CONTROLES DE CIBERSEGURIDAD MÁS UTILIZADOS PARA EL BLOQUEO DE DIFERENTES TIPOS DE CONTENIDO PORNOGRÁFICO EN EL CIBERESPACIO QUE AFECTA PRINCIPALMENTE A NIÑOS Y ADOLESCENTES DE LA REGIÓN

LINA JOHANA JIMÉNEZ GONZÁLEZ

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

CONTROLES DE CIBERSEGURIDAD MÁS UTILIZADOS PARA EL BLOQUEO DE DIFERENTES TIPOS DE CONTENIDO PORNOGRÁFICO EN EL CIBERESPACIO QUE AFECTA PRINCIPALMENTE A NIÑOS Y ADOLESCENTES DE LA REGIÓN

LINA JOHANA JIMÉNEZ GONZÁLEZ

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

Nombre del director:
CHRISTIAN ANGULO RIVERA

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

NOTA DE ACEPTACIÓN

Firma del presidente de jurado

Firma del jurado

Firma del jurado

Ibagué, 02 de octubre de 2023

DEDICATORIA

A Dios quien ha sido mi fundamento y motivación para prepárame profesional y éticamente. A ÉL dedico este proyecto de investigación quien me dio la inteligencia para desarrollarlo.

AGRADECIMIENTOS

Principalmente a mi esposo quien se han convertido mi ayudador, quien en medio de mi vida me ha apoyado, quiero reconocer el esfuerzo que él han hecho continuar mis estudios profesionales, a mi esposo mis más sinceros agradecimientos.

A mis seres queridos, por sus enseñanzas de perseverancia esfuerzo en medio de las dificultades y quienes se han unido a contribuir en aquellos momentos de afán aportando ideas y salidas a cada una de las dificultades que se presentaron a lo largo de este proceso y a mis tutores quiero agradecerles porque gracias a sus conocimientos y disposición he podido culminar este proyecto.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ABUSO: En el Diccionario de Psicología escrito por Anaya[1], se define el abuso como un patrón de control que una persona ejerce sobre otra.

ABUSO SEXUAL: Según la Fundación RED[2], son acciones realizadas por un adulto sobre un niño, niña o adolescente que le proporcionan placer, estimulación o gratificación sexual.

ADOLESCENTE: Según la Real Academia Española (RAE)[3], Hace referencia a un ser humano que está en un período de la vida humana posterior a la niñez y antes de la juventud.

CHAT: Conversación entre dos personas o más, haciendo uso de texto, imágenes o audios usando dispositivos tecnológicos como teléfonos o computadoras.

COVID-19: De acuerdo con la RAE[4], es una enfermedad que causa síndrome respiratorio agudo ocasionado por un coronavirus.

CIBERESPACIO: Según el Blog de Ciberseguridad[5], es un lugar virtual, el cual hace uso de internet para que las personas puedan crear, almacenar, modificar, extraer, usar, compartir, eliminar información, además se puede jugar, hacer negocios, debatir, exponer ideas. Para hacer uso del ciberespacio se requiere de dispositivos conectados a internet como computadoras, teléfonos inteligentes y diferentes cosas conectadas a internet.

---

[1] ANAYA. Diccionario de Psicología. [en línea]. 2004-01-01. [citado el 2022-11-21].
[2] FUNDACIÓN RED. Definiciones. [en línea]. [citado el 2022-11-21]. Disponible en: https://redcontraelabusosexual.org/definiciones/
[3] RAE. Diccionario. [en línea]. [citado el 2021-04-11].
[4] ibíd
[5] ANÓNIMO. Ciberespacio: definición, aplicaciones y límites. [en línea]. [citado el 2022-11-12].

CIBERDELINCUENTE: Persona quien vulnera los derechos de una persona usando los medios tecnológicos.

CIBERSEGURIDAD: de acuerdo con libro de Ciberseguridad[6], es un conjunto de técnicas, procedimientos y protocolos para proteger la información de los usuarios o empresas en el ciberespacio.

CONTENIDO PORNOGRÁFICO: hace referencia a todo texto, imagen, audio, video y juegos que tengan pornografía.

DELITO SEXUAL: según un blog de asesores legales[7] se considere un delito a aquellas acciones voluntarias o acciones imprudentes que están en contra de la ley, por tanto, vulnera los derechos de otras personas u organizaciones.

INSTITUCIÓN EDUCATIVA: según el Ministerio de Educación (Colombia)[8], es un conjunto de personas y bienes promovidas por entidades públicas o privadas, que tengan una infraestructura administrativa, soportes pedagógicos, planta física y medios educativos adecuados para ofrecer educación a niños y adolescentes que viven en el país.

INTERNET: como dice la RAE[9], es una red informática a nivel mundial, donde se conectan computadoras mediante un protocolo especial de comunicación.

---

[6] ARROYO GUARDEÑO, David; GAYOSO MARTINEZ, Victor y HERNANDEZ ENCINAS, Luis. Ciberseguridad. [en línea]. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2020-12-31. p. 13. [citado el 2022-11-12].
[7] ANÓNIMO. ¿Sabes qué se Considera un Delito? [en línea]. 2021-08-05. [citado el 2022-11-21]. Disponible en: https://www.colombialegalcorp.com/blog/se-considera-delito/
[8] MINISTERIO DE EDUCACIÓN NACIONAL (Colombia). ESTABLECIMIENTOS EDUCATIVOS – (NATURALEZA). [en línea]. 2004-10-05. [citado el 2021-04-11].
[9] RAE. Diccionario. [en línea]. [citado el 2021-04-11].

PANDEMIA: según la RAE[10], es una enfermedad epidemiológica que se extiende por muchos países ya ataca a la mayoría de los individuos.

PORNOGRAFÍA: la RAE establece tres definiciones, para esta monografía se adopta la definición la cual dice que la pornografía es una “Presentación abierta y cruda del sexo que busca producir excitación”[11].

PEDOFILIA: Anaya indica que: “Parafilia caracterizada por la presencia, durante un período de al menos seis meses, de fantasías sexuales recurrentes y altamente excitantes e impulsos sexuales o comportamientos que implican actividad sexual con niños prepúberes o niños algo mayores (generalmente de 13 años o menos). Las fantasías, los impulsos sexuales o los comportamientos provocan malestar clínicamente significativo o deterioro social, laboral o de otras áreas importantes de la actividad del individuo. La persona tiene al menos 16 años y es por lo menos 5 años mayor que el niño o los niños. Se clasifica como: con atracción sexual por los hombres, con atracción sexual por las mujeres y con atracción sexual por ambos sexos. Puede limitarse al incesto o ser de tipo exclusivo (atracción solo por los niños)”[12].

RED SOCIAL: según la RAE[13], es una plataforma digital que permite la comunicación de gran número de usuario a nivel mundial.

RIESGO: es un evento que puede ocurrir debido a que un ciberdelincuente encuentra alguna vulnerabilidad en una persona o sistema informático.

---

[10] ibíd
[11] ibíd.
[12] ANAYA, Natalia Consuegra. Diccionario de psicología. [en línea]. Segunda Edición. 2010-01-01. [citado el 2022-11-21]. ISBN 978-958-648-650-7
[13] RAE. Diccionario. [en línea]. [citado el 2021-04-11].

RESUMEN

El uso del internet en niños y adolescentes se ha incrementado con el pasar del tiempo, con la pandemia iniciada en el 2020 por el COVID-19 más menores de 18 años ha incrementado el tiempo conectados a internet, los delincuentes hacen uso de técnicas como el grooming para obtener la confianza de ellos y así obtener imágenes, videos y/o audios y comercializar estos abusos sexuales infantiles a través del ciberespacio, por tanto es recomendable proteger a los niños y adolescentes conectados a internet a través de diferentes técnicas de filtrado de contenido que pueden ser implementadas en hogares e instituciones educativas.

Los softwares para el control parental usan distintas técnicas para filtrar el tráfico de datos que se considera inapropiado para los menores de 18 años, así que se identificarán dichas técnicas para el bloqueo no apto para niños en el ciberespacio. Además, se realiza una revisión sistemática de las técnicas para el filtro de datos en dispositivos y aplicaciones usadas por esta población.

ABSTRACT

The use of the Internet in children and adolescents has increased over time, with the pandemic that began in 2020 by COVID-19, more people under 18 years of age have increased the time connected to the Internet, criminals make use of techniques such as grooming to obtain their trust and thus obtain images, videos and/or audios and market these child sexual abuses through cyberspace, therefore it is advisable to protect children and adolescents connected to the Internet through different content filtering techniques that can be implemented in homes and educational institutions.

Parental control software uses different techniques to filter data traffic that is considered inappropriate for those under the age of 18, so such techniques for non-child-friendly blocking in cyberspace will be identified. In addition, a systematic review of the techniques for data filtering in devices and applications used by this population is carried out.

INTRODUCCIÓN

En la presente monografía, se realiza la revisión de las técnicas más usadas para bloquear contenidos pornográficos en el ciberespacio a los cuales están expuestos los niños, niñas y adolescentes, ya que cada año avanza la tecnología y las conexiones a internet, además en la pandemia del COVID 19 los niños niñas y adolescentes desarrollaron sus estudios en ambientes virtuales, por tanto, como lo evidenció un estudio realizado por Tigo Colombia, se aumentó la cantidad de horas de conexión a internet para estudiar, jugar y socializar en las redes sociales y los ciberdelincuentes aprovechan estas circunstancias para cometer delitos de abuso sexual infantil, grooming, sexting entre otros, y si los padres o instituciones educativas no conocen los riesgos a los cuales están expuestos los niños, niñas y adolescentes, entonces no se podrían tomar medidas para la protección de estos menores de edad.

Por tanto, en este documento se examinan las técnicas de bloqueo de contenido pornográfico a nivel de redes, navegadores y celulares o computadores conectados a internet. Se analizan los riesgos de ciberseguridad a los que están expuestos los niños, niñas y adolescentes como la pornografía implícita en videos, la publicación de datos privados, conversaciones con contactos peligrosos a través de chats, los retos virales, el ciberacoso, el sexting, el grooming y el chantaje sexual y finalmente se proponen buenas prácticas de ciberseguridad para la protección de los menores de edad cuando hacen uso de la internet.

Esta monografía se hace a través de la recopilación sistemática de información contenida en libros, textos y artículos académicos, y se apoya en resultados estadísticos de encuestas realizadas por terceros cuya población fueron los niños niñas y adolescentes de Colombia.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad la tecnología y la conexión a internet está en aumento, así lo demuestra la última encuesta realizada por el DANE[14] en el 2018 a personas mayores de 5 años; en el cual, el 82,2% de la población colombiana accede a internet para navegar en las redes sociales, y el 83,1% de esta población accede a internet desde su hogar. En estadísticas del DANE[15] realizadas en el 2019, se evidencia que el 51,9% de la población colombiana poseía conexión a internet. También en el 2019 el 92,5% de las personas mayores a 5 años que están en Bogotá usan el teléfono celular, seguido de Risaralda, Valle del Cauca y Quindío.

Según estadísticas de Ministerio de Tecnologías de la Información y las Comunicaciones[16] en el primer trimestre de 2022 el acceso a internet está distribuido de la siguiente forma, el 11,6% de los accesos son del estrato 1, el 35,4% son accesos del estrato 2 y el 27,54 pertenece al estrato 3.

Con la pandemia de 2020 causada por el COVID-19, la mayoría de los niños y adolescentes debieron recibir sus clases haciendo uso de la TICs. En un estudio realizado por el operador de telefonía Tigo en Colombia[17] los niños pasaron de 3 a 5 horas conectados a internet, y en adolescentes esta cifra pasó de 5 a 7 horas diarias conectados a internet.

---

[14] DANE. Indicadores básicos de tenencia y uso de Tecnologías de la Información y Comunicación –TIC en hogares y personas de 5 y más años de edad

[15] DANE. Indicadores básicos de TIC en Hogares. [en línea]. [citado el 2022-09-14]. Disponible en: https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares

[16] MINTIC. Internet dedicado. [en línea]. 2022-05-01. [citado el 2022-09-14]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47271.html

[17] REVISTA SEMANA. ¿Cuánto aumentó el uso de internet en niños por la pandemia?

El acceder a internet desde los hogares a las redes sociales se convierte en una combinación adecuada para que los ciberdelincuentes persuadan a niños mayores de 5 años con el fin de ser explotadas sexualmente, o generar imágenes o videos de abusos sexuales infantiles. Esto llevaría a otro delito, la sextorsión, que según la CCIT[18] de Colombia es una tendencia de 2020 de cibercrimen, en la cual se utilizará el envío de correos masivos a través de equipos controlados remotamente.

Según la Policía Nacional de Colombia[19] las amenazas delictivas relacionadas con el abuso sexual infantil han aumentado por causa de la pandemia del COVID-19, ya que los niños pasan más tiempo conectados a internet para estudiar jugar y socializar a través de chats o redes sociales, y con ello las víctimas han distribuido material personal en la internet, todas estas acciones de la víctima han sido aprovechadas por los ciberdelincuentes para cometer delitos de explotación sexual infantil.

1.2 FORMULACIÓN DEL PROBLEMA

Unas de las estrategias para mitigar este riesgo, son los filtros de contenido, el Ministerio de las TICs[20] en Colombia ha establecido a los proveedores de redes o servicios móviles la prohibición de la circulación de material de abuso sexual en niños y adolescentes, por tanto, estas prohibiciones también pueden establecer en redes más pequeñas como la red de los hogares y las instituciones educativas, por tanto, ¿Qué podrían hacer las instituciones educativas y los padres de familia para bloquear imágenes y videos pornográficos en el ciberespacio?.

---

[18] CAMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [en línea]. Primera Edición. Bogotá: 2019-10-29. p. 29.

[19] POLICÍA NACIONAL DE COLOMBIA. RIESGOS Y TENDENCIAS EN RELACIÓN CON EL ABUSO Y LA EXPLOTACIÓN SEXUAL DE MENORES. REPERCUSIONES DEL COVID-19

[20] MINTIC (Colombia). La protección de nuestras niñas, niños y adolescentes en Internet, una prioridad del Gobierno nacional.

2 JUSTIFICACIÓN

Los niños y adolescentes son vulnerables en la internet a los ciber delincuentes, es así como lo describe Barbosa[21], el cual explica la ingeniería social usada para cometer delitos sexuales en niños y adolescentes. Según el Grupo de Información de Criminalidad de Delitos Sexuales[22] de la Dirección de Investigación Criminal e INTERPOL de la Policía Nacional de Colombia de enero a agosto de 2022 se han cometido 18360 delitos sexuales, de los cuales 11602 casos son con adolescentes y niños, una cifra preocupante por la cual se deben tomar medidas para proteger a los niños y adolescentes de estos delitos.

La UNICEF[23] ha identificado distintos tipos de violencia de acuerdo a la edad y sexo de niño o adolescente, por ejemplo, los descuidos y castigos corporales se presenta con mayor frecuencia en niños de 0 a 11 años, el hostigamiento, intimidación y/o acoso ocurren en niños y adolescentes entre 5 y 17 años, y un dato preocupante es la violencia sexual, la cual se puede presentar en niños y adolescentes entre 0 y 18 años.

Una de las formas de prevenir los delitos sexuales son el bloqueo de contenido pornográfico, por ello, se hace necesario identificar las técnicas de filtrado de contenido usadas para el bloqueo de contenido pornográfico en el ciberespacio, con el fin de proteger a los niños y adolescentes de ser víctimas de los ciber delincuentes y pornografía infantil.

---

[21] BARBOSA, I. & Ojeda, A. Ingeniería social utilizada en el abuso de infantes a través de las redes sociales en Colombia.

[22] POLICIA NACIONAL. Delitos Sexuales 2022. [en línea]. Colombia: 2022-09-01. [citado el 2022-09-14]. Disponible en: https://www.policia.gov.co/contenido/delitos-sexuales-2022-0

[23] UNICEF. PANORAMA ESTADÍSTICO DE LA VIOLENCIA CONTRA NIÑAS, NIÑOS Y ADOLESCENTES EN MÉXICO. [en línea]. 1ª edición, 2019. [citado el 2022-09-14].

Con este trabajo en modalidad monografía se aportará al objetivo que tiene UNICEF[24] en cuanto a la protección de niños y adolescentes contra el abuso, la explotación y la violencia en ellos. Ya que se establecerán recomendaciones sobre el filtrado de contenido que pueden ser implementados en hogares e instituciones educativas y así proteger a los niños y adolescentes. Además, esta investigación se hará para analizar los riesgos que las familias pueden tener si no se hace un filtrado de contenido en las redes usadas por los niños y adolescentes.

[24] UNICEF. Protección. [en línea]. [citado el 2021-03-20].

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Compilar las técnicas más usadas para bloquear contenidos pornográficos, con el propósito de definir buenas prácticas de ciberseguridad para proteger a niños y adolescentes cuando están en el ciberespacio.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar las técnicas y nuevas tecnologías más utilizadas para el control de bloqueo de contenido pornográfico en el ciberespacio.
- Analizar los riesgos de ciberseguridad a los que están expuestos los niños y adolescentes que acceden a contenidos pornográficos en el ciberespacio.
- Proponer recomendaciones de ciberseguridad para la protección de niños y adolescentes cuando están en el ciberespacio.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En Colombia, según el boletín informativo de enero de 2021 realizado por el Instituto Nacional de Medicina Legal y Ciencias Forenses[25] el 82,9% de los exámenes médicos legales realizados por presunto delito sexual, son realizados a menores de 18 años, por tanto, los niños y adolescentes son muy vulnerables a estos ataques. Así como lo expresa Osejo[26] con el uso de la internet, la explotación infantil online hace uso de métodos como el grooming, el sexting y la sextorsión para cometer este tipo de delitos, así que las personas que cometen estos delitos por lo general ya no son personas cercanas a la víctima, sino ciberdelincuentes que están en cualquier parte del mundo.

Según información de la BBC[27] en España debido al confinamiento por causa del COVID-19, las descargas de videos de abuso sexual infantil aumentaron un 25% en pandemia. Además, un estudio realizado por la Organización Internacional del Trabajo[28] en el año 2005, 12,3 millones de personas son víctimas de trabajo forzoso en el mundo, y 1,39 millones están trabajando de manera forzosa en la prostitución infantil, muchos de estos abusos a los niños y adolescentes son gravados y compartidos como material pornográfico en la internet.

De acuerdo con WePROTECT Global Alliance[29] el 94% del material de abuso

[25] Instituto Nacional de Medicina Legal y Ciencias Forenses. Boletín estadístico mensual Centro de Referencia Nacional sobre Violencia-CRNV. [en línea]. 2021-01-01. [citado el 2021-03-21].
[26] OSEJO, Wilmar Andrés. LA EXPLOTACIÓN SEXUAL INFANTIL ONLINE EN COLOMBIA. [en línea]. Universidad Católica de Colombia, 2015-01-01. [citado el 2021-03-21].
[27] ATTANASIO Angelo. Coronavirus: el dramático incremento del consumo de pornografía infantil en el confinamiento por el covid-19. [en línea]. 2020-04-25. [citado el 2021-03-28].
[28] CONFERENCIA INTERNACIONAL DEL TRABAJO. Una alianza globalcontra el trabajo forzoso. [en línea]. 2005-01-01. p. 14-15. [citado el 2021-03-27].
[29] WePROTECT. Puntos de datos clave. [en línea]. [citado el 2021-03-28].

sexual infantil encontrado en línea por Internet Watch Foundation contiene imágenes de niños menores de 13 años y 750 mil es el número estimado de personas en todo el mundo que buscan conectarse en línea con niños para fines sexuales en cualquier momento.

La Unión Internacional de Telecomunicaciones, las empresas que prestan servicios de telecomunicaciones deben establecer medidas que protejan los derechos del niño en línea, una de esas medidas es la "clasificación de contenidos y/o clasificación por edad basados en normas nacionales o internacionales aceptadas y en consonancia con las soluciones adoptadas en medios equivalentes"[30]. Por tanto, el Estado Colombiano ha buscado condiciones propicias para que los niños y adolescentes puedan acceder a internet de forma segura y dicho autor recomienda un software de filtrado que impida el acceso a páginas peligrosas para los niños y adolescentes.

En un estudio realizado por la Universidad de Ciencias Informáticas de La Habana en Cuba[31], resalta la importancia de identificar y clasificar la información que provienen de páginas web, es por ello que han desarrollado un software para clasificar las páginas web mediante la inteligencia artificial y minería de datos, lo cual han podido analizar enlaces, los idiomas, e imágenes digitales obteniendo así un clasificador de contenido independiente de la clasificación de URL realizadas por terceros.

---

[30] Unión Internacional de Telecomunicaciones. Directrices sobre la protección de la infancia en línea para la industria 2020. [en línea]. 2020-01-01. pp 41-48 [citado el 2021-03-28]. ISBN: 978-92-61-30413-3

[31] HERNÁNDEZ Yurisleidy, RIPOLL Dovier, SÁNCHEZ Luis, IBAÑEZ Kiuver y VERDECIA Karel. Técnicas de Inteligencia Artificial en el filtro de contenido web Smart Keeper para la clasificación de información. [en línea]. 2012-01-24. [citado el 2021-03-26]. ISSN: 1994-1536

Como lo expresa Ovideo, Manco y Guerra[32] en su publicación: Sistema multiagente para el filtrado de pornografía mediante la evaluación del contenido multimedial de las páginas web, el filtrado de contenido no es perfecto, ya que se puede ser muy restrictivo o permisivo con el filtrado de contenido, es por ello que los autores presentan una solución de filtrado de contenido a través de los sistemas multiagentes, lo que permite que el filtrado de contenido evolucione a través del tiempo ya que usa la inteligencia artificial. Por otra parte, García[33] dice que el filtrado de contenido basado en el aprendizaje se ha destacado, ya que se ha podido filtrar correos spam de manera dinámica de acuerdo con las preferencias del usuario haciendo uso de filtrados bayesianos.

4.2 MARCO CONCEPTUAL

A continuación, se describe los términos importantes para esta monografía.

Explotación sexual: según Lago y Céspedes[34] es la "la utilización de un niño o niña con la finalidad de satisfacer o gratificar sexualmente a un adulto o grupo de adultos" y además de esto, estos niños se usan como objetos comerciales. Aquí está la prostitución infantil, la pedofilia, el tráfico de niños para el turismo sexual y la pornografía que circula a través de internet.

Filtro de contenido: son una serie de técnicas para regular el tráfico de contenido en una red.

Grooming: es un conjunto de conductas en las cuales el delincuente obtiene la

[32] OVIEDO Ana, MANCO Catalina y GUERRA Juan. Sistema multiagente para el filtrado de pornografía mediante la evaluación del contenido multimedial de las páginas web. [en línea]. 2013-06-01. [citado el 2021-03-26]. SSN 2215-8200

[33] GARCÍA MÁRQUEZ Carlos Alberto. Comparación de Dos Métodos de Filtrado de Spam Basados en Bayes. [en línea]. p. 97. [citado el 2021-03-28].

[34] LAGO BARNEY, Gabriel y CÉSPEDES LONDOÑO, Jaime Aurelio. Abuso sexual infantil. [en línea]. p. 16. [citado el 2021-03-21].

confianza de un niño o adolescente con el fin de realizar actos delincuenciales [35]. El grooming es muy usado en los chats de las redes sociales para posteriormente obtener fotos o videos pornográficos de las víctimas.

Ingeniería social: el Instituto Nacional de Ciberseguridad[36] dice que son técnicas de persuasión usadas por una persona para obtener información confidencial como claves, códigos, imágenes.

Pornografía infantil: De acuerdo con Morillas Fernández[37] es un delito grave contra niños en el cual se construye un documento audio visual o escrito de abusos contra dichos niños. Estos archivos circulan a través del ciberespacio.

Red Peer-to-peer: una red peer-to-peer o P2P es una red de computadoras o nodos los cuales al mismo tiempo actúan como cliente y servidor, entre estos nodos comparten una porción de recursos como procesamiento, almacenamiento o ancho de banda. Este concepto de red está desde 1990 y una red P2P puede tener un alcance de hasta millones de usuarios conectados entre sí, por tanto, si existe algún fallo de conexión en algunos nodos, esto no será un inconveniente ya que en redes P2P ningún nodo es indispensable y por tanto se obtendrá el recurso solicitado de otro computador. Según Guzmán Ortega[38], la seguridad en reden P2P no es fuerte, ya que pueden circular archivos infectados de virus o malware.

Sexting: es el envío de mensajes sexuales a través de chats y redes sociales.

---

[35] BARBOSA, I. & Ojeda, A. Ingeniería social utilizada en el abuso de infantes a través de las redes sociales en Colombia. [Internet]. 2018. [citado: 2021, febrero]

[36] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Glosario de Términos de Seguridad. [en línea]. p. 25. [citado el 2021-03-21].

[37] MORILLAS FERNÁNDEZ, David Lorenzo. ANÁLISIS DOGMÁTICO Y CRIMINOLÓGICO DE LOS DELITOS DE PORNOGRAFÍA INFANTIL. [en línea]. Madrid: DYKINSON, S.L. Meléndez Valdés, p. 38. [citado el 2021-03-21]. ISBN: 84-9772-668-5

[38] GUZMAN ORTEGA, Alfredo. Análisis de Difusión de un Gusano en una Red Peer-to-Peer. [en línea]. 2010-05-01. p. 4-5. [citado el 2021-03-21].

4.3 MARCO LEGAL

El Código Penal Colombiano (Ley 599 de 2000), se establece en el artículo 218 y 219A delitos relacionados con contenidos de explotación sexual infantil. El artículo 218 dice: “El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro”[39].

En el Código Penal Colombiano también describe en el artículo 219 la pena establecida por el delito del turismo sexual con menores de edad el cual dice: “El que dirija, organice o promueva actividades turísticas que incluyan la utilización sexual de menores de edad incurrirá en prisión de cuatro (4) a ocho (8) años. La pena se aumentará en la mitad cuando la conducta se realizare con menor de doce (12) años.”[40]

El artículo 219A del mismo Código Penal Colombiano establece pana de prisión de 10 a 14 años y multa de 67 a 750 salarios mínimos legales mensuales vigentes por el siguiente delito: “El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad, incurrirá en pena de prisión de diez (10) a catorce (14) años y multa de sesenta y siete (67) a (750) salarios mínimos legales mensuales vigentes. Las penas señaladas en el inciso anterior se aumentarán

[39] CONGRESO DE LA REPÚBLICA. LEY 599 de 2000. [en línea]. COLOMBIA: 2000-07-24. [citado el 2022-09-01]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
[40] ibíd

hasta en la mitad (1/2) cuando las conductas se realizaren con menores de catorce (14) años."[41]

Además quien omita denuncia de algún delito sexual con menores de edad, el artículo 219B establece: "El que, por razón de su oficio, cargo, o actividad, tuviere conocimiento de la utilización de menores para la realización de cualquiera de las conductas previstas en el presente capítulo y omitiere informar a las autoridades administrativas o judiciales competentes sobre tales hechos, teniendo el deber legal de hacerlo, incurrirá en multa de trece punto treinta y tres (13.33) a setenta y cinco (75) salarios mínimos legales mensuales vigentes. Si la conducta se realizare por servidor público, se impondrá, además, la pérdida del empleo."[42]

Cuando una persona comete un delito sexual, tendrá las siguientes inhabilidades, artículo 219C del Código Penal Colombiano: "Las personas que hayan sido condenados por la comisión de delitos contra la libertad, integridad y formación sexuales de persona menor de 18 años de acuerdo con el Título IV de la presente ley; serán inhabilitadas para el desempeño de cargos, oficios o profesiones que involucren una relación directa y habitual con menores de edad"[43].

En Colombia, la ley 679 de 2001 en la cual se dictan "medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio"[44]. Y con la ley 1336 de 2009 "se adiciona y robustece

---

[41] CONGRESO DE LA REPÚBLICA. LEY 599 de 2000. [en línea]. COLOMBIA: 2000-07-24. [citado el 2022-09-01]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
[42] Ibíd
[43] CONGRESO DE LA REPÚBLICA. LEY 599 de 2000. [en línea]. COLOMBIA: 2000-07-24. [citado el 2022-09-01]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
[44] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 679 DE 2001. [en línea]. 2001-08-04. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html

la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes".[45]

La Ley 1918 de 2018 "Por medio de la cual se establece el régimen de inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones."[46], así mismo, el decreto 753 de 2019[47] reglamenta la ley 1918 de 2018, es por ello que la Policía Nacional de Colombia ha dispuesto un sistema de consulta de inhabilidades por delitos sexuales con menores de edad y se puede consultar en el siguiente link https://inhabilidades.policia.gov.co:8080/

Además a ello la ley 1928 de 2018 aprueba el Convenio sobre la Ciberdelincuencia en el cual se debe tipificar como delito "la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona, la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos"[48]. En el Código Nacional de Seguridad y Convivencia Ciudadana aparada con la ley 1801 de 2016 en el artículo 38 prohíbe el ingreso de niños a

---

[45] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1336 DE 2009. [en línea]. 2009-07-21. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1336_2009.html

[46] CONGRESO DE LA REPÚBLICA DE COLOMBIA. LEY 1918 DE 2018. [en línea]. Colombia: 2018-07-12. [citado el 2022-09-13]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1918_2018.html

[47] PRESIDENTE DE LA REPÚBLICA. Decreto 753 de 2019. [en línea]. Colombia: 2019-04-30. [citado el 2022-09-13]. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?id=30036442

[48] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1928 DE 2018. [en línea]. 2017-07-24. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

lugares donde “se realicen actividades sexuales o pornográficas, o se ejerza la prostitución, o la explotación sexual”[49].

En el 2002, el Congreso de la República de Colombia reglamenta a través del Decreto 1524[50] el artículo 5 de la Ley 679 de 2001. El artículo 5 dice: “INFORME DE LA COMISIÓN. Con base en el informe de que trata el artículo anterior, el Gobierno nacional, con el apoyo de la Comisión de Regulación de Telecomunicaciones, adoptará las medidas administrativas y técnicas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad. Las regulaciones sobre medidas administrativas y técnicas serán expedidas por el Gobierno Nacional dentro de los seis (6) meses siguientes a la fecha de vigencia de la presente ley.”[51], este decreto tiene como objetivo establecer las medidas técnicas y administrativas para prevenir el acceso de menores de edad a contenidos pornográficos en el ciberespacio.

[49] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1801 DE 2016. [en línea]. 2016-07-29. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1801_2016.html

[50] MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. [en línea]. 2015-09-12. [citado el 2022-09-05]. Disponible en: https://www.enticconfio.gov.co/decreto-1524-de-2002

[51] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 679 DE 2001. [en línea]. 2001-08-04. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html

5 DESARROLLO DE OBJETIVOS

5.1 TÉCNICAS Y NUEVAS TECNOLOGÍAS MÁS UTILIZADAS PARA EL CONTROL DE BLOQUEO DE CONTENIDO PORNOGRÁFICO EN EL CIBERESPACIO

En la actualidad existen distintas técnicas para el control de bloqueo de contenido a nivel de redes, navegadores y dispositivos. Dichas técnicas pueden ser combinadas para fortalecer la seguridad informática y proteger a los niños y adolescentes cuando están en el ciberespacio, a continuación, se describen las técnicas más utilizadas para el control de contenido pornográfico.

5.1.1 Técnicas de filtro de tráfico de datos usadas por los softwares de control parental. La Agencia Española de Protección de Datos (AEPD)52 expone algunas opciones para evitar el acceso a contenido inapropiado, dichas opciones son formas parciales y limitan en la medida de lo posible la exposición a contenido inapropiado para niños en instituciones educativas y en los hogares. Entre las herramientas se encuentran los buscadores seguros y las aplicaciones de contenido exclusivo para niños como:

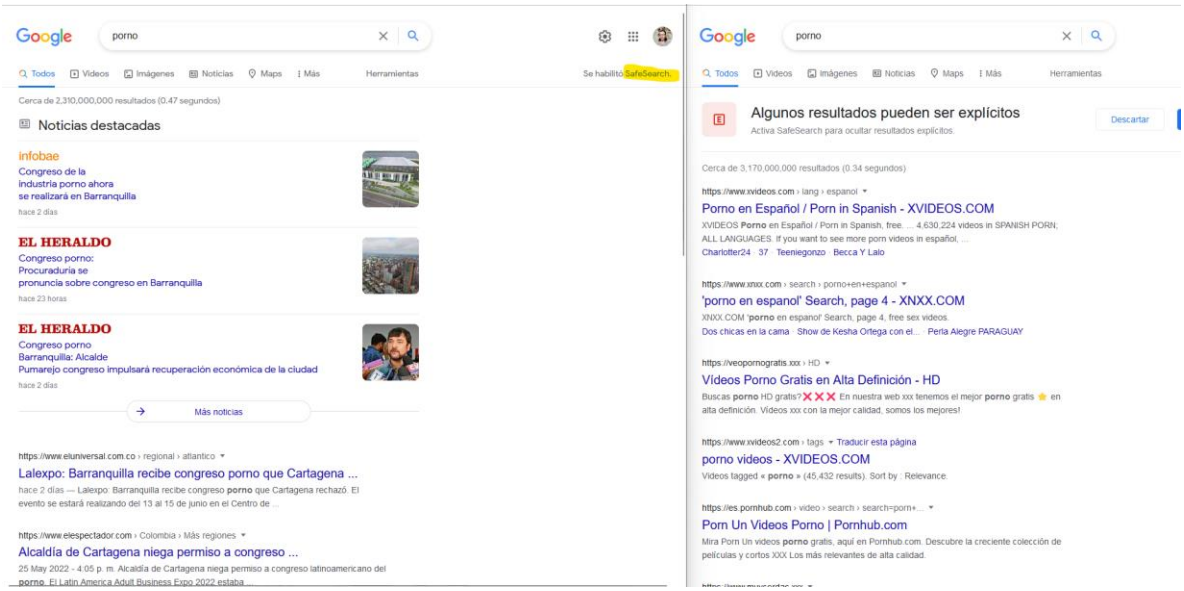
Buscadores

- SafeSearch[53] es una herramienta creada por Google para administrar el contenido en línea apropiado para la familia, SafeSearch se integra con YouTube, PlayStore y el Asistente de Google. Además, esta herramienta se puede activar en los navegador o cuentas personales, también en cuentas y dispositivos supervisados de los niños mediante la app de Family Link o en

[52] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Protección del menoren Internet Evita el contenido inapropiado preservando su privacidad. [en línea]. 2020-02-01. [citado el 2021-05-09]. f
[53] GOOGLE. SafeSearch. [en línea]. [citado el 2021-05-09]. Disponible en: https://safety.google/families/

redes y dispositivos laborales o educativos. Las técnicas usadas por Google son los filtros inteligentes, los bloqueadores de sitios y la clasificación de contenido. En la figura 1 se muestran los resultados de búsqueda en dos navegadores, al navegador del lado izquierdo se activó la opción de SafeSearch y mostró resultados que bloquearon páginas pornográficas, mientras que el navegador del lado derecho muestra resultados explícitos con contenido pornográfico con páginas como xvideos y xnxx, así que activar SafeSearch cuando se usa el buscador de Google ayuda a mitigar los contenidos pornográfico, este SafeSearch no es totalmente infalible, si la persona accede directamente al dominio de una página con contenido pornográfico podrá acceder sin ninguna restricción.

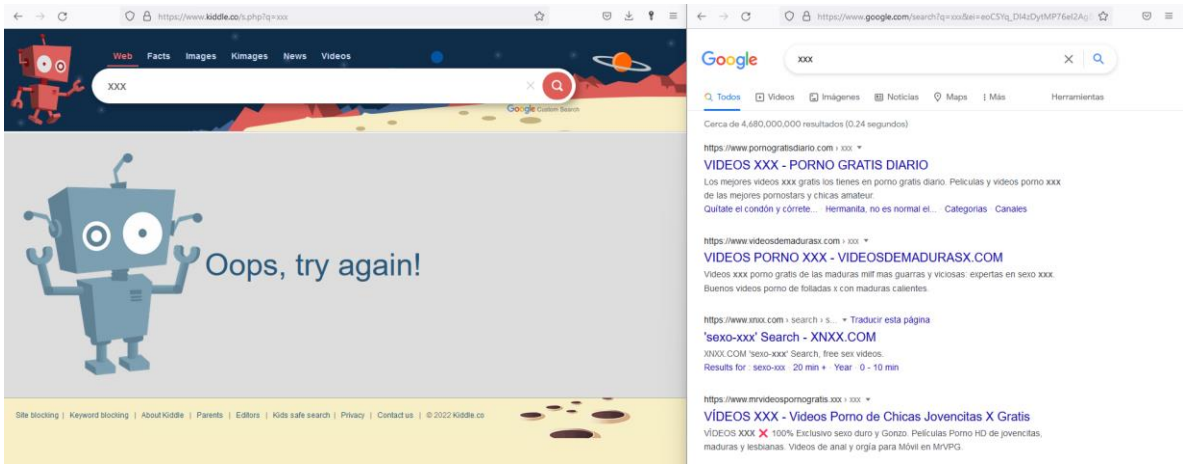
Figura 1. Bloqueo de contenido pornográfico con SafeSearch



Fuente: Buscador de Google

- Kiddle[54] se basa en SafeSearch, pero este buscador es creado por Kiddle, y permite a la comunidad que lo usa solicitar el bloqueo de palabras a través de un formulario dispuesto para este fin. Es un buscador que bloquea el contenido explícito de pornografía y permite la posibilidad sugerir palabras de posibles búsquedas para bloquear los resultados de dicha búsqueda. En la figura 2 se muestra los resultados de búsqueda usando Kiddle y Google, y se evidencia que el buscador Kiddle bloquea los contenidos explícitos de pornografía, sin embargo si desde el navegador se accede al dominio de alguna página con contenido pornográfico, el navegador lo va a permitir sin ninguna restricción.

Figura 2. Bloqueo de contenido explícito de pornografía con Kiddle



Fuente: Buscador de Kiddle y Google

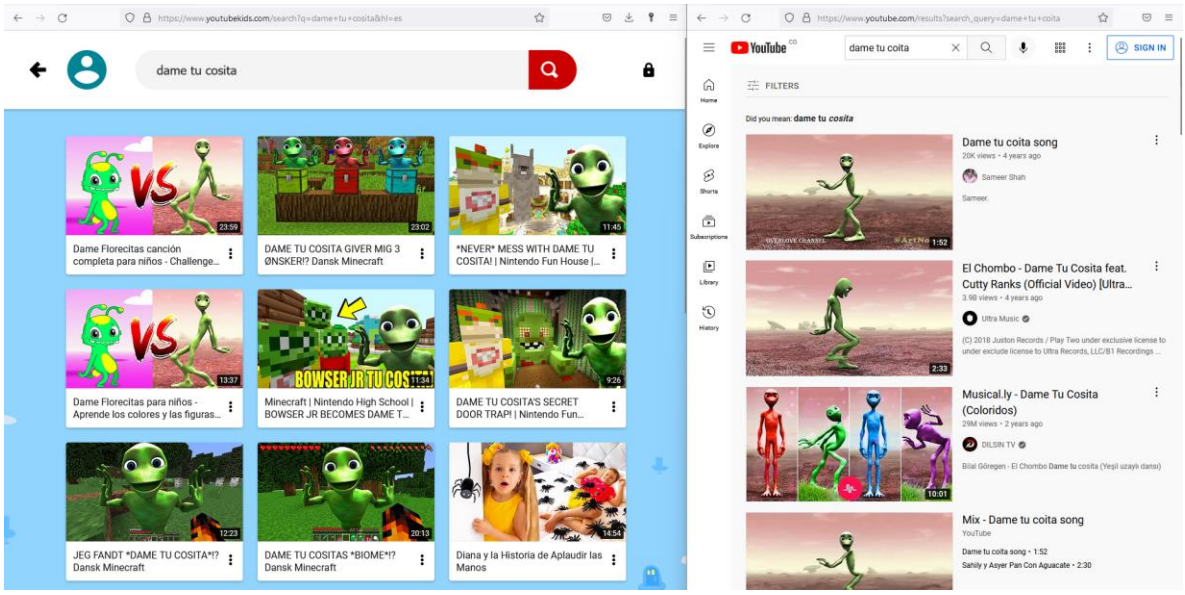
Aplicaciones:

- YouTube for Kids[55] tiene como fin proteger a los niños que navegan en internet, brindando videos que sean aptos para toda la familia. Las técnicas usadas por YouTube for Kids son los filtros automáticos diseñados por ellos

[54] KIDDLE. Kiddle. [en línea]. [citado el 2021-05-09]. Disponible en: https://www.kiddle.co
[55] YouTube. YouTube for Kids. [en línea]. [citado el 2021-05-09]. Disponible en: https://www.youtube.com/kids/

mismos, también realizan revisiones manuales y tienen en cuenta los comentarios de los padres para el bloqueo de videos. Se realizaron pruebas haciendo uso de esta herramienta y notablemente se reduce los videos que no son aptos para menores de edad, es recomendable que los menores de edad usen esta herramienta con el fin de que los niños veo contenido pornográfico por accidente. En la figura 3 se muestra los resultados de búsqueda usando YouTube for Kids y YouTube, al realizar la misma búsqueda, las dos aplicaciones muestran resultados diferentes.

Figura 3. Filtro de contenido usando YouTube for Kids



Fuente: YouTube for Kids

- Qustodio[56]. Es una herramienta para proteger y controlar al menor de edad con el uso que ellos tienen en los dispositivos, esta herramienta se puede implementar en familias y en las instituciones educativas y este software permite bloquear contenido inapropiado, y destacan que en la navegación

[56] QUSTODIO. La mejor aplicación gratis de control parental en Internet. [en línea]. [citado el 2021-05-15].

privada también lo pueden bloquear. Para las redes sociales como YouTube, Facebook, Twitter, Instagram y Whatsapp solo se puede gestionar el tiempo se los menores de edad pueden usar estas redes, lo que no garantiza que se bloqueen contenidos como imágenes y videos con contenido sexuales. Para bloquear contenidos web cuando se navega por internet, Qustodio asegura que el modo restringido de los buscadores de Google, Bing y YouTube estén activados, por tanto son estas empresas quien realizan el filtro de contenido.

- Kaspersky Safe Kids[57]. Es un software de control parental de pago, en el cual supervisa el uso de los dispositivos multiplataforma, en la supervisión de las redes sociales no permite identificar las publicaciones privadas o en los chats, solo muestra su actividad en las publicaciones con un alcance público. El filtro de contenido web se hace solo por medio de la aplicación Kaspersky Safe Kids y solo funciona en PC, Mac y dispositivos Android, en dispositivos con sistema operativo iOS no funciona debido a las restricciones que este sistema operativo tiene.

Control parental ofrecidos por los sistemas operativos

- Family Link[58] es una aplicación creada por Google para dispositivos Android y Chrome que permite establecer reglas digitales básicas para el uso de app y bloqueo de sitios webs, al funcionar en el navegador Chrome, entonces el niño puede usar otro navegador para acceder al ciberespacio y lamentablemente las búsquedas que podría hacer el niño no serán filtradas y podrá ver pornografía explícita. La técnica usada para el bloqueo de sitios webs son las listas negras.

[57] SHAULI ZACKS. Kaspersky Safe Kids Opiniones 2021: es barato pero, ¿merece la pena comprarlo?. [en línea]. 2021-04-27. [citado el 2021-05-15].
[58] GOOGLE. Family Link. [en línea]. [citado el 2021-05-09].

- Control Parental Apple[59] es una funcionalidad de los teléfonos con sistema operativo iOS y iPadOS, tiene funciones para el monitoreo del dispositivo e identifica la cantidad de tiempo que ha usado una app y también bloquea el contenido haciendo uso de la técnica de lista negras.

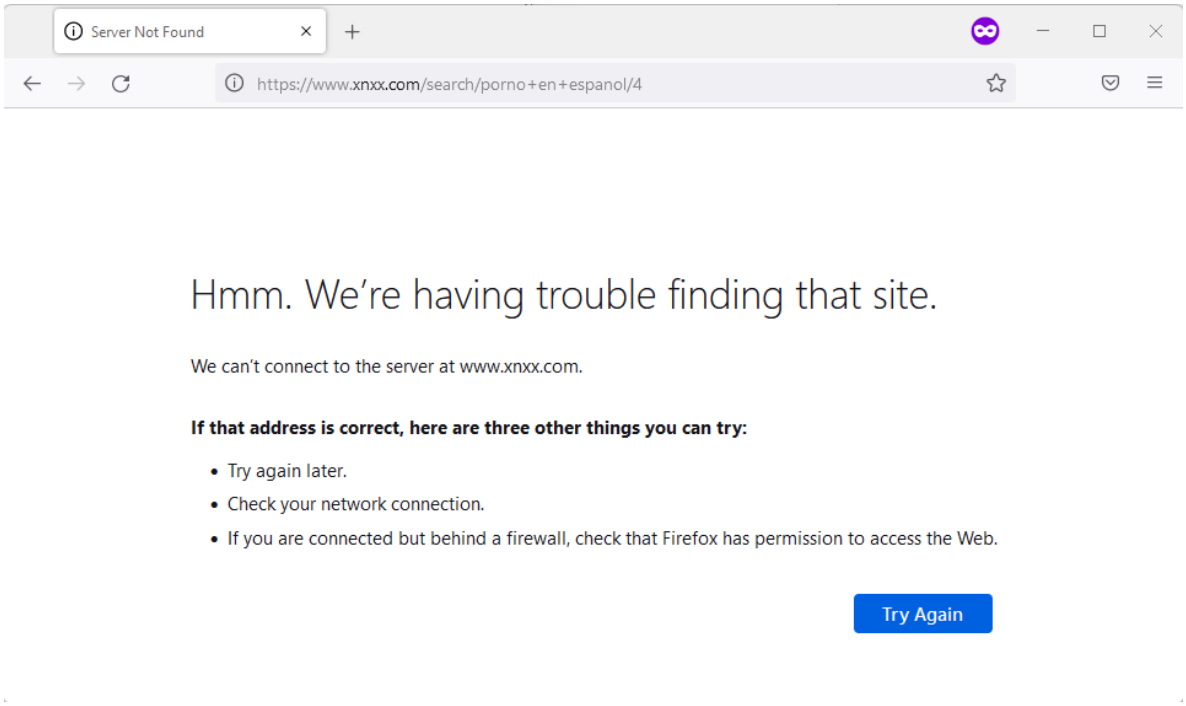
Bloqueo por DNS

- OpenDNS Family Shield[60] es un servidor DNS preconfigurado para bloquear contenido para adultos.
- CleanBrowsing[61] es un filtrado de contenido y la seguridad basados en DNS, tiene filtros para contenido para adultos y pornografía, también bloquea páginas con contenido mixto, como Reddit, el cual es usado para compartir imágenes para adultos, pero también es usado para otros fines. Filtra Torrents y bloquea la conexión a redes P2P y dominios para compartir archivos, además bloquea accesos a proxies y VPN con el fin de no pasar por alto las reglas establecidas por esta solución.

Como se evidenció anteriormente, las aplicaciones y buscadores no bloquean contenido pornográfico si el niño o adolescente ingresa el dominio de estas páginas directamente en el navegador, el bloqueo de contenido por DNS es una opción favorable para impedir que niños y adolescentes accedan directamente a estas páginas con contenido para adultos. En la figura 4 se evidencia el bloqueo de una página con contenido para adultos después de configurar OpenDNS o CleanBrowing.

[59] APPLE. Utilizar los controles parentales del iPhone, iPad y iPod touch de tus hijos. [en línea]. [citado el 2021-05-09].
[60] OPENDNS. Set Up OpenDNS On Your Device. [en línea]. [citado el 2021-05-09].
[61] CLEANBROWSING. Content Filtering & Protection. [en línea]. [citado el 2021-05-09]. Disponible en: https://cleanbrowsing.org/

Figura 4. Bloqueo de contenido pornográfico por DNS



Fuente: Navegador Firefox

Sin embargo, si el niño o adolescente tiene un usuario administrador podría cambiar la configuración del DNS y ya este tipo de contenidos no sería bloqueado, por ello se recomienda que las cuentas de usuario no tengan privilegios de administrador.

5.1.2 Técnicas para el filtro de tráfico. El filtro de tráfico de datos es un proceso en el cual se determina que es aceptable o no en una red. Estos filtros se pueden hacer mediante software o hardware y como se ha visto, se puede hacer los filtros a nivel de red como el servidor DNS, a nivel de navegadores, a nivel de aplicaciones como los softwares de control parental, o filtros basados en servicios, es decir filtros dentro de redes sociales.

5.1.2.1 Filtros Inteligentes y Clasificación de contenido: Estas técnicas usadas por Google, según Carreras62 consisten en el análisis de la popularidad de la página y además analiza el contenido de las páginas web por sus palabras claves, para ello, Google tiene algoritmos que permiten la clasificación de páginas y por tanto las bloquea cuando así esté predefinido.

5.1.2.2 Bloqueo por DNS – Listas Negras: Esta técnica consiste en realizar una lista de todas las páginas web que no son apropiadas para menores de edad y configurar el servidor DNS para que no responda con la IP perteneciente a dicha página web.

Las técnicas para el filtro de tráfico de datos con imágenes y videos pornográficos en redes sociales son escasas en los softwares de control parental, estos softwares se limitan a informar la cantidad de tiempo que los menores han usado dichos aplicativos o a bloquear el uso de estas aplicaciones, además en las redes P2P no bloquean específicamente el contenido del tráfico de red como imágenes y videos pornográficos, algunos softwares bloquean las páginas que están relacionadas a las conexiones P2P, por tanto, los softwares de control parental no bloquean imágenes o videos con contenidos pornográficos.

[62] CARRERAS LARIO, Ricardo. CÓMO CLASIFICA GOOGLE LOS RESULTADOS DE LAS BÚSQUEDAS: FACTORES DE POSICIONAMIENTO ORGÁNICO. [en línea]. Madrid-España: 2012-07-24. p. 494. Disponible en: https://eprints.ucm.es/id/eprint/17450/

5.1.2.3 PICS – Platform For Internet Content Selection:La W3C[63] en su página oficial describe el PICS como una infraestructura de etiquetado para internet, esta plataforma creada en 1996 brinda un formato estándar para el etiquetado de contenidos en internet, el etiquetado se puede hacer de forma manual, es decir, lo creadores etiquetan su propia página, y la otra forma es hacer uso de servidores de clasificación de páginas webs. Los contenidos de las páginas web pueden ser etiquetadas en varias dimensiones. Al hacer uso de softwares de control parental que usen PICS se puede realizar un bloqueo flexible, ya que se puede bloquear información dependiendo de la persona y el contexto.

5.1.2.4 IDetect: es un algoritmo distribuido que fue creado por Jianming Lv, Zhiwen Yu y Tieying Zhang64 para detectar contenidos nocivos e ilegales en redes P2P. La creación de este algoritmo fue inspirado en el mecanismo de detección clona del sistema inmunológico. Así que, los clientes de las redes P2P que tienen implementado el algoritmo iDetect ayudan a detectar el contenido nocivo de manera distribuida y organizada. En los experimentos que han realizado, se demuestra que este algoritmo detecta a los clientes que comparten contenido nocivo en las redes P2P de manera eficiente, eficaz y escalable.

5.1.2.5 Sistema de detección y prevención de intrusos:

- NIDS. En el ámbito informático, el NIDS es una aplicación usada para detectar accesos no autorizados a una determinada red o computador en tiempo real, es decir, monitorea el tráfico de la red. Como explica Salom[65] el

[63] RESNICK, Paul. PICS: Internet Access Controls Without Censorship. [en línea]. AT&T Research, [citado el 2021-05-07]. Disponible en: https://www.w3.org/PICS/iacwcv2.htm
[64] JIANMING Lv, ZHIWEN Yu, TIEYING Zhang, "Towards an immunity based distributed algorithm to detect harmful files shared in P2P networks", *Peer-to-Peer Networking and Applications*, vol. 8, pp. 49, 2015.
[65] SALOM MARTÍN, José Antonio. Ventajas e implementación de un sistema IDS/SIEM en el ámbito familiar. [en línea]. Universitat Oberta de Catalunya (UOC), 2019-06-04. [citado el 2021-05-08]. Disponible en: http://hdl.handle.net/10609/95087

NIDS detecta accesos no autorizados “analizando los paquetes que circulan por la red en busca de coincidencias definidas previamente mediante unas reglas que identifican comportamientos sospechosos en la red”, y además adiciona, que en una red ethernet los paquetes recibidos son los que van dirigidos solo a dichos dispositivos, por ello, para que el NIDS reciba todos los paquetes que hay en el tráfico de red, es necesario establecer la interfaz de red que hará de sniffer en modo promiscuo. Así el NIDS podrá capturar y analizar todos los paquetes del tráfico de una red sin importar el destinatario.

- NIPS. Es un software para proteger a los sistemas de ataques e intrusiones, este software genera alarmas, descarta paquetes y/o desconecta conexiones sospechosas. Los Firewalls tiene este trabajan en conjunto con los NIPS para descartar paquetes sospechosos.

A continuación, se describen algunas herramientas de este tipo.

SNORT[66]: es una herramienta de software libre disponible para Linux y Windows, esta herramienta es muy usada y tiene una gran comunidad que continuamente enriquece la herramienta. SNORT puede usarse como un NIDS o un NIPS y su funcionamiento consiste es capturar el tráfico de red y analizarlo con un conjunto de reglas con el fin de encontrar patrones que presentan anomalías en la red. Snort se configura a través de archivos de reglas que se pueden descargar en la página web www.snort.org, o también se pueden crear las propias reglas para bloquear el tráfico deseado.

[66] DAVIDOCHOBITS. Detección de intrusos con Snort. [en línea]. 2020-09-29. [citado el 2021-04-19]. Disponible en: https://www.ochobitshacenunbyte.com/2020/09/29/deteccion-de-intrusos-con-snort/

Según Escartín[67], la forma más fácil para bloquear las redes P2P usando Snort es dejando habilitado las reglas el archivo de p2p.rules, el cual contiene las reglas necesarias para bloquear los archivos que se comparten punto a punto. Con dichas reglas se crearán alertas cuando se identifiquen este tipo de paquetes.

Según estudio realizado por la Europol[68], existen tres grandes redes P2P que ha aumentado su uso en tiempos de la pandemia por COVID-19 y otros países han tenido un crecimiento similar, las redes P2P más usadas son eMule, BitTorrent y Gnutella. Así que a continuación, se muestra una regla de Snort para detener el tráfico de datos a través de eMule.

```
alert tcp $EXTERNAL_NET 6666:6669 -> $HOME_NET any ( msg:"SERVER-OTHER
eMule buffer overflow attempt"; flow:to_client,established;
content:"PRIVMSG",fast_pattern,nocase;
pcre:"/^PRIVMSG\s+[^\s]+\s+\x3a\s*\x01SENDLINK\x7c[^\x7c]{69}/smi";
metadata:ruleset community; reference:bugtraq,10039;
reference:cve,2004-1892; reference:nessus,12233; classtype:attempted-
user; sid:2584; rev:10;)
```

SURICATA[69]: Es un NIDS/NIPS de código abierto disponible para varias plataformas, desarrollador por OSIF (Open Information Security Fundation), se base en un concepto similar al de Snort. Según Salom[70] la diferencia radica en que aprovecha la modernidad del hardware para analizar eficazmente los

[67] ESCARTÍN VIGO, Jose Antonio. Servidor Linux para conexiones seguras de una LAN a Internet. [en línea]. 2005-06-01. p. 225. [citado el 2021-05-08].
[68] EUROPOL. Catching the virus cybercrime, disinformation and the COVID-19 pandemic. [en línea]. 2020-04-03. [citado el 2021-05-08].
[69] MYSECURITYSTUFF. IDS/IPS Suricata - ¿Qué es y cómo funciona? [en línea]. 2019-05-20. [citado el 2021-04-19].
[70] SALOM MARTÍN, José Antonio. Ventajas e implementación de un sistema IDS/SIEM en el ámbito familiar. [en línea]. Universitat Oberta de Catalunya (UOC), 2019-06-04. [citado el 2021-05-08].

paquetes en el tráfico de la red, además usa el lenguaje de script LUA para la detección de amenazas más complejas. Suricata es compatible con las reglas de la comunidad de Snort, por tanto, se puede migrar de un software a otro sin complicaciones.

Como se plasmó anteriormente, las aplicaciones de control parental y buscadores para niños permiten acceder a páginas con contenidos pornográficos si el niño o adolescente ingresa el dominio de estas páginas directamente en el navegador, por tanto, se debe fortalecer la seguridad usando las técnicas de bloqueo de contenido por DNS, esto con el fin de impedir que niños niñas y adolescentes accedan directamente a estas páginas con contenido para adultos. Además se identificó que el filtro de tráfico de contenidos a través de la red es de mayor eficiencia, ya que cualquier dispositivo conectado a la red se someterá a dichas restricciones, un ejemplo de ello son los NIDS/NIPS que permiten bloquear redes P2P, páginas con contenido pornográfico y redes sociales a través de reglas, pero estas herramientas permiten bloquear toda la red P2P o toda la red social, y no solo el contenido perjudicial para el menor de edad, para mejorar esto, se podría usar el algoritmo iDetect, que permite detectar imágenes y videos pornográficos en redes P2P, en redes sociales, es complejo, ya que la política de privacidad de dichas redes sociales impide que software de terceros examinen las imágenes, videos, audios o textos que circulan en dichas redes sociales para poderlas identificar y bloquear.

5.2 RIESGOS DE CIBERSEGURIDAD A LOS QUE ESTÁN EXPUESTOS LOS NIÑOS Y ADOLESCENTES QUE ACCEDEN A CONTENIDOS PORNOGRÁFICOS

Según el portal Gaptain[71] los niños y adolescentes están expuestos a distintos peligros en internet, los niños de 2 a 5 años el principal uso que le dan a internet es la visualización de videos en YouTube, el cual puede acceder a videos que no son apropiados para la edad del niño o a la pornografía explícita. Niños entre 6 a 9 años comienzan a hacer uso de las redes sociales, y allí pueden publicar datos privados, tener chats con contactos peligrosos. Los adolescentes de 10 a 14 años ya empiezan a tener su celular, y con ello, pueden tener el riesgo de retos virales y ciberacoso. Y los jóvenes de 15 a 17 años, pueden ser víctimas de sexting, grooming, chantaje sexual.

A continuación, se describen algunos riesgos a los que se está expuesto las personas que hacen uso de la internet:

[71] DE PEDRO, Sandra. Los 8 riesgos en Internet para niños y adolescentes que debes seguir de cerca. [en línea]. Gaptain, 2021-12-01. [citado el 2022-03-20]. Disponible en: https://gaptain.com/blog/los-8-principales-riesgos-en-internet-para-ninos-y-adolescentes/

5.2.1 Suplantación de la identidad del usuario. Consiste en que una persona se haga pasar por la identidad de otra en un ambiente virtual para obtener beneficios propios, según datos de la Policía Nacional de Colombia72 dichas personas usan las redes sociales para pedir dinero prestado, para solicitar falsas recolecciones de encomiendas y ventas falsas de divisas, estas personas se hacen pasar por amigos o familiares para generar confianza en la victima y así proceder con la estafa, pero estos delincuentes nunca responden a llamadas o video llamadas para confirmar su identidad.

Como lo expresa García[73] la comunicación con personas desconocidas se puede realizar a través de páginas webs, sitios de chats y mensajería instantánea, los niños y adolescentes acceden a estos sitios y hablan con personas que no conocen en la vida real, y estos niños son víctimas de engaños, abusos, acciones ilícitas contra los niños, solicitudes de información personal

Deepfake.

La DIJIN[74] de la Policía Nacional de Colombia informa que en el año 2020 el delito de suplantación de identidad aumentó en un 409%, y la suplantación de identidad se hace para solicitar créditos o productos a entidades bancarias, es así como el portal de tecnología 20 Minutos[75] expone las 5 grandes amenazas cibernéticas para el año 2023, en el cual muestra que el deepfake será una gran amenaza para

---

[72] POLICIA NACIONAL DE COLOMBIA. Suplantación para estafar en redes sociales. [en línea]. Colombia: Policia Nacional, [citado el 2022-12-16]. https://caivirtual.policia.gov.co/ciberseguridad/boletines/todos

[73] GARCÍA PIÑA C. A, Riesgos del uso de internet por niños y adolescentes. Estrategias de seguridad. Acta Pediátrica de México [Internet]. 2008;29(5):272-278. Recuperado de: https://www.redalyc.org/articulo.oa?id=423640313006

[74] SEMANA. Suplantación de identidad, un flagelo que está al alza. [en línea]. Revista Semana, 2022-01-12. [citado el 2022-12-16]. Disponible en: https://www.semana.com/economia/macroeconomia/articulo/suplantacion-de-identidad-un-flagelo-que-esta-al-alza/202214/

[75] ANAYA, Fernando. 2023 será un año turbulento en ciberseguridad: las 5 grandes amenazas. [en línea]. 2023-01-08. [citado el 2023-01-09]. Disponible en: https://www.20minutos.es/tecnologia/ciberseguridad/2023-sera-un-ano-turbulento-en-ciberseguridad-las-5-grandes-amenazas-5089351/

la suplantación de identidad ya que un delincuente sin tener muchos conocimientos en tecnología puede fácilmente generar audios y videos falsos con la identidad de otra persona.

El portal de tecnología Xataka[76] publicó una noticia que evidencia una estafa por 35 millones de dólares en el año 2020, usando la inteligencia artificial (deepfake), en el cual los delincuentes imitaron la voz de un cliente de un banco de los Emiratos Árabes para solicitarle al funcionario del banco realizar transacciones bancarias a distintas cuentas para una supuesta compra de una empresa, este funcionario reconoció la voz del cliente e inmediatamente comenzó a realizar las transacciones, lo que conlleva a tomar medidas como la verificación de la verdadera identidad, para evitar ser víctimas de este delito.

La técnica de suplantación de identidad que usa la inteligencia artificial como el deepfake, permite que un delincuente genere audios y videos falsos de una persona de confianza para el niño o adolescente, por ejemplo, la pareja sentimental de un adolescente, para así solicitar contenido pornográfico a través de las redes sociales y el ciberdelincuente comete su delito y obtiene sus beneficios.

Sexting.

La suplantación de identidad permite que se practique el sexting, que es la acción de enviar contenido fotográfico o audiovisual producido por el mismo remitente a través de su celular u otro dispositivo tecnológico, y el receptor lo usa para hacer chantaje, burla, amenazas o sextorsión, así lo describe la Policía Nacional de

[76] RODRÍGUEZ, Pablo. Las grandes estafas con deepfakes de voz ya son una realidad: roban 35 millones de dólares a un banco usando esta tecnología . [en línea]. 2021-10-15. Disponible en: https://www.xataka.com/robotica-e-ia/estafas-deepfakes-voz-realidad-roban-35-millones-dolares-a-banco-usando-esta-tecnologia

Colombia[77]. Según un estudio realizado por Rojas y Jhoeen[78] en el 2019, en una universidad de Medellín-Colombia, a estudiantes de pregrado, se evidenció que el 59% de los estudiantes universitarios realizan la práctica del Sexting ya que piensan que es una práctica segura, al usar su propio celular para compartir contenido sexual con sus parejas sentimentales.

En la investigación realizada por Tigo e la Universidad EAFIT[79] se muestra que el 20% de los niños y adolescentes encuestados han recibido mensajes de contenido sexual en internet como fotos, videos, textos, audios o gifs, y el 19% de estas personas han recibido este tipo de mensajes a través de una red social como WhatsApp, Facebook, Twitter, Google+, Instagram, Snapchat…). Además, el 3% de los encuestados reconocen que en el último año ha enviado o publicado mensajes de contenido sexual en internet.

5.2.2 Difusión de software dañino. En la actualidad, los niños y adolescentes saben instalar programas en los computadores, un método que usan los ciberdelincuentes para instalar malware es a través de las descargas de software de páginas no oficiales. Además, los niños y adolescentes buscan los cracks en la internet para tener un software legal, y como se sabe los cracks de estos programas siempre se deben ejecutar por lo tanto es un clásico método para la difusión de software dañino.

Las redes P2P son muy usadas para la difusión de software dañino, en estas redes se encuentran cualquier tipo de contenido llamativo para los niños y

---

[77] POLICIA NACIONAL DE COLOMBIA. Qué es y cómo prevenir el Sexting. [en línea]. [citado el 2022-03-22]. Disponible en: https://caivirtual.policia.gov.co/contenido/que-es-y-como-prevenir-el-sexting

[78] ROJAS-DIAZ, JHOEEN SNEYDER. Sexting: Incidencia de los teléfonos inteligentes en la sexualidad de los universitarios. [en línea]. 2019-04-10. [citado el 2022-03-15]. Disponible en: https://reunir.unir.net/handle/123456789/9508

[79] TIGO. 8 Principales Riesgos que Experimentan Niños y Adolescentes en el Uso de Internet. [en línea]. [citado el 2022-04-10]. Disponible en: https://contigoconectados.com/resultados/riesgos/

adolescentes, como juegos, películas, música entre otros, y al descargar estos contenidos pueden descargar malware.

También los ciberdelincuentes pueden usar el correo electrónico para incitar al niño y adolescente a descargar imágenes y al hacer esto también se descarga software malicioso, recientemente los ciberdelincuentes usaron las imágenes de las fotografías del telescopio James Webb para distribuir software malicioso, así lo expresa el portal web Computer Hoy[80], esta misma técnica la usan para distribuir malware en imágenes pornográficas ya que pueden colocar JavaScript en los metadatos de una imagen.

Esta técnica de ocultar un archivo dentro de otro, se conoce como esteganografía digital y los ciberdelincuentes han usado esta técnica para ocultar el software malicioso dentro de las imágenes, y así, cuando un usuario descarga una imagen del correo o de sitios web poco confiables, inmediatamente se ejecuta el malware y el computador o dispositivo electrónico queda infectado, para evitar ser victimas de estos ataques, los cuales pasan desapercibidos, los usuarios deben evitar las descargas automáticas de las imágenes en los navegadores, es decir, solo permitir la visualización de la imágenes en los navegadores, así lo recomienda el portal web 20 Minutos[81], además sospechar de imágenes cuyo peso sea muy grande con relación a la dimensión de la imagen.

---

[80] CARVAJAL, Chema. Así es cómo están escondiendo software malicioso en las imágenes del telescopio James Webb. [en línea]. 2022-09-01. [citado el 2023-01-09]. Disponible en: https://computerhoy.com/noticias/tecnologia/como-estan-escondiendo-software-malicioso-imagenes-telescopio-james-webb-1117685

[81] HOLGADO, Raquel. Otra amenaza en la red: así ocultan malware en las imágenes (y esto puedes hacer al respecto). [en línea]. 2022-09-26. [citado el 2023-01-18]. Disponible en: https://www.20minutos.es/tecnologia/ciberseguridad/otra-amenaza-en-la-red-asi-ocultan-malware-en-las-imagenes-y-esto-puedes-hacer-al-respecto-5063516/

5.2.3 Divulgación de información. Cuando un computador o celular tiene malware se expone a que datos personales o información financiera sea divulgada en la internet. Además, los delincuentes usan la ingeniería social para obtener información personal y financiera de su víctima. En la darkweb se consigue información financiera a muy bajo precio, se pueden conseguir tarjetas de crédito o débito clonadas por 5 dólares.

Es importante, que las personas no publiquen información personal en las redes sociales, ya que estos datos pueden ser tomados para luego ser vendidos, o para realizar algún tipo de extorsión

5.2.4 Extorsión. Un estudio realizado en el 2015 en la ciudad de La Rioja en España denominado: Factores de Riesgo en el Ciberbullying. Frecuencia y Exposición de los Datos Personales en Internet82, deja en evidencia que la extorsión o ciberacoso está relacionado con la exposición de datos personales en internet, además también está relacionado con la baja percepción de los riesgos y relaciones sociales en redes sociales, en este estudio se demuestra que el 31,4% de los encuestados ha declarado haber sufrido algún tipo de ciberacoso, es decir, uno de cada tres personas ha sido víctima de este delito por causa de publicar datos personales en internet.

Según una investigación de Oliveros, Amemiya, Condorimay, Oliveros, Barrientos y Rivas[83], en el año 2012, ellos demostraron que tener un celular, el computador en el cuarto y acceso a internet fuera de la casa, son factores de riesgo para el ciberacoso, muchos padres permiten que sus hijos tengan un celular desde muy

[82] SABATER FERNÁNDEZ, C., & LÓPEZ HERNÁEZ, L. Factores de riesgo en el Ciberbullying. Frecuencia y exposición de los datos personales en Internet. [en línea]. International Journal of Sociology of Education, [citado el 2022-04-05]. Disponible en: https://doi.org/10.4471/rise.2015.01

[83] OLIVEROS, M., AMEMIYA, I., CONDORIMAY, Y., OLIVEROS, R., BARRIENTOS, A. Y RIVAS, B. Ciberbullying: Nueva tecnología electrónica al servicio del acoso escolar en alumnos de dos distritos de Lima. [en línea]. Perú: 2012-01-01. p. 13-18. [citado el 2022-04-06].

temprana edad y no se concientiza al niño o adolescente de no publicar datos personales en internet, lo que incrementa el riesgo de ser víctima de extorsión.

5.2.5 Ingeniería social. El **grooming** es una técnica de ingeniería social implementada por un adulto para hacerse pasar por un menor de edad y así ganar la confianza de niños y adolescentes con el fin de obtener contenido sexual de parte de estos niños. El grooming se desarrolla en dos fases, la primera es ganarse la confianza del niño o adolescente a treves de las redes sociales para pedir contenido sexual, y la otra fase inicia con el chantaje para obtener más contenido de imágenes o videos que comprometan a la víctima.

En el año 2021 se reportaron 516 denuncias en Colombia de acoso sexual en internet a menores de edad, 621 de sextorsión y 325 de Ciberbullying, y el boletín de la Policía Nacional[84] también informa que las aplicaciones más usadas para cometer estos delitos son WhatsApp, Telegram, Facebook, e Instagram.

En una encuesta realizada por U Report[85] en el 2019 a jóvenes de más de 30 países se muestra que el 30% de los encuestados ha sufrido algún tipo de acoso cibernético y el 71% de los encuestados consideran que el acoso virtual se hace a través de las redes sociales, además, 1 de cada 5 estudiantes dejaron de asistir al colegio ya que eran víctimas de algún tipo de acoso en línea.

[84] POLICIA NACIONAL. Boletín - Material de Abuso Sexual Infantil. [en línea]. 2021-12-15. [citado el 2022-03-14]. Disponible en: https://caivirtual.policia.gov.co/#observatorio

[85] UNICEF. UNICEF busca empoderar a jóvenes para evitar el acoso y prevenir los riesgos en línea. [en línea]. 2020-02-10. [citado el 2022-04-04]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/unicef-busca-empoderar-a-jovenes-para-evitar-el-acoso-y-prevenir-los-riesgos-en-linea

5.2.6 Pornografía implícita en YouTube. En YouTube, “se prohíbe el contenido sexual explícito que incluya a menores o en el que se los explote sexualmente” 86, pero algunos videos evaden estas políticas y se pueden encontrar videos infantiles cuyo trasfondo es pornográfico, un ejemplo de ello es un video publicado en YouTube en el 2018 donde se muestra al Alien verde animado en 3D bailando con movimientos pélvicos sexuales y en repetidas ocasiones se escucha decir “dame tu cosita”87 y en el artículo “La difusión del vídeo musical en YouTube. Análisis de la capacidad viral del vídeoclip”88 donde concluyen que con el transcurrir del tiempo los gustos musicales de los consumidores de videos en internet cambian y por ello, en un determinado momento un video se hace viral, y el video Dame tu cosita fue un video viral que muchos niños visualizaron repetidas veces, consumiendo contenido pornográfico implícito en YouTube.

En YouTube hay gran diversidad de videos, y existen videos que producen placer sexual con objetos comunes, así lo explica un artículo en el diario El País, titulado “La atracción sexual hacia los globos y otras parafilias del mundo moderno”[89] donde relata algunos ejemplos de personas que tiene placer sexual con situaciones u objetos que son normales para la mayoría de los seres humanos, a esto se le llama parafilia, y como lo explica el portal Psicología y Mente[90], las parafilias son patrones de comportamiento sexual poco habituales y entre estos comportamientos está la pedofilia, el fetichismo, el frotismo.

---

[86] YOUTUBE. Políticas sobre imágenes de desnudos y contenido sexual. [en línea]. [citado el 2022-03-17]. Disponible en: https://support.google.com/youtube/answer/2802002?hl=es-419#zippy=%2Cotros-tipos-de-contenido-que-infringen-esta-pol%C3%ADtica

[87] EL CHOMBO. Dame tu cosita. [en línea]. 2018-04-05. [citado el 2022-03-14]. Disponible en: https://www.youtube.com/watch?v=FzG4uDgje3M&list=PLepAqroiLqtQytSjBmOX23CHQ5U0dmMAG

[88] BAÑOS-GONZÁLEZ, M., Canorea Tiralaso, H. y Rajas Fernández, M. (2020). La difusión del vídeo musical en YouTube. Análisis de la capacidad viral del vídeoclip. Revista Latina de Comunicación Social , (77), 117-141. https://www.doi.org/10.4185/RLCS-2020-1452

[89] WIENER, Gabriela. La atracción sexual hacia los globos y otras parafilias del mundo moderno. [en línea]. 2016-06-11. [citado el 2022-03-21]. Disponible en: https://elpais.com/elpais/2016/07/10/tentaciones/1468144394_715728.html

[90] MONTAGUD RUBIOM, Nahum. Las 15 parafilias más comunes (y sus características). [en línea]. [citado el 2022-03-23]. Disponible en: https://psicologiaymente.com/clinica/parafilias-mas-comunes

En la investigación “Contigo Conectados”[91] realizada por la empresa Tigo y la Universidad EAFIT, en dicha investigación se analizan los riesgos que experimentan los niños y adolescentes entre 9 y 16 años de 8 ciudades de Colombia, entre los cuales se evidencia que el 35% de los encuestados ha visto en internet durante el último año personas desnudas o teniendo relaciones sexuales y los medios más usados para ver este tipo de contenido son las redes sociales con un 24%, en ventanas emergentes que aparecían accidentalmente con un 12%, en películas o videos en internet (por ejemplo YouTube) con un 10%, en una página web calificada para adultos con un 7%, y en un 3% en juegos en internet.

5.2.7 Camfecting, cámaras web troyanizadas. El camfecing es la acción de tener el control de la cámara web sin ser detectado. ESET92 explica que los ciberdelincuentes acceden a la cámara de forma remota para hacer grabaciones de audio y video sin necesidad de activar la luz led que indica que la cámara está encendida, luego estas grabaciones son enviadas y así proceden a realizar extorciones. Este tipo de ataque se puede desplegar atraves de archivos adjuntos maliciosos, enlaces, mensajería instantánea, redes sociales y software que parece ser legítimo.

Otra forma que los ciberdelincuentes pueden tomar el control de la cámara web, es a treves de los exploits de las vulnerabilidades de los software, es por ello que se recomienda tener actualizadas las apps o software instalados en los

[91] TIGO. 8 principales Riesgos que Experimentan Niños y Adolescentes en el Uso de Internet. [en línea]. [citado el 2022-04-10]. Disponible en: https://contigoconectados.com/resultados/riesgos/
[92] ESET. Hackeo de webcams: cómo saber si alguien te está espiando a través de tu cámara. [en línea]. 2022-05-10. [citado el 2023-03-10]. Disponible en: https://blogs.protegerse.com/2022/05/10/hackeo-de-webcams-como-saber-si-alguien-te-esta-espiando-a-traves-de-tu-camara/

computadores y teléfonos inteligentes para evitar que los delincuentes exploten estas vulnerabilidades de seguridad.

5.3 RECOMENDACIONES DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE NIÑOS Y ADOLESCENTES CUANDO ESTÁN EN EL CIBERESPACIO

En la actualidad existen distintas organizaciones a nivel internacional y local que protegen los niños, niñas y adolescentes de los delitos cometidos a través del ciber espacio, a continuación, se describen las recomendaciones que estas entidades tienen para evitar que los niños y adolescentes sean víctimas de los delitos como abuso sexual infantil, engaños en línea, sexting, grooming entre otros.

Una de las organizaciones más conocidas a nivel mundial es la **UNICEF**, la cual ha realizado las siguientes recomendaciones para el uso seguro de la internet en tiempos de COVID-19[93]

- Configurar los controles parentales siguiendo estas guías, las cuales están clasificadas según plataformas, redes, dispositivos, redes sociales entre otras, las guías se pueden descargar en: https://www.internetmatters.org/es/parental-controls/
- Activar el filtro de búsquedas seguras todos los navegadores que se usan, para activarlos, la UNICEF recomienda seguir las siguientes indicaciones: https://www.internetmatters.org/es/parental-controls/entertainment-search-engines/
- Establecer configuraciones de privacidad en las redes sociales, aplicaciones y videojuegos en línea. https://www.internetmatters.org/es/parental-controls/social-media/
- Cubrir las cámaras webs que no estén siendo usadas.

[93] UNICEF. Consejos sobre crianza durante la COVID-19. [en línea]. [citado el 2023-02-16]. Disponible en: https://www.unicef.org/es/coronavirus/consejos-crianza-covid19#7

Otra organización es **la National Center for Missing & Exploited Children** (EE. UU.). la cual brinda ayudas a las víctimas de las **imágenes de abuso sexual infantil**[94], donde se evidencia a través de encuestas, que las victimas que se muestran en estas imágenes son revictimizadas ya que las imágenes persisten en el ciberespacio y se reenvían muchas veces a través de redes sociales, plataformas de juegos y correos electrónicos. También ayudan a los niños que son víctimas de los **engaños en línea**[95], la cual, esta organización identificó que hay victimas desde 1 a 17 años de edad, siendo la edad media los 15 años, también se sabe que estos niños no conocen a su abusador, el cual, el 82% son adultos hombres que engañan a los niños, y el 9% son mujeres, el 9% restante no se conoce su genero. Las recomendaciones de seguridad dadas por esta organización son:[96]:

- Para que los niños y adolescentes jueguen de forma segura, la participación de los padres es fundamental, el padre debe tener interés por los juegos que el niño juega y saber si en el juego se establecen comunicaciones entre los jugadores.
- Además, se deben tener las consolas de videojuegos en un lugar de fácil supervisión y estar atento a otros lugares como las casas de sus amigos en donde el niño pueda acceder a estos juegos.
- Se debe enseñar al niño o adolescente que nunca dé información personal mientras juega y tampoco debe reuniese con personas que conoció exclusivamente a través de los juegos en línea.

---

[94] NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (EE. UU.). Imágenes de Abuso Sexual Infantil. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/theissues/csam

[95] NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (EE. UU.). Engaño en Línea. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/theissues/onlineenticement

[96] NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (EE. UU.). Recursos. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/netsmartz/resources

- Establecer reglas del tiempo y los tipos de juegos que puede jugar y usar software de control parental usando algún PIN para evitar que el niño cambie la configuración de este software.
- No guardar automáticamente los detalles de la tarjeta de crédito en las consolas de videojuegos, esto hace que el niño consulte con el padre antes de realizar algún pago.
- Evite iniciar sesión a una plataforma utilizando información de otra cuenta, ya que esto puede permitir acceder a información personal del perfil.
- Usar los mas estrictos softwares de monitoreo no garantiza que los niños estén protegidos mientras están en el ciberespacio, por ello se recomienda dejar los computadores o pantallas en un lugar de fácil visualización para que los padres o cuidadores puedan ver lo que los niños estén haciendo.

Otra organización es la **Common Sense**, cuya misión es ayudar a los niños y adolescentes a desarrollarse y prosperar en el actual mundo de medios y tecnología, ellos hacen una reseña objetiva de juegos, programas de televisión, películas, sitios webs, aplicativos móviles, plataformas, redes sociales, estas reseñas las clasifican por edad, así que es una organización que brinda información valiosa para padres y educadores sobre los medios tecnológicos que están en el mundo. Para bloquear pornografía infantil la Common Sense recomienda:[97]

- Configurar la búsqueda segura en los navegadores como Google SafeSearch y periódicamente revisar los filtros, ya que fácilmente se pueden desactivar.

[97] COMMON SENSE. Cómo bloquear la pornografía en los celulares, tablets y computadoras de tu hijo. [en línea]. 2023-01-09. [citado el 2023-02-21]. Disponible en: https://www.commonsensemedia.org/es/articulos/como-bloquear-la-pornografia-en-los-celulares-tablets-y-computadoras-de-tu-hijo

- Usar controles parentales en los celulares, tabletas y computadores
- Bloqueo de contenido pornográfico por parte del proveedor de servicio de internet
- Instalar software de seguridad
- Hablar sobre la pornografía con los niños y adolescentes de forma apropiada a cada edad

La organización **Internet of Good Things** recomienda que se debe hablar con los niños y adolescentes acerca del uso de internet y dice lo siguiente:[98]

- Hablar con los niños para hacerles entender para qué deben usar internet y las redes sociales
- Preguntar a los niños y adolescentes qué sitios visitan y qué hacen en dichos sitios, además se debe preguntar, que les gusta y lo que nos les gusta de internet.
- Se debe hablar con los niños y adolescentes sobre lo que ellos consideran un buen y un mal comportamiento en internet y en las redes sociales.
- Mantener una buena comunicación abierta con los niños para que se animen a contar lo que les ha sucedido en internet.
- Pedir a los niños y adolescentes que enseñen sobre más cosas que hacen en internet, ya que los niños son muy habilidosos para el uso de internet

La **WeProtected Global Alliance** es una organización a nivel mundial en la cual participan 100 paises, ellos han dado recomendaciones a gobiernos, sociedad

[98] INTERNET of Good Things. ¿Debes hablar con tus hijos acerca de la seguridad en Internet?. [en línea]. [citado el 2023-02-23]. Disponible en: https://www.internetofgoodthings.org/es/sections/spanish-connect-smart/obtener-respuestas/debes-hablar-con-tus-hijos-acerca-de-la-seguridad-en-internet/

civil, comunidades, y los proveedores de servicios en línea. En cuanto a tecnología han recomendado[99]:

- Los proveedores de servicios en línea deben adoptar un enfoque de “Safety by Design” para los servicios destinados a los niños.
- Los proveedores de servicios en línea deben publicar periódicamente informes de transparencia
- Los desarrolladores de tecnología de seguridad en línea debe innovar en sus tecnologías para mejorar la detección del abuso sexual infantil en línea.

El **ICBF** (Instituto Colombiano de Bienestar Familiar) de Colombia, hace las siguientes recomendaciones a distintos públicos para la navegación segura en internet a los padres, cuidadores, empresas de tecnología y proveedores de servicios de internet[100]:

- Generar espacios de confianza para conversar con los niños y adolescentes acerca de los riesgos que pueden tener al navegar en internet
- Conocer las redes sociales que usan los niños y adolescentes y establecer reglas para su uso.
- Reportar situaciones de ciberacoso en www.teprotejo.org
- Las empresas de tecnología deben desarrollar tecnología más seguros para los niños y adolescentes.
- Los proveedores de servicios de internet deben promover protocolos ágiles y eficientes para bloquear contenidos que afectan a los niños y adolescentes

---

[99] WEPROTECTET. Evaluación de amenazas globales 2021. [en línea]. [citado el 2023-02-24]. Disponible en: https://www.weprotect.org/global-threat-assessment-21/

[100] ICBF. En el Día del Internet Seguro, actuemos juntos para proteger a niñas, niños y adolescentes en los entornos digitales. [en línea]. 2021-02-05. [citado el 2023-02-25]. Disponible en: https://www.icbf.gov.co/noticias/en-el-dia-del-internet-seguro-actuemos-juntos-para-proteger-ninas-ninos-y-adolescentes-en

La empresa de ciberseguridad de Europa, ESET[101] hace las siguientes recomendaciones para evitar ser víctima del ataque camfecting:

- Tener el software actualizado de los diferentes dispositivos que tengan cámaras, como computadores, celulares y dispositivos IoT
- Hacer uso de contraseñas seguras y única, si es posible hacer uso de la autenticación en dos pasos.
- No hacer abrir enlaces sospechosos o enlaces que no fueron solicitados.
- Cubrir el objetivo de la cámara, pero esto sigue permitiendo que el ciberdelincuente escuche a través del micrófono del dispositivo.

Para la protección de los niños en línea la INTERPOL[102] recomienda:

- Establecer un diálogo abierto sobre el uso del internet, hablar con claridad que hay cosas buenas y malas
- El uso de software de filtrado y notificaciones son tranquilizadores para los padres, pero el niño debe tener la confianza de hablar con sus padres si algo malo está ocurriendo con el uso de la internet.
- Comprobar los parámetros de privacidad de las aplicaciones
- No compartir el nombre completo, dirección, fecha de cumpleaños, numero de teléfono, dirección, o nombre del colegio.
- Evitar hacer encuentros físicos con amigos en línea, si lo hacen tomen medidas de seguridad y avisen a sus familiares

[101] ESET. Hackeo de webcams: cómo saber si alguien te está espiando a través de tu cámara. [en línea]. 2022-05-10. [citado el 2023-03-10]. Disponible en: https://blogs.protegerse.com/2022/05/10/hackeo-de-webcams-como-saber-si-alguien-te-esta-espiando-a-traves-de-tu-camara/

[102] INTERPOL. Protección de los niños en línea. [en línea]. [citado el 2023-03-10]. Disponible en: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Proteccion-de-los-ninos-en-linea

- Considerar las imágenes y mensajes que se van a compartir, nunca se podrá borrar completamente una publicación
- Si no se está seguro con una conversación en línea, es mejor no contestar.

En la actualidad se está empezando a desarrollar software que usa la inteligencia artificial (IA) para detectar imágenes de abuso sexual infantil. Un ejemplo de ello es 4NSEEK[103], un software desarrollado por INCIBE y en colaboración de algunas universidades de España, actualmente la herramienta ha dejado de ser soportada. Esta herramienta cuenta con módulos de inteligencia artificial para detectar en las imágenes o videos alguna evidencia sobre el delito de abuso sexual infantil. Con esta herramienta se puede detectar rostros para estimar su edad y género, también tiene la capacidad de detectar material de abuso sexual a menores a través del nombre del fichero y su ruta, además, permite la detección de órganos sexuales en dichas imágenes incautadas en alguna investigación.

Otro proyecto que usa la inteligencia artificial para detectar la explotación y el abuso sexual infantil está financiado por End Violence Against Children[104] y en desarrollo por la Universidad de los Andes, el objetivo es usar la inteligencia artificial para estudiar el lenguaje y los patrones de interacción entre los delincuentes y victimas, este proyecto estará disponible para países latinoamericanos y entidades que investiguen sobre el abuso sexual infantil.

Google[105] también está usando la inteligencia artificial para detectar imágenes con abusos sexuales infantiles, cuando una imagen tiene un posible abuso sexual

---

[103] INCIBE. Herramienta 4NSEEK. [en línea]. [citado el 2023-03-13]. Disponible en: https://www.incibe.es/proyectos-europeos/4nseek/herramienta#modulos

[104] END VIOLENCE AGAINST CHILDREN. Using AI tools to end online child sexual exploitation and abuse in Latin America . [en línea]. 2022-03-12. Disponible en: https://www.end-violence.org/articles/using-ai-tools-end-online-child-sexual-abuse-and-exploitation-latin-america

[105] GOOGLE. How we detect, remove and report child sexual abuse material. [en línea]. 2022-10-28. [citado el 2023-03-15]. Disponible en: https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/

infantil, esta es revisada por un equipo de humanos para luego realizar el denuncio y así identificar la victima y evitar que siga siendo abusada.

Muchos de los riesgos a los que niños y adolescentes están expuestos en el ciberespacio como la pornografía implícita en YouTube, el sexting, la publicación de datos personales y el grooming pueden ser mitigados por una buenas prácticas y acciones que la persona puede tomar para no ser víctima de los riesgos en ciberseguridad. Es por ello por lo que se debe tener una buena cultura para el uso de internet, a continuación, se realizan las siguientes recomendaciones:

Instalar un software de control parental como YouTube for Kids, Qustodio, Kaspersky Safe Kids, Family Link y/o Control parental de Apple, expuestos anteriormente ayudan a controlar el uso del ciberespacio en niños y adolescentes, controla la cantidad de tiempo que pueden usar las aplicaciones y los horarios de conexión, esto será de utilidad para evitar que el niño y adolescente se un consumidor excesivo de internet.

Usar un buscador para filtrar el contenido como SafeSearch o Kiddle ayuda notablemente a filtrar las búsquedas para evitar contenido de pornografía explícito en internet, así se demostró en la sección anterior la diferencia de resultados al usar este tipo de buscadores y usar un buscador sin ningún tipo de restricción.

Además, para mejorar la seguridad se recomienda configurar un DNS para filtrar contenido para adultos, existen DNS gratuitas que filtran pornografía, vpn, proxies, con el fin mejorar la protección en el ciberespacio.

Sin embargo, por motivos de privacidad, software de terceros no van a bloquear imágenes o videos pornográficos enviados a través de redes sociales o chats, por tal motivo, cuando una persona está chateando o haciendo uso del ciberespacio, es recomendable evitar compartir contenido de imágenes, videos o audios con

desnudos o mensajes eróticos, ya que estos pueden ser divulgados a través del ciberespacio y causar en la victima problemas de salud mental, como se mostró en las secciones anteriores, para los adolescente el sexting se ha convertido en algo normal, y por tal motivo entre las parejas se comparten entre ellos contenido sexual, que luego dichos contenidos pueden ser publicados con otras personas u otras redes sociales.

Los padres, maestros o adultos responsables deben hablar constantemente con los niños y adolescentes de los riesgos que pueden sufrir al hacer uso inadecuado de la navegación en el ciberespacio y dar consejos para no compartir fotos, videos, audios con contenido sexual, consejos para evitar compartir información personal en la red, también en importante el acompañamiento de los cuidadores a los niños y adolescentes cuando estén en el ciberespacio, aunque no significa que sus cuidadores estén todo el tiempo con los niños y adolescentes cuando estén en el ciberespacio. Con esto se evitar que los niños y adolescentes sean víctimas del grooming.

En la investigación realizada por Tigo Colombia y la Universidad EAFIT[106] se analizó que las medidas técnicas para bloquear contenido pornográfico en el ciberespacio no son tan eficientes, es así como, el 6% de los padres contratan un servicio para limitar el tiempo que el niño o adolescente está en el ciberespacio, además, el 9% de los padres instalan algún software para bloquear el acceso a algunas paginas web y realizar seguimiento a las páginas webs visitadas. Es por ello que es de gran importancia que los niños y adolescentes usen las redes sociales con responsabilidad, respeto y cuiden su cuerpo con el fin de no compartir contenido pornográfico en el ciberespacio.

[106] TIGO. Contigo Conectados. [en línea]. [citado el 2022-04-01]. Disponible en: https://contigoconectados.com/resultados/mediacion/

6 CONCLUSIONES

En esta monografía se examinó las técnicas y nuevas tecnologías más utilizadas para el control de bloqueo de contenido pornográfico en el ciberespacio, a través de consultas sistémicas de distintos trabajos se identificó que las técnicas para el filtro de tráfico de datos con imágenes y videos pornográficos en redes sociales como Facebook, Twitter, Instagram, Whatsapp y TikTok, son escasas en los softwares de control parental, estos softwares se limitan a informar la cantidad de tiempo que los menores han usado dichos aplicativos o a bloquear el uso de estas aplicaciones, por tanto, los softwares de control parental no bloquean imágenes o videos con contenidos pornográficos.

En este documento se examinó que los softwares para el control parental identificados en esta monografía no bloquean específicamente el contenido del tráfico de red como imágenes y videos pornográficos en las redes peer-to-peer (P2P), algunos softwares si pueden bloquear las páginas que están relacionadas a las conexiones P2P.

Además, se describió que el filtro de tráfico de contenidos a través de la red es más eficiente, ya que cualquier dispositivo conectado a la red se someterá a dichas restricciones. iDetect el algoritmo distribuido para detectar imágenes y videos pornográficos ha sido un algoritmo innovador para detectar este tipo de contenidos sin cerrar totalmente la conexión a este tipo de redes P2P.

También se examinó que los NIDS y NIPS permiten bloquear redes P2P y páginas con contenido pornográfico y redes sociales a través de reglas con las que el NIDS/NIPS analiza el tráfico de datos a través de una red, pero estas herramientas solo permiten bloquear toda la red P2P y no solo el contenido perjudicial para el menor de edad.

Conjuntamente se analizó los riesgos de ciberseguridad a los que están expuestos los niños y adolescentes que acceden a contenidos pornográficos en el ciberespacio y se evidenció que todo niño de 2 a 17 años está expuesto a distintos riesgos cuando navegan en el ciberespacio, entre los riesgos está la pornografía implícita que está en los videos de YouTube, el sexting, la publicación de datos personales que pueden ser usados en ciberacoso y el grooming.

También se evidenció que en YouTube hay publicados videos con pornografía, ya que existen formas de evadir la política de prohibición de contenido sexual explícito que tiene YouTube, por tal motivo estos videos siguen publicados en esta red social y se convierten en un riesgo para los niños y adolescentes que navegan en internet.

Las encuestas realizadas por terceros demostraron que el sexting es una práctica común en adolescentes, el 59% de los estudiantes de pregrado envían contenido sexual propio a sus parejas sentimentales desde sus celulares debido a que ellos tienen una percepción de que el sexting es una práctica segura.

Igualmente, las encuestas demostraron que las redes sociales son el medio mas usado por los ciberdelincuentes para cometer delitos como sextorsión y grooming, en Colombia se reportaron 516 denuncias de acoso sexual en internet a menores de edad, 621 de sextorsión y 325 de Ciberbullying.

Así mismo se propusieron recomendaciones de ciberseguridad para la protección de niños y adolescentes cuando están en el ciberespacio.

7 RECOMENDACIONES

Aplicar encuestas a niños y adolescentes en instituciones públicas y privadas donde se evidencie cual es el mayor riesgo a los que están expuestos en el ciberespacio en relación con el aspecto psicológico de cada individuo

Realizar campañas de concientización en las instituciones educativas y los hogares de los diferentes riesgos que tienen los niños y adolescentes al navegar en el ciberespacio.

Educar a los padres de familia y docentes sobre los riesgos de ciberseguridad actuales a los que están expuestos los niños y adolescentes al estar en el ciberespacio, con el fin de que dichos adultos enseñen a los niños para evitar ser víctimas de estas vulnerabilidades.

Montar un escenario virtual o físico donde se evidencie la efectividad de las distintas técnicas y tecnología usadas para el bloqueo de imágenes y videos con contenido de abuso sexual a menores de edad.

Usar la ciencia de datos artificial para analizar el tráfico de datos en una red universitaria o red de hogar. Con el fin de identificar paquetes con contenido pornográfico.

Dado el caso. De ser víctima de algún delito cibernético, denunciar ante las entidades pertinentes en el caso de Colombia, denunciar. Ante el CAI Virtual de la Policía Nacional de Colombia.

8 BIBLIOGRAFÍA

AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Protección del menoren Internet Evita el contenido inapropiado preservando su privacidad. [en línea]. 2020-02-01. [citado el 2021-05-09]. Disponible en: https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf

ANAYA, Fernando. 2023 será un año turbulento en ciberseguridad: las 5 grandes amenazas. [en línea]. 2023-01-08. [citado el 2023-01-09]. Disponible en: https://www.20minutos.es/tecnologia/ciberseguridad/2023-sera-un-ano-turbulento-en-ciberseguridad-las-5-grandes-amenazas-5089351/

ANAYA, Natalia Consuegra. Diccionario de psicología. [en línea]. Segunda Edición. 2010-01-01. [citado el 2022-11-21]. ISBN 978-958-648-650-7

ANÓNIMO. Ciberespacio: definición, aplicaciones y límites. [en línea]. [citado el 2022-11-12]. Disponible en: https://ciberseguridad.com/guias/recursos/ciberespacio/

ANÓNIMO. ¿Sabes qué se Considera un Delito? [en línea]. 2021-08-05. [citado el 2022-11-21]. Disponible en: https://www.colombialegalcorp.com/blog/se-considera-delito/

APPLE. Utilizar los controles parentales del iPhone, iPad y iPod touch de tus hijos. [en línea]. [citado el 2021-05-09]. Disponible en: https://support.apple.com/es-es/HT201304

ARROYO GUARDEÑO, David; GAYOSO MARTINEZ, Victor; HERNANDEZ ENCINAS, Luis. Ciberseguridad. [en línea]. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2020-12-31. p. 13. [citado el 2022-11-12]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/172144?page=13
ISBN 9788400107147

ATTANASIO Angelo. Coronavirus: el dramático incremento del consumo de pornografía infantil en el confinamiento por el covid-19. [en línea]. 2020-04-25. [citado el 2021-03-28]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-52385436

BAÑOS-GONZÁLEZ, M., CANOREA TIRALASO, H. y RAJAS FERNÁNDEZ, M. (2020). La difusión del vídeo musical en YouTube. Análisis de la capacidad viral del vídeoclip. Revista Latina de Comunicación Social, (77), 117-141. https://www.doi.org/10.4185/RLCS-2020-1452

BARBOSA, I. & Ojeda, A. Ingeniería social utilizada en el abuso de infantes a través de las redes sociales en Colombia.

CAMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [en línea]. Primera Edición. Bogotá: 2019-10-29. p. 29.

COMMON SENSE. Cómo bloquear la pornografía en los celulares, tablets y computadoras de tu hijo. [en línea]. 2023-01-09. [citado el 2023-02-21]. Disponible en: https://www.commonsensemedia.org/es/articulos/como-bloquear-la-pornografia-en-los-celulares-tablets-y-computadoras-de-tu-hijo

COLOMBIA. CONGRESO DE LA REPÚBLICA.

LEY 599 de 2000. [en línea]. COLOMBIA: 2000-07-24. [citado el 2022-09-01]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

LEY 679 DE 2001. [en línea]. 2001-08-04. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html

LEY 1336 DE 2009. [en línea]. 2009-07-21. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1336_2009.html

LEY 1801 DE 2016. [en línea]. 2016-07-29. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1801_2016.html

LEY 1918 DE 2018. [en línea]. Colombia: 2018-07-12. [citado el 2022-09-13]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1918_2018.html

LEY 1928 DE 2018. [en línea]. 2017-07-24. [citado el 2021-05-14]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

CONFERENCIA INTERNACIONAL DEL TRABAJO. Una alianza globalcontra el trabajo forzoso. [en línea]. 2005-01-01. p. 14-15. [citado el 2021-03-27]. Disponible en: https://www.ilo.org/public/spanish/standards/relm/ilc/ilc93/pdf/rep-i-b.pdfç

CARRERAS LARIO, Ricardo. CÓMO CLASIFICA GOOGLE LOS RESULTADOS DE LAS BÚSQUEDAS: FACTORES DE POSICIONAMIENTO ORGÁNICO. [en línea]. Madrid-España: 2012-07-24. p. 494. Disponible en: https://eprints.ucm.es/id/eprint/17450/

DANE.

Indicadores básicos de tenencia y uso de Tecnologías de la Información y Comunicación –TIC en hogares y personas de 5 y más años de edad

Indicadores básicos de TIC en Hogares. [en línea]. [citado el 2022-09-14]. Disponible en: https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/tecnologias-de-la-informacion-y-las-comunicaciones-tic/indicadores-basicos-de-tic-en-hogares

DE PEDRO, Sandra. Los 8 riesgos en Internet para niños y adolescentes que debes seguir de cerca. [en línea]. Gaptain, 2021-12-01. [citado el 2022-03-20]. Disponible en: https://gaptain.com/blog/los-8-principales-riesgos-en-internet-para-ninos-y-adolescentes/

EL CHOMBO. Dame tu cosita. [en línea]. 2018-04-05. [citado el 2022-03-14]. Disponible en: https://www.youtube.com/watch?v=FzG4uDgje3M&list=PLepAqroiLqtQytSjBmOX23CHQ5U0dmMAG

END VIOLENCE AGAINST CHILDREN. Using AI tools to end online child sexual exploitation and abuse in Latin America . [en línea]. 2022-03-12. Disponible en: https://www.end-violence.org/articles/using-ai-tools-end-online-child-sexual-abuse-and-exploitation-latin-america

ESCARTÍN VIGO, Jose Antonio. Servidor Linux para conexiones seguras de una LAN a Internet. [en línea]. 2005-06-01. p. 225. [citado el 2021-05-08]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2099.1/3451/52096-9.pdf?sequence=9&isAllowed=y

ESET. Hackeo de webcams: cómo saber si alguien te está espiando a través de tu cámara. [en línea]. 2022-05-10. [citado el 2023-03-10]. Disponible en: https://blogs.protegerse.com/2022/05/10/hackeo-de-webcams-como-saber-si-alguien-te-esta-espiando-a-traves-de-tu-camara/

EUROPOL. Catching the virus cybercrime, disinformation and the COVID-19 pandemic. [en línea]. 2020-04-03. [citado el 2021-05-08]. Disponible en: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

GARCÍA MÁRQUEZ Carlos Alberto. Comparación de Dos Métodos de Filtrado de Spam Basados en Bayes. [en línea]. p. 97. [citado el 2021-03-28]. Disponible en: https://www.researchgate.net/profile/Gildardo-Sanchez-Ante/publication/259343975_Sistemas_Inteligentes_Reportes_Finales_Ago-Dic_2013/links/0c96052b1d0b582e95000000/Sistemas-Inteligentes-Reportes-Finales-Ago-Dic-2013.pdf

FUNDACIÓN RED. Definiciones. [en línea]. [citado el 2022-11-21]. Disponible en: https://redcontraelabusosexual.org/definiciones/

GARCÍA PIÑA C. A, Riesgos del uso de internet por niños y adolescentes. Estrategias de seguridad. Acta Pediátrica de México [Internet]. 2008;29(5):272-278. Recuperado de: https://www.redalyc.org/articulo.oa?id=423640313006

GOOGLE.

SafeSearch. [en línea]. [citado el 2021-05-09]. Disponible en: https://safety.google/families/

Family Link. [en línea]. [citado el 2021-05-09]. Disponible en: https://families.google.com/intl/es-419/familylink/

GUZMÁN ORTEGA, Alfredo. Análisis de Difusión de un Gusano en una Red Peer-to-Peer. [en línea]. 2010-05-01. p. 4-5. [citado el 2021-03-21]. Disponible en: https://repositorio.tec.mx/bitstream/handle/11285/569659/DocsTec_10455.pdf?sequence=1&isAllowed=y

HERNÁNDEZ Yurisleidy, RIPOLL Dovier, SÁNCHEZ Luis, IBAÑEZ Kiuver y VERDECIA Karel. Técnicas de Inteligencia Artificial en el filtro de contenido web Smart Keeper para la clasificación de información. [en línea]. 2012-01-24. [citado el 2021-03-26]. Disponible en: https://www.redalyc.org/pdf/3783/378343674005.pdf ISSN: 1994-1536

HOLGADO, Raquel. Otra amenaza en la red: así ocultan malware en las imágenes (y esto puedes hacer al respecto). [en línea]. 2022-09-26. [citado el 2023-01-18]. Disponible en: https://www.20minutos.es/tecnologia/ciberseguridad/otra-amenaza-en-la-red-asi-ocultan-malware-en-las-imagenes-y-esto-puedes-hacer-al-respecto-5063516/

ICBF. En el Día del Internet Seguro, actuemos juntos para proteger a niñas, niños y adolescentes en los entornos digitales. [en línea]. 2021-02-05. [citado el 2023-02-25]. Disponible en: https://www.icbf.gov.co/noticias/en-el-dia-del-internet-seguro-actuemos-juntos-para-proteger-ninas-ninos-y-adolescentes-en

INCIBE. Herramienta 4NSEEK. [en línea]. [citado el 2023-03-13]. Disponible en: https://www.incibe.es/proyectos-europeos/4nseek/herramienta#modulos

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Glosario de Términos de Seguridad. [en línea]. p. 25. [citado el 2021-03-21]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES. Boletín estadístico mensual Centro de Referencia Nacional sobre Violencia-CRNV. [en línea]. 2021-01-01. [citado el 2021-03-21]. Disponible en: https://www.medicinalegal.gov.co/documents/20143/628335/Boletin+enero+2021+crnv.pdf

INTERNET of Good Things. ¿Debes hablar con tus hijos acerca de la seguridad en Internet?. [en línea]. [citado el 2023-02-23]. Disponible en: https://www.internetofgoodthings.org/es/sections/spanish-connect-smart/obtener-respuestas/debes-hablar-con-tus-hijos-acerca-de-la-seguridad-en-internet/

INTERPOL. Protección de los niños en línea. [en línea]. [citado el 2023-03-10]. Disponible en: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Proteccion-de-los-ninos-en-linea

JIANMING Lv, ZHIWEN Yu, TIEYING Zhang. Towards an immunity based distributed algorithm to detect harmful files shared in P2P networks, Peer-to-Peer Networking and Applications, vol. 8, pp. 49, 2015.

KIDDLE. Kiddle. [en línea]. [citado el 2021-05-09]. Disponible en: https://www.kiddle.co

LAGO BARNEY, Gabriel y CÉSPEDES LONDOÑO, Jaime Aurelio. Abuso sexual infantil. p. 16. [citado el 2021-03-21].

MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. [en línea]. 2015-09-12. [citado el 2022-09-05]. Disponible en: https://www.enticconfio.gov.co/decreto-1524-de-2002

MINISTERIO DE EDUCACIÓN NACIONAL (Colombia). ESTABLECIMIENTOS EDUCATIVOS – (NATURALEZA). [en línea]. 2004-10-05. [citado el 2021-04-11]. Disponible en: https://www.mineducacion.gov.co/1621/articles-127853_archivo_pdf_Naturaleza_4.unknown

MINTIC (Colombia).

La protección de nuestras niñas, niños y adolescentes en Internet, una prioridad del Gobierno nacional.

Internet dedicado. [en línea]. 2022-05-01. [citado el 2022-09-14]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47271.html

MONTAGUD RUBIOM, Nahum. Las 15 parafilias más comunes (y sus características). [en línea]. [citado el 2022-03-23]. Disponible en: https://psicologiaymente.com/clinica/parafilias-mas-comunes

MORILLAS FERNÁNDEZ, David Lorenzo. ANÁLISIS DOGMÁTICO Y CRIMINOLÓGICO DE LOS DELITOS DE PORNOGRAFÍA INFANTIL. Madrid: DYKINSON, S.L. Meléndez Valdés, p. 38. [citado el 2021-03-21]. ISBN: 84-9772-668-5

MYSECURITYSTUFF. IDS/IPS Suricata - ¿Qué es y cómo funciona? [en línea]. 2019-05-20. [citado el 2021-04-19]. Disponible en: https://www.mysecuritystuff.com/suricata-introduccion/

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (EE. UU.).

Imágenes de Abuso Sexual Infantil. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/theissues/csam

Engaño en Línea. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/theissues/onlineenticement

Recursos. [en línea]. [citado el 2023-02-15]. Disponible en: https://esp.missingkids.org/netsmartz/resources

OLIVEROS, M., AMEMIYA, I., CONDORIMAY, Y., OLIVEROS, R., BARRIENTOS, A. Y RIVAS, B. Ciberbullying: Nueva tecnología electrónica al servicio del acoso escolar en alumnos de dos distritos de Lima. Perú: 2012-01-01. p. 13-18. [citado el 2022-04-06].

OPENDNS. Set Up OpenDNS On Your Device. [en línea]. [citado el 2021-05-09]. Disponible en: https://www.opendns.com/setupguide/#familyshield

OSEJO, Wilmar Andrés. LA EXPLOTACIÓN SEXUAL INFANTIL ONLINE EN COLOMBIA. [en línea]. Universidad Católica de Colombia, 2015-01-01. [citado el 2021-03-21]. Disponible en: https://repository.ucatolica.edu.co/handle/10983/15384

OVIEDO Ana, MANCO Catalina y GUERRA Juan. Sistema multiagente para el filtrado de pornografía mediante la evaluación del contenido multimedial de las

páginas web. [en línea]. 2013-06-01. [citado el 2021-03-26]. Disponible en: https://repository.upb.edu.co/handle/20.500.11912/6590 SSN 2215-8200

PRESIDENTE DE LA REPÚBLICA. Decreto 753 de 2019. [en línea]. Colombia: 2019-04-30. [citado el 2022-09-13]. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?id=30036442

POLICÍA NACIONAL DE COLOMBIA.

RIESGOS Y TENDENCIAS EN RELACIÓN CON EL ABUSO Y LA EXPLOTACIÓN SEXUAL DE MENORES. REPERCUSIONES DEL COVID-19

Qué es y cómo prevenir el Sexting. [en línea]. [citado el 2022-03-22]. Disponible en: https://caivirtual.policia.gov.co/contenido/que-es-y-como-prevenir-el-sexting

Boletín - Material de Abuso Sexual Infantil. [en línea]. 2021-12-15. [citado el 2022-03-14]. Disponible en: https://caivirtual.policia.gov.co/#observatorio

Delitos Sexuales 2022. [en línea]. Colombia: 2022-09-01. [citado el 2022-09-14]. Disponible en: https://www.policia.gov.co/contenido/delitos-sexuales-2022-0

Suplantación para estafar en redes sociales. [en línea]. Colombia: Policia Nacional, [citado el 2022-12-16]. https://caivirtual.policia.gov.co/ciberseguridad/boletines/todos

RAE. Diccionario. [en línea]. [citado el 2021-04-11]. Disponible en: https://dle.rae.es

RESNICK, Paul. PICS: Internet Access Controls Without Censorship. [en línea]. AT&T Research, [citado el 2021-05-07]. Disponible en: https://www.w3.org/PICS/iacwcv2.htm

REVISTA SEMANA.

¿Cuánto aumentó el uso de internet en niños por la pandemia?

Suplantación de identidad, un flagelo que está al alza. [en línea]. Revista Semana, 2022-01-12. [citado el 2022-12-16]. Disponible en: https://www.semana.com/economia/macroeconomia/articulo/suplantacion-de-identidad-un-flagelo-que-esta-al-alza/202214/

RODRÍGUEZ, Pablo. Las grandes estafas con deepfakes de voz ya son una realidad: roban 35 millones de dólares a un banco usando esta tecnología . [en línea]. 2021-10-15. Disponible en: https://www.xataka.com/robotica-e-ia/estafas-deepfakes-voz-realidad-roban-35-millones-dolares-a-banco-usando-esta-tecnologia

ROJAS-DIAZ, JHOEEN SNEYDER. Sexting: Incidencia de los teléfonos inteligentes en la sexualidad de los universitarios. [en línea]. 2019-04-10. [citado el 2022-03-15]. Disponible en: https://reunir.unir.net/handle/123456789/9508

SABATER FERNÁNDEZ, C., & LÓPEZ HERNÁEZ, L. Factores de riesgo en el Ciberbullying. Frecuencia y exposición de los datos personales en Internet. [en línea]. International Journal of Sociology of Education, [citado el 2022-04-05]. Disponible en: https://doi.org/10.4471/rise.2015.01

SALOM MARTÍN, José Antonio. Ventajas e implementación de un sistema IDS/SIEM en el ámbito familiar. [en línea]. Universitat Oberta de Catalunya (UOC), 2019-06-04. [citado el 2021-05-08]. Disponible en: http://hdl.handle.net/10609/95087

SHAULI ZACKS. Kaspersky Safe Kids Opiniones 2021: es barato pero, ¿merece la pena comprarlo? [en línea]. 2021-04-27. [citado el 2021-05-15]. Disponible en: https://es.wizcase.com/parental-control/kaspersky-safe-kids/

TIGO.

8 principales Riesgos que Experimentan Niños y Adolescentes en el Uso de Internet. [en línea]. [citado el 2022-04-10]. Disponible en: https://contigoconectados.com/resultados/riesgos/

Contigo Conectados. [en línea]. [citado el 2022-04-01]. Disponible en: https://contigoconectados.com/resultados/mediacion/

UNICEF.

Protección. [en línea]. [citado el 2021-03-20]. Disponible en: https://www.unicef.org/colombia/proteccion

UNICEF busca empoderar a jóvenes para evitar el acoso y prevenir los riesgos en línea. [en línea]. 2020-02-10. [citado el 2022-04-04]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/unicef-busca-empoderar-a-jovenes-para-evitar-el-acoso-y-prevenir-los-riesgos-en-linea

PANORAMA ESTADÍSTICO DE LA VIOLENCIA CONTRA NIÑAS, NIÑOS Y ADOLESCENTES EN MÉXICO. [en línea]. 1ª edición, 2019. [citado el 2022-09-14]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiF8fvP_pT6AhWVtYQIHbarA9EQFnoECBAQAQ&url=https%3A%2F%2Fwww.unicef.org%2Fmexico%2Fmedia%2F1731%2Ffile%2FUNICEF%2520PanoramaEstadistico.pdf&usg=AOvVaw3T1KxN96VQcWxHR08i6qoh

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Directrices sobre la protección de la infancia en línea para la industria 2020. [en línea]. 2020-01-01. pp 41-48 [citado el 2021-03-28]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.IND-2020-PDF-S.pdf ISBN: 978-92-61-30413-3

WEPROTECT. Puntos de datos clave. [en línea]. [citado el 2021-03-28]. Disponible en: https://www.weprotect.org/

WIENER, Gabriela. La atracción sexual hacia los globos y otras parafilias del mundo moderno. [en línea]. 2016-06-11. [citado el 2022-03-21]. Disponible en: https://elpais.com/elpais/2016/07/10/tentaciones/1468144394_715728.html

YOUTUBE.

YouTube for Kids. [en línea]. [citado el 2021-05-09]. Disponible en: https://www.youtube.com/kids/

Políticas sobre imágenes de desnudos y contenido sexual. [en línea]. [citado el 2022-03-17]. Disponible en: https://support.google.com/youtube/answer/2802002?hl=es-419#zippy=%2Cotros-tipos-de-contenido-que-infringen-esta-pol%C3%ADtica