 177 denuncias de acoso sexual en internet a menores. [En línea] 02 de julio de 2021. (Recuperado en agosto de 2021) Disponible en: https://www.radionacional.co/actualidad/judicial/en-2021-se-han-reportado-177-denuncias-de-acoso-sexual-en-internet-menores

RED CONTRA EL ABUSO SEXUAL Los peligros de la era digital. [En línea] 2020. (Recuperado en agosto de 2021) Disponible en: https://redcontraelabusosexual.org/los-peligros-de-la-era-digital/

ROMERO FRANCISCO SACRISTÁN. Escenarios actuales de agresiones al derecho a la intimidad personal del menor. [En línea] 2021. Revista DH/ED: derechos humanos y educación, no 4, p. 137-155. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8126366

RUIZ FRANCISCO. Algunas distros de Linux especiales para los más pequeños. [En línea] SF (Recuperado en abril de 2023) Disponible en: https://ubunlog.com/algunas-distros-de-linux-especiales-para-los-mas-pequenos/

SÁNCHEZ MAURICIO. Identificar el ciberbullying o ciberacoso El ciberbullying suele ser una 'extensión' del bullying tradicional, por lo que identificar sus manifestaciones puede ser clave en la detección del acoso 'cara a cara'. 2020. Fuentes, no 26. (Recuperado en marzo de 2023) Disponible en: https://www.menteyciencia.com/identificar-el-ciberbullying-o-ciberacoso/

SANCRISTOBAL. El uso responsable de WhatsApp por menores. [En línea] (Recuperado en octubre de 2021) Disponible en: https://www.sancristobalsl.com/blog/el-uso-responsable-del-whatsapp-en-menores/

SAN LUIS NOTICIAS "My Sugar Daddy": Un peligroso juego, entre menores y adultos, que encubre posibles abusos o riesgo de trata. [En línea] 5 de diciembre de 2022. (Recuperado en marzo de 2023) Disponible en: https://sanluisnoticias.com/post/mi-sugar-daddy-advierten-sobre-peligroso-juego-sexual-entre-adolescentes-y-adultos#:~:text=Adolescentes%20entre%2011%20y%2016,fantas%C3%ADas%20y%20deseos%20generalmente%20sexuales.

SANTANDER DIGITAL SERVICES. Las 6 mejores distribuciones Linux para niños. [En línea] 22 de octubre de 2020. (Recuperado en abril de 2023) Disponible en: https://santandergto.com/las-6-mejores-distribuciones-linux-para-ninos/

SANZ JOSÉ LUIS. Microsoft Edge Recibe El Modo Para Niños Con Herramientas De Control Parental. [En línea] 16 de abril de 2021. (Recuperado en abril de 2023) Disponible en: https://cincodias.elpais.com/cincodias/2021/04/16/lifestyle/1618549732_764528.html

SARRALDE MILENA. ¿Hay delitos en el 'sexting'? Estas son las aclaraciones de la Corte [En línea] 03 de noviembre de 2019 El tiempo (Recuperado en 23 de noviembre de 2022) Disponible en: https://www.eltiempo.com/justicia/cortes/cuales-son-los-delitos-sexuales-en-internet-segun-la-corte-suprema-429966

SAVE THE CHILDREN. Grooming. Qué es, Cómo detectarlo y Prevenirlo. [En línea] 01 de julio de 2019 (Recuperado en: septiembre de 2021) Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

SCHWAB, KLAUS. La Cuarta Revolución Industrial. [En línea] 2020. Futuro Hoy, 1(1), 06–10. DOI: https://doi.org/10.52749/fh.v1i1.1 (Recuperado en marzo de 2023) Disponible en: http://ojs.ssh.org.pe/index.php/Futuro-Hoy/article/view/1/118

SEMANA. ¿Cuánto aumentó el uso de internet en niños por la pandemia? [En línea] 22 de enero de 2021 (Recuperado en septiembre de 2022) Disponible en: https://www.semana.com/educacion/articulo/cuanto-aumento-el-uso-de-internet-en-ninos-por-la-pandemia/202104/

SERRA KARINA. Radiografía del grooming y ciberacoso en pandemia. [En línea] 29 de enero de 2021 Diario El Perfil. (Recuperado en agosto 2021) Disponible en: https://www.perfil.com/noticias/opinion/karina-serra-radiografia-del-grooming-y-ciberacoso-en-pandemia.phtml

SIN EMBARGO. "Instagram, WhatsApp, Facebook y TikTok, redes usadas para 'cazar' niños en Argentina". [En línea]. 02 de junio de 2021 (Recuperado en septiembre de 2022) Disponible en: https://www.noroeste.com.mx/internacional/instagram-whatsapp-facebook-y-tiktok-redes-usadas-para-cazar-ninos-en-argentina-NBNO1222708

SJD. Cómo evitar que los menores sufran grooming (acoso sexual por Internet) [En línea] 06 de febrero de 2021 (Recuperado en marzo de 2023) Disponible en: https://faros.hsjdbcn.org/es/articulo/como-evitar-menores-sufran-grooming-acoso-sexual-internet

SKÓRZEWSKA-AMBERG MAŁGORZATA. Online Child Grooming–Some Remarks Against the Background of the Pandemic. Krytyka Prawa. Niezależne studia nad prawem [On line] 2021, vol. 13, no 4, p. 72-87. (Recuperado en noviembre de 2022) Disponible en: https://www.ceeol.com/search/article-detail?id=1062176

SOCIALMEDIAVICTIMS. Social Media and Online Grooming [On line] 14 de abril de 2023. (Recuperado en abril de 2023) Disponible en: https://socialmediavictims.org/sexual-violence/online-grooming/

STATISTA. ¿CUÁLES SON LAS REDES SOCIALES MÁS UTILIZADAS? [En línea] 2023. (Recuperado en abril de 2023) Disponible en: https://2immarketing.com/cuales-son-las-redes-sociales-mas-usadas/

SUESCA LIZETH, Delitos cibernéticos en Colombia ascendieron un 17 % en 2022. [En línea] 2022. Caracol radio. (Recuperado en abril 2023) Disponible en: https://caracol.com.co/radio/2021/12/26/politica/1640514049_007856.html

TPLINK. How to configure Parental Controls on the Wi-Fi Routers (case 1)? [On line] 18 de marzo de 2022. (Recuperado en 12 de abril de 2022) Disponible en: https://www.tp-link.com/co/support/faq/1531/

TRIANA CARLOS, OLIVA EDGAR. Esquema para la prevención del grooming en niños, niñas y adolescentes desde los 7 a 14 años en Bogotá a través de un análisis de riesgos basados en la norma ISO 27005. [En línea] 2021. Bogotá: Universidad Católica de Colombia, 202261 páginas (Recuperado en marzo 2023) Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/35315784-6fd2-41e9-baf1-c75910b5e537/content

USECIM El perfil criminal del Groomer. [En línea] 31 de julio de 2021 (Recuperado en septiembre de 2021) Disponible en: https://canalnoticias.usecim.es/el-perfil-criminal-del-groomer/

UNICEF. Educando en el derecho a la información: contenidos falsos, nocivos e ilícitos. [En línea] SF (Recuperado en 24 de septiembre de 2022) Disponible en: https://www.unicef.es/educa/blog/educando-derecho-informacion-contenidos-falsos-nocivos-ilicitos

_____ Mantener seguros a niñas, niños y adolescentes en Internet. [En línea]. SF (Recuperado en agosto de 2021) Disponible en: https://www.unicef.org/mexico/mantener-seguros-ni%C3%B1as-ni%C3%B1os-y-adolescentes-en-internet

_____Violencia contra niñas, niños y adolescentes en tiempos de COVID-191 [En línea] noviembre 2020 (Recuperado en marzo de 2022) Disponible en: https://www.unicef.org/lac/media/19611/file/violencia-contra-nna-en-tiempos-de-covid19.pdf

WEBFINDYOU. El uso de las redes sociales en Colombia. [En línea] 09 de septiembre de 2021 (Recuperado en setiembre de 2021) Disponible en: https://www.webfindyou.com.co/blog/uso-redes-sociales-colombia/

WOOD AMY, WHEATCROFT JACQUELINE. Young adult perceptions of internet communications and the grooming concept. [On line] 2020 Sage open, vol. 10, no 1, p. 2158244020914573 (Recuperado en abril de 2023) Disponible en: https://journals.sagepub.com/doi/pdf/10.1177/2158244020914573

ZAGALSKY ALEJO Los acrónimos sexuales y las palabras que pueden indicar ciberacoso en las redes sociales. [En línea] 18 de julio 2021 (Recuperado en septiembre de 2021) Disponible en: https://tn.com.ar/tecno/redes-sociales/2021/07/18/los-acronimos-sexuales-y-las-palabras-que-pueden-indicar-ciberacoso-en-las-redes-sociales/

ANEXOS

Resumen Analítico Especializado RAE

Fecha de Realización:	20/06/2023
Programa:	Especialización en seguridad Informática
Línea de Investigación:	Administración de tecnología
Título:	Herramientas y/o métodos para proteger a la comunidad infantil de ataques de ingeniería social en redes sociales.
Autor(es):	Sandoval Camelo Karina
Palabras Claves:	Grooming, Ciberacoso, Controles parentales, Redes Sociales.

Descripción:

El trabajo se divide en 4 fases: la primera identifica los riesgos a los que se ve expuesta la comunidad infantil en las redes sociales y enfatiza en el grooming como un ataque de ingeniería social dirigida hacia los niños; la segunda explora los métodos o herramientas actuales en las redes sociales para proteger a los niños de las amenazas existentes en los entornos digitales, demostrando que dichos controles tienen muchas falencias y que actualmente casi toda la responsabilidad se ha delegado a la educación y cuidado de los padres a sus hijos; la tercera expone las consecuencias que estos riesgos, ya materializados provocan en los niños para demostrar la importancia de mejorar la protección infantil en los entornos digitales y finalmente la cuarta es una breve recopilación de distintos controles parentales integrados en los diferentes medios usados para conectarse a internet, y que integrados pueden ayudar a los padres a mejorar la seguridad de sus hijos.

Fuentes bibliográficas destacadas:

ABC. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años. [En línea] Sección Padres e Hijos. 10 de marzo de 2019. (Recuperado en agosto de 2021) Disponible en: https://www.abc.es/familia/padres-hijos/abci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ffamilia%2Fpadres-hijos%2Fabci-grooming-y-aumentado-410-por-ciento-ultimos-anos-201903081632_noticia.html

CEBALLOS PAULA. Grooming, el peligro que acecha a los menores de edad en internet [En línea] LA FM. (Recuperado en abril de 2023) Disponible en https://www.lafm.com.co/tecnologia/grooming-el-peligro-que-asecha-a-los-menores-de-edad-en-internet

CONTIGOCONECTADOS. Grooming, la amenaza disfrazada de confianza que engaña a los niños en internet [En línea] (Recuperado en marzo de 2022) Disponible en: https://contigoconectados.com/sexualidad/grooming-la-amenaza-disfrazada-de-confianza-que-engana-a-los-ninos-en-internet/

FALESTCHI DEMIAN. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. [En línea] 11 de noviembre de 2020. IABCOLOMBIA. (Recuperado en agosto de 2021) Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-y-el-avance-del-grooming-en-america-latina/

MICUCCI MARIO. Grooming: una problemática que crece durante la cuarentena. [En línea] 20 de mayo 2020 WELIVESECURITY (Recuperado en agosto 2021) Disponible en: https://www.welivesecurity.com/la-es/2020/05/20/grooming-crece-durante-cuarentena/

SERRA KARINA. Radiografía del grooming y ciberacoso en pandemia. [En línea] 29 de enero de 2021 Diario El Perfil. (Recuperado en agosto 2021) Disponible en: https://www.perfil.com/noticias/opinion/karina-serra-radiografia-del-grooming-y-ciberacoso-en-pandemia.phtml

UNICEF Mantener seguros a niñas, niños y adolescentes en Internet. [En línea]. SF (Recuperado en agosto de 2021) Disponible en: https://www.unicef.org/mexico/mantener-seguros-ni%C3%B1as-ni%C3%B1os-y-adolescentes-en-internet

Contenido del documento:

- Antecedentes o estado actual
- Marco legal

Riesgos de ingeniería social que enfrentan los niños en las redes sociales

- Escenarios de ataque de ingeniería social.
- Fases de ataque del grooming.
- Perfil del ciberdelincuente.
- Símbolos de alerta de grooming y pornografía infantil.

Herramientas y métodos actuales para combatir los ataques de ingeniería social contra la comunidad infantil existentes en las redes sociales.

- Apoyo a padres y niños.
- Reconocimiento de perfiles falsos.
- Facebook e Instagram.
- WhatsApp.
- Unicef y el ICBF

¿por qué se debe mejorar la seguridad infantil en el ciberespacio?

Estrategias para mejorar la seguridad de la comunidad infantil en redes sociales

- enfocados en padres.
- enfocados en las plataformas de redes sociales.
- enfocado en profesionales de sistemas, seguridad y tics

Conclusiones

Recomendaciones

Marco Metodológico:

La monografía se basa en una investigación documental, esto indica que la información obtenida nace a partir de la recopilación, organización y análisis de distintas fuentes documentales, como informes realizados por organizaciones de protección infantil como UNICEF o el ICBF, distintos portales sobre el cuidado de los niños en los entornos digitales y artículos donde se exponen los riesgos a los que se ve expuesta la comunidad infantil en las redes sociales.

Conceptos adquiridos:

CONTROL PARENTAL: Son una serie de características que ayudan a controlar no sola las actividades del menor, sino a denunciar y evitar situaciones de riesgo

GROOMING: tácticas de engaño que realizan los adultos para con fines de satisfacción sexual contra niñas, niños y adolescentes en el entorno digital

RIESGOS DE CONDUCTA: riesgos a los que se ven expuestos los niños y que pueden alterar su comportamiento de forma negativa.

RIESGOS DE CONTACTO: riesgo a los que los niños se ven expuestos por la conexión con personas que pueden engañarlos y abusar de ellos.

RIESGOS DE CONTENIDO: riesgo de que un niño sea expuesto a contenidos no apropiados, como aquellos de alto contenido sexual o violencia.

Conclusiones:

Se establecieron los tipos de amenazas a los que se expone la comunidad infantil al usar redes sociales, a través de una revisión sistemática de informes realizados por organizaciones que protegen el bienestar infantil, como son los distintos informes de UNICEF, el ICBF Instituto colombiano de bienestar familiar, y diferentes portales de apoyo para la denuncia de delitos contra la comunidad infantil a través de las redes sociales, Identificando el ciberacoso y el grooming como las amenazas más recurrentes, y comparando el grooming con los ataques de ingeniera social del mundo adulto.

Se examinaron los métodos actuales que utilizan las redes sociales para garantizar la seguridad de sus usuarios mediante la revisión de las políticas de seguridad y la exploración de los controles que ofrecen estas aplicaciones para mejorar la seguridad de los menores de edad, identificando falencias en estos e identificando que se centran más que todo en controles de contenido y educación del correcto uso de las redes sociales.

Se justificó la necesidad de proteger en el ciberespacio a la población infantil a partir de estadísticas y casos registrados en plataforma digitales del gobierno, que exponen las consecuencias tanto físicas como mentales que se pueden presentar en los niños a raíz de haber sido víctimas de estos ataques.

Se propusieron medidas y estrategias de contingencia que permitan mejorar la seguridad infantil en entornos digitales, mediante el uso y apropiación de herramientas y/o métodos existentes en el mercado e investigando controles parentales de otras herramientas usadas en el entorno digital como sistema operativos y navegadores que mejoran la seguridad de la comunidad infantil.