Neutrosophic Computing and Machine Learning {Número especial: "Neutrosofía aplicada a los dilemas bioéticos: una mirada transdisciplinaria desde la medicina, el derecho y la educación"}, Vol. 38, 2025

University of New Mexico

Método neutrosófico para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal.

Neutrosophic method to evaluate the crime of cyber-bullying and the protection of minors in the Integral Penal Code.

Andrea Katherine Bucaram Caicedo [1], Mauro Alejandro Pérez Solís [2], Stefani Camila Guanoluisa Barrionuevo [3], and Pamela Stephanie Piñuela Narváez [4]

[1] Universidad Regional Autónoma de Los Andes, Ambato, Ecuador. ua.andreabucaram@uniandes.edu.ec
[2] Universidad Regional Autónoma de Los Andes, Ambato, Ecuador. maurops17@uniandes.edu.ec
[3] Universidad Regional Autónoma de Los Andes, Ambato, Ecuador. stefanigb20@uniandes.edu.ec
[4] Universidad Regional Autónoma de Los Andes, Ambato, Ecuador. pamelapn57@uniandes.edu.ec

Resumen. La carencia de una adecuada categorización en el Código Integral Penal aumenta la vulnerabilidad de los menores al acoso cibernético. Para abordar esta problemática, se realiza una comparación entre los sistemas legales de Alemania y Ecuador, destacando las fortalezas y debilidades de cada uno. En Ecuador, donde se ha registrado un notable incremento en el acceso a internet en los últimos años, la falta de normativas específicas ha expuesto a niños y adolescentes a diversas formas de hostigamiento en línea. El presente estudio tiene como objetivo desarrollar un Método neutrosófico para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal. Este estudio multidisciplinario se basa en la comparación de regulaciones, el análisis crítico de las categorías penales y la identificación de vacíos legales que facilitan el acoso cibernético. Los hallazgos obtenidos tienen como objetivo servir de base para futuras modificaciones legales y políticas públicas que refuercen la protección de las víctimas y prevengan el delito de hostigamiento en el contexto ecuatoriano.

Palabras Claves: método neutrosófico, protección de menores, tipificación penal, acoso cibernético, comparación normativa, reformas legislativas.

Abstract. The lack of adequate categorization in the Comprehensive Criminal Code increases the vulnerability of minors to cyberbullying. To address this issue, a comparison is made between the legal systems of Germany and Ecuador, highlighting the strengths and weaknesses of each. In Ecuador, where there has been a notable increase in internet access in recent years, the lack of specific regulations has exposed children and adolescents to various forms of online harassment. This study aims to develop a neutrosophic method to evaluate the crime of cyberbullying and the protection of minors in the Comprehensive Criminal Code. This multidisciplinary study is based on the comparison of regulations, the critical analysis of criminal categories, and the identification of legal loopholes that facilitate cyberbullying. The findings obtained are intended to serve as a basis for future legal amendments and public policies that strengthen victim protection and prevent the crime of harassment in the Ecuadorian context.

Keywords: Neutrosophic method, child protection, criminal classification, cyberbullying, normative comparison, legislative reforms.

1. Introducción

En la actualidad, la era digital y los avances tecnológicos han transformado nuestra vida cotidiana, generando nuevas oportunidades y desafíos. Uno de estos retos es el metaverso, un espacio virtual donde los usuarios pueden interactuar mediante avatares personalizados, revolucionando así internet a través de la interoperabilidad entre diversos entornos virtuales y la interacción con sus componentes [1].

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

En Ecuador, el acoso cibernético ha encontrado en el metaverso un nuevo medio para llevar a cabo actos ilegales que aún no están tipificados en la legislación vigente. La dificultad para proteger la identidad en este entorno se complica con la presencia de "deepfakes" y contenido falso generado por inteligencia artificial, que facilitan el fraude de identidad. La ausencia de un sistema de identidad interoperable que garantice la autenticidad en diferentes plataformas digitales pone en riesgo la seguridad de los usuarios, ya que no hay un control efectivo sobre la creación y uso de avatares [2].

Un caso documentado por Business Insider ilustra esta problemática: una investigadora de SumOfUs experimentó acoso sexual mientras utilizaba gafas de realidad virtual, lo que resalta la falta de medidas de seguridad y controles de privacidad en el metaverso [3].

Además, el acceso a internet ha crecido considerablemente en las últimas décadas, exponiendo a los menores a múltiples formas de acoso en línea. La inexistencia de legislación específica deja a los niños y adolescentes vulnerables, y el metaverso añade una capa adicional de complejidad. La problemática principal gira en torno a los riesgos legales relacionados con la protección de la identidad en estos entornos, lo que revela la necesidad de investigar y abordar estas complejidades jurídicas [4].

En estos entornos virtuales, no hay un registro de identidad ni protocolos para almacenar direcciones IP, lo que facilita la suplantación de identidades debido a la falta de medidas de seguridad y controles de privacidad. Aunque se han propuesto soluciones a estos retos jurídicos, aún no se cuenta con una normativa que regule estas conductas o acciones. La falta de una tipificación adecuada en el Código Integral Penal ecuatoriano facilita el acoso cibernético a menores, mientras que el metaverso amplifica estos riesgos [5].

2. Materiales y métodos

La toma de decisiones es un proceso de selección entre cursos de alternativas, basado en un conjunto de criterios, para alcanzar uno o más objetivos [6]. La toma de decisiones es definida como [7]: el proceso de identificación de un problema u oportunidad y la selección de una alternativa de acción entre varias existentes, es una actividad diligente clave en todo tipo de organización. Un proceso de toma de decisiones donde varían los objetos o decisiones, es considerado como un problema de toma de decisiones multicriterio [8]. La evaluación multicriterio constituye una optimización con varias funciones objetivo simultaneas y un agente decisor. La ecuación 1 formaliza el problema planteado.

$$Max = F(x), x \in X \tag{1}$$

Donde:

x: es un vector $[x_1, , x_n]$ de las variables de decisión.

X: es la denominada región factible. Representa el dominio de valores posible que puede tomar la variable.

F(x): es un vector $[F_1 x, , F_n x]$ de las P funciones objetivos que recogen los criterios.

Max: representa la función a maximizar, esta no es restrictiva.

Específicamente los problemas multicriterio discretos constan básicamente de dos tipos de datos que constituyen el punto de partida para diferentes problemas de toma de decisiones multicriterio discreto (DMD).

2.1 Tomas de decisiones

Cada problema de toma de decisiones presenta características únicas, lo que significa que no existe un enfoque universal que pueda aplicarse en todos los casos. Debido a la diversidad de situaciones, se puede establecer un procedimiento general que sirva como guía para la resolución de problemas. Este procedimiento puede incluir etapas como la identificación del problema, la recopilación y análisis de información, la generación de alternativas, la evaluación de opciones y, finalmente, la implementación de la decisión elegida. La aplicación de un esquema estructurado, como se muestra en la Figura 1, permite a los tomadores de decisiones navegar de manera más eficaz por el proceso y abordar los desafíos de manera más sistemática. Esto no solo facilita una mejor comprensión del problema en cuestión, sino que también promueve una toma de decisiones más informada y basada en datos.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

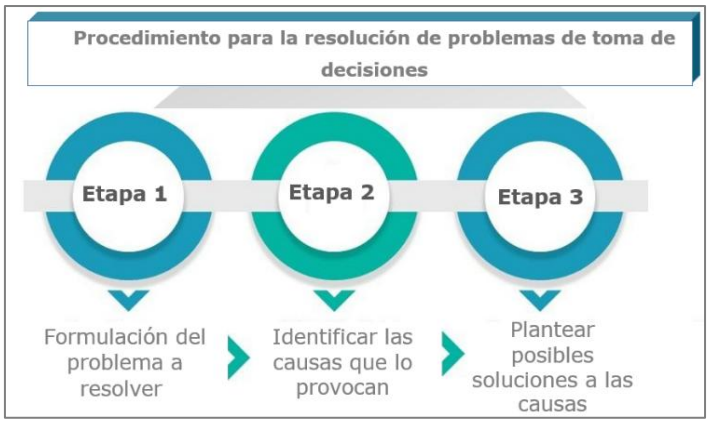

Figura 1: Procedimiento para la resolución de problemas de toma de decisiones.

Para la resolución de problemas de toma de decisiones, diversos han sido los métodos multicriterios propuestos. Cuando se desea emitir una ponderación para una determinada alternativa, los métodos de ordenamiento y agregación representan una forma viable para su aplicación [9-11]. Dentro de los métodos multicriterio clásicos se encuentra la ponderación lineal [12]. El método consiste en calcular una puntuación global r_i para cada alternativa A_i tal como expresa la ecuación 2.

$$R_i = \sum_j W_j \, r_{ij} \tag{2}$$

La ponderación lineal representa un método compensatorio, se aplica posterior a una normalización previa. El método es aplicado en casos donde se posee un conjunto *m* de alternativas y *n* criterios [13, 14]. Para cada criterio *j* el decisor estima cada alternativa *i*. Se obtiene la evaluación a_{ij} de la matriz de decisión que posee una ponderación cardinal ratio [15-17]. Se asigna un peso $W_j(j = 1, n)$ también del tipo cardinal ratio para cada uno de los criterios C_j.

En el contexto de los métodos multicriterio, se introducen los números neutrosóficos con el objetivo de representar la neutralidad [18, 19]. Constituye las bases de teorías matemáticas que generalizan las teorías clásicas y difusas tales como los conjuntos neutrosóficos y la lógica neutrosófica [20, 21]. Un número neutrosófico (N) se representa de la siguiente forma [22, 23]:

Definición 1: Sean $N = \{(T, I, F) : T, I, F \subseteq [0, 1]\}n$, una valuación neutrosófica es un mapeo de un grupo de fórmulas proporcionales a N , esto es que por cada sentencia p se tiene [24-26]:

$$v\,(p) = (T, I, F) \tag{3}$$

Donde:

T: representa la dimensión del espacio que representa la verdad,
I: representa la falsedad,
F: representa la indeterminación.

Matemáticamente se puede definir un método de Ponderación Lineal Neutrosófico como una 3-tupla (R,W,r) tal como representa la ecuación 4:

$$R_{i(T,I,F)} = \sum_j W_{j(T,I,F)} \, r_{ij(T,I,F)} \tag{4}$$

Donde:

- $R_{i(T,I,F)}$: representa la función resultante que refiere una dimensión del espacio verdad, falsedad e indeterminación (T, I, F).
- $W_{j(T,I,F)}$: representa el peso del criterio $_j$ asociados a los criterios que refiere una dimensión del espacio verdad, falsedad e indeterminación (T, I, F).
- $r_{ij:}$ representa la evaluación de la alternativa i respecto al criterio j que refiere una dimensión del espacio verdad, falsedad e indeterminación (T, I, F).

3. Diseño del método neutrosófico para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal

El método neutrosófico propuesto está diseñado para evaluar el delito de acoso cibernético y la protección de

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

menores en el Código Integral Penal. Basa su funcionamiento a partir de técnicas multicriterio, multiexperto donde se modela el cumplimiento de los criterios necesarios para la evaluación. Utiliza en su inferencia el método multicriterio Ponderación Lineal Neutrosófica. El método está diseñado mediante una estructura de tres etapas:

Etapa 1: Identificación de los criterios evaluativos

Representa el conjunto de criterios que se valoran para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal. Constituye un enfoque multicriterio formalizado como:

$C = \{c_1, \dots c_n\}$, n ≥ 2, criterios que se valoran para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal.

Etapa 2: Determinación de los pesos

Para la determinación de los pesos asociados a los criterios evaluativos, se utiliza un enfoque multiexperto de modo que:

$E = \{e_1, \dots e_m\}$, $m \geq 2$, donde E, representa los expertos que intervienen en el proceso.

Etapa 3: evaluación neutrosófica del delito de acoso cibernético y la protección de menores en el Código Integral Penal

La etapa de evaluación representa el procesamiento del método para emitir el resultado de la inferencia propuesta. Se procesan los datos empleando el método de la ponderación lineal mediante la ecuación 4. Como resultado se evalúa el delito de acoso cibernético y la protección de menores en el Código Integral Penal.

4. Implementación del método

Para la implementación del método propuesto se realizó un estudio de caso donde se analizó el comportamiento de los criterios evaluativos del delito de acoso cibernético y la protección de menores en el Código Integral Penal. Obteniéndose los siguientes resultados:

Etapa 1: Identificación de los criterios evaluativos

Para identificar los criterios que permitan evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal, se consultó a un total de 11 expertos en diversas áreas del conocimiento. Este panel estuvo compuesto por profesionales

Un panel de expertos destinado a evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal debe contar con una serie de características y competencias específicas para garantizar que su trabajo sea efectivo, riguroso y relevante. A continuación se detallan algunas de estas características y competencias:

Características del Panel de Expertos:

Diversidad de Especialidades: El panel debe estar compuesto por expertos de diversas disciplinas, incluyendo derecho penal, ciberseguridad, psicología, educación, sociología y criminología. Esta diversidad permite un enfoque integral y multidimensional del acoso cibernético.

Experiencia Práctica: Los miembros del panel deben tener experiencia en la aplicación de leyes relacionadas con el ciberacoso y la protección de menores, lo que proporciona un contexto realista a las evaluaciones y recomendaciones.

Compromiso Ético: Deben demostrar un fuerte compromiso con las normas éticas y la protección de los derechos humanos, en especial los derechos de los menores y su bienestar en entornos digitales.

Conocimiento de Tecnologías Emergentes: Los expertos deben estar al tanto de las tecnologías digitales actuales y emergentes, así como de sus implicaciones para el acoso cibernético y la seguridad de los menores.

Capacidad de Trabajo en Equipo: Dado que el panel abordará un problema complejo y multifacético, los expertos deben ser capaces de trabajar de manera colaborativa y respetuosa en un entorno multidisciplinario.

Competencias del Panel de Expertos:

Competencia Jurídica: Deben tener un profundo conocimiento del marco legal vigente en relación con el acoso cibernético y la protección de menores, incluyendo no solo la legislación nacional, sino también las normativas internacionales y las mejores prácticas en otros países.

Conocimiento en Ciberseguridad: Los miembros del panel deben ser competentes en cuestiones de ciberseguridad, para comprender las vulnerabilidades que enfrentan los menores en línea y los métodos utilizados por los acosadores.

Habilidades de Investigación: Deben ser capaces de llevar a cabo investigaciones exhaustivas y críticas, analizando datos, estudios de caso, y literatura relevante para formular recomendaciones basadas en evidencia.

Capacidad de Análisis Crítico: Deben poder evaluar críticamente la legislación existente y las políticas relacionadas, identificando lagunas y debilidades que podrían afectar la protección de los menores.

Comunicación Efectiva: Los expertos deben tener habilidades efectivas de comunicación para presentar sus hallazgos y recomendaciones de manera clara y accesible, tanto a legisladores como a la sociedad en general.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

Sensibilidad Cultural y Social: Deben tener la capacidad de considerar el contexto cultural y social del país, reconociendo cómo diferentes comunidades pueden ser afectadas de manera diferente por el ciberacoso.

Orientación hacia la Prevención: La habilidad para desarrollar estrategias de prevención y programas educativos también es crucial, para proponer acciones que minimicen el riesgo de acoso cibernético entre los menores.

Recursos y Redes de Colaboración: Los miembros del panel deben estar bien conectados con otras organizaciones, tanto nacionales como internacionales, que trabajen en temas de ciberseguridad y protección de menores, lo que puede enriquecer su trabajo y facilitar la implementación de sus recomendaciones.

El panel de expertos para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal necesita una combinación de experiencia profesional, conocimiento técnico y un enfoque multidisciplinario, todo ello bajo principios éticos sólidos, para abordar eficazmente este problema complejo y en constante evolución

A continuación, se presentan los 12 criterios evaluativos sugeridos por los expertos para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal:

Tabla 1: Criterios para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal.

ID	Criterios
C_1	Definición Clara de Delitos: Evaluar si el Código Integral Penal incluye definiciones claras y específicas de delitos cibernéticos, como el acoso cibernético, la suplantación de identidad y el uso de tecnologías como deepfakes.
C_2	Protección Específica para Menores: Analizar si existen disposiciones específicas en la legislación que abordan la protección de menores en el contexto digital, reconociendo su vulnerabilidad en entornos online.
C_3	Sanciones Adecuadas: Examinar si las penas estipuladas para el acoso cibernético en el Código Integral Penal son proporcionales a la gravedad del delito y si incluyen medidas que actúen como disuasivos efectivos.
C_4	Procedimientos de Denuncia: Evaluar la existencia de procedimientos claros y accesibles para que las víctimas, en especial los menores, puedan denunciar casos de acoso cibernético sin temor a represalias o dificultades adicionales.
C_5	Mecanismos de Protección a Víctimas: Analizar la existencia de medidas que protejan a las víctimas durante el proceso legal, como la posibilidad de declarar a puerta cerrada, y la provisión de apoyo psicológico y social.
C_6	Responsabilidad de las Plataformas Digitales: Evaluar si el Código establece la responsabilidad de las plataformas digitales en la prevención del acoso cibernético y en la protección de los menores en sus entornos.
C_7	Interoperabilidad e Identificación: Examinar si existen disposiciones que faciliten la identificación y seguimiento de agresores, así como la protección de la identidad de las víctimas, incluyendo la regulación de sistemas de autenticación.
C_8	Prevención y Educación: Evaluar la inclusión de programas de prevención y educación digital dirigidos a menores, padres y educadores, promoviendo la concienciación sobre riesgos y medidas de protección.
C_9	Colaboración Internacional: Analizar la integración de disposiciones que faciliten la cooperación internacional en la persecución de delitos de acoso cibernético que trascienden fronteras, incluyendo la armonización con leyes de otros países.
C_{10}	Adaptabilidad a Nuevas Tecnologías: Evaluar si el Código Integral Penal tiene la flexibilidad necesaria para adaptarse a avances tecnológicos y nuevas formas de ciberacoso, asegurando su relevancia en un ambiente digital en constante evolución.
C_{11}	Evaluación y Monitoreo de Efectividad: Considerar si el Código establece mecanismos para la evaluación continua de la efectividad de las medidas legales y su implementación, así como la posibilidad de realizar reformas basadas en evidencia.
C_{12}	Enfoque en Derechos Humanos: Analizar si la legislación protege adecuadamente los derechos humanos, incluida la privacidad de las víctimas y el derecho a un juicio justo para los acusados, garantizando un equilibrio entre seguridad y derechos individuales.

Etapa 2: Determinación de los pesos

Para la etapa de determinación de los pesos atribuidos a los criterios, se realizó la consulta al panel de expertos que expresaron sus valoraciones sobre los criterios. Se obtuvieron las tablas valorativas las cuales fueron agregadas en una tabla resultante mediante números neutrosóficos definidos en la tabla 2.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

Tabla 2: Términos lingüísticos empleados.

Término lingüístico	Números SVN
Extremadamente alto(EA)	[1,0,0]
Muy muy alto (MMA)	[0.9, 0.1, 0.1]
Muy alto (MA)	[0.8,0,15,0.20]
Alto (A)	[0.70,0.25,0.30]
Medianamente alto (MDA)	[0.60,0.35,0.40]
Media(M)	[0.50,0.50,0.50]
Medianamente bajo (MDB)	[0.40,0.65,0.60]
Bajo (B)	[0.30,0.75,0.70]
Muy bajo (MB)	[0.20,0.85,0.80]
Muy muy bajo (MMB)	[0.10,0.90,0.90]
Extremadamente bajo (EB)	[0,1,1]

La tabla 3 muestra el resultado de la valoración de los criterios una vez realizado el proceso de agregación.

Tabla 3: Peso atribuido a los criterios a partir de la consulta a expertos.

Criterios	Valoración del criterio $W_{(T,I,F)}$
C_1	[0.9, 0.1, 0.1]
C_2	[1,0,0]
C_3	[1,0,0]
C_4	[1,0,0]
C_5	[0.9, 0.1, 0.1]
C_6	[0.8,0,15,0.20]
C_7	[0.9, 0.1, 0.1]
C_8	[0.8,0,15,0.20]
C_9	[0.9, 0.1, 0.1]
C_{10}	[0.8,0,15,0.20]
C_{11}	[0.9, 0.1, 0.1]
C_{12}	[0.8,0,15,0.20]

Etapa 3: evaluación neutrosófica del delito de acoso cibernético y la protección de menores en el Código Integral Penal

A partir del comportamiento de los pesos atribuidos a las alternativas y el desarrollo de los criterios definidos, se determina mediante un proceso de agregación el grado de pertenencia de cada criterio para el caso de estudio. La tabla 4 muestra el resultado del cálculo realizado.

Tabla 4: Procesamiento del sistema de toma de decisiones.

Criterios	Pesos $W_{(T,I,F)}$	Preferencias	$R_{i(T,I,F)}$
C_1	[0.9, 0.1, 0.1]	[1,0,0]	[0.95, 0.1, 0.1]
C_2	[1,0,0]	[1,0,0]	[1,0,0]
C_3	[1,0,0]	[1,0,0]	[1,0,0]
C_4	[1,0,0]	[0.9, 0.1, 0.1]	[0.95, 0.1, 0.1]
C_5	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]
C_6	[0.8,0,15,0.20]	[0.8,0,15,0.20]	[0.8,0,15,0.20]
C_7	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]
C_8	[0.8,0,15,0.20]	[0.9, 0.1, 0.1]	[0.85,0,15,0.20]
C_9	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]
C_{10}	[0.8,0,15,0.20]	[0.9, 0.1, 0.1]	[0.85,0,15,0.20]
C_{11}	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]	[0.9, 0.1, 0.1]
C_{12}	[0.8,0,15,0.20]	[0.9, 0.1, 0.1]	[0.85,0,15,0.20]
Índice			[0.9, 0.1, 0.1]

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

En la investigación realizada, se obtuvo un índice de 0.90 en la evaluación del delito de acoso cibernético y la protección de menores en el Código Integral Penal, lo que indica un nivel muy alto de eficacia y relevancia en las medidas legislativas y protocolos existentes en relación con este tema.

Resultados de la Investigación:

Alto Nivel de Eficacia: El índice de 0.90 sugiere que las disposiciones legales y los mecanismos de protección para los menores están estructurados de manera sólida y efectiva. Esto implica que, en términos generales, el marco legal establece un reconocimiento claro del problema del acoso cibernético y proporciona herramientas adecuadas para su abordaje.

Protección Adecuada para Menores: Este alto índice indica que la legislación vigente ha logrado incorporar consideraciones específicas para la protección de menores, reflejando una comprensión de su vulnerabilidad en entornos digitales y la necesidad de salvaguardarlos de las diversas formas de acoso cibernético.

Estructuras de Denuncia y Soporte: La investigación destaca la existencia de procedimientos claros y accesibles para que los menores y sus familias puedan denunciar casos de acoso cibernético. Se identifican mecanismos de apoyo, como la atención psicológica y social, que están disponibles para las víctimas durante el proceso legal.

Conciencia y Prevención: Un índice tan alto también sugiere que existen iniciativas de educación y concienciación que están funcionando. Esto incluye programas dirigidos a menores, padres y educadores que informan sobre los riesgos del ciberacoso y enseñan estrategias efectivas para la prevención y el manejo de situaciones de riesgo.

Colaboración Interinstitucional: La evaluación revela que hay un grado adecuado de colaboración entre diferentes entidades, incluyendo agencias gubernamentales, organizaciones no gubernamentales y plataformas digitales, lo que contribuye a una respuesta integral al problema del acoso cibernético.

Adaptabilidad a Nuevas Problemáticas: El índice indica que el Código Integral Penal tiene la capacidad de adaptarse a nuevas realidades y tecnologías que emergen en el contexto digital. Esto es crucial para mantener la relevancia de las legislaciones a medida que el entorno online evoluciona.

A pesar de que el índice de 0.90 es un resultado alentador, es importante reconocer que la perfección no puede ser alcanzada en un tema tan dinámico y complejo como el acoso cibernético. Por lo tanto, se recomienda llevar a cabo un monitoreo continuo y una evaluación crítica de la legislación vigente. Esto permitirá identificar áreas de mejora, así como la necesidad de revisiones periódicas para abordar nuevos desafíos a medida que surgen en el entorno digital. En resumen, el alto índice alcanzado sugiere que Ecuador está en un camino positivo hacia la protección de menores en el ámbito digital, aunque siempre debe haber un compromiso constante para optimizar y actualizar las medidas existentes.

5. Análisis de los resultados

Este análisis pone de relieve varios hallazgos clave sobre cómo la falta de tipificación adecuada en el Código Integral Penal del Ecuador facilita el acoso cibernético a menores en el contexto del metaverso. El acceso a internet ha aumentado significativamente en Ecuador, exponiendo a los menores a diversas formas de acoso en línea. La ausencia de legislación específica para abordar estas situaciones deja a los niños y adolescentes en una posición vulnerable. La creciente conectividad permite a los agresores acceder a las víctimas a través de múltiples plataformas digitales. Los menores son especialmente susceptibles debido a su falta de experiencia y conocimiento sobre los peligros en línea, lo que incrementa el riesgo de sufrir acoso y explotación cibernética.

La introducción del metaverso añade una nueva capa de complejidad a la protección de la identidad. La proliferación de "deepfakes" y la falta de control sobre la creación de avatares facilitan la suplantación de identidad y otros tipos de acoso. En estos entornos virtuales, la falta de un sistema de identidad interoperable y la ausencia de protocolos para almacenar direcciones IP dificultan la identificación y persecución de los agresores. Un caso reportado por Business Insider ilustra esta problemática: una investigadora de SumOfUs sufrió acoso sexual mientras utilizaba gafas de realidad virtual, lo que destaca la falta de medidas de seguridad y controles de privacidad en el metaverso [27,28].

Al comparar los marcos legales de Alemania y Ecuador, se identifican fortalezas y debilidades en cada sistema. Alemania cuenta con regulaciones más estrictas y específicas para proteger a los menores en entornos digitales, y estas podrían servir como modelo para mejorar la legislación ecuatoriana. Las leyes alemanas incluyen disposiciones claras sobre la autenticación de identidad y la responsabilidad de las plataformas digitales. Su sistema ha implementado medidas efectivas, como la verificación obligatoria de identidad y sanciones estrictas para los infractores, lo que ha resultado en una disminución de los incidentes de acoso cibernético.

La falta de tipificación adecuada en el Código Integral Penal ecuatoriano es una de las principales causas de la proliferación del acoso cibernético contra menores. Se recomienda adoptar las mejores prácticas observadas en el sistema alemán para ofrecer una mejor protección a las víctimas. La legislación ecuatoriana debe actualizarse para incluir definiciones claras y específicas de delitos cibernéticos y establecer procedimientos para la protección y apoyo a las víctimas.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

En entornos virtuales como el metaverso, la ausencia de un sistema de identidad interoperable incrementa el riesgo de suplantación de identidad y otros delitos, resaltando la necesidad de medidas de seguridad más robustas. La implementación de tecnologías de autenticación y verificación de identidad podría ayudar a mitigar estos riesgos. Los peligros asociados con la falta de control sobre la identidad digital incluyen la explotación de menores, el fraude y el acoso persistente sin posibilidad de rastrear a los agresores.

Para mejorar la protección de los menores en el entorno digital, se sugieren las siguientes acciones:

- Crear legislaciones que aborden directamente el acoso cibernético y la suplantación de identidad en el metaverso, definiendo claramente estos delitos y las sanciones correspondientes.
- Proponer la inclusión de capítulos específicos sobre delitos cibernéticos en el Código Integral Penal, que traten las nuevas formas de acoso y explotación en entornos virtuales.
- Desarrollar sistemas de autenticación robustos para garantizar la identidad de los usuarios en entornos virtuales. La adopción de tecnologías como la verificación biométrica y el uso de certificados digitales puede ser crucial.
- Implementar un sistema de identidad digital interoperable que permita la verificación y autenticación segura de usuarios en diferentes plataformas y entornos virtuales.
- Fortalecer la colaboración internacional para compartir mejores prácticas y estrategias legales efectivas. La cooperación internacional puede facilitar la armonización de las leyes y asegurar una respuesta coordinada contra el acoso cibernético, participando en foros y alianzas internacionales dedicadas a la ciberseguridad y la protección de menores en línea.
- Fomentar la educación y concienciación mediante programas de educación digital para menores, padres y educadores sobre los riesgos del acoso cibernético y cómo protegerse en línea. Esto incluye el desarrollo de campañas educativas y recursos informativos que enseñen a los menores a identificar y reaccionar ante situaciones de riesgo en línea.
- Mejorar la infraestructura tecnológica asegurando que las plataformas digitales y los entornos virtuales implementen medidas de seguridad adecuadas, como el monitoreo de contenido y la moderación proactiva para prevenir el acoso. También es fundamental establecer normas y regulaciones que obliguen a las plataformas digitales a mantener altos estándares de seguridad y privacidad para sus usuarios.

La investigación resalta la urgente necesidad de actualizar y reforzar la legislación ecuatoriana para proteger de manera efectiva a los menores en un entorno digital en constante evolución. Adoptar un enfoque integral que combine medidas legales, tecnológicas y educativas es esencial para combatir el acoso cibernético y asegurar un entorno digital seguro para los menores. Implementar estas recomendaciones podría mejorar significativamente la protección de la identidad digital y reducir la incidencia del acoso cibernético en Ecuador.

6. Discusiones

El análisis presentado en esta ponencia destaca la urgente necesidad de una reforma legislativa en Ecuador para abordar el acoso cibernético y la protección de la identidad en el metaverso. Al comparar con el marco legal alemán, se evidencian claras deficiencias en la legislación ecuatoriana, que deben ser tratadas para garantizar una protección efectiva de los menores en entornos digitales.

La carencia de tipificación específica de delitos cibernéticos en el Código Integral Penal ecuatoriano deja a los menores expuestos a diversas formas de acoso en línea. La legislación actual no considera las nuevas realidades tecnológicas y, por lo tanto, resulta insuficiente para enfrentar problemas como los "deepfakes" y la suplantación de identidad en el metaverso. Es esencial actualizar el código penal para incluir estas nuevas infracciones y definir claramente las sanciones correspondientes.

En entornos virtuales, la falta de un sistema de identidad interoperable y la ausencia de protocolos para el almacenamiento de direcciones IP dificultan la identificación y persecución de los agresores. Implementar sistemas de autenticación robustos, como la verificación biométrica y los certificados digitales, puede ayudar a mitigar estos riesgos. La experiencia alemana demuestra que la verificación obligatoria de identidad y sanciones estrictas son efectivas para reducir los incidentes de acoso cibernético.

Un aspecto crítico que aún no se ha abordado adecuadamente en la legislación actual es la necesidad de programas de educación digital para menores, padres y educadores. Estos programas deben centrarse en enseñar a los usuarios a identificar y protegerse contra el acoso cibernético y la explotación en línea. La concienciación es una herramienta poderosa para prevenir el acoso y promover un uso seguro de la tecnología digital. Fomentar la participación de la comunidad en la creación y promoción de campañas educativas puede aumentar la efectividad de estas iniciativas [1]. Dichas campañas deben ser inclusivas y accesibles, especialmente para las comunidades con menor acceso a recursos tecnológicos.

La colaboración internacional es esencial para abordar el acoso cibernético de manera efectiva. Armonizar las leyes a nivel global facilitará la persecución de delitos que cruzan fronteras nacionales. Ecuador debe participar activamente en foros internacionales y alianzas dedicadas a la ciberseguridad y la protección de menores en línea.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

Aprender de las mejores prácticas observadas en otros países, como Alemania, puede proporcionar un valioso modelo a seguir. La cooperación internacional también puede incluir el intercambio de tecnologías y estrategias para implementar sistemas de seguridad y autenticación más robustos.

Es fundamental llevar a cabo una evaluación crítica de las políticas actuales en Ecuador para identificar brechas y áreas de mejora. Esto abarca no solo la legislación penal, sino también las políticas educativas y de protección social. La evaluación debe basarse en datos empíricos y estudios de caso para ofrecer una comprensión integral del problema. Las políticas deben ser dinámicas y adaptarse continuamente a las nuevas tecnologías emergentes. La rápida evolución del metaverso y otras plataformas digitales requiere una respuesta legislativa y regulatoria ágil que pueda anticipar y mitigar nuevos riesgos.

La protección de la identidad digital no solo es una cuestión de seguridad, sino también de derechos humanos. Es esencial garantizar que las medidas de autenticación y verificación no infrinjan los derechos de privacidad de los usuarios. Las políticas deben equilibrar la necesidad de seguridad con la protección de los derechos individuales. Además, las medidas legislativas y educativas deben contemplar el impacto social del acoso cibernético y la protección de la identidad digital, incluyendo los efectos psicológicos en las víctimas y las repercusiones sociales para las comunidades afectadas. Las políticas deben integrar mecanismos de apoyo y rehabilitación para las víctimas de acoso cibernético.

Para enfrentar el acoso cibernético y proteger la identidad digital en Ecuador, es imprescindible llevar a cabo una reforma legislativa integral, acompañada de medidas educativas y tecnológicas. Aprender de las experiencias internacionales, como el modelo alemán, y adaptar estas prácticas a la realidad ecuatoriana puede ofrecer soluciones efectivas. La colaboración internacional, la educación y una revisión crítica de las políticas actuales son pasos necesarios para garantizar un entorno digital seguro y protegido para los menores en Ecuador. Adoptar un enfoque integral y dinámico permitirá a Ecuador enfrentar los desafíos del acoso cibernético y asegurar la protección de los derechos de sus ciudadanos en un entorno digital en constante evolución.

7. Conclusión

Los resultados arrojados a partir del desarrollo del método neutrosófico para evaluar el delito de acoso cibernético y la protección de menores en el Código Integral Penal identificó falta de una adecuada tipificación de delitos cibernéticos en el Código Integral Penal ecuatoriano, junto con su comparación con el marco legal alemán, ha puesto de manifiesto diversas áreas cruciales que requieren mejoras para proteger a los menores en entornos digitales, especialmente en el contexto del metaverso.

En primer lugar, se ha evidenciado la urgente necesidad de actualizar el Código Integral Penal ecuatoriano para incluir definiciones claras y específicas de delitos cibernéticos, tales como la suplantación de identidad y el uso de "deepfakes". La falta de una legislación específica actualmente coloca a los menores en una situación de vulnerabilidad considerable y dificulta la persecución efectiva de los agresores.

En segundo lugar, la protección de la identidad digital en el metaverso demanda la implementación de sistemas robustos de autenticación y verificación de identidad. Métodos como la biometría y los certificados digitales son esenciales para mitigar los riesgos relacionados con la suplantación de identidad y otros delitos cibernéticos.

La educación y la concienciación son igualmente fundamentales. Es vital desarrollar programas de educación digital dirigidos a menores, padres y educadores, que se enfoquen en los riesgos del acoso cibernético y las formas de protegerse en línea. La concienciación es una herramienta clave para prevenir el acoso y fomentar un uso seguro y responsable de las tecnologías digitales.

Además, la colaboración internacional se muestra como un componente esencial para abordar el acoso cibernético de manera efectiva. La armonización de las leyes a nivel global facilita la persecución de delitos que trascienden fronteras nacionales. La participación de Ecuador en foros internacionales y la adopción de las mejores prácticas observadas en otros países, como Alemania, puede fortalecer significativamente la respuesta nacional ante estos desafíos.

Asimismo, es imprescindible llevar a cabo una evaluación crítica de las políticas actuales en Ecuador para identificar brechas y áreas de mejora. Las políticas deben ser dinámicas y adaptarse continuamente a las nuevas tecnologías emergentes, anticipando y mitigando así nuevos riesgos.

La protección de los derechos humanos y la privacidad debe ser una prioridad. Las medidas de seguridad y autenticación deben equilibrarse cuidadosamente con la protección de los derechos de privacidad de los usuarios, asegurando que no se infrinjan los derechos individuales mientras se mejora la seguridad en línea. Además, es crucial incorporar mecanismos de apoyo y rehabilitación para las víctimas de acoso cibernético, abordando el impacto psicológico y social del acoso y ayudando a las víctimas a recuperarse y reintegrarse en un entorno digital seguro.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

Referencias

[1] D. P. Barráez-Herrera, “Metaversos en el Contexto de la Educación Virtual,” *Revista Tecnológica-Educativa Docentes 2.0,* vol. 13, no. 1, pp. 11-19, 2022.

[2] E. S. M. Fernández, M. L. M. García, and F. J. B. Jiménez, "Social media marketing, redes sociales y metaversos." pp. 353-366.

[3] J. Anacona, E. Millán, and C. Gómez, “Aplicación de los metaversos y la realidad virtual en la enseñanza,” *Entre ciencia e ingeniería,* vol. 13, no. 25, pp. 59-67, 2019.

[4] D. Arruda Gomes, and M. Castelo Branco Araújo, “Oferta turística virtual: Un estudio de metaverso,” *Estudios y perspectivas en turismo,* vol. 21, no. 4, pp. 876-903, 2012.

[5] R. M. Mujica-Sequera, “El Metaverso como un Escenario Transcomplejo de la Tecnoeducación,” *Revista Tecnológica-Educativa Docentes 2.0,* vol. 13, no. 1, pp. 20-28, 2022.

[6] S. Herbert, “The new science of management decision,” *New York,* 1960.

[7] E. B. F. Fincowsky, “Toma de decisiones empresariales,” *Contabilidad y Negocios* vol. Vol 6, No 11, pp. 113-120. ISSN 1992-1896, 2011.

[8] B. B. Fonseca, K. M. Kelly, and W. S. Grass, “Sistema informático para la gestión de reportes de incidencias de mantenimiento en la Facultad de Ciencias y Tecnologías Computacionales,” *Serie Científica de la Universidad de las Ciencias Informáticas,* vol. 12, no. 6, pp. 40-54, 2019.

[9] R. Bello, A. Puris, A. Nowe, Y. Martínez, and M. M. García, "Two step ant colony system to solve the feature selection problem." pp. 588-596.

[10] J. A. L. García, A. B. Peña, P. Y. P. Pérez, and R. B. Pérez, “Project control and computational intelligence: trends and challenges,” *International Journal of Computational Intelligence Systems,* vol. 10, no. 1, pp. 320-335, 2017.

[11] Y. Martínez, A. Nowé, J. Suárez, and R. Bello, "A reinforcement learning approach for the flexible job shop scheduling problem." pp. 253-262.

[12] F. Morey Cortès, “El sistema alimentario global: ponderación cuantitativa de las variables del modelo en el entorno de Cataluña,” Universitat Politècnica de Catalunya, 2019.

[13] B. Bron Fonseca, and O. Mar Cornelio, “Método para el análisis lingüístico de estadísticas médica,” *Serie Científica de la Universidad de las Ciencias Informáticas,* vol. 18, no. 1, pp. 110-127, 2025.

[14] O. M. Cornelio, A. R. Rodríguez, W. L. S. Álava, P. G. A. Mora, L. M. S. Mera, and B. J. P. Bravo, “La Inteligencia Artificial: desafíos para la educación,” *Editorial Internacional Alema,* 2024.

[15] B. B. Fonseca, and O. M. Cornelio, “Método para el análisis lingüístico de estadísticas médica,” *Serie Científica de la Universidad de las Ciencias Informáticas,* vol. 18, no. 1, pp. 110-127, 2025.

[16] B. B. F. Omar Mar Cornelio, “Neutrosophic computational model for identifying trends in scientific articles using Natural Language Processing,” *Neutrosophic Sets and Systems,* vol. 84, pp. 134-145, 2025.

[17] B. E. P. Sheila, Crespo-Berti, L.A., Fabiola, H.T.L., Cornelio, O.M., Turaeva, D., “Neutrosophic decision making using Saaty's AHP method and VIKOR,” *Journal of Intelligent Systems and Internet of Things,* vol. 12, no. 1, pp. 164-176, 2024.

[18] F. Smarandache, “Neutrosofía y Plitogenia: fundamentos y aplicaciones,” *Serie Científica de la Universidad de las Ciencias Informáticas,* vol. 17, no. 8, pp. 164-168, 2024.

[19] F. Smarandache, “Significado Neutrosófico: Partes comunes de cosas poco comunes y partes poco comunes de cosas comunes,” *Serie Científica de la Universidad de las Ciencias Informáticas,* vol. 18, no. 1, pp. 1-14, 2025.

[20] M. Leyva-Vázquez, and F. Smarandache, *Computación neutrosófica mediante Sympy*: Infinite Study, 2018.

[21] O. Mar Cornelio, Y. Zulueta Véliz, and M. Leyva Vázquez, “Sistema de apoyo a la toma de decisiones para la evaluación del desempeño en la Universidad de las Ciencias Informáticas,” 2014.

[22] M. L. Vázquez, and F. Smarandache, *Neutrosofía: Nuevos avances en el tratamiento de la incertidumbre*: Infinite Study, 2018.

[23] O. Mar, I. Santana, YunweiChen, and G. Jorge, “Model for decision-making on access control to remote laboratory practices based on fuzzy cognitive maps,” *Revista Investigación Operacional,* vol. 45, no. 3, pp. 369-380, 2024.

[24] J. E. Ricardo, M. Y. L. Vázquez, A. J. P. Palacios, and Y. E. A. Ojeda, “Inteligencia artificial y propiedad intelectual,” *Universidad y Sociedad,* vol. 13, no. S3, pp. 362-368, 2021.

[25] I. A. González, A. J. R. Fernández, and J. E. Ricardo, “Violación del derecho a la salud: caso Albán Cornejo Vs Ecuador,” *Universidad Y Sociedad,* vol. 13, no. S2, pp. 60-65, 2021.

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/

[26] G. Á. Gómez, J. V. Moya, J. E. Ricardo, and C. V. Sánchez, “La formación continua de los docentes de la educación superior como sustento del modelo pedagógico,” *Revista Conrado,* vol. 17, no. S1, pp. 431-439, 2021.

[27] O. Y. A. Gómez, O. L. O. Ortiz, and J. G. M. Angulo, “La convergencia de aprendizajes en el metaverso,” *Revista Interamericana de Investigación Educación y Pedagogía RIIEP,* vol. 15, no. 2, pp. 385-398, 2022.

[28] von Feigenblatt, O. F. “Research Ethics in Education. In Ethics in Social Science Research: Current Insights and Practical Strategies”, pp. 97-105. Singapore: Springer Nature Singapore, 2025. Availble: https://link.springer.com/chapter/10.1007/978-981-97-9881-0_7

Recibido el 23 de marzo de 2025. Aceptado el 17 de mayo de 2025

Esta obra está bajo una licencia: https://creativecommons.org/licenses/by/4.0/