Neutrosophic Computing and Machine Learning, Vol. 36, 2025
University of New Mexico

Mapa Cognitivo Neutrosófico para el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información.

Neutrosophic Cognitive Map for the analysis of the criminality of digital violence in the COIP and the right to privacy of information.

Juan Alejandro Coloma Armijos[1], Jeannette Amparito Urrutia Guevara[2] and Diego Patricio Gordillo Cevallos[3]

[1] Universidad Regional Autónoma de Los Andes, Ambato. Ecuador. juanca75@uniandes.edu.ec
[2] Universidad Regional Autónoma de Los Andes, Ambato. Ecuador. ua.jeannetteurrutia@uniandes.edu.ec
[3] Universidad Regional Autónoma de Los Andes, Ambato. Ecuador. ua.diegogordillo@uniandes.edu.ec

Resumen. La creciente prevalencia de la violencia digital ha impactado de manera significativa la intimidad, honra y seguridad personal en todo el mundo, afectando especialmente a la sociedad ecuatoriana. Este fenómeno, que carece de una base jurídica específica en muchos Estados, plantea un desafío para la moral y ética social, exacerbado por el avance tecnológico. La presente investigación propone desarrollar un Mapa Cognitivo Neutrosófico para analizar la tipicidad de la violencia digital en el Código Orgánico Integral Penal (COIP) y su relación con el derecho a la intimidad de la información. El objetivo es contribuir a la creación de un anteproyecto de ley reformatoria que modifique la sección sexta "Delitos contra el derecho a la intimidad personal y familiar" del COIP. Se buscará añadir articulados que complementen el artículo 178 y tipifiquen adecuadamente la violencia digital en Ecuador, garantizando así la protección del derecho a la intimidad de las víctimas. Para ello, se emplearán métodos cuantitativos como encuestas, cuestionarios y entrevistas, permitiendo a las víctimas conocer sus opciones de defensa jurídica. Al abordar este vacío normativo, la investigación pretende fomentar un entorno más seguro y resguardar los valores éticos en la sociedad ecuatoriana ante el crecimiento de la violencia digital.

Palabras Claves: violencia digital, intimidad de la información, COIP, Mapa Cognitivo Neutrosófico.

Abstract. The increasing prevalence of digital violence has significantly impacted privacy, honor and personal security throughout the world, especially affecting Ecuadorian society. This phenomenon, which lacks a specific legal basis in many States, poses a challenge to social morality and ethics, exacerbated by technological progress. This research proposes to develop a Neutrosophic Cognitive Map to analyze the typicality of digital violence in the Comprehensive Organic Criminal Code (COIP) and its relationship with the right to privacy of information. The objective is to contribute to the creation of a draft reform law that modifies the sixth section "Crimes against the right to personal and family privacy" of the COIP. We will seek to add articles that complement article 178 and adequately typify digital violence in Ecuador, thus guaranteeing the protection of the right to privacy of victims. To do so, quantitative methods such as surveys, questionnaires and interviews will be used, allowing victims to know their legal defense options. By addressing this regulatory gap, the research aims to foster a safer environment and safeguard ethical values in Ecuadorian society in the face of the growth of digital violence.

Keywords: digital violence, information privacy, COIP, Cognitive Neutrosophic Map.

1 Introducción

El ciberacoso ha emergido como un fenómeno destructivo que impacta directa e indirectamente la intimidad y reputación de las personas en la esfera digital. Este tipo de violencia, que puede manifestarse a través de textos difamatorios y otros métodos de acoso en línea, puede dañar la autoestima y la integridad de las víctimas, sin que estas hayan sido necesariamente objeto de tales ataques [1]. La gravedad de esta problemática ha llevado a la necesidad de una respuesta jurídica efectiva para combatir estas conductas nocivas.

Conceptos como la sextorsión, definida por la Corte Suprema de Justicia de El Salvador como un tipo de violencia sexual digital, ponen de manifiesto la vulnerabilidad de los individuos en la era de la tecnología. Este tipo de coerción no solo atenta contra la dignidad de las víctimas, sino que también muestra las lagunas existentes en las legislaciones actuales [2]. En México, la reforma penal conocida como la Ley Olimpia surgió como una respuesta legislativa a un caso emblemático de difusión no consensuada de contenido íntimo, evidenciando la necesidad de reformas que protejan adecuadamente a las víctimas de violencias digitales [3].

En Ecuador, si bien se han realizado avances en la tipificación de delitos informáticos en el Código Orgánico Integral Penal (COIP), la violencia digital sigue siendo un área escasamente abordada. El artículo 178 del COIP establece una base para la protección de la intimidad; sin embargo, es fundamental ampliar y fortalecer la legislación para incluir específicamente los diferentes tipos de violencia digital y garantizar así una vida libre de violencia para todas las personas, tal como lo establece la Constitución de la República del Ecuador.

En el contexto de la lucha contra los delitos digitales, Ecuador ha mostrado avances significativos con la presentación del proyecto de Ley Orgánica para prevenir la violencia, el acoso digital y la violación a la intimidad en 2021. Este proyecto fue una respuesta a diversas problemáticas sociales y buscó actualizar la normativa penal ecuatoriana, tipificando nuevos delitos derivados de la era digital, como el *deep fake porn* y el *mobbing*. Junto a este, se presentó el "Proyecto de Ley Orgánica Reformatoria al Código Orgánico Integral Penal", que tenía como objetivo tipificar los delitos de sexting y hostigamiento.

A pesar de ser procesadas por la Comisión de Justicia, la Asamblea Nacional aprobó solo la segunda iniciativa con 107 votos a favor el 7 de mayo de 2021, posicionando a Ecuador como potencial líder en la región en la lucha contra la violencia digital. Sin embargo, la aprobación de la Ley Orgánica de Violencia Digital fue objeto de críticas por parte de grupos como Fundamedios y diversos colectivos, que argumentaron que su contenido podría servir como herramienta de censura para investigaciones periodísticas y proteger intereses políticos. Esta preocupación llevó a una de las legisladoras a retractarse de su apoyo al proyecto, señalando que podría ser manipulado para encubrir actos corruptos. Tras su aprobación, el proyecto fue enviado al ejecutivo, donde el presidente Guillermo Lasso vetó parcialmente catorce artículos. Finalmente, el 21 de julio de 2021 se aprobó el "Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos", el cual incluyó varios artículos que tipifican delitos relacionados con la violencia digital, evidenciando un compromiso estatal por fortalecer la protección ante estas nuevas modalidades de agresión.

A pesar de las iniciativas implementadas en Ecuador para combatir la violencia digital, persiste una escasa tipicidad de este fenómeno en el Código Orgánico Integral Penal, lo que afecta gravemente el derecho a la intimidad de la información. Esta falta de regulación adecuada deja a muchas víctimas desprotegidas y vulnerables ante diversas formas de agresión digital, como el *deep fake porn* [4] y el *mobbing* [5], que han proliferado en el contexto tecnológico actual. Por ello, el objetivo de esta investigación es contribuir a la creación de un anteproyecto de ley reformatoria que modifique la sección sexta del COIP, referida a "Delitos contra el derecho a la intimidad personal y familiar". Para lograrlo, se empleará un Mapa Cognitivo Neutrosófico que permitirá un análisis exhaustivo de la tipicidad de la violencia digital en el marco legal ecuatoriano, buscando así fortalecer la protección de los derechos de las víctimas y ofrecer un enfoque integral que responda a las complejidades de la era digital.

2. Preliminares

La revolución digital ha transformado radicalmente la forma en que interactuamos, comunicamos y compartimos información, dando paso a nuevas realidades que, aunque ofrecen oportunidades, también han propiciado la aparición de delitos que vulneran la dignidad, la intimidad y los derechos de las personas. Entre estos delitos figuran el *deep fake porn*, que utiliza tecnologías avanzadas para manipular imágenes y videos en detrimento de las mujeres, y el *mobbing*, que se ha trasladado a entornos digitales y afecta especialmente a estudiantes universitarios. Estos fenómenos resaltan la importancia de establecer un marco legal sólido que aborde las complejidades de la violencia digital, protegiendo así la intimidad y los derechos fundamentales de las víctimas en una era en la que el acceso y el procesamiento de la información son cruciales. A continuación, se examinarán estos delitos y su impacto, así como la necesidad urgente de medidas efectivas para garantizar la seguridad y el respeto hacia todos los individuos en el entorno digital:

Deep Fake Porn: Desde 2017, el delito conocido como *deep fake porn* ha cobrado notoriedad en la esfera digital, evidenciando cómo la combinación de tecnología y abuso puede generar un impacto devastador sobre las mujeres. Esta práctica consiste en la manipulación de videos para insertar el rostro de actrices célebres en escenas pornográficas, lo que ha dado lugar a subcategorías como *deepnudes*, *nudefakes* y *celeb-porn*. En 2021, el desarrollo de inteligencia artificial que permite desnudar a mujeres a partir de fotografías incrementó la gravedad del problema, originando un fenómeno denominado *Automate abuse image* [6], que afectó a alrededor de 100,000 mujeres en 2020 . Este delito no solo plantea serias cuestiones éticas y legales, sino que también resalta la necesidad de una regulación específica.

Mobbing: El mobbing, descrito por René Pedroza Flores de la Universidad Autónoma del Estado de México como un acoso psicológico y moral ejercido por una persona o grupo sobre otra, ha aumentado de forma alarmante,

especialmente en los entornos universitarios [7]. Hoy en día, el *mobbing* se materializa principalmente a través de medios digitales, como WhatsApp, Facebook, Instagram y TikTok, afectando gravemente las relaciones interpersonales y la salud mental de los afectados. Este tipo de acoso se ha visto favorecido por el anonimato y la inmediatez que ofrecen las plataformas digitales, lo que complica aún más su identificación y sanción.

La intimidad de las víctimas de violencia digital es un tema central de esta investigación. Ricardo Yepes Stork define la intimidad como el mundo interior de un hombre, aludiendo a la singularidad y la irrepetibilidad de cada individuo [8]. De acuerdo con Yepes, este mundo interior es inviolable, lo que significa que la intimidad no puede ser compartida sin el consentimiento de la persona. Comprender la intimidad desde esta perspectiva es fundamental, ya que se considera un espacio que solo puede ser accedido por el propietario o por aquellos a quienes se les otorgue permiso. Así, la intimidad se presenta como un aspecto esencial de la dignidad humana, cuyo respeto debería ser garantizado por el marco legal.

Las generaciones digitales, que han crecido en la era informática, son las que más sufren las consecuencias de estos nuevos delitos. A pesar de sus habilidades para manejar la tecnología e información, estas generaciones enfrentan adicciones al uso excesivo del internet, lo que ha generado preocupaciones sobre su salud mental. Investigaciones, como las de Morrison y Gore, han evidenciado que los adolescentes que se consideran dependientes de internet muestran niveles más altos de depresión, mientras que otros estudios han vinculado el uso intensivo de la red con comportamientos agresivos y problemas en la adaptación social [9].

En Ecuador, las estadísticas sobre violencia digital siguen siendo alarmantes, aunque carecemos de cifras precisas proporcionadas por el Instituto Nacional de Estadísticas y Censos. Sin embargo, investigaciones del Taller Comunicación Mujer indican que el contacto sexual con niños y adolescentes a través de medios digitales es uno de los delitos más denunciados en el país. Asimismo, la ciberviolencia ha tomado la forma de violación a la intimidad, que se reportó con 7,822 casos entre agosto de 2014 y julio de 2019, de los cuales solo un pequeño porcentaje llegó a juicio. Estos números reflejan la desproporción entre la cantidad de denuncias y las sanciones efectivas, lo que genera un entorno de impunidad y temor entre las víctimas. Sin un marco jurídico adecuado, muchas víctimas se sienten desprotegidas y prefieren no denunciar, lo que perpetúa la violación de sus derechos a la intimidad, honra, dignidad y buen nombre. La falta de acciones concretas por parte del sistema judicial solo agrava la situación, dejando a las víctimas en un estado de indefensión y vulnerabilidad.

3. Materiales y métodos

Los problemas presentes para combatir la violencia digital que afecta gravemente el derecho a la intimidad de la información, pueden ser modelado como un problema de toma de decisiones multicriterio a partir del conjunto de tendencias que representan las alternativas a analizar en el proceso sobre el pensamiento en el que:

El número de hechos delictivos $P= \{P_1, ... P_n\}, n \geq 1,$

Que poseen un conjunto de características relacionadas al ciberacoso, que representan los múltiples criterios valorativos donde:

$C= \{C_1, ... C_m\}, m \geq 2.$

La investigación se enmarca en el objeto de estudio del análisis en los indicadores que permite evaluar la escasa tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información. Utiliza técnicas de inteligencia artificial para la inferencia sobre el análisis de incidencias y basa su funcionamiento a partir del método científico del criterio de expertos para obtener la base de conocimiento necesaria en el desarrollo de la investigación. Para el desarrollo de la presente, se modeló las relaciones causales de los indicadores que permite evaluar la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información. En este estudio es necesario comprender los siguientes conceptos:

- **Modelos causales:** existen diferentes tipos de causalidad que son expresadas en forma de grafos, donde cada modelo causal que se puede representar por un grafo son representaciones de la causalidad entre conceptos. Los modelos causales permiten modelar la causa o efecto de un determinado evento [10, 11] . La Figura 1 muestra un esquema con las diferentes relaciones causales.

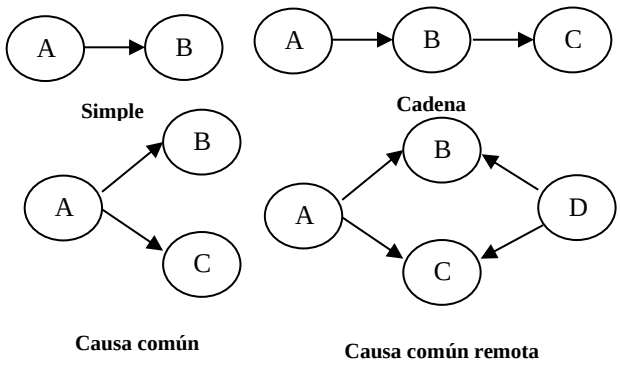

Figura 1: Ejemplo de grafos causales.

- **Mapa Cognitivo Neutrosófico (MCN):** es una técnica que permite la representación de las relaciones causales de diferentes conceptos propuesta por Kosko [12] como una extensión de los modelos mentales empleando valores difusos en un intervalo de [-1,1]. Los MCN se representan mediante modelos difusos con retroalimentación para representar causalidad [13, 14].

En el MCD existen tres posibles tipos de relaciones causales entre conceptos [15]:

• $W_{ij} > 0$, indica una causalidad positiva entre los conceptos C_j y C_i. Es decir, el incremento (o disminución) en el valor de C_j lleva al incremento (o disminución) en el valor de C_i.

• $W_{ij} < 0$, indica una causalidad negativa entre los conceptos C_j y C_i. Es decir, el incremento (o disminución) en el valor de C_j lleva a la disminución (o incremento) en el valor de C_i.

• $W_{ij} = 0$, indica la no existencia de relaciones entre los conceptos C_j y C_i.

3.1 Método para el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información

El sistema propuesto está estructurado para soportar el proceso de gestión en el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información. Basa su funcionamiento mediante un enfoque multicriterio multiexperto donde se modela la integración de la tipicidad de la violencia digital con el derecho a la protección de la intimidad, a partir del conjunto de criterios que definen el caso. Utiliza en su inferencia modelos causales como forma de representar el conocimiento a partir de la técnica de inteligencia artificial Mapa Cognitivo Neutrosófico. El método está diseñado mediante una arquitectura en tres capas: entradas, procesamiento y salida de información.

Metodo para el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información

Entradas	Procesamiento	Salidas
Indicadores	1. Identificación de los indicadores	
Expertos	2. Determinación de las relaciones causales	Relaciones causales
Causalidad	3. Determinación de los pesos	
	4. Identificación de las preferencias	Inferencia
Preferencias	5. Generación de la inferencia	

Figura 2. Estructura del método propuesto.

El método para el análisis de la tipicidad de la violencia digital, está conformado por cinco actividades: (1) identificación de las incidencias; (2) determinación de las relaciones causales; (3) identificación de los pesos atribuidos a las incidencias; (4) identificación de las preferencias; y (5) generación de la inferencia. Estas actividades son descritas a continuación.

Actividad 1 identificación de los indicadores: La identificación de los indicadores para el análisis de la tipicidad de la violencia digital, en la que se determinan el conjunto general de indicadores que determinar la base de

inferencia [16-18]. Se utiliza un enfoque multicriterio para analizar la base de casos, por lo que se identifican la mayor cantidad de indicadores posibles.

Actividad 2 determinación de las relaciones causales: En esta actividad se utiliza un enfoque multicriterio multiexperto. Garantiza la representación del conocimiento causal de los indicadores [19, 20]. La actividad consiste en extraer el conocimiento que poseen los expertos sobre los casos de ciberacoso y la protección a las víctimas. Las relaciones causales son expresadas mediante un dominio de valores que expresan relaciones de implicación directas o inversas para lo cual se utiliza la escala tal como muestra la Tabla1. Esta actividad es muy importante ya que el conocimiento que poseen los expertos sobre los delitos digitales no está registrado en la base de casos analizada.

Tabla 1: Dominio de valores para expresar causalidad.

Término lingüístico	Números SVN
Extremadamente buena (EB)	[1,0,0]
Muy muy buena (MMB)	[0.9, 0.1, 0.1]
Muy buena (MB)	[0.8,0,15,0.20]
Buena (B)	[0.70,0.25,0.30]
Medianamente buena (MDB)	[0.60,0.35,0.40]
Media (M)	[0.50,0.50,0.50]
Medianamente mala (MDM)	[0.40,0.65,0.60]
Mala (MA)	[0.30,0.75,0.70]
Muy mala (MM)	[0.20,0.85,0.80]
Muy muy mala (MMM)	[0.10,0.90,0.90]
Extremadamente mala (EM)	[0,1,1]

Durante la determinación de las relaciones causales se realiza un proceso de agregación donde se obtiene un arreglo denominado matriz de adyacencia que representa los valores asignados a los arcos [21], [22], [23] de modo que:

$$M = \begin{bmatrix} \cdot\cdot & \cdot\cdot & \cdot\cdot \\ \cdot\cdot & W_{ij} & \cdot\cdot \\ \cdot\cdot & \cdot\cdot & \cdot\cdot \\ \cdot\cdot & \cdot\cdot & \cdot\cdot \end{bmatrix}$$

La matriz de adyacencia $M = M(C_i C_j)$ representa el valor causal de la función del arco, el nodo C_i que es imparte C_j. C_i incrementa causalmente a C_j si $M_{ij} = -1$, y no imparte causalmente sí $M_{ij} = 0$.

Actividad 3 identificación de los pesos atribuidos a los indicadores: a partir de la obtención en la actividad 2 de la matriz de adyacencia, los valores agregados emitidos por los expertos agrupados, conforman las relaciones con los pesos de los nodos, a través del cual es generado el Mapa Cognitivo Neutrosófico resultante [24], [25]. Mediante un análisis estático del resultado de los valores obtenidos en la matriz de adyacencia se puede calcular el grado de salida utilizándose la ecuación (1) donde se obtienen los pesos atribuidos a cada caso.

$$id_i = \sum_{i=1}^{n} \left\| I_{ji} \right\| \tag{1}$$

Actividad 4 identificaciones de las preferencias: la identificación de las preferencias es la actividad que consiste en determinar cuál es el comportamiento actual la tipicidad de la violencia digital en el COIP. Para ello se entrevista a los especialistas y se determina el grado de preferencia que poseen los indicadores a partir de la evaluación. La Tabla 2 muestra el dominio de valores con sus etiquetas lingüísticas utilizados para expresar las preferencias sobre los casos se ciberacoso.

Tabla 2: Dominio de valores para expresar preferencias.

Valor	Impacto
[0,1,1]	Ausencia del indicador (AI)
[0.20,0.85,0.80]	Ligera presencia del indicador (LP)
[0.50,0.50,0.50]	Baja presencia del indicador (BP)
[0.70,0.25,0.30]	Presencia del indicador (PS)
[1,0,0]	Alta presencia del indicador (AP)

Actividad 5 generación de la inferencia: el proceso de generación del análisis se basa en la simulación del escenario propuesto por Glykas [19, 26-28] los nuevos valores de los conceptos expresan la influencia de los conceptos interconectados al concepto específico y se calculan mediante la ecuación (2):

$$A_i^{(K+1)} = f\left(A_i^{(K)} \sum_{i=1;\, j\neq i}^{n} A_i^{(K)} * W_{ji}\right) \quad (2)$$

Donde:

$A_i^{(K+1)}$: es el valor del concepto C_i en el paso k+1 de la simulación,

$A_i^{(K)}$: es el valor del concepto C_j en el paso k de la simulación,

W_{ji}: es el peso de la conexión que va del concepto C_j al concepto C_i y f (x) es la función de activación [29].

4 Resultados y discusión

La presente sección realiza una descripción de la implementación del método para el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información, mediante Mapa Cognitivo Neutrosófico. El caso de estudio analiza el comportamiento en casos atendidos en Ecuador durante el año 2024. A partir del análisis de casos es posible determinar el comportamiento de las diferentes alternativas en función del análisis de los indicadores. A continuación se describen los resultados del estudio:

Actividad 1 identificación de los indicadores:

Para determinar los indicadores se utilizó el criterio de experto llegando a las siguientes conclusiones propuestas en la tabla 3.

Tabla 3: Identificación de los indicadores.

Nodo	Indicadores evaluativos
C_1	Definiciones relevantes en el COIP: ¿Está claramente tipificado el delito en la legislación? Verifica si el caso específico de ciberacoso se enmarca dentro de las definiciones legales existentes en el COIP.
C_2	Número de denuncias: ¿Se ha reportado el caso a las autoridades pertinentes? Evalúa cuántas denuncias han sido presentadas en relación con el caso particular.
C_3	Proporción de sanciones: ¿Qué porcentaje de casos similares han resultado en condenas? Determina si el caso ha resultado en una sanción o condena. ¿Se ha dictado alguna sentencia en relación con el ciberacoso?
C_4	Mecanismos de protección para la víctima: ¿Existen recursos legales o protección que la víctima pueda utilizar para salvaguardar su intimidad? Analiza si se han ofrecido mecanismos de protección a la víctima durante el proceso.
C_5	Conciencia y educación sobre derechos: ¿Hay acceso a información o recursos sobre cómo actuar ante el ciberacoso? Considera el nivel de conocimiento de la víctima sobre sus derechos a la intimidad y cómo manejar situaciones de ciberacoso.

Actividad 2 determinación de las relaciones causales:

La determinación de las relaciones causales entre las incidencias se utiliza en la escala propuesta en la Tabla 1, donde participaron 5 expertos, se obtuvieron los 5 Mapas Cognitivos Neutrosóficos agregando las respuestas en un único resultado. La Tabla 4 muestra la matriz de adyacencia obtenida como resultado del proceso.

Tabla 4: Matriz de adyacencia resultante

	C_1	**C_2**	**C_3**	**C_4**	**C_5**
C_1	[0, 0,0]	[1,0,0]	[0.5, 0.25,0]	[0.5, 0.25,0]	[0.75, 0.5,0.25]
C_2	[1,0,0]	[0, 0,0]	[0.75, 0.5,0.25]	[1,0,0]	[0.5, 0.25,0]
C_3	[0.5, 0.25,0]	[0.5, 0.25,0]	[0, 0,0]	[0.5, 0.25,0]	[1,0,0]
C_4	[0.5, 0.25,0]	[1,0,0]	[0.5, 0.25,0]	[0, 0,0]	[0.75, 0.5,0.25]
C_5	[0.75, 0.5,0.25]	[0.75, 0.5,0.25]	[0.5, 0.25,0]	[1,0,0]	[0, 0,0]

Actividad 3 identificación de los pesos atribuidos a los indicadores:

Para la identificación de los pesos se tiene en cuenta la base de conocimiento almacenado en la matriz de adyacencia de la Tabla 4, aplicando la ecuación (1), se obtiene el comportamiento del peso los indicadores para el análisis de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información. La Tabla 5

muestra los pesos resultantes.

Tabla 5: Peso atribuido a los indicadores

Nodos	Indicadores	Peso
C_1	Definiciones relevantes en el COIP	[0.55,0.50,0.50]
C_2	Número de denuncias	[0.65,0.35,0.40]
C_3	Proporción de sanciones	[0.50,0.50,0.50]
C_4	Mecanismos de protección para la víctima	[0.55,0.50,0.50]
C_5	Conciencia y educación sobre derechos	[0.60,0.35,0.40]

Actividad 4 identificación de las preferencias:

A partir de la entrevista a la víctima se determinó el grado de preferencia que poseen los indicadores evaluativos en la protección del derecho a la intimidad de la información. El estudio fue realizado en una alternativa que representa la víctima objeto de estudio. La Tabla 6 muestra los valores resultantes.

Tabla 6: preferencia atribuida a las incidencias de los indicadores

Alternativa	C_1	C_2	C_3	C_4	C_5
A_1	[0.5, 0.25,0]	[0.75, 0.5,0.25]	[0.75, 0.5,0.25]	[0.5, 0.25,0]	[0.5, 0.25,0]

Actividad 5 generación de la inferencia:

A partir del proceso de simulación de escenario, se obtuvieron las predicciones de los comportamientos en el tiempo de la efectividad de la tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información, mediante el empleo de la ecuación (2). La predicción modela las relaciones de causalidad de los indicadores que miden la efectividad de la tipicidad actual. La Figura 2 muestra el resultado de la simulación donde se muestran su evolución.

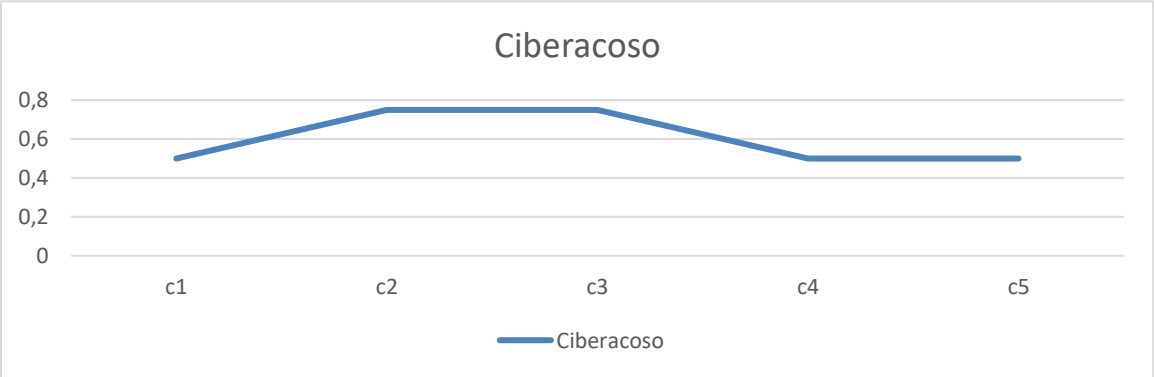

Figura 2: Resultado de la simulación de los indicadores.

A partir del comportamiento de los pesos atribuidos a la alternativa y las preferencias se determina mediante un proceso de agregación el grado de pertenencia del indicador. La Tabla 6 muestra el resultado del cálculo realizado.

Tabla 6: Procesamiento de la inferencia

Alternativa A_1	**Pesos**	**Preferencias**	**Agregación**
C_1	[0.55,0.50,0.50]	[0.5, 0.25,0]	[0.52, 0.25,0]
C_2	[0.65,0.35,0.40]	[0.75, 0.5,0.25]	[0.7, 0.5,0.25]
C_3	[0.50,0.50,0.50]	[0.75, 0.5,0.25]	[0.62,0.35,0.40]
C_4	[0.55,0.50,0.50]	[0.5, 0.25,0]	[0.52, 0.25,0]
C_5	[0.60,0.35,0.40]	[0.5, 0.25,0]	[0.55, 0.25,0]
Índice			[0.53, 0.25,0]

A partir del índice determinado se realiza una comparación del valor obtenido donde se evidencia un índice de

tipicidad de la violencia digital en el COIP y el derecho a la intimidad de la información de un I= 0.53, lo que representa un bajo índice de efectividad y protección.

Formulación de la propuesta

El resultado de la implementación del método neutrosófico ha revelado una escasa tipicidad de la violencia digital en el Código Orgánico Integral Penal (COIP) y en la protección del derecho a la intimidad de la información. Esta situación evidencia la necesidad urgente de reformar la legislación actual para que Ecuador cuente con un marco legal que sancione de manera efectiva a quienes vulneran los derechos establecidos en la Constitución y en los Tratados y Convenios internacionales suscritos por el país. En este contexto, se propone la creación de un anteproyecto de ley reformatoria a la sección sexta del COIP, titulada "Delitos contra el derecho a la intimidad personal y familiar", incluyendo nuevos articulados que complementen lo estipulado en el artículo 178.

Implementar esta reforma no solo brindará un respaldo legal sólido que proteja la honra, dignidad y buen nombre de los ciudadanos ecuatorianos, sino que también contribuirá a generar bienestar y seguridad en la sociedad. Es fundamental que el nuevo Código permita a las víctimas de ciberacoso y violaciones a la intimidad contar con un marco que legitimice sus denuncias y garantice un proceso de justicia efectivo. Esta transformación legal será un paso crucial en el desarrollo de nuevas políticas públicas que aborden la problemática actual en el país, movilizando la participación de todos los actores y niveles de gobierno para brindar soluciones integrales a esta grave cuestión social.

La construcción de un marco legal robusto y comprensivo es indispensable para enfrentar los retos que plantea la era digital, asegurando así que los derechos de cada individuo sean salvaguardados y respetados, mediante políticas que promuevan una convivencia más segura y equitativa en el ámbito digital.

5. Discusión

La reforma a la sección sexta "Delitos contra el derecho a la intimidad personal y familiar" del Código Orgánico Integral Penal está destinada a actualizar la normativa penal ecuatoriana, reconocer y sancionar los nuevos tipos de violencia que surgen en el entorno digital.

Dentro de la investigación "Análisis de la Ley de Violencia Digital en Ecuador Una mirada a las experiencias de la violencia machista en el ámbito digital" realizado por Jhanela Anahí Durán González como tema para Maestría de Investigación en Género y Comunicación en la Universidad Andina Simón Bolívar encontramos varias aristas concordantes respecto de la problemática que planteamos en la presente investigación, datos como el informe de la Comisión de las Naciones Unides para Banda Ancha "tres cuartas partes de las mujeres han estado expuestas en línea a alguna forma de ciberviolencia" (ONU 2015). Además, agrega "73 % de las mujeres ya se ha visto expuesta o ha experimentado algún tipo de violencia en línea" (ONU 2015). Es importante adicionar la investigación realizada por los autores Miguel Ángel Guambo Llerena y Olivia Mishell Andrade Valle en su artículo "La violencia sexual digital y el derecho a la intimidad" abordando la situación grave que atraviesa el Ecuador respecto de la violencia en los medios digitales, llegamos a un mismo punto al considerar que el legislativo debe empezar a normar estas tipologías de delitos sexuales, que castiguen con normas claras y precisas, que otorguen protección a aquellas víctimas que únicamente se hallan en un estado de indefensión.

6. Conclusión

Los resultados de esta investigación evidencian la necesidad de reformar el Código Orgánico Integral Penal de Ecuador, dado el bajo índice de efectividad observado en la tipicidad de la violencia digital y la protección del derecho a la intimidad de la información. A través de la implementación del Mapa Cognitivo Neutrosófico, se pudo realizar un análisis exhaustivo que reveló la escasez de normativas específicas capaces de sancionar adecuadamente los delitos relacionados con el ciberacoso y otras formas de violencia digital. Esta carencia no solo deja a las víctimas en una situación de indefensión, sino que también perpetúa la impunidad en un contexto donde la violencia digital está en aumento. Por lo tanto, se concluye que la creación de un anteproyecto de ley reformatoria a la sección sexta del COIP, que incluya nuevos artículos complementarios al artículo 178, es fundamental para establecer un marco legal que proteja los derechos fundamentales de los ciudadanos. Solo mediante una legislación robusta y clara se podrá proporcionar bienestar y seguridad a la población, garantizando así el respeto a la honra, la dignidad y el buen nombre de cada individuo en el entorno digital.

Referencias

[1] M. Mukred, U. A. Mokhtar, F. A. Moafa, A. Gumaei, A. S. Sadiq, and A. Al-Othmani, "The roots of digital aggression: Exploring cyber-violence through a systematic literature review," *International Journal of Information Management Data Insights,* vol. 4, no. 2, pp. 100281, 2024.

[2] J. Van Ouytsel, Y. Lu, Y. Shin, B. L. Avalos, and J. Pettigrew, "Sexting, pressured sexting and associations with dating violence among early adolescents," *Computers in human behavior,* vol. 125, pp. 106969, 2021.

[3] A. E. N. Garcés, and J. N. Ruiz, "La violencia digital en México (Ley Olimpia)," *Revista Criminalia Nueva Época,* vol. 87, no. Conmemorativo, 2020.

[4] E. Meskys, J. Kalpokiene, P. Jurcys, and A. Liaudanskas, "Regulating deep fakes: legal and ethical considerations," *Journal of Intellectual Property Law & Practice,* vol. 15, no. 1, pp. 24-31, 2020.

[5] J. G. Carvajal Oroz, and C. A. Dávila Londoño, "Mobbing o acoso laboral. Revisión del tema en Colombia," *Cuadernos de Administración (Universidad del Valle),* vol. 29, no. 49, pp. 95-106, 2013.

[6] E. Bursztein, E. Clarke, M. DeLaune, D. M. Elifff, N. Hsu, L. Olson, J. Shehan, M. Thakur, K. Thomas, and T. Bright, "Rethinking the detection of child sexual abuse imagery on the internet." pp. 2601-2607.

[7] R. P. Flores, "Mobbing en la universidad, violencia y hostigamiento grupal," *Revista Electrónica de Psicología Iztacala,* vol. 23, no. 1, 2020.

[8] L. M. Gómez Rivas, "A Chronicle of Liberal Thought in Spain: From Salamanca to Vienna Through Madrid," *The Emergence of a Tradition: Essays in Honor of Jesús Huerta de Soto, Volume II: Philosophy and Political Economy*, pp. 85-94: Springer, 2023.

[9] C. M. Morrison, and H. Gore, "The relationship between excessive Internet use and depression: a questionnaire-based study of 1,319 young people and adults," *Psychopathology,* vol. 43, no. 2, pp. 121-126, 2010.

[10] O. M. Cornelio, B. B. Fonseca, and F. R. Marzo, "Metodología para la reutilización de la basura tecnológica en la asignatura de Arquitectura de Computadoras," *UNESUM-Ciencias. Revista Científica Multidisciplinaria,* vol. 5, no. 2, pp. 183-198, 2021.

[11] 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.

[12] B. KOSKO, "Fuzzy cognitive maps," *International Journal of Man-Machine Studies,* vol. 24, no. 1, pp. 65-75, 1986.

[13] 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.

[14] 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.

[15] Gonzalo Nápoles, Maikel Leon Espinosa, Isel Grau, Koen Vanhoof, and R. Bello, *Fuzzy Cognitive Maps Based Models for Pattern Classification: Advances and Challenges*, p.^pp. 83-98, Soft Computing Based Optimization and Decision Models, 2018.

[16] B. B. Fonseca, and O. Mar, "Implementación de operador OWA en un sistema computacional para la evaluación del desempeño," *Revista Cubana de Ciencias Informáticas*, 2021.

[17] C. Marta Rubido, and O. M. Cornelio, "Práctica de Microbiología y Parasitología Médica integrado al Sistema de Laboratorios a Distancia en la carrera de Medicina," *Revista de Ciencias Médicas de Pinar del Río,* vol. 20, no. 2, pp. 174-181, 2016.

[18] O. Mar, and B. Bron, "Procedimiento para determinar el índice de control organizacional utilizando Mapa Cognitivo Difuso," *Serie Científica,* pp. 79-90.

[19] B. B. Fonseca, O. M. Cornelio, and I. P. Pupo, "Sistema de recomendaciones sobre la evaluación de proyectos de desarrollo de software," *Revista Cubana de Informática Médica,* vol. 13, no. 2, 2021.

[20] M. Cornelio, "Estación de trabajo para la práctica de Microbiología y Parasitología Médica en la carrera de medicina integrado al sistema de laboratorios a distancia," *Revista de Ciencias Médicas de Pinar del Río,* vol. 20, no. 2, pp. 174-181, 2016.

[21] W. Stach, L. Kurgan, and W. Pedrycz, "Expert-Based and Computational Methods for Developing Fuzzy Cognitive Maps," *In M. Glykas (Ed.), Fuzzy Cognitive Maps* B. Springer, ed., pp. 23- 41, 2010.

[22] J. E. Ricardo, N. B. Hernández, R. J. T. Vargas, A. V. T. Suntaxi, and F. N. O. Castro, "La perspectiva ambiental en el desarrollo local," *Dilemas contemporáneos: Educación, Política y Valores*, 2017.

[23] O. Mar Cornelio, "Modelo para la toma de decisiones sobre el control de acceso a las prácticas de laboratorios de Ingeniería de Control II en un sistema de laboratorios remoto," 2019.

[24] E. White, and D. Mazlack, "Discerning suicide notes causality using fuzzy cognitive maps." pp. 2940-2947.

[25] M. Y. L. Vasquez, G. S. D. Veloz, S. H. Saleh, A. M. A. Roman, and R. M. A. Flores, "A model for a cardiac disease diagnosis based on computing with word and competitive fuzzy cognitive maps," *Revista de la Facultad de Ciencias Médicas de la Universidad de Guayaquil,* vol. 19, no. 1, 2018.

[26] Author ed.^eds., "Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications," *Secaucus, NJ, USA*: Springer Verlag, 2010, p.^pp. Pages.

[27] O. Mar-Cornelio, I. Santana-Ching, and J. González-Gulín, "Sistema de Laboratorios Remotos para la práctica de Ingeniería de Control," *Revista científica,* vol. 3, no. 36, 2019.

[28] M. Y. L. Vázquez, I. A. M. Alcivar, M. E. P. González, R. M. A. Flores, R. L. Fernández, and M. A. T. Bonifaz, "Obtención de modelos causales como ayuda a la comprensión de sistemas complejos," *Revista de la Facultad de Ciencias Médicas de la Universidad de Guayaquil*, vol. 18, no. 2, 2018.

[29] R. Giordano, and M. Vurro, *Fuzzy cognitive map to support conflict analysis in drought management fuzzy cognitive maps*, 2010.

Recibido: noviembre 18, 2024. **Aceptado:** diciembre 08, 2024