Universidad San Gregorio De Portoviejo

Carrera De Derecho

Trabajo de investigación de Artículo Científico previo a la obtención del Título de Abogado

Título:

La cibercriminalidad un nuevo desafío para el derecho penal ecuatoriano.

Autores:

Juleidy Auxiliadora Macías Alcívar

Victoria Monserrate Bravo Jaya

Tutor:

Ab. Tania Muñoa Vidal, Mg.

Cantón Portoviejo – Provincia de Manabí - República del Ecuador

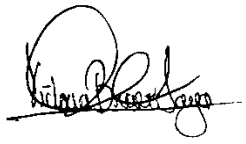
Octubre 2023 – marzo 2024

Declaración de autoría y cesión de derechos de propiedad intelectual

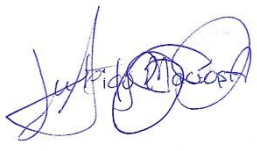
Nosotras Juleidy Auxiliadora Macías Alcívar y Victoria Monserrate Bravo Jaya declaramos, en forma libre y voluntaria, ser las autoras del presente trabajo de investigación, cuyo contenido es auténtico, original y no infringe derechos de propiedad intelectual de terceros. En este sentido, asumimos la responsabilidad correspondiente ante cualquier falsedad, ocultamiento u omisión de la información obtenida en el proceso de investigación. Así como también los contenidos, ideas, análisis, conclusiones y propuestas son exclusiva responsabilidad de mi persona, como autor/a.

De manera expresa cedemos los derechos de propiedad intelectual del Artículo Científico "La cibercriminalidad un nuevo desafío para el Derecho penal ecuatoriano", a la Universidad San Gregorio de Portoviejo, por ser la institución de Educación Superior que nos acogió en todo el proceso de desarrollo del mismo, y autorizo a su difusión en formato digital, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior.

Portoviejo, 27 de marzo de 2024



C.C: 131680612-2



C.C: 131573718-7

La cibercriminalidad un nuevo desafío para el Derecho penal ecuatoriano.

Cybercrime a new challenge for ecuadorian criminal law.

Datos de los autores:

Victoria Monserrate Bravo Jaya.
E-mail: e.vmbravo@sangregorio.edu.ec
ORCID: https://orcid.org/0009-0006-4464-5398

Juleidy Auxiliadora Macías Alcívar.
E-mail: e.jamaciasa@sangregorio.edu.ec
ORCID: https://orcid.org/0009-0007-7340-0426

Datos del tutor:
Ab. Tania Muñoa Vidal, Mg.
E-mail: tmunoa@sangregorio.edu.ec
ORCID: https://orcid.org/0000-0003-4820-9666

Resumen

El Derecho penal ecuatoriano se enfrenta a una serie de necesidades de regulación en un territorio complejo, el del ciberespacio, con lo cual el objetivo principal del artículo se basó en analizar las nuevas formas de delincuencia emergentes en el ámbito digital y cómo estas desafían las leyes penales tradicionales del Ecuador, con ello, se buscó comprender las características de la cibercriminalidad así como su rápida evolución información con la cual se pudo evaluar la eficacia del actual marco legal ecuatoriano para combatirla. El artículo exploró las bases legales que se podrían implementar para enfrentar este nuevo desafío de manera efectiva. Este análisis se hizo mediante metodología de estudio como la comparación jurídica y la teórica jurídica. Tras el análisis de la cibercriminalidad, se obtuvo como resultado la identificación de limitaciones normativas significativas, además se concluyó que se requieren reformas urgentes para fortalecer la protección ciudadana, con lo que se recomendó la actualización y la ampliación de leyes que abordan específicamente los delitos en el ámbito digital.

Palabras clave: Ciberamenzas; cibercriminalidad; ciberespacio; delito informático; seguridad ciudadana.

Abstract

Ecuadorian criminal law faces a series of regulatory needs in a complex territory, that of cyberspace, which is why the main objective of the article was based on analyzing the new forms of crime emerging in the digital sphere and how these challenge the laws. traditional criminal penalties of Ecuador, with this, we sought to understand the characteristics of cybercrime as well as its rapid evolution, information with which it was possible to evaluate the effectiveness of the current Ecuadorian legal framework to combat it. The article explored the legal bases that could be implemented to address this new challenge effectively. This analysis was done through study

methodology such as legal comparison and legal theory. After the analysis of cybercrime, the result was the identification of significant regulatory limitations, and it was also concluded that urgent reforms are required to strengthen citizen protection, which recommended updating and expanding laws that specifically address crimes in cybercrime. the digital realm.

Keywords: Cyber threats; cybercrime; cyberspace; cybercrime; citizen security.

Introducción

El mundo de las tecnologías ha desarrollado consigo problemas que requieren de la intervención legal, es por ello que, bajo la iniciativa de regulación se definen y categorizan diversas acciones en el medio según sus características, causas y efectos para entender a la cibercriminalidad como un nuevo desafío para el Derecho penal ecuatoriano; de este modo, al ser un tema relativamente actual, se mantiene la duda acerca de si la normativa penal ecuatoriana es suficiente para la protección de la seguridad ciudadana frente a la cibercriminalidad.

Bajo esta visión se formula una pregunta que aborda la problemática del tema de la siguiente manera: ¿Es la normativa penal ecuatoriana suficiente para la protección de la seguridad ciudadana frente a la cibercriminalidad?

Ante este dilema, varios pensadores del Derecho han clasificado y desglosado los elementos necesarios para entender este fenómeno de la cibercriminalidad con el objetivo de crear formas de defensa e incluso, maneras de combatir estas acciones, tales opiniones como las de Roxin, Muñoz, Morón y demás posiciones legales, han llevado a entender los componentes legales o armas con las cuales se puede poner rente a este fenómeno en el área legal de todas las ramas y bajo diferentes actividades.

Gracias a las investigaciones doctrinales previas, se ha podido comprender que, en la era digital, el ciberespacio se ha convertido en un espacio vital para la sociedad, pero también ha

abierto las puertas a nuevas formas de delitos y riesgos legales, con lo cual la autora Isabel Morón Pendas, especialista en Derecho penal y ciberseguridad, se ha destacado por su análisis profundo de estas problemáticas. Así pues, en uno de sus trabajos explora los riesgos que el ciberespacio genera para los derechos fundamentales, como la privacidad, la libertad de expresión y la seguridad jurídica, además Morón Pendas analiza elementos como el cibercrimen, las ciberamenazas, la ciberdelincuencia como componentes de impacto en las normas y leyes tradicionales.

A partir de ello, se ha podido comprender de estas cuestiones además de renombrar de manera prioritaria su importancia para construir un marco legal adecuado para que proteja a los ciudadanos en el mundo digital, con ello se entiende que sus aportes son fundamentales para avanzar en este campo, ya que ofrecen una perspectiva integral que combina el Derecho, la tecnología y la criminología.

El presente artículo de reflexión se realiza bajo la necesidad de comprender las nuevas formas de delincuencia que surgen en el ámbito digital y cómo estas impactan en la sociedad ecuatoriana, el rápido crecimiento de las tecnologías de la información y la comunicación ha generado nuevas oportunidades para la comisión de delitos, lo que exige una respuesta legal adecuada, así pues, se entiende que el estudio busca analizar las características de la cibercriminalidad y evaluar la eficacia del marco legal actual para combatirla.

El objetivo de esta investigación se basa principalmente en analizar si la normativa ecuatoriana es competente para tratar la cibercriminalidad, considerando los elementos y acciones que comprometen un comportamiento legalmente reconocido como antisocial en el tema tecnológico, con lo que se busca entender para crear romas legales de prevención de estas actividades o defensa.

Se debe tener en cuenta que, para poder llegar a comprender lo anterior, es necesario estudiar cuáles figuras delictivas previstas en el COIP, tiene como escenario el ciberespacio; además, se requiere del poder definir las ciberamenazas que ponen en riesgo bienes jurídicos protegidos por el ordenamiento jurídico penal para finalmente poder determinar las actividades delictivas que corresponden a la cibercriminalidad como problema de seguridad ciudadana.

Gracias a los grandes avances tecnológicos, se abarca el desarrollo del Derecho penal, considerando que aún hay temas de atención para la regulación de actividades ilícitas, por eso, con el análisis de las limitaciones de la legislación ecuatoriana ante la cibercriminalidad, se considerarán factores que aún no se contemplan o regulan implícitamente y que resultan un grave problema en la sociedad y las actividades ejecutadas dentro del ciberespacio, lo que lleva a entender que la investigación del tema es de suma conveniencia para el avance de las actividades.

En virtud de esto, el desarrollo jurídico social se ha aparejado con otros desafíos, tal es el caso entre el desarrollo tecnológico y la ampliación de los niveles de riesgos que propician la criminalidad, por lo que, los avances tecnológicos han facilitado la comisión de delitos, por ejemplo, los delincuentes pueden utilizar los sistemas informáticos para el robo de datos personales o para interrumpir el funcionamiento de infraestructuras críticas, por lo que, para hacer frente a estos nuevos riesgos, es necesario que las autoridades desarrollen nuevas estrategias de seguridad, estas estrategias deben incluir la educación de los ciudadanos sobre los riesgos tecnológicos, así como la inversión en nuevas tecnologías de seguridad.

La intención del estudio del presente trabajo de investigación es el análisis del cibercrimen, entendido como un fenómeno complejo que involucra diversas dimensiones, tales como la tecnológica, la jurídica y la social, además, la importancia y pertinencia de este tema

radica en el creciente aumento de los delitos cibernéticos, los cuales representan una grave amenaza para la seguridad de datos e información no solo de las personas sino también de organizaciones.

Ahora bien, con respecto al desarrollo de la investigación sobre la cibercriminalidad, se pueden identificar varios aspectos que no han sido regulados actualmente, con lo cual, en virtud de esto será posible principalmente mejorar la comprensión de este fenómeno y por ende facilitar su prevención y sanción; a partir de esto se podrá posteriormente elaborar normas jurídicas adecuadas para enfrentar aquellas actividades dedicadas a la cibercriminalidad; lo que podría direccionar finalmente a desarrollar nuevas tecnologías y herramientas para la lucha contra la cibercriminalidad.

La investigación servirá principalmente para incluir en una categoría criminal aquellas actividades que no han sido reguladas por ninguna normativa vigente hasta el momento y de esta manera plantear consecuencias ante las acciones cibernéticas ilícitas que corrompen a los miembros de una comunidad, de esa manera, se aporta con una nueva visión del área cibernética y aquellas categorías que requieren de atención para mantener una regulación u orden como en otros campos.

El tema se desarrolla bajo un enfoque jurídico- sociológico que aborda las limitaciones de la legislación ecuatoriana frente a la cibercriminalidad, lo que se acompaña a su vez desde una perspectiva jurídica la cual se respalda en las normativas nacionales e internacionales pertinentes, delineando comparaciones legislativas para identificar las brechas y desafíos existentes en la cibercriminalidad, lo que lleva a analizar las percepciones contemporáneas entorno al ciberespacio, logrando así plantear un escenario complejo que requiere atención específica en materia de ciberseguridad.

El análisis se centra en la tipicidad y antijuricidad de los actos delictivos en este contexto, evidenciando la necesidad de adaptar y fortalecer la legislación vigente, lo que da a entender que, para abordar este estudio, se emplea el método exegético, sustentado en fundamentos legales normativos, jurisprudenciales y doctrina pertinente, esto debido a que se busca explorar la interpretación y aplicación de las leyes existentes, identificando vacíos legales y desafíos en su implementación.

Ahora bien, la interrelación entre el marco normativo nacional y las convenciones internacionales permite contextualizar las limitaciones y proponer posibles soluciones desde una perspectiva integral, asimismo, se apunta a reflexionar sobre la necesidad de actualizar y adaptar la legislación para enfrentar eficazmente los delitos en el ciberespacio, considerando el dinamismo y la complejidad de los entornos digitales en la actualidad.

El desarrollo del trabajo investigativo será pionero para crear posteriormente una serie de posibles soluciones ante los ciberdelitos específicos que no se encuentran regulados de manera implícita dentro del territorio ecuatoriano, se podrán crear hipótesis mediante las cuales se fomentar la progresividad de esta legislación, beneficiándose así a los miembros de la sociedad de manera colectiva dado que, al existir una solución ante las problemáticas emergentes de la cibercriminalidad, es posible contar con la posibilidad de proteger colateralmente las actividades realizadas en el ámbito del ciberespacio.

Es necesario tener en cuenta que, el Derecho penal es el conjunto de normas que regulan las conductas delictivas y las sanciones correspondientes, así pues se entiende que se trata de un Derecho positivo, lo que a su vez significa que está establecido por ley escrita; este Derecho se encuentra estrechamente relacionado con el principio de legalidad, el cual establece que nadie puede ser castigado por un delito que no esté previamente tipificado en la ley, esto trata de una

garantía fundamental para los ciudadanos, ya que les permite saber con certeza qué conductas son delictivas y qué sanciones se les aplicarán.

De acuerdo a lo anterior, es posible derivar a la multigarantía como un conjunto de garantías que protegen los derechos de los ciudadanos en el proceso penal, entre estas garantías se encuentran el Derecho a la defensa, el Derecho a un juicio justo y el Derecho a la presunción de inocencia, ahora bien, la garantía penal y criminal es una garantía que se deriva del principio de legalidad, la cual consiste en que la ley penal debe interpretarse de manera restrictiva, de modo que se evite la sanción de conductas que no estén claramente tipificada, lo que trae consigo la necesidad de que el Derecho sea adaptado a las nuevas tecnologías.

Implementar una solución ante las conductas de los tipos penales que entrañan afectaciones colaterales, por ejemplo, para los datos o información personal como una problemática activa para la sociedad en el área del Derecho, el desarrollo es proporcional entre el Derecho y la tecnología como un tema novedoso que permitirá posteriormente llenar un vacío no solo de conocimiento sino también normativo.

Metodología

Se trabajó en el desarrollo de un artículo de reflexión que adoptó un enfoque cualitativo, con la utilización de métodos de deducción con la finalidad de contribuir y complementar las categorías necesarias para una investigación cabal, ordenada y clara, es por ello que, se dió uso del método exegético para analizar críticamente las bases normativas desde un punto de vista jurídico y sociológico.

Los métodos de investigación jurídica se reconocen como herramientas que permitieron a los investigadores jurídicos comprender y analizar este fenómeno, como es el caso del análisis teórico-jurídico, el cual se centra en el estudio de los conceptos, principios y teorías jurídicas,

este método fue útil para comprender el significado y alcance de las normas jurídicas; además, también fue necesario el uso del método histórico-jurídico, el cual se encargó de estudiar la evolución del Derecho a lo largo del tiempo, este método fue útil para comprender el contexto histórico en el que se crearon las normas jurídicas.

Otro método importante fue el de comparación jurídica, la cual se encargó de estudiar las similitudes y diferencias entre las normas de diferentes sistemas, este método fue útil para comprender la diversidad del Derecho, así como también para identificar soluciones jurídicas innovadoras; así mismo, el método exegético-jurídico, logró ayudar con el análisis de los textos legales y fue útil para interpretar el significado de las normas jurídicas.

Ahora bien, en lo que respecta a los métodos utilizados, es importante tener en cuenta que, en el ámbito de la investigación cualitativa se encuentra el método de saturación, el cual funciona como una herramientas esencial para la investigación científica, a más de que permitió a los investigadores organizar, interpretar y comprender los datos recopilados en sus estudios, así pues, se entiende que el método de saturación es un método cualitativo que se utiliza para determinar el punto en el que se han recopilado suficientes datos para alcanzar la saturación, esto significa que se identificaron todos los temas y conceptos relevantes para el estudio.

De este modo, es posible entender que, los métodos de análisis reconocidos y aplicados son importantes para la investigación científica por el motivo dado de que permiten a los investigadores alcanzar conclusiones válidas y confiables, además apoyar con el orden, interpretación, comprensión de la información en el estudio, lo que permite alcanzar conclusiones válidas y confiables.

En este contexto, los enfoques representaron la perspectiva teórica y conceptual desde la cual se aborda el estudio, centrándose en comprender y contextualizar los fenómenos sociales y

legales relacionados con la temática, así pues, se entiende que las técnicas empleadas incluyeron el análisis documental detallado de las normativas pertinentes, la revisión exhaustiva de doctrina especializada, lo que llevó a entender que los instrumentos de investigación se orientan hacia la interpretación y comprensión profunda de las leyes y su aplicación en el ámbito sociocultural, empleando la comparación legislativa como herramienta clave para identificar vacíos legales y desafíos en la regulación.

Del mismo modo se valoró la triangulación de fuentes y la construcción de argumentos desde una perspectiva crítica, fomentando la reflexión y el análisis profundo de las implicaciones sociales y jurídicas de la cibercriminalidad en el contexto ecuatoriano. El artículo científico enfatizó la importancia de considerar múltiples perspectivas y abordajes metodológicos para enriquecer la comprensión de la realidad jurídica y social en el entorno digital, lo que impulsó las propuestas de mejora y adaptación legislativa que responden a los retos emergentes en la era digital.

Fundamentos teóricos

Derecho penal positivo

El concepto de los términos penales se centra en los principios de la regulación de los actos penales y las sanciones significativas, que es una ley positiva establecida por la ley, este concepto se entiende por el acto del individuo y la sanción correspondiente a este. Guamán sobre la multigarantía nos acerca a comprender que se pueden comprender como la protección escrita que avala y justamente protege y garantiza esos derechos tales como el derecho a la defensa, un juicio justo y la presunción de inocencia, estas garantías se derivan de la interpretación restrictiva de la ley penal, adaptándose a los avances tecnológicos (Guamán, Ríos & Yuqui, 2021).

Derecho penal objetivo

El delito tiene dos componentes el objetivo y el subjetivo, el objetivo correspondiendo al valor del tipo y a la antijuricidad, y el subjetivo correspondiendo a valorar la culpabilidad que él lo comprende como la relación psíquica entre el autor y el resultado. En este texto de Valarezo, consta después que es insostenible caracterizar el injusto de un modo objetivo, ya que a nivel típico debe existir determinados elementos subjetivos para que llegue a ser típico (Valarezo, Valarezo & Durán, 2019).

Elementos de la teoría del delito

Para que un delito sea considerado delito informático debe cumplir con los elementos de tener sujeto, qué es la persona que comete el delito, el medio que en el caso de los delitos informáticos pueden ser un ordenador o un dispositivo electrónico, es decir va a ser el instrumento que se utiliza para cometer el delito, y finalmente el otro elemento sería el objeto que se refiere a la acción o conductas que infringen las normas establecidas en la legislación es decir el objeto va a ser el resultado o el propósito de la conducta ilícita ejemplo de ellos puede ser el acoso no autorizado, difusión de malware, suplantación de identidad, entre otros (Saltos, Robalino, & Pazmiño, 2021).

Es posible reconocer como un primer elemento del delito el cual es denominado como la tipicidad, y lo valoran como la conducta o conductas socialmente relevante que infringe un bien jurídico protegido, llevando a la reflexión inmediata de qué si existe la ausencia de algún elemento en el tipo penal, dihoc en otras palabras, lo que en el tema abarca va a significar la anti-tipicidad de la conducta (Tixi, Machado & Bonilla, 2022).

La literatura epistemológica analítica permite articular de una forma más rigurosa las exigencias que satisfacen la culpabilidad como conocimiento de la antijuridicidad de la conducta:

esta oración hace referencia a ciertas formas de creencia que, bajo ciertas condiciones evidenciables, pueden adscribírsele a una persona y cuyo objeto es una determinada forma de comportamiento que tiene la característica de ser antijurídica (Fernández, 2021).

Ahora bien, es necesario contemplar también las características fundamentales de quienes llevan a cabo los delitos informáticos, quienes lo sufren, y qué elementos pueden estar incidiendo en la comisión, denuncia y condena de estos delitos informáticos. Tomando en cuenta entonces, los autores, la disponibilidad de víctimas, es decir cuántas personas hay que puedan ser blanco o presas fáciles para los actores de estos delitos, y por último la ausencia de mecanismos que protejan o que ayuden a controlar la comisión de estos delitos (Mayer, 2018).

Sujetos del delito

Es evidente que entre más se utilice el Cyber espacio, ya sea por trabajo, por estudio o por la agilidad en la realización de trámites que estos nos generan, los cyber delincuentes bus servidores RDP mal configurados para poder ingresar a los sistemas de las personas. Chávez explica cómo funciona el RDP qué significa Protocolo de Escritorio Remoto, y es un estándar técnico desarrollado por Microsoft que permite a los usuarios controlar de forma segura y remota un ordenador de escritorio, y el problema surgiría cuando estos RDP no se encuentran bien configurados y convierten al usuario en vulnerable para ataques de los Cyber delincuentes, para que estos puedan entrar sin permisos robar información oponer software malicioso. Por eso, Chávez nos da una recomendación y es mantener el software actualizado y configurar correctamente los RDP, así como también utilizar contraseñas seguras para una mayor seguridad (Chávez, Malpartida, Villacorta et al., 2021).

En cuanto a las características que poseen las personas que expresamente se dedican a esto, Crespo hace un aporte sobre ello e indica que por lo general estas tienen un avanzado

conocimiento sobre la manipulación de software y además también hace referencia al entorno desde el que las manejan, y este sería salas de máquinas o centros clandestinos con software y hardware altamente sofisticados y avanzados destinados a afines maliciosos e ilegales (Crespo, 2020).

El tema de los sujetos de delitos puede ser simplificado a lo anterior, sin embargo es necesario recalcar la importancia de manejar cientos conceptos derivados el, esto claramente muestra la necesidad de qué se clasifique y se identifique la perspectiva penal al sujeto penalmente responsable del ciberdelito, ya que es evidente la falta de profesionales capaces de actuar ante los delitos informáticos debido a que no existe una buena telemática que rija los sistemas digitales en el país (Gonzales at al., 2019).

Punibilidad

La impunidad es la falta de castigo; no es más que la libertad que se le otorga a un delincuente para logra quedar absuelto de una pena que ha incurrido, por lo tanto, se afirma que la impunidad es la causa más común en su ámbito, generalmente es el accionar que más hiere la sensibilidad colectiva por no castigar a los verdaderos culpables de un hecho delictivo, en algunos casos, recae en personalidades conocidos, que son perseguidos por razones políticas, siempre abusivas y propias de organismos del Estado, donde la libertad ha sido cercenada, la prensa en todas sus modalidades amordazada, los tribunales sesgados y el poder entregado en manos de una minoría sostenida por la coacción, el miedo y la cobardía general (Acosta, Benavides & García, 2020).

Cibercriminalidad, ciberespacio y seguridad ciudadana

La mayoría de los ciudadanos en estos momentos, dependemos en un gran porcentaje de la tecnología, así como también de los procesos informáticos en general, para nuestras

actividades sociales diarias, tales como trámites e incluso procesos económicos diarios, que al estar vinculados directamente con nuestra información personal y por ende con nuestro dinero, abre sin duda un universo nuevo para delinquir, poniendo este escenario en manos de delincuentes (Pons, 2017).

Dicho de otra forma, actualmente es la tecnología una realidad y una nueva forma de desenvolvernos que sin duda será irreversible, es decir que esta nueva forma de comunicarnos y llevar nuestro día se quedará para siempre. Por este motivo es importante analizar los derechos y las leyes en cuanto a la protección del sistema legal para los derechos de los ciudadanos que giran en torno a la tecnología, ya que se ha puesto en evidencia que los modelos punitivos tradicionales no serán suficientes para una nueva era tecnológica (Leyva, 2021).

Es real que el cibercrimen aumentado, y este aumento tiene mucho peso en la pandemia mundial de COVID-19, ya que debido a la condición de quedarse todos en casa, incluso hasta los países o los pueblos más remotos acudieron a la tecnología como un medio primordial innecesario para poder seguir desarrollando sus actividades de estudio, trabajo y de trámites básicos innecesarios diarios de las personas. Por este motivo es necesario protegerse de este ciber crimen, y los sistemas jurídicos deben garantizarnos una protección hacia ello (Linares, 2021).

A pesar de que el cibercrimen sea clasificado como un fenómeno nuevo, el derecho debe adaptarse a este tipo de cambios sociales e innovarse para poder alcanzar un equilibrio entre las nuevas necesidades que la sociedad pueda surgir y con ello, adaptar las normas y penas de manera proporcional según las acciones realizadas, entendiendo con esto como aquellas normas a las que se deben ajustar (Deluca, & Del Carril, 2017).

Que las leyes puedan combatir la cibercriminalidad, y que puedan abarcar los límites geográficos para la imposición de cada sanción según corresponda, es un tema de grande

demanda, ya que en el Cyber espacio no hay límite geográfico para perpetrar los delitos, así que una correcta regulación debería poder permitir que se defina qué acciones son criminales en el mundo digital con leyes que permitan combatir las y también describir con exactitud el tema de los límites geográficos, para poder decidir el ordenamiento jurídico de qué país va a ser tomado para juzgar un caso específico (Mozo, & Ardila, 2022).

Ahora bien, se entiende que es importante que exista un estudio profundo en cuanto a la identificación de los diferentes delitos que se puedan cometer dentro del ciberespacio, ya que actualmente hemos proporcionado nuestra información personal generalmente todo está puesto sobre una base de datos, que puede ser fácilmente manipulada por otros y finalmente tener un uso no debido (Macías, at al., 2022).

Además de tener conocimiento sobre cómo funcionan estos programas elaborados por hackers que pueden llevarnos a ser víctimas de estos delitos tecnológicos, lo más importante sin duda es que exista en el derecho una manera de regular a los actores de esta situación, y sobre todo que a estos se los pueda combatir, ya que en el futuro serán más las personas con conocimientos avanzados de tecnología y que puedan aprovecharlos para delinquir (Ávila, 2023).

Ecuador es un país que en los últimos años ha avanzado muchísimo hacia la era de la tecnología, en conjunto con el mundo Ecuador está avanzando paralelo a esta era tecnológica, teniendo esto grandes beneficios para la educación y para el desarrollo como país, es por ello que la preocupación de la delincuencia cibernética es de gran importancia, ya que con el uso progresivo de las redes sociales los posibles delincuentes también utilizan estas plataformas para cometer sus actos delictivos. Por ello se considera fundamental que Ecuador, así como está avanzando a la era tecnológica, también su ordenamiento jurídico avance paralelo a ello, y así

pueda garantizar la protección de los derechos tales como la de los datos personales y la seguridad de los usuarios en línea (Solano, et al., 2023).

Cabe mencionar que hay una gran diferencia entre la delincuencia tradicional y la delincuencia en Internet, es por ello que resulta imprescindible analizar términos relacionados para poder comprenderla detectarla y perseguir, esto debido a que como lo habíamos mencionado atrás no tiene fronteras y genera un problema geográfico, dificultando a las autoridades la persecución de los delincuentes entre países (López, 2022).

Se puede establecer, que efectivamente el software funciona conforme éste haya sido configurado, y el responsable del mismo es el administrador del sistema, que si bien es cierto no pueda presentar ninguna clase de hackeo a las medidas de seguridad impuestas que presenten alguna intromisión o ataque al mismo, si puede presentar un exceso en la autorización para poder manejar el sistema o subsistema ejecutando una tarea diferente a la que se encuentra detallada en la ley (Santillán, Vinueza & Benavides, 2022).

El fraude informático implica usar la tecnología para obtener dinero ilegalmente, por lo que a menudo se confunde con intentos o la preparación del fraude, aunque estos no sean delitos, es un acto ilegal que se vale de la tecnología para beneficio propio de manera incorrecta, esto implica engañar o aprovecharse de otros a través de medios digitales, buscando ganancias económicas de manera deshonesta y contra la ley (Mayer & Calderón, 2020).

Resulta importante hacer énfasis en lo que se entiende como la vinculación que tienen los datos personales con las nuevas tecnologías, tomando en cuenta que se trata de una realidad que se aplica diariamente se puede tratar con la atención que le corresponde dado que esto involucra un almacenamiento de datos importante, llevando a una interacción de varios sujetos activos, implicando el acceso inadecuado o el acceso no autorizado de datos y suministración de la

información (Garzón & Cuero, 2023).

Citando a Mayer y Vera, el fraude informático se refiere a la manipulación o alteración de datos o programas en sistemas informáticos con el objetivo de causar un perjuicio patrimonial. Este delito puede involucrar la transferencia electrónica de fondos y se ha convertido en un tema relevante debido al impacto económico y la frecuencia con la que ocurre, especialmente en el contexto del comercio electrónico (Mayer & Vera, 2020).

Por otro lado, el sabotaje informático implica la destrucción o inutilización de un sistema de tratamiento de información, por lo general, estas figuras delictivas se encuentran relacionadas con el espionaje informático, que castiga la interceptación, interferencia o acceso indebido a sistemas informáticos. Un ejemplo de un país que contempla esta conducta en su regulación es Chile, en donde la ley contempla estas conductas y establece sanciones para quienes las cometan. Por ello es de suma importancia que las regulaciones legales expresan claramente los alcances y límites de estos delitos para poder abordar adecuadamente la Ciber criminalidad (Mayer & Vera, 2020).

Está demás decir que siempre será necesario y primordial que las personas tengan un mayor conocimiento y mayor capacitación de los nuevos temas sociales, y en este caso siendo la tecnología la protagonista de esta nueva adaptación social, las personas deben tener conocimiento sobre las medidas de seguridad de estas, tales como contraseñas seguras, actualizar el software y tener cuidado con los enlaces y archivos que se abren (Morón, 2021).

Los asuntos sobre protección y defensa en internet se han enfocado en las leyes y reglas que regulan diferentes aspectos en línea, sin embargo, se ha prestado menos atención al grado de independencia que tienen los ejércitos al proteger y defender el ciberespacio, esto implica que se debe considerar cómo las fuerzas militares manejan la seguridad en internet, algo que ha sido

menos analizado en comparación con la regulación y las normativas en este ámbito (Cujabante, Bahamón, Prieto et al., 2020).

La persistencia de una práctica que va en contra de las normas de un grupo social es una señal de que las políticas que se han implementado para evitarla son ineficaces, en otras palabras, si una práctica sigue ocurriendo, a pesar de que existen normas que la prohíben, es porque esas normas no se están aplicando correctamente o no son lo suficientemente estrictas para evitar que esto ocurra, es necesario que las políticas sean efectivas y que se apliquen de manera consistente (Cañete, Adam, Blanco et al., 2023).

La ciberseguridad se enfoca entonces en la protección de la infraestructura computacional y de la información circulante en las redes informáticas, aunque también del diseño de normas, procedimientos, métodos y técnicas que posibiliten seguridad y confiabilidad en los sistemas de información, esto es importante pues los ataques en el ciberespacio afectan no solo en el mundo digital, sino que pueden concretarse en el ámbito físico, por ejemplo, dañando sistemas estructurales de una organización, una nación o una región (Ospina & Sanabria, 2020).

Asimismo, la ciberseguridad juega un papel fundamental para que se puedan proteger los recursos de las personas, entendiéndose como los objetos refugiados al dinero y los datos personales que actualmente se encuentran en una gran base de datos y, justamente la ciberseguridad se trata de un conjunto de prevenciones personales que se pueden tomar para evitar caer en manos de un ciberdelito (Flores, & Mena, 2023).

Es por ello que la ciberseguridad aplicada y promovida desde la categoría nacional puede ayudar en gran parte a prevenir los riesgos que trae consigo la dependencia del ciberespacio, en la que actualmente estamos sumergidos, para de esa forma poder evitar los riesgos que ésta tiene, tales como la pérdida de información confidencial, robo de datos, entre otros aspectos y

categorías relacionadas (Morón, 2021).

Este tipo de tratados, podrían ser de suma importancia para nuestro país, ya que un tratado siempre va a tener un objetivo en común, y en este caso es importante acogerse a un tratado que tenga como objetivo definir qué acciones se consideran delitos en el ámbito cibernético y establecer las leyes necesarias para enfrentar estas conductas. Esto puede significar una medida crucial para abordar y regular los crímenes en línea, logrando instaurar pautas legales que combatan de manera radical la delincuencia digital (Medina, Cárdenas & Mejía, 2021).

Las policías autonómicas en España no tienen un papel importante en la lucha contra el cibercrimen., esto se debe a que, a pesar de que las leyes les otorgan funciones de mantenimiento del orden y lucha contra la criminalidad, en la práctica, la autoría de las actuaciones policiales en este ámbito corresponde a la Policía Nacional y la Guardia Civil, que están mejor dotadas de medios y personal especializado, las policías autonómicas pueden realizar labores de información y físicas por proximidad, pero no tienen la capacidad para investigar y perseguir el cibercrimen de manera efectiva, esto se debe a que el cibercrimen es una forma de delincuencia compleja que requiere conocimientos y recursos especializados (González, & Girao, 2020).

La nueva ley italiana de delitos informáticos incluyó en sus disposiciones a los sistemas informáticos, el software y todo el patrimonio informático, sin embargo, esta reforma fue criticada porque no estableció una sección autónoma para los delitos informáticos dentro de la legislación italiana, para mejorar la lucha contra el cibercrimen en Italia, es necesario que se creen secciones específicas para los delitos informáticos dentro de la legislación italiana, esto permitiría a los agentes de policía y a los jueces tener una formación y una experiencia específica en esta materia, lo que facilita la investigación y el enjuiciamiento de los delitos informáticos

(Fusco, 2020).

El Mando Conjunto de Ciberdefensa es responsable de cuidar las computadoras y redes del Ministerio de Defensa, además, supervisa los Centros de Operaciones de Seguridad, los cuales se encargan de identificar y actuar contra posibles peligros en internet, este equipo protege las tecnologías que utiliza el Ministerio, asegurándose de que estén a salvo de cualquier amenaza digital que pueda afectar su funcionamiento o seguridad (García, & Herrero, 2021).

Tabla 1

Bases normativas

Normativas internacionales contra los ciberdelitos	**Normas nacionales e internacionales relevantes para la lucha contra los ciberdelitos**
Convenio sobre la Ciberdelincuencia de Budapest (*Budapest Convention*)	Normas sobre derechos humanos
Convenio de las Naciones Unidas contra la Corrupción (Convención de Mérida)	Normas sobre seguridad de la información
Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo)	

Nota: Estas normativas, en el contexto ecuatoriano son herramientas fundamentales para prevenir, investigar y sancionar estos delitos, su aplicación efectiva en conjunto con la cooperación internacional y la educación en ciberseguridad, son claves para proteger a las

personas y garantizar un espacio digital seguro.

Tabla 2

Triangulación de normativas nacionales contra los ciberdelitos

Ecuador	
Articulo 66 **Constitución de la República del Ecuador (CRE)**	**Articulo 190** **Código Orgánico Integral Penal (COIP)**
Busca salvaguardar derechos en general de los ciudadanos de manera individual y colectiva, esto incluye la protección frente a ciberdelitos, con lo cual establece principios legales para proteger la privacidad, seguridad y libertad en el entorno digital, garantizando la justicia electrónica.	Tipifica como delitos una serie de conductas relacionadas con la informática, como el acceso no autorizado a sistemas informáticos, el robo de datos, el ciberacoso, la pornografía infantil en línea, etc.
Colombia	
Código Penal	**Ley 1273 de 2009**
Tipifica como delitos una serie de conductas relacionadas con la informática, como el acceso no autorizado a sistemas informáticos,	Establece normas para la protección de los datos personales en el contexto digital.

el robo de datos, el ciberacoso, la pornografía infantil en línea, etc.

España

Código Penal	**Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**	**Tratado de la unión europea**
Tipifica como delitos una serie de conductas relacionadas con la informática, como el acceso no autorizado a sistemas informáticos, el robo de datos, el ciberacoso, la pornografía infantil en línea, etc.	Establece normas para la protección de los datos personales en el contexto digital.	Establece directrices para proteger la privacidad y seguridad digital, promoviendo la cooperación entre países miembros para abordar amenazas cibernéticas de manera efectiva.

Nota: Ecuador, Colombia y España comparten el objetivo de combatir los ciberdelitos con sus normativas y presentan diferencias en cuanto a la tipificación, penas y mecanismos de cooperación. En Ecuador, la Ley de Delitos informáticos se enfoca en los tradicionales, mientras

que en Colombia y España se incluyen delitos más recientes como la ciberviolencia y el robo de datos; en cuanto a las penas, España establece las más severas, seguida por Colombia y Ecuador, ahora bien, la cooperación es un punto fuerte en las tres legislaciones, aunque con diferentes niveles de desarrollo.

Análisis de resultados y discusión

Tras un análisis doctrinal y normativa en el tema de la cibercriminalidad, se reveló una insuficiencia para salvaguardar la seguridad ciudadana, este hallazgo destaca las limitaciones legales frente a este fenómeno lo cual, mediante una revisión de escritos de juristas destacados, se ha revelado un enfoque de necesidad de reformas legales para fortalecer la protección ante los delitos cibernéticos, de este modo, se ha evidenciado que, si bien la legislación ecuatoriana ha realizado avances en la tipificación de delitos informáticos, aún existen limitaciones significativas.

Las limitantes encontradas se sitúan principalmente en la desactualización o tipificaciones incompletas con lo cual se han planteado posibles medidas de reparación en términos teóricos tras el estudio, con la proposición de una reforma integral a la normativa penal ecuatoriana, que incluya actualización de las tipificaciones penales de manera que se incorporen nuevos tipos penales que respondan a las últimas tendencias de la ciberdelincuencia o bien la posibilidad de redactar los tipos penales de forma más precisa y abarcativa.

De este modo se pudo comprender que, la reforma a la normativa penal ecuatoriana es indispensable para garantizar una adecuada protección de la seguridad ciudadana frente acciones que promueven o ejecutan la cibercriminalidad, la investigación y el análisis doctrinario han demostrado la necesidad de actualizar y fortalecer la legislación, así como de fortalecer las capacidades institucionales.

Ahora bien, el presente estudio tuvo como objetivo general analizar la competencia de la normativa ecuatoriana para el tratamiento de la cibercriminalidad, con lo cual se pudo determinar que el Código Orgánico Integral Penal (COIP) y otras leyes ecuatorianas no son del todo suficientes para combatir eficazmente los delitos informáticos y proteger los bienes jurídicos de los ciudadanos en el ámbito digital.

En la misma línea investigativa también se pudieron estudiar las figuras delictivas previstas en el COIP que tienen como escenario el ciberespacio y con esto se entendió en detalle cada tipo penal, su tipicidad, elementos y las penas previstas; con la definición de las ciberamenazas que ponen en riesgo bienes jurídicos protegidos por el ordenamiento jurídico penal, se lograron determinar las principales amenazas que la cibercriminalidad que se interponen como tal para la seguridad de los ciudadanos y el Estado ecuatoriano; y, con la finalidad de determinar las actividades delictivas que corresponden a la cibercriminalidad como problema de seguridad ciudadana se logró determinar el alto nivel de impacto de la cibercriminalidad en la sociedad ecuatoriana, idea con la cual se pudieron proponer de manera teórica o reflexiva medidas para combatirla de manera efectiva.

Con el análisis de las limitaciones de la legislación penal ecuatoriana frente a la cibercriminalidad es posible identificar de manera masiva la creciente amenaza que representa la ciberdelincuencia se pudo identificar la falta de actualización y adaptación de las leyes a los avances tecnológicos como un factor limitante para la protección efectiva o bien ciberseguridad y la persecución de ciberdelitos.

Finalmente, el análisis de las limitaciones de la legislación penal ecuatoriana frente a la cibercriminalidad revela diversas facetas, en primer lugar, la competencia de la normativa penal nacional se ve desafiada por la naturaleza transnacional de los delitos cibernéticos, ahora, aunque

el COIP tipifica algunos delitos, como el acceso no autorizado a sistemas informáticos, las principales ciberamenazas, como el phishing o el ransomware, no están abordadas exhaustivamente, esto genera un vacío legal que dificulta la persecución efectiva de actividades delictivas en el ámbito digital, afectando la seguridad ciudadana.

Conclusiones

Tras el análisis y recopilación de información previa, se pudieron desarrollar las siguientes ideas como conclusiones de la investigación realizada en base al tema de las limitaciones de la legislación penal ecuatoriana ante la cibercriminalidad.

En primer lugar, se entiende que si bien el Código Orgánico Integral Penal (COIP) ecuatoriano tipifica algunos delitos informáticos, su alcance se ve limitado por la rápida evolución de la cibercriminalidad, de este modo, la legislación penal no siempre logra adaptarse a la velocidad con la que surgen nuevas modalidades delictivas en el ámbito digital; es por ello que, el COIP tipifica delitos como el acceso no consentido a un sistema informático, la interceptación de datos informáticos y la estafa informática, sin embargo, esta tipificación no es exhaustiva y deja fuera muchas otras formas de cibercriminalidad, como el ciberacoso, la pornografía infantil y el robo de identidad.

En cuanto al análisis sobre las ciberamenazas y actividades delictivas, se puede concluir que las principales ciberamenazas en Ecuador incluyen el *malware*, el *phishing*, el *ransomware* y los ataques a la infraestructura crítica, de este modo se entiende que las actividades delictivas asociadas a la cibercriminalidad son variadas, desde el robo de información personal y financiera hasta la propagación de desinformación y la manipulación de procesos electorales.

Finalmente, tras la identificación de los elementos, causas y efectos de estas actividades desarrolladas en un escenario tecnológico, es posible determinar las normativas y sanciones

cumplen una función básica para la protección y preservación de la seguridad ciudadana, principalmente porque estas actividades ilícitas en el medio cibernético representan una grave amenaza para la seguridad ciudadana, ya que puede afectar a la privacidad, la economía y la estabilidad social. Por ello se concluye añadiendo la idea de fortalecer la legislación penal ecuatoriana para que responda eficazmente a las nuevas formas de delincuencia del mundo digital.

Referencias

Acosta, M., Benavides, M. & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89), 351-368. https://dialnet.unirioja.es/servlet/articulo?codigo=8890269

Ávila, F. (2023). *Ransomware*, una amenaza latente en Latinoamérica. *InterSedes*, 24(49), 92-119. https://www.scielo.sa.cr/scielo.php?pid=S2215-24582023000100092&script=sci_abstract&tlng=es

Cañete, P.; Adam, C.; Blanco, O.; Garidel, C. & Becerra, C. (2023). Fechorías de nuevo cuño: neologismos de la delincuencia. *Lengua y Sociedad*, 22(1), 421-447. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2413-26592023000100020

Chávez, J.; Malpartida, D.; Villacorta, A. & Orellano, J. (2021). La influencia de la automatización inteligente en la detección del cibercrimen financiero. *Boletín de Coyuntura*, (31), 26 – 33. https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/1462

Crespo, L. (2020). La acción nuclear del delito informático en la novísima reforma parcial del código orgánico integral penal. *Revista internacional*, 9(1), 17-27. https://ojs.docentes20.com/index.php/revista-docentes20/article/view/89

Cujabante, X.; Bahamón, M.; Prieto, J. & Quiroga, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista colombiana de estudios militares y estratégicos*, 18(30), 357-377. https://revistacientificaesmic.com/index.php/esmic/article/view/588

Deluca, S. & del Carril, E. (2017). Cooperación internacional en materia penal en el Mercosur: el cibercrimen. *Revista de la Secretaría del Tribunal Permanente de Revisión*, (10), 13-28. http://scielo.iics.una.py/scielo.php?script=sci_abstract&pid=S2304-78872017001000013&lng=en&nrm=iso&tlng=es

Fernández, J. (2021). Razonabilidad como exigencia para el conocimiento de la antijuricidad: el caso de la persona inimputable. *Ius et Praxis*, 27(2), 55-71. https://www.scielo.cl/scielo.php?pid=S0718-00122021000200055&script=sci_abstract&tlng=es

Flores, S. & Mena, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. *Digital Publisher CEIT*, 8(4), 159-173. https://www.593dp.com/index.php/593_Digital_Publisher/article/view/1652/1649

Fusco, L. (2020). Los delitos informáticos en el Código Penal Italiano. Derecho global. *Estudios sobre Derecho y justicia*, 5(14), 127-149. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362020000100105

García, J. & Herrero, L. (2021). La ciberdefensa en los sistemas de información sanitarios militares. Sanidad Militar. *Sanidad Militar*, 76(3), 140-142. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140

Garzón, J. & Cuero, K. (2023). Una mirada a la cibercriminalidad en Colombia y su asimilación

con los delitos de impacto. *Revista Criminalidad*, 64(3), 203-225. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082022000300203

Gonzales, J., Hidalgo, C., Arce, J. & Ordoñez, P. (2019). Análisis y revisión sobre delitos informáticos en el Ecuador. Conference Proceedings *UTMACH*, 3(1), 194-205. https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/367

González, A. & Girao, F. (2020). Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español. *Revista relaciones internacionales*, 29(58), 241-256. http://www.scielo.org.ar/scielo.php?pid=S2314-27662020000100241&script=sci_abstract

Guamán, K., Ríos, V. & Yuqui, C. (2021). La teoría del delito: fundamentos filosóficos. *Dilemas contemporáneos: educación, política y valores*, (18), 1-22. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/2697

Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris Et Investigatio*, (1), 29-48. https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/download/18373/16528/68634

Linares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *Revista de internet, Derecho y política*, (32), 1-17. https://raco.cat/index.php/IDP/article/view/n32-miro

López, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista chilena de Derecho y tecnología*, 11(1), 121-147. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100121

Macías, R. Boné, M., Quiñonez, F., Mendoza, J., Estupiñán, G. & Rodríguez, J. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. *Sapienza*, 3(2), 231-243. https://www.researchgate.net/publication/360554562_Casos_frecuentes_penalizacion_y_prevencion_de_los_delitos_informaticos_en_el_Ecuador_una_breve_revision_sistematica

Mayer, L. & Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista chilena de Derecho y tecnología*, 9(1), 151-184. https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0719-25842020000100151&lng=en&nrm=iso

Mayer, L. & Vera, J. (2020). El delito de espionaje informático: Concepto y delimitación. *Revista chilena de Derecho y tecnología*, 9(2), 221-257. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200221

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, 24(1), 159-206. https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext

Medina, J.; Cárdenas, C. & Mejía, M. (2021). Análisis del phishing y la ley de delitos informáticos en Colombia. *Cuaderno de investigaciones semilleros andina*, (14), 75-80. https://revia.areandina.edu.co/index.php/vbn/article/view/1948/1870

Morón, I. (2021). Riesgos que genera el ciberespacio para los derechos fundamentales. *Revista Penal México*, (18), 185-200. https://dialnet.unirioja.es/servlet/articulo?codigo=7749169

Mozo, O. & Ardila, J. (2022). El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia. *Revista perspectivas en inteligencia*,

14(23), 63-95. https://revistascedoc.com/index.php/pei/article/view/333/543

Ospina, M. & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2), 199-217. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO *Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992017000200080

Saltos, M.; Robalino, J. & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, 17(78), 343-351. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

Santillán, A., Vinueza, N. & Benavides, C. (2022). Derecho, informática y corrupción. Un enfoque a la realidad ecuatoriana. *Dilemas contemporáneos: educación, política y valores*, 9(1), 1-26. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-78902021000800106

Solano, G., Cedeño, L., Quintero, N. & Eras, S. (2023). Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador. *Polo del conocimiento*, 8(5), 1137-1153, https://mail.polodelconocimiento.com/ojs/index.php/es/article/download/5630/13965

Tixi, D., Machado, M. & Bonilla, C. (2022). El juicio de tipicidad y su importancia jurídica en sentencias de carácter penal en el Ecuador. *Dilemas contemporáneos: educación, política y valores*, 9(1), 1-18. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-

78902021000800095

Valarezo, E., Valarezo, R. & Durán, A. (2019). Algunas consideraciones sobre la tipicidad en la teoría del delito. *Revista universidad y sociedad*, 11(1), 331-338.