

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

[DOI 10.35381/cm.v11i4.2061](https://doi.org/10.35381/cm.v11i4.2061)

Evolución del ciberdelito en contexto del ciberespacio: Análisis jurídico y tecnológico del fenómeno delictivo digital

The evolution of cybercrime in the context of cyberspace: Legal and technological analysis of the phenomenon of digital crime

Ariana Belén Mora-Troya
arianabmt16@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Babahoyo, Los Ríos
Ecuador
<https://orcid.org/0000-0002-3051-290X>

Ignacio Fernando Barcos-Arias
ub.ignaciobarcos@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Babahoyo, Los Ríos
Ecuador
<http://orcid.org/0000-0002-9493-7931>

Josselyn Brigitte Vilela-Verdezoto
ub.josselynvv41@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Babahoyo, Los Ríos
Ecuador
<http://orcid.org/0009-0005-2557-7150>

Recibido: 20 de agosto 2025
Revisado: 10 de octubre 2025
Aprobado: 15 de noviembre 2025
Publicado: 01 de diciembre 2025

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

RESUMEN

El objetivo de la presente investigación fue analizar la evolución del ciberdelito en contexto del ciberespacio jurídico y tecnológico del fenómeno delictivo digital. Metodológicamente el diseño de la investigación fue de diseño no experimental de nivel descriptivo para analizar la evolución del ciberdelito en el contexto del ciberespacio. Los resultados indicaron que la ciberdelincuencia es una amenaza silenciosa de rápida expansión y generadora de daños de gran impacto. Esta realidad exige la armonización de normas jurídicas entre los países de la región Iberoamericana, lo mismo que la actualización y capacitación constante en la materia, incluyendo aspectos importantes para la detección temprana de las redes organizadas de cibercrimen o individuos actuando en solitario. En conclusión, solo a través de un esfuerzo conjunto será posible mitigar los riesgos y garantizar un ciberespacio más seguro para todos.

Descriptor: Cibercrimen; crimen informático; tecnología; delito informático; protección de datos. (Tesauro UNESCO).

ABSTRACT

The objective of this research was to analyze the evolution of cybercrime in the context of the legal and technological cyberspace of the digital crime phenomenon. Methodologically, the research design was non-experimental and descriptive in order to analyze the evolution of cybercrime in the context of cyberspace. The results indicated that cybercrime is a rapidly expanding silent threat that causes significant damage. This reality requires the harmonization of legal norms among countries in the Ibero-American region, as well as constant updating and training in the field, including important aspects for the early detection of organized cybercrime networks or individuals acting alone. In conclusion, only through a joint effort will it be possible to mitigate risks and ensure a safer cyberspace for all.

Descriptors: Cybercrime; computer crime; technology; computer crime; data protection. (UNESCO Thesaurus).

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

INTRODUCCIÓN

El ciberespacio, configurado como un entorno comunicativo e interactivo paralelo al mundo físico, ha transformado drásticamente las dinámicas de interacción humana a nivel social, económico, político y personal. Este fenómeno ha redefinido las fronteras tradicionales de la comunicación, el comercio y las relaciones interpersonales, generando nuevas oportunidades y desafíos inéditos. Uno de los cambios más disruptivos se ha dado en el ámbito del comportamiento delictivo, donde Internet ha desafiado las nociones convencionales sobre la jurisdicción y la aplicación de la ley. Hoy en día, los delincuentes pueden operar sin necesidad de estar físicamente presentes en el lugar donde se comete el delito, complicando la acción judicial y las respuestas gubernamentales a los crímenes cibernéticos (Maruzito Mecías, 2024).

El ciberdelito ha emergido como una de las formas más sofisticadas de crimen transnacional. Lo que caracteriza a este tipo de delitos es su capacidad para trascender las fronteras físicas y jurisdiccionales, dando lugar a una nueva clase de criminales globales. A diferencia de los delitos tradicionales, donde los actores suelen estar confinados a un territorio específico, los delincuentes cibernéticos pueden operar desde cualquier parte del mundo y cometer delitos en otras regiones, ocultándose detrás de complejas capas de anonimato proporcionadas por la tecnología. Esto les permite no solo perpetrar actos delictivos a gran escala, sino también lavar dinero y realizar transacciones ilegales sin dejar rastro (Beltran López, 2024; Porras, 2023).

El ciberdelito se ha convertido en una manifestación compleja de crimen organizado, en la que los criminales operan dentro de estructuras organizativas que facilitan la realización de actos ilícitos como el robo de datos, el fraude financiero, el ciberterrorismo y la explotación infantil en línea. La particularidad de estos crímenes radica en su carácter descentralizado, permitiendo a los delincuentes colaborar a nivel global y, en muchos casos, operar desde lugares remotos. Este fenómeno plantea un desafío único para las autoridades de seguridad, que deben coordinar

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

sus esfuerzos a nivel internacional para enfrentar actividades delictivas que no reconocen fronteras (Wall, 2023).

El avance de las tecnologías de cifrado y las criptomonedas ha proporcionado a los ciberdelincuentes herramientas eficaces para ocultar sus identidades y realizar transacciones ilícitas sin dejar huella. El uso de sistemas de cifrado avanzado garantiza que los delincuentes puedan operar con un nivel de anonimato casi completo, dificultando la identificación de los responsables de los delitos. Además, el auge de las monedas digitales como Bitcoin ha permitido a los criminales realizar pagos transfronterizos de manera rápida y sin intervención de las autoridades financieras, facilitando el crecimiento de un mercado negro global en línea (Intriago Franco Abogados, 2023).

Entre los crímenes facilitados por estas tecnologías se incluyen actividades como el robo de identidad, el fraude bancario, la venta de datos personales y financieros, la distribución de material pornográfico infantil y el secuestro de datos mediante ransomware. Los delincuentes cibernéticos también han aprovechado la infraestructura digital para establecer mercados oscuros donde se intercambian servicios ilegales, como el tráfico de armas, drogas y otros bienes ilícitos, reforzando la naturaleza transnacional de este fenómeno.

Además de los crímenes financieros y personales, los ciberdelitos han afectado gravemente a las instituciones supranacionales y han alterado el orden político global. Los ataques cibernéticos con fines ideológicos o políticos, como el hacktivismo y el ciberterrorismo, han sido utilizados por actores estatales y no estatales para desestabilizar gobiernos, interferir en procesos electorales o difundir propaganda. Estos actos buscan causar daño a las infraestructuras críticas de un país y tienen un fuerte componente simbólico, aprovechando la conectividad global del ciberespacio para llegar a una audiencia masiva (ONU, 2023).

Los ataques de denegación de servicio (DDoS), las infecciones de malware y otros tipos de intrusiones cibernéticas pueden paralizar instituciones gubernamentales y empresas privadas durante horas o incluso días, con consecuencias devastadoras

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

para la estabilidad económica y política. A nivel global, los gobiernos y las organizaciones internacionales han comenzado a reconocer la necesidad de una respuesta colectiva ante la creciente amenaza del ciberdelito, pero la naturaleza descentralizada y anónima de Internet hace que la cooperación internacional sea compleja y, en muchos casos, ineficaz (ONU, 2023).

El impacto económico del ciberdelito es otro de los aspectos más alarmantes de este fenómeno. Los costos asociados con los ataques cibernéticos son enormes y afectan a empresas de todos los tamaños, desde pequeños startups hasta gigantes corporativos. Entre las pérdidas más significativas se incluyen la corrupción de datos, el robo de fondos, la propiedad intelectual y los datos personales y financieros. Además, la interrupción de las operaciones empresariales tras un ciberataque puede resultar en pérdidas millonarias, sin contar el daño reputacional que sufren las organizaciones afectadas, lo que puede llevar incluso a la quiebra de algunas de ellas (García, 2016).

Según un informe del Banco Interamericano de Desarrollo (BID), se estima que los costos globales derivados de los delitos cibernéticos alcanzarán los seis billones de dólares para el año 2021. Este monto es equivalente al Producto Interno Bruto (PIB) de la tercera economía más grande del mundo, subrayando la magnitud de la amenaza económica que representa el ciberdelito a nivel global. Las empresas deben invertir grandes sumas de dinero en protección cibernética, pero incluso con estas medidas de prevención, los ciberdelincuentes siguen siendo una amenaza constante, planteando preguntas sobre la capacidad de las organizaciones para defenderse eficazmente frente a un adversario tan sofisticado (Banco Interamericano de Desarrollo, 2020).

Dada la creciente magnitud del ciberdelito, las respuestas internacionales se han vuelto más urgentes y coordinadas. En los últimos años, diversas organizaciones y foros internacionales han empezado a desarrollar estrategias para combatir los crímenes cibernéticos, como el Convenio de Budapest sobre Ciberdelinc: El objetivo de este estudio fue analizar la evolución del ciberdelito en el contexto del crecimiento

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

del ciberespacio, identificando los factores que han impulsado su expansión y evaluando las estrategias más efectivas para su prevención.

MÉTODO

La metodología empleada está fundamentada en un enfoque mixto, ya que se utilizó para comprender la relación entre el desarrollo del ciberespacio y la evolución del ciberdelito. Se llevó a cabo un análisis exhaustivo de la normativa legal nacional e internacional, doctrinas especializadas, jurisprudencia relevante y casos emblemáticos relacionados con la temática. Para lograr el objetivo de este trabajo investigativo, se aplicaron encuestas a la ciudadanía con el propósito de conocer su percepción sobre los ciberdelitos más comunes, su evolución y el impacto que tienen en la sociedad.

Asimismo, se realizó un estudio de casos relevantes sobre delitos cibernéticos, analizando patrones y tendencias en la actividad delictiva dentro del ciberespacio. La combinación de estas técnicas permitió obtener una visión integral sobre el fenómeno y sus implicaciones legales y sociales. El diseño de la investigación fue diseño no experimental de nivel descriptivo para analizar la evolución del ciberdelito en el contexto del ciberespacio. Se busca comprender los factores que han influido en el aumento de los delitos cibernéticos y su impacto en la sociedad.

RESULTADOS

Los resultados de las encuestas reflejan una creciente preocupación por la seguridad en el ciberespacio, con un 95% de los encuestados reconociendo que la digitalización ha aumentado los riesgos de ciberdelitos. A pesar de que la mayoría de los participantes considera que el ciberespacio ha transformado la forma en que interactúan y trabajan, existe una clara brecha en el conocimiento sobre la prevención de delitos digitales. Solo el 30% de los encuestados se siente completamente informado sobre los ciberdelitos, lo que indica que muchas personas pueden ser vulnerables a ataques cibernéticos sin ser plenamente conscientes de

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

los riesgos. Además, el hecho de que casi la mitad de los encuestados haya sido víctima de algún tipo de ciberdelito resalta la urgencia de fortalecer las estrategias de protección y concienciación en seguridad digital.

Por otro lado, el 68% de los encuestados considera que la falta de educación en ciberseguridad es uno de los principales factores que contribuyen al aumento de los ciberdelitos. Esta percepción sugiere que la implementación de programas educativos sobre seguridad digital podría ser una herramienta clave para reducir la incidencia de delitos en línea. Sin embargo, aunque el 50% de los participantes afirma utilizar contraseñas seguras y diferentes para cada cuenta, todavía hay un porcentaje considerable que no sigue buenas prácticas de seguridad. Esto pone en evidencia la necesidad de reforzar la educación sobre el manejo seguro de datos personales y la prevención de ataques cibernéticos, promoviendo el uso de herramientas de protección y fomentando una mayor responsabilidad digital en los usuarios.

La mayoría de los encuestados reconoce que la evolución del ciberespacio ha cambiado significativamente la forma en que vivimos y trabajamos. Solo un pequeño porcentaje no está de acuerdo con esta afirmación, lo que sugiere que hay un consenso general sobre la influencia del ciberespacio en la sociedad moderna. Existe una fuerte percepción de que el crecimiento del ciberespacio ha incrementado los riesgos de seguridad, con un 95% de los encuestados que están de acuerdo en algún nivel. Esto refuerza la idea de que la seguridad cibernética es una preocupación creciente entre los usuarios.

Aunque la mayoría de los encuestados tiene cierto nivel de conocimiento sobre ciberdelitos, solo 30% se siente completamente seguro en este tema. Esto indica una posible necesidad de mayor educación y concienciación sobre los distintos tipos de ciberdelitos y sus impactos. Casi la mitad de los encuestados ha sido víctima de un ciberdelito, lo que subraya la prevalencia de estas amenazas. Esta cifra es significativa y resalta la necesidad de implementar más medidas de seguridad para proteger a los usuarios.

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

La gran mayoría de los encuestados considera que la falta de educación en ciberseguridad es un factor clave en el aumento de los ciberdelitos. Esto sugiere que programas de concienciación y formación podrían ser una solución efectiva para reducir estos incidentes. Aunque la mitad de los encuestados usa contraseñas seguras, aún hay un 25% que no sigue buenas prácticas en este aspecto. Esto indica que todavía hay margen para mejorar la concienciación sobre la seguridad en línea.

DISCUSIÓN

El ciberespacio, en su configuración como un entorno comunicativo e interactivo paralelo al mundo físico, ha transformado de manera drástica las dinámicas de interacción humana, tanto a nivel social como económico, político y personal. Este fenómeno ha redefinido las fronteras tradicionales de la comunicación, el comercio y las relaciones interpersonales, generando nuevas oportunidades, pero también desafíos inéditos.

Hay delitos relacionados con el uso del ciberespacio que parecen no tener control y, por el contrario, según el Internet Crime Complaint Center de la Oficina de Investigaciones Federales, este siglo documenta un aumento de las distintas formas de ciberdelincuencia, con más de 2000 denuncias recibidas diariamente y pérdidas financieras que superan los 4200 millones de dólares al año en ataques de ciberseguridad en el continente americano, y un aumento del 1885% en los ataques dirigidos a la inutilización y los datos de las víctimas.

El ciberdelito ha emergido como una de las formas más sofisticadas de crimen transnacional. Lo que caracteriza a este tipo de delitos es su capacidad para trascender las fronteras físicas y jurisdiccionales, lo que ha dado lugar a la aparición de una nueva clase de criminales globales. La ciberdelincuencia es una amenaza silenciosa de rápida expansión y generadora de daños de gran impacto.

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

CONCLUSIONES

El avance del ciberespacio ha transformado significativamente la sociedad, generando oportunidades, pero también nuevos riesgos en el ámbito del delito cibernético. La evolución del ciberdelito ha demostrado ser un desafío creciente para los sistemas legales y de seguridad, ya que los criminales aprovechan la tecnología para operar más allá de las fronteras físicas y dificultar la acción judicial.

Los resultados de la investigación reflejan una creciente preocupación por la seguridad digital y evidencian que, aunque la población reconoce los riesgos asociados al uso de la tecnología, aún existe una falta de conocimiento y preparación para prevenir estos delitos. La falta de educación en ciberseguridad, sumada a la rápida evolución de las técnicas delictivas, ha contribuido al aumento de estos crímenes, afectando tanto a individuos como a instituciones y empresas.

Es fundamental que los gobiernos, las empresas y la sociedad en general adopten estrategias efectivas para combatir el ciberdelito tal como está establecido en la Constitución Nacional de Ecuador y en Código Orgánico Procesal Penal (Asamblea Nacional Constituyente de Ecuador, 2008; Asamblea Nacional de Ecuador, 2014). La implementación de regulaciones más estrictas, la cooperación internacional, el fortalecimiento de las medidas de ciberseguridad y la educación continua son claves para reducir la vulnerabilidad en el entorno digital. Solo a través de un esfuerzo conjunto será posible mitigar los riesgos y garantizar un ciberespacio más seguro para todos.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A todos los factores sociales que influyeron en el desarrollo de esta investigación.

Ariana Belén Mora-Troya; Ignacio Fernando Barcos-Arias; Josselyn Brigitte Vilela-Verdezoto

REFERENCIAS CONSULTADAS

- Asamblea Nacional Constituyente del Ecuador (2008). Constitución De La Republica Del Ecuador 2008. *Registro Oficial 449 de 20-oct-2008*, Quito, Ecuador. <https://n9.cl/hd0g>
- Asamblea Nacional de Ecuador. (2014). Código Orgánico Integral Penal, Quito: Lexis. <https://n9.cl/s1o44>
- Bazurto Mecías, C. J., Jurado Cabello, Y. K., Sifa Mueses, L. M., & Reinoso Paredes, A. G. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica*, 7(Especial 5), 594–612. <https://n9.cl/108oe>
- Beltrán López, P., Gil Pérez, M., & Nespoli, P. (2024). Cyber Deception: State of the art, trends and open challenges. arXiv preprint arXiv:2409.07194. <https://n9.cl/pwabb>
- Banco Interamericano de Desarrollo (BID). (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. <https://n9.cl/un3jxk>
- García, S. B. (2016). Impacto Económico de la Ciberdelincuencia en América Latina. *Ciberprisma – Alianza por la Ciberseguridad*. <https://n9.cl/6m57p7>
- Intriago Franco Abogados. (2023). Ciberdelitos en Ecuador. <https://n9.cl/ks7pi>
- Organización de las Naciones Unidas (ONU). (2023). El costo del cibercrimen a nivel global. <https://n9.cl/hyhfg>
- Porras Montufar, R. X., Herrera Zapata, L. M., & Ortiz Laverde, S. M. (2023). Análisis de las actividades ciberdelictivas desarrolladas en el Ecuador, durante el período 2020-2021. Universidad Externado de Colombia. <https://n9.cl/1i8b0>
- Wall, D. S. (2020). Cybercrime: The transformation of crime in the information Age, (2nd ed.). <https://n9.cl/f7o0t>