Revista de Estudios Generales (REG).
ISSN: 3073-1259Vol.4 (N°.4). enero - marzo 2026
DOI:10.70577/reg.v4i4.445

REG
Revista Multidisciplinar
ISSN: 3073-1259

Delitos informáticos en la era digital: retos y desafíos actuales

Cybercrimes in the digital age: current challenges and opportunities

Verónica Teresa Veloz Segura
Universidad Estatal De Bolívar
vveloz@ueb.edu.ec
https://orcid.org/0000-0002-1440-0115
Ecuador

Elizabeth Alexandra Veloz Segura
Universidad Estatal De Bolívar
eveloz@ueb.edu.ec
https://orcid.org/0000-0003-4562-7619
Ecuador

Javier Alonso Veloz Segura
Universidad Estatal De Bolívar
jveloz@ueb.edu.ec
https://orcid.org/0009-0009-0396-2487
Ecuador

Formato de citación APA
Veloz, V., Veloz, E. & Veloz, J. (2026). Delitos informáticos en la era digital: retos y desafíos actuales. Revista REG, Vol. 5 (N°. 1), p. 1 - 13.

CIENCIA INTERACTIVA
Vol. 5 (N°. 1). Enero – marzo 2026.
ISSN: 3073-1259
Fecha de recepción: 26 -11-2025
Fecha de aceptación :07-01-2026
Fecha de publicación:31-03-2026

RESUMEN

La acelerada transformación digital ha generado nuevas oportunidades de desarrollo social, económico y jurídico; paralelamente, se ha evidenciado un incremento sostenido de los delitos informáticos, los cuales afectan la seguridad de la información, la privacidad de los datos y la confianza en los sistemas digitales. El presente artículo tiene como objetivo analizar, a través de una revisión sistemática de la literatura científica, los principales tipos de delitos informáticos, sus tendencias recientes y los retos que enfrentan los Estados y las organizaciones en su prevención y control. La metodología empleada se fundamenta en el protocolo PRISMA, mediante la selección de artículos científicos publicados entre 2019 y 2025 en bases de datos académicas reconocidas. Los resultados evidencian un crecimiento sostenido de delitos como el acceso no autorizado, el phishing, el ransomware y el fraude digital, así como limitaciones en los marcos normativos y en las capacidades técnicas institucionales. Se concluye que es indispensable fortalecer la cooperación internacional, la actualización normativa y la educación digital como estrategias clave para enfrentar los desafíos actuales de los delitos informáticos.

PALABRAS CLAVE: delitos informáticos, ciberseguridad, era digital, fraude digital, PRISMA.

ABSTRACT

The rapid digital transformation has generated new opportunities for social and economic development; however, it has also led to an increase in cybercrime, which poses a significant threat to information security, privacy, and trust in digital systems. This article aims to analyze, through a systematic review of the scientific literature, the main types of cybercrime, their recent trends, and the challenges faced by states and organizations in their prevention and control. The methodology employed is based on the PRISMA protocol, using scientific articles published between 2019 and 2025 in recognized academic databases. The results show a sustained increase in crimes such as unauthorized access, phishing, ransomware, and digital fraud, as well as limitations in regulatory frameworks and institutional technical capacities. It is concluded that strengthening international cooperation, updating regulations, and promoting digital education are key strategies for addressing the current challenges of cybercrime.

KEYWORDS: cybercrime, cybersecurity, digital age, digital fraud, PRISMA.

REG Revista Multidisciplinar
ISSN: 3073-1259

INTRODUCCIÓN

La acelerada expansión de las tecnologías digitales ha transformado de manera profunda las dinámicas sociales, económicas y comunicacionales a nivel global. La denominada era digital ha generado nuevas formas de interacción, producción y gestión de la información; sin embargo, también ha propiciado escenarios propensos al surgimiento y fortalecimiento de conductas delictivas en el ciberespacio (Castells, 2019). En este contexto, los delitos informáticos se consolidan como una de las principales amenazas para la seguridad digital, la confianza ciudadana y la estabilidad institucional.

Los delitos informáticos en la era digital constituyen una problemática creciente asociada al uso intensivo de las tecnologías de la información y la comunicación. La expansión de internet, los sistemas digitales y las plataformas en línea ha generado nuevos escenarios de riesgo que facilitan la comisión de conductas ilícitas, afectando tanto a individuos como a organizaciones. Sin embargo, los principales retos y desafíos actuales se relacionan con la constante evolución de las modalidades delictivas, la dificultad para su detección oportuna y la necesidad de fortalecer las estrategias de prevención, concienciación y protección de la información en los entornos digitales.

Desde una perspectiva sociotécnica, el delito informático no puede comprenderse únicamente como una infracción de carácter tecnológico, sino como un fenómeno social complejo que surge de la interacción entre el comportamiento humano, la innovación tecnológica y las limitaciones de los marcos normativos vigentes (Wall, 2020). Esta interacción ha permitido la aparición de múltiples modalidades delictivas que aprovechan las vulnerabilidades de los sistemas digitales y la escasa alfabetización digital de los usuarios (Holt & Bossler, 2020).

La globalización del cibercrimen representa uno de los principales retos para los Estados, debido a su carácter transnacional y a la dificultad de identificar, perseguir y sancionar a los responsables. Las acciones delictivas pueden originarse en una jurisdicción, afectar a víctimas en otra y utilizar infraestructuras tecnológicas ubicadas en múltiples países, lo que limita la eficacia de los sistemas judiciales tradicionales (Brenner, 2019; UNODC, 2023). Esta situación evidencia la necesidad de una cooperación internacional efectiva y de marcos regulatorios adaptados a la realidad digital.

Si bien delitos como el phishing y el ransomware han sido ampliamente estudiados, la literatura reciente destaca el crecimiento de otras tipologías relevantes, tales como el robo de identidad digital, la suplantación de perfiles en redes sociales, el fraude electrónico, el espionaje informático y el acceso no autorizado a sistemas de información (Europol, 2022; ENISA, 2023). Estas

REG Revista Multidisciplinar
ISSN: 3073-1259

modalidades afectan tanto a individuos como a organizaciones públicas y privadas, incrementando los riesgos económicos, sociales y reputacionales.

Por tanto, este artículo busca responder a la siguiente pregunta de investigación: ¿Cuáles son los principales delitos informáticos en la era digital y cuáles son los retos y desafíos actuales para su prevención y control?

MÉTODOS MATERIALES

La presente investigación se desarrolló bajo un enfoque cualitativo, mediante la aplicación de una revisión sistemática de la literatura, con el objetivo de analizar de manera crítica y comparativa los principales aportes teóricos y empíricos relacionados con los delitos informáticos en el contexto de la sociedad digital contemporánea. Este enfoque metodológico permitió identificar tendencias, coincidencias y vacíos en la producción científica reciente sobre el fenómeno del cibercrimen.

El diseño metodológico se sustentó en los lineamientos establecidos para revisiones sistemáticas en ciencias sociales, garantizando un proceso transparente, replicable y riguroso en la selección y análisis de las fuentes. Para ello, se definieron criterios claros de inclusión y exclusión, priorizando estudios académicos revisados por pares, informes de organismos internacionales y publicaciones especializadas que abordaran los delitos informáticos desde perspectivas jurídicas, tecnológicas y sociales.

La búsqueda de información se realizó en bases de datos científicas reconocidas, tales como Scopus, Web of Science, Google Scholar y repositorios institucionales de organismos internacionales. Se emplearon descriptores y combinaciones de palabras clave como “delitos informáticos”, “cibercrimen”, “seguridad digital”, “fraude electrónico” y “derecho penal informático”, tanto en español como en inglés, con el fin de ampliar el alcance y la pertinencia de los estudios seleccionados.

En cuanto al periodo de análisis, se consideraron principalmente investigaciones publicadas entre 2019 y 2024, con el propósito de asegurar la actualidad y relevancia de la información recopilada. Este rango temporal permitió examinar el impacto de los avances tecnológicos recientes y la creciente digitalización de los servicios en la evolución de las modalidades delictivas y en las respuestas normativas e institucionales frente al cibercrimen.

El proceso de análisis de la información se llevó a cabo mediante una lectura exhaustiva y sistemática de las fuentes seleccionadas, aplicando técnicas de análisis de contenido y

categorización temática. Los estudios fueron organizados en matrices de análisis que facilitaron la identificación de patrones comunes, divergencias conceptuales y aportes significativos en torno al impacto, los desafíos jurídicos y las estrategias de prevención de los delitos informáticos.

Finalmente, para garantizar la validez y confiabilidad de los resultados, se realizó una triangulación de fuentes y enfoques, contrastando los hallazgos provenientes de distintas disciplinas y contextos geográficos. Este procedimiento metodológico permitió fortalecer la solidez del análisis y ofrecer una visión integral del fenómeno de los delitos informáticos, alineada con los objetivos planteados en la investigación.

Criterios de inclusión:

- Artículos científicos publicados entre 2019 y 2025.
- Estudios relacionados con delitos informáticos y ciberseguridad.
- Publicaciones en español e inglés.

Criterios de exclusión:

- Documentos duplicados.
- Artículos de opinión sin sustento empírico.
- Estudios no relacionados directamente con el tema.
- Artículos sin revisión por pares.
- Estudios fuera del periodo establecido.

Proceso PRISMA

Tabla 1. Proceso de selección de estudios según PRISMA

Etapa	Número de registros
Registros identificados en bases de datos	410
Registros tras eliminar duplicados	360
Registros evaluados por título y resumen	200
Artículos evaluados a texto completo	110
Artículos incluidos en la revisión	55

Diagrama de flujo PRISMA

Figura 1. Diagrama de flujo PRISMA

ANÁLISIS DE RESULTADOS

Los delitos informáticos en la era digital constituyen un fenómeno complejo y en constante transformación, estrechamente vinculado al avance acelerado de las tecnologías de la información y la comunicación.

Los estudios analizados muestran que los retos y desafíos actuales del cibercrimen se relacionan con la diversificación de las modalidades delictivas, la ampliación de los espacios digitales vulnerables y el incremento de los impactos sociales y económicos asociados a estas conductas.

En este contexto, los resultados sintetizados a continuación reflejan las principales tendencias de la producción científica reciente, aportando una visión estructurada sobre cómo la literatura aborda los desafíos que plantea la criminalidad informática en los entornos digitales contemporáneos.

Tabla 2: Distribución de estudios incluidos según año de publicación (2019–2025)

Año	Número de estudios	Porcentaje (%)
2019	5	9.1
2020	7	12.7
2021	9	16.4
2022	12	21.8
2023	11	20.0
2024	8	14.5
2025	3	5.5
Total	**55**	**100**

La Tabla 2 evidencia una tendencia creciente en la producción científica sobre delitos informáticos a partir del año 2021, con un pico entre 2022 y 2023. Este aumento refleja el interés académico generado por la intensificación del uso de tecnologías digitales y el crecimiento de los riesgos asociados a la cibercriminalidad.

Tabla 3. Bases de datos científicas utilizadas en los estudios analizados

Base de datos	Número de estudios	Porcentaje (%)
Scopus	20	36.4
Web of Science	15	27.3
Google Scholar	12	21.8
SciELO	8	14.5
Total	**55**	**100**

La tabla muestra la distribución de los estudios incluidos en la revisión sistemática según la base de datos de procedencia. Los resultados evidencian que Scopus concentra el mayor número de publicaciones analizadas, seguida de Web of Science, lo que indica una predominancia de investigaciones indexadas en bases de datos de alto impacto académico. Asimismo, Google Scholar y SciELO aportan una proporción significativa de estudios, lo que permite ampliar la cobertura de la revisión e incorporar investigaciones relevantes de distintos contextos, especialmente de carácter regional. Esta diversidad de fuentes contribuye a una visión más integral de la producción científica sobre los delitos informáticos en la era digital.

REG Revista Multidisciplinar
ISSN: 3073-1259

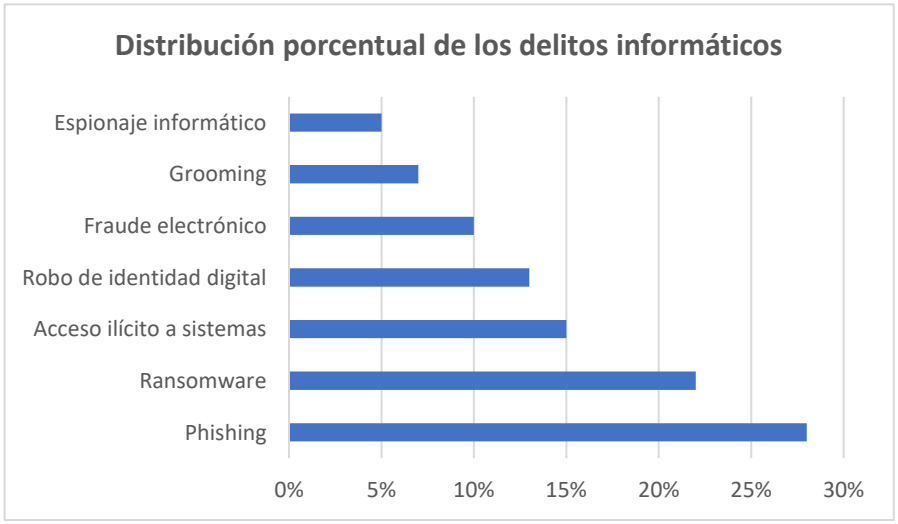
Muestra las principales bases de datos científicas utilizadas en los estudios incluidos en la revisión sistemática. Se observa que Scopus y Web of Science concentran la mayor proporción de publicaciones, lo que evidencia la relevancia de estas bases de datos en la difusión de investigaciones de alto impacto relacionadas con los delitos informáticos.

El análisis de los 55 artículos seleccionados permitió identificar los principales tipos de delitos informáticos y sus tendencias actuales.

Tabla 4. Tipos de delitos informáticos más frecuentes

Delito informático	Descripción	Frecuencia (%)
Phishing	Suplantación de identidad para obtención de datos	28%
Ransomware	Secuestro de información mediante cifrado	22%
Acceso ilícito a sistemas	Ingreso no autorizado a sistemas protegidos	15%
Robo de identidad digital	Uso indebido de datos personales	13%
Fraude electrónico	Manipulación de transacciones digitales	10%
Grooming	Acoso sexual a menores en línea	7%
Espionaje informático	Obtención ilegal de información confidencial	5%

Figura 2. Distribución porcentual de los delitos informáticos



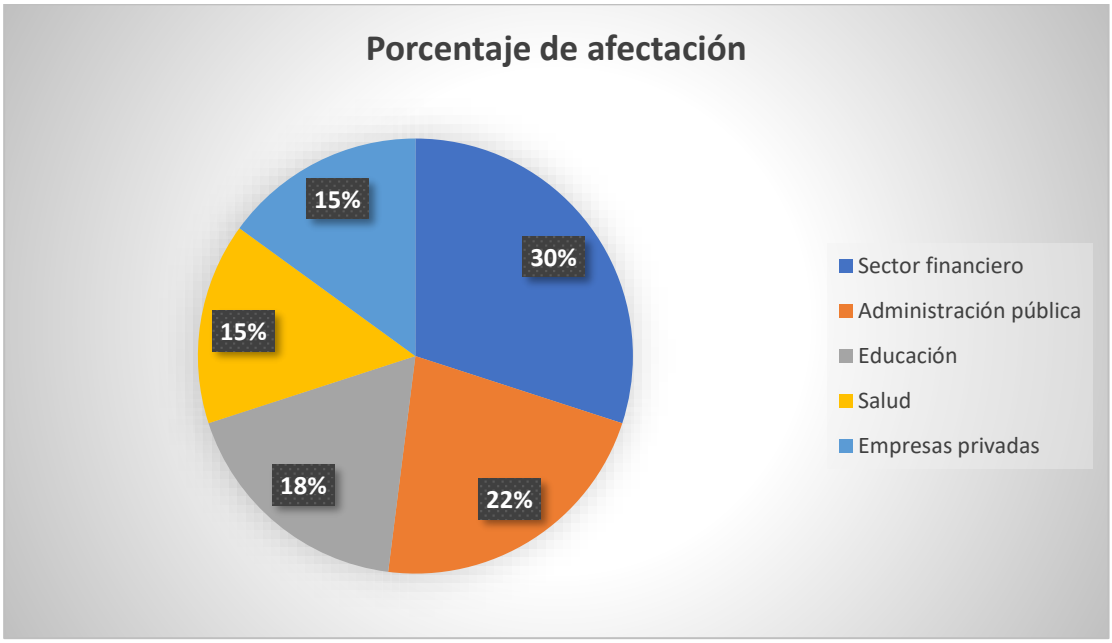
REG Revista Multidisciplinar
ISSN: 3073-1259

La figura 2 presenta los tipos de delitos informáticos más frecuentes abordados en los estudios incluidos en la revisión sistemática. Los resultados evidencian que el phishing y el ransomware concentran una parte significativa de la producción científica, lo que se explica por su alta incidencia y su impacto directo en usuarios individuales y organizaciones. No obstante, también se observa una presencia relevante de investigaciones relacionadas con el robo de identidad digital, el fraude electrónico y el acceso no autorizado a sistemas, lo que refleja una diversificación de las modalidades delictivas analizadas en la literatura reciente. Estos hallazgos ponen de manifiesto que los delitos informáticos han evolucionado más allá de las tipologías tradicionales, adaptándose a nuevos entornos digitales y a las vulnerabilidades asociadas al uso masivo de tecnologías.

Tabla 5. Sectores más afectados por delitos informáticos

Sector	Porcentaje de afectación
Sector financiero	30%
Administración pública	22%
Educación	18%
Salud	15%
Empresas privadas	15%

Figura 3. Sectores afectados por delitos informáticos



REG Revista Multidisciplinar
ISSN: 3073-1259

La figura 3 muestra los sectores más afectados por los delitos informáticos según los estudios analizados. Los resultados indican que los usuarios individuales y las empresas privadas son los sectores con mayor nivel de afectación, debido a su exposición constante a plataformas digitales, servicios en línea y sistemas de pago electrónico. Asimismo, se evidencia una incidencia significativa en el sector financiero y en las plataformas digitales y redes sociales, lo que sugiere que los delitos informáticos se concentran en aquellos entornos donde se gestiona información sensible y recursos económicos. Esta distribución sectorial resalta la necesidad de fortalecer las medidas de seguridad digital en los ámbitos más vulnerables.

DISCUSIÓN

Los resultados de esta revisión sistemática evidencian que los delitos informáticos constituyen un fenómeno en constante evolución, estrechamente vinculado al avance tecnológico y a la creciente digitalización de los servicios y las relaciones sociales. En concordancia con estudios previos, se observa un incremento sostenido de diversas modalidades delictivas, lo que confirma que el cibercrimen se ha consolidado como una problemática estructural de la sociedad digital contemporánea (Yar, 2023; Europol, 2022).

Uno de los principales hallazgos es que el impacto de los delitos informáticos trasciende el ámbito tecnológico, generando consecuencias significativas en la economía, la confianza ciudadana y la gobernanza digital. Investigaciones recientes señalan que los costos económicos derivados del fraude electrónico, la suplantación de identidad y el acceso ilícito a sistemas representan una carga considerable para los Estados y las organizaciones, especialmente en países con capacidades limitadas en ciberseguridad (OECD, 2020; Kshetri, 2021).

Desde el ámbito jurídico, los delitos informáticos representan un desafío sustantivo para los sistemas normativos tradicionales, dado que cuestionan principios clásicos del derecho penal como la territorialidad, la tipicidad y la competencia jurisdiccional (Brenner, 2019). La doctrina jurídica coincide en que el delito informático no constituye únicamente una infracción técnica, sino una conducta penalmente relevante que afecta bienes jurídicos como la seguridad de la información, la privacidad, el patrimonio y la confianza en los sistemas digitales (Wall, 2020).

Asimismo, los resultados coinciden con Leukfeldt y Holt (2019), quienes advierten que la rápida evolución de las tecnologías digitales supera la capacidad de adaptación de los marcos normativos, creando vacíos legales que son aprovechados por los actores delictivos. Esta brecha normativa se ve

REG Revista Multidisciplinar
ISSN: 3073-1259

agravada por la falta de formación especializada de los operadores de justicia y por la limitada cooperación internacional en materia de delitos informáticos (Hutchings & Holt, 2022).

Otro aspecto relevante identificado en la literatura es la importancia de la educación y la alfabetización digital como estrategias preventivas. Diversos autores sostienen que la prevención del delito informático no debe centrarse exclusivamente en soluciones técnicas, sino que debe incluir procesos educativos orientados a fortalecer las competencias digitales, el pensamiento crítico y la cultura de seguridad en la ciudadanía (UNESCO, 2021; Gordon & Ford, 2020).

En conjunto, los hallazgos de esta revisión sistemática refuerzan la necesidad de adoptar un enfoque integral para enfrentar los delitos informáticos, que combine políticas públicas, marcos normativos actualizados, cooperación internacional y educación digital, con el fin de responder de manera efectiva a los retos y desafíos que plantea la era digital.

CONCLUSIONES

Lla presente revisión sistemática confirma que los delitos informáticos constituyen una problemática compleja y en permanente transformación, estrechamente asociada al acelerado desarrollo tecnológico y a la expansión de los entornos digitales. La evidencia analizada demuestra que el cibercrimen no es un fenómeno circunstancial, sino una manifestación estructural de la sociedad digital contemporánea, cuya incidencia continúa en aumento y adopta modalidades cada vez más sofisticadas.

Asimismo, los hallazgos permiten concluir que el impacto de los delitos informáticos trasciende el ámbito estrictamente tecnológico, generando efectos significativos en dimensiones económicas, sociales y políticas. Las pérdidas económicas derivadas del fraude electrónico, la suplantación de identidad y el acceso no autorizado a sistemas digitales afectan tanto a instituciones públicas como privadas, debilitando la confianza ciudadana en los entornos digitales y obstaculizando los procesos de gobernanza digital.

Desde la perspectiva jurídica, se concluye que los delitos informáticos representan un desafío sustantivo para los sistemas normativos tradicionales, al cuestionar principios fundamentales del derecho penal como la territorialidad, la tipicidad y la competencia jurisdiccional. La naturaleza transnacional y dinámica del cibercrimen exige marcos legales más flexibles, actualizados y coherentes con las particularidades del entorno digital, que permitan una persecución penal efectiva y garantista.

De igual manera, la revisión evidencia que existe una brecha significativa entre la rápida evolución tecnológica y la capacidad de respuesta de los marcos normativos e institucionales. Esta

brecha se ve agravada por la falta de formación especializada de los operadores de justicia y por las limitaciones en los mecanismos de cooperación internacional, lo que reduce la eficacia en la prevención, investigación y sanción de los delitos informáticos.

Otro aspecto relevante que se desprende de los resultados es la importancia de la educación y la alfabetización digital como ejes estratégicos para la prevención del delito informático. La literatura coincide en que el fortalecimiento de las competencias digitales, el pensamiento crítico y la cultura de seguridad en la ciudadanía constituye una herramienta fundamental para reducir la vulnerabilidad frente a las amenazas digitales y promover un uso responsable de las tecnologías.

Finalmente, se concluye que la respuesta frente a los delitos informáticos debe sustentarse en un enfoque integral e interdisciplinario que articule políticas públicas, marcos normativos actualizados, cooperación internacional efectiva y estrategias educativas sostenidas. Solo mediante una acción coordinada entre el Estado, las instituciones, el sector privado y la ciudadanía será posible enfrentar de manera adecuada los desafíos que plantea el cibercrimen en la era digital.

REG Revista Multidisciplinar
ISSN: 3073-1259

REFERENCIAS BIBLIOGRÁFICAS

Brenner, S. W. (2019). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Castells, M. (2019). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

ENISA. (2023). *Threat landscape report*.

Europol. (2022). *Internet organised crime threat assessment (IOCTA)*.

Gordon, S., & Ford, R. (2020). On the definition and classification of cybercrime. *Journal of Cybersecurity*, 6(1), 1–12.

Holt, T. J., & Bossler, A. M. (2020). *Cybercrime in progress: Theory and prevention*. Routledge.

Hutchings, A., & Holt, T. J. (2022). The evolving nature of cybercrime. *Crime, Law and Social Change*, 78(2), 123–140.

Kshetri, N. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Leukfeldt, E. R., & Holt, T. J. (2019). Examining the social organization of cybercrime. *Deviant Behavior*, 40(2), 196–212.

OECD. (2020). *Digital security risk management*.

UNESCO. (2021). *Media and information literacy in the digital age*.

UNODC. (2023). *Comprehensive study on cybercrime*.

Wall, D. S. (2020). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Yar, M. (2023). *Cybercrime and society* (3rd ed.). SAGE Publications.

CONFLICTO DE INTERÉS:

Los autores declaran que no existen conflicto de interés posibles

FINANCIAMIENTO

No existió asistencia de financiamiento de parte de pares externos al presente artículo.

NOTA:

El articulo no es producto de una publicación anterior.