FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

Propuesta de instructivo para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación, 2023 – 2024.

Profesor

Lorena Naranjo Godoy

Autores

Dayanne González Romero

Bryan Terán León

2023-2024

DEDICATORIAS

A mi hermosa hija Amelia:

Por ser la luz de mi vida y la fuerza que me impulsa a mejorar siempre. Este trabajo de titulación te lo dedico a ti, con la firmeza que te ayude como un ejemplo para perseguir tus sueños con determinación. Gracias por tu hermosa sonrisa, eres una niña inteligente, hermosa y con mucho potencial.

A mis Padres:

Por su inmenso amor, apoyo incondicional y por inspirarme a mejorar no solo en los aspectos personales, sino también como la profesional en la que me he convertido. Gracias por enseñarme el valor de la perseverancia, el trabajo duro y la transparencia.

- **Dayanne**

A mis padres, quienes con su amor incondicional y apoyo constante han sido la piedra angular en mi vida. Gracias por sus sacrificios y enseñanzas. Este logro también es suyo.

A Teresita, por su amor y apoyo inquebrantable. Gracias por tu motivación y comprensión y por ser mi mayor aliento. Tu compañía ha sido y será fundamental para alcanzar muchas metas más.

- **Bryan**

ÍNDICE

RESUMEN EJECUTIVO

El avance de las nuevas tecnologías trae consigo varios beneficios para el desarrollo académico y social como desventajas al dar apertura al cometimiento de delitos dentro del mundo digital. Los niños, niñas y adolescentes se encuentran expuestos a temas de violencia en internet debido al acceso temprano a redes sociales y la falta de capacitación en el uso adecuado de estas herramientas. A pesar de los esfuerzos por regular este desconocimiento a través de un protocolo de actuación en casos de violencia digital en el entorno educativo, no se corrobora la existencia de un claro proceso que proteja la integridad de los niños y adolescentes cuando se han convertido en víctimas, frente a contenido nocivo que los puede afectar. Por lo tanto, este proyecto de titulación tiene como finalidad plantear una propuesta para la implementación de estrategias que ayuden a la detección oportuna, prevención de repetición y bloqueo de contenido perjudicial en internet que puede causar cualquier tipo de violencia digital.

ABSTRACT

The advance of new technologies brings with it both benefits for academic and social development and disadvantages by opening the door to the commission of crimes in the digital world. Children and adolescents are exposed to violence on the Internet due to early access to social networks and the lack of training in the proper use of these tools. Despite efforts to regulate this lack of knowledge through a Protocol for action in cases of digital violence in the educational environment, there is no clear process to protect the integrity of children and adolescents when they have become victims, in the face of harmful content that may affect them. Therefore, this project aims to create mechanisms for early detection, prevention of repetition and blocking of harmful content on the Internet.

Palabras clave: violencia digital, contenido nocivo, estrategias, ciberdelitos, política criminal.

1. Introducción

1.1. Contexto Interno

El uso de las nuevas tecnologías digitales ha permitido la conexión de los niños, niñas y adolescentes a la red, y como consecuencia los riesgos para los menores ya suponen una amenaza en caso de no existir mecanismos de protección en el entorno familiar y educativo. Es por ello por lo que, este grupo que conforma el Sistema Nacional de Educación se encuentra expuesto a delitos cibernéticos, como, pornografía infantil, acoso, extorsiones, amenazas o publicación de información privada, donde evidentemente se está atentando contra su dignidad e integridad humana.

Con la finalidad de prevención, el Ministerio de Educación con ayuda de otros Organismos sin fines de lucro, desarrollaron medidas de actuación frente a situaciones de violencia digital que se pueden presentar en el Sistema Nacional de Educación. Esto con el fin de garantizar una educación de calidad, integral e inclusiva, libres de violencia de cualquier tipo. Sin embargo, del análisis realizado a las medidas de actuación, no se evidenció la manera correcta para la detección, prevención de repetición y bloqueo de contenido nocivo.

1.2. Contexto Externo

A raíz de la pandemia por COVID-19 suscitado en el año 2020, contribuyó a que los niños, niñas y adolescentes tengan mayor facilidad de acceso al internet, sea por motivos escolares o con la intención de interactuar con sus familiares o amigos. La desinformación y falta de capacitación de todos los miembros que pueden ser parte del Sistema Nacional de Educación es un factor importante frente a los riesgos a los que se encuentran expuestos los niños, niñas y adolescentes.

En la mayoría de los países del mundo, el acceso a internet ha ido en aumento con el paso de los años. Por ello, la violencia digital dentro del Sistema Nacional de

Educación ha tenido un impacto fuerte que ha afectado a este grupo por el uso excesivo e imprudente de medios tecnológicos por largas horas, sin la supervisión de los padres lo que ha ocasionado el aumento de ciberdelitos causados por los adolescentes. Ante esto, es importante tomar medidas para proteger a este grupo vulnerable a través de programas de capacitación sobre la convivencia digital y la elaboración de protocolos o instructivos de respuesta efectiva ante situaciones de violencia digital en las instituciones educativas.

El entorno económico del Ecuador influye significativamente en la prevalencia y el impacto de la violencia digital en el Sistema Nacional de Educación. Al invertir en acceso a la tecnología, recursos educativos digitales, programas de sensibilización, infraestructura e incluso políticas públicas, ayudaría de manera crucial a combatir este problema que ha impactado al desarrollo de los niños, niñas y adolescentes.

Dentro del entorno político y legal del Ecuador se ha ido presentando avances en la lucha contra la violencia digital dentro del Sistema Nacional de Educación. Sin embargo, es necesario continuar con esfuerzos para fortalecer la implementación de un marco legal más amplio e integro, en el cual, se regule y sancione los delitos relacionados a la violencia digital; más la capacitación de actores clave y la asignación de recursos, a fin de garantizar un entorno de aprendizaje seguro y libre de violencia digital para todo este grupo vulnerable.

De la misma manera, el entorno sociocultural del Ecuador presenta desafíos y oportunidades en la lucha contra la violencia digital. Abordar esta problemática requiere estrategias multisectoriales que consideren la reducción de la brecha digital, la promoción de una cultura digital responsable, la educación integral de la ciudadanía digital, el fortalecimiento de las vías de denuncia y apoyo, y el involucramiento activo de las autoridades, la familia y en sí, de la ciudadanía.

Finalmente, el entorno tecnológico en el Ecuador sigue presentando varios desafíos en la lucha contra la violencia digital. Esto debido a que, no se ha fortalecido la infraestructura tecnológica, no se ha promovido el uso responsable de las

plataformas digitales, y no se ha desarrollado competencias digitales adecuadas para los niños, niñas y adolescentes. Por ello, es necesario implementar medidas de ciberseguridad y establecer medidas humanas o herramientas tecnológicas adecuadas de monitoreo para abordar esta problemática y garantizar un entorno educativo digital seguro para todos.

2. Identificación del Objeto de Estudio

La presente investigación tiene como objeto de estudio el planteamiento de una propuesta de instructivo para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación. El periodo temporal que abarcará el presente proyecto corresponde al periodo 2023-2024.

3. Planteamiento del Problema

3.1. El problema

El uso excesivo e imprudente de las nuevas tecnologías de la información y comunicación (TIC) por parte de los niños, niñas y adolescentes, ha generado distintos tipos de violencia digital en el ámbito educativo. La falta de una legislación que regule el uso correcto de estas nuevas tecnologías es un problema que ha causado la vulneración de derechos y libertades fundamentales de las víctimas.

En el Ecuador se publicó en el año 2023 el “Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación”, el mismo que establece parámetros claros de actuación frente a casos de violencia digital que se puedan producir en las instituciones educativas a nivel nacional. Pese a ser un documento con varios lineamientos para la detección, seguimiento, derivación y reparación, no se establece correctamente como se puede detectar, prevenir la repetición y bloquear el contenido nocivo en la red. En consecuencia, es necesario que el protocolo se apoye con una política criminal para responder a una

necesidad que las entidades del Estado, unidades educativas y padres de familia buscan para que el desarrollo y la integridad de los niños, niñas y adolescentes no se vulnere.

3.2. Pregunta General de Investigación

¿Cómo diseñar una propuesta de instructivo para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación, 2023 – 2024?

3.3. Preguntas específicas de investigación

1. ¿Cuáles son los tipos de violencia digital que sufre una persona dentro del Sistema Nacional de Educación ecuatoriano?
2. ¿Cuál es el alcance y el objetivo de la detección, prevención de repetición y bloqueo de contenido nocivo dentro del Sistema Nacional de Educación?
3. ¿Cuál es el organismo competente para dictar la política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación?
4. ¿Cuáles son los recursos tecnológicos y/o humanos a observar para garantizar la detección, prevención de repetición y bloqueo de contenido nocivo?
5. ¿Cómo estructurar las estrategias para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación?

3.4. Efectos del problema

Dentro de nuestro Sistema Nacional de Educación, los actos de agresión, amenazas, intimidación, acoso, difusión de información personal o íntima, entre

otros delitos, son muy comunes en el entorno de los niños, niñas y adolescentes por el uso excesivo e imprudente de redes sociales o distintas plataformas digitales. Esto conlleva efectos perjudiciales para las víctimas y para la sociedad. Entre los efectos más comunes podemos tener el daño a la autoestima, a la integridad, aislamiento social, efectos físicos en la salud causados por el estrés y la ansiedad.

3.5. Causas del Problema

- El acceso temprano a redes sociales y a las nuevas tecnologías de la información y comunicación sin ningún tipo de instrucción, concientización o educación por parte de los padres, educadores e incluso del mismo gobierno, ha generado un uso irresponsable del internet, por parte de los niños, niñas y adolescentes.
- Por un tema de poder y control sobre otros, los adolescentes acceden al internet con la finalidad de dañar o perjudicar a personas que estos agresores consideran débiles o vulnerables.
- La desigualdad de género es una causa muy marcada dentro del uso de las nuevas tecnologías, las mujeres en su gran mayoría son el eje central de este tipo de ataques, hasta el punto de llegar a usar sus rostros para la creación de videos de carácter sexual con ayuda de la inteligencia artificial.

3.6. Escenarios

Las Tecnologías de la Información y Comunicación (TIC) han generado varios cambios en la vida cotidiana de los niños, niñas y adolescentes. La alfabetización digital debe ser importante dentro del Sistema Nacional de Educación, ya que, pese a tener un documento con lineamientos para detectar, rastrear, derivar y reparar a las víctimas, no se estableció un apartado o capítulo para la detección, prevención de repetición y bloqueo de contenido nocivo compartido en internet. Esto produciría graves consecuencias en el desarrollo integral de niños, niñas y adolescentes, por lo que es importante diseñar una política criminal que aborden el problema.

La implementación de una política criminal no solo protegería a este grupo vulnerable de los riesgos existentes por el uso inadecuado de las TIC, sino que de la misma forma promovería un entorno digital más seguro y propicio para el aprendizaje y el desarrollo personal. Es por ello, que el Ministerio de Educación debería trabajar juntamente con distintas entidades como el Ministerio de Telecomunicaciones para abordar esta problemática de manera integral para generar espacios libres de violencia digital en el ámbito educativo.

4. Revisión de la Literatura

4.1. Antecedentes teóricos del problema

La era digital en la que nos encontramos a raíz de la pandemia de COVID-19 sin duda alguna, ha permitido mayor conexión desde cualquier parte del mundo, aumentando la necesidad del uso de las redes sociales con la finalidad de mantenerse conectado casi las 24 horas del día. Si bien es cierto, esto ha generado aspectos positivos por la transformación digital a gran escala y el fácil acceso para las diferentes industrias en temas de innovación. Sin embargo, también ha generado aspectos negativos dando como consecuencia el cometimiento de diferentes tipos de violencia digital o ciberdelitos en el ciberespacio.

Actualmente, la vida de una persona depende alrededor de un 70% de la tecnología, de acuerdo con un artículo de Bit Life Media. Niños, niñas y adolescentes dependen de las (TIC) para desarrollar sus tareas y esparcimiento; el acceso no ha sido controlado debidamente por los padres, educadores, ni por el Estado, lo que ha provocado la exposición personal en las redes sociales, sin considerar la privacidad. Además, este acceso irresponsable ha dado paso a que muchos niños, niñas y adolescentes usen de manera inadecuada las TIC e incluso cometan distintos ciberdelitos.

Conforme se establece en el “Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación”, se ha

evidenciado que más de un tercio de los usuarios de internet son menores de 18 años y el 56% de las niños, niñas y adolescentes entre 15 y 24 años han experimentado algún tipo de violencia en línea. (2023, p.7).

De acuerdo con lo antes señalado, el porcentaje de personas que han sufrido algún tipo de violencia digital es alto y, por lo tanto, acarrea consecuencias fuertes en contra de las víctimas. Además, la falta de legislación en el acceso y uso adecuado de las nuevas tecnologías, así como el desconocimiento por parte de los menores en el uso adecuado del internet, genera un alto riesgo en el crecimiento del índice de violencia que se registra hasta la actualidad.

Si bien es cierto, el Ecuador busca una solución eficaz en los problemas presentados en las Unidades Educativas a nivel nacional. Por ello, el Ministerio de Educación conjuntamente con la Fundación *ChildFund* publicaron un protocolo de atención en los casos de violencia digital, pero este no incluye un apartado o capítulo donde se establezcan medidas o pasos a seguir para asegurarse que este contenido violento o nocivo no se reproduzca y se bloquee de manera permanente en la red, y así proteger la intimidad de las víctimas o afectados de estos hechos.

4.2. Marco conceptual

4.2.1. Sistema Nacional de Educación frente a la violencia digital

El Sistema Nacional de Educación Ecuatoriano es consciente de que en gran parte de las Unidades Educativas a nivel nacional en algún momento se han presentado casos de violencia digital entre los estudiantes. Por ello, se estructuró una metodología que permite evaluar las situaciones de riesgo según las escalas de leve, medio y alto, que se explica a continuación, de acuerdo con la siguiente figura:

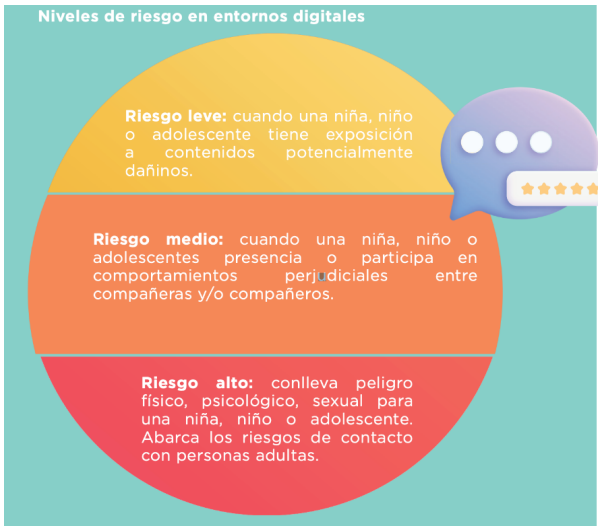


Figura 1: Niveles de riesgo en entornos digitales.

Fuente: Protocolo de actuación frente a situaciones de violencia digital detectadas en el sistema nacional de educación.

Es importante señalar que en más de un 50% la actuación de las Unidades Educativas dependerá de la denuncia realizada por la víctima o víctimas. En base a lo manifestado, dentro del protocolo en mención, se ha establecido una ruta frente a casos de violencia digital que se presenta a continuación:

Figura 2: Ruta frente a casos de violencia digital

Fuente: Protocolo de actuación frente a situaciones de violencia digital detectadas en el sistema nacional de educación.

Como se puede observar, el protocolo en mención estructuró un proceso claro y sencillo a tomar en cuenta para los casos de violencia digital que se presenten en la Unidades Educativas, señalando como punto de partida la detección del caso a través de la denuncia, sin perjuicio de la legitimación de la víctima o cualquier persona natural o jurídica que conozca de los hechos conforme señala el Código Orgánico Integral Penal (COIP).

Una vez presentada la denuncia, se tendrá que derivar a las instancias especializadas, sea el Departamento de Consejería Estudiantil (DECE), Autoridades de las Unidades Educativas y a la Fiscalía General del Estado, con la finalidad de que se dé inicio con los procesos y procedimientos establecidos en mismo protocolo, y en la normativa legal aplicable. Las Autoridades Competentes determinarán el nivel de gravedad de los hechos y definirán las acciones concretas, y la reparación integral a la o las víctimas; así lo establece el Protocolo de actuación frente a situaciones de violencia digital en el Sistema Nacional de Educación.

Del portal El Universo informaron que “en el Ecuador 4 de cada 10 adolescentes han enfrentado algún tipo de violencia digital.” (29 de septiembre 2023). Estos datos generan gran preocupación ante autoridades estatales, padres de familia, autoridades escolares, entre otros, y con esto se observa la necesidad de contar con esta ruta de atención. Actualmente se reporta un caso de relevancia en el Ecuador sobre violencia digital, el cual se detalla a continuación:

> “En un colegio privado de Quito se registró un caso se violencia digital usando la inteligencia artificial en contra de al menos 24 adolescentes de la institución, por tal motivo, la Fiscalía General del Estado apertura una investigación por el presunto delito de pornografía con utilización de niñas, niños y adolescentes.” (Ecuavisa, 5 de octubre de 2023).

De este caso, la actuación de la Fiscalía General del Estado debe ser completa y oportuna, ya que el rostro de varias adolescentes está en páginas pornográficas, redes sociales y se compartió a través de mensajería instantánea, y no se registra protección o reparación a las víctimas hasta el momento, de acuerdo con lo manifestado por su abogada defensora. En este caso, se ve afectado el derecho de imagen de las víctimas, y deberían poder ejercer su derecho de eliminación contemplado en la Ley Orgánica de Protección de Datos Personales y su Reglamento General.

4.2.2. Marco jurídico

La Constitución de la República del Ecuador; Título II: Derechos; Capítulo III: Derechos de las Personas y Grupos de Atención Prioritaria; Sección V: Niños, niñas y adolescentes, señala:

> "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.
> 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." (Ecuador, 2008).

> "Art. 45.- Las niñas, niños y adolescentes gozarán de los derechos comunes del ser humano, además de los específicos de su edad. El Estado reconocerá y garantizará la vida, incluido el cuidado y protección desde la concepción.

> Los niños, niñas y adolescentes tienen derecho a la integridad física y psíquica; a su identidad, nombre y ciudadanía; a la salud integral y nutrición; a la educación y cultura, al deporte y recreación; a la seguridad social; a tener una familia y disfrutar de la convivencia familiar y comunitaria; a la participación social; al respeto de su libertad y dignidad; a ser consultados en los asuntos que les afecten; a educarse de manera prioritaria en su idioma y en los contextos culturales propios de sus pueblos y nacionalidades; y a recibir información acerca de sus progenitores o familiares ausentes, salvo que fuera perjudicial para su bienestar.
>
> El Estado garantizará su libertad de expresión y asociación, el funcionamiento libre de los consejos estudiantiles y demás formas asociativas" (Ecuador, 2008)

> "Art. 78. - Las víctimas de infracciones penales gozarán de protección especial, se les garantizará su no revictimización, particularmente en la obtención y valoración de las pruebas, y se las protegerá de cualquier amenaza u otras formas de intimidación. Se adoptarán mecanismos para una reparación integral que incluirá, sin dilaciones, el conocimiento de la verdad de los hechos y la restitución, indemnización, rehabilitación, garantía de no repetición y satisfacción del derecho violado.
>
> Se establecerá un sistema de protección y asistencia a víctimas, testigos y participantes procesales." (Ecuador, 2008).

La Convención sobre los Derechos del Niño del 20 de noviembre de 1989 señala que: "se reconoce que los niños (seres humanos menores de 18 años) son individuos con derecho de pleno desarrollo físico, mental y social, y con derecho a expresar libremente sus opiniones." (2006, p. 6). En consecuencia, los niños, niñas y adolescentes requieren protección en su vida diaria, incluyendo su desarrollo en el mundo online, al conocer que ahora es parte fundamental del crecimiento de ellos. Además, el artículo 12 de la Convención señala:

*“*Artículo 12

1. Los Estados Parte garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño.

2. Con tal fin, se dará en particular al niño oportunidad de ser escuchado, en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional.” (2006, p. 14).

De igual manera, en el 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, señala:

“(…) Preocupados por la disponibilidad cada vez mayor de pornografía infantil en la Internet y otros medios tecnológicos modernos y recordando la Conferencia Internacional de Lucha contra la Pornografía Infantil en la Internet (Viena, 1999) y, en particular, sus conclusiones, en las que se pide la penalización en todo el mundo de la producción, distribución, exportación, transmisión, importación, posesión intencional y propaganda de este tipo de pornografía, y subrayando la importancia de una colaboración y asociación más estrechas entre los gobiernos y el sector de la Internet, se ha convenido lo siguiente:

Artículo 8

1. Los Estados Partes adoptarán medidas adecuadas para proteger en todas las fases del proceso penal los derechos e intereses de los niños víctimas de las prácticas prohibidas por el presente Protocolo y, en particular, deberán:

a) Reconocer la vulnerabilidad de los niños víctimas y adaptar los procedimientos de forma que se reconozcan sus necesidades especiales, incluidas las necesidades especiales para declarar como testigos; b) Informar a los niños víctimas de sus derechos, su papel, el alcance, las fechas y la marcha de las actuaciones y la resolución de la causa; c) Autorizar la presentación y consideración de las opiniones, necesidades y preocupaciones de los niños víctimas en las actuaciones en que se vean afectados sus intereses personales, de una manera compatible con las normas procesales de la legislación nacional; d) Prestar la debida asistencia durante todo el proceso a los niños víctimas; e) Proteger debidamente la intimidad e identidad de los niños víctimas y adoptar medidas de conformidad con la legislación nacional para evitar la divulgación de información que pueda conducir a la identificación de esas víctimas; f) Velar por la seguridad de los niños víctimas, así como por la de sus familias y los testigos a su favor, frente a intimidaciones y represalias; g) Evitar las demoras innecesarias en la resolución de las causas y en la ejecución de las resoluciones o decretos por los que se conceda reparación a los niños víctimas. (...) 5. Los Estados Parte adoptarán, cuando proceda, medidas para proteger la seguridad e integridad de las personas u organizaciones dedicadas a la prevención o la protección y rehabilitación de las víctimas de esos delitos". (2006, p. 41 – 45)

La Convención sobre los Derechos del Niño; Comité de los Derechos del Niño; Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, señala:

*"*4. Los derechos de todos los niños deben respetarse, protegerse y hacerse efectivos en el entorno digital. Las innovaciones en las tecnologías digitales tienen consecuencias de carácter amplio e interdependiente para la vida de los niños y para sus derechos, incluso cuando los propios niños no tienen acceso a Internet. La posibilidad de acceder a las tecnologías digitales de forma provechosa puede ayudar a los niños a ejercer efectivamente toda la

gama de sus derechos civiles, políticos, culturales, económicos y sociales. Sin embargo, si no se logra la inclusión digital, es probable que aumenten las desigualdades existentes y que surjan otras nuevas.” (ONU, 2021).

Ley de Seguridad Pública y del Estado, Título III: Del Sistema y de los Órganos de Seguridad Pública; Capítulo Innumerado: Consejo Nacional de Política Criminal:

> “Art. 10.1.- Consejo Nacional de Política Criminal. - El Consejo Nacional de Política Criminal es el organismo interinstitucional encargado de aprobar la política criminal, articulada al Plan Nacional de Seguridad Integral del Estado. La política criminal es el conjunto de respuestas que el Estado adopta, de manera integral e intersectorial, para prevenir y enfrentar la delincuencia y criminalidad con el fin de garantizar la protección de los intereses esenciales del Estado y los derechos de sus habitantes.” (Ley de Seguridad Pública y del Estado, 2023).
>
> “Art. 10.5.- Plan de Política Criminal. - El Plan de Política Criminal incluirá un diagnóstico del fenómeno de la criminalidad en el país y las respuestas planificadas y coordinadas a corto, mediano y largo plazo que el Estado debe adoptar para prevenirlo y combatirlo. Definirá políticas, acciones y recomendaciones dirigidas a la prevención de las causas del delito, respuestas penales para sancionarlo y mecanismos de rehabilitación y reinserción de las personas infractoras en la sociedad. El Plan de Política Criminal contendrá objetivos, metas e indicadores medibles de cumplimiento, así como, la estrategia de intervención de las entidades públicas involucradas en su ejecución. El Ente rector de la planificación estatal establecerá criterios y metodología que garanticen la evaluación integral periódica, anual y quinquenal de la Política Criminal.” (Ley de Seguridad Pública y del Estado, 2023).

Código Orgánico Integral Penal; Libro Primero: Infracción Penal; Título IV: Infracciones en particular; Capítulo Primero: Graves violaciones a los derechos humanos y delitos contra el Derecho Internacional Humanitario; Capítulo Primero:

Graves violaciones a los derechos humanos y delitos contra el Derecho Internacional; Sección Tercera: Diversas formas de explotación:

> “Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, 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.” (COIP, 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.” (COIP, 2014).
>
> “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.” (COIP, 2014)

“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.” (COIP, 2014)

“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.” (COIP, 2014)

4.2.3. Tipos de delitos en entornos digitales

4.2.3.1. Violencia Digital

La violencia digital o ciber violencia se refiere al uso de medios digitales o plataformas en línea para intimidar, acosar, amenazar o cualquier otra manera de causar daño a una persona dentro de la red. “El término de violencia digital o

violencia cibernética se refiere a un abuso repetitivo cometido por una persona o varias hacia una o varias personas utilizando un medio cibernético o digital.” (Laboy-Vélez et al., 2021).

Este tipo de violencia ha ido en aumento con el alcance que ha tenido la tecnología en los últimos tiempos. Igualmente, los niños, niñas y adolescentes que acceden a internet se exponen ante fenómenos que pueden causar efectos devastadores en su salud mental, desarrollo e integridad por el mal manejo de los dispositivos electrónicos o digitales; y acceso desmedido a plataformas sin supervisión de un adulto. No cabe duda de que, la violencia digital se ha vuelto un problema que va en aumento en el ámbito educativo.

4.2.3.2. Ciberbullying

El *ciberbullying* ha emergido como un tema muy preocupante como la manera de intimidación entre los niños, niñas y adolescentes facilitada por las tecnologías digitales que hoy tenemos. “Se trata de emplear cualquiera de las posibilidades de uso de las nuevas tecnologías de la información y de la comunicación para hostigar con ensañamiento a su víctima.” (Hernández Prados & Solano Fernández, 2012). Entre las distintas vías de acosar en redes a una persona encontramos varios tipos de ciberacoso como, por ejemplo, a través de mensajes de texto, mensajes multimedia, redes sociales e incluso vía correo electrónico.

La mayoría de los estudiantes disponen de una cuenta de correo electrónico que pudieron crearla dentro de la Unidad Educativa o en su hogar; y tienen acceso algún dispositivo electrónico que les permite ingresar a la red. Las consecuencias de este ciberdelito pueden ser graves. De hecho, los niños, niñas y adolescentes que son víctimas de aquello, pueden llegar a tener ansiedad, depresión, aislamiento e incluso pensamientos suicidas. Sin duda alguna, las escuelas deben implementar medidas que ayuden a prevenir y combatir este daño, así como brindar apoyo a los estudiantes afectados.

4.2.3.3. Grooming

El *grooming*, también conocido como *"online grooming"* (acoso y abuso sexual online), es una forma de abuso y manipulación en la que un adulto busca ganarse la confianza de un menor de edad con fines sexuales, aprovechando la conectividad y el uso de las redes sociales, mediante los dispositivos que tienen los estudiantes. Este fenómeno tiene distintos niveles de interacción y peligrosidad, desde hablar de sexo y conseguir material íntimo, hasta llegar a tener un encuentro sexual.

El diario La Vanguardia define al *grooming* como "todas las acciones deliberadas que un adulto realiza con un menor de edad con el objetivo de establecer una amistad, crear una conexión emocional con el niño, disminuir las preocupaciones del menor y así poder obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual." (La Vanguardia Barcelona, 2022). En otras palabras, el adulto que comete este ciberdelito (*Groomer*) suele aprovecharse del anonimato que ofrece el internet para crear falsas identidades y así, engañar a los niños para conseguir su objetivo final.

Por lo tanto, el Groomer termina incurriendo en un delito de pornografía infantil a través del chantaje, engaño e incluso extorsión. Por eso, es importante la prevención y educación sobre este problema en el Sistema Nacional de Educación para proteger a los niños, niñas y adolescentes.

4.2.3.4. Pornografía Infantil

La pornografía infantil es un delito donde las víctimas son niños, niñas y adolescentes, y es un problema de carácter crítico a nivel internacional. La Organización de Estados Americanos define a la pornografía infantil como "captar, preparar, entregar o controlar a un menor con el fin de crear pornografía infantil o con multas de posesión, divulgación, transmisión, exhibición o venta de pornografía infantil." (OEA, 2009). Ante esta definición, se entiende que este delito es toda representación visual o multimedia que involucre de manera real a menores de edad

en actividades de naturaleza sexual. De igual forma, esto constituye una forma inaceptable de explotación infantil y este tipo de contenido representa un abuso contra los menores y un crimen reprochable, que destruye la infancia e integridad de los más vulnerables.

4.2.3.5. Sextorsión

De la misma manera que los delitos antes mencionados, la sextorsión es un delito muy común en la era digital, donde los agresores utilizan fotos o videos íntimos de la víctima como herramienta de chantaje para extorsionar. “La sextorsión es una forma de abuso sexual infantil que consiste en amenazar con publicar material sexualmente explícito de la víctima a menos que se cumplan determinadas exigencias. Lo más habitual es que el agresor amenace con compartir imágenes sexuales de la víctima (reales o falsas) con el fin de obtener contenido sexual explícito adicional, contacto sexual con la víctima, dinero u otras exigencias.” (Allison, 2023). Este delito representa una grave violación de la privacidad y la dignidad humana contra los niños, niñas y adolescentes causando un gran daño emocional. Por ello, es importante abordar este tema, promoviendo la educación, el fortalecimiento de las leyes y la concientización para proteger a este grupo vulnerable y erradicar esta conducta abusiva.

4.2.4. Huella digital

La Autora Ana María Salas Fernández en su Proyecto de fin de carrera señala: “La huella digital es información que se encuentra en internet de un individuo o empresa, ya pueda ser en una red social, en un blog, foro o cualquier página Web”. (Salas, 2010. P, 39). Toda actividad en internet deja un rastro, cada página web que se visita queda dentro historial de los dispositivos electrónicos que se usaron.

El rastro que dejamos al utilizar la tecnología, en la actualidad beneficia al mercado tecnológico para el desarrollo de distintos proyectos, por ejemplo, el *Big Data*, la inteligencia artificial, *Bussines Inteligent*, entre otros. Se ha establecido que: “es muy

sencillo dejar una huella digital en la red, basta con poner nuestro nombre en un buscador de internet e inmediatamente sabremos qué dice o que conoce la red de nosotros.” (Vidal, 2019, p. 18).

Es muy común que las personas no consideren lo que van a publicar en sus redes sociales, ni tampoco toman en cuenta los riesgos que pueden generar. De igual manera, es común escuchar que una persona no pudo conseguir empleo porque el empleador revisó la red social y encontró videos, fotografías o incluso textos con los que se juzga al candidato y se lo rechaza.

4.2.4.1. Tipos de huella digital

El autor Vidal ha considerado que se pueden distinguir dos tipos de huella digital, se describe a continuación:

- *“*Huella digital activa: cada vez que ejecutamos una acción o compartimos algo online, es decir, si somos nosotros los que ejecutamos la acción.
- Huella digital pasiva: en el caso en que sean otros los que publican sobre nosotros.” (Vidal, p.18, 2019).

Es decir, una huella digital activa radica en el consentimiento y conocimiento por parte del usuario al momento de publicar contenido de sí mismo, los datos que se comparten no miden los riesgos; mientras más publicaciones desde el punto de vista del usuario es mejor, ya que, tendrá mayor existencia en la red. Por ejemplo, publicaciones en redes sociales, formularios en línea, correos electrónicos o juegos en línea. (Qué es la huella digital y por qué es importante, s.f.).

Mientras que, la huella digital pasiva son aquellas publicaciones que se realizan en la red sin consentimiento del titular de la información. No existe una gravedad en las acciones de terceras personas que publican sobre un titular específico, no existe tampoco una filtración de datos como tal, pero existe un riesgo inminente de

afectación al titular en su cotidianidad. (Qué es la huella digital y por qué es importante, s.f.).

4.2.4.2. Rastreo de la actividad en línea

Es vital que los usuarios protejan su información personal y de igual manera que se encuentren alertas de las publicaciones que puedan hacer terceras personas y puedan afectar al titular. Las personas se encuentran constantemente conectados a la red, no se dan cuenta lo que publican y si podría o no ser nocivo para ellos a futuro. Existe una frase típica en el Derecho Penal que señala: “Todo lo que digas, podrá ser usado en su contra”, en el caso del internet cabría la frase: “Todo lo que publicas, podrá ser usado en su contra”.

Muchas empresas suelen recabar información sobre posibles candidatos desde las redes sociales o páginas web de acceso público, lo que condiciona si se les contrata o no a partir de su pasado digital. También se ha dado casos en los cuales se recopila esta información directamente de los dispositivos y comportamientos en línea, como por ejemplo “el caso de una empresa en Londres conocida como *Cambrige Analytica* que tiene como objeto social el análisis de datos para desarrollar campañas para marcas y políticos que buscan cambiar el comportamiento de la audiencia.” (BBC, 2018).

Se expone este ejemplo, ya que, desde la red social Facebook, la empresa recopiló datos para analizar el comportamiento de los usuarios de esta red, datos supuestamente privados, con el único objetivo de inferir en perfiles psicológicos de cada usuario en las elecciones de los Estados Unidos a favor de la campaña de Donald Trump.

Los sitios web están configurados para recopilar información de los usuarios a través de dispositivos de almacenamiento o también conocidos como *Cookies*. A partir de estas, los sitios web y aplicaciones pueden indagar la actividad de los usuarios y las empresas pueden gozar de un beneficio de esta actividad guardando

preferencias, mostrar contenido personalizado y anuncios. Por tanto, los usuarios deberán ser cautelosos con las publicaciones que hagan, estando al tanto que sus datos quedan totalmente expuestos.

4.2.4.3. Reputación online

El *New York Times* en su artículo “lo que tienes que saber sobre tu huella digital y cómo se usa para rastrearte”, señala: “A pesar de asegurar los datos para no ser rastreados en línea, la industria publicitaria en internet encontrará maneras de monitorear la actividad digital de los usuarios” (8 de julio de 2019).

Los mecanismos implementados para proteger la actividad de las personas en línea no son suficientes y nunca lo serán, se debe ser consciente de que la tecnología avanza a pasos agigantados, por lo que, la mejor manera de proteger la privacidad será limitar las publicaciones en internet.

Muchos autores hablan de la marca personal y de la importancia de explotar esta de forma positiva, señalando que “es una disciplina novedosa, concluyendo que es uno de los activos intangibles más importantes de un usuario sobre todo en internet” (La reputación es uno de los intangibles más prometedores para la gestión empresarial, 2022). Los nuevos empresarios o pequeños emprendedores saben que su presencia en la red determinará el éxito o fracaso de su negocio, por lo que manejan un perfil profesional en cada red social e incluso muchos tratan de mantener su vida personal transparente para generar confianza a su clientela.

Dentro del Sistema Nacional de Educación a penas se están implementando capacitaciones que enseñe el uso adecuado de su imagen o reputación online a los estudiantes; los niños, niñas y adolescentes se exponen sin limitación alguna en redes sociales, esto con la finalidad de generar contenido que los convierte de una u otra forma en “influencers” ya que su acceso ilimitado a la red les genera la certeza de mientras más absurdo o inseguro sea el contenido, más seguidores tendrán.

4.2.5. Derecho al olvido

A lo largo del presente trabajo, se ha tratado sobre el potencial riesgo que existe por el uso inadecuado del internet, se han implementado planes de prevención para que los niños, niñas y adolescentes aprendan a usar esta herramienta de una manera adecuada. Sin embargo, a pesar de los esfuerzos que se puedan gastar para un resultado positivo, no tendrá un alcance del 100%, muchos jóvenes se quedarán y seguirán haciendo mal uso de este, como es el caso presentado en el colegio privado detallado en párrafos anteriores y también será a consecuencia de las brechas digitales que se encuentran arraigadas en la sociedad.

Una de las mejores maneras de hacerlo es mediante la solicitud e impedimento de la reproducción de videos o contenidos que perjudique su buen nombre. La Autora Verónica Astudillo, en su tesis señala: *"*el derecho al olvido o a la supresión es el derecho a poder solicitar e impedir la reproducción de información personal que se pública en medio electrónicos como el internet, cuya información de no ser la adecuada o carecer de los permisos necesarios para ser compartida de acuerdo con lo que indica la Ley." (Astudillo, 2022. p, 14)

Es decir, este derecho le da facultad y el poder a una persona de evitar que la información de cualquier tipo sea compartida, sobre todo a personas víctimas de violencia digital que tendrán la facultad de solicitar que el contenido que pueda dañar su honra y buen nombre sea eliminado o suprimido de manera inmediata de cualquier lugar en donde esta se encuentre, puede ser en un motor de búsqueda o una red social como Facebook, Instagram, WhatsApp, Telegram, entre otros.

En el caso de los niños, niñas y adolescentes, la facultad y poder para evitar que cierta información se divulgue en el internet será de los padres, ya que, tienen la representación legal del menor. Especialmente, se requerirá la intervención de los padres cuando se trate de temas de violencia digital, ya que, podrán seguir todos los procesos establecidos en la normativa interna de la Unidad Educativa.

El Derecho al Olvido en España tiene 3 objetivos específicos, que señala lo siguiente:

> "1. Desindexación de la información de las personas de los motores de búsqueda de internet; 2. Caducidad de la información digital en medios después de cierto tiempo; y, 3. Autonomía sobre su propia información en cuanto acceso y rectificación de la información publicada en internet." (Astudillo. 2022. p,15).

4.2.6. Privacidad y protección de datos personales

La privacidad se relaciona con cualquier información, como nombres completos, número de cédula, número telefónico, fotografías e incluso sus huellas digitales, así como cualquier dato personal de carácter identificativo de un titular. El uso de las tecnologías de la información y de la comunicación (TIC) ha permitido que los datos personales se utilicen para distintos fines y sin consentimiento del titular de la información. Por ello, en Ecuador se promulgó la Ley Orgánica de Protección de Datos Personales y su Reglamento General con la finalidad de establecer parámetros claros para la protección.

Dentro de esta normativa, se encuentra los derechos ARCO (acceso, rectificación, cancelación y oposición) que son un conjunto de derechos que buscan la privacidad y la protección de los datos personales, permitiendo a cada persona controlar su información personal. La Ley Orgánica de Protección de Datos Personales en sus artículos 13, 14, 15 y 16 determina lo siguiente con respecto a cada uno de los derechos:

> *"*Art. 13.- **Derecho de acceso.** - El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el

ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días […]"

"Art. 14.- **Derecho de rectificación y actualización**. - El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos. Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice."

"Art. 15.- **Derecho de eliminación. -** El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando: […] El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito."

"Art. 16.- **Derecho de oposición. -** El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos: […] El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones."

Los derechos ARCO pretenden un control de los titulares sobre sus propios datos, incluyendo conocer información de los responsables y corregir datos inexactos, bloquear datos contrarios a la legislación aplicable y pedir el cese del tratamiento de datos cuando se obtengan sin consentimiento. Los derechos ARCO son importantes para proteger la privacidad de niños, niñas y adolescentes dentro del

Sistema Nacional Educativo. Con estos, los padres pueden solicitar el acceso a los datos de sus hijos para supervisar la información que la Unidad Educativa tiene sobre ellos.

4.2.7. Uso seguro de las TIC

4.2.7.1. Seguridad informática

La seguridad informática con el tiempo se ha considerado un elemento crítico en la era digital que vivimos, ya que gran parte de nuestra información personal se encuentra en un sistema cibernético. Gabriel Baca Urbina define a la seguridad informática como *"*la disciplina que, con base en políticas, normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos a los que está expuesta*"*. Cabe decir que, la seguridad informática es una disciplina de suma importancia para proteger uno de los activos más valiosos en el mundo moderno, que es la información digital.

La seguridad informática implica la implementación de control de acceso, políticas, procedimientos, tecnologías diseñadas para proteger la confidencialidad, privacidad, integridad ante amenazas internas como externas que puedan presentarse. Implementar medidas de seguridad de la información es indispensable para proteger la información personal tanto en el ámbito privado como en las instituciones públicas y privadas, como sería en este caso, en todo el Sistema Nacional Educativo.

Dentro del contexto educativo, la seguridad informática es de suma importancia para prevenir y combatir lo que llamamos violencia digital, la cual puede manifestarse en las formas señaladas en apartados anteriores, como lo es el ciberbullying, grooming, sextorsión, pornografía infantil, filtración y robo de información personal entre

estudiantes, los cuales pueden causar problemas psicológicos y emocionales graves.

Para afrontar estas amenazas, el Sistema Nacional Educación requiere implementar medidas de seguridad informática que abarquen la educación a niños, niñas y adolescentes sobre la ciudadanía digital responsable, los peligros de compartir información y como buscar ayuda en caso de ser víctimas de violencia digital.

Una mayor conciencia y preparación en seguridad informática desde temprana edad escolar permitirá formar profesionales y ciudadanos digitales más competentes y responsables en el futuro. Es una tarea conjunta que nos permite forjar por un Ecuador más resiliente y seguro en la era digital.

4.2.7.2. Educación digital

La educación digital es indispensable dentro del Sistema Nacional de Educación ante los avances tecnológicos que se han ido presentando. Incorporar las tecnologías de la información y comunicación (TIC) en la enseñanza de los niños, niñas y adolescentes en las Unidades Educativas puede traer grandes beneficios como el desarrollo o fomento de habilidades digitales desde temprana edad.

De este modo, la integración de estas tecnologías digitales en la educación trae consigo grandes beneficios, pero también desafíos como la violencia digital. El ciberbullying y otros delitos que se pueden cometer son algunas de las amenazas que deben enfrentar las Unidades Educativas; al adoptar estas medidas preventivas, son claves para garantizar que los entornos de aprendizaje sean seguros.

Con la entrega del **“**Protocolo de Actuación Frente a Situaciones de Violencia Digital en el Sistema Nacional Educativo” en el mes de septiembre del 2023, por parte del Ministerio de Educación se han establecido políticas y directrices claras contra la

violencia digital, pero no se han determinado formas de protección o bloqueo del contenido nocivo que puede afectar a los niños, niñas y adolescentes de las Unidades Educativas, peor aún sanciones a perpetradores. Solo la concientización y acciones conjuntas permitirán aprovechar la educación digital al tiempo que se previenen daños al bienestar y reputación de los estudiantes ecuatorianos.

Hoy, la educación digital debe ser de carácter obligatorio para los estudiantes y puedan desarrollar habilidades importantes para que contribuyan a la sociedad ecuatoriana. La colaboración entre las instituciones públicas, privadas y sociedad civil es determinante para diseñar e implementar iniciativas efectivas de prevención y respuesta.

4.2.8. Formas de detección, prevención de repetición y bloqueo del contenido nocivo del internet

4.2.8.1. Formas de detección del contenido nocivo en internet

En base a la realidad actual a nivel mundial, es imperativo garantizar todo tipo de protección a los niños, niñas y adolescentes de los riesgos o amenazas a los que se encuentran expuestos en internet. A lo largo del presente trabajo se abordó temas que ayuden a entender los nuevos derechos que surgen para a favor de los niños, niñas y adolescentes frente a la grave vulneración de su privacidad, intimidad e integridad por cualquier tipo de contenido nocivo que se pueda cargar a las redes sociales y de como consecuencia un acto de violencia digital. Si bien es cierto el Protocolo de actuación frente a casos de violencia digital detectadas en el sistema nacional de educación señala un mecanismo de detectar estos casos, el cual propone:

> “El personal educativo y administrativo deberá detectar e identificar presuntos casos de violencia digital por medio de señales de alerta y/o de reportes de estudiantes, docentes, familiares o terceros, a partir de los riesgos y las vulneraciones de derechos presentes en el mundo físico que también se

> trasladan al entorno digital, como por ejemplo el acoso escolar que más adelante se podrá convertir en un caso de ciberacoso.” (Ministerio de Educación, 2023, p.39).

La propuesta del Ministerio de Educación hasta cierto punto se podrá considerar viable, ya que el estudio del comportamiento de los estudiantes podría arrojar resultados de quien puede ser víctimas de violencia digital y con ello ayudar a las autoridades, maestros e incluso padres de familia; con la finalidad de actuar de manera oportuna para la prevención o ejecución de cualquier tipo de mecanismo que salvaguarde la integridad de la víctima en el espacio físico. Sin embargo, en el espacio digital al ser víctimas de un ciberdelito (pornografía infantil, *grooming*, ciberacoso o sextorsión) no se garantiza una protección integral, puesto que, carecen de herramientas fiables que ayude a controlar a que este tipo de material se viralice en el internet, incluyendo redes sociales o incluso llegue a la *Dark Web*.

Los Prestadores de Servicios de Internet (ISP) juegan un papel importante en el otorgamiento y puesta en práctica de herramientas fiables que ayuden a detectar y controlar actos ilícitos en la red. Los ISP por la magnitud del servicio que prestan deberían contar con herramientas de monitoreo, que gestione la seguridad de los diferentes motores de búsqueda, redes sociales y páginas de internet. Se planteó incluso el uso del *Machine Learning* como una medida a implementar por los ISP y redes sociales para que detecten cualquier tipo de contenido nocivo o malicioso.

“Machine Learning supone un conjunto de modelos matemáticos y estadísticos, cuyas tareas involucran el reconocimiento, diagnóstico, control de robots, predicciones, etc.” (Rivero, 2017, p. 11). El aprendizaje automático es una herramienta técnica que puede ayudar a combatir el contenido nocivo incluido en las diferentes plataformas digitales, ya que permitirá un análisis enorme de datos de manera oportuna y eficiente, a través de la identificación de patrones y características que indiquen la presencia de contenido dañino como: pornografía infantil, grooming, entre otro tipo de ciberdelitos.

El autor Rivero señala un ejemplo del uso de *Machine Learning*:

> “Un sistema de predicción de mails spam, donde la entrada es un conjunto de mails que han sido etiquetados como spam por el humano. El proceso de aprendizaje consiste en reconocer un conjunto de palabras y características que aparecen en un spam mail. Luego, cuando un nuevo mail es recibido, se revisarán sus características y si encajan en el conjunto de contenido sospechoso, será etiquetado como mail spam. Este sistema, con una base adecuada de datos de entrenamiento, está capacitado para correctamente predecir la etiqueta de todo nuevo mail entrante” (Rivero, 2017, pp. 11-12)

Al aplicar un mecanismo de aprendizaje automático ayudará a los ISP y plataformas digitales en general, con el objetivo de iniciar una lucha contra la violencia digital generada a través de la publicación de contenido nocivo, sin embargo, esta propuesta supone desafíos al momento de garantizar un uso responsable, ético y transparente.

Un aspecto negativo señalado por el Virtual Global Taskforce (VGT) es “el lanzamiento del cifrado de extremo a extremo (E2EE) que se encuentra implementando por Meta de forma predeterminada en sus principales aplicativos como Facebook Messenger y WhatsApp.” (National Crime Agency, 2024). Este E2EE pone en jaque la actuación que pretenda realizar el Estado con la finalidad de detectar, prevenir la repetición y bloquear el contenido nocivo que genera violencia digital en el Sistema Nacional de Educación. Esto se debe a que esta herramienta permite que la información compartida entre los usuarios se convierta en simples códigos y así resguardar la información personal y privada que se comparte entre sí. Sin embargo, en caso de detectar cualquier tipo de actividad ilícita que se haya compartido, genera una mayor dificultad para los ISP y organismos estatales que tengan orden judicial para acceder a esta información por cualquier tipo de sospecha o seguridad de que se ha cometido un ilícito por medio de estas plataformas.

Finalmente, para hacer frente a este problema es importante contar con respuestas efectivas como la cooperación internacional, con el objetivo de combatir este tipo de delitos y prevenir de toda forma la consumación, siendo principal tarea del Estado regularlo de forma correcta y así que los ISP que operan legalmente en el país tengan la obligación de implementar estos mecanismos de prevención y actuación oportuna en sus redes a favor de la integridad de los niños, niñas y adolescentes.

4.2.8.2. De la repetición del contenido nocivo en internet

En la era digital que hoy vivimos, donde el intercambio de información y contenido multimedia a través de internet es masivo, existe también el riesgo de que el material nocivo se propague de manera incontrolada. Es por eso, que ciertas formas de contenido requieren ser detectadas para proteger a las posibles víctimas y mantener un entorno en línea más seguro. Ante este desafío, se han desarrollado diversas tecnologías y recursos para prevenir la repetición y distribución descontrolada de estos contenidos dañinos en la red.

Algunas soluciones por considerar son: las marcas de agua digitales, el análisis de huellas digitales y los sistemas automatizados de monitoreo y bloqueo en plataformas. Estas herramientas tecnológicas, implementadas con el instructivo que se propone, tienen el potencial de limitar significativamente la propagación de material sensible, al permitir su identificación, rastreo y bloqueo oportuna del Internet.

De acuerdo con ssori Canela Internacional (OMCI) a partir de una encuesta en la cual participaron madres y padres con hijos de 3 a 17 años se concluyó:

> “Si hablamos del uso de dispositivos para ocio, un 26,5% de los menores de entre 3 y 18 años tienen un dispositivo propio para jugar en casa. Este porcentaje aumenta con la edad y casi la mitad (44,9%) de los menores en edades de 12 a 18 años tienen un dispositivo propio para jugar. Respecto a los de 6 a 12 años, un 29,1% tiene dispositivos propios para ocio y solamente

> un 4,1% de ellos no tiene ningún dispositivo con acceso a internet dedicado a jugar en casa. Finalmente, un 93,4% de los menores de 6 años tienen dispositivos con internet dedicados al ocio en casa y un 11,3% de estos tienen uno de estos dispositivos para ellos/as solos/as. (Observatorio sobre el uso de internet en menores de edad: riesgos, beneficios y límites, 2021).

De estos porcentajes no se podría determinar que dispositivos propios tengan mecanismos de protección para los menores o control parental, lo que conlleva un riesgo latente de acceder a contenido nocivo, inapropiado o incluso ilícito. El autor Martín Peidro señaló: “Internet constituye un medio privilegiado para la transmisión de información, prescindiendo de las limitaciones de las fronteras” (2003, p. 207).

En este trabajo se reconocen varios delitos contra la integridad de menores de edad, mediante la generación de contenido perjudicial como videos de carácter sexual, el ciberbullying, entre otros; por ello varios autores han señalado que los contenidos ilícitos y nocivos son diversos, por su naturaleza y tratamiento (Peidro, 2003, p. 207). El Estado, a través del Ministerio de Educación ha pretendido dar el primer paso para iniciar a combatir contra estos ilícitos a través de la publicación de un protocolo estructurado para actuar frente a situaciones de violencia digital dirigido a la protección de niños, niñas y adolescentes del Sistema Nacional de Educación.

Este protocolo tiene como objetivo: “Establecer lineamientos de actuación para todas las personas que conformen la comunidad educativa, con el fin de garantizar la prevención, detección, intervención, derivación, seguimiento y reparación frente a situaciones de violencia digital detectadas o cometidas en el sistema educativo”. (2023, p. 12). Si bien es cierto, se establece varios pasos para la prevención y actuación dentro del Sistema Nacional de Educación, sin embargo, este no cuenta con un proceso claro a seguir de cómo debería ser el actuar de las autoridades en los sistemas informáticos que reproducen este tipo de contenido con violencia digital, se requiere un instructivo o proceso claro que ayude a la protección integral de las víctimas.

Los menores tienen acceso ilimitado a internet y muchos de ellos no han sido educados para el uso correcto, ni mucho menos tienen limites o restricciones de las páginas a las que acceden. Aunque depende de la educación que los padres den a los niños, mucho de estos tampoco se conocen de protocolos de seguridad que activan en sus computadores, de ahí nace la necesidad de capacitar a los padres de familia. Por ejemplo, un padre que se encuentre correctamente informado de los peligros a los que expone a su hijo al publicar fotografías de estos sin restricciones, evitará este tipo de publicaciones, siempre que conozcan del tema.

La Organización Mundial de la Salud (OMS) que establece lo siguiente:

> “Cada año 200 millones de niños sufren abusos sexuales. Gran parte de estos abusos se dan en línea o se captan y distribuyen digitalmente. La base de datos de INTERPOL sobre explotación sexual infantil contiene más de 1,5 millones de imágenes y vídeos, que registran colectivamente el abuso de más de 19400 víctimas en todo el mundo. Se reconoce que esas cifras son solo una pequeña fracción de todo el Material de Abuso sexual de niños, niñas y adolescentes (CSAM por sus siglas en inglés Child Sexual Abuse Materials) disponible, y que gran parte permanece sin detectar.” (Los peligros de navegar por internet para los niños, 2023)

Los datos publicados por la OMS en su material sobre abuso sexual infantil son impactantes y da a lugar una serie de cuestionamientos sobre qué acciones han tomado los Estados para prevenir efectivamente este tipo de abusos contra menores de edad; en el mismo artículo en referencia señala:

> “Según la Internet Watch Foundation (IWF), la víctima suele tener entre 11 y 13 años (55%) o menos de 10 años (39%) (solo el 5% tiene entre 14 y 15 años). La mayor parte del material CSAM representa a niñas (78%), mientras que los niños sólo están representados en el 17% (el 4% representa a ambos sexos). Casi una cuarta parte de todo el CSAM en línea en 2018 (23%) fue

> del tipo más grave, incluidas imágenes de violación y tortura.” (Los peligros de navegar por internet para los niños, 2023)

Es así como, en el protocolo de actuación de acuerdo con las cifras a las que ha tenido acceso ha visto la importancia de distinguir claramente las situaciones de riesgo o violencia entre pares y violaciones de derechos cometidas por personas adultas:

> “Las situaciones entre pares se refieren a problemas entre compañeras y/o compañeros de la institución, en las que participan niños, niñas y adolescentes. Aquí se puede incluir situaciones de riesgo de nivel leve o medio, que pueden abordarse a través de prácticas restaurativas como parte de acciones educativas disciplinarias. No obstante, cuando se trate de un caso de violencia, no aplican estas prácticas, conforme con lo establecido en el Reglamento de la Ley Orgánica de Educación Intercultural.
>
> Por otra parte, las situaciones perpetradas por una persona adulta contra niños, niñas y adolescentes pueden involucrar formas sofisticadas de violencia en línea que constituyen en su mayoría delitos y deben ser denunciadas.” (Protocolo de actuación frente a casos de violencia digital en el Sistema Nacional de Educación, 2023, p. 31-32).

4.2.8.3. Bloqueo del contenido nocivo en Internet

Las medidas de protección que puedan garantizar un tipo de alivio o reparación para las víctimas de violencia digital se han transformado en un eje fundamental al desarrollo del presente trabajo. Internet Society señala que “las autoridades nacionales utilizan el bloqueo por políticas públicas para restringir el acceso a información o servicios relacionados que es ilegal en una jurisdicción determinada, y se considera una amenaza al orden público.” (Internet Society, 2017, p. 7). Con lo mencionado, se entiende que los gobiernos cuentan con mecanismos tecnológicos que ayudan a bloquear páginas web que a los gobiernos no les conviene que sus

ciudadanos accedan, un ejemplo bastante claro es China por la habilidad de bloquear el uso del buscador Google o WhatsApp. Se entiende que al existir estos mecanismos, que muchas veces vulneran el derecho constitucional a la libertad de expresión, podría ser utilizado para garantizar una protección integral a víctimas de violencia digital a causa de contenido nocivo.

Los niños, niñas y adolescentes no siempre son conscientes de los peligros que existen en el internet, no saben cómo responder a amenazas que existen en la red; por ello, como solución a este problema se ha planteado un plan de alfabetización digital dirigido al Sistema Nacional de Educación. Sin embargo, a pesar de contar con esta medida de prevención, sigue existiendo la posibilidad de acceder a cierto contenido inapropiado y también son vulnerables a ser víctimas en estos contenidos.

Internet Society también menciona en su investigación que “muchos países tienen el deseo de bloquear cualquier tipo de contenido inapropiado para evitar el acceso de menores de edad y también evitar el acceso de cualquier persona a materia de abuso infantil.” (Internet Society, 2017, p. 7). Varios gobiernos pretenden poner en marcha un plan seguro para proteger a las víctimas mediante política criminal y así dar lucha de manera eficazmente a los ciberdelitos.

En un país como Ecuador, en donde “77% de las niñas y jóvenes participantes indicó que ellas u otras niñas que conocen han experimentado alguna forma de violencia en línea de manera frecuente (50%) y muy frecuente (27%).” (Ecuador, 2020), es más complicado implementar herramientas efectivas para proteger a los niños, niñas y adolescentes. Sin embargo, a partir de la Ley de Seguridad Pública y del Estado, con el señalamiento de emitir una política criminal, se puede convertir en una realidad. Lo único que se requiere es una propuesta efectiva que pueda combatir este problema tan arraigado, que acontece principalmente dentro del Sistema Nacional de Educación.

En este punto, es importante hacer referencia a la necesidad de la colaboración no solo internacional, sino de los Proveedores de Servicios de Internet y Plataformas de redes sociales, ya que estos dos por la magnitud del servicio que poseen, también cuentan con formas de bloquear la información que puede ser perjudicial, de manera efectiva. Por ejemplo, en Facebook al encontrar un contenido con cualquier tipo de índole sexual, te da la opción de realizar un reporte que de manera instantánea desaparece de la vista del perfil denunciante, pero este ingresa en un análisis profundo para validar si infringe o no con las Normas comunitarias establecidas por la plataforma y saber si hay necesidad de bloquear de manera definitiva.

4.2.9. La política criminal como política pública dirigida al Sistema Nacional de Educación

La necesidad de dar frente al crimen en el Ecuador se ha hecho fundamental para garantizar la protección del Estado y de los ciudadanos. Es así como la Asamblea Nacional adoptó la postura de construir y adecuar un plan de política criminar con la finalidad de combatir la inseguridad que existe. Por ello, se define a la Política Criminal como: “un tipo de política pública que contiene el conjunto de respuestas que el Estado adopta, de manera íntegra e intersectorial, para prevenir y enfrentar la delincuencia y criminalidad, y así garantizar la protección de los intereses esenciales del Estado y los derechos de sus habitantes.” (Asamblea Nacional Del Ecuador, 2023).

La postura del poder legislativo es el más adecuado frente al aumento de la delincuencia hasta la fecha actual; los ciudadanos exigen al Estado adoptar medidas eficaces para proteger su integridad y seguridad. Las reformas que se realice a la normativa penal vigente no son suficientes para combatir todos los sucesos que se han estado presentando en los últimos tiempos, siendo conscientes que el objetivo del derecho penal es de acción no de prevención.

Conforme al párrafo anterior, se entiende que es obligación del Estado en general proteger los derechos de sus ciudadanos, incluyendo a los niños, niñas y adolescentes; no solo en el ámbito físico, ya que, es importante recordar sobre la existencia de delitos que ocurren en el ciberespacio, en el cual, en su gran mayoría perjudica a los menores de edad por la falta de información del uso correcto del internet.

El Ministerio de Justicia y del Derecho de Colombia se encargó de levantar un informativo dirigido a sus ciudadanos sobre ¿Qué es la Política Criminal?, en este se establece los elementos con el cual deberá contar la Política criminal y señala: “1. Es una especie de política pública; 2. Esta se encarga de la prevención y reacción del delito, y hace frente a las consecuencias; y, 3. Es una respuesta frente a comportamientos desviados”. (Cita, Cuesta, Lozano, Osorio, Pérez y Velásquez, 2015, p. 4).

Lo señalado en este documento es realmente importante, ya que se requiere el levantamiento urgente de la política que regule en el Ecuador un procedimiento claro en donde se establezca los pasos a seguir cuando exista una publicación de contenido nocivo que causa cualquier tipo de violencia digital en el Sistema Nacional de Educación, considerando que, en la Ley de Seguridad Pública y del Estado señala claramente que se planteará solución de manera intersectorial con la finalidad de prevenir y enfrentar la delincuencia, a partir de la evaluación de las consecuencias y comportamientos que tengan los agresores en línea.

Una vez que se ha declarado la necesidad de una política fuerte que prevenga y de frente al crimen, es importante señalar quien será el organismo encargado de estructurarla, para ello en la Ley de Seguridad Pública y del Estado manda la creación del Consejo Nacional de Política Criminal que se conformará por parte de un delegado del Presidente de la República, así como de autoridades ministeriales y de organismos de justicia que se requiere su participación en base a los conocimientos que estos manejan.

5. Objetivo General

Diseñar una propuesta de instructivo de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación, 2023 – 2024.

6. Objetivos Específicos

1. Identificar los tipos de violencia digital que sufren los niños, niñas y adolescentes dentro del Sistema Nacional de Educación del Ecuador.
2. Establecer el alcance y el objetivo del diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación.
3. Identificar el organismo competente para dictar la política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación.
4. Definir los recursos tecnológicos y/o humanos a observar para garantizar la detección, prevención de repetición y bloqueo de contenido nocivo.
5. Estructurar las estrategias para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación.

7. Justificación y aplicación de la metodología

7.1. Nivel de estudio

La metodología de investigación a emplear será el método descriptivo, el cual guiará a definir de manera precisa los conceptos, lineamientos y descripción de eventos o situaciones relacionadas a la violencia digital en el Sistema Nacional de Educación. Esto con el objetivo de estructurar y desarrollar de manera adecuada un instructivo para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el

Sistema Nacional de Educación. Dicho instructivo servirá para dar apoyo al "Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación", convirtiéndose en una valiosa herramienta para abordar esta problemática de forma efectiva.

7.2. Modalidad de investigación

La investigación para el desarrollo de este instructivo tendrá un enfoque documental y estará orientada a la creación de un producto específico que ayudará en la detección, prevención de la repetición y bloqueo de contenido nocivo para niños, niñas y adolescentes en internet. Además, se realizará una recopilación y selección de las mejores técnicas de prevención de repeticiones y bloqueo de contenido nocivo a través de la lectura y análisis de tesis, libros, revistas científicas, videos, instructivos y otros recursos relevantes. Así, se obtendrá un sólido sustento teórico y práctico que permita desarrollar un instructivo efectivo y actualizado para abordar el problema dentro del Sistema Nacional de Educación.

7.3. Método

El método por utilizarse en el presente proyecto será deductivo, ya que, iremos de lo general a lo específico, permitiendo a través del análisis de casos reales que se han presentado de violencia digital; la efectividad de una política criminal para dar apoyo al actual "Protocolo de Actuación Frente a Situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación" y así lograr la detección, prevención de repetición y el bloqueo de contenido nocivo que puede causar cualquier tipo de violencia digital en el Sistema Nacional de Educación.

7.4. Protocolo de investigación

Para el correcto desarrollo del presente proyecto de titulación se desarrollará con los parámetros establecidos en la metodología SCRUM, ya que al ser un método de trabajo ágil permitirá abordar de forma eficiente el acceso a información y correcto

desarrollo del trabajo. Está metodología también proporcionará un plan de valores, roles y pautas a seguir que permitirá un desarrollo correcto y rápido de la propuesta de instructivo para el diseño de una política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación.

8. Propuesta de solución del problema identificado

En este trabajo se abordó una problemática que en la actualidad afecta a los niños, niñas y adolescentes que son parte del Sistema Nacional de Educación, sobre la seguridad que tienen en la red. Los derechos han sido vulnerados en varias ocasiones, y nadie ha garantizado que estos sean restituidos de manera inmediata y eficaz, principalmente hablando en cuanto a ciberdelitos (*grooming,* pornografía infantil, *sextorsión*, ciberbullying). La Autora Edith Rivera señala: “el contenido que todo usuario encuentra mientras accede a la web puede aprovecharse como información valiosa para el usuario que lo obtiene, sin conocer las intenciones que pueda tener en cuanto a los datos a los que accedió.” (2017, p. 4).

En el punto 4 de este proyecto se abordó sobre delitos a los que se exponen los menores, estos se tendrán en cuenta para la solución del presente trabajo, por lo cual se detalla a continuación:

Tabla 1. Ciberdelitos

DELITO	DEFINICIÓN	MUNDO OFFLINE	MUNDO ONLINE
Grooming	Acaso para solicitar contenido sexual a un menor.	Comienza con un adulto que se acerca a un menor con intenciones sexuales.	Acercamiento y manipulación de un adulto hacia un menor a través de internet, con el objetivo de abusar

			sexualmente de este.
Sextorsión	Chantaje para no enviar o publicar contenido sexual de la víctima.	Una persona que mantiene una relación de confianza o una amenaza física.	Se produce a través de plataformas digitales, donde chantajistas amenazan en divulgar imágenes o videos íntimos para que la víctima cumpla sus demandas.
Pornografía Infantil	Representación visual o multimedia de menores de edad en conductas sexuales.	Producción y distribución de videos con contenido sexual de manera física.	Internet facilita la difusión y acceso a material ilegal relacionado con menores.
Ciberbullying	Aquella persona que mediante el uso de las TIC acosa, amenaza, insulta o humilla a otra de manera repetida.	El acosador puede comenzar en persona y extenderse al mundo digital.	Se manifiesta a través de plataformas en línea, como redes sociales o mensajes de texto.

Fuente: Elaboración propia

Los daños que se puede causar a un niño, niña o adolescente a causa del cometimiento de un delito tendrá un impacto negativo en su vida cotidiana sea que este se perpetre en el mundo offline u online. Se planteó encontrar soluciones para resarcir estos daños, no solo desde un aspecto psicológico, sino garantizando la no repetición de contenido que sea perjudicial en el libre desarrollo de los menores. El autor Jorge Calderón señala: “Frente a un caso de vulneración de derechos humanos, como la integridad de la persona, el Estado tendrá la obligación de reparar daños tanto materiales como inmateriales, además deberá investigar los hechos que originaron esta violación, sancionar a los responsables, entre todas las demás necesarias para restituir el daño a la víctima, familiares o beneficiarios. (Calderon, 2005, p. 16).

En los casos de violencia digital generada por cualquier tipo de contenido nocivo, no es suficiente la reparación económica. Recordemos que existen diversas formas de resarcir un daño desde la perspectiva internacional: “otro elemento que señala y es de relevancia para el Derecho Internacional, es que para ser justa y equitativa una reparación debe ser pronta, adecuada y efectiva” (Calderón, 2005, p. 16-17). Es decir, se requiere una evaluación exhaustiva del daño causado, con la finalidad de aplicar un resarcimiento del daño efectivo y que satisfaga la integridad de la víctima.

8.1. Creación de un Instructivo para el levantamiento de una política criminal dirigida al Sistema Nacional de Educación.

A partir de la reforma realizada en el 2023 a la Ley de Seguridad Pública y del Estado, se estableció la creación de un Consejo Nacional de Política Criminal este organismo tendrá como objetivo planificar, supervisar y dar seguimiento a la política criminal del Ecuador. Además se encargará de señalar el ente rector que se hará cargo del cumplimiento de la misma.

Un aspecto importante en el desarrollo de esta política, es que la normativa señala que deberá ser intersectorial, es decir que el diseño de esta debe involucrar diferentes actores y sectores de la sociedad, no solo a las entidades del sistema

penal tradicional. Esto permitirá una comprensión casi exacta del fenómeno que se presenta, además favorece la implementación de medidas y estrategias oportunas y protege a los ciudadanos.

En base a ello, se propone la creación de un instructivo para el diseño de una política criminal, que se dirija al Sistema Nacional de Educación, en la cual se incluirá las diferentes perspectivas que existen en entorno a los peligros en la niñez y adolescencia frente a su desarrollo integral en el ámbito educativo. Con ello, se podrá conocer las causas, los factores de la delincuencia, pero sobre todo la manera correcta de actuar.

Esta política estará atravesada por tres factores importantes:

- El objeto de intervenvión, es decir a quien se encuentra dirigido la norma, que en este caso será para el Sistema Nacional de Educación frente a la protección integral de los niños, niñas y adolescentes víctimas de violencia digital. (Cita, Cuesta, Lozano, Osorio, Pérez y Velásquez, 2015, p. 5)
- Los medios que se escogen la intervención, que será a partir de la detección, prevención de repetición y bloqueo de contenido nocivo que produce violencia digital. (Cita, Cuesta, Lozano, Osorio, Pérez y Velásquez, 2015, p. 5)
- Los fines que persigue con el catálogo de medidas de la política, que es este caso es la protección integral de los derechos de los niños, niñas y adolescentes en el Sistema Nacional de Educación, que han sido vulnerados a causa de cualquier forma de violencia digital. (Cita, Cuesta, Lozano, Osorio, Pérez y Velásquez, 2015, p. 5)

8.1.1. Detección del contenido nocivo en internet

Se vuelve imperativo conocer oportunamente cuando el derecho de algún menor se ve afectado, la necesidad de reportarlo de manera inmediata por parte de cualquier víctima de violencia digital por alguno de los ciberdelitos explicados anteriormente, esto permitirá una actuación rápida por parte de los colegios y de las personas

adecuadas. Existen diferentes maneras de conocer esta vulneración, y para dar solución al problema planteado, se detallará a continuación:

8.1.1.1. Denuncia de la víctima

La denuncia impuesta por parte de la víctima dirigido a autoridades competentes, autoridades educativas, padres de familia y terceros cercanos a la víctima será fundamental para conocer si existe algún tipo de contenido que este dañando o dañó su integridad. Podrá ser verbal o escrita, e incluso podrá imponerse ante la Fiscalía o no, dependiendo de las decisiones que tome la víctima en ese momento, lo imperativo será conocer para iniciar un plan para evitar que se siga afectando sus derechos.

8.1.1.2. De los proveedores de plataformas como redes sociales

Para detectar cualquier tipo de contenido nocivo en contra de niñas niños y adolescentes dentro de redes sociales existen dos mecanismos a los que se debe poner énfasis e importancia para su correcto uso. “Los usuarios tienen al alcance la información de sus pares relacionados, así como notificaciones de la información que ha sido publicado por estas o que terceras personas publican por estas” (Rivero, 2017, P. 5-6). En el caso que estos usuarios llegasen a tener acceso a videos, fotografías o publicaciones que afecta a la integridad y buena honra de una persona, pueden denunciar y bloquear ese contenido casi de manera inmediata.

En el caso de menores de edad que forman parte del Sistema Nacional de Educación, podrán activar las actuaciones previstas en el Protocolo de actuación frente a casos de violencia digital detectadas en el Sistema Nacional de Educación. Pero para el tratamiento de este tipo de contenido deberán aplicar medidas adicionales. Por ejemplo, Facebook e Instagram incluyeron en sus sistemas formas de denunciar contenido inapropiado o malicioso, que de manera inmediata desaparece de la vista del usuario denunciante. Pero en caso de contener imágenes o mensajes explícitos de menores de edad ingresan en un proceso de evaluación para bloquear el acceso del mismo de toda la red social.

Estas redes sociales cuentan con “normas comunitarias y mecanismos de moderación para evitar contenido malicioso, sin embargo, muchos contenidos pasan de manera desapercibida debido al volumen de contenido subidos” (pornografía en Facebook, 2024). Por ello se hace imprescindible la colaboración de los usuarios y el reforzamiento de medidas de seguridad implementadas por parte de estas redes sociales, por ejemplo, con el uso del filtrado de contenido o incluso con la implementación técnicas de machine Learning.

MathWorks señala que *Machine Learning* “es una técnica que forma parte de la Inteligencia Artificial, que enseña a los equipos informáticos a aprender de la experiencia a partir de los datos, sin depender de una ecuación predeterminada como modelo” (MathWorks, s/n). Al incluir está técnica permitirá una detección fiable y mucho más rápida de contenido que pueda perjudicar sobre todo a un niño, niña o adolescente, y esto permitirá que sus respuestas sean más certeras.

De acuerdo con el mismo portal web MathWorkS, *Machine Learning* “emplea dos tipos de técnicas: aprendizaje supervisado, que entrena un modelo con datos de entrada y salida conocidos para predecir salidas futuras; y aprendizaje no supervisado que identifica patrones ocultos o estructuras intrínsecas en los datos de entrada” (MathWorks, s/n). Es viable que la herramienta pueda ser entenada con la finalidad de dar pelea al contenido malicioso que encontramos en estas plataformas, sin embargo, no serán al 100% confiables ya que existirá un margen de error, por tema de sesgos y cometimiento de errores, que se deberá estipular en el margen de error que estas podrían cometer.

8.1.1.3. De la responsabilidad en general

La cantidad de información que se pública diariamente a nivel mundial es muy grande, tener un control efectivo es muy complicado, por lo que, cada Gobierno se encuentra en la obligación de generar medidas que puedan actuar eficazmente contra contenido que general cualquier tipo de daño a la integridad de la persona, sobre todo en materia de la niñez y adolescencia. Además de los proveedores de redes sociales, existen otros actores que se requiere su compromiso constante con

la lucha frente a estos casos, y si bien es cierto es complicado regularlo, se requiere implementar requisitos básicos como obligación para estos.

Tenemos en primer lugar a los buscadores, muchos han determinado que no pueden ser responsables de lo publicado diariamente en su espacio, ya que no pueden ejercer un control eficaz y efectivo diario de toda la información que se encuentra, además señalan que: “los buscadores -en tanto intermediarios y no productores de contenidos- no son responsables, salvo que, debidamente notificados, no actúen con diligencia para bloquear el acceso –por su intermedio- a dichos contenidos- y que el factor de atribución es subjetivo” (Molina, 2015, p. 4).

Si bien es cierto, estos no podrán responder por todo el contenido, probablemente tratar de prevenir a través de la filtración por palabras clave e inclusión de Inteligencia Artificial podría ayudar a que se detecte con mayor rapidez cualquier clase de contenido nocivo. Sin embargo, el Estado no se encuentra en la facultad de ordenar ese tipo de implementación. Es en este punto, donde interviene la participación de los proveedores de servicios de internet, ya que será un punto clave para la detección, prevención de repetición y bloqueo de contenido nocivo con enfoque especial en niños, niñas y adolescentes.

La filtración del contenido permite regular y controlar el acceso a contenido específico. *AirDroid Parental Control*, señala que:

> “El filtrado de contenido utiliza técnicas para evaluar y administrar el contenido en internet de forma efectiva. El procedimiento comienza con un sistema de restricción del contenido, el cual típicamente intercepta todo el tráfico de Internet entrante y saliente a nivel de red. El sistema analiza las direcciones de las páginas webs, palabras claves, y características del contenido usando criterios y reglas predefinidas para determinar si el acceso debería permitirse o denegarse. Las listas negras incluyen términos o páginas webs inapropiadas o dañinas, mientras que las listas blancas contienen webs fiables y permitidas”. (AirDroid Parental Control, 21 de diciembre del 2023).

Por ejemplo, la filtración de contenido podría combatir con la publicación y descarga de material de pornografía infantil, al utilizar la lista negra incluyendo términos utilizados generalmente por pedófilos que buscan obtener este contenido, esta tipología se puede obtener a partir de una investigación en el campo, en la cual seguramente se llegarán a encontrar hasta con un “manual para pedófilos” que guía a este tipo de persona a como encontrar contenido con menores de edad.

Conforme al derecho comparado, muchos países han señalado que los proveedores de servicios de internet no tienen la obligación de supervisar constantemente lo que se publica o almacena en internet, sin embargo, si tendrían la obligación de actuar de manera eficaz una vez se enteren de lo sucedido, a partir de una notificación, denuncia o con el solo hecho de conocer el suceso. La Corte Suprema de Justicia de la Nación (Argentina) señaló: “a pesar que no existe previsión legal, y es clara la ausencia de una regulación legal específica, conviene sentar una regla que distinga nítidamente los casos en que el daño es manifiesto y grosero.” (Molina, 2015, p. 5).

Por lo tanto, es importante que los proveedores de servicio de internet creen métodos internos que al conocimiento de un caso de contenido nocivo los guíe como actuar frente a plataformas de redes sociales, generadores de contenido e incluso contra los buscadores a partir de un trabajo conjunto y seguimiento, para efectivizar el bloqueo y prevenir la repetición a partir de descargas de este contenido.

8.1.1.4. **De la Colaboración Internacional**

A nivel internacional se presentan retos mucho más fuertes para encontrar resoluciones adecuadas en cuanto a delitos cibernéticos, aún más cuando estos delitos involucran niños, niñas y adolescentes. La tecnología avanza a pasos agigantados y algunos Estados se encuentran mucho más preparados para abordar estos temas frente a otros más pequeños. También existen organizaciones como la INTERPOL que cuenta con especialistas y tecnología necesaria que puede ayudar a los países a la resolución oportuna de estos casos.

El Gobierno ecuatoriano tiene la obligación de hacer mayor énfasis en buscar alianzas estratégicas que fortalezcan la resolución de casos de violencia digital, con un mayor enfoque en prevención de repetición y bloqueo de contenido nocivo que se cuelga diariamente en internet; al contar con estas alianzas permitirá que el Ecuador tenga mayor efectividad en la lucha de ciberdelitos.

El Ecuador como miembro activo en la INTERPOL cuenta con el apoyo de este organismo con “soporte operacional e investigativo, inteligencia cibernética y análisis, forense digital e investigación” (Proaño, 2018, p. 221). Esta participación puede ser muy útil frente a la lucha contra ciberdelitos, principalmente los que afectan a niños, niñas y adolescentes.

Si bien es cierto Ecuador forma parte de un “Programa de asistencia contra el Crimen Transnacional Organizado (PAcCTO), el cual tiene como finalidad la cooperación internacional para buscar la seguridad y justicia en toda América Latina, abordando toda la cadena penal desde una perspectiva integral” (El PAcCTO, s/f). Este convenio suscrito por Ecuador ha permitido identificar la falta de una legislación específica en temas de ciberseguridad de acuerdo con lo señalado en el informe emitido en el 2017. Este problema no afecta solo al territorio ecuatoriano, sino también a otros países como Argentina, Chile, Colombia.

Estos países vecinos han tomado acción frente a esta falta de legislación y han suscrito acuerdos internacionales como es el Convenio de Budapest sobre la Ciberdelincuencia en América Latina, el cual fomenta la cooperación internacional. Sin embargo, el Ecuador a pesar de ser consciente sobre las falencias en legislación penal frente a ciberdelitos no ha tomado medidas efectivas para que la colaboración internacional se fortifique y de una verdadera lucha contra delitos que afectan a niños, niñas y adolescentes.

8.1.2. Prevención de repetición del contenido nocivo en internet

La protección de los niños, niñas y adolescentes en el entorno digital es un desafío crucial en la era actual. Con el aumento del uso de Internet y las redes sociales, el riesgo de exposición de contenido nocivo se ha vuelto alarmante.

En este contexto, es importante que se implementen medidas eficaces para prevenir la repetición y propagación de este tipo de material. Una de las soluciones a considerar es el uso de huellas digitales, marcas de agua, entre otro tipo de herramientas tecnológicas, que permitirán identificar y rastrear el origen del contenido de manera única e inequívoca. Este enfoque innovador no solo ayudará a mitigar la difusión de material nocivo, sino que también promoverá un entorno en línea más seguro y protegido para este grupo vulnerable.

Al abordar este desafío, el Sistema Nacional de Educación deberá comprometerse a participar activamente para salvaguardar el bienestar y el desarrollo sano de las generaciones futuras en el mundo digital. A continuación, se explicará a detalle sobre las herramientas tecnológicas que será de apoyo para prevenir el contenido nocivo que se puede encontrar en el internet:

8.1.2.1. Huella digital

Como lo hemos indicado en capítulos anteriores, la huella digital se refiere a una identificación única e inequívoca que se asigna a un archivo digital, como una imagen, video o documento. La huella digital es el rastro que cada persona deja al navegar por el internet. Es por esto, que la huella digital se encuentra compuesta por: datos públicos, datos publicados por otros y datos que genera cada persona.

En respuesta a como se recopilan los datos de la huella digital; los datos se almacenan a través de las “cookies”. Las cookies son “una cadena de letras y números, sin ningún significado intrínseco que un sitio web envía a su navegador web. Esta información permite a los proveedores de servicios de internet vincular

todas las acciones realizadas por un usuario y convertirlas en un hilo conectado". (*¿Qué es la huella digital en internet?*, 2020).

Las cookies desempeñan un rol fundamental para mejorar la experiencia del usuario en internet. Por ejemplo, al acceder frecuentemente a una página web, las cookies almacenadas permiten que la carga sea más ágil en comparación con visitar un nuevo sitio web. Estas pueden contribuir a incrementar la seguridad de las transacciones individuales realizadas en línea.

Como ya lo mencionamos, la huella digital de una persona comprende información de carácter público a la cual puede acceder diversos actores. En manos de ciberdelincuentes por así llamarlos, el acceso a datos sensibles y hasta a ese contenido nocivo de niños, niñas y adolescentes podría derivar en escenarios no deseados con consecuencias de gravedad considerable. Por eso, se deberían adoptar medidas para gestionar la huella digital. Alexandra Roiba, columnista del periódico español "*La Vanguardia*" sostiene que para reducir la huella digital en internet tenemos que tomar en cuenta lo siguiente:

> "Revisar la huella digital. El primer paso consiste en descubrir, por medio del uso de los motores de búsqueda, cuáles son los datos que se encuentran actualmente disponibles. Así se podrán iniciar los procesos pertinentes para tratar de eliminarlos si es lo que se desea.
> Desactivar las cookies de terceros. Así se evitará que hagan seguimiento de la actividad del usuario.
> Cuidado con las redes sociales. Antes de compartir contenido, o incluso de crear una cuenta en estas, habrá que tener en cuenta cómo afectará esto a la huella digital.
> Usar varios navegadores. De esta manera lo que se consigue es evitar que toda la información personal se concentre en un solo perfil.
> Crear contraseñas seguras. Además, hay que recordar cambiarlas de forma regular para aumentar su capacidad de protección.

Reducir el número de aplicaciones en el smartphone. Muchas de ellas exigen datos, registran la ubicación y recopilan información, por lo que será mejor mantenerlas en un límite fácil de controlar.” (Roiba, 2023)

8.1.2.2. **Marcas de agua**

Las marcas de agua (watermarking) son una técnica que se utiliza para insertar información adicional de manera imperceptible en archivos digitales como imágenes, videos o documentos. Esta información adicional puede ser un identificador, un logotipo o cualquier otro dato que permita identificar la propiedad, la autenticidad o el origen del contenido digital. “El marcado de agua digital es la técnica de embeber información en un contenido digital conocido como “host” o “anfitrión” con el objetivo de protegerlo contra la manipulación o uso ilegal.” (Vargas et al., 2016)

Las marcas de agua, lejos de ser una simple técnica de protección de derechos de autor, han evolucionado hasta convertirse en una herramienta versátil para la aplicación en diversos ámbitos como los que se detallan a continuación:

a. Protección de derechos de autor

Una de las aplicaciones más frecuentes de las marcas de agua digitales es la protección de los derechos de autor sobre contenidos multimedia como imágenes, vídeos o documentos. Las técnicas de marcado de agua permiten la inserción de información relativa a la propiedad intelectual dentro del propio contenido multimedia, dotando a dicha información de la solidez requerida para resistir distintos tipos de procesamiento sobre el archivo marcado.

b. Rastreo de distribución

Las marcas de agua se pueden utilizar para rastrear la distribución de contenido digital. Al insertar ésta de forma única en cada copia del contenido, el propietario puede rastrear dónde se ha distribuido el contenido y quien lo ha accedido. Con el

método *fingerprinting* que “es una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de identificarlo, singularizarlo y, de esa forma, poder hacer un seguimiento de la actividad del usuario de este con el propósito de perfilarlo.” (Agencia Española Protección Datos, s/f) Gracias a este método, si alguna persona realiza la distribución ilegal del archivo adquirido, se podrá identificar al responsable.

c. Autenticación de documentos

Al incrustar una marca de agua en las imágenes o documentos servirá para autenticar los mismos, con el fin de verificar su autenticidad y así, evitar su falsificación o prevenir la repetición del contenido nocivo que se haya subido la internet.

De igual forma, dependiendo el grado de resistencia que se necesite para la marca de agua ante algún tipo de modificación o alteración que se le haga al archivo, las marcas de agua se pueden clasificar en:

- **Robustas**

Las que pueden detectar o recuperar la marca de agua insertada en la imagen después de que esta se haya modificado o alterado.

- **Frágiles**

Altera o destruye al modificar la imagen en la que se inserta, para poner en evidencia los cambios realizados en ella.

En función de la percepción por parte de las personas, las marcas de agua pueden clasificarse en:

d. Marcas de agua visibles

Son aquellas que se encuentran a plena vista sobre la imagen. Esta puede ser cualquier información o elemento gráfico que identifique al autor o propietario del contenido.

e. Marcas de agua invisibles

Al contrario de las anteriores, son las que no son visibles, pero puede detectarse con alguna herramienta especializada para generar mayor seguridad y protección, ya que permite rastrear y verificar la autenticidad de la imagen.

8.1.3. Bloqueo del contenido nocivo en internet

Un objetivo compartido con la mayoría de los países es restringir el acceso de las personas a contenido nocivo y limitar la disponibilidad de este material en la red. Uno de los principales desafíos que enfrentan las autoridades al buscar el bloqueo de contenido nocivo en internet es la naturaleza transfronteriza de quienes proveen dicho contenido a los usuarios.

Muchas técnicas de bloqueo de contenido nocivo en la red pueden utilizarse en diferentes puntos como a nivel nacional cuando así lo ordena una política pública. Ante esto, se describen tres tipos de bloqueo de contenido que ayudarían de alguna manera a que el material nocivo no siga circulando por la red, ya que, estos apuntan a intervenir en el ciclo habitual de búsqueda y recuperación de información por parte de los usuarios, entre ellos, el uso de motores de búsqueda y visualización de información con navegadores web. Los tipos de bloqueo de contenido son:

1. Bloqueo basado en el protocolo y en la IP
2. Bloqueo basado en la inspección profunda de paquetes (DPI)
3. Bloqueo basado en URL

En el primero, se implementa un dispositivo en la red que restringe el acceso bloqueado de direcciones IP específicas o determinadas. “El bloqueo basado en la IP coloca barreras en la red, como firewalls, que bloquean todo el tráfico hacia un

grupo de direcciones IP. El bloqueo basado en el protocolo utiliza otros identificadores de red de bajo nivel, como el número de puerto TCP/IP, que pueden identificar una aplicación específica en un servidor o un tipo de protocolo de aplicación.” (Internet Society, 2017). Este método no bloquea directamente el contenido, sino el tráfico a direcciones IP o a puertos TCP/IP conocidos que están asociados a determinado contenido. Este método tiene una eficiencia limitada, debido a que, suele resultar sencillo cambiar las direcciones IP y reubicar el contenido para evadir el bloqueo. Solo es eficaz cuando el agresor que publica el contenido nocivo no busca eludir el bloqueo activamente.

El segundo, se instala un dispositivo en la red que bloquea el acceso a contenidos específicos mediante la detección de palabras clave. “El bloqueo basado en la inspección profunda de paquetes usa dispositivos entre el usuario final y el resto de Internet para filtrar por contenido, patrones o tipos de aplicaciones específicos.” (Internet Society, 2017). Este método de bloqueo es eficaz cuando la información bloqueada es fácil de caracterizar e ineficaz cuando se requiere realizar el bloqueo general, como, por ejemplo, *“bloquear contenido nocivo de niños, niñas y adolescentes”* o cuando existe cifrado.

El tercero, implementa un dispositivo en la red que intercepta las solicitudes web y las compara con una lista de URL bloqueadas, denegando el acceso a las que coincidan con dicha lista. “En el bloqueo basado en URL, el dispositivo de bloqueo tiene una lista de las URL que debe bloquear. El intento de ver cualquier URL de la lista ocasionará una interrupción. El bloqueo basado en URL puede arrojar falsos positivos y falsos negativos. Si la intención de un editor es evitar el filtro, a menudo lo consigue con un simple cambio en el nombre del archivo o del servidor.” (Internet Society, 2017). Aunque es un método muy utilizado para restringir el acceso a categorías generales de información, tiene dificultades para bloquear paginas nuevas y servidores web con cifrado, que logran evadir el filtrado fácilmente.

Estos métodos para bloquear contenido nocivo en el internet pueden llegar a ser más eficaces mediante la cooperación de algunas herramientas tecnológicas como el filtrado de contenido web, firewalls, antivirus o antimalware, controles parentales e incluso la ayuda de la inteligencia artificial.

El bloqueo del contenido nocivo se convierte en una prioridad fundamental para salvaguardar el bienestar físico, emocional y psicológico de los niños, niñas y adolescentes del Ecuador. Mediante la utilización de los tipos de bloqueo de contenido, el apoyo de herramientas tecnológicas, la colaboración entre las instituciones del Estado, unidades educativas, los padres de familia e incluso la cooperación internacional es posible crear un espacio en línea seguro y protegido, donde este grupo de niños, niñas y adolescentes puedan explorar y aprender sin temor a ser expuestos a contenidos perjudiciales.

8.1.4. Estrategias para el bloqueo de contenido

En referencia a la colaboración internacional, con la ayuda de la INTERPOL, que busca trabajar para bloquear y retirar del internet el material nocivo, una de sus estrategias es el bloqueo de acceso a dominios de internet que puede difundir todo este material. Con esto, ayudaría a que se detenga la revictimización de los niños, niñas y adolescentes afectados. La autoridad competente puede dar con los proveedores de servicios de internet una lista de los dominios o páginas web para bloquear sus redes. Cuando el usuario quiera acceder a este contenido nocivo de niños, niñas y adolescentes, puede desviarse a una página donde lance una advertencia e información sobre las razones por las que se está redirigiendo.

Otra estrategia para el bloqueo de contenido consiste tener en cuenta el sistema *Baseline* que maneja la INTERPOL. Este sistema “permite a socios del público y de los sectores público y privado reconocer, denunciar y retirar de sus redes material conocido relacionado con abuso sexual de menores” (INTERPOL, s/f). Este sistema aprovecha la colaboración internacional y tecnología para identificar, denunciar y

bloquear contenido nocivo de niños, niñas y adolescentes, protegiendo a este grupo y apoyando las investigaciones contra los delitos de violencia digital.

8.2. Herramientas tecnológicas para la detección, prevención de repetición y bloqueo de contenido nocivo.

Como fuente de apoyo para la detección, prevención y bloqueo de contenido nocivo, la protección contra este material maligno en la red es una preocupación creciente en la era digital, donde la presencia de malware, phishing y otro tipo de amenazas es omnipresente. Para abordar esta problemática, se han desarrollado una variedad de herramientas tecnológicas especializadas en la detección, prevención de repetición y bloqueo de contenido dañino. Como, por ejemplo, las siguientes:

Tabla 2. Herramientas tecnológicas de apoyo para bloqueo de contenido nocivo

Tecnología	Definición	Beneficio
Filtros de contenido Web	Filtra las aplicaciones web a las que acceden los usuarios y restringe el acceso a sitios web o contenido nocivo o inapropiado.	- Se logra un control sobre el contenido accesible. - Se garantiza una gestión adecuada del contenido y su seguridad.
Software antivirus y antimalware	**Antivirus** es aquel software que se instala para detectar, proteger y eliminar amenazas en el sistema informático de un dispositivo. **Antimalware** es una solución que ayuda a proteger los archivos de malware como troyanos, spyware, gusanos, ransomware, entre otros.	- Ambos ayudan a detectar, escanear, proteger y eliminar cualquier software maligno.

Firewalls	“Es un dispositivo de seguridad de la red que monitorea el tráfico de red (entrante y saliente) y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.” (*¿Qué es un firewall?*, s/f)	- Ayuda a bloquear las conexiones no deseadas de usuarios no autorizados y de data maliciosa.
Herramientas de control parental	Son aquellas que ayudan a los padres a controlar el uso de internet y de dispositivos electrónicos, y evitan el acceso de los niños, niñas y adolescentes a contenidos nocivos o inapropiados en la red.	- Bloquea el acceso del niño, niña o adolescente a contenidos inapropiados dentro de la red.
Inteligencia Artificial (IA)	“Es la capacidad de un sistema informático de imitar funciones cognitivas humanas, como el aprendizaje y la solución de problemas.” (*¿Qué es la inteligencia artificial?*, s/f)	- La IA ofrece beneficios reales que abarcan casi todos los ámbitos.

Fuente: Elaboración propia

Al implementar estas herramientas tecnológicas brindará un apoyo adicional a los tipos de bloqueo de contenido para mejorar la seguridad y la protección de los sistemas informáticos y en sí, a los niños, niñas y adolescentes para que puedan tener un entorno digital más seguro, y una educación de calidad, integral e inclusiva, libres de cualquier tipo de violencia.

9. Conclusiones

a. El ciberespacio ofrece una gran cantidad de beneficios para la humanidad en general, sin embargo, dentro de este se han desarrollado nuevas técnicas para delinquir, poniendo en riesgo la integridad de varias personas, incluyendo grupos vulnerables que no se encuentran formados correctamente sobre el buen uso y los riesgos que trae consigo el internet.
b. El Ecuador cuenta con un protocolo de atención frente a casos de violencia para el Sistema Nacional de Educación, sin embargo, este no ha sido socializado correctamente y existe desconocimiento por varias instituciones educativas de cuál sería la forma correcta de poner en marcha los planes de capacitación que se establecen como mecanismos de prevención y formación para los niños, niñas y adolescentes.
c. Se identifica que en el Ecuador existe una brecha digital bastante grande, ya que se evidencia la falta de interés por parte de los gobiernos otorgar capacitaciones específicas en el uso correcto y riesgos del internet dirigido a los niños, niñas y adolescentes, así como a padres de familia, profesores y autoridades de instituciones educativas. Esto conlleva a que incluso los padres no puedan tomar acción en sus hogares para prevenir y detectar oportunamente cuando sus hijos pueden o son víctimas de delitos digitales y actuar adecuadamente.
d. A pesar de contar con un protocolo de atención en casos de violencia digital con enfoque en el Sistema Nacional de Educación, este carece de una estrategia efectiva para atender ciberdelitos que atentan contra la integridad de niñas, niños y adolescentes, que aseguren que cualquier tipo de contenido nocivo sea detectado y bloqueado oportunamente dentro de ciberespacio.
e. El Sistema Judicial Ecuatoriano no está preparado en un 100% para atender oportunamente ciberdelitos de cualquier clase, ya que carecen de un procedimiento claro y eficaz que los guíe en la investigación, dando como resultado la necesidad de levantar un proceso el cual conlleve tiempos de

cumplimiento, así como herramientas tecnológicas que les ayude con la investigación y protección integral de la víctima.

f. La normativa penal ecuatoriana reconoce ciertos delitos informáticos como la pornografía infantil, ataque a sistemas electrónicos, entre otros; sin embargo, existen falencias al momento de identificar y categorizar los diferentes tipos de ciberdelitos que existen por la falta de experiencia y formación de los profesionales que colaboran en las instituciones públicas como Fiscalía General del Estado, Ministerios y en general el Consejo de la Judicatura, siendo necesario reconocer que no existe una protección integral a las víctimas de estos delitos, sobre todo a los niños, niñas y adolescentes, a pesar de ser un grupo vulnerable reconocido en la Constitución.
g. El legislador ecuatoriano conoce sobre la existencia de la cibercriminalidad a partir de la identificación de ciertos actos que se cometen dentro del ciberespacio y con ayuda de este, sin embargo, no reconoce que el alcance de estos actos delictivos es amplio y con tendencia a un crecimiento que para futuro podría ser difícil de controlar. Por este desconocimiento, los legisladores solo han incluido en normativa penal delitos que hacen referencia al cometimiento de delitos por el internet, sin categorizar adecuadamente cuales podrían ser.
h. La vía adecuada para proteger la integridad de la víctima frente a situaciones de violencia digital en las cuales se generen o presenten cualquier tipo de contenido nocivo, será a partir del levantamiento de una política criminal enfocada a la protección de los niños, niñas y adolescentes en el Sistema Nacional de Educación frene a situaciones de violencia digital, que le ayudé a conocer los parámetros claros para la detección del contenido, prevención de repetición y bloqueo de contenido nocivo que afecte sus derechos fundamentales.
i. Las huellas digitales y las marcas de agua son herramientas básicas y fundamentales para contrarrestar la propagación de contenido nocivo en la red y evitar su reproducción indebida. Estas técnicas posibilitan el

reconocimiento y seguimiento del contenido original, facilitando su remoción de plataformas digitales y la identificación de quienes lo generan y divulgan, a fin de tomar las acciones correspondientes.

j. La incorporación de herramientas tecnológicas avanzadas, la colaboración entre distintos actores, educación digital y actualización continua es fundamental para proteger efectivamente a los niños, niñas y adolescentes del contenido nocivo en línea y que se consuma algún tipo de ciberdelito.

10. Recomendaciones

a. Es importante tipificar delitos informáticos en contra de los niños, niñas y adolescentes con principal enfoque en el Sistema Nacional de Educación, para ello se requiere presentar un proyecto de reforma al Código Orgánico Integral Penal, en el cual se detalle las justificaciones del caso.
b. Es fundamental un abordaje integral que combine esfuerzos legales, tecnológicos y educativos para proteger de manera efectiva a niños, niñas y adolescentes en el entorno digital.
c. Es importante contar con el apoyo incluso de las empresas proveedores de servicios de internet, quienes deberán regular internamente su actuación en casos de violencia digital en contra de niñas, niños y adolescentes, otorgándoles un trato especial frente a la vulneración de derechos.
d. Es importante mantener un equipo especializado de fiscales, jueces y agentes investigadores con formación en materia de delitos informáticos con principal enfoque en niñas, niños y adolescentes, así como al grupo poblacional vulnerable. Esta experticia permitirá que las causas de violencia digital sean procesadas correctamente, a partir de la comprensión de complejidades legales y técnicas que envuelven estos delitos, optimizando así los procesos de investigación, persecución y sanción.
e. Es necesario estructurar un plan de capacitación permanente dirigido a fiscales, jueces y agentes investigadores en temas de ciberdelitos. Estos planes deben abarcar aspectos legales técnicos, que aseguren a los

profesionales se mantengan actualizados con las últimas tendencias y herramientas en la lucha contra este tipo de delitos.

f. Es crucial adoptar un enfoque de protección centrado en las víctimas, en este caso en observancia a los niños, niñas y adolescentes, atendiendo oportunamente las necesidades que tienen y el tratamiento adecuado que se le debe dar en casos de violencia digital. Esto implica priorizar la protección de los menores dentro del ámbito digital, garantizando un trato digno y respetuoso.
g. Es importante iniciar con un análisis adecuado en cuanto a la suscripción por parte del Ecuador al Convenio de Budapest dirigido para América Latina, ya que este ayudará con el fortalecimiento del marco nacional ecuatoriano para combatir adecuadamente el cibercrimen, podrá mejorar las capacidades de la justicia ecuatoriana para investigar adecuadamente un delito cibernético, se podrá solicitar ayuda internacional no sola para la investigación también para la implementación de herramientas tecnológicas que protejan a la víctima de manera integral frente a casos de violencia digital y contenido nocivo.
h. Es importante promover la coordinación y colaboración entre las autoridades del Estado, organismos internacionales como la INTERPOL, organizaciones sin fines de lucro, instituciones educativas, y en sí de la ciudadanía para abordar las consecuencias que conlleva un mal manejo del internet, desde un enfoque multidisciplinario y garantizar la protección efectiva de los derechos de los niños, niñas y adolescentes del Ecuador.
i. Será importante que se regule normativamente o por autoridad competente la manera correcta de aplicar el mecanismo de actuaciones fiscales urgentes en todos los aspectos que detalla el Código, ya que esto otorgará una guía más estructurada para su correcta aplicabilidad y evitar posibles daños a derechos y libertades fundamentales.
j. Es importante que las plataformas digitales, navegadores y dispositivos electrónicos integren herramientas tecnológicas efectivas que permitan

bloquear y restringir el acceso a contenido nocivo o dañino para niños, niñas y adolescentes.

11. Referencias bibliográficas

L. (2003). Los contenidos ilícitos y nocivos en internet. *Revista Chilena De Derecho Informático*, (3). https://doi.org/10.5354/rchdi.v0i3.10670

¿Qué es la huella digital y por qué es importante. (s/f). AVG SIGNAL. Recuerado el 11 de abril del 2024, de https://www.avg.com/es/signal/what-is-a-digital-footprint

¿Qué es la inteligencia artificial? | *Microsoft Azure*. (s/f). Recuperado el 26 de mayo de 2024, de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-artificial-intelligence

¿Qué es Machine Learning?. (s/n). MathWorks. Recuperado el 9 de junio del 2024, de https://la.mathworks.com/discovery/machine-learning.html#:~:text=Machine%20Learning%20emplea%20dos%20tipos,en%20los%20datos%20de%20entrada.

¿Qué es un firewall? (s/f). Cisco. Recuperado el 26 de mayo de 2024, de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Agencia Española Protección Datos. (s/f). *Estudio Fingerprinting o Huella digital del dispositivo*. https://www.aepd.es/guias/estudio-fingerprinting-huella-digital.pdf

Astudillo, V. (2022). El derecho al olvido: Análisis y propuesta para su implementación en Ecuador. Universidad Católica de Santiago de Guayaquil: Guayaquil – Ecuador. http://repositorio.ucsg.edu.ec/bitstream/3317/19976/1/T-UCSG-PRE-JUR-DER-MD-444.pdf

Ayuda a las mujeres supervivientes a la violencia de género y violencia digital | AEPD. (2023, septiembre 15). https://www.aepd.es/areas-de-actuacion/recomendaciones

BBC Mundo. (2018). 5 claves para entender el escándalo de Cambrige Analytica que hizo que Facebook perdiera US$37.000 millones en un día. https://www.bbc.com/mundo/noticias-43472797

Calderon, J. (2005). Reparación del daño al proyecto de vida por violaciones a derechos humanos. Editorial Porrúa. México. https://www.corteidh.or.cr/tablas/24484-1.pdf

Cita, R; Cuesta, A; Lozano, S; Osorio, D; Pérez, A; y Velásquez, A. (2015). ¿Qué es la política Criminal? Colombia. Recuperado el 5 de junio del 2023, de https://www.politicacriminal.gov.co/Portals/0/documento/queespoliticacriminal-ilovepdf-compressed.pdf

Comisión Europea. (2018). Recomendaciones (UE) 2018/334 de la Comisión de 1 de marzo de 2018 sobre medidas para compatir eficazmente los contenidos ilícitos en línea. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018H0334

Corte Constitucional del Ecuador. (2018). Reparación Integral: análisis a partir de la jurisprudencia de la Corte Constitucional del Ecuador. http://bivicce.corteconstitucional.gob.ec/bases/biblo/texto/2018_RI/RI.pdf

De Terwangne, C. (2012). Internet Privacy and the Right to Be Forgotten/Right to Oblivion. *IDP Revista de Internet Derecho y Política*, *0*(13), 53. https://doi.org/10.7238/idp.v0i13.1400

Delitos informáticos y menores de edad. (2021). Peritos-informáticos. https://peritos-informaticos.com/blog/delitos-informaticos-y-menores-de-edad/

Delitos informáticos. (s/f). Recursos. Educación. https://recursos.educacion.gob.ec/art2/

Ecuador, A, N. (2023). Ley de Seguridad Pública y del Estado.

Ecuador, A.N. (2008). Constitución de la República del Ecuador.

Ecuador, A.N. (2014). Código Orgánico Integral Penal.

Ecuador, A.N. (2021). Ley Orgánica de Protección de Datos Personales.

El 70% de la población española tiene dependencia a la tecnología: estas son sus consecuencias. (2023, mayo 3). Bit life Media.

https://bitlifemedia.com/2023/05/el-70-de-la-poblacion-espanola-tiene-dependencia-a-la-tecnologia-estas-son-sus-consecuencias/

En Ecuador 4 de cada 10 adolescentes han enfrentado algún tipo de violencia digital *Ecuador | Noticias | El Universo*. (s.f.) Recuperado 8 de junio de 2024, de https://www.eluniverso.com/noticias/ecuador/violencia-digital-ninos-adolescentes-educacion-protocolo-proteccion-casos-riesgo-nota/

Hernández Prados, M. Á., & Solano Fernández, I. M. (2012). CIBERBULLYING, UN PROBLEMA DE ACOSO ESCOLAR. *RIED. Revista Iberoamericana de Educación a Distancia*, *10*(1). https://doi.org/10.5944/ried.1.10.1011

Internet Society. (2017). Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión General. https://www.internetsociety.org/wp-content/uploads/2017/09/ContentBlockingOverview_ESLA.pdf

Internet Society. (2017). *Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión general*. 12. https://www.internetsociety.org/wp-content/uploads/2017/09/ContentBlockingOverview_ESLA.pdf

Internet Society. (2017). *Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión general*. 14. https://www.internetsociety.org/wp-content/uploads/2017/09/ContentBlockingOverview_ESLA.pdf

Internet Society. (2017). *Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión general*. 16. https://www.internetsociety.org/wp-content/uploads/2017/09/ContentBlockingOverview_ESLA.pdf

Interpol. (2024). Metaverso: una perspectiva de aplicación de la ley. Casos de uso, delitos, ciencia forense, investigación y gobernanza. Recuperado el 9 de junio del 2024, de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Radicalizacion-ciberataques-y-ciberenganos-pederastas-INTERPOL-alerta-sobre-los-metadelitos

INTERPOL. (s/f). *Bloqueo y categorización de contenido*. Recuperado el 8 de mayo de 2024, de https://www.interpol.int/es/Delitos/Delitos-contra-menores/Bloqueo-y-categorizacion-de-contenido

La política criminal que propone la Asamblea prevé la coordinación interinstitucional del Estado para combatir y prevenir delitos. (2023). Asamblea Nacional del Ecuador. Recuperado el 5 de junio del 2024, de https://www.asambleanacional.gob.ec/es/noticia/86383-la-politica-criminal-que-propone-la-asamblea-preve-la

La reputación es uno de los intangibles más prometedores para la Gestión empresarial. (2022, febrero). Ethic. https://ethic.es/2022/02/la-reputacion-es-uno-de-los-intangibles-mas-prometedores-para-la-gestion-empresarial/

Laboy-Vélez, L., Ríos-Steiner, A. I., & Flores- Suárez, W. (2021). La violencia digital como amenaza a un ambiente laboral seguro. *Fórum Empresarial*, *26*(1), 99–112. https://doi.org/10.33801/fe.v26i1.19494

Lara, J. y Vera, F. (s/n). Responsabilidad de los prestadores de servicios de internet. Chile. Recuperado el 5 de junio del 2024, de https://www.derechosdigitales.org/wp-content/uploads/pp03.pdf

Lo que tienes que saber sobre tu huella digital y como se usa para rastrearte. (2019, julio 8).The New York Times. https://www.nytimes.com/es/2019/07/08/espanol/fingerprinting-internet-web-aplicaciones.html

Marínoms

Ministerio de Educación. (2023). Protocolo de actuación frente a situaciones de violencia digital ecuador 2023. https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/protocolo_frente_a_violencia_digital.pdf

Molina, E. (2015). Responsabilidad de los buscadores por contenidos publicados en internet. https://jndcbahiablanca2015.com/wp-content/uploads/2015/09/Molina-Quiroga_DA%C3%91OS.pdf

Normas comunitarias Facebook. (2024). Facebook. https://www.facebook.com/help/477434105621119

Observatorio sobre el uso de internet en menores de edad: riesgos, beneficios y lpimites. (2021). Montessori Caneral Internacional. Recuperado el 3 de abril de 2024, de: https://www.montessoricanela.com/observatorio-sobre-el-uso-de-internet-en-menores-de-edad-riesgos-beneficios-y-limites/

Organización de las Naciones Unidas. (1998). Convención sobre los Derechos del Niño. https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Organización de las Naciones Unidas. (2000). 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. https://www.ohchr.org/es/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

Organización de las Naciones Unidas. (2021). Observación general núm. 25 (2021) relativa a los derechos de ls niños en relación con el entorno digital. https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12

Proaño, G. (2018). La necesidad de incorporar al agente encubierto cibernético en la legislación ecuatoriana. Universidad San Francisco de Quito. file:///Users/dayanne/Downloads/administrator,+iuris_022_014.pdf

Rivero, E. (2017). Detección de contenido malicioso mediante técnicas de Machine Learning en las redes sociales. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0560_RiveroE.pdf

Salas, A. (2010). Extractor web de huella digital. Universidad Carlos III de Madrid. https://core.ac.uk/download/pdf/29402257.pdf

Technological Tipping Point Reached in Fight Against Child Sexual Abuse. (2014, abril 22). National Crime Agency. Recuperado el 5 de junio de 2024, de

https://nationalcrimeagency.gov.uk/technological-tipping-point-reached-in-fight-against-child-sexual-abuse

Urbina, G. B. (2017). Introducción a la seguridad informática. Grupo Editorial Patria.

Vargas, L. M., Payer, E. V. de, & Gianantonio, A. D. (2016). Marcas de Agua: Una Contribución a la Seguridad de Archivos Digitales. *Revista de la Facultad de Ciencias Exactas, Físicas y Naturales*, *3*(1), Article 1. https://revistas.unc.edu.ar/index.php/FCEFyN/article/view/11961

Vidal, G. (2019). La Big Data y la Huella Digital: la importancia de los datos y como son utilizados por las empresas. Madrid. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/33063/TFG-Preciado%20Vidal-AragoIn%2c%20Gerardo..pdf?sequence=1&isAllowed=y

OEA. (2009, agosto 1). *OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo*. https://www.oas.org/ios/glossarydetails.aspx?lang=es&type=0&id=72

¿Qué es la huella digital en internet? (2020, abril 17). Argentina.gob.ar. (de, s. f.)

Ecuador, p. (2020, octubre 4). La violencia en línea esta silenciando las voces de las niñas y los jóvenes. Plan Internacional. https://plan.org.ec/la-violencia-en-linea-esta-silenciando-las-voces-de-las-ninas/#:~:text=En%20Ecuador%2C%2077%25%20de%20las,y%20acoso%20sexual%20(44%25).

Fiscalía General del Estado. (2021, diciembre). Perfil criminológico Fiscalía General del Estado. Recuperado el 9 de junio del 2024, de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

La Vanguardia Barcelona. (2022, mayo 12). *¿Qué es el grooming y cómo prevenir que les pase a nuestros hijos?* La Vanguardia. https://www.lavanguardia.com/mamas-y-papas/infancia/20220512/8261523/grooming-consejos-padres-edad-pequenos-pmv.html

Los peligros de navegar por internet para los niños. (2023, marzo 21). Humanium.org. https://www.humanium.org/es/los-peligros-de-navegar-por-internet-para-los-ninos/

Allison, B. (2023, junio 16). *¿Qué es la sextorsión?* Saprea. https://saprea.org/es/blog/que-es-la-sextorsion/

Redacción. (2023, octubre 5). Quito: un caso de violencia sexual digital usando inteligencia artificial se denuncia en un colegio; Fiscalía abre investigación. https://www.ecuavisa.com/noticias/quito/violencia-sexual-inteligencia-artificial-estudiantes-colegio-quito-YX6099221

Roiba, A. (2023, octubre 16). *6 consejos para reducir tu huella digital en la red*. La Vanguardia. https://www.lavanguardia.com/tecgrnologia/ciberseguridad/20231016/9296101/6-consejos-reducir-huella-digital-red-pvlv.html

Enriquez, A. (2023, diciembre 21). Filtrado de Contenido: todo lo que necesitas saber. https://www.airdroid.com/es/parent-control/content-filter/

Statement on End-to-End Encryption. (2024, abril 22). National Crime Agency. Recuperado el 5 de junio del 2024, de https://nationalcrimeagency.gov.uk/statement-on-end-to-end-encryption

Enriquez, A. (2024, Abril 30). Ponografía en Facebook: Cómo bloquear contenido para adultos. https://www.airdroid.com/es/parent-control/facebook-porn/#part2

ANEXO 1

INSTRUCTIVO PARA EL DISEÑO DE UNA POLÍTICA CRIMINAL PARA LA DETECCIÓN, PREVENCIÓN DE REPETICIÓN Y BLOQUEO DE CONTENIDO NOCIVO QUE CAUSA VIOLENCIA DIGITAL EN EL SISTEMA NACIONAL DE EDUCACIÓN

I. INTRODUCCIÓN

Mediante Suplemento del Registro Oficial 279, con fecha 29 de marzo del 2023 se publicaron las reformas de la Ley de Seguridad Pública y del Estado las cuales marcan como objetivo regular la seguridad integral del Estado y de todos los habitantes del Ecuador. En la normativa en mención se ha dispuesto la creación de una política criminal a través de un organismo interinstitucional, misma que se define como: “conjunto de respuesta que el Estado adopta, de manera integral e intersectorial, para prevenir y enfrentar la delincuencia y criminalidad con el fin de garantizar la protección de los intereses esenciales del Estado y los derechos de sus habitantes” (Ley de Seguridad Pública y del Estado, 2023, p. 8).

Se aprecia la necesidad de analizar cada uno de los sectores con mayores porcentajes de criminalidad, así como determinar las acciones que se han tomado hasta la fecha actual y evaluar cuán efectivas fueron. De esta manera se establecerán lineamientos claros para fortalecer la prevención y dar una respuesta adecuada a la problemática por la cual el sector esté pasando. En base a lo señalado, este instructivo se levantará de acuerdo con la problemática de la violencia digital que se ha dado en el Sistema Nacional de Educación, sea cometida por pares o adultos contra niños, niñas y adolescentes.

En la actualidad vivimos en una era digital a causa del avance tecnológico a pasos agigantados. Esta era ha traído consigo numerosos beneficios para el ámbito educativo, pero también ha planteado nuevos desafíos en cuanto a la seguridad y el bienestar de los niños, niñas y adolescentes. Esto se debe al incremento del

cometimiento de delitos a partir de plataformas digitales y en general a través del uso del internet. El *ciberbullying, grooming, sexting*, pornografía infantil y en sí, la difusión de contenido nocivo que genera cualquier tipo de violencia en el ciberespacio, son algunas de las amenazas que pueden socavar el entorno de aprendizaje y poner en riesgo el desarrollo integral de este grupo vulnerable.

En el Ecuador, el Ministerio de Educación con la colaboración de organizaciones sin fines de lucro como *ChildFund*, publicaron el *"Protocolo de Actuación frente a situaciones de Violencia Digital Detectadas en el Sistema Nacional de Educación"* con el fin de garantizar una educación segura e integral en entornos libres de violencia digital. Sin embargo, dentro del protocolo no se evidencia un marco en el que se proponga la manera correcta para la detección oportuna, prevención de repetición y bloqueo de contenido nocivo que generan entre pares o personas adultas en el ciberespacio en contra de niños, niñas y adolescentes.

II. OBJETIVO GENERAL

El presente instructivo tiene como objetivo brindar los lineamientos claros para el levantamiento de una política criminal en observancia a la detección, prevención de repetición y bloqueo de contenido nocivo que causa cualquier tipo de violencia digital en el Sistema Nacional de Educación.

III. OBJETIVOS ESPECÍFICOS

a. Plantear lineamientos claros para reducir los niveles de violencia digital en el Sistema Nacional de Educación, con la finalidad de minimizar el impacto negativo en contra de los niños, niñas y adolescentes.
b. Proporcionar una guía clara y concisa para la construcción de una política criminal, definiendo elementos esenciales, así como ofrecer ejemplos y recursos útiles para cada etapa del proceso.
c. Fomentar la participación de todos los actores internos – externos y verticales – horizontales, con la función de determinar su nivel de participación.

d. Garantizar la adecuación de lineamientos claros en observancia a las necesidades específicas del contexto educativo, a partir de recomendaciones para adaptar la política a las características y desafíos en particular.
e. Contribuir con la creación de un entorno educativo seguro y libre de violencia digital.

IV. TÉRMINOS Y DEFINICIONES

TÉRMINOS	SIGNIFICADO
Ciberdelitos	Acciones u omisiones que se encuentra tipificado como un delito en algunas legislaciones, su principal característica es que se realiza a partir de uso de las Tecnologías de la Información y Comunicación (TIC).
Ciberespacio	Espacio virtual e intangible que se produce a través de la interconexión de uno o más dispositivos a nivel global.
Contenido nocivo	Engloba la violencia, discursos de odio, abuso sexual infantil, ciberacoso, contenido que promueve comportamientos autodestructivos.
Dark Web	Espacio de internet que no está indexada por los motores de búsqueda convencionales.
Denuncia	Acción de informar a las autoridades competentes sobre el cometimiento de un delito.

Educación digital	También conocida como alfabetización digital, siendo un proceso educativo y de aprendizaje que se lleva sobre las nuevas tecnologías de la información y comunicación.
Integridad	Derecho fundamental de los niños, niñas y adolescentes a no ser víctimas de lesiones físicas o psicológicas, desde la perspectiva offline y online.
INTERPOL	International Criminal Police Organization.
ISP	Internet Service Provider
Machine Learning	Aprendizaje automático de las computadoras sin ser programadas para una tarea especifica.
Marcas de agua	Su principal función es ayudar en la identificación el propietario de un archivo, y así evitar el uso no autorizado e incluso inapropiado.
Offline	Encontrarse fuera de línea, referente al estado en el cual no estás conectado a una red informática o de internet.
OMS	Organización Mundial de la Salud.
Online	Estar en línea, referente a encontrarse conectado a una red informática o a internet.
Pares	Igual o compañero.

Política Criminal	Estrategias y acciones que toma el Estado para prevenir y combatir la delincuencia.
Política Pública	Conjunto de decisiones tomadas por el Estado o autoridades competentes para abordar un problema o necesidad que afecta a la sociedad.
Prestador de servicios de internet	Persona jurídica que brinda acceso a internet.
Protocolo	Conjunto de reglas y procedimientos que se siguen para realizar una tarea o proceso de manera efectiva.
Reparación Integral	Resarcir a una víctima de violencia de manera integral, completa y justa; a través de la restauración de su dignidad, el bienestar y la integridad física, psicológica y social.
Sistema Nacional de Educación	Conjunto de estructuras, niveles, modalidades educativas de un país.
TIC	Tecnologías de la información y la comunicación.
Víctima digital	Persona que sufre cualquier tipo de daño o perjuicio como resultado del mal uso de las TIC.
Violencia digital	Actos que pueden o buscan dañar o controlar a una persona a través del uso de las TIC.

V. MARCO LEGAL

- Código Orgánico Integral Penal.
- Constitución de la República del Ecuador.
- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional
- Convención sobre los Derechos del Niño del 20 de noviembre de 1989;
- Convenio Sobre la Ciberdelincuencia – Budapest
- Ley de Seguridad Pública y del Estado
- Ley Orgánica de Cooperación entre el Estado Ecuatoriano y la Corte Penal Internacional.
- Ley Orgánica de Educación Intercultural
- Ley Orgánica de Protección de Datos Personales.
- Ley Orgánica de Telecomunicaciones
- Política pública para una Internet segura para niños, niñas y adolescentes.
- 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;
- Reglamento General a la Ley Orgánica de Educación Intercultural
- Reglamento General de la Ley Orgánica de Protección de Datos Personales.
- Reglamento General de la Ley Orgánica de Telecomunicaciones

VI. DISEÑO DE LA POLÍTICA CRIMINAL CON ENFOQUE EN RESULTADOS

1. Definición de una política criminal con enfoque en resultados

La política criminal comprende, mediante acciones del Estado, dar respuesta a las necesidades de la ciudadanía. Esta política prioriza objetivos y acciones claras para resolver los desafíos nacionales, sectoriales o multisectoriales.

Una política criminal con enfoque en resultados implica tomar decisiones basadas en información confiable sobre los efectos que se generan para la ciudadanía en

virtud de las actividades de los ciberdelincuentes. De esta manera, se logrará generar cambios a través de la cadena de valor público, lo cual sería la detección temprana, prevención de repetición y bloqueo de contenido nocivo evitando la violencia digital dentro del Sistema Nacional de Educación para garantizar una educación integral y segura dentro del internet para los niños, niñas y adolescentes.

Con enfoque ciber criminológico y de la política criminal propuesta, el diseño de esta requiere una evaluación más rigurosa e identificación de las alternativas de acción a implementar para la detección temprana, prevención de repetición y bloqueo de contenido nocivo que cause violencia digital en el Sistema Nacional de Educación.

a. Definición del problema público

Constituye el punto de partida para la formulación del proceso y establece las estrategias para la política criminal, especialmente en el ámbito ciber criminológico. Es por ello por lo que, es fundamental realizar un diagnóstico convincente y proporcionar información crucial para las autoridades competentes que comprendan la magnitud del problema y tomen medidas acertadas.

b. Determinación de criterios de evaluación

Esta etapa implica evaluar distintas alternativas que busquen resolver el problema público. Entre los métodos que se recomienda para seleccionar estos criterios de evaluación son los siguientes:

- Revisar los antecedentes del problema para identificar qué aspectos pueden triunfar al proponer la política criminal. Con esto, se permitirá analizar y medir las escalas de satisfacción de esta nueva política criminal.
- Enfocar las causas centrales y graves que generan la existencia del problema central, para abordarlas desde su raíz y lograr una solución efectiva.

c. Identificación de alternativas al problema planteado

La formulación de una política criminal en el ámbito ciber criminológico - educativo requiere de un enfoque multidisciplinario, ya que los fenómenos delictivos son varios y complejos. En este contexto, resulta indispensable conformar equipos integrados por profesionales de diversas disciplinas, autoridades competentes, cooperación entre entidades públicas, como el Ministerio de Educación y Ministerio de Telecomunicaciones, entidades privadas, nacionales e internacionales, Unidades Educativas y la ciudadanía en sí, lo cual permitirá contar con un abanico de perspectivas, enfoques y alternativas para abordar un mismo problema de manera integral.

d. Evaluación de alternativas y decisión

La evaluación de la propuesta debe abordarse desde las distintas perspectivas como lo anunciamos anteriormente para atender el problema público. Para esto, se debe considerar la viabilidad, sostenibilidad, legitimidad y análisis del contexto para lograr atender de manera efectiva el problema.

En fin, es importante que el proceso desarrollado desde la definición hasta la decisión cumpla rigurosamente las fases del diseño de la política criminal con enfoque de resultados para responder de manera efectiva el problema frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación.

2. La elaboración de objetivos

La elaboración de objetivos a alcanzar resulta fundamental para solucionar el problema identificado, orientado los esfuerzos hasta lo deseado, esto es la detección, prevención de repetición y bloqueo de contenido nocivo. Los objetivos deben ser claros, concretos, íntegros y realizables dentro un periodo de tiempo determinado y cumplir con todos los criterios establecidos. Por ende, se debe establecer la siguiente estructura al formular los objetivos:

Tabla 1. Formulación de objetivos

Verbo (en infinitivo) + condición de cambio + sujeto = Objetivo	
Verbo	Cumplimiento que permita llegar al cambio deseado.
Condición de cambio	Situación que se desea cambiar.
Sujeto	Grupo de personas cuya condición desea cambiar.
Ejemplo	**Detectar, prevenir** la repetición y **bloquear** el contenido nocivo que causa violencia digital en el Sistema Nacional de Educación.

Fuente: Elaboración propia

3. **Medición de resultados en el marco de detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en el Sistema Nacional de Educación.**

La violencia digital es un problema que afecta a todas las edades dentro del Sistema Nacional de Educación, su cometimiento tiene un impacto negativo tanto en el desarrollo integral de las víctimas, su bienestar emocional y psicológico de cada uno de los estudiantes. Es importante contar con estrategias efectivas para detectar, prevenir la repetición y bloquear el contenido que pueda causar violencia digital. Para ello se debe evaluar la efectividad de estas estrategias, por ello se requiere implementar un sistema de medición, que se detalla a continuación:

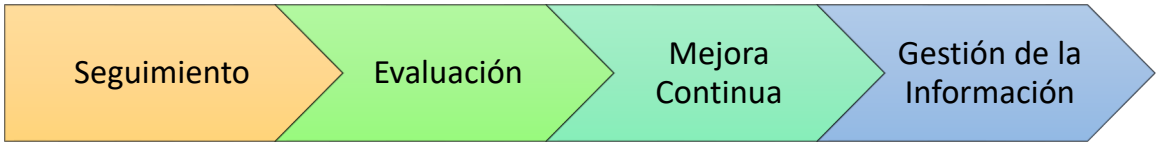
a. Sistema de seguimiento y evaluación basado en resultados

Para el seguimiento y evaluación se requiere la elección de una metodología precisa que ayude con la información exacta sobre el desempeño de las estrategias adoptadas en la política criminal. A través de este análisis se podrá concluir si la política estructurada es suficiente o no para el sector al que se dirige.

Establecer este sistema ampliará la eficacia de cumplimiento de la política que se diseñe para que establezca vinculaciones claras sobre intervenciones pasadas, presentes y futuras, lo cual arrojará resultados fiables que gestionarán mejoras a futuro. “El objetivo general del seguimiento y la evaluación es la medición y análisis de desempeño, a fin de gestionar con más eficacia los efectos y servicios que son el resultado en materia de desarrollo” (Programa de las Naciones Unidas para el Desarrollo de Oficina de Evaluación, 2002, p. 5).

Con la finalidad de asegurar los resultados y que estas sean reales y transparentes, la política a elaborar se deberá basar en:

Gráfico 1: Sistema de seguimiento y evaluación basado en resultados



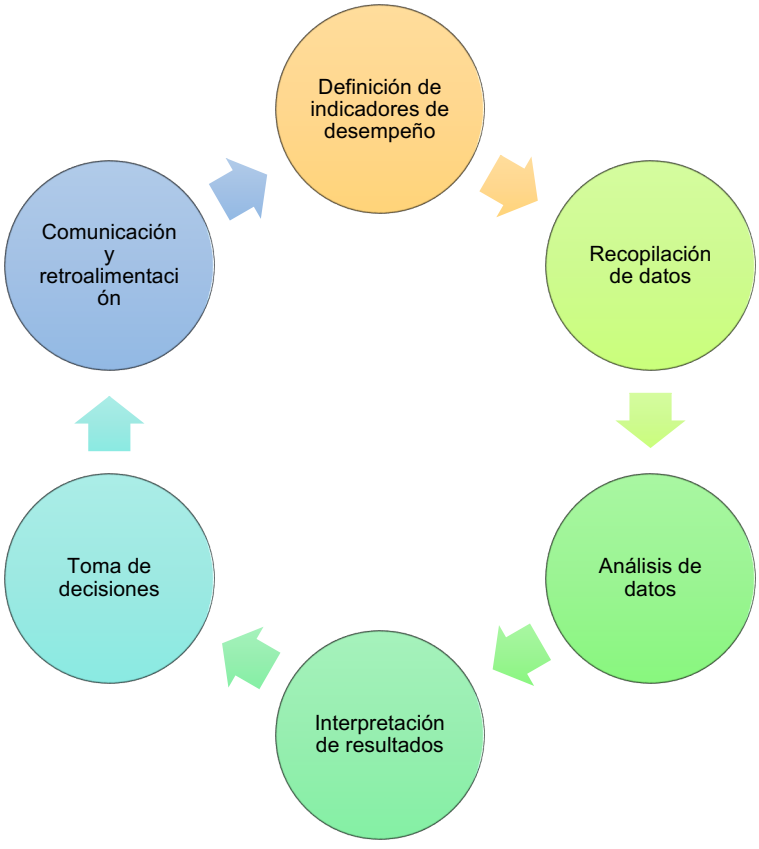
Fuente: PCM. (2022).

Seguimiento:

Se deberán establecer indicadores clave de rendimiento (KPIs) que sean claros, medibles y relevantes para cada etapa del proceso de prevención de la violencia digital. Establecer KPIs específicos, medibles, alcanzables, relevantes y con un plazo determinado para cada etapa de la detección, prevención de repetición y bloqueo de contenido nocivo que causa cualquier tipo de violencia digital, se vuelve imprescindible. Además, deberán estar alineados con los objetivos generales y reflejar los aspectos críticos de las estrategias implementadas.

Además, el seguimiento permitirá generar datos que puedan responder preguntas como: “¿La implementación de esta política criminal se está desarrollando según lo esperado? ¿Los resultados son consistentes con lo esperado? ¿Por qué lo obtenido difiere de lo esperado? ¿Los servicios son asequibles? ¿La calidad es adecuada? ¿Se llega a la población meta?” (Consejo Nacional de Política Criminal, 2024, p. 37). Al analizar el avance de la ejecución de las metas propuestas, en un periodo de tiempo determinado, ayudará a detectar oportunamente deficiencias, obstáculos y/o necesidades que se ajusten en la fase de implementación de la política. (Consejo Nacional de Política Criminal, 2024, p. 37).

Gráfico 2: Metodología para el análisis de seguimiento



Fuente: Elaboración propia

Evaluación:

Este punto permitirá evaluar de manera periódica la efectividad de las estrategias implementadas para detectar, prevenir repeticiones y bloquear contenido nocivo que genere cualquier clase de violencia digital en el Sistema Nacional de Educación. Para ello se deberá imponer objetivos y metas claras, alcanzables, relevantes y con un plazo determinado, que reflejarán los aspectos críticos de las estrategias y mecanismos implementados.

Además, esto permitirá retroalimentar y subsanar problemas o necesidades que posiblemente no se detectaron al momento del diseño de la política.

Mejora continua:

Permitirá ingresar en un ciclo de aprendizaje y adaptación para las estrategias y mecanismos adoptados. A partir del seguimiento y evaluación se obtendrá respuestas certeras sobre las falencias, y en este punto se podrá estructurar un plan adecuado para mejorar los puntos débiles detectados. Esto con el objetivo de resolver diversas problemáticas multicausales y multinivel que se presentan en territorio. (Consejo Nacional de Política Criminal, 2024, p. 38).

Gestión de la información:

Implica generar conocimiento que permitirá tomar decisiones informadas y adecuadas. (Consejo Nacional de Política Criminal, 2024, p. 38).

Tabla 2. Ejemplos de indicadores de la detección, prevención de repetición y bloqueo de contenido nocivo.

NOMBRE DE INDICADOR	PARÁMETRO	SUJETO	CARACTERÍSTICA
Número de estudiantes que han presentado cualquier tipo de reclamo por cualquier tipo de contenido	Porcentaje	Menores de edad	Denuncia presentada

nocivo publicado en internet.			
Número de casos resueltos sobre contenidos de violencia digital que fueron presentados por estudiantes.	Porcentaje	Menores de edad	Gestión de incidentes
Tiempo promedio de respuesta a los incidentes de violencia digital reportados.	Porcentaje	Menores de edad	Gestión de incidentes

Fuente: Elaboración propia

Conforme a lo mencionado en este apartado, es importante realizar una evaluación exhaustiva, con un equipo multidisciplinario que ayude a generar una metodología que se adapte correctamente al problema. Esto permitirá obtener resultados mucho más certeros y subsanar cualquier tipo de error, todo esto con la única finalidad de proteger la integridad de niños, niñas y adolescentes que fueron víctimas de cualquier tipo de contenido nocivo que causa cualquier tipo de violencia digital.

b. Articulación o coordinación intersectorial

En este apartado se valorará la “capacidad que tiene el Estado para conformar diferentes áreas para abordar problemas sociales y alcanzar metas en común”. (Consejo Nacional de Política Criminal, 2024, p. 45). En base a la controversia social que vivimos en la actualidad por el uso desmedido del internet por parte de los niños, niñas y adolescentes, quienes no tienen ningún tipo de control o restricciones en su

uso. A causa de lo manifestado, se ven expuestos a delitos que se pueden consumar dentro del mundo online y offline, como por ejemplo el grooming.

En este instructivo no solo se planteará las estrategias para la efectividad en la detección, prevención de repetición y bloqueo del contenido nocivo; también pretende dar luces al organismo correspondiente sobre las instituciones y otros organismos que deberán participar activamente, sea institución pública o privada, pero que a la final se encuentran reguladas por el ámbito público.

c. Importancia de la articulación

La problemática planteada requiere un enfoque integral que resulte en la participación de diversos actores. El Consejo Nacional de Política Criminal del Perú, señala que la importancia radica en tres aspectos:

> "i) Promueve el aprovechamiento de los escasos recursos. En un trabajo articulado se puede intercambiar, compartir y generar tres tipos de recursos: conocimiento, medios materiales e influencia; ii) Potencia los resultados para atender un problema en común que no se podría abordar desde el trabajo que cada organización realiza por separado en el ámbito local o regional; y, iii) Favorece la planificación total del trabajo en el territorio" (Consejo Nacional de Política Criminal, 2024, p. 45).

d. Tipos de articulación: interna – externa y horizontal – vertical

Para formular correctamente la política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo, es importante realizar un amplio análisis de los organismos que deberían participar, tanto internos – externos, así como horizontales – verticales.

Tabla 3. Tipos de articulación: interna – externa y horizontal – vertical

TIPO	DESCRIPCIÓN
INTERNA	Coordinación interna entre distintas áreas de un organismo y/o institución perteneciente al Estado. Esta coordinación se

	basa en compartir recursos humanos, tecnológicos, económicos e incluso la infraestructura.
EXTERNA	Coordinación externa entre instituciones y/u organizaciones con diferentes competencias, pero que de una u otra forma se ven vinculadas para la atención de la política que se desarrolla.
HORIZONTAL	Coordinación que se establece con organizaciones o instituciones del mismo nivel de gestión gubernamental, con la finalidad de fortalecer estrategias y mayor eficacia de respuesta.
VERTICAL	Articulación con diferentes niveles de jurisdicción (gobierno local o provincial, incluyendo al gobierno nacional).

Fuente: Consejo Nacional de Política Criminal, 2024

e. Pasos para una efectiva articulación

De acuerdo con lo señalo en párrafos anteriores, queda claro que la articulación intersectorial es importante para que se desarrolle una política criminal que aborde la detección, prevención de repetición y bloqueo de contenido nocivo que afecta a los niños, niñas y adolescentes en el Sistema Nacional de Educación. Por ello se deberá observar lo siguiente:

Tabla 4. Pasos para una articulación intersectorial para política criminal

Definir un marco legal	Se deberá identificar legislación específica que identifique y penalice ciberdelitos. Identificar la necesidad de realizar reformas en materia penal, en los casos que no se presenten ciberdelitos

	expuestos en el presente instructivo. Se deberá analizar claramente su viabilidad. Establecer mecanismos para la detección, prevención de repetición y bloqueo del contenido nocivo que genere cualquier tipo de violencia digital. Establecer métricas claras para la estructuración de normativa interna de los actores obligados en la política.
Crear o establecer un organismo coordinador	Designación de un facilitador o director que se encargue de dirigir las sesiones de levantamiento de la política criminal, así como organizar la intervención de cada uno de los participantes. Establecer un organismo que se encargue de la elaboración de la política criminal de acuerdo con el diagnóstico y evaluación del fenómeno social que se plantea. Establecer el ente regulador que se encargue de la coordinación interinstitucional, así como el cumplimiento de las medidas señaladas en la política criminal. Detallar con claridad las principales funciones que tendrán cada uno de los organismos que intervendrán en la ejecución de la política.
Fortalecer las capacidades de los actores involucrados	Será importante brindar capacitaciones a los funcionarios de los diferentes organismos que participarán en la creación, y funcionarios que pondrán en práctica la política criminal para la detección, prevención de repetición y bloqueo del contenido

	nocivo que genera cualquier tipo de violencia digital contra los niños, niñas y adolescentes.
Sensibilizar a la población	Se deberán crear planes de capacitación para la sensibilización de la población en general, estos planes deberán ser estructurados en base al grupo al que se haya dirigido: niños, niñas, adolescentes; adultos o personas de la tercera edad. Promover el uso responsable del internet y la educación digital, esto con la finalidad de dar cumplimiento a lo señalado en el *Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación.*
Establecer mecanismos de cooperación internacional o nacional	En observancia a convenios internacionales como, por ejemplo: Convención de las Naciones Unidas sobre la Ciberdelincuencia o el Convenio de Budapest, mismo que otorgan medidas claras para enfrentar casos de violencia digital e incorporarlo en la normativa legal vigente. Será necesario que se evalúe la ratificación por parte del Ecuador de estos convenios. De igual manera se deberá observar la colaboración con organismos o Agencias de inteligencia cibernética como la INTERPOL que a la hora de detección y bloqueo en casos más complicados, podrían ser excelentes aliados. También será importante que el gobierno detalle la colaboración con instituciones privadas, que de por si se encuentran reguladas por diferentes organismos

	estatales, esto ayudará a que la política sea más certera en la necesidad que presenta.

Fuente: Elaboración propia

f. Identificación y análisis de actores claves vinculados

En este instructivo se reconocerá las articulaciones intersectoriales más importantes para la efectividad de la política criminal para la detección, prevención de repetición y bloqueo de contenido nocivo que cause cualquier tipo de violencia digital en contra de los niños, niñas y adolescentes que forman parte del Sistema Nacional de Educación, en base al análisis de la siguiente Tabla:

Tabla 5. Actores claves vinculados:

ACTOR	DESCRIPCIÓN
Consejo Nacional de Política Criminal	Es el organismo encargado de aprobar la política criminal, este se conformará por los siguientes actores: 1. Un delegado o delegada del Presidente o Presidenta de la República; 2. El Ministro o Ministra del ente rector de la política de derechos humanos; 3. El Ministro o Ministra de la entidad encargada de la coordinación de la seguridad pública y del Estado; 4. El Ministro o Ministra del ente rector de seguridad ciudadana, protección interna y orden público; 5. El Ministro o Ministra del ente rector de la Defensa Nacional;

	6. El Ministro o Ministra responsable de la coordinación y supervisión de la gestión de las gobernaciones provinciales; 7. El Ministro o Ministra del ente rector del Sistema Nacional de Inteligencia; 8. La Ministra o Ministro del organismo técnico del Sistema Nacional de Rehabilitación Social y de Atención Integral a Adolescentes Infractores; 9. El Ministro o la Ministra responsable de la coordinación del sector social o que sea designada por el Presidente o Presidenta de la República con este fin; 10. El Presidente o Presidenta del Consejo de la Judicatura o en ausencia, la delegada o delegado del Pleno del organismo; 11. El Presidente o Presidenta de la Corte Nacional de Justicia o en ausencia, la delegada o delegado del Pleno del organismo; 12. El o la Fiscal General del Estado o su delegada o delegado; 13. El o la Comandante General de la Policía Nacional; 14. La autoridad del Servicio Nacional de Aduanas o su delegada o delegado; y, 15. La autoridad de la Unidad de Análisis Financiero y Económico.

Ministerio de Telecomunicaciones y de la Sociedad de la Información	La rectoría de la política criminal será ejercida por un Ministerio, que tendrá las siguientes atribuciones y competencias: 1. Ejercer la rectoría de la política criminal y derechos humanos; 2. Actuar como Secretaría Técnica del Consejo Nacional de Política Criminal; 3. Diseñar, definir e implementar planes, programas y proyectos en el ámbito de la política criminal y los derechos humanos; 4. Preparar una propuesta de Plan de Política Criminal que será puesta en conocimiento del Consejo Nacional de Política Criminal, para su aprobación; 5. Formular y ejecutar políticas para la erradicación de todas formas de violencia y discriminación, en particular, contra mujeres, niñas niños, adolescentes y otros grupos de atención prioritaria; 6. Coordinar y ejecutar, en su ámbito de competencia, la implementación del Plan de Política Criminal; 7. Articular acciones con las demás entidades de la Función Ejecutiva y con la Función Judicial para asegurar el cumplimiento de la política criminal del país; 8. Articular la política criminal a la política de seguridad integral del país, en coordinación con las entidades competentes;

	9. Transversalizar la política pública de derechos humanos en la administración pública; 10. Garantizar el cumplimiento de todas las obligaciones nacionales e internacionales en materia de derechos humanos; 11. Vigilar el cumplimiento de los estándares internacionales de derechos humanos en el Sistema de Rehabilitación Social, en coordinación con el organismo técnico del Sistema; 12. Protección a pueblos indígenas en aislamiento voluntario; y, 13. Otras establecidas en la ley.
Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)	La ARCOTEL juega un rol importante en la lucha contra el contenido nocivo que genera cualquier tipo de violencia digital y afecta gravemente a los niños, niñas y adolescentes. La manera en la que ARCOTEL podría participar es de la siguiente manera: 1. Limitar requisitos básicos para que las plataformas puedan operar en Ecuador, incluyendo medidas de detección, prevención de repetición y bloqueo de contenido nocivo que afecta a los niños niñas y adolescentes. 2. Trabajar con empresas de telecomunicaciones para la detección y bloqueo de páginas web que contengan contenido nocivo. 3. Promover la implementación de herramientas de control parental por parte de empresas de telecomunicaciones.

	4. Colaboración conjunta con otros organismos gubernamentales, organismos internacionales, organizaciones sin fines de lucro e incluso instituciones privadas para la detección, prevención de repetición y bloqueo de contenido nocivo. 5. Publicación de resoluciones y lineamientos generales en donde se establezca la obligación de cumplimiento por parte de los Proveedores de Servicios de Internet, para la adaptación de medidas de detección, prevención de repetición y bloqueo de contenido nocivo que afecta a los niños, niñas y adolescentes.
Ministerio de Educación	El Ministerio de Educación en primera instancia deberá asegurar el cumplimiento del “Protocolo de actuación frente a casos de violencia digital en el Sistema Nacional de Educación”, a través del levantamiento de un plan de verificación de cumplimiento, en el cual se establezca tiempos para talleres de educación digital que deberán dictar las instituciones educativas. Con una participación vertical y horizontal con las instituciones nombradas en recuadros anteriores, tendrá la obligación de dar a conocer a las Instituciones Educativas que componen el Sistema Nacional de Educación, sobre la política criminal, cómo aplicarla y su obligatoriedad de cumplimiento.

Fuente: Ley de Seguridad Pública y del Estado (2023). Elaboración propia

4. **Lineamientos para la detección, prevención de repetición y bloqueo del contenido nocivo que causa cualquier tipo de violencia digital en el Sistema Nacional de Educación**

a. **Enfoques transversales de la violencia digital en el Sistema Nacional de Educación**

Enfoque de Derechos Humanos

Se origina en el sentido que todos los niños, niñas y adolescentes que forman parte del Sistema Nacional de Educación, tienen derecho a una educación libre de cualquier tipo de violencia, incluida la violencia digital. La promoción de los derechos humanos que gozan los estudiantes, como el derecho a la privacidad, derecho a la libre expresión y derecho a la integridad sexual.

“Desde este enfoque, los planes, las políticas y los procesos de desarrollo están anclados en un sistema de derechos y de los correspondientes deberes establecidos por el derecho internacional, así como nacional” (Consejo Nacional de Política Criminal, 2024, p. 15).

Enfoque centrado en la víctima

Se observan las necesidades que tiene la víctima, así como la experiencia en cuanto a la violencia digital que vulneró sus derechos y libertades fundamentales. Con este enfoque se pretende crear un espacio seguro en el cual las víctimas se sientan cómodas denunciando y recibiendo apoyo.

“Los estándares de este enfoque son priorizar las necesidades de la víctima, evitar la revictimización, garantizar en todo momento su protección y cuidado, asegurar el acceso a la justicia, empoderar y promover la participación de la víctima en todo el proceso y promover la restitución de sus derechos”. (Consejo Nacional de Política Criminal, 2024, p. 15).

Enfoque de género en la política criminal

Se reconoce la existencia de la violencia digital como un fenómeno que está demasiado arraigado en la sociedad. Se centra en la creación de políticas y medidas de prevención para proteger a las víctimas y posibles víctimas de la violencia digital.

“Este enfoque aporta elementos centrales para la formulación de medidas (políticas, mecanismos, acciones afirmativas, normas, etc.) que contribuyen a superar las brechas entre mujeres y hombres, erradicar toda forma de violencia de género, asegurando el acceso de ambos a recursos y servicios públicos y fortaleciendo su participación política en igualdad”. (Consejo Nacional de Política Criminal, 2024, p. 15).

Se identifica los delitos que se deberán observar principalmente para la creación de esta política, los cuales se detalla a continuación:

Tabla 6. Catálogo de delitos para observar

DELITO	DEFINICIÓN	MUNDO OFFLINE	MUNDO ONLINE
Grooming	Acaso para solicitar contenido sexual a un niño, niña y adolescentes.	Comienza con un adulto que se acerca a un menor con intenciones sexuales.	Acercamiento y manipulación de un adulto hacia un menor a través de internet, con el objetivo de abusar sexualmente de este.
Sextorsión	Chantaje para enviar o publicar contenido sexual de la víctima.	Una persona que mantiene una relación de confianza o una amenaza física.	Se produce a través de plataformas digitales, donde chantajistas amenazan en divulgar imágenes o videos íntimos

			para que la víctima cumpla sus demandas.
Pornografía Infantil	Representación visual o multimedia de niñas, niños y adolescentes en conductas sexuales.	Producción y distribución de videos con contenido sexual de manera física.	Internet facilita la difusión y acceso a material ilegal relacionado con niñas, niños y adolescentes.
Ciberbullying	Aquella persona que mediante el uso de las TIC acosa, amenaza, insulta o humilla a otra de manera repetida.	El acosador puede comenzar en persona y extenderse al mundo digital.	Se manifiesta a través de plataformas en línea, como redes sociales o mensajes de texto.

Fuente: Elaboración propia

b. Identificación de medidas de detección

Existen diferentes formas de detección de contenido nocivo que genera cualquier tipo de violencia digital en contra de los niños, niñas y adolescentes que forman parte del Sistema Nacional de Educación, que se detallará a continuación:

Tabla 7. Medidas de detección de contenido nocivo

Denuncia por parte de la víctima, compañeros de la víctima, padres de familia, autoridades educativas, profesores o por un tercero	Permitirá a la víctima poner en conocimiento de Autoridades competentes, incluyendo los actores de la presente política, quienes identificarán de manera inmediata el contenido nocivo en contra de la víctima y podrá aplicar mecanismos y

	estrategias de prevención de repetición y bloqueo.
Técnicas de Machine Learning	Enseñanza a los algoritmos para la identificación a través de patrones y palabras clave que indiquen el tipo de contenido. Reconocimiento de actividades sospechosas y redes de distribución. Ayudaría a una respuesta rápida para evitar la descarga y bloquear el contenido casi de manera inmediata. Estas técnicas podrían ser implementadas por plataformas de redes sociales.
Opciones de Filtrado	Selección de palabras clave utilizadas en la mayoría de los ciberdelitos, incluyendo temas de pornografía infantil. Así se podrá detectar el contenido con la única finalidad de bloquear. Permitirá a los usuarios establecer sus propias restricciones. Supervisará la actividad de los niños, niñas y adolescentes en línea.
Aplicaciones de Control Parental	Se podrá evidenciar los sitios web a los cuales acceden los niños, niñas y adolescentes. Monitorear la búsqueda en internet de los niños, niñas y adolescentes que ayudará a identificar si accedieron algún tipo de contenido nocivo.

Fuente: Elaboración propia

c. Diseño de estrategias de prevención de repetición

El diseño de estrategias de prevención de repetición de contenido nocivo, como la implementación de huellas digitales y marcas de agua a documentos o archivos digitales, son herramientas por considerar para proteger a niños, niñas y adolescentes en internet. La aplicación de estos mecanismos es importante por lo que se necesita establecer los medios o soluciones para prevenir el problema público presentado.

Gráfico 3: Procedimiento de huellas digitales y/o marcas de agua

Fuente: Elaboración Propia

d. Incorporación de huellas digitales y marcas de agua: se busca que cada documento o archivo digital que tenga información sensible debe tener una huella digital única y una marca de agua visible o invisible.
e. Monitoreo y detección: Se identifica mecanismos para detectar la presencia de huella digital o marca de agua en plataformas no autorizadas.
f. Identificación de la fuente: Si se detecta una fuga no autorizada del contenido protegido.

g. Acciones correctivas: Se revisan los procedimientos de seguridad para evitar futuras fugas.

g. Prevención: Se toman medidas de corrección y acciones legales contra los agresores para prevenir futuras repeticiones de distribución de contenido nocivo.

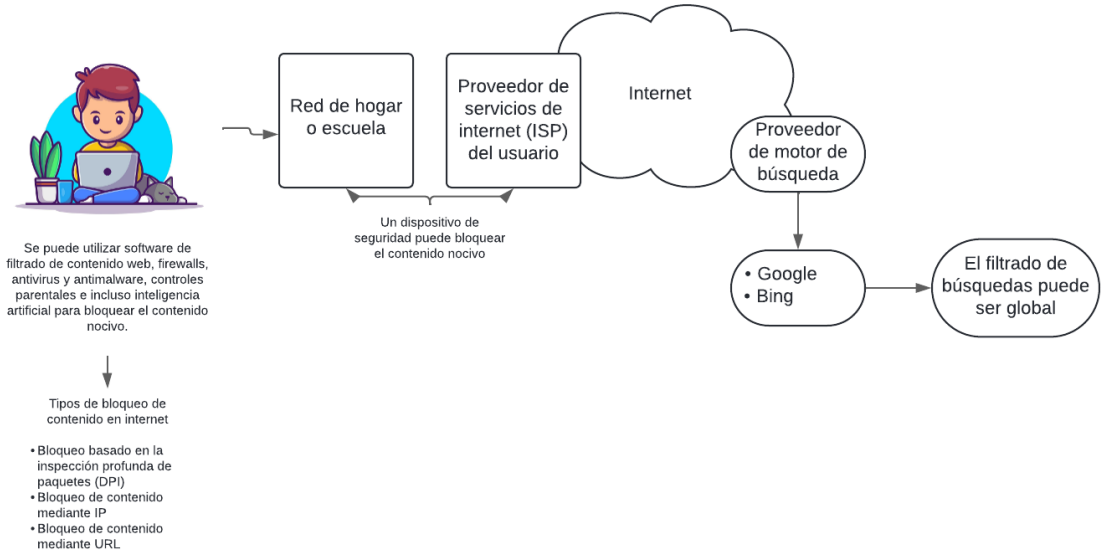
h. Mejora continua: Se realizan revisiones de las huellas digitales y marcas de agua para mantener la seguridad contra nuevas amenazas.

h. Establecimiento de mecanismos de bloqueo

Como establecimiento de mecanismos de bloqueo de contenido nocivo en internet podríamos utilizar los siguientes métodos y como apoyo el uso de herramientas tecnológicas.

El bloqueo de contenido nocivo de internet puede aplicarse de distintas maneras como se indica en el flujo que se detalla a continuación:

Gráfico 4: Proceso de bloqueo de contenido



Fuente: Elaboración Propia

En este grafico fácil de entender, se representa cómo se puede controlar y bloquear el contenido nocivo en internet que afecte a niños, niñas y adolescentes. El flujo comienza con la red del hogar o escuela, donde este grupo vulnerable empieza su conectividad a internet por el prestador del servicio de este. Desde esta etapa, se pueden implementar distintos métodos de bloqueo de contenido nocivo e incluso usar herramientas tecnológicas como apoyo; por ejemplo, el filtro de contenido para los proveedores de motor de búsqueda como *Google*, que es el más utilizado a nivel mundial, *firewalls*, antivirus o *antimalware* para mitigar los virus que pueden entrar y dañar al ordenador o dispositivo electrónico, controles parentales e incluso la inteligencia artificial para detectar y bloquear el material inapropiado.

VII. BIBLIOGRAFÍA

Consejo Nacional de Política Criminal. (2024). Lineamientos del Consejo Nacional de Política Criminal para la elaboración de estrategias regionales de política criminal. Perú. Recuperado el 9 de junio del 2024, de https://cdn.www.gob.pe/uploads/document/file/5663272/5016635-anexo-03-lineamientos-del-conapoc-para-elaborar-erpc.pdf

Ecuador. (2023). Ley de Seguridad Publica y del Estado. Registro Oficial 279, con fecha 29 de marzo del 2023.

Programa de las Naciones Unidad para el Desarrollo, Oficina de Evaluación. (2002). Medidas de seguimiento y evaluación de resultados. Recuperado el 9 de junio del 2024, de https://www.inec.gob.pa/redpan/sid/docs/documentos%20marco/Documentos_Referencia_regionales/manual%20seg%20y%20eval.pdf