UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE CIENCIAS SOCIALES Y DERECHO

CARRERA DE DERECHO

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO (A) DE LA REPÚBLICA DEL ECUADOR

TITULO:

NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES: ESTUDIO SOBRE LOS SISTEMAS DE PROTECCIÓN Y PREVENCIÓN JUDICIAL.

TUTOR:

ABG. César Humberto Moreira de la Paz. MGS

AUTORES:

Cueva Jaigua Susan Yuliet

Tapia Arámbulo Franklin Eladio

Guayaquil

2022

REPOSITARIO NACIONAL EN CIENCIA Y TECNOLOGÍA	
FICHA DE REGISTRO DE TESIS	
TÍTULO Y SUBTÍTULO: Niños, niñas y adolescentes en las redes sociales: Estudio sobre los sistemas de protección y prevención judicial	
AUTOR/ES: Susan Yuliet Cueva Jaigua Franklin Eladio Tapia Arámbulo	**REVISORES O TUTORES:** Abg. César Humberto Moreira de la Paz. MSC
INSTITUCIÓN: **Universidad Laica Vicente Rocafuerte de Guayaquil**	**Grado obtenido:** Abogado de los Juzgados y Tribunales de la República del Ecuador.
FACULTAD: Ciencias Sociales y derecho	**CARRERA:** DERECHO
FECHA DE PUBLICACIÓN: 2022	**N. DE PAGS:** 90
ÁREAS TEMÁTICAS: DERECHO	
PALABRAS CLAVE: Ciberdelitos, niños niñas y adolescentes, normativa, legalidad.	
RESUMEN: Los delitos cibernéticos han implementado nuevas tendencias para su cometimiento dado a la migración que hemos tenido al internet a causa de la pandemia es aquí donde los	

menores pasan un mayor tiempo navegando en sus plataforma para, interactuar con la sociedad sin existir ninguna medida de protección para precautelar su integridad física, psicológica y sexual, quedando libremente expuestos y vulnerables para estas personas inescrupulosas dedicadas a estos crímenes electrónicos como lo son el sexting, child grooming, chantaje sexual, pornografía infantil, ciberacoso, phishing, siendo absolutamente virtuales, llegando a causar daños irreparables en los menores y el daño volviéndose cada vez más grande por la poca atención que el estado ecuatoriano les ha dado estas conductas y delitos.

Las personas que se dedican a cometer estos tipos de delitos tienen habilidades en el manejo de sistema informáticos que le facilitan el acceso a informaciones proporcionadas por los niños, niñas y adolescentes al ingresar a diferentes plataformas sin un conocimiento básico sobre el peligro y las consecuencias que acarrearía el desconocimiento del peligro que contiene el internet, dado estos antecedentes y acontecimientos se realizó una investigación mediante encuestas a abogados y profesores, de los cuales obtuvimos resultados para que se implementen medidas de prevención en las unidades educativas para un manejo seguro de las plataformas digitales y un mayor control por parte del estado para proteger a este sector vulnerable de los delitos cibernéticos, con la intención de que se garantice y se respete los derechos de los niños, niñas y adolescentes.

N. DE REGISTRO	**N. DE CLASIFICACIÓN:**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF:	**SI** [X]	**NO** [ ]
CONTACTO CON AUTOR/ES: Susan Yuliet Cueva Jaigua Franklin Eladio Tapia Arámbulo	**Teléfono:** 0959455155 0969244767	**E-mail:** scuevaj@ulvr.edu.ec ftapiaa@ulvr.edu.ec
CONTACTO EN LA	Master Diana Almeida Aguilera	

INSTITUCIÓN:	Decana de la Facultad de Ciencias Sociales y Derecho **Teléfono:** 2596500 **Ext.** 249 **E-mail:** dalmeidaa@ulvr.edu.ec Master Carlos Pérez Leyva Director de la Carrera de Derecho **Teléfono:** 2596500 **Ext.** 249 **E-mail:** cperezl@ulvr.edu.ec

CERTIFICADO DE ORIGINALIDAD ACADÉMICA

Cueva y Tapia tesis final

INFORME DE ORIGINALIDAD

5%	4%	2%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

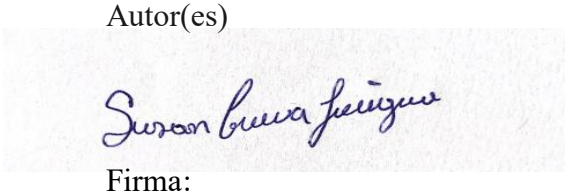
1	Submitted to Universidad Alas Peruanas Trabajo del estudiante	<1%
2	eresmama.com Fuente de Internet	<1%
3	www.metroecuador.com.ec Fuente de Internet	<1%
4	www.venezuelanattorneys.com Fuente de Internet	<1%
5	María de Lourdes Larrea, Christian Paula, Milena Almeida, Paulina Palacios, Daniela Acosta, María José, Jeimy López. "Marco normativo", FapUNIFESP (SciELO), 2020 Publicación	<1%

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

El (Los) estudiante(s) egresado(s) **SUSAN YULIET CUEVA JAIGUA y FRANKLIN ELADIO TAPIA ARÁMBULO** declara (mos) bajo juramento, que la autoría del presente proyecto de investigación, **NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES: ESTUDIO SOBRE LOS SISTEMAS DE PROTECCIÓN Y PREVENCIÓN JUDICIAL**, corresponde totalmente a el(los) suscrito(s) y me (nos) responsabilizo (amos) con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedo (emos) los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

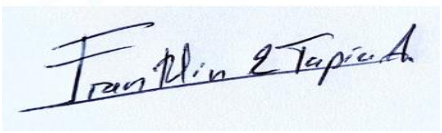
Autor(es)



Firma:

SUSAN YULIET CUEVA JAIGUA

C.I. 0706779295



Firma:

FRANKLIN ELADIO TAPIA ARAMBULO

C.I. 0942093212

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del Proyecto de Investigación **NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES: ESTUDIO SOBRE LOS SISTEMAS DE PROTECCIÓN Y PREVENCIÓN JUDICIAL** designado(a) por el Consejo Directivo de la Facultad de derecho de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Proyecto de Investigación titulado: **NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES: ESTUDIO SOBRE LOS SISTEMAS DE PROTECCIÓN Y PREVENCIÓN JUDICIAL**, presentado por los estudiantes **SUSAN YULIET CUEVA JAIGUA Y FRANKLIN ELADIO TAPIA ARAMBULO** como requisito previo, para optar al Título de ABOGADO (A) DE LA REPÚBLICA DEL ECUADOR, encontrándose apto para su sustentación.

Firma:

ABG, CÉSAR HUMBERTO MOREIRA de la PAZ MSG.

C.C. 0907857239

AGRADECIMIENTO

Mis agradecimientos a mis guías y tutores de tesis, por brindarnos su ayuda y conocimiento en la culminación del mismo, a todos los docentes de la Universidad Laica Vicente Rocafuerte de Guayaquil que han servido de orientación para encaminarme por el mundo de la abogacía y compartir sus conocimientos y a todas las personas que con una palabra de apoyo nunca me dejaron caer en este gran pero no imposible camino.

Susan Yuliet Cueva Jaigua

Agradezco a la universidad Laica Vicente Rocafuerte por haberme dado la oportunidad de ser parte de ella, a sus docentes que con sus conocimientos y profesionalismo me han formado y forjado como hombre del Derecho, a mis padres y hermana que por ellos pude concluir mi carrera y a mis compañeros de clase quienes junto a mi caminaron estos 9 semestres brindándonos inspiración, apoyo y fortaleza.

Franklin Eladio Tapia Arámbulo

DEDICATORIA

Dedico de manera muy especial esta Tesis a mis padres y hermana quienes me han apoyado en este arduo camino y soporte en todos los ámbitos de mi vida, sirviéndome de ayuda y nunca dejarme sola en ninguna etapa académica, a mi sobrino Elian Chalen que espero me vea como ejemplo a seguir y hacerlo sentir orgulloso siempre y por último a mi perrita Franchesca que siempre estuvo a mi lado cada que me sentaba a redactar, por su compañía y fidelidad.

Susan Yuliet Cueva Jaigua

Dedico esta tesis a mis padres y hermana, quienes por su amor, sacrificio y trabajo en estos 5 años he logrado convertirme en lo que soy ahora, gracias por su apoyo moral que me mantuvo con firmeza, por eso dedico y doy este logro a ustedes en ofrenda a todo el apoyo y motivación de seguir mis anhelos, para amigos, profesores y abogados que sin esperar nada a cambio, confiaron y compartieron sus conocimientos que han formado en mi bases de gran importancia para seguir creciendo como profesional del Derecho.

Franklin Eladio Tapia Arámbulo

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Los delitos cibernéticos han tenido un avance y nuevas tendencias en los últimos años debido al aumento de usuarios en el internet debido a la pandemia, siendo así que la utilización de la tecnología es imprescindible para los niños, niñas y adolescentes en su educación, comunicación e interacción con la sociedad llevándolos a ser un grupo muy vulnerable en el internet, dando como resultado el poco control que tiene el Estado a estas nuevas conductas y delitos.

Las nuevas conductas y delitos informáticos sexting, child grooming, chantaje sexual, pornografía infantil, ciberacoso, phishing, tienen una nula regulación y control por parte del Estado y legislación ecuatoriana, haciendo que vayan en aumento, siendo necesario que las autoridades ecuatorianas protejan a los niños, niñas y adolescentes, dado estos antecedentes el problemas de investigación lleva relación con las conductas y delitos informáticos que violentan la integridad psicológica, física y sexual de los menores de edad como lo son los niños, niñas y adolescentes dentro de la normativa legal ecuatoriana.

Para una mejor comprensión del desarrollo del presente trabajo investigativo, éste ha sido dividido en los siguientes capítulos:

CAPÍTULO I EL PROBLEMA, se detalla la problemática del tema a investigar y los antecedentes básicos e información clave para el trabajo de tesis, desde una perspectiva general y específica, delimitando el fenómeno de estudio y el objeto del problema dentro del área de estudio, identificando de manera clara y precisa el alcance de la investigación, delimitando el trabajo al aspecto temporal, sobre el contenido y relacionado a la población de estudio.

CAPÍTULO II MARCO TEÓRICO, donde se expone el desarrollo del trabajo investigado, tomando en consideración lo que respecto establecen nuestra legislación tomando como base la Constitución de la República del Ecuador, Código Orgánico de la Niñez y Adolescencia, Código Orgánico Integral Penal, revistas científicas, doctrina de tratadistas relacionados al temas de la presente investigación, legislación internacional y derecho comparado, usando fuentes investigativas y bibliográficas, las cuales sustentarán lo expuesto y brindarán soporte al desarrollo del proyecto de Tesis.

CAPÍTULO III METODOLOGÍA, dentro de este capítulo se presentarán los tipos de metodología empleados, enfoques e instrumentos utilizados para la recolección de información

mediante un enfoque cualitativo como lo son las entrevistas que fueron realizadas a diferentes profesionales, quienes aportarán información necesaria mediante sus opiniones para el desarrollo y análisis presente trabajo investigativo.

CONCLUSIONES Y RECOMENDACIONES, que servirá para determinar el punto clave del problema planteado dentro de lo expuesto en capítulos anteriores, en base a las referencias bibliografías, recolección de datos y trabajo de campo, donde se podrá validar la idea a defender, así mismo determinar si los objetivos planteados con anterioridad fueron debidamente cumplidos y aportar ideas y recomendaciones sobre las posibles soluciones al objeto del problema de estudio.

CAPÍTULO I

DISEÑO DE LA INVESTIGACIÓN

1.1.Tema

"NIÑOS, NIÑAS Y ADOLESCENTES EN LAS REDES SOCIALES: ESTUDIO SOBRE LOS SISTEMAS DE PROTECCIÓN Y PREVENCIÓN JUDICIAL"

1.2.Planteamiento del problema

El internet es un medio de comunicación que tuvo sus inicios en el año 1969 siendo en la actualidad muy utilizado en todas las edades, pero su uso se denota más en jóvenes, en él se pueden realizar consultas y adquirir información relevante para un tema de estudio, teniendo grandes ventajas, pero así también se presentan inconvenientes que pueden llegar a ser perjudiciales para el individuo que le dé un mal uso, ya que cualquier persona que posea un dispositivo como computadoras, Tabletas, celulares, entre otros tiene acceso directo y así distorsionar la información a través de perfil falsos.

Conforme el mundo ha ido avanzando, la tecnología ha abarcado grandes campos en la cotidianeidad de las personas en especial de los jóvenes, quienes buscan mantenerse en contacto con la vida tecnológica implementando nuevos métodos de comunicación mediante redes sociales para adquirir conocimientos de ciertos temas de interés o tener un acceso fácil a fotografías o videos dentro de la red que pueden afectar al interés o bienestar de los niños, niñas y adolescentes, por lo que, debido a este crecimiento poblacional informático, la normativa jurídica ecuatoriana se ha visto inmersa en modificaciones para acoplarse a la realidad tecnológica y las problemáticas que ésta conlleva, según estudios de la Unidad Especial de Delitos Cibernéticos, las cifras de ciberataques han ido en ascenso dentro de nuestro país alarmando a los representantes de los niños, niñas y adolescentes.

Dentro de las normas reguladoras de delitos tenemos al CÓDIGO ORGÁNICO INTEGRAL PENAL, en el cual se pueden encontrar delitos tipificados en relación con los medios electrónicos de los cuales las víctimas son niños, niñas y adolescentes y como norma preventiva

tenemos el CÓDIGO ORGÁNICO DE LA NIÑEZ Y ADOLESCENCIA, sin embargo dentro de ésta normativa, no se prevee ésta problemática relacionada al uso de las redes sociales y los delitos que se pueden incorporar a la tecnología, como consecuencia de esto, el problema a analizar dentro del presente trabajo de investigación, es el vacío legal al momento de referirse a delitos cibernéticos y cómo estos afectan a niños, niñas y adolescentes dentro de las redes sociales.

1.3. Formulación del Problema

¿De qué manera los ciberdelitos lesionan y vulneran los derechos de los niños, niñas y adolescentes?

1.4.Objetivo General

Analizar de qué forma los ciberdelitos lesionan y vulneran los derechos de los niños, niñas y adolescentes.

1.5. Objetivos Específicos

- Identificar las acciones que deberían ser considerados delitos cibernéticos dentro de la normativa jurídica ecuatoriana.
- Analizar si el mal uso y el poco control que existen en las redes sociales, atenta contra la integridad física y psicológica de los niños, niñas y adolescentes.
- Detallar las maneras en la que pueden ser prevenidos los casos de delitos cibernéticos que afectan a niños, niñas y adolescentes.

1.6.Idea a defender

¿De qué forma los ataques cibernéticos contra los niños, niñas y adolescentes dentro de las redes sociales, conllevan a develar la existencia de la poca seguridad jurídica en la normativa ecuatoriana?

1.7.Línea de investigación institucional/ faculta

Línea 2. Sociedad Civil, Derechos Humanos y Gestión de la Comunicación.

Cohesión Social y fortalecimiento de la institucionalidad democrática.

Derecho Procesal con aplicabilidad al género, la identidad cultural y Derechos Humanos.

CAPÍTULO II

MARCO TEÓRICO

2.1. Tema:

DELITOS CIBERNÉTICOS CONTRA NIÑOS, NIÑAS Y ADOLESCENTES Y SU VACÍO EN LA NORMATIVA ECUATORIANA

2.1.1. Antecedentes

Según Ron (2014) el internet surge como una necesidad cuando se llevaba a cabo la guerra fría en 1962; Estados Unidos quería llevar la delantera en cuestión de información y para la época de los 60 se desarrolló el "PROTOCOLO DE CONTROL DE TRANSMISIÓN/Protocolo internet (TCP/IP)" por parte de la Agencia de Investigación Avanzados (ARPA) de ese país. El objetivo de este sistema operativo era precautelar los lugares aislados de zonas de ataques militares y nucleares mediante el sistema comunicacional establecido por el departamento de defensa.

Este Protocolo de Control de Transmisión denominado TCP/IP según lo establecido por el autor tiene como finalidad mantener estable la comunicación que se emite por dos ejes al momento en enviar y receptar la información, es decir, la misma que se expresa pasa a través de la red por varios ordenadores o computadoras repitiendo la fuente enviada hasta lograr llegar al objetivo establecido de usuario a usuario, uniendo así la fuente reordenando y validando una información original.

Andalia (2004) en 1975 Estados Unidos ya contaba con 4 universidades que se mantenían interconectadas por TCP/IP, usando la denominación "ARPANET" para referirse a las cadenas interconectadas que surgieron en la época, siendo aún su objetivo el de precautelar la seguridad de los pueblos, mediante informaciones frecuentes sobre los acontecimientos de la guerra, solo contaban con una red centralizada inestable ya que el sistema que se mantenía podía ser bloqueado de manera rápida.

Otra red que abarca de manera íntegra la incorporación del internet en diferentes ordenadores a nivel mundial es "Usenet" que se da desde el año 1979, dando viabilidad en noticias

que recorren el mundo. Así también la "World Wide Web" (WWW) el avance de esta red radica en el proyecto de códigos elaborados para permitir a los usuarios que gocen de su servicio correlacionándose con ordenadores y fusionándose al sistema de telecomunicaciones (Yirda, 2021).

En el año de 1983, la expansión del internet tuvo como objetivo conectar todas las unidades militares usando a "ARPANET" para incluirlas de manera general, marcando así una etapa crucial para este medio, ya que allí la red se empieza a expandir y pasar su fase de experimental a una red más producente y de uso útil y eficiente, consolidando a Ethernet como una red local en desarrollo; dentro de ese mismo año la tecnología tomó auge dentro de la sociedad ya que en el ámbito laboral, los trabajos en escritorio y las redes locales se expandieron.

La compañía "Merit Network Inc." en el año de 1987 logró celebrar un contrato en el cual se conseguía expandir la red la cual operaba en Michigan, colaborando con IBM y MCI, mejorando así la velocidad dentro de su sistema y las líneas telefónicas para los usuarios portadores.

2.1.2. El uso de herramientas tecnológicas como el internet

Para Cuadra (1996) "Internet es una gran red internacional de ordenadores, la cual permite como todas las redes compartir recursos, es decir mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener información sobre un tema que nos interesa" (pág. 1). Es decir, el término internet se limita a una gran red global conjunta, integrada por redes que a su vez son manejadas y codificadas mediante ordenadores que tienen el objetivo de establecer una comunicación no sólo informática por medio de los usuarios que la utilizan, definiéndolo, así como un conjunto de redes que están interconectadas entre sí, pero con la característica que, pese a estar unidas su función no se adapta para un solo ordenador, puede estar conectada a varios ordenadores.

Para Rubio (2009) el uso o empleo de la herramienta del internet tiene un fin específico, tiene como objetivo ser fuente de información, también es utilizado como mecanismo de distracción o entretenimiento, así como también como medio de comunicación, teniendo así la

facilidad de interactuar con diferentes personas alrededor del mundo, abriendo paso a peligros que se puedan presentar por este medio tecnológico.

Desde su creación, el internet ha evolucionado considerablemente, actualmente gracias a esta herramienta tecnológica se puede cargar y verificar información de distintos lugares y diferentes épocas, pese a que hace unas cuantas décadas era un repositorio de almacenamiento de bases de datos, el alcance que se le da hoy en día es mundial, considerando sus beneficios para cualquier usuario, teniendo en cuenta las grandes amenazas que se presentan al ser una red que abarca a usuarios del mundo entero.

La mayoría de la población mundial tiene acceso libre a Internet y se estima que, en un corto plazo, se incrementará el número de usuarios, porque se están creando planes de internet y equipos móviles como celulares inteligentes cada vez más asequibles y de fácil uso.

2.1.3. El uso del internet como herramienta de comunicación

Según Montserrat et al. (2007) la información y el conocimiento han cambiado conforme el mundo ha ido evolucionando, generando así estabilidad y progreso para las diferentes sociedades y culturas, así como, el avance tecnológico ha mejorado aspectos fundamentales en el diario vivir, sin embargo cabe mencionar que también ha provocado un uso distorsionado por parte de personas inescrupulosas para captar la atención de personas vulnerables como son los niños, niñas y adolescentes.

El internet se usa para navegar por diferentes sitios web porque da la oportunidad de desarrollar al ser humano, permitiéndole realizar actividades en las cuales no solo puede investigar sobre un tema de interés, si no también comunicarse, porque al acceder a los diferentes sitios buscando información o entretenimiento es muy factible hacer uso del mismo.

Comunicación. - el internet es muy utilizado para comunicarse, porque es más ágil tener noción de la sociedad y lo que pasa en ella sin acudir al lugar de los hechos, proporcionando información rápida y segura, empleando así la comunicación en distintas actividades ya sean investigativas, pedagógicas o interpersonales por medio de redes sociales, correos electrónicos o

cualquier medio de comunicación que se dé por la red.

Interacción. - los usuarios que hagan uso de los sitios web pueden desarrollar habilidades creativas, compartir documentación o relacionarse con otros usuarios manteniendo juegos en línea, participando así en diferentes grupos sociales, no solo se pueden dar esas actividades que estimulen la creatividad del individuo si no también incursionar en sus negocios o economía.

Información. – Se emplea como método de búsqueda o difusión de información dentro de los usuarios que utilicen las diferentes plataformas que ofrecen el internet en conjunto con las páginas web y redes sociales, proporcionado así la facilidad de indagar sobre diferentes temas proporcionando así un alto conocimiento dentro de las personas que hagan uso de su sistema.

Educación. - El acceso a Internet puede mejorar la calidad de la educación de muchas maneras, abre la puerta a una gran cantidad de información, conocimientos y recursos educativos, lo que aumenta las oportunidades de aprendizaje dentro y fuera del aula. Los docentes pueden usar materiales en línea para preparar sus clases y los estudiantes los usan para ampliar su aprendizaje. Igualmente, los métodos de enseñanza interactivos respaldados por Internet permiten a los maestros prestar más atención a las necesidades individuales de los alumnos y apoyar el aprendizaje colaborativo, lo cual puede ayudar a favorecer la inclusión en la educación; por otra parte, el acceso a Internet ayuda a los administradores educativos a reducir costos y mejorar la calidad de escuelas y universidades.

2.1.4. Amenazas o riesgos de la mala utilización de las herramientas digitales o informáticas como el internet.

El sistema de internet nos permite aprender de diversas formas y nos enseña un mundo diferente de conectividad que nos da el libre acceso a información que aporta en aprendizaje y conocimientos, el aspecto negativo se forma en los límites que esta plataforma proporciona, en relación a niños, niñas y adolescentes, los cuales son grupos que pueden ser vulnerables en relación a tecnología y redes sociales.

Según Díaz y López (2015) resulta fundamental, hoy por hoy, estar suficientemente persuadidos acerca de los posibles efectos negativos y de las transformaciones que a nivel de las

relaciones en general, pueden forjarse por causa del uso intensivo de las tecnologías de comunicación como el Smartphone, Internet o las redes sociales digitales, sobre todo desde una perspectiva psicosocial.

Además del evidente redimensionamiento de las fronteras físicas y de la superación hasta de brechas geográficas o de barreras idiomáticas, las nuevas tecnologías han creado una cierta cultura de la inmediatez. Las personas ya no quieren aguardar la respuesta a un SMS o a un email, todo lo quieren saber al instante, dado que pueden encontrarlo todo en todas partes y todo el tiempo y en casi todas las circunstancias. A veces esto puede incluso provocar ansiedad y posibles trastornos depresivos entre los grandes usuarios o adictos a estas tecnologías.

Al ser usuarios menores de edad, estos no tienen el conocimiento suficiente para discernir entre situaciones que generen peligro o simplemente la ingenuidad los vuelve blanco fácil para sujetos o personas inescrupulosas que se sirven de esta herramienta tecnológica para manipular a los niños, niñas y adolescentes mediante la utilización de las redes sociales y así pueden atentar contra la integridad física y psicológica de las víctimas. Es recomendable que los padres o un adulto responsable esté siempre pendiente de las actividades que se realizan dentro de los ordenadores ya que pueden ser propensos a diferentes ciberdelitos.

Entre los peligros más frecuentes tenemos:

Delitos cibernéticos. – dentro del objeto de estudio de este trabajo investigativo se detallaron los diferentes tipos de ciberdelitos, que son los que atentan contra la integridad física y psicológica de los usuarios, en especial de niños, niñas y adolescentes.

Adicción al uso de redes sociales. - por estimaciones a nivel global, es bien sabido que los usuarios menores de edad, sobre todo adolescentes, pasan una importante proporción de horas al día en las redes sociales, en comparación con el tiempo que invierten los jóvenes un tanto mayores y los adultos en general. Ello deviene del auge de los teléfonos inteligentes y de otros dispositivos que ofrecen accesibilidad permanente a las redes sociales.

Publicación de datos privados. – Los delitos de clonación y publicación de datos cuando

no se tiene la seguridad idónea dentro de cuentas web o información personal, puede ser uso para diferentes delitos informáticos.

2.1.5. Las redes sociales

Para Requena (2011) dar un concepto claro sobre redes sociales, requiere del análisis desde una perspectiva analítica, en el cual se debe de describir a los diferentes puntos de conexión dentro de la red, las cuales se relacionan o la intensidad e interacción de los diferentes usuarios.

Las redes sociales, son instrumentos que permiten crear, construir y nutrir comunidades virtuales y relaciones interactivas entre individuos y grupos; permiten a las personas de ideas afines estar en contacto entre sí mediante sitios web y aplicaciones basadas en la web; puede decirse que más allá de esta generalidad, la definición es todavía muy vaga, puesto que es una tecnología relativamente nueva que está sujeta a cambios acelerados.

Conocemos a las redes sociales como la evolución de las tradicionales formas de comunicación que tiene el ser humano, la cuales han avanzado con el uso de nuevos canales y herramientas donde involucran a un conjunto de personas en este caso los niños, niñas y adolescentes que se identifican con las mismas necesidades o problemáticas, donde principalmente se da el intercambio permanente de informaciones entre los usuarios, las cuales se van formando como estructuras en internet desarrolladas por personas u organizaciones con el fin de conectarse a partir de diferentes intereses en común. En el mundo virtual las redes sociales son conocidas como sitios o aplicaciones que operan en diferentes niveles como podría ser el profesional, social, educativo, entre otros, debiendo mantener el intercambio de información entre personas.

Indudablemente que al hablar de redes sociales asociamos el término con sitios en la web como Twitter, Facebook, Instagram y con tantas aplicaciones que existen en la actualidad. Pero como concepto, se trata de algo de mucho mayor antigüedad. A nivel sociológico, por ejemplo, el concepto se puede vincular con otras formas de interacción a nivel individual o grupal con organizaciones existentes desde finales del siglo XIX.

En la actualidad, las redes sociales han llegado a propiciar una diversidad de discusiones relacionadas con la privacidad de las personas, aunque al mismo tiempo han funcionado como un medio de convocatoria para distintas manifestaciones contestatarias a nivel social. Puede decirse que, en última instancia, se trata de plataformas que han instaurado nuevas relaciones personales, grupales y organizaciones, generando una apertura para distintos tipos de interacciones y también para la promoción de productos y servicios de una naturaleza muy variada.

2.1.5.1. Facebook

El origen de esta red social se remonta al año 2004, teniendo un proceso de despliegue que abarca aproximadamente desde ese año, hasta el año 2013, incorporando paulatinamente distintas innovaciones. Y esos cambios realizados durante la existencia de esta red social han sido tan grandes como rápidos, de hecho, Facebook era tan aburrido cuando se fundó que probablemente no habría tenido el éxito que hoy tiene en la actualidad. En los primeros días de febrero de aquel año inicial del 2004 se abrió thefacebook.com, para estudiantes de la Universidad de Harvard en Cambridge, Massachusetts. El objetivo consistía en crear una página con informaciones básicamente personales para mantener contactos estudiantiles. Los únicos requisitos exigidos para ese entonces eran tener una dirección de correo electrónico que terminara en harvard.edu y tener más de 18 años, además, había la posibilidad de agregar amigos, compartir mensajes, fotografías y unirse a grupos.

El servicio brindado por Facebook originalmente fue creado por Mark Zuckerberg, un joven estudiante de la Universidad de Harvard de apenas 19 años, quien lo ejecutó desde una computadora en su salón de la universidad. A él se unieron cuatro compañeros de estudios, y la forma en que los fundadores se presentaban evidencia claramente que este servicio web fue creado por y para jóvenes estudiantes. De modo que esta red social surgió originalmente como una red de amigos que se relacionaban socialmente entre sí. Pero aproximadamente seis meses después del lanzamiento, las opciones para compartir se ampliaron con la introducción del llamado muro es decir en cada página de perfil, donde los usuarios podían publicar mensajes para sus amigos y escribir en dichos muros.

Los usuarios de Facebook inicialmente podían compartir mensajes entre ellos y más tarde fue posible compartir fotos, concretamente desde octubre de 2005, sin embargo, al compartir, tenían que ir a las páginas de perfil de sus amigos para ver si habían hecho actualizaciones, por ejemplo, si habían escrito nuevos mensajes en su muro o subido nuevas fotos a su sitio. Por lo tanto, las actualizaciones no eran visibles para la red de cada usuario, a menos que visitaran su página de perfil, sin embargo, era posible ponerse en contacto con uno de sus amigos, pinchando o enviando un mensaje y desde finales del 2005 ya era posible etiquetar a una persona en una foto.

Todas las redes sociales que no son aptas para menores tienen una edad mínima de acceso, pero dicha edad a la que los niños obtienen un teléfono móvil oscila entre los 10 y los 12 años. En muchos casos, es un teléfono inteligente, si los padres no configuran el control parental o instalan una aplicación de control dentro de los dispositivos de los menores que puedan bloquear ciertos accesos en el teléfono, les permitirá acceder fácilmente a Internet en cualquier momento. Si se usa correctamente y comprende los peligros y riesgos que pueden traer, el uso de las redes sociales no es necesariamente una actividad negativa. Sin embargo, no todos los niños y jóvenes son conscientes de estas amenazas, a veces porque son jóvenes y otras porque crecieron en un entorno donde las redes sociales siempre han existido, y creen saber todo lo que necesitan (Ramírez, 2021).

2.1.5.2. Instagram

Instagram es una de las aplicaciones más descargadas en la actualidad, también es una de las más prolíficas, con personas de todo el mundo que comparten fotos casi cada segundo del día. La aplicación fue creada en San Francisco en el año 2010 por Kevin Systrom, un programador de computadoras y empresario estadounidense y por Mike Krieger, un ingeniero de software y empresario brasileño.

Para el año 2013 Instagram ya contaba con más de 150 millones de usuarios y comenzó la tendencia de permitir que las fotos se insertarán en los diferentes sitios web. A fines de ese mismo año, también se puso a disposición de los usuarios el servicio de mensajería privada denominado Instagram Direct, lo cierto es que la historia de Instagram apenas comienza ya que seguramente no es sólo una moda pasajera sino una aplicación para la historia, actualmente, una de las funciones más populares de la aplicación son las llamadas historias de Instagram. Con esta característica, los

usuarios pueden publicar fotos y videos en una fuente separada de contenido dentro de la aplicación. Según Instagram, 500 millones de personas usaron Instagram Stories todos los días en 2020.

Moreira (2019) manifiesta que, para los jóvenes, subir fotos y compartir datos personales no es algo malo, sin embargo, no todo el mundo tiene buenas intenciones, y esta inocencia a menudo se utiliza con fines indebidos, como engaño, acoso o ser vulnerables a diferentes delitos sexuales. Esta red social es tan popular, no sólo atractiva, sino también muy influyente en la vida diaria de niños y jóvenes, es fácil para ellos tomarlo demasiado en serio y comprometerse a publicar contenido para ganar reconocimiento social y, por supuesto, gratificación instantánea.

Desde el punto de vista de la interactividad social propiamente dicha, Instagram pone a disposición de sus usuarios una amplia variedad de herramientas. En este sentido, Galvao (2017) señala que se trata de una red social definitivamente abocada hacia un atractivo comunicacional de tipo visual, de rápido accionar, con posibilidades de generar una constante y fluida narratividad de imágenes.

2.1.5.3. TikTok

Fernández (2021) define a TikTok como "una aplicación que permite crear, editar y subir videoselfies musicales de un minuto, pudiendo aplicarles varios efectos y añadirles un fondo musical. También tiene algunas funciones de Inteligencia Artificial, e incluye llamativos efectos especiales, filtros, y características de realidad aumentada", por ende, la función principal que tiene esta aplicación se centra en crear una comunidad global de videos cortos que permite a los usuarios crear y editar videos de baile, comedia, deportes, animales, dando opciones extras de animaciones y sonidos para la animación del mismo.

Después del gran impacto social que obtuvo Musical.ly en donde la mayoría de sus usuarios eran adolescentes, la empresa de tecnología Bytedance decide cambiar el nombre a TikTok debido a la independencia que tendría la aplicación que se establecen en China y Japón. La aplicación siguió con sus mismas funciones pese al cambio de nombre, actualmente existen nuevas actualizaciones, pero sin perder su esencia.

El peligro que se presenta dentro de esta aplicación es igual que en las otras, todo depende del uso que le den y la supervisión que deben de tener los niños, niñas y adolescentes por parte sus padres o personas responsables que estén encargadas de sus tutelas, para así evitar ciberdelitos que atenten contra la integridad física y psicológica de los niños, niñas y adolescentes. Los usuarios de estas redes sociales por lo general lo que buscan es la validación o verificación de sus cuentas de usuario, se ha comprobado que los videos que suelen ser sexualizados son los que más popularidad tienen entre los internautas, originando así múltiples peligros, por ello es importante que se tenga conocimiento de las configuraciones de privacidad ya que el no hacerlos permite que los menores se expongan a todo público, incluyendo los victimarios quienes se hacen pasar por "seguidores".

La edad mínima para ingresar como usuario de esta red social es de 14 años, pero con facilidad dentro de la misma aplicación se puede modificar la fecha de nacimiento permitiendo el acceso a usuarios de todas las edades, para ellos los padres deben establecer "líneas rojas" que limiten el uso de TikTok según el caso, bajo la supervisión de un adulto responsable, que pueda evitar el mal uso y la afectación de los niños, niñas y adolescentes.

2.1.5.4. Tinder

Tinder es una aplicación móvil de citas lanzada en 2012, los perfiles de Tinder son muy limitados y contienen solo un nombre, edad, intereses y una breve biografía. Los usuarios estipulan su pareja deseada seleccionando el rango de edad y género, así como escribiendo una breve descripción de sí mismos. Cuando un usuario enciende la aplicación, su ubicación se informa al servidor de Tinder, que luego devuelve un conjunto de perfiles que coinciden con los criterios estipulados por el usuario dentro de un rango determinado, luego, al usuario se le presenta una imagen de un usuario cercano, esta pantalla contiene dos botones grandes, etiquetados con una cruz y un corazón permitiendo al usuario estipular si le gusta o no le gusta el perfil.

Si dos usuarios dicen que se gustan, se les notifica a ambos. A partir de ese momento, los dos usuarios pueden interactuar a través de mensajes de texto dentro de la aplicación, este es el límite de la funcionalidad de la aplicación y, como tal, constituye una versión extremadamente reducida de una experiencia de citas en línea. De hecho, no existe un medio formal para informar

lo que un usuario desea de una coincidencia y, por lo tanto, Tinder puede incluso usarse simplemente para conocer nuevos amigos.

A pesar de la creciente popularidad de Tinder y su estilo de emparejamiento poco convencional, ha recibido una atención limitada ya que hay estudios sobre la privacidad de las aplicaciones móviles de citas, principalmente relacionados con la capacidad de los atacantes para rastrear la ubicación de usuarios. Esto quizás se vea intensificado por el uso frecuente de aplicaciones de citas basadas en la ubicación para encuentros sexuales inmediatos. Más allá de esto, muy poco se conoce sobre la naturaleza y el uso de esta aplicación de manera exhaustiva.

Tinder ofrece un potencial interesante, ya que puede proporcionar datos sobre las primeras impresiones sobre el atractivo físico, este último componente está fuertemente suprimido, favoreciendo las primeras impresiones basadas en imágenes. Desde luego que hay personas que usan una variedad de estrategias para reducir la incertidumbre cuando interactúan con gente nueva. La divulgación de información es una parte importante de esto, ya que se ha descubierto que el engaño es un lugar común, este tema es particularmente importante en Tinder, ya que la divulgación inicial de información es muy limitada, sobre todo debido a la simplicidad de los perfiles.

2.1.6. Vulneración en redes sociales

Las redes sociales se han convertido en una parte importante de la vida cotidiana, sirven a un gran número de usuarios, sin embargo, cada usuario comparte contenido solo con un pequeño subconjunto de estos usuarios. Este subconjunto puede incluso cambiar según el tipo de contenido o el contexto actual del usuario, por ejemplo, un usuario puede compartir información de contacto con todos sus conocidos, mientras que una imagen puede compartirse sólo con amigos, si la imagen muestra a la persona enferma, es posible que el usuario ni siquiera quiera que todos sus amigos requieran sistemas para emplear un acuerdo de privacidad personalizable con sus usuarios. Sin embargo, cuando eso sucede, es difícil hacer cumplir los requisitos de privacidad de los usuarios.

Los ejemplos típicos de violaciones de la privacidad en las redes sociales se parecen a las violaciones del control de acceso, en escenarios típicos de control de acceso, hay una sola autoridad que es el administrador del sistema, quien puede otorgar accesos según sea necesario, sin embargo, en las redes sociales existen múltiples fuentes de control, cada usuario puede contribuir compartiendo contenido, publicando sobre sí mismo y sobre los demás. Además, la audiencia de una publicación puede permitir el acceso a otros usuarios, estas interacciones conducen a violaciones de la privacidad, algunas de las cuales son difíciles de detectar por los usuarios y están más allá del control de acceso.

De modo que resulta importante tener claro cuándo se viola realmente la privacidad de un individuo en función de un contenido que se comparte en la red social en línea. Vale decir, el contenido que puede ser compartido por el propio usuario o por otros, de hecho, el contenido puede variar, incluyendo imágenes, mensajes de texto, informaciones de registro o incluso una declaración de información personal, cada vez que se comparte dicho contenido, está destinado a ser visto por ciertas personas, a veces un conjunto de amigos o a veces toda la red social y es importante estar conscientes de que cada vez que este contenido revela información a una audiencia no deseada, se viola la privacidad del usuario.

Por otra parte, también resulta importante señalar que, si se viola la privacidad de un usuario, el sistema toma las medidas adecuadas para evitarlo o, si es inevitable, al menos informa al usuario para que pueda abordar la violación, en las redes sociales en línea actuales, se espera que los usuarios controlen cómo circula su contenido en el sistema y averigüen manualmente si se ha violado su privacidad. Esto, desde luego, resulta la mayoría de las veces poco práctico e incluso puede resultar hasta cierto punto imposible de detectar o de manejar adecuada y oportunamente.

2.1.7. Las redes sociales y su relación con los niños, niñas y adolescentes

En la actualidad, los niños, niñas y adolescentes utilizan ampliamente las redes sociales, en función de entretenimiento, enriquecimiento y crecimiento personal, por lo tanto, los padres están llamados a animar a sus hijos para que hagan un uso sumamente juicioso de las mismas, haciéndolos conscientes de los riesgos potenciales que conlleva al exponer a los usuarios a contenido negativo como la pornografía, la violencia, el comercialismo, el ciberacoso, las

relaciones sociales sin una supervisión adecuada y los problemas de privacidad y seguridad que esto conlleva.

Teniendo en cuenta tanto la capacidad de crecimiento personal como las vulnerabilidades inherentes a los niños, niñas y adolescentes, una de las tareas más importantes para su desarrollo tiene que ver, principalmente, con la formación de redes sociales de apoyo y el mantenimiento de las conexiones sociales ya que ambos aspectos juegan un papel definitivamente muy preponderante en la navegación exitosa de los desafíos de los jóvenes a nivel personal, comunitario y social.

Sádaba (2011) manifiesta, "la relación de los/as menores con las redes sociales ha causado interés desde su inicio, no sólo por el potencial comercial que encierra un medio capaz de atraer la atención y el tiempo de los/as más jóvenes" (pág. 175). Este grupo de edad tienen una afinidad por la tecnología, este evento ha llevado a las instituciones a establecer acciones de protección a favor del menor y así poder conocer las implicaciones que el uso de la misma conlleva; así las diferentes redes sociales tienen como requisito para su uso una edad mínima la cual es de 14 años, es aquí donde los niños, niñas y adolescentes comienzan su incursión en el mundo del internet en el que ocupan una gran parte de su tiempo; pero puede llegar el punto donde estas actividades en el internet dejan de ser una simple actividad de ocio para convertirse en un grave problema para el núcleo familiar.

Los niños, niñas y adolescentes ven la necesidad de sentirse parte de un grupo social en el internet, es por ello que pasan más tiempo conectados en las redes sociales tratando de intentar interactuar con amigos o desconocidos quedando en un punto vulnerable para aprovecharse de su inocencia y falta de conocimiento en este mundo del internet cayendo en manos de ciberdelincuentes.

La navegación en internet y en redes sociales en los niños, niñas y adolescentes se ha incrementado desproporcionadamente en los últimos años, dado al desarrollo de nuevas plataformas educativas y sociales, incluyendo también las nuevas funcionalidades o actualizaciones de las redes ya existentes. Los niños, niñas y adolescentes usan el internet con la

finalidad de socializar con compañeros, amigos, familiares, o seguidores, y visualizar videos y fotografías como entretenimiento o curiosidad, por eso en innumerables ocasiones descuidan valores y principios propios del ser humano tales como: su identidad e intimidad, convirtiéndose en un mundo sin fronteras donde los niños, niñas y adolescentes pueden acceder a cualquier información, como por ejemplo acceder a información no apta para niños, niñas y adolescentes (imágenes, pornografía, violencia, etc.), contactarse con personas con malas intenciones, compartir informaciones privadas como (domicilio, ciudad donde vive, colegio donde estudia, números de tarjetas, etc.), acosos por parte de pedófilos, compartir videos o imágenes exhibiéndose o ser víctimas de amenazas o chantajes, todo esto se debe por la falta de conocimiento de los peligros a los que están expuestos los menores.

2.1.8. Los delitos cibernéticos

Los delitos cibernéticos se definen como aquellos que se cometen en Internet utilizando los dispositivos electrónicos como herramientas y a los usuarios como víctimas específicas, es muy difícil clasificar los delitos en general en grupos distintos, ya que muchos delitos evolucionan a diario. Incluso en el mundo real, los delitos como la violación, el asesinato o el robo no necesariamente tienen que estar separados. Sin embargo, todos los delitos cibernéticos involucran tanto a la computadora como a la persona detrás de ella como víctimas, sólo depende de cuál de los dos es el objetivo principal.

Cuando el individuo es el objetivo principal del delito cibernético, la computadora se convierte en una herramienta y no como el objetivo central, estos delitos generalmente involucran menos experiencia técnica ya que el daño causado se manifiesta en el mundo real, generalmente se explotan las debilidades humanas, el daño infringido es en gran medida psicológico e intangible, lo que dificulta las acciones legales contra el victimario. Estos son los delitos que han existido durante siglos fuera de línea, las estafas, los robos y similares han existido incluso antes del desarrollo de equipos de alta tecnología, al mismo criminal simplemente se le ha dado una herramienta que aumenta su grupo potencial de víctimas y lo hace aún más difícil de rastrear y detener (Urueña, 2015).

A diferencia de los delitos que utilizan la computadora como herramienta, cuando ésta u otro dispositivo son propiamente el objetivo, se requiere obviamente el conocimiento técnico de los perpetradores. Estos delitos son relativamente nuevos, ya que desde que existen la tecnología informática, explica lo poco que está preparada nuestra sociedad y el mundo en general para combatir este tipo de delitos, que se han incrementado en forma vertiginosa.

La lucha contra el ciberdelito necesita un enfoque integral, dado que las medidas técnicas por sí solas no pueden prevenir ningún delito, es fundamental que los organismos encargados de hacer cumplir la ley, puedan investigar y enjuiciar los delitos cibernéticos de manera eficaz. Las medidas legales se centran en cómo abordar los desafíos legislativos que plantean las actividades delictivas cometidas a través de las redes se deben centrar en acciones claves para promover la seguridad y la gestión de riesgos en el ciberespacio, incluidos los esquemas, protocolos y estándares pertinentes para cada delito.

Las estructuras organizativas se centran en la prevención, detección, respuesta y gestión de crisis de ciberataques, incluida la protección de los sistemas de infraestructura de información crítica, asimismo, el desarrollo de capacidades se centra en la elaboración de estrategias para mecanismos de desarrollo de capacidades para crear conciencia, transferir conocimientos e impulsar la ciberseguridad en la agenda política nacional. Por último, la cooperación internacional se centra en la cooperación, el diálogo y la coordinación internacionales para hacer frente a las ciber-amenazas (Subijana, 2008).

A un nivel general, los especialistas consultados distinguen las siguientes características fundamentales dentro de los delitos cibernéticos:

A. Los ciberdelitos, se pueden cometer con facilidad, y requieren de pocos recursos, considerando el perjuicio que pueden causar.
B. Estos delitos se pueden cometer en una jurisdicción sin necesidad de estar físicamente en un territorio.
C. Este delito usufructúa de lagunas de punibilidad, que pueden generarse en las legislaciones de ciertos Estados, denominados paraísos cibernéticos, donde la voluntad política para tipificar y sancionar estos delitos es nula.

2.1.9. Clasificación de los ciberdelitos

Para la Convención de Delitos Cibernéticos del Consejo de Europa de 2001, dentro de las acciones que son de carácter lesivo dentro de los delitos cibernéticos e informáticos los clasifica en cuatro:

1. Delitos que afecten a la privacidad y confidencialidad de un usuario vulnerando y dando un uso lesivo a los datos de las personas afectadas.
2. Delitos de fraude o falsificación.
3. Delitos en cuanto a su forma o contenido, esto corresponde directamente a la distribución de contenido ya sean fotos o videos de los usuarios sin su consentimiento o adquiridos de manera dolosa.
4. Delitos de propiedad intelectual vulnerando así el derecho de autor.

2.1.10. Sujetos de los ciberdelitos

Dentro del área del derecho, el supuesto de ejecución de una conducta de carácter punible, se encuentran inmersos dos sujetos que intervienen de forma directa dentro de la acción de los ciberdelitos: uno que es el sujeto activo, el actor de acto punible y el otro el sujeto pasivo que es la víctima, donde el victimario o autor del delito , se pueden presentar como personas naturales o jurídicas, donde el bien jurídico protegido será la integridad física y psicológica del sujeto pasivo y quien vulnere o lesiones los derechos serán el sujeto activo.

2.1.10.1. Sujeto Activo

El sujeto activo o victimario es aquel que realiza la acción dolosa o participa de ella para lesionar los derechos de los niños, niñas y adolescentes; y en la mayoría de los casos es una persona mayor de edad. Los sujetos activos de los ciberdelitos no presentan características o un factor en común que tienen otros delincuentes dentro de otro tipo de delitos.

Para Olson (2007) la denominación adecuada para los sujetos activos dentro de los delitos cibernéticos es el vocablo inglés “entrapping” dado que el autor manifiesta que los delincuentes cibernéticos tienen como prioridad “atrapar” a las víctimas, que en este caso serían los niños, niñas y adolescentes usando la “communication theory of seduction” o “teoría de la comunicación de la

seducción" en la cual el sujeto activo o victimario mediante la persuasión busca la confianza de sus víctimas con la finalidad de vulnerar su integridad física o sexual.

2.1.10.2. Sujeto Pasivo

El concepto de sujeto pasivo es inherente a la víctima de un delito y según entendidos en la materia, no es requisito que dicho delito haya sido denunciado para que las víctimas sean reconocidas como tales, lo cual es particularmente importante en el caso de las víctimas de delitos cibernéticos. Sin embargo, si bien no es necesario denunciar un delito a la fiscalía para que un sujeto pasivo pueda acceder a los servicios para víctimas, en la práctica, el remitir un caso a la policía es la forma más común de acceder a estos servicios, como tal, no queda del todo claro si los servicios para víctimas se ponen a disposición de aquellos que no intentan denunciar un delito cibernético o que, al intentar hacerlo, son rechazados por no cumplir con los criterios que se supone definen a las víctimas (Carta Judicial Iberoamericana, 2012).

Dada la amplia gama de partes interesadas e involucradas en la respuesta al delito cibernético más allá de la policía y el apoyo a las víctimas, existe la necesidad de un enfoque coordinado de múltiples partes interesadas, se supone que los Estados deben garantizar que existan medidas disponibles para proteger a las víctimas y sus familiares de la victimización secundaria y repetida, de la intimidación y de las represalias, incluso contra el riesgo de daño emocional o psicológico, en función de proteger la dignidad de las víctima, de ahí que se requiera una evaluación de los factores a nivel micro que hacen que las víctimas sean más vulnerables a la victimización, la intimidación o las represalias secundarias y repetidas, a fin de determinar el nivel de apoyo que se debe proporcionar para una protección adecuada.

En el caso de los sujetos pasivos o víctimas que son niños, niñas y adolescentes la vulnerabilidad evidentemente se acrecienta significativamente, puede implicar incluso trastornos mentales, inconvenientes de comunicación o de aprendizaje, de hecho, como testigos para prestar testimonio pueden verse afectados por miedo o angustia o pueden también llegar a ser víctimas de abuso doméstico o sexual, desde luego que esta es una concepción bastante amplia de la vulnerabilidad y, por lo tanto, las víctimas del delito cibernético pueden ser sujetos pasivos de ataques persistentes o como sujetos pasivos muy vulnerables o intimidados, de modo que en las

limitadas circunstancias en las que las víctimas de delitos cibernéticos son reconocidas como vulnerables, la mayoría de los derechos que se adjuntan a este estado se relacionan con los procedimientos judiciales, en el marco legislativo de cada Estado.

2.1.11. Tipos de delitos cibernéticos contra niños niñas y adolescentes

Internet, las redes sociales y en general las tecnologías de la información y la comunicación han creado un espacio totalmente nuevo para que los niños, niñas y adolescentes aprendan y jueguen, su área de oportunidades va también de la mano con los riesgos de ser víctimas del ciberdelito, dados que estos medios permiten a los delincuentes tenerlos como su objetivo de forma individual y conjunta. Los motivos potenciales de los delincuentes incluyen la gratificación personal, generalmente mediante la explotación sexual, la creación de dinero, etc.

Las tipologías de delitos cibernéticos contra niños, niñas y adolescentes son muy variadas y también el grado de vulnerabilidad que representan para esta población, entre los más frecuentes está la pornografía infantil, el acoso cibernético con todos sus alcances, la piratería, el tráfico de niños en línea, la extorsión en línea, el acoso sexual en línea y las diferentes variantes de violaciones de la privacidad, entre otros.

2.1.11.1. Sexting

En la última década, la tecnología ha alterado la forma en que los niños, niñas y adolescentes se comunican e interactúan con sus compañeros, en muchos casos, el uso del llamado sexting es parte de esta forma de comunicación. Sextear a menudo se define vagamente, pero se considera un fenómeno social que generalmente se refiere al envío y/o recepción de imágenes o mensajes sexualmente sugerentes a compañeros a través de un teléfono celular.

Las nuevas formas de comunicación electrónica, dentro de las cuales las redes sociales tienen un papel preponderante, las mismas que han generado preocupación entre los padres, los profesionales de la salud, los educadores y las fuerzas del orden, estas preocupaciones son por los comportamientos dañinos que los jóvenes pueden adoptar a medida que estos tipos de comunicación se vuelven más dominantes. Los comportamientos de riesgo en los que los jóvenes pueden participar en línea pueden incluir comunicarse con posibles depredadores sexuales en línea

o ser solicitados por ellos, participar en acoso cibernético y publicar imágenes sexuales de ellos mismos y de otros.

Para Mejía (2014), el sexting, junto con la experimentación sexual adolescente, la curiosidad y la sexualización de la juventud, ha presentado una nueva forma de conducta de riesgo, lo que resulta en posibles consecuencias legales para los jóvenes que participan en tales actos. Algunas de estas intervenciones legales tienen el potencial de dejar a los jóvenes tildados de delincuentes sexuales. Por lo tanto, las consecuencias del sexting son graves y pueden afectar negativamente a los niños, niñas y adolescentes durante muchos años después de que se haya producido el acto, como la dificultad para obtener un futuro empleo, vivienda, licencias y beneficios económicos para la educación.

En los últimos años, los casos de sexting de alto perfil en los medios han generado una percepción entre el público; está presente en todas partes y en todas sus variantes. Al tiempo que llama la atención sobre las consecuencias legales de participar en este tipo de comportamiento de riesgo. Sin embargo, en muchos países desarrollados y en vías en desarrollo han comenzado a implementar programas alternativos para evitar que los jóvenes estén sujetos a las leyes de pornografía infantil destinadas a depredadores sexuales adultos.

A diferencia de los adultos, los niños, niñas y adolescentes no tienen la misma capacidad para tomar decisiones racionales antes de involucrarse en conductas de riesgo. Entre los especialistas en el tema se considera que, debido a la capacidad limitada de este sector de la población para la autorregulación y la susceptibilidad a la presión de los compañeros, los niños, niñas y los adolescentes corren cierto riesgo a medida que navegan y experimentan con las redes sociales (Pantallas, 2013). Por lo tanto, debido al menos en parte a su inmadurez e impulsividad, pueden llevar al sexting junto con otros comportamientos de riesgo en línea.

La mayoría de las investigaciones revelan que el sexting es predominante entre adolescentes mayores y adultos jóvenes. Los adolescentes mayores tienen más probabilidades de enviar imágenes de mensajes sexuales que los participantes más jóvenes. Las mismas

investigaciones señalan que el sexting ocurre con mayor frecuencia entre adolescentes en una relación romántica y está asociado con otros comportamientos sexuales de riesgo.

2.1.11.2. Chantaje sexual

El chantaje sexual es un tipo específico de abuso sexual que se caracteriza por la explotación sexual por parte de adultos o jóvenes mayores mediante amenazas a niños, niñas o adolescentes a través del internet y redes sociales en general. A pesar del hecho de que cada incidente varía en muchos aspectos entre sí, tales actos se cometen de la siguiente manera en términos simples: Una vez que el abusador obtiene los materiales sexuales del niño, niña o adolescente, el abusador amenaza con abusar de ellos a menos que cumplan con su /sus demandas (Rubio M. , 2018).

La prevalencia del uso de teléfonos celulares también se ha asociado con una mayor probabilidad de enviar y recibir imágenes de sexting. Los hallazgos investigativos al respecto sugieren que los niños, niñas y adolescentes que generalmente envían mensajes de texto con más frecuencia también tienen más probabilidades de enviar y recibir mensajes de sexting, en comparación con los adolescentes que no usan mensajes de texto con regularidad.

Sin embargo, aunque los teléfonos celulares siguen siendo un modo dominante de comunicación, esta forma de tecnología ha expuesto a los jóvenes a daños potenciales que resultan del uso inapropiado de los dispositivos móviles. Las graves ramificaciones que presentan estas acciones justifican la preocupación y los esfuerzos persistentes de prevención a través de la educación en nombre de los jóvenes, padres, educadores y policías.

2.1.11.3. Ciberacoso

Es considerado como una representación de intimidación que se produce mediante dispositivos electrónicos o digitales, como lo son las computadoras, teléfonos celulares, tabletas, etc. Las actividades delictivas de esa modalidad virtual se pueden dar mediante redes sociales, por correo electrónico o por mensajes de texto, se presentan comúnmente en escuelas y colegios en la cual se comparte o publican contenido negativo que afecta a la integridad física o psicológica de aquellos a los que se afecta, compartiendo información privada o personal de manera alterada con

la finalidad de crear humillación a sus víctimas, estas conductas que se reflejan en internet pasan a considerarse ilegales o criminales.

El ciberacoso empezó a utilizarse como un concepto básico en la década del 2000, de esta forma el profesor canadiense Bill Belsey fue una de las primeras personas en establecer y comenzar a implementar dicha definición debido al avance tecnológico que se estaba incrementando en la sociedad. Lo que caracteriza a este tipo de delitos cibernéticos no sólo es el comportamiento o la acción que provoca si no también la forma en cómo se efectúan, así mismo cuenta con dos elementos, el primero se refiere al acoso que es la causa y los medios electrónicos que es la vía por el cual se cometen estos delitos.

De esta manera para García (2011) definen al ciberbullying o ciberacoso dentro de sus estudios como algo particularmente dañino para los niños, niñas y adolescentes experimentar si son objetivos. Y señalan que hay varias razones posibles para esto. Porque, a diferencia del acoso tradicional, que a menudo se limita a la escuela y a los acosadores conocidos, el ciberacoso puede ocurrir en cualquier momento, de día o de noche, y ser perpetrado por fuentes anónimas. Esto lo hace más implacable y, a menudo, más cruel. Incluso el tipo de victimización puede afectar la gravedad de sus consecuencias. Y es así como se establece la finalidad que tiene este fenómeno, el cual se manifiesta de manera abierta dentro de la interacción entre víctimas y victimarios, originando así una situación sumamente peligrosa para quienes son agredidos por este medio, especialmente niños, niñas y adolescentes.

Standler (2002) manifiesta que el ciberacoso se puede definir por las acciones que este provoca, como lo son las amenazas, hostigamiento, humillaciones y cualquier forma de negatividad para con un individuo que es expuesto por otro, mediante tecnologías de comunicación como lo son; el internet, telefonía móvil, videoconsolas online entre otros. El origen del ciberacoso no se puede esclarecer debido a que se produce paulatinamente con el desarrollo de la tecnología de las telecomunicaciones y la implementación de materiales que permitan a los usuarios obtener grandes cantidades de información, lo cual ayuda a promover la capacidad de los acosadores o agresores a no solo conocer sobre el diario vivir o situaciones personales que comparte mediante

redes sociales sino también en cómo las personas ven o creen en la existencia de la convivencia social.

El ciberacoso posee tres características para ser consideradas agresión de este tipo: la primera se refiere a la falsa acusación, la que consiste en manipular a otros con la finalidad de dañar su integridad, las personas que promueven el ciberacoso que en este caso serían los victimarios crean un falso testimonio para desestimar las acciones o personalidades de los afectados con el objetivo de generar una exclusión social logrando así su cometido, creando rumores gracias a la información personal que ha extraído de redes sociales principalmente. Dentro de lo mencionado es importante resaltar que al dañar la imagen de las personas con afirmaciones que se alejan de la realidad, se puede tipificar esta acción como un delito de injuria y calumnia que está regulado por el Código Orgánico Integral Penal en relación al Código de la Niñez y Adolescencia, norma que se encarga de precautelar el bienestar de los niños, niñas y adolescentes.

Lo segundo que lo caracteriza se relaciona a la difusión de la información alterada mediante el uso de redes sociales, lo cual se faculta debido a que mediante esta vía los acosadores logran llegar a los demás usuarios y pueden difundir su contenido gracias a las nuevas tecnologías crean un gran impacto en contra de las víctimas. Y como terceras características sucede cuando esta conducta es repetida en varias ocasiones produciendo así un acoso constante.

2.1.11.4. Phishing

Se deriva de la palabra inglesa "fishing" qué quiere decir pesca en español, refiriéndose metafóricamente a como hacen caer en la red a los usuarios para robar sus datos e información privada. También es conocida como suplantación de identidad y se faculta en un abuso informático que se caracteriza por adquirir de manera ilegal información confidencial de diferentes usuarios mediante el internet y las redes sociales; la modalidad de operar de los phisher (cibercriminales) es la de manifestar al usuario que son conocidos que necesitan de información personal porque tienen algún problema o situación de emergencia.

Para Bolaños, Simone, Becerra, (2005) "[...] consiste en una modalidad de estafa que tiene como objetivo intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de

tarjetas de crédito, identidades, etc. En resumen, extrae todas las referencias posibles para después usarlas con fines fraudulentos" (pág. 20). En su obra científica, los tratadistas nos mencionan que esta clase de ciberdelito tiene como relevancia sus consecuencias y saber a fondo su modo de operar para los usuarios puedan identificar cuando se encuentren en una situación de estafa.

Según lo manifiesta Miranda (2021) son las amenazas más frecuentes para todo aquel que utilice Internet en su día a día, es decir, prácticamente todo el mundo. Pero "los llamados ciberdelincuentes también ponen el punto de mira de sus fraudes en niños y adolescentes, cada vez más conectados al mundo digital a edades muy tempranas y que pueden ser objetivo fácil de todo tipo de estafas" (pág. 1).

Se hace habitual que dentro de las redes sociales se presentan publicaciones que presenta publicidad que entrelazan a tiendas digitales que son falsas en donde insertan un producto llamativo con rebajas y demás para que los usuarios con solo un clic den acceso a la información que contengan en su ordenadores o dispositivo móvil que estén usando. La problemática se presenta cuando a los usuarios se les solicita el pago o información personal para poder adquirir el producto, una persona mayor puede darse cuenta en su mayoría cuando se trata de una estafa, pero cuando son jóvenes o niños es más fácil que caigan en el engaño.

2.1.11.5. Child Grooming

Para Puyol (2019) el child grooming o acoso sexual de menores por Internet es:

> Conjunto o serie de "conductas realizadas por un mayor de edad, generalmente adulto, utilizando Internet, en muchos casos las redes sociales, para atraer a menores de edad, con el objeto de ganarse su amistad o estableciendo una conexión emocional con el niño o menor de edad, con la finalidad de desinhibirle y poder abusar sexualmente de él, o bien para obtener imágenes de pornografía infantil, para consumo propio o para distribuirlas" (pág. 5).

Es el término utilizado para hacer referencia al contacto que tienen los adultos mediante internet, en especial redes sociales con los niños, niñas y adolescentes, usando identidades falsas con la finalidad de que el menor confíe en ellos, hasta el punto en el que puedan abordar temas sexuales dentro de las conversaciones, esto con el objetivo de que los niños, niñas o adolescentes envíen imágenes o videos para el placer sexual de los victimarios, a su vez usa estos contenidos

enviados para usarlos como chantaje para obtener material adicional sexual o para abusar de ellos físicamente.

2.1.11.6. Pornografía infantil

La pornografía infantil en Internet es diferente a la mayoría de los delitos que manejan los departamentos de policía a nivel local. Los ciudadanos en cada localidad pueden acceder a imágenes de pornografía infantil que fueron producidas y/o almacenadas en otra ciudad o en otro continente. Alternativamente, pueden producir o distribuir imágenes que son descargadas por personas a miles de kilómetros de distancia (Morrillo, 2019).

De ahí que es casi seguro que una investigación que comienza en un distrito policial cruzará los límites jurisdiccionales. Por lo tanto, la mayoría de las principales investigaciones sobre pornografía infantil en Internet involucran la cooperación entre jurisdicciones, a menudo a nivel internacional. Debido al uso cada vez mayor de computadoras en la sociedad, es probable que la mayoría de los departamentos de policía enfrenten delitos de pornografía infantil en Internet (Romero, 2017).

En nuestro país se han adoptado, a nivel penal, una serie de resoluciones originalmente generadas en el ámbito de la Asamblea General de las Naciones Unidas, en el marco del Protocolo Facultativo de la Convención sobre los Derechos del Niño, las cuales se vinculan con la venta de niños, con la prostitución infantil y con el uso de estos menores pornográficamente, entendida ésta como todo tipo de explotación sexual directa o indirecta y por cualquier medio, en los cuales los niños, niñas y adolescentes expongan sus órganos genitales.

2.1.12. Derechos vulnerados de los niños, niñas y adolescentes por la falta de prevención de los delitos cibernéticos

Paradójicamente, Internet apoya aún más la industria del turismo sexual infantil al proporcionar a los patrocinadores de los desvíos un medio por el cual conectarse fácilmente con otros pasos afines a través del mundo. Las leyes nacionales y las normativas acordadas en el seno de la ONU se han establecido para proteger a los niños de la explotación cibernética. Pero no son pocos

los expertos en este tema que reconocen que todavía hay formas de delitos cibernéticos que necesitan ser tipificados como delito y que también es necesario formular la forma apropiada de castigo para los delincuentes cibernéticos que resultaron en niños como víctimas.

Los esfuerzos de protección a las víctimas de un acto delictivo es un esfuerzo para recuperar las pérdidas que ha obtenido la víctima. Esto se interpreta mejor si las víctimas están directamente involucradas en el proceso de resolución de casos penales. La aplicación de la ley es un esfuerzo de desarrollo que tiene como objetivo continuo la realización de la vida nacional y un entorno dinámico estatal seguro, ordenado y pacífico en el mundo independiente (Lenta & Zaldúa, 2020).

La finalidad de otorgar una indemnización no es otra que desarrollar la justicia y el bienestar de la víctima como miembro de la comunidad mediante referentes en la práctica, las víctimas tienen derechos y obligaciones para que se desarrollen como personas, los niños también son personas. Por lo tanto, se requieren normas estrictas, sencillas y de fácil comprensión para que pueda evitarse la discriminación en la aplicación por parte de las fuerzas del orden y la intimidación de determinadas partes que agudiza la condición de la víctima en su sufrimiento prolongado.

En el desarrollo de leyes y reglamentos nacionales e internacionales, las sanciones por desventajas de compensación no solo son dominio del derecho civil, sino que también han entrado en el derecho penal. Y esto sucede porque cada vez es mayor la atención de la comunidad mundial para acceder a las víctimas de hechos delictivos en el sistema de justicia penal.

La pena por daños y perjuicios es un delito que obliga a alguien que ha obrado en detrimento de otro a pagar algún dinero o bienes a la persona perjudicada. En el contexto de la pornografía cibernética la sanción compensatoria también puede ser en forma de víctimas colectivas representadas por el Estado y su uso para la rehabilitación mental de las víctimas de la pornografía. Además, se puede otorgar compensación a las personas que son víctimas directas de la pornografía cibernética (Huaccha, 2013).

El Ecuador es un país que ha ratificado la Convención sobre los Derechos del Niño a través del Decreto Presidencial Número 36 de 1990 del 25 de agosto de 1990, ha integrado aún más los

derechos del niño en la legislación nacional, concretamente en la Ley Número 23 de 2002 relativa a la Protección del Niño que ha reformada la ley número 35 de 2014.

Al igual que una serie de otras cuestiones de protección infantil, el abuso y la explotación de niños en línea está en la intersección de dos conjuntos estándares de los convenios internacionales. En conjunto, proporcionan un marco para abordar el fenómeno e informar la creación de un entorno protector para niños, niñas y adolescentes. Por un lado, algunos instrumentos internacionales se centran en el abuso y la explotación como una violación de los derechos del niño, en el contexto más amplio de la promoción y protección de los derechos del niño y su interdependencia e indivisibilidad. Estos instrumentos internacionales tratan de abordar diversas formas de transaccionalidad de la delincuencia, teniendo en cuenta los derechos humanos de las personas afectadas; y tienden a concentrarse sobre la respuesta y el enjuiciamiento. En este contexto, las principales organizaciones internacionales instrumentos son:

- Convención sobre los Derechos del Niño (1989)
- Protocolo Facultativo de la Convención sobre la Derechos del Niño sobre la venta de niños, prostitución infantil y pornografía infantil (2000)
- Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente de
- Mujeres y Niños, complementando la Convención de las Naciones Unidas contra el Crimen Organizado Transnacional (Protocolo de Palermo, 2000)
- Convenio del Consejo de Europa sobre Ciberdelincuencia (2001)
- Convenio del Consejo de Europa sobre la Protección de los niños contra la violencia sexual Explotación y Abuso Sexual (2007).

2.1.13. Medidas de prevención en delitos cibernéticos para niños, niñas y adolescentes

El uso de Internet para cometer delitos crea la posibilidad de efectos mayores. Cuando un determinado tipo de delito migra a Internet, debería tener una pena mayor; si bien no existe un instrumento internacional que recomiende a los Estados que consideren el uso de Internet para delinquir como una circunstancia agravante, existen varios países que lo han hecho en su legislación nacional.

En particular, Internet tiene el potencial de aumentar los efectos del almacenamiento y distribución de material de abuso infantil. En consecuencia, algunos países han creado la obligación de que los proveedores de servicios de Internet supervisen el uso de sus plataformas. Algunos países latinoamericanos han incluido en su legislación el deber de desarrollar Códigos de Conducta, medida recomendada por el Pacto de Río (Hernández, 2014).

La mayoría de las legislaciones latinoamericanas promueven y fomentan adecuadamente la creación de sistemas de autorregulación y códigos de conducta para Internet, y la creación de un grupo formado por representantes y usuarios. Sin embargo, no parece que esta medida sea adecuada ya que la deja en gran medida a la discreción de funcionarios (Ferro, 2020).

También, a nivel latinoamericano en general, se ha establecido que quienes presten servicios de almacenamiento de acceso a este tipo de material a través de redes informáticas están sujetos a las mismas penas que los autores de los delitos de distribución o difusión de pornografía infantil. Esto solo se aplica cuando se les notifica que suspendan o detengan el acceso a personas que están usando Internet ilegalmente para almacenar o difundir pornografía infantil y, posteriormente, no lo hacen.

Internet crea otra dimensión para una posible escena del crimen para la difusión y distribución de material de abuso infantil, por lo que los países deben adoptar medidas para abordarlo. Como se mencionó anteriormente, aunque los instrumentos internacionales no exigen que los países adopten el principio de jurisdicción universal, algunos países lo han hecho a través de disposiciones aplicables a los delitos cometidos contra los niños.

Hay países que contemplan en sus legislaciones la posibilidad de ejercer su jurisdicción sobre delitos cometidos en el extranjero, independientemente de dónde o por quién hayan sido cometidos, cuando los delitos estén relacionados con la pornografía o los derechos humanos regulados por tratados suscritos por el país. Muchas veces se aplica el principio de jurisdicción universal cuando los delitos cometidos afectan derechos protegidos por el derecho internacional, o menoscaban gravemente los derechos humanos universalmente reconocidos.

También se aplica el principio de jurisdicción universal para los delitos que el país se ha comprometido a combatir mediante la firma de tratados o la ratificación de convenciones. Ecuador lo aplica para delitos relacionados con los derechos humanos protegidos por instrumentos internacionales que han sido ratificados por el país. Otros países lo aplican por delitos cometidos contra los derechos humanos reconocidos por la comunidad internacional. Y hay Estados que lo aplican para delitos relacionados con delitos sexuales cometidos contra niños, niñas o adolescentes.

Es hora de que la comunidad internacional reconozca la responsabilidad conjunta de todos los países para combatir los delitos de pornografía infantil mediante la adopción del principio de jurisdicción universal para permitir el castigo efectivo de los infractores. Está más allá del alcance de los estudios regionales analizar el turismo sexual infantil y la trata de personas, pero dado que estos temas están estrechamente relacionados con la pornografía infantil, y debido a que Internet también se utiliza en la comisión de estos delitos, se insta a los países a adoptar medidas legislativas. también medidas para combatir estas prácticas.

Entre los países latinoamericanos, existen estados que tipifican como delito la conducta de promover, organizar, facilitar o coordinar el turismo sexual con menores de edad a través de cualquier medio de comunicación. También se tipifica como delito la organización o facilitación del turismo sexual. Se sanciona la conducta de promover, publicar, invitar, facilitar o coordinar la entrada a su territorio o salida de él de personas con la intención de practicar actos sexuales reales o simulados. Todos los países de América Latina, que son considerados países de destino de este tipo de delitos, deberían criminalizar el turismo sexual y cualquier tipo de publicidad relacionada con la explotación sexual infantil.

Independientemente de la ausencia de un instrumento regional, algunos países están penalizando conductas según sea necesario en la región. Casi todos los estados latinoamericanos incluyen en sus Códigos Penales delitos relacionados con conductas que anteceden a la propia producción de pornografía infantil, tales como buscar, requerir, reclutar, inducir, coaccionar a un niño para realizar escenas de abuso sexual infantil; o para mediar la participación de un niño en

una producción que involucre abuso sexual (UNICEF Argentina e Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo, 2011).

Facilitar la producción de pornografía infantil, por cualquier medio, está penalizado en casi todas las naciones de la región. Lo mismo ocurre con la mera exhibición, exhibición o divulgación de material de abuso infantil, que está tipificado como delito en todos nuestros países. También se ha tipificado como delito el acto de compartir el escenario con un niño en una producción que involucre pornografía infantil. Vale la pena señalar que el actor/actriz no es necesariamente responsable de la producción, y no sería procesado si esta conducta no estuviera tipificada como delito (UNICEF Argentina e Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo, 2011).

Se criminaliza también el financiamiento de producciones de pornografía infantil, lo que desincentiva la industria de la pornografía. Aunque muchos países latinoamericanos penalizan la visualización o el acceso a material de pornografía infantil, Bolivia, Brasil, Ecuador y México penalizan la adquisición de este tipo de material. Esta es una iniciativa muy interesante ya que la adquisición no implica posesión; más bien es equivalente a un pago por acceso.

NÚMERO DE DENUNCIAS SOBRE DELITOS INFORMÁTICOS EN ECUADOR

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24 052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17 913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	**3118**	**8230**	**8796**	**8421**	**9571**	**10 279**	**5048**	**53 463**

Figura 1: *Delitos Informáticos en Ecuador 2014-2020*
Fuente: Fiscalía General del Estado; 2020

2.2. Marco Legal

2.2.1. Tratados o Convenios Internacionales

2.2.1.1. Convenio De Budapest Sobre Ciberdelincuencia O Convenio De Budapest

Artículo 9 – Delitos relacionados con la pornografía infantil

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su "derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

a) la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

b) la difusión o la transmisión de pornografía infantil a través de un sistema informático;

c) la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;

d) la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

1. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:
   a) un menor adoptando un comportamiento sexualmente explícito;
   a) una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
   b) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.
2. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2" (Convenio De Budapest Sobre Ciberdelincuencia O Convenio De Budapest, 2001, págs. 24-28).

2.2.1.2. Convención Sobre Los Derechos Del Niño

Art. 16.-

1. Ningún niño será objeto de injerencias arbitrarias o "ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.

2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques" (Convención Sobre Los Derechos Del Niño, 2006, pág. 15) .

Art. 34.- Los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abuso sexuales. "Con este fin, los Estados Partes tomarán, en particular, todas las medidas de carácter nacional, bilateral y multilateral que sean necesarias para impedir:

a) La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal;
b) La explotación del niño en la prostitución u otras prácticas sexuales ilegales;
c) La explotación del niño en espectáculos o materiales pornográficos" (Convención Sobre Los Derechos Del Niño, 2006, pág. 24).

2.2.1.3. Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía

Art 1.- "Los Estados Partes prohibirán la venta de niños, la prostitución infantil y la pornografía infantil, de conformidad con lo dispuesto en el presente Protocolo" (Protocolo facultativo de la Convención sobre los Derechos del Niño, 2000, pág. 2).

Art 2.- A los efectos del presente Protocolo:

a) "Por venta de niños se entiende todo acto o transacción en virtud del cual un niño es transferido por una persona o grupo de personas a otra a cambio de remuneración o de cualquier otra retribución;

b) Por prostitución infantil se entiende la utilización de un niño en actividades sexuales a cambio de remuneración o de cualquier otra retribución;
c) Por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales" (Protocolo facultativo de la Convención sobre los Derechos del Niño, 2000, pág. 2).

2.2.1.4. Declaración Universal de los Derechos Humanos

Art.- 12.- Nadie "será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honra o a su reputación. Nadie podrá ser víctima de entrometimiento a su vida privada ni de su familia" (Declaración Universal de los Derechos Humanos, 1948, pág. 4).

Análisis

Algunos tratados y convenios internacionales regulan los delitos que se cometen en contra niños, niñas y adolescentes en relación a la tecnología y redes sociales, pero dentro de los países latinoamericanos, la presencia de Ecuador es inexistente, las leyes que ya se encuentran establecidas en el marco penal no son suficiente y no se actualizan al mismo ritmo que la tecnología y los ataques cibernéticos avanzan, todavía hay una brecha en la ley con relación a los delitos cibernéticos o ciberdelitos, a veces, no existe un departamento o procedimiento específico permitido a nivel judicial que permitan brindar una vigilancia adecuada para sancionar el ciberdelito, lo cual puede interpretarse a que la mayoría de ellos no son sancionados y los usuarios no están protegidos.

Una medida de prevención es la creación de una página estatal para prevenir los delitos cibernéticos dada a su nueva tendencia, la cual servirá como un canal de denuncia en la que se puede poner en conocimiento los diferentes delitos de manera anónima, esta página tendrá como prioridad entender los casos que involucre contenido sexual, ya que es el delito que con mayor frecuencia se presenta contra los niños, niñas y adolescentes en el internet, pero también se encargara de las demás situaciones que afecten a los derechos y bienestar de esta comunidad, como

contenido inapropiado, como es de esperarse el estado debe proteger los derechos de los niños, niñas y adolescentes cuando se trata de situaciones en las que se ven vulnerados como es el caso de la pornografía infantil y el ciberacoso, en donde necesitamos medidas contundentes e inmediatas por esta razón esta página debe nacer como una línea virtual de denuncia en el país para la protección de los niños, niñas y adolescentes, donde ayude a identificar a los niños, niñas y adolescentes que aparecen en imágenes o videos de abusos sexuales en las redes para brindarles protección y apoyo psicosocial pertinente, ya que las imágenes pueden circular en internet durante muchos años, por lo que el contenido sexual de una niña de 5 años puede seguir en línea veinte años después, además con la ayuda de esta plataforma crear una base de datos de protección para determinar si ha violentado anteriormente a la víctima o identificar al actor del delito.

Adoptar medidas pedagógicas en el sistema educativo de las escuelas y colegios para un seguro uso del internet con los niños, niñas y adolescentes donde aprenderán los peligros y riesgos que esconden las diferentes plataformas tanto en internet y las redes sociales, como estado es una oportunidad y un desafío acompañarlos en el camino del aprendizaje sobre el uso responsable de la web, además restringir la edad en el uso de redes sociales dando como edad mínima de 12 años y que el estado en el sistema educativo involucre usar plataformas seguras para niños, niñas y adolescentes. Por otra parte, los delitos registrados por la fiscalía contra la libertad e indemnidad sexuales con víctimas menores han descendido un 7%, pero en los años anteriores tenía una "consolidada línea ascendente", según el informe.

2.2.2. Constitución de la República del Ecuador

Art. 3.- Son deberes primordiales del Estado:

1. "Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes" (Constitución de la República del Ecuador, 2011, pág. 9).

Art 44.- El Estado, la sociedad y la familia "promoverán de forma prioritaria el desarrollo integral de las niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos; se

atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas" (Constitución de la República del Ecuador, 2011, pág. 21).

> "Las niñas, niños y adolescentes tendrán derecho a su desarrollo integral, entendido como proceso de crecimiento, maduración y despliegue de su intelecto y de sus capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de afectividad y seguridad. Este entorno permitirá la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales, con el apoyo de políticas intersectoriales nacionales y locales" (Constitución de la República del Ecuador, 2011, pág. 21).

Art. 46.- El Estado adoptará, entre otras, las siguientes medidas que aseguren a las niñas, niños y adolescentes:

4. "Protección y atención contra todo tipo de violencia, maltrato, explotación sexual o de cualquier otra índole, o contra la negligencia que provoque tales situaciones" (Constitución de la República del Ecuador, 2011, pág. 22). Las acciones y las penas por delitos contra la integridad sexual y reproductiva cuyas víctimas sean niñas, niños y adolescentes serán imprescriptibles.

Art. 66.- Se reconoce y garantizará a las personas:

19. "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación" (Constitución de la República del Ecuador, 2011, pág. 30).

Art. 424.- "La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica" (Constitución de la República del Ecuador, 2011, pág. 126).

"La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público" (Constitución de la República del Ecuador, 2011, pág. 127).

2.2.3. Código Orgánico Integral Penal (COIP)

Art. 78.- Mecanismos de reparación integral. - Las formas no excluyentes de reparación integral, individual o colectiva, son:

> 2. La rehabilitación: "se orienta a la recuperación de las personas mediante la atención médica y psicológica, así como a garantizar la prestación de servicios jurídicos y sociales necesarios para esos fines.
>
> 3. Las indemnizaciones de daños materiales e inmateriales: se refieren a la compensación por todo perjuicio que resulte como consecuencia de una infracción penal y que sea evaluable económicamente" (Código Orgánico Integral Penal, 2014, pág. 18).

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes. – "La persona que fotografié, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca

al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años" (Código Orgánico Integral Penal, 2014, pág. 21).

Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.- "La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años" (Código Orgánico Integral Penal, 2014, pág. 22).

Art. 154.3.- Contravenciones de acoso escolar y académico. –

1. Acoso académico: "Se entiende por acoso académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo, se dé por parte de un docente, autoridad o con quienes la víctima o víctimas mantiene una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de una o varias personas, por cualquier medio incluyendo a través de las tecnologías de la información y comunicación. Esta contravención será sancionada con una o más de las medidas no privativas de libertad previstas en los números 1,2, 3 y 6 del artículo 60 de este Código, y además el juzgador impondrá las medidas de reparación integral que correspondan según el caso.

2. Acoso escolar entre pares: Cuando las mismas conductas descritas en el párrafo anterior se produzcan entre estudiantes niñas, niños y adolescentes, se aplicarán las medidas socioeducativas no privativas de libertad correspondientes y el tratamiento especializado reconocido en la ley de la materia, garantizando los derechos y protección especial de niñas, niños y adolescentes" (Código Orgánico Integral Penal, 2014, pág. 27).

Art. 168.- "Distribución de material pornográfico a niñas, niños y adolescentes. - La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico, será sancionada con pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014, pág. 28).

Art 172.- Utilización de personas para exhibición pública con fines de naturaleza sexual. – La persona que utilice a "niñas, niños o adolescentes, a personas mayores de sesenta y cinco años o personas con discapacidad para obligarlas a exhibir su cuerpo total o parcialmente con fines de naturaleza sexual, será sancionada con pena privativa de libertad de siete a diez años" (Código Orgánico Integral Penal, 2014, pág. 29).

Art. 172.1.- Extorsión sexual. - La persona que, "mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero", ya sea de carácter sexual o de cualquier otro tipo, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, pág. 29).

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

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años" (Código Orgánico Integral Penal, 2014, pág. 30).

Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. – "La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad" será sancionada con pena privativa de libertad de siete a diez años (Código Orgánico Integral Penal, 2014, pág. 30).

Art. 178.- Violación a la intimidad. – "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley" (Código Orgánico Integral Penal, 2014, pág. 30).

2.2.4. Código de la Niñez y Adolescencia

Art. 19.- Sanciones por violación de derechos. – "Las violaciones a los derechos de los niños, niñas y adolescentes serán sancionadas en la forma prescrita en este Código y más leyes, sin perjuicio de la reparación que corresponda como consecuencia de la responsabilidad civil" (Código de la Niñez y Adolescencia, 2014, pág. 2).

Art. 46.- Prohibiciones relativas al derecho a la información. - Se prohíbe:

1.- "La circulación de publicaciones, videos y grabaciones dirigidos y destinados a la niñez y adolescencia, que contengan imágenes, textos o mensajes inadecuados para su desarrollo; y cualquier forma de acceso de niños, niñas y adolescentes a estos medios" (Código de la Niñez y Adolescencia, 2014, pág. 5).

Art. 47.- Garantías de acceso a una información adecuada. – "Para garantizar el derecho a la información adecuada, de que trata el artículo anterior, el Estado deberá:

f) Sancionar de acuerdo a lo previsto en esta Ley, a las personas que faciliten a los menores: libros, escritos, afiches, propaganda, videos o cualquier otro medio auditivo y/o visual que hagan apología de la violencia o el delito, que tengan imágenes o contenidos pornográficos o que perjudiquen la formación del menor" (Código de la Niñez y Adolescencia, 2014, pág. 6).

Art. 50.- Derecho a la integridad personal. – "Los niños, niñas y adolescentes tienen derecho a que se respete su integridad personal, física, psicológica, cultural, afectiva y sexual. No podrán ser sometidos a torturas, tratos crueles y degradantes" (Código de la Niñez y Adolescencia, 2014, pág. 6).

2.2.5. Código Orgánico de la Función Judicial

Art. 25.- "Las juezas y jueces tienen la obligación de velar por la constante, uniforme y fiel aplicación de la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y las leyes y demás normas jurídicas" (Código Orgánico de la Función Judicial, 2015, pág. 7).

Análisis

Al hablar del problema jurídico que presenta la falta de tipicidad de los delitos cibernéticos que han sido mencionados, pese a que Ecuador ya este encaminado a la generación de normas y leyes que examinan aspectos muy marcados con respecto a las nuevas tecnologías, así como se ha establecido, dentro del Código Integral Penal están regulados delitos como la pornografía infantil y acercare a niños, niñas y adolescentes para abusar física y psicológicamente y estos a su vez se encuentran sancionados con sus respectivas sanciones, aun se ve reflejada la falta de legislación, debido a que existen nuevas modalidades de persuasión hacia los niños, niñas y adolescentes, debido a esto es necesario que se incorporen dentro del marco legal los delitos cibernéticos como el grooming, sexting, pfishing y otros que no están tipificados como tal pero tienen algún artículo relacionado como el chantaje sexual y el ciberacoso, estos deben estar legislados de una manera integral dentro de la normativa ecuatoriana.

El Estado Ecuatoriano garantiza por medio de las leyes los derechos constitucionales de las personas, la normativa legal define un ordenamiento interno mediante la observación de la conducta de los individuos, así como también por medio de los principios, con el objetivo de poder garantizar la eficacia de los derechos. Las leyes y reglamentos penales deben garantizar la efectividad de la protección integral de los derechos constituidos por la ley y prevenir daños, vulneraciones o perjuicios por falta de ley, así mismo la constitución le otorga y reconoce el derecho a la protección de datos de los ciudadanos, es decir, ninguna persona puede vulnerar la privacidad de las personas exponiendo su información o vida personal, el derecho a la propiedad desde la perspectiva constitucional debe ser aplicado a la ley para garantizar efectivamente la clasificación y sanción de las nuevas formas de cometimiento del delito.

Lo que hay que destacar es que al hablar de ciberacoso, no nos limitamos a las áreas sexuales claramente definidas dentro del Código Orgánico Integral Penal, sino que también incluimos una serie de incidentes que pueden ser considerados como tales, como acoso, burlas, calumnias a otras personas, usar cuentas falsas para usurpar los nombres de las personas, causar mala reputación, etc., a través de medios electrónicos, en muchas ocasiones estas situaciones son notorias muchas veces, este tipo de comportamiento puede convertirse en algo más común y grave ya que no se conoce la identidad de la persona que realiza la acción de ciberacoso.

Si bien se han implementado varios artículos relacionados con los delitos informáticos en el Código Orgánico Integral Penal, el ciberacoso no es considerado como una nueva figura delictiva, lo que significa que aún no existen restricciones legales a esta conducta, y el número de casos permitidos de este tipo está aumentando. En su mayoría las víctimas son niños, niñas y adolescentes, cuando se realiza una denuncia relacionada a los diferentes delitos cibernéticos, estos quedan inconclusos debido a la falta de normativa que los regule, de esta forma otra problemática dentro del proceso judicial de estos delitos es la falta de peritos cibernéticos o informáticos.

El Estado tiene que garantizar los derechos, deberes y obligaciones que gozan los niños, niñas y adolescentes que están consagrados en la constitución de la República del Ecuador y en el Código Orgánico de la Niñez y Adolescencia, brindando un desarrollo idóneo y sano, teniendo en cuenta sus necesidades, ya que el Estado, la familia y la sociedad son piezas claves para la

protección y cuidado de este gran grupo de individuos vulnerables, puesto que demandan una prioridad dentro del marco legal del país, de esta manera las conductas delictivas dentro de las redes sociales no impidan un debido desarrollo integral dentro de los niños, niñas y adolescentes.

En su mayoría los niños, niñas y adolescentes se han visto envueltos en reiterados actos delictivos debido al uso de las redes sociales y las nuevas tecnologías que transgreden sus derechos constitucionales, al no implementar una normativa específica dentro del Código Orgánico Integral Penal, se está otorgando la libertad jurídica para que estas conductas dentro de la sociedad sean vistas como normales, pese a la existencia de algunas normativas en las cuales aparentemente se protegen los derechos de los niños, niñas y adolescentes, estos dentro de su desconocimiento e inocencia son víctimas dentro de las redes sociales.

2.2.6. Legislación Comparada

2.2.6.1. Argentina

La ley 26904, menciona en su artículo 131:

> "Será penado con seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos contactarse con una persona menor de edad con el propósito de cometer cualquier delito contra la integridad sexual por medios informáticos, por lo que hace referencia únicamente a menores de edad". (Ley 26904, 2013)

Al analizar el artículo 173 y 174 del Código Orgánico Integral Penal, se puede mencionar que el acoso sexual por medios electrónicos y el ciberacoso pueden confundirse en cuestión de términos, por ende la legislación argentina carece de tipificación en cuanto a delitos cibernéticos que atenten contra niños, niñas y adolescentes, en el año de 2020 según la AALC, en Argentina los delitos cibernéticos contra niños, niñas y adolescentes crecieron en un 47%, por otro la lado este país regula la ciberdelincuencia por su normativa que al igual que Ecuador se encuentra muy generalizada y mediante los convenios y tratados internacionales en los que participa.

2.2.6.2. México

En Nuevo León en la ciudad de México en el año 2012, se agregó una reforma en el Código Penal de Nuevo León en el cual se sanciona con una pena privativa de libertad de máximo 5 años al ciberacoso, de esta misma forma cuando se trate de niños, niñas y adolescentes se agrega una multa de cien a mil cuotas, por ende, la legislación mexicana si tienen regulado al ciberacoso e incluso puede agregare el agravante de grooming dentro del delito.

2.2.6.3. Colombia

El acoso mediante redes sociales es un hecho latente en Colombia que va aumentando de una manera constante, los estudios indican que hasta el año 2014 se habían suscitado un total de 6.898 denuncias de acoso cibernéticos entre ellos como víctimas menores de edad.

En marzo del año del 2013 entró en vigencia una ley en el que su objetivo principal fue la prevención del ciberbullying fomentando y fortaleciendo la convivencia entre niños, niñas y adolescentes, proteger los derechos humanos y minimizar los índices de acoso y abuso mediante tecnologías de información.

En el año 2009 también entró en vigencia la ley 1273, de protección de la información y de datos, su objetivo es regular las conductas que quebrantan el buen uso de los medios informáticos, o a la suplantación o sustracción de datos personales dejando a un lado el ciberacoso, pero teniendo también con mayor índice de víctimas a niños, niñas y adolescentes.

2.2.6.4. Chile

Siendo el caso de Chile el cual realizo una reforma en septiembre del 2011 a la ley General de Enseñanza, con el objetivo de reglamentar y prevenir la violencia dentro de las escuelas o bullying, que refleja un elevado índice en el país, dado también en el resto del mundo, comenzando a estas edades lo que en el futuro se convertirían en ciberacosadores.

En el mismo año la ley número 20.526 reguló una sanción para el acoso sexual de menores, posesión de material foto o video pornográfico infantil y pornografía infantil. Evidenciando claramente que en esta ley tampoco se encuentra la tipificación del acoso cibernético, dada en

cierta forma esa normativa guarda cierta similitud con la nuestra ya que en ambas se reflejan vacíos legales que deberían ser cubiertos.

2.2.6.5. Perú

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO I FINALIDAD Y OBJETO DE LA LEY

En su artículo 1 nos menciona el Objeto de la Ley, la presente Ley la cual tiene por esencia "prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra los ciberdelitos.

En su segundo capítulo establece los delitos informáticos contra la indemnidad y libertades sexuales, mencionando en su artículo quinto. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos; el que a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años" (Constitución Política del Perú, 1993).

2.2.6.6. España

La fiscalía española registra un aumento del 175% en el delito de acoso sexual a menores online. Según recoge la fiscalía, "los delitos de acoso sexual a menores o el child grooming ha aumentado un 175% desde 2018, y un 55% desde el 2019, lo que el informe califica como preocupante. Los delitos online contra la libertad sexual de menores de edad suponen un 8.5% del total, pero este porcentaje ha aumentado también respecto al año pasado.

La Unión Europea como medida preventiva mediante directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y explotación sexual de los menores y la pornografía infantil por internet, reemplazó a la decisión marco 2004/68/JAI relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, unifico en toda la unión europea las infracciones penales relativas a los abusos sexuales sobre menores, su

explotación sexual y la pornografía infantil y estableció disposiciones conducentes a luchar contra la pornografía infantil a través de internet" (Ministerio Fiscal España, 2018).

2.2.7. Ciberdelitos en las redes sociales

Tabla 1:

Ciberdelitos en las redes sociales

DELITO	DESCRIPCIÓN	TIPIFICACIÓN DENTRO DEL COIP	APARECE EL DELITO EN REDES SOCIALES
Chantaje Sexual	El chantaje sexual, también conocido como "sextorsión", ocurre cuando un atacante usa imágenes tomadas por otros (selfis) para obtener beneficios sexuales o dinero, y lo amenaza con publicar estas imágenes. En muchos casos, la característica de los chantajistas es que la influencia y la manipulación se producirán durante un largo período de tiempo. Una vez que se persuade a la persona para que envíe su primera imagen pornográfica, las amenazas, la intimidación y la coacción aumentarán rápidamente.	El Código Orgánico Integral Penal en su artículo 172.1 menciona a la extorsión sexual, pese a que este artículo se relaciona no menciona de manera específica a los niños, niñas y adolescentes ni al uso del internet mediante plataformas digitales.	Si
Child grooming	Mediante las redes sociales una persona adulta mantiene comunicación con u niño o niña menor de 13 años con el objetivo de mantener relaciones sexuales, abusar de ellos o agredir sexualmente, el agresor usa la estrategia de suplantar identidad para cometer el delito.	Dentro del Ecuador no hay un artículo que sancione de manera específica el delito, sin embargo, dentro del art. 173 tiene relación al acto.	Si
Ciberacoso	Es la agresión psicológica que reciben los niños, niñas y adolescentes de manera constante mediante las redes sociales.	El artículo 154.3 menciona al acoso ESCOLAR como contravención	Si
Phishing	Mediante engaños y suplantación de identidad, el delincuente	No se encuentra tipificado.	Si

	cibernético engaña a los usuarios para obtener información personal con el objetivo de realizar fraude económico. En el caso de los niños, niñas y adolescentes, los delincuentes utilizan las plataformas de gameplays para obtener números de tarjetas bancarias de sus padres o direcciones de los menores.	Un artículo relacionado es el 186 que hace mención a la estafa, sin embargo, no se refiere de manera específica a esta modalidad cibernética.	
Pornografía Infantil	Es toda representación gráfica, visual o textual, incluso juegos de videos y dibujos animados que involucren de forma real o simulada a niños, niñas y adolescentes en el cual se vean involucrados en actividades sexuales o muestren sus genitales, Actualmente este delito se difunde con mayor rapidez gracias al avance de la tecnología y los distintos medios y redes sociales.	**Art 103.- "**Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografié, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años. Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años" (Código	Si

		Orgánico Integral Penal, 2014). **Art 104.- "**Comercialización de pornografía con utilización de niñas, niños o adolescentes. - La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años" (Código Orgánico Integral Penal, 2014).	
Sexting	Se define al sexting como los mensajes mediante redes sociales de contenido sexual, en este caso son protagonizados por la persona que envía el mensaje, el delito existe cuando ese contenido es difundido sin autorización.	Dentro del COIP no se encuentra un artículo que tipifique este acto. El Artículo 178 del COIP menciona a la violación a la intimidad, que se correlaciona al tema del sexting.	Si

Nota: la tabla 1, describe la presencia de los delitos descritos dentro de las redes sociales.

Fuente: Código Orgánico Integral Penal**;** 2021

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Metodología

La metodología de la investigación conlleva un procedimiento investigativo lo que nos permite la creación de diferentes conocimientos que se basan en las ciencias llevándonos a obtener las técnicas necesarias para solucionar los problemas, cuyo propósito es el de obtener resultados confiables para sustentar el valor investigativo del trabajo de tesis, utilizando el método inductivo, ya que este tipo de metodología va de lo general hasta desglosarse particularmente en la información necesaria obteniendo así conclusiones generales y precisos hasta particulares.

3.2 Tipo de Investigación

En esta tesis existes diferentes tipos de investigación lo que nos permite plantear temas e información importantes, aplicaremos estos tipos de investigación con la finalidad de llevar un buen desenvolvimiento en el estudio y análisis del tema planteado: "Niños, niñas y adolescentes en las redes sociales: Estudio sobre los sistemas de protección y prevención judicial", su planteamiento y formulación con sus objetivos, son los siguientes:

Descriptiva:

Este tipo de investigación recopila investigación importante y establece una descripción completa sobre las características del tema que se está estudiando. "Una investigación descriptiva pretende dar cuenta de las características de un fenómeno u objeto sujeto a investigación, de sus propiedades, características, atributos, componentes, elementos y relaciones entre ellos. Por ejemplo, en el caso de investigaciones jurídicas, se busca encontrar la naturaleza jurídica de la institución" (Rocha C. M., 2015)

Es decir que el objetivo para la investigación de carácter descriptivo es el de describir las características fundamentales dentro del objeto de la investigación, la cual utiliza diferentes criterios que nos permite establecer la estructura del fenómeno de estudio, arrojándonos información sistemática y comparable.

Experimental:

Este tipo de investigación ve cual es el enfoque científico por medio de variables; realiza un estudio en el cual de manera intencional una o más variables independientes (supuestas casusas-antecedentes) son manipuladas para su estudio, cuyo objetivo es analizar las diversas consecuencias que una o distintas variables dependientes, sobre un escenario controlado que ha sido elaborado por el investigador, utilizando dentro de este tipo investigativo el método cuantitativo.

Analítico y sintético:

Estos tipos de investigación nos ayuda a estudiar ciertos hechos que van en función a la investigación la cual empieza desde su descomposición del objeto de estudio que se refiere a: los "Delitos cibernéticos contra niños, niñas y adolescentes y su vacío en la normativa ecuatoriana", con la finalidad de la obtención de una información más reducida para determinar la exactitud de la investigación.

3.3 Enfoque de la investigación

Al hablar de los enfoques de una investigación, nos referimos a la naturaleza de la del objeto de estudio, que se divide en cuantitativa y cualitativa, la cual abarca todas las etapas del proceso de investigación, desde la definición del tema, el planteamiento del problema de investigación, desde una visión de carácter teórico definir los métodos y estrategias, analizando las diferente etapas de recolección, análisis e interpretación de datos, llegando a plantear los dos enfoques dentro del trabajo investigativo para una mayor comprensión de estudio.

- **Enfoque Cualitativo:** Este enfoque va direccionado al análisis y estudio de los métodos empleados mediante la recolección de datos por medio de un tipo descriptivo, así también análisis de opiniones, textos bibliográficos o de ámbito argumentativo los cuales son obtenidos por los instrumentos de investigación tal como la entrevista a distintos profesionales en el área del objeto de estudio.

3.4 Técnicas de la investigación

Para una recolección de datos claros y precisos dentro de la investigación, se desarrollará un enfoque cualitativo utilizando las entrevistas para el desarrollo del trabajo de tesis.

- **Entrevistas:** Las entrevistas permitirán que mediante criterios jurídicos y razonamientos lógicos de profesionales en materia de derecho de niñez analizar de manera descriptiva sobre sus diferentes perspectivas en relación al objeto del problema de la investigación, así como también a docentes de nivel primeria y secundaria sobre el manejo de redes sociales dentro del área educativa.

3.5 Población y muestra

La población utilizada para recolectar datos necesarios mediante entrevistas para la elaboración del presenta trabajo de tesis son abogados que manejan el área de niñez y adolescencia o dentro de su campo laboral abordan en gran magnitud temas relacionados al investigado, así como peritos de la Policía Nacional de la Unidad Especial de Delitos Sexuales y Docentes de primaria y secundaria.

3.6 Análisis de los resultados

3.6.1 Entrevistado #1

Abogado César Peña Morán

Fiscal del Cantón Balao

¿Considera usted que, por la falta de control del uso de las plataformas digitales de comunicación, socialización y educación, queden en la impunidad las conductas y delitos cibernéticos que se comentan contra los niños, niñas y adolescentes?

Los delitos cibernéticos que se comenten contra las victimas en este caso niños, niñas y adolescentes, no es que quedan en la impunidad, lo que debería existir un control de parte de la entidad reguladora de dicho sistema, en este caso le correspondería a la súper intendencia de telecomunicaciones que son las que dan la autorización a las empresas de internet, debe existir control, en cuanto a la sanción y a la investigación del delito, existe una unidad de la policía judicial y la fiscalía también cuenta una unidad de delitos cibernéticos en cuanto a la ubicación de estas plataformas para determinar de dónde se origina los delitos.

¿Cree que los niños, niñas y adolescentes se ven expuestos para ser víctimas de conductas y delitos cibernéticos por la digitalización globalizada como consecuencia de la pandemia?

Si son expuestos lastimosamente los niños, a mi criterio personal si, y más aún a raíz del surgimiento de las medidas preventivas del COVID desde marzo del año 2020 donde la mayoría de niños, niñas y adolescentes tienen que hacer sus clases virtuales, esto ha originado que habrán ciertos enlaces o paginas no autorizadas de adultos donde pueden ser vulnerables a ciertos tipos de delitos de Naturaleza sexual, aparte de eso las comunicaciones que suelen tener con diversas personas a nivel mundial, que le envían solicitudes de amistad en el caso de Facebook, videos por Messenger o integran que es lo más común que como fiscalía investigamos en donde se puede determinar que efectivamente los menores son los más vulnerables por este tipos de personas que delinten a través de los medios en este caso el internet.

¿Considera que es necesario que se cree una unidad especializada para tratar las conductas y delitos cibernéticos que atenten contra la integridad física, sexual y psicológica de los niños, niñas y adolescentes?

La unidad especializada en investigaciones de delitos que se comenten en contra de niños, niñas y adolescentes se llama unidad de violencia de genero funciona en la ciudad de Guayaquil, son diez unidades y a nivel de todos los cantones todas las fiscalías son multi competentes, autorizadas y facultadas para ese tipo de investigaciones, adicional a eso la policía judicial cuenta con una unidad de delitos cibernéticos, lo que debe existir mayor control de los entes del estado que regulan los temas de internet para evitar este tipo de páginas o bloquear esas páginas de personas que van a cometer delitos hacia los menores

¿Considera usted que el Estado debe fomentar medidas de prevención y protección de los ciberdelitos en los niños, niñas y adolescentes?

El código orgánico de la niñez y adolescencia establece ya las medidas de prevención en este caso están en el artículo 8, 46, 51 y a su vez también encontramos la tipicidad en el Código Orgánico Integral Penal de los delitos de pornografía infantil en el artículo 103 y a su vez 104 comercialización de pornografía infantil y los delitos de violación a la propiedad privada o delitos de Difusión de información de circulación restringida en los artículos 180 y 181, la tipificación de delitos están en el COIP y en cuanto a los principios rectores de la prevención que debe establecer

el estado a favor de los niños, niñas y adolescentes están establecidos en el CONA en los artículos 4, 8, 47 y 51 y en la constitución artículos 1, 11, 35

¿Considera que se debe implementar en el sector educativo medidas de seguridad para un manejo seguro de plataformas digitales?

Tengo conocimiento que el ministerio de educación si ha implementado hace años un sistema de internet para el bloqueo de ciertas páginas en las unidades educativas, pero no debemos olvidar que muchas unidades educativas cuentan con apertura de wifi, o en caso de los menores llevan sus teléfonos ya con planes pagados donde se pueden conectar a cualquier tipo de plataformas o paginas no autorizadas para menores de edad, el ministerio de educación lo que debe ya es fomentar un nivel educativo en cuanto a la prevención de los menores de edad de que se conecten o tengan algún tipo de contacto con páginas, en este caso diríamos paginas no autorizadas o de pornografía, igualmente con personas desconocidas, muchos menores le digo por experiencia propia, tienen contacto con personas adultas de otras partes del mundo, ya que sus papa no los vigilan y suben información de carácter personal, familiar y ubicaciones en tiempo y espacio, esto origina que muchas personas dedicadas a los delitos cibernéticos los estén cazando para verificar la informaciones y cometer delitos.

3.6.2 Entrevistado #2

Abogado. Oswaldo Farfán Vera

Abogado de la Junta Cantonal de Protección de Derechos del Cantón Balao

¿Considera usted que, por la falta de control del uso de las plataformas digitales de comunicación, socialización y educación, queden en la impunidad las conductas y delitos cibernéticos que se comentan contra los niños, niñas y adolescentes?

El estado a través de su gobierno de control debería controlar las plataformas digitales con la finalidad de que tengan mayor seguridad para ingresar a las páginas y que los niños, niñas y adolescentes no tengan facilidad de entrar a estas páginas, también aparte de eso es responsabilidad de los padres, de tener mayor cuidado de lo que hacen nuestros hijos con los celulares, Tablet, computadoras cuando están en su libre albedrío con esos aparatos electrónicos, en lo personal si me parece que debería haber un mayor control de parte del estado para que si en el momento en

que cundo un menor por curiosidad vaya a ingresar a paginas prohibida no pueda tener el fácil acceso y evitar que caigan como víctimas de estos delitos cibernéticos.

¿Cree que los niños, niñas y adolescentes se ven expuestos para ser víctimas de conductas y delitos cibernéticos por la digitalización globalizada como consecuencia de la pandemia?

En este estado donde nos encontramos en pandemia, tanto las unidades educativas están en clases virtuales donde los chicos van acceder o tener mayor facilidad para estar con estos dispositivos y así aprovechar de entrar a otras páginas, en todo caso si están expuestos, como le vuelvo a repetir los padres deben controlar más ese tiempo que tienen los menores para hacer sus tareas y recibir sus clases virtuales que hoy en día la pandemia nos conllevo a esto , pero si hay una formas de cómo controlar el tiempo prudencial con la finalidad de evitar ciertas situaciones que posterior se podría considerar como delito.

¿Considera que es necesario que se cree una unidad especializada para tratar las conductas y delitos cibernéticos que atenten contra la integridad física, sexual y psicológica de los niños, niñas y adolescentes?

Mi apreciación no sería de crear nuevas unidades especializadas, porque no conseguimos nada con eso, podrían ser miles de unidades especializadas, pero si no atacamos la raíz al problema en sí, de donde nace, de donde se suscita, no llegaremos a nada, porque las unidades especializadas siempre se va a dedicar a proveer e investigar los delitos ocasionados, pero lo que queremos es evitar que existan esos delitos, que nuestros menores no caigan en esas trampas que están en las redes sociales, más bien sería una concientización, hablar con los chicos en las escuelas, en fin vuelvo a repetir la mayor responsabilidad recae en los padres de los chicos, en conclusión crear más unidades para mí no es lo más ideal.

¿Considera usted que el Estado debe fomentar medidas de prevención y protección de los ciberdelitos en los niños, niñas y adolescentes?

Si, el estado está obligado, está llamado a proteger a todos los habitantes, más aún esta sector vulnerable que son los niños, niñas y adolescentes como parte más débil de esta sociedad, existen medidas de protección, lo que conlleva es que se debe utilizarla de la mejor manera, la prevención seria el punto de partida para evitar que los niños, niñas y adolescentes, en lo posterior necesiten de una medida de protección, pero si el estado las tiene, la junta cantonal obviamente

cuando existe esta clase de vulneración de derechos otorga mediad de protección respecto a esto, porque los niños siempre van a estar protegido, dentro del estado si existen medidas de protección para proteger los derechos de los niños, niñas y adolescentes.

¿Considera que se debe implementar en el sector educativo medidas de seguridad para un manejo seguro de plataformas digitales?

Si, considero que si, en estos últimos tiempos por la pandemia, como ya lo había mencionado que ha llevado a que los chicos utilicen estos dispositivos para sus clases, pero eso también lleva una mayor responsabilidad por parte del ministerio de educación, no sé, se me ocurre a mí de pronto crear una página exclusivamente para sus clases para que no tengan potro acceso los chicos, entonces yo que creo que el sector educativo debería implementar estas seguridades para el manejo seguro de diferente plataformas, esto conlleva a la curiosidad de los menores ingresar a las páginas que en lo posterior lo único que le trae problemas siendo atrapados por cibernautas delincuentes, si debería implementar mayor seguridad el sector educativo.

3.6.3 Entrevistado #3

Abogado Johnny Bayas Gaibor

Defensor público de la Unidad Judicial De La Familia Mujer Niñez Y Adolescencia de la ciudad de Milagro

¿Considera usted que, por la falta de control del uso de las plataformas digitales de comunicación, socialización y educación, queden en la impunidad las conductas y delitos cibernéticos que se comentan contra los niños, niñas y adolescentes?

Para mí el control sería un poco complejo por la magnitud que esto implica, pero claramente es correcto que esta clase de delitos se encuentran en su mayoría impunes a consecuencias de falta de políticas públicas y desconocimiento de a dónde dirigir las denuncias y conocer qué clase de hechos constituye delito cibernético.

¿Cree que los niños, niñas y adolescentes se ven expuestos para ser víctimas de conductas y delitos cibernéticos por la digitalización globalizada como consecuencia de la pandemia?

Se encuentran expuestos desde hace mucho tiempo atrás, no podemos culpar a la pandemia si el uso de los sistemas informáticos y de información globalizada, se viene haciendo uso desde la

aparición de los sistemas informáticos y uso de redes sociales.

¿Considera que es necesario que se cree una unidad especializada para tratar las conductas y delitos cibernéticos que atenten contra la integridad física, sexual y psicológica de los niños, niñas y adolescentes?

Totalmente de acuerdo en que se deba crear una unidad especializada, pero no solo para niños niñas y adolescentes sino también para la sociedad en general, misma que sufre esta clase de violación de sus derechos y no sabe dónde y cómo denunciar.

¿Considera usted que el Estado debe fomentar medidas de prevención y protección de los ciberdelitos en los niños, niñas y adolescentes?

Debería de realizar mayor fomento en capacitación a los niños niñas y adolescentes dentro de las aulas de estudio, respecto al riesgo de sufrir graves consecuencias a causa de delitos cibernéticos.

¿Considera que se debe implementar en el sector educativo medidas de seguridad para un manejo seguro de plataformas digitales?

Lo veo un poco incontrolable en la sociedad, puesto que los medios digitales no solo se manejan en el área educativa, sino en todas partes en los hogares con conectividad, más surtiría efecto el control por parte de los padres o familiares a quienes estén a cargo del cuidado de los niños niñas y adolescentes.

3.6.4 Entrevistado #4

Sargento Segundo Danny Javier Villegas Damián

Encargado de la Unidad Nacional de Investigación Contra La Integridad Sexual de zona Guayas

¿Considera usted que, por la falta de control del uso de las plataformas digitales de comunicación, socialización y educación, queden en la impunidad los delitos cibernéticos que se comentan contra los niños, niñas y adolescentes?

Para dar una relevancia de los delitos cibernéticos que hoy en día existen y la serie de riesgos que lleva navegar en la red mediante la utilización de herramientas tecnológicas de información y

comunicación, debo manifestar que efectivamente no pueden quedar en la impunidad ciertas conductas ya que son delitos que tienen gran repercusión sobre los niños, niñas y adolescentes debido al auge de comunidad Millenials que se ha presentado, así también hay niños que desconocen el manejo de estas herramientas tecnológicas dentro lo que es internet, gracias a la unidad de delitos sexuales, los relacionados a este ámbito reciben una ayuda extra, aun no se ha hablado ampliamente sobre las nuevas figuras de delitos que se presentan en la red pero se está trabajando en ello.

¿Cree que los niños, niñas y adolescentes se ven expuestos para ser víctimas de delitos cibernéticos por la digitalización globalizada como consecuencia de la pandemia?

Debido a la pandemia de Covid-19 las personas pasan mucho más tiempo conectados en casa, en especial los jóvenes y niños ya que no se están frecuentando las unidades educativas, usan mucho el internet para buscar información para sus estudios, así como también usar mucho las redes sociales pero así también no debemos olvidar que el tema tecnológico acarrea muchas consecuencias a los adolescentes y niños, ya que son sujetos vulnerables de violencia de internet, no solo su integridad personal sino también su salud mental.

¿Considera que es necesario que se cree una unidad especializada para tratar los delitos cibernéticos que atenten contra la integridad física, sexual y psicológica de los niños, niñas y adolescentes?

Con la globalización han surgido innumerables cambios a la sociedad en diversas áreas por tal razón dentro de las zonas de Guayaquil y Quito con unidades especializadas en delitos cibernéticos que abarca a personas mayores, una unidad dirigida directamente a tratar con menores de edad, donde únicamente existan profesionales encargados y especializados no hay pero debido al alto incremento de casos si es una opción muy acertada, en mi Unidad de Integridad Sexual nos especializamos en casos de este tipo de delitos cibernéticos relacionados a la integridad sexual.

¿Considera usted que el Estado debe fomentar medidas de prevención y protección de los ciberdelitos en los niños, niñas y adolescentes?

A través de la asistencia técnica para la eliminación de la violencia sexual, el estado en conjunto con el entorno educativo debe hacer un proceso de identificar las mejores estrategias para que se desarrollen planes y proyectos para garantizar la prevención y que se pueda identificar de manera oportuna a los ciberdelincuentes, para que exista protección para los niños, niñas y adolescentes y

así no sean vulnerados dentro de las plataformas virtuales.

¿Considera que se debe implementar en el sector educativo medidas de seguridad para un manejo seguro de plataformas digitales?

Dentro de las plataformas que usan las unidades educativas para conectar a sus estudiantes, si deberían implementar medidas de seguridad en apoyo con personal del sector público para aplicar guías y formatos para evitar los delitos cibernéticos, capacitar a la comunidad estudiantil para que eviten caer en el amplio mundo de la ciberdelincuencia.

3.6.5 Entrevistada #5

Msc. Yadira Chica Cisneros

Directora de la Escuela Fiscal "Rosa Amada Espinoza"

¿Conoce las consecuencias del mal uso de las plataformas digitales y las redes sociales?

Si, el problema en conocer o no es el uso desmedido de estas plataformas digitales que genera un caos familiar, personal y muchas veces hasta educativo porque prefieren ingresar a unas páginas indebidas con el fin de pasar el tiempo y no hacer lo que deben de realizar dentro de lo debido.

¿Considera usted si los niños, niñas y adolescentes tienen debido conocimiento sobre el mal uso de las redes sociales?

En cuanto al uso de las redes por la necesidad las han incrementado entro de su vida cotidiana pero no conocen de manera clara las netiquetas, que se refiere al uso correcto del ingreso o el acceso a ciertas plataformas digitales y de esta manera hacerlo más eficiente manteniendo las medidas necesarias para un control armoniosos dentro de la conectividad, es por ello que no todo los niños o adolescentes tienen el conocimiento idóneo de uso de redes sociales.

¿Considera que el sistema judicial y educativo está preparado para prevenir el cometimiento de los delitos cibernéticos que atenten contra los niños, niñas y adolescentes?

Con respecto a esta pregunta y como estudiante de derecho que también soy, considero que no ya que con esto de la masificación de las redes sociales estamos más expuestos, ya que hay muchas personas que proveen mucha información personal dentro de sus redes sociales y esto genera que las personas de manera equivocada hagan el uso innecesario de esta información y se

vean afectadas por estos delitos de carácter cibernético, debido a la digitalización que se ha vivido por tema pandemia se han presentado nuevas figuras por lo tanto el sistema judicial necesitaría capacitarse mucho más dentro de esa áreas, conoce los delitos comunes pero se van presentado nuevos con la actualidad digital .

¿Considera que la digitalización académica traerá nueva tendencia de delitos cibernéticos afectando directamente a los niños, niñas y adolescentes?

En parte si, ya que si no se prepara a la sociedad para este nuevo mecanismo que se va a incrementar dentro de este sistema si podríamos tener un lado de perjuicio, ya que los menores quedarían un poco más expuestos ya que brindan de manera inocente información por la cual pueden verse afectadas por ello debe a ver un soporte o un lineamento adecuado para que se estructure de una manera en el cual ellos no se vean afectados o expuestos ya que si la virtualidad educativa va a seguir se debe afianzar esas nuevas políticas.

¿Considera usted que es necesario que los niños, niñas y adolescentes sean educados dentro de los planteles educativos para un manejo seguro de plataformas digitales y redes sociales?

Debería ser inculcado, pues a nosotros los docentes siempre nos han dado la potestad de educar, de transformar la sociedad entonces sí debería incluirse dentro de las mallas curriculares ese uso ahora que se está dando la virtualidad más aún que esta digitalización académica nos tomó por sorpresa entonces debemos ya preparar con ese conocimiento previo, incrementar de manera fortalecida dentro del plan académico para que de esta manera los niños, niñas y adolescentes tengan un conocimiento idóneo.

3.6.6 Entrevistada #6

Msc. Magali Rosado

Rectora de la Unidad Educativa Balao

¿Conoce las consecuencias del mal uso de las plataformas digitales y las redes sociales?

Claro que sí, en este tiempo de pandemia y ya que todas las personas utilizamos las redes sociales, todo lo relacionado con el mundo digital hace que este medio sea una ventana abierta para todo tipo de personas, hay que tener cuidado con las publicaciones que se realizan dentro de

las redes sociales porque cualquiera pude ser víctima de engaños, amenazas, robos, todos los delitos que se realizan de manera digital.

¿Considera usted si los niños, niñas y adolescentes tienen debido conocimiento sobre el mal uso de las redes sociales?

Los niños no tienen el debido conocimiento porque ellos no saben quiénes están detrás de estos medios, nosotros al momento de publicar alguna información dentro de las redes sociales más comunes como son Facebook, Instagram o WhatsApp, nos exponemos a cualquier peligro, principalmente lo menores ya que ellos no tienen el debido conocimiento, es ahí donde los padres deben estar pendientes de las publicaciones que realizan en esto medios para poder prevenir cualquier tipo de acto.

¿Considera que el sistema judicial y educativo está preparado para prevenir el cometimiento de los delitos cibernéticos que atenten contra los niños, niñas y adolescentes?

Dentro del sistema judicial creería que existen aún alguna falencia para solventar estos casos, ya que dentro de nuestra institución se presentó un caso de hackeo del sistema, pero no se logró resolver el inconveniente pese a que exista una denuncia de por medio, por cuanto al sistema educativo se trató de resolver dentro de lo posible, falta un poco más de capacitación para ambas áreas.

¿Considera que la digitalización académica traerá nueva tendencia de delitos cibernéticos afectando directamente a los niños, niñas y adolescentes?

Considero que no siempre y cuando nosotros como docentes implementemos una educación virtual adecuada para que todos nuestros estudiantes tengan conocimiento y estén preparados para posibles situaciones de delitos cibernéticos.

¿Considera usted que es necesario que los niños, niñas y adolescentes sean educados dentro de los planteles educativos para un manejo seguro de plataformas digitales y redes sociales?

Claro que si ya que los menores no miden los peligros que existen dentro de las redes sociales, piensan que todos los usuarios de internet son personas buenas o correctas que no les causaran daños, por eso es importante educarlos para evitar el riesgo que abunda dentro del medio electrónico.

CONCLUSIONES

1. El uso del internet y las redes sociales ha tenido un gran realce en las últimas décadas debido a la globalización y digitalización en distintas áreas, en especial por la Pandemia de COVID- 19 incrementado el uso del internet y redes sociales, lo que hace que miles de niños, niñas y adolescentes intercambien información de carácter personal interactuando así con diferentes usuarias dentro de la red de internet, algunos de estos usuarios buscan ocasionar daño, de tal manera que por estos medios electrónicos y plataformas digitales cometen actos ilegales que vulneran a los niños y adolescentes dentro de ese espacio, provocando una serie de hechos delictivos que atentan contra la seguridad e integridad jurídica de todos los usuarios de internet, de manera especial, a los menores de edad que se ven afectados en su mayoría.

2. Los niños niñas y adolescentes en la actualidad ven el internet como una necesidad de aprender, interactuar y comunicarse con personas, conllevando a la migración al mundo digital, provocando así la presencia de nuevas conductas delictivas a nivel cibernético por ello es necesario tipificar y sancionar los nuevos modelos de delitos cibernéticos para precautelar de manera especial la integridad y la intimidad de los niños, niñas y adolescentes, el Estado Ecuatoriano aún tiene mucho por trabajar en cuento a estos delitos ya que únicamente han preferido relacionarlo con otras figuras jurídicas o asociarlas con conductas dentro del ordenamiento jurídico ya tipificadas como las agresiones sexuales.

3. Dentro de los resultados adquiridos en las entrevistas existe falta de prevención hacia los niños, niñas y adolescentes en el sistema educativo sobre los delitos cibernéticos y poco conocimiento y poca atención del Estado en relación a las nuevas figuras delictivas cibernéticas que atentan y vulneran la integridad física, sexual y psicológica como el sexting, child grooming, chantaje sexual, pornografía infantil, ciberacoso, phishing, debiéndolos considerar como actos antijurídicos y ser causa de una sanción, debido a que vulnera derechos constitucionales de esta población vulnerable.

RECOMENDACIONES

1. Se debe de controlar el acceso a las plataformas digitales para los niños, niñas y adolescentes dada a la digitalización, restringir la edad a diferentes plataformas debido al gran avance que han tenido las tecnologías de la educación, comunicación e información, que exista supervisión constante de un adulto y así proteger a los menores de estas nuevas conductas y delitos cibernéticos.

2. Dentro del Código Orgánico Integral Penal es necesario que dentro del rango de delitos cibernéticos se revise de manera constante debido a la actualización del mundo digital que provoca nuevas figuras ilícitas de carácter ilegal, así también se debe de incluir dentro del ordenamiento penal la tipificación de las nuevas figuras cibernéticas las cuales vulneran de manera especial a los niños, niñas y adolescentes debido a su estado de ingenuidad y desconocimientos.

3. Se recomienda implementar dentro de las Unidades Educativas primarias y secundarias específicamente programas que ayuden a los niños y adolescentes a tener un manejo seguro de las distintas plataformas digitales, así mismo el Estado como ente regulador aparte de tipificar las nuevas figuras de delitos cibernéticos, también debe incorporar programas para el manejo de redes sociales para prevenir y precautelar el cometimiento de estos delitos.

REFERENCIAS BIBLIOGRÁFICAS

Andalia, R. (2004). Aproximaciones para una historia de Internet. *Scielo*, 1-33. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000100005

Avalos, K. (2013). La gestión responsable de redes sociales digitales en las organizaciones. *Digital Universitaria*, 14.

Blodget, H. (1 de octubre de 2009). *Insider*. Obtenido de Insider: https://www.businessinsider.com/mark-zuckerberg-innovation-2009-10

Bolaños, Simone, & Becerra. (2005). Phising Nueva Forma de Ciberestafa. *Revista Coruña*, 20-21. Obtenido de Phising Nueva Forma de Ciberestafa.

Carta Judicial Iberoamericana. (Abril de 2012). *CUMBRE JUDICIAL IBEROAMERICANA*. Obtenido de CUMBRE JUDICIAL IBEROAMERICANA: https://contralaviolenciavial.org/uploads/file/LEGISLACION/Carta%20Iberoamericana%20de%20Derechos%20de%20las%20Victimas.pdf

Código de la Niñez y Adolescencia. (2014). *Registro Oficial 737 -2003.* Quito: República del Ecuador. Obtenido de https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-06-C%C3%93DIGO-DE-LA-NI%C3%91EZ-Y-ADOLESCENCIA-Leyes-conexas.pdf

Código Orgánico de la Función Judicial. (2015). *Registro Oficial Suplemento 544.* Quito: Pleno de la Comisión Legislativa y de Fiscalización. Obtenido de https://www.funcionjudicial.gob.ec/www/pdf/normativa/codigo_organico_fj.pdf

Código Orgánico Integral Penal. (2014). *Oficio No. SAN-2014-0138.* Quito: Asamblea Nacional. Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Constitución de la República del Ecuador. (2011). *Registro Oficial 449 de 20-oct-2008.* Quito: República del Ecuador. Obtenido de http://bit.ly/2LAnpsc

Constitución Política del Perú. (1993). *Constitución Política del Perú.* Perú: Constitución Política del Perú. Obtenido de https://www.oas.org/juridico/spanish/per_res17.pdf

Convención Sobre Los Derechos Del Niño. (2006). *Convención Sobre Los Derechos Del Niño.* España: UNICEF. Obtenido de https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Convenio De Budapest Sobre Ciberdelincuencia O Convenio De Budapest. (2001). *Delitos relacionados con la pornografía infantil.* Europa: Comité de Ministros del Consejo de Europa. Obtenido de https://rm.coe.int/16802fa403

Cuadra, E. (1996). Internet: Conceptos Básicos. *revistas científicas complutenses*, 1.

Declaración Universal de los Derechos Humanos. (1948). *Asamblea General en su resolución*

217 A (III). Naciones Unidas. Obtenido de https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Díaz, A., & López, E. (2015). Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos. *Revista Médica Clínica Las Condes*, 7-13. Obtenido de https://www.elsevier.es/es-revista-revista-medica-clinica-las-condes-202-articulo-impacto-redes-sociales-e-internet-S0716864015000048

Fernández, Y. (7 de abril de 2021). *Xataca basic*. Obtenido de Xataca basic: https://www.xataka.com/basics/que-tiktok-donde-viene-que-ofrece-red-social-videos

Ferro, F. (13 de julio de 2020). ¿Cómo evitar ser víctima de delitos cibernéticos? *Noticentral*, 1-3. Obtenido de https://www.ucentral.edu.co/noticentral/como-evitar-ser-victima-delitos-ciberneticos

Galvao, R. (14 de septiembre de 2017). *Rockconten*. Obtenido de https://rockcontent.com/es/blog/herramientas-para-instagram/

García, G., Velázquez, V., Martínez, G., & Llanes, A. (2011). Ciberbullying: forma virtual de intimidación escolar. *Scielo*, 119. Obtenido de http://www.scielo.org.co/pdf/rcp/v40n1/v40n1a10.pdf

Hernández, R. (10 de Junio de 2014). *Fiscalía General del Estado*. Obtenido de Fiscalía General del Estado: https://fge.jalisco.gob.mx/prevencion-social/medidas-preventivas-para-protegerse-del-internet

Huaccha, J. (2013). Derecho a la privacidad. Delitos contra el honor y la intimidad a través de los medios de comunicación. *Revista de la comunicación*, 56.

Lenta, M., & Zaldúa, G. (2020). Vulnerabilidad y Exigibilidad de Derechos: la Perspectiva de Niños, Niñas y Adolescentes. *Anuario de investigación*, 25-36. Obtenido de https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-22282020000100106&lng=es&tlng=es

Martínez, M., Rosales, S., & Gándara, J. L. (2015). *Access Medina*. Obtenido de https://accessmedicina.mhmedical.com/content.aspx?bookid=2448&sectionid=193961431

Mejía, G. (2014). Sexting: una modalidad cada vez más extendida de violencia sexual entre jóvenes. *Perinatología y reproducción humana*, 217-221.

Ministerio Fiscal España. (2018). *Fiscalía Española*. Obtenido de https://www.fiscal.es/

Miranda, E. (25 de abril de 2021). *Diario Sur*. Obtenido de Diario Sur: https://www.diariosur.es/tecnologia/internet/fraudes-internet-menores-20210414132817-nt.html

Montserrat, R., Sánchez, X., Jordana, C., & Beranuy, M. (2007). El adolescente ante las tecnologías de la información y la comunicación: internet, móvil y videojuegos. *researchgate*, 197-199. Obtenido de https://www.researchgate.net/publication/242199439_EL_ADOLESCENTE_ANTE_LA

S_TECNOLOGIAS_DE_LA_INFORMACION_Y_LA_COMUNICACION_INTERNET_MOVIL_Y_VIDEOJUEGOS

Moreira, A. (3 de febrero de 2019). *Los riesgos de Instagram para niños y adolescentes*. Obtenido de Los riesgos de Instagram para niños y adolescentes: https://eresmama.com/los-riesgos-de-instagram-para-ninos-y-adolescentes/

Morrillo, F. (2019). La Pornografía Infantil. (e. nueva, Ed.) *Scielo.*

Olson, L. (2007). *Entrapping the innocent. Toward a theory of child sexual predator´s luring communication.* Londres: Communication Theory.

Pantallas, A. (22 de mayo de 2013). *Blog Pantallas Amiga*. Obtenido de Blog Pantallas Amiga: http://blog.pantallasamigas.net/2013/05/sexting-una-amenaza-desconocida/

Protocolo facultativo de la Convención sobre los Derechos del Niño. (2000). *Asamblea General - Resolución A/RES/54/263.* Naciones Unidas. Obtenido de https://www.ohchr.org/sp/professionalinterest/pages/opsccrc.aspx

Puyol, J. (2019). ¿En qué consiste el «child grooming» acoso sexual de menores por Internet] y qué medidas de prevención deben adoptarse? *ConfiLegal*, 1-7. Obtenido de https://confilegal.com/20190128-en-que-consiste-el-child-grooming-acoso-sexual-de-menores-por-internet-y-que-medidas-de-prevencion-deben-adoptarse/

Ramírez, H. (2021 de marzo de 2021). *Grupo Ático.* Obtenido de Grupo Ático: https://protecciondatos-lopd.com/empresas/peligros-redes-sociales/#Challenge_o_retos_muy_peligrosos_en_ocasiones_delictivos

Requena, F. (2011). Redes sociales y sociedad civil d. *Espacios Públicos, 14 (31)*, 264-268. Obtenido de https://www.redalyc.org/pdf/676/67621192015.pdf

Rocha, C. (2015). Metodología de la investigación. En C. M. Rocha, *Ciencias Sociales* (pág. 45). México: Oxford University Press. Obtenido de https://issuu.com/malurojas19/docs/56-metodologia-de-la-investigacion-carlos-i.-munoz

Romero, M. (2017). Tecnología y pornografía infantil en Colombia. *Revista Criminalidad*, 27-47. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082017000100027

Ron, N. (22 de Junio de 2014). *Introducción a la Investigación*. Obtenido de Introducción a la Investigación: http://introinvestigacion002.blogspot.com/2014/06/uso-del-internet-como-herramienta-de.html

Rubio, A. (2009). Los jóvenes y la red: usos y consumos de los nuevos medios en la sociedad de la información y la. *Signo y Pensamiento, 28*(54), 265-275. Obtenido de https://www.redalyc.org/articulo.oa?id=86011409017

Rubio, M. (2018). Agresión sexual y abuso con prevalimiento. *Revista de Derecho, Empresa y Sociedad (REDS)* (12), 82-95. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6596393

Sádaba, C., & Bringué, X. (2011). Menores y redes sociales. *static, 1*, 1-260. Obtenido de https://dadun.unav.edu/bitstream/10171/20593/1/GGII-Madrid-final.pdf

Standler, R. (8 de enero de 2002). *Computer crime*. Obtenido de http://www.rbs2.com/ccrime.htm

Subijana, I. (2008). El ciberterrorismo: una perspectiva legal y judicial. *Eguzkilore*, 169-187. Obtenido de http://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf.

UNICEF Argentina e Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo. (2011). *UNICEF*. Obtenido de https://www.unicef.org/elsalvador/media/1206/file/Manual_Internet_Segura_UNICEF_-_TIGO_2016.pdf

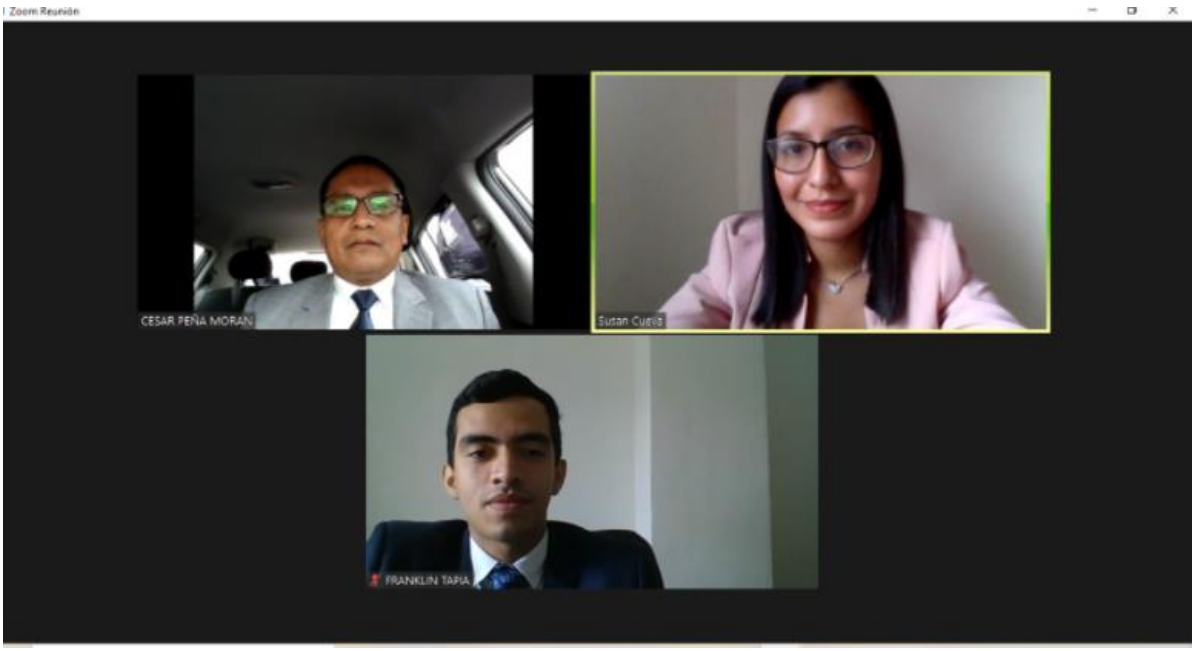
Urueña, F. (2015). Ciberataques, la mayor amenaza actual. *Instituto Español de Estudios Estratégicos*, 1-18.

Yirda, A. (5 de abril de 2021). *Concepto Definición*. Obtenido de https://conceptodefinicion.de/internet/.

ANEXOS

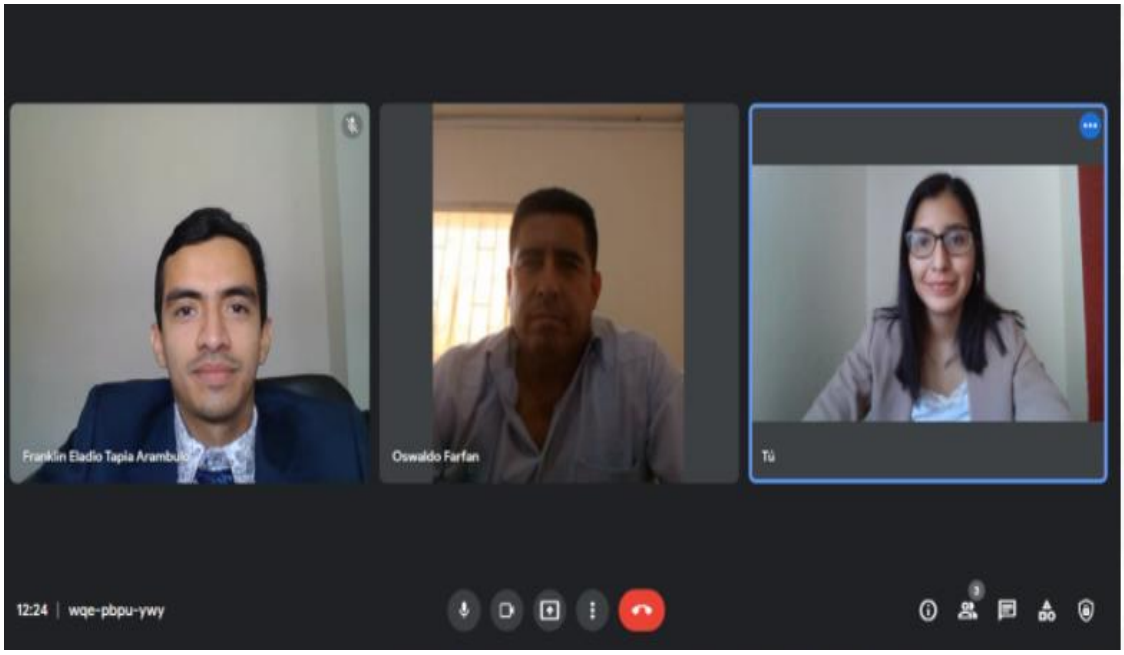
Anexo 1:

Entrevistado 1



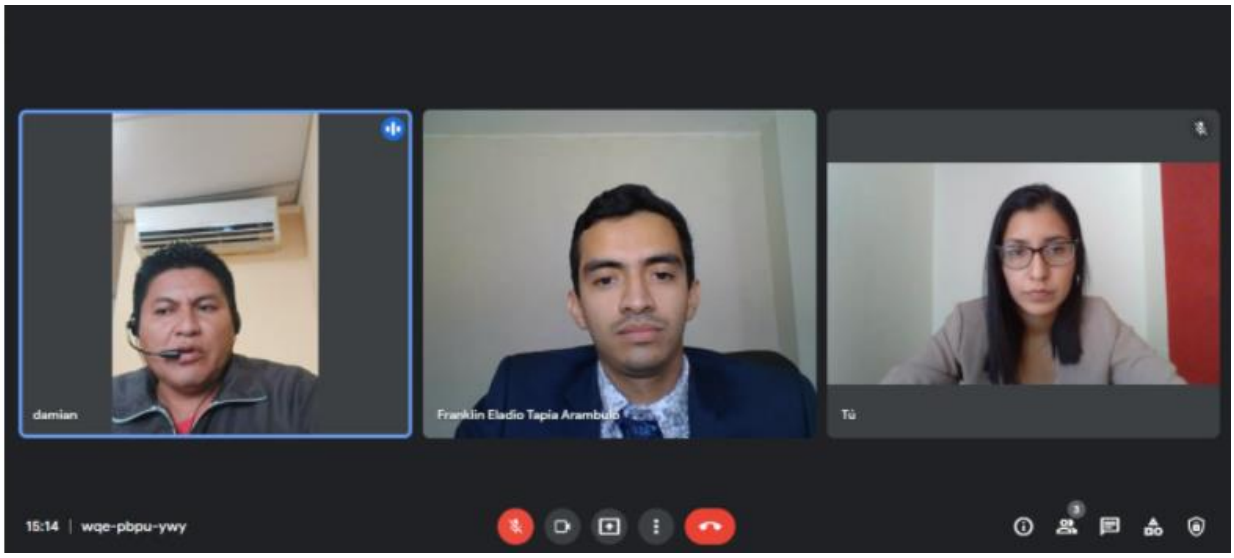
Anexo 2:

Entrevistado 2



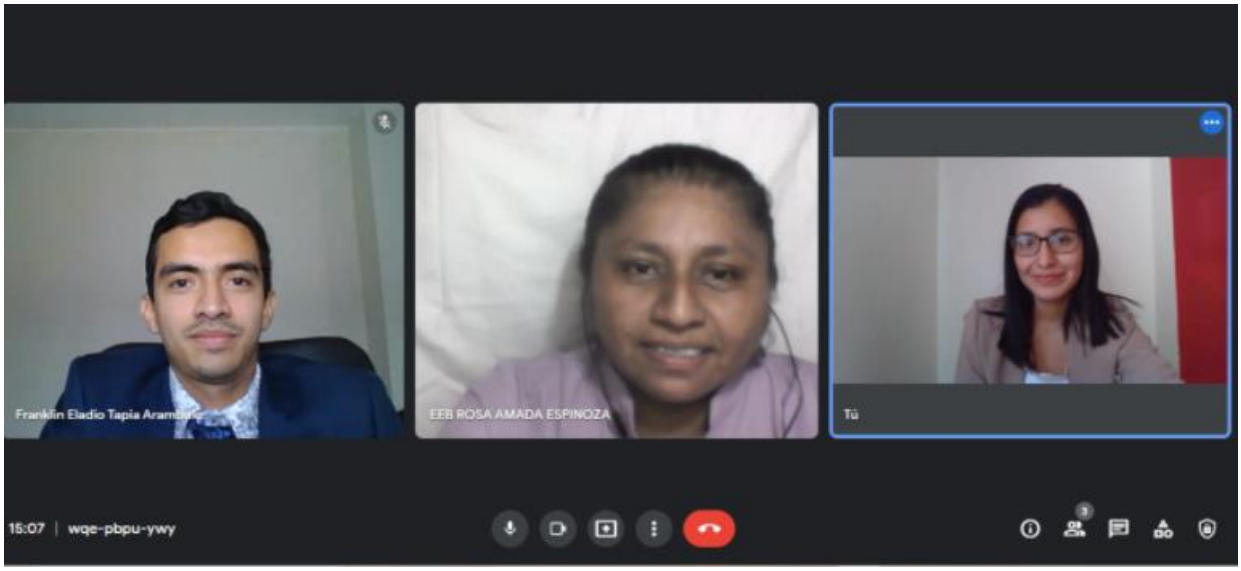
Anexo 3:

Entrevistado 3



Anexo 4:

Entrevistado 4



Anexo 5:

Entrevistado 5