FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS

Trabajo fin de Maestría titulado:

"LA EDUCACIÓN DIGITAL Y SU ROL EN LA PREVENCIÓN ANTE LA CIBERDELINCUENCIA JUVENIL EN ECUADOR."

Realizado por:

Willian Geovanny Casa Murillo

Directa del proyecto:

Estefany Johana Alvear Tobar

Como requisito para la obtención del título de:

MAGISTER EN CRIMINOLOGÍA

Quito, 07 de abril de 2025

DECLARACIÓN JURAMENTADA

Yo, WILLIAN GEOVANNY CASA MURILLO, ecuatoriano, con cédula de ciudadanía No. 1724143118, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido presentado anteriormente para ningún grado o calificación profesional, y se basa en las referencias bibliográficas descritas en este documento.

A través de esta declaración, cedo los derechos de propiedad intelectual a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y normativa institucional vigente.

Firmado electrónicamente por:
WILLIAN GEOVANNY CASA MURILLO

Willian Geovanny Casa Murillo

C.C.: 1724143118

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el la estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

ESTEFANY JOHANA ALVEAR TOBAR

Firmado digitalmente por ESTEFANY JOHANA ALVEAR TOBAR
Fecha: 2025.04.07 21:20:35 -05'00'

Estefany Johana Alvear Tobar

C.C. 1722402144

EL PROFESOR INFORMANTE:

Andrea Gómez Martínez

Después de revisar el trabajo presentado lo ha calificado como apto para su defensa oral ante el tribunal examinador.

Firmado por
GOMEZ ANDREA -
***9955** el

Mgtr. Andrea Gómez Martínez

Quito, 07 de abril de 2025

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

Firmado electrónicamente por:
WILLIAN GEOVANNY
CASA MURILLO

Willian Geovanny Casa Murillo

C.C.: 1724143118

AGRADECIMIENTOS

A lo largo de mi investigación, he contado con el apoyo invaluable de personas que hicieron posible este logro. Familia por su, comprensión y por motivarme incluso en los momentos más difíciles, compañeros de trabajo, por su constante ánimo y apoyo. Agradezco también a la Universidad Internacional SEK y a sus docentes, cuya experiencia en criminología aportó conocimientos y herramientas esenciales para el desarrollo de mi estudio.

Este trabajo es el resultado de un esfuerzo compartido, y a todos los que formaron parte de él, les estaré siempre agradecido.

DEDICATORIA

Nathy

Gracias por ser mi fuerza constante y mi mayor inspiración. Tu frase *"Sigue adelante y nunca pares, tú puedes"* me sostuvo en cada momento de duda. Cuando tuve que desprenderme de algo valioso (B16), tu apoyo hizo que ese sacrificio tuviera sentido.

Este logro también es tuyo, por tu confianza y presencia marcaron cada paso de este camino.

ÍNDICE DE CONTENIDOS

Índice de tabla

RESUMEN

La presente investigación titulada “La educación digital y su rol en la prevención ante la ciberdelincuencia juvenil en Ecuador” tuvo como objetivo general analizar el rol de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador, evaluando su efectividad e identificando estrategias educativas que contribuyan a la reducción de amenazas y conductas delictivas en el entorno digital. La metodología utilizada fue mixta, combinando enfoques cuantitativos y cualitativos. En el enfoque cuantitativo, se utilizaron encuestas a estudiantes y docentes para medir la efectividad de las estrategias educativas, mientras que el componente cualitativo consistió en entrevistas semiestructuradas que permitieron profundizar en las percepciones de los participantes. Los resultados mostraron que las iniciativas educativas existentes en el país no son suficientemente efectivas para prevenir la ciberdelincuencia juvenil, ya que, aunque se reconocen los riesgos digitales, los programas educativos carecen de una estructura integral y práctica que involucre a los jóvenes en la prevención real de delitos en línea. A pesar de los esfuerzos realizados, la ciberdelincuencia, en especial el ciberacoso y la suplantación de identidad, sigue siendo un problema importante. La conclusión más relevante de la investigación es que es necesario fortalecer los programas educativos sobre ciberseguridad, haciéndolos más interactivos y prácticos, además de capacitar continuamente a los docentes para que puedan adaptarse a las nuevas amenazas digitales. Se recomienda la implementación de políticas públicas que garanticen una educación integral y dinámica para enfrentar los riesgos digitales.

Palabras clave: Educación digital, Ciberdelincuencia juvenil, Prevención, Ciberseguridad, Estrategias educativas

ABSTRACT

This research titled “Digital Education and Its Role in the Prevention of Juvenile Cybercrime in Ecuador” aimed to analyze the role of digital education in the prevention of juvenile cybercrime in Ecuador, evaluating its effectiveness and identifying educational strategies that contribute to reducing threats and criminal behaviors in the digital environment. The methodology used was mixed, combining both quantitative and qualitative approaches. The quantitative approach involved surveys of students and teachers to measure the effectiveness of educational strategies, while the qualitative component consisted of semi-structured interviews that allowed for a deeper understanding of participants' perceptions. The results showed that existing educational initiatives in the country are not sufficiently effective in preventing juvenile cybercrime, as, although digital risks are recognized, educational programs lack an integrated and practical structure that engages young people in the actual prevention of online crimes. Despite efforts made, cybercrime, especially cyberbullying and identity theft, remains a significant problem. The most relevant conclusion of the research is that cybersecurity education programs need to be strengthened, making them more interactive and practical, while continuously training teachers to adapt to new digital threats. The implementation of public policies is recommended to ensure comprehensive and dynamic education to address digital risks.

Keywords: Digital Education, Juvenile Cybercrime, Prevention, Cybersecurity, Educational Strategies

INTRODUCCIÓN

En la era digital actual, la ciberdelincuencia juvenil se ha convertido en una preocupación creciente en Ecuador. El acceso masivo a internet y el uso extendido de dispositivos electrónicos han facilitado la aparición de diversas amenazas digitales que afectan a la juventud. Entre los ciberdelitos más comunes en el país se encuentran el robo de información personal, fraudes en línea, ataques informáticos y ciberacoso

Según Primicias (2025) alrededor del 98% de las personas mayores de 12 años en Ecuador, especialmente los adolescentes, tienen una cuenta en redes sociales, lo que aumenta su exposición a riesgos digitales. Estos datos reflejan la vulnerabilidad de la juventud ecuatoriana frente a las amenazas digitales y resaltan la necesidad de intervenciones efectivas.

La educación digital se presenta como una herramienta esencial para mitigar estos riesgos. Sin embargo, en Ecuador, la implementación de programas educativos enfocados en la seguridad digital aún enfrenta desafíos significativos. La falta de formación adecuada en ciberseguridad aumenta la vulnerabilidad de los jóvenes frente a las amenazas en línea

En respuesta a esta problemática, el Ministerio de Educación ha desarrollado protocolos y cursos en su programa “Prevención de riesgos en entornos digitales” para prevenir y educar a niños, niñas y adolescentes en el uso responsable de las Tecnologías de la Información y la Comunicación (TIC). Estas iniciativas buscan promover una cultura de prevención y protección en el entorno digital, garantizando la integridad y dignidad de los menores en línea.

La presente investigación tiene como objetivo analizar el papel de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador. Se evaluará la efectividad de las estrategias educativas existentes, se identificarán las principales formas de cibercrimen

que afectan a la juventud y se analizarán las iniciativas implementadas en el país. Este estudio busca contribuir al desarrollo de políticas y programas que promuevan una convivencia digital segura y consciente.

La estructura de la tesis se divide en cuatro capítulos. El primero aborda el marco teórico, presentando los conceptos fundamentales relacionados con la educación digital y la ciberdelincuencia juvenil. El segundo capítulo describe la metodología de investigación adoptada, detallando el enfoque, diseño y técnicas de recolección de datos. En el tercer capítulo se analizan los resultados obtenidos, y finalmente, el cuarto capítulo presenta las conclusiones y recomendaciones derivadas del estudio.

Planteamiento del problema.

La ciberdelincuencia juvenil se ha convertido en una problemática creciente a nivel mundial, y Ecuador no es la excepción. Con el avance acelerado de la tecnología y el acceso masivo a dispositivos digitales, los jóvenes se encuentran cada vez más expuestos a amenazas cibernéticas como el ciberacoso, la suplantación de identidad, el robo de información y el fraude en línea (Villavicencio et al., 2021). Según el Instituto Nacional de Estadística y Censos (2023), el 95% de los adolescentes ecuatorianos entre 12 y 18 años utiliza internet de manera frecuente, lo que los convierte en un grupo vulnerable frente a este tipo de delitos.

A pesar de la creciente incidencia de ciberdelitos, la educación digital en Ecuador aún no ha alcanzado el nivel de efectividad necesario para prevenir estas amenazas. Diversos estudios señalan que la falta de formación adecuada en ciberseguridad y el uso responsable de las Tecnologías de la Información y la Comunicación (TIC) incrementan el riesgo de los jóvenes de ser víctimas o incluso partícipes involuntarios de actividades delictivas en el entorno digital (Mendoza & Torres, 2022).

El Ministerio de Educación de Ecuador ha implementado iniciativas orientadas a promover el uso seguro y responsable de internet, pero estas acciones aún resultan insuficientes para mitigar el impacto de la ciberdelincuencia (Ministerio de Educación de Ecuador, 2023). En este contexto, la educación digital juega un papel crucial no solo en la prevención de estos delitos, sino también en la formación de ciudadanos digitales responsables, conscientes de sus derechos y deberes en el entorno virtual.

Por lo tanto, esta investigación busca abordar la efectividad de la educación digital como herramienta preventiva frente a la ciberdelincuencia juvenil en Ecuador. Se pretende identificar las principales amenazas cibernéticas que afectan a los jóvenes, analizar las iniciativas educativas existentes y evaluar su impacto en la reducción de este fenómeno. De esta manera, se espera contribuir al diseño de estrategias educativas más eficientes que fomenten una cultura de seguridad y responsabilidad digital en el país.

Justificación

La presente investigación sobre la educación digital y su rol en la prevención de la ciberdelincuencia juvenil en Ecuador es relevante tanto a nivel social como educativo, debido al crecimiento acelerado de las amenazas cibernéticas que afectan a la población joven. Según el informe de la Cámara Ecuatoriana de Comercio Electrónico (2023), los casos de ciberdelitos han aumentado un 35% en los últimos tres años, siendo los adolescentes uno de los grupos más vulnerables por su constante interacción en plataformas digitales. Esta situación evidencia la necesidad de fortalecer la formación en competencias digitales que promuevan el uso responsable y seguro de las tecnologías.

Desde una perspectiva educativa, esta investigación se justifica porque la educación digital se convierte en una herramienta fundamental para la prevención de delitos cibernéticos, al fomentar la alfabetización digital y la concienciación sobre las consecuencias de la interacción irresponsable en entornos virtuales (García & López,

2021). En Ecuador, si bien existen programas y políticas públicas orientadas al uso seguro de las Tecnologías de la Información y la Comunicación (TIC), aún se observa una falta de estrategias efectivas y sostenibles que permitan mitigar el riesgo de la ciberdelincuencia juvenil (Ministerio de Educación de Ecuador, 2023)

A nivel social, esta investigación es pertinente porque la ciberdelincuencia no solo afecta a las víctimas directas, sino también al entorno familiar y comunitario, generando problemas como el ciberacoso, el robo de identidad y el fraude electrónico (Pérez et al., 2022). Por lo tanto, promover una educación digital adecuada contribuirá a la construcción de una ciudadanía digital responsable, capaz de protegerse y actuar éticamente en el espacio virtual.

En el ámbito académico, este estudio llenará un vacío en la literatura actual al proporcionar un análisis detallado sobre la efectividad de la educación digital en Ecuador, identificando las principales amenazas cibernéticas y evaluando las iniciativas existentes. Los resultados permitirán generar propuestas innovadoras para fortalecer la formación digital en instituciones educativas, impactando positivamente en la prevención de delitos informáticos.

Finalmente, esta investigación será una herramienta valiosa para la formulación de políticas públicas y programas educativos que integren la educación digital como eje transversal, promoviendo el desarrollo de habilidades tecnológicas y de seguridad digital desde edades tempranas. De esta manera, se contribuirá a la reducción de la ciberdelincuencia juvenil y al fortalecimiento de un entorno digital más seguro y responsable en Ecuador.

Objetivos

Objetivo general

Analizar el rol de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador, evaluando su efectividad e identificando estrategias educativas que contribuyan a la reducción de amenazas y conductas delictivas en el entorno digital.

Objetivos específicos

- Evaluar la efectividad de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador, identificando estrategias educativas efectivas que aporten a una reducción de tendencias y amenazas asociados al entorno digital.
- Identificar las principales formas de ciberdelincuencia que afectan a la juventud en Ecuador.
- Analizar las iniciativas educativas existentes en Ecuador para la prevención del cibercrimen juvenil.

Sistematización del problema

La creciente incidencia de la ciberdelincuencia juvenil en Ecuador plantea una serie de desafíos que afectan tanto a la seguridad de los jóvenes como a la calidad de su educación en el entorno digital. La sistematización del problema en este contexto se orienta a entender cómo la educación digital puede jugar un papel clave en la mitigación de la ciberdelincuencia y cómo las políticas públicas actuales pueden ser más efectivas en su implementación. La pregunta central que guía la investigación es:

¿Cómo puede la educación digital prevenir la ciberdelincuencia juvenil en Ecuador?

Preguntas de investigación

- ¿Qué tan efectivas son las estrategias de educación digital implementadas en Ecuador para prevenir la ciberdelincuencia juvenil y reducir las tendencias y amenazas asociadas al entorno digital?
- ¿Cuáles son las principales formas de ciberdelincuencia que afectan a los jóvenes en Ecuador?
- ¿Qué iniciativas educativas existen en Ecuador para la prevención del cibercrimen juvenil y cuáles han sido sus resultados en términos de efectividad?

Capítulo 1 Marco teórico

1.1 La educación digital en Ecuador

La educación digital en Ecuador ha experimentado un notable crecimiento en los últimos años, especialmente impulsada por la necesidad de adaptarse a las nuevas tecnologías en el proceso educativo. Según Barberá (2021) el uso de plataformas digitales ha transformado las dinámicas pedagógicas, haciendo que la enseñanza sea más interactiva y accesible para los estudiantes. Este cambio también ha permitido una mayor personalización del aprendizaje, con herramientas que se ajustan a las necesidades específicas de cada alumno. Sin embargo, todavía existen desafíos significativos en términos de infraestructura y formación docente.

Para Suarez (2020) la pandemia de COVID-19 aceleró la adopción de herramientas digitales en el ámbito educativo en Ecuador, lo que se refleja en el aumento del uso de plataformas como Moodle, Google Classroom y otras aplicaciones que permiten la interacción remota entre estudiantes y docentes. Según una investigación de la Comisión Económica para América Latina y el Caribe (2020) el 85% de las instituciones educativas en Ecuador implementaron alguna forma de educación digital durante el confinamiento, lo que evidenció el potencial de las tecnologías en la

enseñanza, aunque también resalta las brechas en acceso y capacitación en ciertas regiones rurales del país.

La educación digital en Ecuador no solo ha sido una respuesta a la emergencia sanitaria, sino también una oportunidad para repensar la educación a largo plazo. Al respecto, Sánchez (2022) sostiene que la integración de la tecnología en el sistema educativo puede facilitar el acceso a contenidos actualizados y fomentar la participación activa de los estudiantes en su propio proceso de aprendizaje. No obstante, esta transición debe ser acompañada de políticas públicas que aseguren la equidad en el acceso a la tecnología, especialmente en las zonas más desfavorecidas.

En este contexto, la educación digital se presenta como una herramienta clave para el desarrollo educativo y social de Ecuador. Sin embargo, es crucial que el sistema educativo impulse una formación integral tanto para los docentes como para los estudiantes en el uso de tecnologías, como indica Diez (2020). De acuerdo con la autora, la formación continua de los educadores es esencial para la implementación efectiva de la educación digital, ya que son ellos quienes guiarán el uso adecuado de las herramientas tecnológicas en el aula.

1.2 Contexto actual de la educación digital en Ecuador

El contexto actual de la educación digital en Ecuador está marcado por la transición de un sistema educativo tradicional hacia uno más inclusivo y flexible, basado en el uso de las tecnologías. Según Loja (2020), la brecha digital en el país sigue siendo uno de los principales obstáculos para la implementación exitosa de la educación digital, especialmente en áreas rurales y de difícil acceso. A pesar de los esfuerzos por mejorar la conectividad, todavía existen regiones donde la infraestructura tecnológica es limitada, lo que afecta negativamente la calidad de la educación.

Además, la pandemia de COVID-19 dejó en evidencia la desigualdad en el acceso a dispositivos tecnológicos y a internet, lo que acentuó las disparidades en la educación tal y como indica Lugo (2020) aunque se han implementado iniciativas para proporcionar dispositivos y mejorar la conectividad, como el programa "Internet para Todos", los avances siguen siendo insuficientes para cubrir la totalidad de la población estudiantil en el país. Esto limita la efectividad de la educación digital, ya que no todos los estudiantes tienen las mismas oportunidades de acceso.

En cuanto a la formación docente, la situación también es variable. Según Loachamin (2023), aunque muchos profesores han recibido capacitación en herramientas digitales, la calidad de la formación es heterogénea y no todos los docentes tienen las competencias necesarias para integrar efectivamente las tecnologías en sus clases. Esto implica que la transición hacia una educación digital efectiva requiere, además de infraestructura, una capacitación constante para los educadores, para que puedan aprovechar al máximo las herramientas digitales disponibles.

Finalmente, el gobierno ecuatoriano ha reconocido la importancia de la educación digital en su agenda política, implementando diversas políticas públicas para fomentar el uso de la tecnología en las aulas. Sin embargo, como señala Camacho (2020) el éxito de estas políticas depende de la participación activa de todos los actores educativos, incluidos los estudiantes, padres de familia y la comunidad en general. Esto requiere un esfuerzo conjunto para garantizar que la educación digital sea accesible, inclusiva y de calidad para todos los estudiantes en Ecuador.

1.3 El acceso a la tecnología y su impacto en los jóvenes.

El acceso a la tecnología tiene un impacto significativo en el desarrollo académico y personal de los jóvenes en Ecuador. Según Vinces (2022), los estudiantes que tienen acceso a dispositivos tecnológicos y a internet muestran un mejor desempeño

académico debido a la posibilidad de acceder a una mayor cantidad de recursos educativos. Estos recursos incluyen plataformas de aprendizaje en línea, bibliotecas digitales y otros materiales que complementan su educación formal. De esta manera, la tecnología se convierte en una herramienta poderosa para fomentar el aprendizaje autónomo.

Sin embargo, no todo el acceso a la tecnología es equitativo, y las desigualdades en el acceso a dispositivos y conectividad afectan a los jóvenes en áreas rurales y marginalizadas. Según Loeza (2021), la falta de acceso a estas herramientas digitales genera una brecha de conocimiento y habilidades entre los jóvenes de diferentes regiones del país, lo que puede afectar su futuro académico y profesional. Esta brecha digital es una de las principales barreras para lograr una educación inclusiva y de calidad, que permita a todos los jóvenes desarrollar su potencial.

Además, el impacto de la tecnología en los jóvenes va más allá del ámbito académico. Según Pérez y Lodoño (2022), el uso de las redes sociales y otras plataformas digitales también influye en el desarrollo social y emocional de los jóvenes. Si bien estas herramientas pueden ser beneficiosas para la interacción social y el desarrollo de habilidades digitales, también presentan riesgos, como el ciberacoso y la exposición a contenidos inapropiados. Por lo tanto, es crucial que los jóvenes reciban una formación adecuada sobre el uso responsable y seguro de la tecnología.

A pesar de los desafíos, la tecnología ofrece una oportunidad para que los jóvenes en Ecuador desarrollen competencias clave para el siglo XXI, como el pensamiento crítico, la creatividad y la resolución de problemas. Para Lago (2021), la integración de las tecnologías digitales en el proceso educativo puede motivar a los jóvenes a participar activamente en su aprendizaje y explorar nuevas formas de adquirir conocimientos. Para aprovechar este potencial, es esencial que el acceso a la

tecnología sea universal y que se implementen políticas educativas que fomenten un uso equilibrado y responsable de las herramientas digitales.

1.4 La integración de la educación digital en el currículo escolar

La integración de la educación digital en el currículo escolar es un proceso complejo que requiere una planificación estratégica y un enfoque pedagógico adecuado. Según Ledesma (2022), la incorporación de tecnologías en el currículo debe ser gradual y adaptada a las necesidades y características de los estudiantes. Además, esta integración debe ir más allá de la simple incorporación de herramientas digitales, y debe implicar un cambio en los métodos de enseñanza y aprendizaje, promoviendo el uso de recursos digitales para la investigación, la colaboración y el desarrollo de habilidades críticas.

En Ecuador, la integración de la educación digital en el currículo escolar enfrenta desafíos significativos, principalmente relacionados con la falta de formación docente y la infraestructura limitada. Según Del Carmen (2022) indica que muchos docentes carecen de los conocimientos necesarios para diseñar e implementar estrategias pedagógicas que aprovechen al máximo las herramientas digitales. Por lo tanto, es esencial proporcionar formación continua a los maestros para que puedan integrar la tecnología de manera efectiva en sus clases.

Además, la implementación de la educación digital en el currículo requiere una revisión de los contenidos y métodos tradicionales de enseñanza. Según García (2022), el currículo escolar debe incluir el desarrollo de competencias digitales, como la alfabetización informática, la capacidad de trabajar con herramientas digitales y la habilidad para navegar en entornos virtuales. Esto permitirá a los estudiantes no solo adquirir conocimientos específicos, sino también desarrollar habilidades esenciales para el mundo laboral y la vida cotidiana.

Finalmente, la integración de la educación digital debe ser acompañada de políticas públicas que promuevan la innovación educativa y el uso equitativo de la tecnología. Según Loayza (2023) la inclusión de la educación digital en el currículo escolar debe ser vista como una inversión a largo plazo que beneficie tanto a los estudiantes como a la sociedad en general. Esto implica un compromiso de los gobiernos, las instituciones educativas y la comunidad en general para garantizar que la educación digital sea accesible, inclusiva y de calidad para todos los estudiantes en Ecuador.

1.5 Concepto de alfabetización digital

La alfabetización digital hace referencia a la capacidad de una persona para utilizar de manera efectiva las tecnologías digitales, especialmente aquellas relacionadas con el acceso y el uso de internet. Según Reyes (2021), la alfabetización digital implica más que simplemente saber usar una computadora; se trata de tener las competencias necesarias para comprender y gestionar información digital de manera crítica y segura. En la sociedad actual, donde la tecnología avanza rápidamente, estas habilidades se han convertido en esenciales para el acceso a la información, la participación en actividades económicas y sociales, y la educación continua.

Para Ascencio (2021) la alfabetización digital no solo abarca el uso de herramientas tecnológicas, sino también la capacidad para evaluar la calidad y fiabilidad de la información en línea. De acuerdo con estos autores, es crucial que los individuos puedan discernir entre fuentes confiables y aquellas que pueden ser engañosas o fraudulentas. Esto es particularmente importante en un mundo lleno de información contradictoria, donde las noticias falsas y la desinformación son comunes.

Además, la alfabetización digital involucra la comprensión de los riesgos asociados al uso de la tecnología. Según García y Martínez (2021), los usuarios deben ser conscientes de las amenazas cibernéticas y de las implicaciones de compartir información personal en

línea. La capacidad de proteger la privacidad personal y profesional, al mismo tiempo que se gestionan de forma segura los datos, es una parte fundamental de la alfabetización digital moderna.

En términos educativos, varios estudios han resaltado la necesidad de integrar la alfabetización digital en el currículo escolar. Samaniego (2024) sostiene que los jóvenes que están bien informados sobre las herramientas digitales tienen más probabilidades de adaptarse rápidamente a nuevos entornos tecnológicos y de hacer un uso responsable de internet. Por tanto, fomentar esta alfabetización desde edades tempranas es clave para preparar a los estudiantes para los desafíos del mundo digital.

1.6 La importancia de la formación en seguridad en línea

La formación en seguridad en línea es esencial para prevenir riesgos cibernéticos y proteger a los usuarios de las amenazas que existen en internet. Según Anton (2022), enseñar a los usuarios, especialmente a los jóvenes, sobre prácticas seguras en línea es fundamental para evitar fraudes, robo de identidad y otros tipos de ciberdelitos. Los jóvenes, al ser más vulnerables debido a su experiencia limitada, deben recibir educación continua sobre cómo proteger sus cuentas personales y cómo identificar posibles riesgos en la red.

De acuerdo con Monzón (2020), la falta de formación en seguridad en línea puede tener consecuencias graves para los individuos, incluyendo la exposición a virus informáticos, el secuestro de datos y el fraude financiero. La educación sobre temas como contraseñas seguras, la protección de la información personal y el uso adecuado de redes sociales es clave para minimizar estos riesgos. Además, la formación ayuda a crear una cultura de seguridad que se extiende a la comunidad en general.

En este sentido, la capacitación sobre seguridad en línea también desempeña un papel vital en la prevención de delitos cibernéticos. Según Del Pino (2023), los cibercriminales suelen

explotar la falta de conocimiento de los usuarios sobre prácticas de seguridad básicas, como el uso de software antivirus o la importancia de mantener actualizado el sistema operativo. Enseñar a los usuarios a reconocer las señales de advertencia de los ciberdelincuentes, como los correos electrónicos fraudulentos o los enlaces sospechosos, es fundamental para proteger la información personal y evitar ser víctima de estos delitos.

Finalmente, algunos expertos como Álvarez (2021) sugieren que la formación en seguridad en línea debe ser parte de la educación formal y continua. Las escuelas, universidades y organizaciones deben promover actividades que enseñen a los jóvenes a navegar de forma segura en la web, utilizando recursos interactivos, simulaciones y talleres prácticos. De esta manera, se puede crear una generación de usuarios de internet más consciente y mejor preparada para enfrentar los desafíos cibernéticos.

1.7 Herramientas y plataformas utilizadas para educar a los jóvenes sobre los riesgos en internet.

Existen diversas herramientas y plataformas diseñadas específicamente para educar a los jóvenes sobre los riesgos en internet y promover un comportamiento seguro en línea. Según Beltrán (2023), plataformas como "Common Sense Media" ofrecen recursos educativos para estudiantes y padres, proporcionando información sobre cómo navegar por internet de manera segura, y cómo identificar y evitar los peligros en línea, como el ciberacoso y el robo de identidad. Estas herramientas también ofrecen actividades interactivas que ayudan a los jóvenes a entender mejor los riesgos.

Otra herramienta popular es "NetSmartz", creada por el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC). Según Rubio (2020), esta plataforma ofrece una variedad de recursos educativos, como videos y juegos, que enseñan a los jóvenes sobre la seguridad en línea y la protección de su privacidad. La plataforma es especialmente útil

para sensibilizar a los adolescentes sobre los peligros del sexting, la ciberintimidación y el contacto con extraños en la web.

Tal como indica Calloapaza (2022), las redes sociales también están empezando a jugar un papel clave en la educación sobre los riesgos en internet. Plataformas como Instagram, Twitter y Facebook, a menudo en colaboración con expertos en seguridad cibernética, están implementando campañas y anuncios que promueven prácticas seguras, como el uso de contraseñas fuertes y la configuración de privacidad en las cuentas. Estas campañas tienen un gran alcance y son útiles para enseñar a los jóvenes cómo proteger su información personal mientras interactúan en estos espacios digitales.

Finalmente, plataformas de aprendizaje como "Khan Academy" y "Edmodo" también han comenzado a incorporar módulos sobre seguridad en línea en sus currículos. Según González y Pérez (2021), estas plataformas ofrecen contenido accesible que abarca desde conceptos básicos de seguridad en línea hasta temas más avanzados sobre la protección de datos. Estas herramientas ayudan a crear una base sólida de conocimiento sobre la seguridad digital que puede beneficiar a los estudiantes en su vida personal y profesional.

1.8 Ciberdelincuencia juvenil: definición y tipos de delitos

1.8.1 Concepto de ciberdelincuencia juvenil

La ciberdelincuencia juvenil se refiere a la realización de actividades ilícitas a través de medios digitales por parte de adolescentes. Según Gonzales (2023), este fenómeno involucra a menores de edad que utilizan tecnologías como internet, redes sociales y dispositivos electrónicos para cometer delitos que afectan tanto a individuos como a organizaciones. Estos delitos pueden incluir desde el acceso no autorizado a sistemas hasta el uso indebido de información personal, lo que pone en riesgo la seguridad de los datos de terceros. De acuerdo con Carrasco (2024), los jóvenes suelen verse atraídos por la

facilidad de anonimato y la falta de una vigilancia estricta en línea, lo que puede facilitar la perpetración de actos delictivos sin consecuencias inmediatas.

El concepto de ciberdelincuencia juvenil también se aborda en el contexto del desarrollo cognitivo y social de los adolescentes. Según González (2021), los adolescentes pueden ser vulnerables a influencias externas, como la presión social o la búsqueda de aceptación en grupos online, lo que aumenta a cometer delitos en internet. La ciberdelincuencia no solo incluye delitos graves, sino también conductas menos visibles, como el hacking ético no autorizado o el uso irresponsable de plataformas para propagar información falsa. Estos comportamientos pueden, con el tiempo, escalar hacia crímenes más graves si no se les aborda de manera temprana.

Además, la ciberdelincuencia juvenil plantea un desafío significativo en términos de la legislación y el control. Según Punín (2021) los sistemas legales en muchos países no están completamente preparados para enfrentar los delitos cometidos por menores en entornos digitales, lo que crea una brecha de protección. En muchos casos, los adolescentes no son plenamente conscientes de la magnitud de sus acciones, y la legislación vigente no siempre proporciona herramientas claras para sancionar estos delitos de manera efectiva. Es fundamental, por tanto, establecer un marco legal y educativo que pueda prevenir estos actos y ofrecer a las jóvenes alternativas positivas para el uso de las tecnologías.

Finalmente, el concepto de ciberdelincuencia juvenil debe incluir la comprensión de los impactos sociales y psicológicos de estas conductas. Según Arroyo (2020), los delitos informáticos cometidos por jóvenes pueden tener repercusiones duraderas en las víctimas, generando daños emocionales y financieros. Además, los jóvenes que participan en actividades delictivas en línea pueden experimentar problemas emocionales y legales, que pueden obstaculizar su desarrollo personal y académico. La prevención de la

ciberdelincuencia juvenil debe centrarse tanto en los efectos negativos para las víctimas como en los riesgos que enfrentan los propios jóvenes involucrados en estos delitos.

1.8.2 Los principales delitos informáticos cometidos por jóvenes

Entre los delitos informáticos más comunes cometidos por adolescentes se encuentran el ciberacoso, el robo de identidad y el fraude en línea. Según Chalen (2023), el ciberacoso se refiere a la utilización de plataformas digitales para intimidar, amenazar o difamar a otros usuarios, y es uno de los delitos más frecuentes entre los jóvenes. Este comportamiento puede manifestarse a través de mensajes, publicaciones en redes sociales o incluso en aplicaciones de mensajería instantánea. A menudo, los adolescentes recurren a estas plataformas para infligir daño a sus compañeros debido a la percepción de anonimato que otorgan estas herramientas. El ciberacoso puede tener consecuencias graves para las víctimas, incluyendo trastornos emocionales y, en casos extremos, suicidio.

Otro delito común es el robo de identidad, donde los jóvenes obtienen acceso ilegal a las cuentas de otras personas para robar su información personal y financiera. Según Ticona (2024), muchos adolescentes no comprenden completamente las implicaciones legales y personales del robo de identidad. Con el acceso a plataformas en línea y las crecientes habilidades tecnológicas de los jóvenes, esta práctica se ha vuelto más frecuente. Además, algunos jóvenes pueden verse atraídos por el deseo de obtener beneficios rápidos a través de la suplantación de identidad en actividades como compras fraudulentas o la apertura de cuentas bancarias falsas.

El fraude en línea también ha crecido entre los jóvenes como un delito informático común. De acuerdo con Sierra (2022), los adolescentes participan en actividades fraudulentas como la creación de perfiles falsos, la venta de productos inexistentes o el uso de tarjetas de crédito robadas para realizar compras. Este tipo de actividades ilícitas es facilitado por

la facilidad de acceso a internet y la proliferación de plataformas de compraventa en línea, donde los jóvenes pueden operar de manera casi invisible. A pesar de que muchos jóvenes no tienen la intención de causar daño a gran escala, la acumulación de pequeñas acciones fraudulentas puede resultar en grandes pérdidas para las víctimas.

El hacking y el acceso no autorizado a sistemas también están presentes en la ciberdelincuencia juvenil. Según Hernández (2021), algunos adolescentes desarrollan habilidades avanzadas en programación y ciberseguridad, pero las utilizan para hackear cuentas, plataformas o bases de datos sin el permiso de los propietarios. Este tipo de delitos pueden ser el resultado de la curiosidad o la necesidad de desafiar las reglas, sin que el joven comprenda completamente las consecuencias legales de sus actos. Los adolescentes que participan en el hacking pueden enfrentar consecuencias legales severas si sus actividades son detectadas por las autoridades.

1.8.3 Factores de riesgo que favorecen la ciberdelincuencia en adolescentes

Existen varios factores de riesgo que pueden contribuir a la ciberdelincuencia en adolescentes, entre los que se incluyen la falta de supervisión parental, el acceso ilimitado a internet y las influencias sociales. Según Ramos (2023) la falta de supervisión de los padres sobre el uso que los adolescentes hacen de internet es uno de los principales factores que favorecen la ciberdelincuencia juvenil. Cuando los padres no establecen límites claros o no están al tanto de las actividades en línea de sus hijos, estos últimos tienen mayor libertad para participar en comportamientos delictivos. La falta de vigilancia permite que los adolescentes accedan a sitios peligrosos, interactúen con personas desconocidas o cometan delitos en línea sin enfrentar consecuencias inmediatas.

Otro factor importante es el acceso ilimitado a internet. Según Fernández (2020), la facilidad con la que los jóvenes pueden acceder a dispositivos conectados a internet aumenta las posibilidades de involucrarse en ciberdelincuencia. Muchos adolescentes

pasan largas horas en línea, lo que puede llevar a una exposición excesiva a contenidos inapropiados o delictivos. Sin una orientación adecuada sobre el uso responsable de la tecnología, los jóvenes pueden ser fácilmente influenciados por otras personas para involucrarse en actividades ilegales. Además, el constante acceso a plataformas de redes sociales y aplicaciones de mensajería les permite actuar sin restricciones, facilitando la realización de actos delictivos.

Las influencias sociales también juegan un papel importante en la ciberdelincuencia juvenil. Según García (2021), los adolescentes pueden verse impulsados a cometer delitos en línea debido a la presión de sus amigos o el deseo de ser aceptados en ciertos grupos. Las redes sociales y los foros en línea a menudo promueven una cultura de desafíos y competencia, donde los jóvenes pueden sentirse motivados a realizar actos ilegales para ganar reconocimiento o estatus dentro de su círculo social. Esta dinámica puede generar un entorno propenso a la perpetración de delitos informáticos, ya que la oportunidad de obtener "likes" o seguidores a menudo se asocia con comportamientos audaces e incluso ilícitos.

Finalmente, el desarrollo de la personalidad en la adolescencia también puede contribuir a la ciberdelincuencia. Según Herrerías (2025), los adolescentes, debido a su etapa de búsqueda de identidad, pueden experimentar una falta de juicio o una desconexión entre sus acciones y las consecuencias de estas. Este proceso de exploración de límites y autonomía puede llevar a algunos jóvenes a realizar actividades en línea sin considerar la gravedad de sus actos. Además, la percepción de anonimato en internet puede disminuir la sensación de responsabilidad, lo que hace que los adolescentes se sientan más inclinados a cometer delitos informáticos sin temer consecuencias.

1.9 Factores de protección para la ciberdelincuencia juvenil

1.9.1 El rol de la familia, la escuela y la comunidad en la prevención.

La familia desempeña un papel crucial en la prevención de la ciberdelincuencia juvenil. Según Torrado (2021), el vínculo familiar sólido y el monitoreo de las actividades en línea de los hijos pueden reducir significativamente el riesgo de involucrarse en actividades delictivas en internet. La presencia activa de los padres, especialmente en la supervisión de los hábitos digitales, crea un entorno seguro que protege a los jóvenes de los peligros asociados con el uso irresponsable de la tecnología. Además, la comunicación abierta sobre los riesgos de la web, como la exposición a contenidos inapropiados o el contacto con personas desconocidas, también juega un rol fundamental en la prevención de comportamientos peligrosos en línea (Rodríguez, 2020).

La escuela, como un espacio educativo y formativo, tiene un impacto directo en la formación de los jóvenes en cuanto a la seguridad digital. Según Martínez (2021), los programas de educación digital en las escuelas son esenciales para enseñar a los estudiantes sobre el uso responsable de la tecnología y los riesgos asociados con la ciberdelincuencia. A través de la implementación de talleres y cursos específicos sobre ciberseguridad, los jóvenes adquieren herramientas para identificar amenazas y protegerse de posibles ataques o estafas en línea. Además, los docentes pueden fomentar valores como el respeto y la ética digital, contribuyendo a crear una cultura de responsabilidad en el entorno virtual (Gómez, 2022).

La comunidad también juega un papel fundamental en la prevención de la ciberdelincuencia juvenil, ya que las redes de apoyo social pueden influir en las decisiones de los jóvenes en línea. Según Sánchez (2018), la participación en actividades comunitarias y el acceso a programas de concientización sobre ciberseguridad contribuyen a crear un entorno social que protege a los jóvenes. Los programas comunitarios

orientados a la educación digital no solo informan sobre los riesgos, sino que también ofrecen alternativas positivas de ocupación para los adolescentes, disminuyendo las probabilidades de que busquen soluciones en actividades ilícitas en línea (Vázquez, 2019). Por tanto, la cooperación entre familia, escuela y comunidad es clave para prevenir la ciberdelincuencia juvenil.

Finalmente, la cooperación interinstitucional es un factor relevante en la prevención de la ciberdelincuencia juvenil. En este sentido, Seguil (2023) destacan que los esfuerzos combinados de instituciones gubernamentales, educativas y sociales son necesarios para implementar políticas públicas que aborden la problemática de manera integral. Estos esfuerzos permiten desarrollar estrategias de prevención adaptadas a las necesidades específicas de cada contexto social y familiar, asegurando así una mayor eficacia en la reducción de la ciberdelincuencia entre los jóvenes.

1.9.2 La influencia de las redes sociales y los videojuegos en el comportamiento de los jóvenes

Las redes sociales han demostrado ser una de las plataformas más influyentes en la vida de los jóvenes, modelando su comportamiento y, en algunos casos, impulsándolos hacia la ciberdelincuencia. Según Rodríguez (2021), las redes sociales permiten la creación de identidades virtuales que pueden llevar a los jóvenes a involucrarse en conductas riesgosas, como el acoso en línea o la divulgación de información personal que facilita el fraude o el robo de identidad. Esta influencia se ve reforzada por la necesidad de aceptación social, lo que puede llevar a los adolescentes a tomar decisiones impulsivas sin considerar las consecuencias legales o morales de sus actos (Martín, 2019).

Los videojuegos, por su parte, también han sido señalados como un factor de riesgo en la ciberdelincuencia juvenil. Según Ruiz (2021), ciertos videojuegos de contenido violento o con mecánicas que premian el comportamiento antisocial pueden fomentar actitudes

despectivas hacia las normas sociales. Estos juegos, a menudo de interacción en línea, pueden ofrecer una vía para que los jóvenes se conecten con otras personas que fomentan comportamientos ilícitos, como el hacking o el fraude digital. Además, los videojuegos en línea pueden ser un espacio propenso para el engaño, donde los delincuentes pueden manipular a los jugadores más jóvenes y vulnerables.

La interacción de los jóvenes con las redes sociales y los videojuegos también está vinculada a la adicción digital, un factor que puede aumentar la vulnerabilidad a la ciberdelincuencia. Según Huamani (2022), el uso excesivo de estas plataformas puede aislar a los jóvenes de su entorno social y familiar, reduciendo la capacidad de tomar decisiones racionales y éticas. Este aislamiento puede hacer que los jóvenes sean más susceptibles a las influencias negativas en línea y más propensos a involucrarse en actividades peligrosas sin reconocer el daño que causan a otras personas o a ellos mismos (Gómez, 2021).

Por otro lado, Pérez y López (2018), destacan que las redes sociales y los videojuegos también pueden tener un impacto positivo si se gestionan adecuadamente. Si los jóvenes aprenden a utilizar estas herramientas para fines educativos, de entretenimiento positivo y con la guía adecuada, pueden evitar los riesgos asociados. Es crucial que padres, educadores y la comunidad en general se involucren en el monitoreo y la educación sobre el uso responsable de estas plataformas, para que los jóvenes desarrollen una actitud crítica frente a los riesgos y las amenazas que enfrentan en línea.

1.9.3 El desconocimiento de los riesgos tecnológicos y sus consecuencias legales

El desconocimiento de los riesgos tecnológicos es uno de los factores más relevantes en la ciberdelincuencia juvenil. Según Rojas (2022), muchos jóvenes no comprenden completamente las consecuencias legales que pueden derivarse de sus acciones en línea, como el robo de identidad, el hackeo o el envío de contenido ilícito. Este desconocimiento

puede llevarlos a cometer delitos sin ser conscientes de la gravedad de sus actos. La falta de educación sobre las leyes digitales y las sanciones legales puede incentivar una sensación de impunidad entre los jóvenes, lo que aumenta la probabilidad de que se involucren en actividades delictivas sin temor a ser castigados.

El desconocimiento de las implicaciones legales de la ciberdelincuencia se ve amplificado por la facilidad con la que los jóvenes pueden acceder a herramientas digitales que facilitan la realización de delitos. Tal como menciona Ramírez (2020), la disponibilidad de software de hacking, aplicaciones para la manipulación de datos personales y servicios de pago en línea anónimos han permitido que los jóvenes cometan delitos sin una comprensión adecuada de las consecuencias legales. A menudo, estos delitos son considerados como simples travesuras, ya que los infractores no son conscientes de la legislación vigente ni de los daños que pueden causar a otras personas o empresas.

Además, el desconocimiento de los riesgos tecnológicos también afecta a la capacidad de los jóvenes para protegerse de los ciberataques. Según Cadillo (2023), los adolescentes no siempre están capacitados para reconocer las amenazas cibernéticas, como los virus, el phishing o el malware. Esto los hace vulnerables a los delitos digitales, como el robo de información personal o el ransomware en línea. La falta de educación sobre ciberseguridad y protección en línea es un factor clave que contribuye al aumento de la ciberdelincuencia juvenil.

Por último, una de las formas de contrarrestar este desconocimiento es la implementación de programas educativos en las escuelas y en las comunidades. Según Sánchez (2021), la educación en ciberseguridad es fundamental para que los jóvenes comprendan no solo los riesgos asociados con la tecnología, sino también las repercusiones legales de sus acciones en línea. Al proporcionar una formación adecuada sobre las leyes digitales y la seguridad

en línea, se puede reducir el riesgo de ciberdelincuencia juvenil y empoderar a los jóvenes para que naveguen por internet de manera responsable y segura.

1.10 El rol del gobierno y las instituciones en la protección de los jóvenes frente a la ciberdelincuencia

1.10.1 Políticas públicas en Ecuador relacionadas con la protección digital y la ciberdelincuencia

En Ecuador, las políticas públicas orientadas a la protección digital y la prevención de la ciberdelincuencia se han venido desarrollando a lo largo de los últimos años. Conforme lo expresado por Mecias (2024), el gobierno ecuatoriano ha reconocido la creciente amenaza que representa la ciberdelincuencia para los jóvenes y ha comenzado a implementar estrategias para mitigar los riesgos asociados. El Ministerio de Telecomunicaciones y de la Sociedad de la Información ha promovido diversas iniciativas para crear un marco normativo y preventivo que asegure el bienestar de los menores de edad en el entorno digital. Estas políticas no solo están enfocadas en la protección, sino también en la promoción de un uso responsable de las tecnologías de la información.

El enfoque de las políticas públicas ecuatorianas ha sido integral, buscando la cooperación entre instituciones gubernamentales, organizaciones no gubernamentales y actores internacionales. De acuerdo con Juca (2023), el fortalecimiento de las políticas de ciberseguridad en Ecuador se ha convertido en una prioridad, dada la vulnerabilidad de la población joven ante la ciberdelincuencia. En este contexto, el gobierno ha impulsado la creación de campañas informativas que alertan a los jóvenes sobre los riesgos de las redes sociales, el fraude electrónico y el acoso cibernético. La implementación de políticas públicas busca empoderar a los jóvenes con las herramientas necesarias para navegar por Internet de manera segura y responsable.

Sin embargo, a pesar de los esfuerzos realizados, algunos expertos señalan que la implementación efectiva de estas políticas sigue enfrentando obstáculos. Según Pérez (2022), la falta de recursos y la capacitación insuficiente en áreas clave de la ciberseguridad dificultan una protección integral de los jóvenes. A pesar de estos desafíos, las políticas públicas siguen evolucionando, y cada vez son más las instituciones que se suman a esta causa. Así, la colaboración interinstitucional se presenta como un factor clave para garantizar la seguridad digital en Ecuador.

Por otro lado, la vigilancia y monitoreo constante de las actividades cibernéticas en el país se ha convertido en una estrategia fundamental. Al respecto, Esquivel (2023) menciona que las políticas gubernamentales deben estar acompañadas de un sistema de monitoreo eficiente que permita detectar actividades ilegales en tiempo real, especialmente cuando se trata de menores involucrados en delitos cibernéticos. Este tipo de medidas debe ser complementado con una mayor cooperación internacional en la lucha contra la ciberdelincuencia, particularmente en el ámbito de la trata de personas y el abuso infantil en línea.

1.10.2 La legislación ecuatoriana sobre ciberdelincuencia y su aplicación en menores de edad

La legislación ecuatoriana ha avanzado en la creación de normas que regulan el uso de las tecnologías de la información y combaten la ciberdelincuencia, especialmente en lo que respecta a los menores de edad. Según Trucios (2023), el Código Orgánico Integral Penal (COIP) ha establecido sanciones específicas para delitos como el acceso no autorizado a sistemas informáticos, el ciberacoso y la distribución de material pornográfico infantil. Estas leyes buscan brindar una respuesta adecuada a las víctimas menores de edad y garantizar la protección de sus derechos en el entorno digital. Sin embargo, el desafío sigue siendo la correcta aplicación de estas normativas, ya que

muchos de estos delitos se cometen fuera del ámbito nacional, lo que complica su transnacionalidad.

A pesar de la existencia de esta legislación, varios expertos coinciden en que es necesario fortalecer la aplicación efectiva de la ley, especialmente en casos que involucren a menores de edad. Según Vargas (2020), aunque el marco legal es adecuado, la implementación en casos específicos relacionados con jóvenes aún enfrenta debilidades. La capacitación y especialización de los cuerpos de seguridad, junto con un sistema judicial ágil, son esenciales para hacer frente a la ciberdelincuencia que afecta a los jóvenes. Además, Pérez (2021) señala que la legislación debe adaptarse continuamente a los avances tecnológicos, ya que las formas de ciberdelincuencia evolucionan rápidamente y surgen nuevos riesgos constantemente.

La protección de los menores de edad también ha implicado un esfuerzo por parte de las autoridades para sensibilizar sobre las implicaciones legales del mal uso de las tecnologías. De acuerdo con Guamán (2022), campañas de sensibilización han sido impulsadas para educar tanto a los jóvenes como a sus padres sobre los peligros de los delitos cibernéticos y las responsabilidades legales que implica el uso inapropiado de la tecnología. En este sentido, la educación en derechos digitales y las consecuencias legales de la ciberdelincuencia se presentan como una herramienta preventiva de gran relevancia.

Finalmente, según Saltos (2021) una de las áreas donde la legislación ecuatoriana aún necesita mejorar es en la protección de los datos personales de los menores. Aunque existen leyes como la Ley de Protección de Datos Personales, su aplicación en el contexto digital sigue siendo incipiente. Es fundamental que las leyes no solo castiguen los delitos, sino que también protejan de manera más efectiva la privacidad

y los derechos fundamentales de los jóvenes en el mundo virtual. En este sentido, Vargas se destaca la necesidad urgente de reforzar la legislación en torno a la protección de la identidad digital y la privacidad de los menores en línea.

1.10.3 Iniciativas del gobierno para fomentar una educación digital segura

El gobierno de Ecuador ha impulsado diversas iniciativas para promover una educación digital segura entre los jóvenes, con el objetivo de protegerlos de los riesgos asociados con el uso de la tecnología. Conforme a lo señalado por Hueso (2020), uno de los principales esfuerzos ha sido la implementación de programas de alfabetización digital en las escuelas, donde se enseña a los estudiantes no solo a utilizar las tecnologías, sino también a hacerlo de forma responsable y segura. Estas iniciativas buscan dotar a los jóvenes de las habilidades necesarias para reconocer y evitar los peligros en línea, como el ciberacoso, la manipulación y las estafas digitales.

Además, el Ministerio de Educación (2022) ha trabajado en colaboración con expertos en ciberseguridad para diseñar contenidos educativos que aborden específicamente los riesgos digitales. Donde se han implementado módulos de educación en línea que cubren temas como la protección de la privacidad, la seguridad en redes sociales y el respeto hacia los demás en el entorno digital. Estos contenidos buscan sensibilizar a los jóvenes sobre las consecuencias de las acciones inapropiadas en línea y fomentar el uso responsable de Internet.

Por otro lado, el gobierno ecuatoriano ha fomentado la creación de alianzas entre instituciones públicas y privadas para promover una cultura digital segura. Según Pineda (2023), el gobierno ha trabajado con empresas tecnológicas para ofrecer recursos educativos y herramientas de protección a los jóvenes. Estas alianzas también han permitido la implementación de sistemas de alerta temprana para detectar posibles riesgos digitales a los que los jóvenes puedan estar expuestos, como el ciberacoso o la

trata de personas en línea. La colaboración entre el sector público y privado es clave para garantizar una respuesta efectiva ante los riesgos digitales.

Finalmente, algunas de las iniciativas más recientes del gobierno han incluido la creación de espacios de debate y sensibilización sobre la seguridad digital. Como indica Calle (2024), el gobierno ha organizado foros y talleres en los que se invita tanto a jóvenes como a educadores y padres de familia para discutir sobre la importancia de la ciberseguridad.

Capitulo II Metodología

2.1 Enfoque de investigación

El enfoque de la investigación fue mixto, combinando tanto el cuantitativo como el cualitativo. Esta combinación permitió obtener una comprensión completa sobre la efectividad de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador.

La parte cuantitativa se centró en la medición y evaluación de las estrategias educativas mediante encuestas. Se buscó obtener datos estadísticos sobre la efectividad de las iniciativas de educación digital para prevenir ciberdelitos entre los jóvenes, así como su impacto en la reducción de las tendencias relacionadas con el cibercrimen.

El componente cualitativo consistió en entrevistas semiestructuradas y grupos focales con docentes y estudiantes para profundizar en las percepciones, actitudes y experiencias de los jóvenes frente a la ciberdelincuencia. Esto permitió captar de forma detallada las opiniones y vivencias sobre las iniciativas educativas y su relación con la prevención de la ciberdelincuencia juvenil.

La combinación de ambos enfoques garantizó una visión más completa del fenómeno en estudio y facilitó la triangulación de los datos, aumentando la validez y fiabilidad de los resultados.

2.2 Tipo de investigación

La investigación fue de tipo descriptivo y explicativo. El enfoque descriptivo permitió detallar y caracterizar las diferentes formas de ciberdelincuencia que afectaron a los jóvenes en Ecuador. Además, se describieron las iniciativas educativas existentes, cómo se implementaron y cómo los estudiantes percibieron la educación digital en relación con la prevención de la ciberdelincuencia. A través del enfoque explicativo, se intentó determinar las relaciones causales entre las estrategias educativas de prevención y la disminución de la ciberdelincuencia juvenil. Se analizaron las formas de ciberdelito más comunes y cómo las iniciativas educativas influyeron en las actitudes y comportamientos de los jóvenes con respecto a la seguridad digital.

Este tipo de investigación también permitió examinar los factores que contribuyeron al éxito o fracaso de las iniciativas educativas, aportando información clave para la mejora de las políticas públicas y programas educativos en el ámbito de la ciberseguridad juvenil.

2.3 Población y muestra

Población

La población de esta investigación estuvo compuesta por estudiantes de educación secundaria y docentes de instituciones educativas dentro del Cantón Vinces, Provincia de los Rios, particularmente aquellos involucrados en programas relacionados con la educación digital y la prevención de ciberdelincuencia. La población objetivo incluyó jóvenes de entre 12 y 18 años, además de los educadores responsables de implementar programas de sensibilización sobre los riesgos digitales y la ciberseguridad.

Muestra

La muestra fue seleccionada de manera no probabilística e intencional. Se seleccionaron un total de 150 a 200 estudiantes de diversas instituciones educativas del Cantón Vinces, que participaron en programas educativos sobre ciberseguridad. Además, se incluyeron 30 docentes de estas mismas instituciones, los cuales fueron responsables de implementar dichas iniciativas educativas.

La selección de la muestra se basó en la experiencia directa de los participantes con los programas educativos de prevención de ciberdelincuencia, asegurando que los participantes tuvieran un conocimiento adecuado sobre el tema de estudio.

2.4 Operacionalización de variables

Tabla 1
operacionalización de las variables

Variable	Indicador	Dimensión	Ítem
Estrategias educativas	Tipos de programas implementados	Estrategias educativas digitales	1. Estrategias de sensibilización en ciberseguridad
	Porcentaje de instituciones que aplicaron estrategias educativas	Tipo de intervención educativa	2. Uso de plataformas educativas para la prevención de delitos
	Porcentaje de estudiantes que recibieron educación sobre ciberseguridad	Integración en el currículo académico	3. Frecuencia de talleres, cursos o actividades formativas
Efectividad de la educación digital	Resultados percibidos en la reducción de ciberdelitos	Impacto en la prevención de ciberdelincuencia	1. Cambios en el comportamiento digital de los jóvenes
	Cambios en las actitudes de los estudiantes hacia la seguridad digital	Conocimiento sobre ciberdelincuencia	2. Conocimiento sobre medidas preventivas
Formas de ciberdelincuencia	Tipos de ciberdelitos más comunes	Conocimiento sobre ciberdelincuencia juvenil	1. Ciberacoso, fraude, robo de identidad, etc.

	Incidencia de ciberdelincuencia juvenil en la comunidad estudiantil	Actitudes hacia los riesgos cibernéticos	2. Percepción del riesgo digital entre los estudiantes

2.5 Técnicas e instrumentos de recolección de información

Para la recolección de información, se emplearon tres técnicas principales: encuestas, entrevistas semiestructuradas y grupos focales. Estas técnicas permitieron abordar tanto el aspecto cuantitativo como cualitativo de la investigación, garantizando una recopilación de datos diversa y completa.

Encuestas

Se utilizaron encuestas estructuradas como técnica principal para obtener datos cuantitativos de los estudiantes y docentes. Estas encuestas se diseñaron con el objetivo de evaluar el nivel de conocimiento de los jóvenes sobre los riesgos de ciberdelincuencia, las estrategias educativas implementadas y la efectividad de las iniciativas de educación digital. Las encuestas fueron distribuidas de manera presencial en las instituciones seleccionadas y contaron con preguntas cerradas y una escala Likert para medir las actitudes y percepciones de los participantes respecto a la educación digital en relación con la ciberdelincuencia. La información obtenida a través de estas encuestas fue analizada estadísticamente para identificar patrones y correlaciones relevantes entre la educación digital y la reducción de comportamientos de riesgo.

Entrevistas semiestructuradas

Las entrevistas semiestructuradas fueron realizadas con docentes, coordinadores de programas educativos y expertos en ciberseguridad. A diferencia de las encuestas, las entrevistas permitieron obtener información más profunda sobre la implementación de las estrategias educativas, los desafíos encontrados en el proceso y las percepciones de los

docentes sobre la efectividad de estas iniciativas. Las preguntas abiertas de la entrevista permitieron explorar las experiencias y opiniones de los entrevistados de manera detallada. Además, las entrevistas proporcionaron un contexto más amplio sobre la relación entre la formación académica y la prevención del cibercrimen, ayudando a contextualizar los datos cuantitativos obtenidos a través de las encuestas.

Instrumentos de recolección

Para la implementación de estas técnicas, se diseñaron instrumentos específicos adaptados a cada una de las técnicas utilizadas. Para las encuestas, se desarrolló un cuestionario estructurado que incluía tanto preguntas cerradas como de escala Likert, lo que facilitó la cuantificación de los datos y permitió obtener información sobre el nivel de conocimiento y las actitudes de los participantes. En el caso de las entrevistas, se diseñó una guía de entrevista semiestructurada que contenía preguntas abiertas enfocadas en los desafíos y experiencias de los docentes y expertos en la implementación de estrategias educativas. Finalmente, para los grupos focales, se preparó una guía de discusión con temas clave sobre la ciberdelincuencia y la efectividad de las iniciativas educativas, lo que permitió obtener un análisis más exhaustivo y detallado de las percepciones y opiniones de los jóvenes.

2.6 Procedimientos del proceso de investigación

El proceso de investigación se desarrolló siguiendo una serie de pasos ordenados, con el fin de garantizar la validez y la coherencia en la recolección de información, así como en el análisis de los resultados obtenidos.

Fase de planificación

En primer lugar, se llevó a cabo una fase de planificación en la cual se definieron los objetivos de la investigación, los instrumentos a utilizar, y las instituciones que formarían parte de la muestra. Durante esta fase, se elaboró un cronograma detallado que organizaba

las actividades y las fechas clave para cada etapa del proceso. La selección de la muestra de instituciones educativas se realizó de forma intencionada, tomando en cuenta aquellos centros que implementaran alguna estrategia educativa relacionada con la prevención de la ciberdelincuencia juvenil. Además, en esta fase se diseñaron los instrumentos de recolección de datos, como las encuestas, las guías de entrevistas y las guías para los grupos focales, asegurando que fueran adaptados a las características del contexto educativo y del público objetivo.

Fase de recolección de datos

Una vez definida la muestra y los instrumentos, se procedió a la recolección de datos. Este proceso se realizó de manera presencial en las instituciones educativas seleccionadas. Las encuestas fueron aplicadas a los estudiantes de secundaria, con la colaboración de los docentes encargados de facilitar el acceso a los alumnos. Las encuestas fueron entregadas en grupos y recogidas al finalizar el periodo de respuesta. Las entrevistas semiestructuradas fueron realizadas en un entorno controlado, con los docentes, coordinadores y expertos en ciberseguridad, quienes fueron convocados con antelación para garantizar su disponibilidad. Estas entrevistas fueron grabadas con el consentimiento de los participantes para permitir un análisis detallado de las respuestas. En paralelo, se organizaron los grupos focales, los cuales se desarrollaron en un ambiente cómodo y relajado, permitiendo a los estudiantes expresar sus opiniones sobre las estrategias educativas y su percepción de las amenazas cibernéticas. Los grupos focales fueron moderados por un investigador especializado, quien guió las discusiones de acuerdo con los temas predefinidos en la guía de discusión.

Fase de análisis de datos

Una vez recolectados todos los datos, se procedió a la fase de análisis. Los datos obtenidos de las encuestas fueron procesados y analizados estadísticamente utilizando software

especializado, lo que permitió identificar patrones de conocimiento y actitudes entre los jóvenes hacia la ciberdelincuencia y las estrategias educativas implementadas. Para las entrevistas y los grupos focales, se realizó un análisis cualitativo mediante la codificación de las respuestas y la identificación de temas recurrentes, desafíos comunes y estrategias educativas efectivas. El análisis cualitativo permitió integrar la información obtenida en las encuestas con las percepciones de los expertos y de los estudiantes, proporcionando un panorama más completo sobre la efectividad de las iniciativas educativas.

Fase de interpretación de resultados

Con base en el análisis de los datos, se procedió a la interpretación de los resultados. En esta fase, los resultados cuantitativos y cualitativos fueron comparados y contrastados para obtener conclusiones relevantes sobre la efectividad de las estrategias educativas en la prevención de la ciberdelincuencia juvenil en Ecuador. Además, se identificaron las principales formas de ciberdelincuencia que afectan a los jóvenes, así como las iniciativas educativas existentes en el país. La interpretación de los resultados permitió establecer recomendaciones para mejorar las estrategias de prevención, así como sugerir nuevas formas de abordar el problema en el sistema educativo ecuatoriano.

Fase de presentación de resultados

Finalmente, los resultados obtenidos fueron presentados en un informe final. En este informe, se incluyeron tanto los hallazgos cuantitativos como cualitativos, así como las conclusiones y recomendaciones. El informe también incluyó gráficos y tablas que facilitaron la visualización de los datos y proporcionaron una base sólida para las recomendaciones propuestas. Este informe fue compartido con las autoridades educativas y expertos en ciberseguridad, con el fin de contribuir a la mejora de las políticas educativas y las estrategias de prevención de ciberdelincuencia en el ámbito juvenil.

Capítulo III Resultados

Con el objetivo de evaluar la efectividad de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador, se aplicó una encuesta a una muestra de 385 personas. La encuesta permitió identificar las principales formas de ciberdelincuencia que afectan a la juventud, así como analizar las iniciativas educativas existentes en el país para prevenir estos delitos. A continuación, se presentan los resultados obtenidos, los cuales reflejan la percepción de la población sobre la accesibilidad, efectividad y desafíos de la educación digital en este contexto.

3.1 Resultados de la encuesta

Tabla 2
¿Qué tan efectiva considera la educación digital en la prevención de la ciberdelincuencia juvenil?

Respuesta	Frecuencia	Porcentaje (%)
Muy efectiva	107	27.79%
Algo efectiva	144	37.40%
Poco efectiva	94	24.41%
Nada efectiva	40	10.39%

El 27.79% de los encuestados considera que la educación digital es muy efectiva en la prevención de la ciberdelincuencia juvenil, mientras que el 37.40% la percibe como moderadamente efectiva. Por otro lado, un 24.41% cree que es poco efectiva y un 10.39% la considera nada efectiva. Esto indica que, aunque la mayoría la valora positivamente (65.19% en total), existe un 34.80% de la población que no percibe un impacto significativo.

Tabla 3

¿En qué medida la educación digital ayuda a reducir las amenazas en el entorno digital juvenil?

Respuesta	Frecuencia	Porcentaje (%)
En gran medida	119	30.91%
En medida moderada	140	36.36%
En poca medida	88	22.86%
No ayuda en nada	38	9.87%

El análisis de la tabla muestra que la mayoría de los encuestados (67.27%) considera que la educación digital tiene un impacto positivo en la reducción de las amenazas en el entorno digital juvenil, con un 30.91% que la percibe como muy efectiva y un 36.36% como moderadamente efectiva. No obstante, un porcentaje significativo, el 32.73%, tiene dudas sobre su efectividad, ya que un 22.86% la ve como poco útil y un 9.87% considera que no ayuda en nada. Esto sugiere que, aunque hay un consenso general sobre la importancia de la educación digital, todavía existen diferencias en cuanto a su eficacia percibida.

Tabla 4

¿Qué tan accesible es la educación digital sobre prevención de ciberdelincuencia en Ecuador?

Respuesta	Frecuencia	Porcentaje (%)
Muy accesible	79	20.52%
Medianamente accesible	157	40.78%
Poco accesible	109	28.31%
Nada accesible	40	10.39%

Con respecto a la pregunta 3, considera que la educación digital sobre prevención de ciberdelincuencia en Ecuador es accesible en algún grado, con un 20.52% que la considera muy accesible y un 40.78% medianamente accesible. Sin embargo, un 38.7% percibe que el acceso es limitado, ya que un 28.31% la considera poco accesible y un 10.39% opina que no es accesible en absoluto. Esto sugiere que, aunque una parte significativa de la población ve la educación digital como accesible, todavía existen barreras para una mayor disponibilidad y alcance.

Tabla 5

¿Cuál considera que es la forma más común de ciberdelincuencia que afecta a los jóvenes?

Respuesta	Frecuencia	Porcentaje (%)
Suplantación de identidad	127	32.99%
Ciberacoso	120	31.17%
Fraudes en línea	73	18.96%
Acceso indebido a datos personales	65	16.88%

La suplantación de identidad es señalada por el 32.99% como el delito más frecuente, seguido del ciberacoso con un 31.17%. Los fraudes en línea representan un 18.96%, mientras que el acceso indebido a datos personales es identificado por el 16.88%. Esto evidencia que los delitos más percibidos afectan directamente la seguridad y privacidad de los jóvenes.

Tabla 6

¿Qué nivel de exposición considera que tienen los jóvenes a la ciberdelincuencia?

Respuesta	Frecuencia	Porcentaje (%)
Muy alto	117	30.39%
Alto	158	41.04%
Moderado	90	23.38%
Bajo	20	5.19%

El 30.39%de los encuestados considera que los jóvenes tienen un nivel muy alto de exposición a la ciberdelincuencia, seguido por un 41.04%que lo califica como alto. Un 23.38%cree que la exposición es moderada, mientras que solo un 5.19%la considera baja. Esto significa que el 71.43% percibe una alta vulnerabilidad juvenil.

Tabla 7

¿Qué tan informados cree que están los jóvenes sobre los peligros de la ciberdelincuencia?

Respuesta	Frecuencia	Porcentaje (%)
Muy informados	58	15.06%
Algo informados	140	36.36%
Poco informados	147	38.18%
Nada informados	40	10.39%

Solo el 15.06% de los encuestados considera que los jóvenes están muy informados sobre la ciberdelincuencia, mientras que el 36.36% cree que están algo informados. Un 38.18%los percibe poco informados y el 10.39% cree que no tienen información al respecto. Esto indica que el 50.65% los ve con un conocimiento deficiente sobre el tema.

Tabla 8

¿Conoce programas educativos en Ecuador sobre prevención de ciberdelincuencia?

Respuesta	Frecuencia	Porcentaje (%)
Sí, varias	41	10.65%
Sí, algunas	98	25.45%
He oído hablar de ellas, pero no mucho	150	38.96%
No conozco ninguna	96	24.94%

El análisis de la tabla muestra que un 38.96% de los encuestados tiene un conocimiento limitado sobre los programas educativos en Ecuador relacionados con la prevención de ciberdelincuencia, ya que solo ha oído hablar de ellos, pero no en detalle. Un 25.45% conoce algunas iniciativas y un 10.65% tiene conocimiento de varias. Es así que un 38.96% de los encuestados tiene algún nivel de conocimiento sobre estos programas, mientras que un 24.94% no conoce ninguno, lo que refleja que, aunque hay algo de conciencia, la falta de conocimiento generalizado sobre estos programas podría ser una barrera para su efectividad.

Tabla 9

¿Considera que las iniciativas educativas en Ecuador son suficientes para prevenir la ciberdelincuencia juvenil?

Respuesta	Frecuencia	Porcentaje (%)
Sí, son suficientes	38	9.87%
Son algo suficientes	117	30.39%
Son insuficientes	154	40.00%
Son totalmente ineficaces	76	19.74%

Solo el 9.87% considera que las iniciativas educativas existentes son suficientes y efectivas, mientras que el 30.39% las percibe suficientes pero ineficaces. Un 40.00% las califica como insuficientes y un 19.74% considera que no existen. Esto significa que el 59.74% de los encuestados cree que los programas actuales no cumplen con su propósito.

Tabla 10

¿Cuál cree que es el principal obstáculo para la efectividad de los programas educativos en ciberseguridad?

Respuesta	Frecuencia	Porcentaje (%)
Falta de recursos	113	29.35%
Desinterés de los jóvenes	65	16.88%
Falta de capacitación en docentes	102	26.49%
Escasa difusión de los programas	105	27.27%

El 29.35% de los encuestados identifica la falta de recursos como el mayor problema, seguido por la escasa difusión con un 27.27%. La falta de capacitación docente es mencionada por un 26.49%, mientras que el 16.88% considera que el desinterés juvenil es la mayor barrera. Esto sugiere que los principales problemas son estructurales y no solo de interés por parte de los jóvenes.

Tabla 11

¿Qué tan importante considera la educación digital en la prevención de la ciberdelincuencia juvenil?

Respuesta	Frecuencia	Porcentaje (%)
Muy importante	196	50.91%
Algo importante	104	27.01%
Poco importante	63	16.36%
Nada importante	22	5.71%

Un 50.91% considera que la educación digital es muy importante en la prevención de la ciberdelincuencia juvenil, seguido de un 27.01% que la califica como algo importante. Por otro lado, un 16.36% cree que es poco importante y un 5.71% opina que no tiene importancia. Esto significa que, aunque el 77.92% reconoce su valor, un 22.07% aún no percibe su relevancia.

3.2 Resultados de la entrevista.

En el presente capítulo, se exponen los resultados obtenidos a través de una serie de entrevistas realizadas a tres profesionales expertos en criminología y áreas afines, con el objetivo de analizar el rol de la educación digital en la prevención de la ciberdelincuencia juvenil en Ecuador. Los participantes, un criminólogo, un experto en ciberseguridad forense y un abogado penalista especializado en delitos informáticos, fueron seleccionados debido a su amplia experiencia en el ámbito de la seguridad digital y la criminología. Las entrevistas se centraron en evaluar la efectividad de las iniciativas educativas actuales, identificar las barreras para su implementación, y entender las formas predominantes de ciberdelincuencia que afectan a los jóvenes en el país.

Tabla 12
Matriz de respuestas de profesionales

Pregunta	Profesional 1 (Criminólogo)	Profesional 2 (Experto en Ciberseguridad Forense)	Profesional 3 (Abogado Penalista especializado en delitos informáticos)
1. ¿Considera que la educación digital ha sido efectiva para prevenir la ciberdelincuencia juvenil en Ecuador? ¿Por qué?	No del todo. Aunque hay avances, la educación digital no está estructurada para abordar de manera integral la prevención del crimen digital.	Parcialmente. Se han implementado algunas iniciativas, pero los ciberdelitos evolucionan más rápido que la capacidad de prevención.	No, ya que la legislación y la educación digital van a ritmos distintos. La normativa avanza, pero los jóvenes aún desconocen los riesgos legales.
2. ¿Cuáles son las principales barreras que dificultan la implementación de estrategias educativas efectivas en ciberseguridad?	Falta de una política pública integral que articule educación, seguridad y tecnología.	Carencia de personal capacitado en ciberseguridad dentro del sistema educativo y actualización deficiente de los programas de estudio.	Desconocimiento de la normativa vigente por parte de estudiantes y docentes. Hay un vacío en la enseñanza de las implicaciones legales de estos delitos.
3. ¿Cuáles considera que son	El ciberacoso y la captación de	Phishing, robo de identidad y	Difusión de contenido íntimo

los tipos de ciberdelincuencia que más afectan a los jóvenes en Ecuador?	menores por redes delictivas son problemas en crecimiento.	sextorsión son las amenazas más comunes en adolescentes.	sin consentimiento, fraudes electrónicos y suplantación de identidad son los casos que más se judicializan.
4. ¿Cree que los jóvenes tienen suficiente conocimiento sobre cómo protegerse de la ciberdelincuencia? ¿Por qué?	No. Aunque usan tecnología a diario, no poseen una educación sobre ciberseguridad y prevención del delito digital.	Tienen una idea general, pero carecen de hábitos sólidos de protección digital, como el uso de contraseñas seguras o la verificación en dos pasos.	No. Muchos adolescentes desconocen que algunas prácticas digitales pueden ser delitos con consecuencias legales.
5. ¿Qué opinión tiene sobre las iniciativas educativas actuales en Ecuador para la prevención de la ciberdelincuencia juvenil?	Son incipientes y no abarcan todas las formas de ciberdelincuencia. Deben incluirse en la educación básica y media.	Existen esfuerzos en universidades y empresas privadas, pero en la educación pública aún hay una brecha importante.	A nivel legal, se han dado charlas y capacitaciones, pero no hay un programa sistemático dentro del currículo escolar.
6. ¿Qué estrategias o mejoras sugeriría para fortalecer la educación digital como herramienta de prevención en el país?	Incorporar la prevención del cibercrimen en los programas educativos desde edades tempranas.	Crear alianzas entre el sector educativo, el tecnológico y el de seguridad para diseñar programas de formación integral.	Implementar campañas nacionales de concienciación sobre los delitos informáticos y sus consecuencias legales, dirigidas a jóvenes y docentes.

Análisis general de la entrevista sobre educación digital y prevención de la ciberdelincuencia juvenil en ecuador

A partir de las respuestas obtenidas de los tres expertos en criminología y áreas relacionadas, se destacan varios puntos clave sobre la efectividad de la educación digital y las barreras en la prevención de la ciberdelincuencia juvenil en Ecuador.

En cuanto a la efectividad de la educación digital, los tres profesionales coinciden en que, aunque existen avances, la educación actual no ha logrado ser completamente

eficaz en la prevención de ciberdelitos. Según el criminólogo y el experto en ciberseguridad, la educación no está lo suficientemente estructurada para abordar de manera integral las amenazas digitales y evolucionar con ellas. El abogado penalista resalta que la falta de conocimiento sobre las implicaciones legales de las acciones digitales por parte de los jóvenes agrava este problema.

Las barreras para la implementación de estrategias educativas efectivas en ciberseguridad son varias. El criminólogo señala la ausencia de una política pública integral que conecte la educación, la seguridad y la tecnología. El experto en ciberseguridad forense subraya la carencia de personal capacitado y programas de estudio actualizados en ciberseguridad. Por su parte, el abogado penalista destaca el vacío existente en la enseñanza de las implicaciones legales de la ciberdelincuencia, lo cual es crucial para que los jóvenes comprendan las consecuencias de sus acciones en el entorno digital.

En cuanto a las formas de ciberdelincuencia más prevalentes que afectan a los jóvenes, todos los expertos coinciden en la relevancia del ciberacoso, la suplantación de identidad y la sextorsión. El criminólogo y el experto en ciberseguridad coinciden en que las plataformas digitales facilitan la captación de menores por parte de grupos delictivos, mientras que el abogado penalista apunta a la creciente difusión de contenido íntimo sin consentimiento y los fraudes electrónicos como problemas emergentes.

Respecto al conocimiento de los jóvenes sobre cómo protegerse de la ciberdelincuencia, las respuestas indican que hay una deficiencia significativa en este aspecto. El criminólogo y el abogado penalista coinciden en que, aunque los jóvenes están familiarizados con el uso de la tecnología, carecen de una educación adecuada sobre ciberseguridad. El experto en ciberseguridad refuerza esta idea, señalando que

los jóvenes no adoptan prácticas de protección digital adecuadas, como el uso de contraseñas seguras y la verificación en dos pasos.

Finalmente, en relación con las iniciativas educativas actuales, los tres expertos coinciden en que son insuficientes para cubrir las diversas formas de ciberdelincuencia y que la educación digital en el país aún está en una fase incipiente. El criminólogo sugiere que estas iniciativas deben ser incorporadas en los programas educativos desde niveles tempranos, mientras que el experto en ciberseguridad aboga por la creación de alianzas entre sectores educativos, tecnológicos y de seguridad para diseñar programas de formación más completos. El abogado penalista destaca la importancia de llevar a cabo campañas nacionales de concienciación sobre las implicaciones legales de la ciberdelincuencia.

Los resultados de la entrevista revelan que, aunque existen esfuerzos por parte de diversas entidades, hay una necesidad urgente de una educación digital más robusta y una mejor preparación en ciberseguridad para prevenir y mitigar la ciberdelincuencia juvenil en Ecuador. Las estrategias deben abordar tanto la prevención técnica como el conocimiento legal para equipar a los jóvenes con las herramientas necesarias para navegar de manera segura en el entorno digital.

Conclusiones

Se pudo llevar a cabo el primer objetivo, concluyendo que la educación digital en Ecuador aún presenta deficiencias en términos de efectividad para prevenir la ciberdelincuencia juvenil. A pesar de que existen esfuerzos en algunas áreas, se percibe que las estrategias educativas no son lo suficientemente integrales ni adaptadas a la evolución constante de las amenazas digitales. Los jóvenes carecen de un conocimiento adecuado sobre las implicaciones legales y las prácticas de protección digital necesarias. Por lo tanto, es evidente que las estrategias actuales no han logrado reducir de manera significativa las tendencias de ciberdelincuencia entre los jóvenes, y se requiere una revisión profunda y un enfoque más robusto para abordar estas problemáticas.

Se pudo llevar a cabo el segundo objetivo, identificando las formas predominantes de ciberdelincuencia que afectan a los jóvenes en Ecuador. Las principales amenazas que enfrentan los jóvenes incluyen el ciberacoso, la suplantación de identidad, el sextorsión y el robo de datos. Estas prácticas delictivas se han visto facilitadas por la expansión de las plataformas digitales y la creciente conectividad de los adolescentes. Se destacó que, aunque los jóvenes están conscientes de los riesgos, no siempre cuentan con los recursos o la educación necesaria para prevenir o enfrentar estas situaciones, lo que agrava el impacto de la ciberdelincuencia en este grupo

Se pudo llevar a cabo el tercer objetivo, encontrando que las iniciativas educativas en Ecuador son limitadas y no están suficientemente estructuradas para abordar de manera efectiva la prevención del cibercrimen juvenil. A pesar de la existencia de algunos programas y recursos, se identificó que no existe una política pública integral que conecte la educación, la seguridad y la tecnología de manera coherente. Además, se observó una falta de capacitación adecuada tanto en los jóvenes como en los

docentes sobre las amenazas digitales y las mejores prácticas para la protección en línea. Esto revela la necesidad urgente de mejorar la coordinación entre las diferentes instituciones educativas, de seguridad y tecnológicas para ofrecer una educación digital más efectiva y amplia.

De este modo los resultados indican que, aunque hay esfuerzos por mejorar la educación digital en el país, aún existen importantes vacíos que limitan su efectividad en la prevención de la ciberdelincuencia juvenil. Para lograr una verdadera reducción en las amenazas digitales, es necesario fortalecer las iniciativas educativas, actualizarlas de acuerdo con las nuevas tendencias tecnológicas y ofrecer formación integral en ciberseguridad tanto para los jóvenes como para los educadores.

Recomendaciones

Se recomienda desarrollar programas educativos más completos que aborden no solo el uso seguro de la tecnología, sino también las implicaciones legales y éticas de las acciones digitales. Es fundamental que estos programas sean implementados desde etapas tempranas de la educación, adaptados a los cambios tecnológicos y que incluyan contenidos prácticos de prevención, promoviendo una cultura de seguridad digital entre los jóvenes.

Se recomienda implementar campañas de sensibilización y prevención del ciberacoso, suplantación de identidad y otros crímenes cibernéticos dirigidas a los jóvenes, padres de familia y educadores. Estas campañas deben enfocarse en enseñar a los jóvenes cómo identificar y protegerse de estas amenazas, así como promover una mayor responsabilidad en el uso de las redes sociales y otras plataformas digitales.

Se recomienda la creación de una política pública nacional que integre la ciberseguridad y la educación digital en todos los niveles educativos, promoviendo la capacitación continua de docentes y estudiantes. Es necesario un enfoque coordinado entre el Ministerio de Educación, entidades gubernamentales, organismos de seguridad y el sector privado para diseñar programas educativos que preparen a los jóvenes para enfrentar las amenazas digitales de manera efectiva. Además, se deben establecer alianzas para capacitar a los docentes en el manejo de herramientas digitales y la prevención de ciberdelitos.

Bibliografía

Alvarez, E. (2021). *Uso crítico y seguro de tecnologías digitales de profesores universitarios.* Formación universitaria, 14(1), 33-44. https://www.scielo.cl/scielo.php?pid=S0718-50062021000100033&script=sci_arttext

Antón, M. (2022). *El impacto de las tecnologías de la información y la comunicación en la educación. La importancia de la formación, la información y la sensibilización.* Revista Tecnología, Ciencia y Educación, (21), 155-182. https://revistas.um.es/red/article/view/444751

Arroyo, S. (2020). *Criminología y perspectiva de género: la delincuencia juvenil femenina.* IgualdadES, 2(3), 519-555. https://dialnet.unirioja.es/servlet/articulo?codigo=7682861

Asencio, L. (2021). *El docente y la alfabetización digital en la educación del siglo XXI.* Sociedad & Tecnología, 4(S2), 377-390. https://institutojubones.edu.ec/ojs/index.php/societec/article/view/158

Barberá, E. (2021). *Evaluación de la educación digital y digitalización de la evaluación.* RIED-Revista Iberoamericana de Educación a Distancia, 24(2), 33-40. https://www.redalyc.org/journal/3314/331466109007/331466109007.pdf

Beltrán , S. (2023). *Análisis sobre los riesgos de seguridad en internet y redes sociales en adolescentes y menores de edad de la provincia de Los Ríos (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).* https://dspace.utb.edu.ec/handle/49000/14160

Cadillo, R. (2023). *Los riesgos y los desafíos que enfrentan los trabajadores frente al uso de la inteligencia artificial en el trabajo.* Revista de Derecho Procesal del Trabajo, 6(7), 289-313. https://revistas.pj.gob.pe/revista/index.php/rdpt/article/view/778

Calle, M. (2024). *Políticas de Inclusión Digital en la Educación: Perspectivas para el Ecuador.* Revista Docentes 2.0, 17(2), 355-361. https://ojs.docentes20.com/index.php/revista-docentes20/article/view/564

Calloapaza, K. (2022). *Redes sociales virtuales y la salud mental en tiempos de COVID-19: una revisión de literatura.* LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 3(2), 773-783. https://latam.redilat.org/index.php/lt/article/view/146

Camacho, R. (2020). *Innovación y tecnología educativa en el contexto actual latinoamericano.* https://repositoriobibliotecas.uv.cl/bitstream/uvscl/2036/1/28064146030.pdf

Cámara Ecuatoriana de Comercio Electrónico. (2023). *Informe sobre el aumento de ciberdelitos en Ecuador.*

Carrasco , P. (2024). *DELINCUENCIA JUVENIL: UN ENFOQUE CRIMINOLÓGICO INTEGRAL.* https://burjcdigital.urjc.es/items/aa24bbfa-d042-4813-ae67-5e3e0035559f

CEPAL UNESCO. (2020). *La educación en tiempos de Covid 19.* https://repositorio.cepal.org/server/api/core/bitstreams/c29b3843-bd8f-4796-8c6d-5fcb9c139449/content

Chalen, E. (2023). *Delitos informáticos: Vulneración de los derechos humanos en niñas, niños y adolescentes en la provincia de Guayas, 2014-2023.* Revista de Derechos

Humanos y de la Naturaleza, (4), 32-41. https://revistas.uasb.edu.ec/index.php/andares/article/view/4446

Del Carmen, M. (2022). *Integración de las tecnologías de la información y la comunicación en la educación inicial del Ecuador.* LATAM Revista Latinoamericana de Ciencias Sociales. https://latam.redilat.org/index.php/lt/article/view/69

Del Pino, S. (2023). *Formación del profesorado sobre control, seguridad y privacidad en internet.* https://rodin.uca.es/handle/10498/28014

Diez , R. (2020). *Transformación digital en la educación en tiempos del COVID-19.* https://repositorio.usil.edu.pe/entities/publication/c8538b13-9204-40be-9bcf-c1205501187a

Esquivel, A. (2023). *El Estado y la defensa del ciberespacio.* Revista de la Academia del Guerra del Ejército Ecuatoriano, 16(1), 11-11. https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/2965

González, E. (2023). *Posibilidades de desjudicialización de la ciberdelincuencia juvenil. In El proceso penal ante una nueva realidad tecnológica europea (pp. 463-489). Thomson Reuters Aranzadi.* https://dialnet.unirioja.es/descarga/articulo/8857611.pdf

Herrerías, A. (2025). *Ciberdelincuencia en jóvenes menores de edad: un estudio centrado en la ciudad autónoma de Ceuta (Doctoral dissertation, Universidad de Granada).* https://digibug.ugr.es/handle/10481/102617

Huamani, C. (2022). *Uso de redes sociales virtuales y la salud mental en tiempos de pandemia.* http://www.revistas.unah.edu.pe/index.php/puriq/article/view/398

Hueso, L. (2020). *La enseñanza digital en serio y el derecho a la educación en tiempos del coronavirus.* Revista de educación y derecho= Education and law review, (21), 8. https://dialnet.unirioja.es/servlet/articulo?codigo=7388655

Instituto Nacional de Estadística y Censos (INEC). (2023). *Uso de internet en adolescentes ecuatorianos.*

Juca, F. (2023). *Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectiva.* Portal de la Ciencia, 4(3), 325-337. https://institutojubones.edu.ec/ojs/index.php/portal/article/view/394

Lago, L. (2021). *Jóvenes y pandemia: experiencias estudiantiles en Chubut.* https://sedici.unlp.edu.ar/handle/10915/139533

Ledesma, A. (2022). *Las competencias digitales en el currículo argentino de educación digital.* IE Revista de Investigación Educativa de la REDIECH, 13, 1-22. https://www.redalyc.org/journal/5216/521670731005/521670731005.pdf

Loachamin, L. (2023). *Desigualdades Tecnológicas en la Educación en Ecuador: Abordando la Brecha Educativa.* Código Científico Revista de Investigación, 4(2), 238-251. http://www.revistacodigocientifico.itslosandes.net/index.php/1/article/view/239

Loayza, M. (2023). *Recurso educativo digital como herramienta de retroalimentación en la educación superior modalidad híbrida.* Polo del Conocimiento: Revista científico-profesional, 8(9), 27-4. https://dialnet.unirioja.es/servlet/articulo?codigo=9152597

Loeza, G. (2021). *Impacto del uso de dispositivos móviles en el aprendizaje de estudiantes adolescentes.* Emerging Trends in Education, 3(6). https://revistaemerging.ujat.mx/index.php/emerging/article/view/4040

Loja, E. (2020). *Diseño de políticas de TIC para la educación en el Ecuador: el caso de la Agenda Educativa Digital 2017-2021*. Revista Estudios de Políticas Públicas, 6(1), 1-19. https://pdfs.semanticscholar.org/e071/e812518add0aca19f1d6803e76eedcd9adf7.pdf

Lugo, M. (2020). *Hacia una nueva agenda educativa digital en América Latina.* Documento de trabajo, 188.

Mecias, C. (2024). *La ciberdelincuencia y la protección de datos personales.* Sinergia Académica, 7(Especial 5), 594-612. http://sinergiaacademica.com/index.php/sa/article/view/289

Ministerio de Educación de Ecuador. (2023). *Protocolos de prevención y uso responsable de las TIC.*

Monzón, D. (2020). *Alfabetización digital en el aula.* https://biblioteca.galileo.edu/xmlui/handle/123456789/960

Perez, J., & Londoño, E. (2022). *Análisis de la relación entre educación y tecnología.* Cultura, educación y sociedad, 13(2), 47-68. https://dialnet.unirioja.es/servlet/articulo?codigo=8838315

Pineda, L. (2023). *El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz.* Revista de Cultura de paz, 7, 123-140. https://revistadeculturadepaz.com/index.php/culturapaz/article/view/143

Punín, P. (2021). *Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica.* Revista Ruptura, 3(03), 40-40. http://www.revistaruptura.com/index.php/ruptura/article/view/85

Ramos, J. (2023). *Estado de arte sobre indicadores de salud mental tras experiencias de grooming online en niños, niñas y adolescentes entre el 2013-2023 (Doctoral dissertation, Tesis de grado, Universidad Peruana Cayetano Heredia).* https://repositorio.upch.edu.pe/bitstream/handle/20.500.12866/14181/Estado_MallquiRamos_Wendy.pdf?sequence=1

Reyes, C. (2021). *Alfabetización digital en la educación. Revisión sistemática de la producción científica en Scopus.* Revista de Educación a Distancia (red), 21(66). https://revistas.um.es/red/article/view/444751

Rodríguez, M. (2021). *El uso de videojuegos en adolescentes.* Un problema de Salud Pública. Enfermería Global, 20(2), 557-591. https://revistas.um.es/eglobal/article/view/438641

Rojas, S. (2022). *Panorama de riesgos por el uso de la tecnología en América Latina.* Trilogía Ciencia Tecnología Sociedad, 14(26). http://www.scielo.org.co/scielo.php?pid=S2145-77782022000100300&script=sci_arttext

Rubio , G. (2020). *La orientación y el uso responsable de las nuevas tecnologías.* Zaragoza:(Trabajo de Master). Universidad de Zaragoza. https://zaguan.unizar.es/record/100872

Saltos , F. (2021). *Análisis conceptual del delito informático en Ecuador.* http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext

Samaniego, J. (2024). *Alfabetización digital crítica: genealogía, crítica fundacional y estado del arte.* Revista Colombiana de Educación, (91), 403-425.

http://www.scielo.org.co/scielo.php?pid=S0120-39162024000200403&script=sci_arttext

Sánchez, M. (2022). *El metaverso:¿ la puerta a una nueva era de educación digital?* Investigación en educación médica, 11(42), 5-8. https://www.scielo.org.mx/scielo.php?pid=S2007-50572022000200005&script=sci_arttext

Seguil, C. (2023). *Estrategia para enfrentar la ciberdelincuencia que afecta la Seguridad Nacional en Perú.* https://repositorio.esup.edu.pe/handle/20.500.12927/335

Sierra, P. (2022). *Los delitos informáticos y la problemática trasnacional: el caso colombiano. De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa.* https://www.academia.edu/download/100243219/Capitulo_5_De_los_delitos_transnacionales.pdf

Suarez, R. (2020). *La educación digital en Colombia en tiempos de Covid 19 y su impacto en las organizaciones educativas.* Universidad Militar Nueva Granada. Colombia. https://repository.umng.edu.co/server/api/core/bitstreams/8913d7fd-bda0-4448-ab6a-626fbdb7b7a5/content

Ticona, J. (2024). *Causas y consecuencias del incremento de los delitos informáticos en la ciudad de Puno 2023.* Revista de Derecho: Universidad Nacional del Altiplano de Puno, 9(1), 2. https://dialnet.unirioja.es/servlet/articulo?codigo=9386290

Torrado, A. (2021). *"CIBERPol" Propuesta de una plan formativo en ciberdelincuencia para agentes formadores de la policía municipal de Sabadell (Barcelona). Prevenir la ciberdelincuencia formando a los alumnos en las escuelas.* https://openaccess.uoc.edu/handle/10609/133367

Trucios, A. (2023). *La ciberdelincuencia y la captación en menores de edad Lima Metropolitana, 2021*. https://repositorio.autonoma.edu.pe/handle/20.500.13067/2704

Vinces, G. (2022). *Uso de internet por parte de los jóvenes y dependencia de los teléfonos móviles.* UNESUM-Ciencias. Revista Científica Multidisciplinaria, 6(3), 20-30. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/471