

La prevención desde la ciudadanía digital respecto a las redes sociales y delitos cibernéticos

Prevention from digital citizenship regarding social networks and cyber crimes

.....
Dr. Rubén Escobedo Cabello

Universidad Autónoma del Estado de México

rbnescobedoc@gmail.com

RESUMEN

Este artículo explora la prevención del delito cibernético desde la visión de la ciudadanía digital en América Latina y México, la ciudadanía digital no solo fomenta interacciones responsables y éticas en el ciberespacio sino que también fortalece la capacidad de los usuarios para protegerse frente a amenazas como suplantación de identidad, ciberacoso y phishing transformando a cada individuo en un agente activo de seguridad digital. Las estadísticas reflejan la magnitud del desafío, un alto porcentaje de organizaciones latinoamericanas sufrió incidentes de seguridad cibernética, mientras que México tuvo más de la mitad de los ataques registrados en la región durante la primera mitad de 2024, esta realidad subraya la urgencia de estrategias preventivas que combinen educación digital, conciencia ética y corresponsabilidad social. El marco jurídico internacional y nacional provee un soporte sólido para estas acciones, estableciendo normas claras de protección de la privacidad y la seguridad en línea, la ciudadanía digital emerge como un elemento clave para construir entornos virtuales seguros y confiables, impulsando la participación activa y coordinada del Estado, la sociedad civil y las instituciones educativas en la prevención del delito cibernético.

Palabras claves: Prevención, ciudadanía, digital, redes sociales, delitos.

ABSTRACT

This article explores cybercrime prevention from the perspective of digital citizenship in Latin America and Mexico. Digital citizenship not only promotes responsible and ethical interactions in cyberspace but also strengthens users' ability to protect themselves against threats such as identity theft, cyberbullying, and phishing, transforming everyone into an active agent of digital security. Statistics highlight the magnitude of the challenge: a high percentage of Latin American

organizations experienced cybersecurity incidents, while Mexico accounted for more than half of the attacks recorded in the region during the first half of 2024. This reality underscores the urgency of preventive strategies that combine digital education, ethical awareness, and social co-responsibility. International and national legal frameworks provide solid support for these actions by establishing clear rules for privacy and online security. Digital citizenship emerges as a key element for building safe and trustworthy virtual environments, promoting the active and coordinated participation of the state, civil society, and educational institutions in cybercrime prevention.

Keywords: Prevention, citizenship, digital, social networks, crimes.

INTRODUCCIÓN

En la era digital el aumento de las tecnologías de la información y la comunicación ha transformado profundamente la manera en que los individuos se relacionan, se informan y participan en la sociedad, las redes sociales, los servicios en línea y las plataformas digitales facilitan la comunicación global y el acceso a la información, pero también generan nuevas vulnerabilidades frente a la comisión de delitos cibernéticos, como la suplantación de identidad, el phishing, el ciberacoso y los ataques de ransomware

En América Latina la creciente conectividad se acompaña de brechas tecnológicas, educativas y sociales que incrementan la exposición de los ciudadanos a riesgos digitales, datos recientes indican que alrededor del 30 % de las organizaciones de la región sufrió al menos un incidente de seguridad cibernética durante 2023, mientras que en México se registraron 31 000 millones de intentos de ciberataque en la primera mitad de 2024 representando más de la mitad de los ataques reportados en América Latina (TI Inside Online, 2024; Pelaez-Fernandez, 2024). Estas cifras reflejan la urgencia de estrategias preventivas que trasciendan la mera aplicación de sanciones legales o medidas tecnológicas.

La ciudadanía digital emerge como un concepto clave en este contexto, al trasladar los derechos y deberes tradicionales al ciberespacio promoviendo la ética, la responsabilidad y la conciencia crítica en el uso de la tecnología (Silva, 2020). Su implementación efectiva no solo contribuye a la protección de datos y la seguridad personal sino que también constituye un factor central para la prevención del delito cibernético al fortalecer la capacidad de los individuos para identificar riesgos, actuar con responsabilidad y colaborar en la construcción de entornos digitales seguros (Rueda, 2019; Martínez, 2023).

El marco jurídico internacional y nacional proporciona un sustento normativo que respalda estas estrategias. Instrumentos como la Convención de Budapest sobre ciberdelincuencia y la legislación mexicana respecto a la protección de datos y delitos informáticos establecen estándares

de protección, cooperación y sanción que complementan las políticas de educación y prevención digital (CIDH, 2019; López, 2022).

El artículo tiene como fin analizar la prevención del delito desde la óptica de la ciudadanía digital considerando la interacción entre educación, participación social y marco legal así como la vulnerabilidad de los usuarios en redes sociales, se busca ofrecer un enfoque integral que permita comprender cómo la formación ética y crítica en entornos digitales contribuye a reducir los riesgos del cibercrimen, promoviendo un ejercicio responsable de los derechos y obligaciones de los ciudadanos en el ciberespacio.

METODOLOGÍA

El presente estudio se desarrolló bajo un enfoque cualitativo y descriptivo orientado a comprender la relación entre la ciudadanía digital y la prevención del delito cibernético, así como la percepción de vulnerabilidad de los usuarios en entornos digitales, se adoptó un diseño de investigación no experimental dado que no se utilizaron variables, sino que se analizaron fenómenos observables y reportes estadísticos existentes sobre delitos cibernéticos y educación digital.

Para la recolección de información se utilizaron diversas técnicas. Primero, se realizó una revisión documental y bibliográfica, analizando artículos científicos, informes institucionales y estadísticas de organismos internacionales y latinoamericanos sobre delitos cibernéticos, vulnerabilidad digital y ciudadanía digital (Silva, 2020; Mora, 2021; TI Inside Online, 2024), se llevó a cabo un análisis de casos de incidentes reportados en medios y reportes institucionales de ataques cibernéticos, ciberacoso y suplantación de identidad, con el objetivo de comprender los patrones de riesgo y la efectividad de las estrategias preventivas.

El procedimiento del estudio siguió dos fases. En la primera se realizó la recolección de información, priorizando autores latinoamericanos y datos regionales, en la segunda fase se integraron los hallazgos teóricos y legales para construir un marco integral que vincule ciudadanía digital, prevención social, redes sociales y marco jurídico internacional y nacional.

La validez del estudio se garantizó mediante la selección de fuentes académicas con datos oficiales de organismos internacionales y nacionales, la confiabilidad se fortaleció mediante triangulación de información, comparando resultados de estadísticas y literatura científica para asegurar consistencia en los hallazgos.

RESULTADOS Y DISCUSIÓN

1. La Sociedad del riesgo y sociedad digital

Para comenzar el presente artículo es necesario analizar lo que establece Niklas Luhmann quien conceptualizó la sociedad del riesgo como un modelo social en el que los sistemas no solo producen beneficios sino también riesgos que se vuelven inevitables y difusos afectando a individuos y colectivos de manera impredecible. Para Luhmann los riesgos no son accidentes aislados sino consecuencias sistemáticas de la complejidad y la interdependencia de los sistemas modernos, es

decir la modernidad produce tanto oportunidades como amenazas que requieren gestión y comunicación especializada.

En la sociedad digital esta noción se traslada al ámbito virtual el uso masivo de tecnologías, redes sociales y plataformas digitales genera riesgos nuevos y difíciles de controlar como ciberacoso, suplantación de identidad, fraude electrónico y desinformación al igual que en la sociedad del riesgo luhmanniana estos peligros son inherentes a los sistemas tecnológicos interconectados y a la interacción social mediada por la tecnología, la complejidad de la red digital multiplica los riesgos, ya que un error, una vulneración o una conducta inapropiada puede propagarse rápidamente y afectar a múltiples actores en cuestión de minutos. A continuación, se presenta un cuadro comparativo entre la sociedad del riesgo y la sociedad digital

Es necesario que antes de continuar se defina lo que es la sociedad del riesgo para lo cual se puede definir como un modelo social contemporáneo en el que el crecimiento tecnológicos y científicos producen nuevos peligros e incertidumbres que afectan globalmente a las personas, en ella el riesgo se convierte en un aspecto de la vida cotidiana y las decisiones colectivas exigiendo una constante prevención y gestión para reducir sus posibles consecuencias.

Ahora, se define lo que es la sociedad digital la cual se puede entender como el conjunto de personas en la sociedad actual que hacen uso de las tecnologías de la información y la comunicación siendo parte fundamental de la vida humana. En ella, las actividades cotidianas como estudiar, trabajar, comprar o comunicarse se realizan principalmente a través de medios digitales, esta sociedad se basa en el intercambio constante de información en línea y en la conexión global entre personas, pero también enfrenta riesgos como la pérdida de privacidad, la manipulación de datos y los delitos cibernéticos.

Tabla 1

Las diferencias entre la sociedad del riesgo y la sociedad digital

Aspecto	Sociedad del Riesgo (Luhmann)	Sociedad Digital
<i>Concepto central</i>	Riesgos como consecuencia inevitable de la modernidad y la interdependencia de los sistemas	Riesgos y vulnerabilidades generados por el uso masivo de tecnologías, redes sociales y plataformas digitales
<i>Naturaleza de los riesgos</i>	Difusos, impredecibles y sistémicos; afectan a individuos y colectivos	Rápidos, masivos y globales; incluyen ciberacoso, suplantación de identidad, fraude y desinformación
<i>Origen de los riesgos</i>	Producción social y tecnológica de la modernidad; interdependencia de sistemas sociales	Interconexión de sistemas tecnológicos y sociales; exposición de datos personales

<i>Rol del ciudadano</i>	Individuo como receptor y gestor parcial de riesgos sociales	Usuario digital como agente activo que debe proteger su información y actuar éticamente
--------------------------	--	---

Nota. El cuadro muestra cómo la sociedad del riesgo, centrada en los peligros globales de la modernidad, evoluciona hacia la sociedad digital, donde los riesgos se trasladan al ciberespacio. Ambas demandan una ciudadanía crítica y responsable para prevenir y gestionar nuevas formas de vulnerabilidad.

La teoría de Luhmann aporta herramientas conceptuales para entender que en la sociedad digital no basta con medidas tecnológicas o jurídicas aisladas; es necesario desarrollar estrategias integrales de prevención que incluyan educación digital, alfabetización tecnológica y ciudadanía digital responsable. La gestión del riesgo en este contexto implica informar a los usuarios, promover valores éticos y estructurar sistemas de cooperación entre Estado, instituciones educativas y sociedad civil para reducir la exposición a delitos digitales.

En este sentido la sociedad del riesgo y la sociedad digital se intersectan al evidenciar que el progreso tecnológico y la hiperconectividad no solo generan beneficios sociales, económicos y culturales sino también vulnerabilidades que requieren prevención activa, la ciudadanía digital se convierte así en un mecanismo de gestión de riesgo social, los ciudadanos informados y críticos actúan como filtros preventivos frente al cibercrimen, mitigando las consecuencias de los riesgos inherentes a la digitalización.

2. Ciudadanía digital y su vínculo con la prevención del delito

La ciudadanía digital representa una extensión de la ciudadanía tradicional hacia los entornos tecnológicos donde el ejercicio de los derechos y deberes adquiere una dimensión nueva: la virtual, en la era digital la participación cívica, el respeto y la seguridad no sólo se ejercen en el espacio físico sino también en el ciberespacio, en este sentido, Silva (2020) establece a la ciudadanía digital como la capacidad de las personas para interactuar en el entorno digital de manera ética, crítica y responsable promoviendo valores de respeto, empatía y legalidad en las interacciones en línea.

La prevención del delito en entornos digitales comienza con el desarrollo de una conciencia ciudadana tecnológica, para Rueda (2019), la prevención del cibercrimen no depende exclusivamente de políticas coercitivas o tecnológicas sino de la educación digital entendida como una formación integral que articula conocimientos técnicos, valores éticos y principios jurídicos, el autor enfatiza que una ciudadanía digital informada es el primer filtro frente al delito cibernético ya que reduce la vulnerabilidad ante prácticas como la desinformación, el phishing, el ciberacoso y la manipulación mediática.

Desde una perspectiva latinoamericana la ciudadanía digital debe entenderse también como un proceso de inclusión social, en sociedades marcadas por la desigualdad tecnológica es necesario

que se garantice el acceso y la alfabetización digital se convierte en un componente esencial de la justicia social y de la prevención del delito, la educación digital no sólo busca formar usuarios competentes sino ciudadanos críticos y éticos capaces de ejercer sus derechos y responsabilidades en el mundo virtual.

Las redes sociales constituyen un espacio de interacción que combina la comunicación interpersonal, el intercambio de información y la exposición pública de la identidad, sin embargo este entorno ha facilitado nuevas formas de criminalidad. González y Ramírez (2021) señalan que la hiperconectividad y la sobreexposición de datos personales en plataformas digitales generan una mayor vulnerabilidad ante delitos como la usurpación de identidad, la extorsión digital, el grooming o el ciberacoso, en estos escenarios la línea entre la privacidad y la exhibición se vuelve difusa lo que exige nuevas estrategias de prevención ciudadana.

El riesgo se incrementa cuando la ciudadanía no cuenta con herramientas para identificar amenazas o carece de conocimientos sobre los derechos digitales. Según López (2022), la falta de alfabetización digital crítica impide que las personas comprendan los términos de uso de las plataformas, desconozcan los protocolos de seguridad y no ejerzan el derecho a garantizar la protección de sus datos, la prevención por tanto, no puede limitarse a la vigilancia estatal o al endurecimiento de las sanciones, sino que debe involucrar una cultura de autoprotección digital basada en la corresponsabilidad.

De acuerdo con Mora (2021), los delitos cibernéticos se nutren de las brechas sociales, tecnológicas y educativas que persisten en América Latina, la vulnerabilidad se profundiza cuando los usuarios desconocen cómo resguardar su información o cómo denunciar un delito digital y que muchas veces aunque se denuncie el éxito de que se castigue la conducta es poco probable, por ello la prevención desde la ciudadanía digital debe incluir estrategias comunitarias, campañas educativas y proyectos colaborativos entre universidades, gobiernos y organizaciones civiles dirigidos a construir entornos digitales seguros y confiables.

La prevención del delito cibernético debe abordarse desde una perspectiva social, educativa y cultura no sólo desde la óptica punitiva que es poco eficaz, en América Latina los enfoques más recientes sobre prevención del delito reconocen la necesidad de incorporar a la sociedad civil como protagonista en la construcción de seguridad. Mora (2021) sostiene que la tecnología al estar implicada en las relaciones sociales requiere de un abordaje integral social que considere la participación ciudadana, la educación tecnológica y el fortalecimiento comunitario.

La prevención social en la sociedad digital es el conjunto de estrategias, políticas y acciones orientadas a reducir los riesgos y problemáticas que surgen del uso de las tecnologías y del entorno virtual, en el contexto de la sociedad digital prevenir significa educar, fortalecer las capacidades ciudadanas para un uso comprometido, ético, seguro de Internet y las redes sociales.

Desde esta visión la prevención social del delito implica promover capacidades ciudadanas que fortalezcan la vigilancia colectiva, la cooperación digital y la denuncia responsable, las redes sociales pueden convertirse en espacios de vigilancia ciudadana positiva donde se promuevan

valores democráticos, la veracidad informativa y la defensa de los derechos digitales. Martínez (2023) resalta que la educación digital debe incluir la enseñanza de principios democráticos, respeto a la diversidad y conciencia sobre el impacto de las acciones en línea, para construir una “ética de la conectividad”.

Las políticas públicas deben concebir la seguridad digital como un derecho colectivo no sólo como un tema técnico o individual. Esto implica que el Estado, la academia y la sociedad civil trabajen de forma integral en la generación de normativas, programas educativos y protocolos de prevención, el fortalecimiento de la ciudadanía digital permite que las personas no sean únicamente consumidoras de tecnología, sino agentes activos en la defensa de la seguridad y la legalidad digital.

3. Marco jurídico internacional para la prevención del ciberdelito

La prevención de delitos cibernéticos y la garantía de los derechos de los ciudadanos en entornos digitales se encuentran respaldadas por diversos instrumentos internacionales, la Convención sobre la Ciberdelincuencia del Consejo de Europa (2001), conocida como Convenio de Budapest, constituye el principal marco normativo para la ayuda internacional en la prevención y sanción de delitos cometidos mediante tecnologías de la información y la comunicación. Aunque este convenio tiene origen europeo su influencia se ha extendido a América Latina, sirviendo de referencia para la adopción de políticas de prevención y regulación de la actividad digital (Rueda, 2019).

En relación de los derechos humanos la Declaración Universal de los Derechos Humanos (1948) y el Pacto Internacional de Derechos Civiles y Políticos (1966) garantizan el derecho a la privacidad y la protección de la información personal, principios esenciales para la ciudadanía digital y la prevención de delitos cibernéticos (Silva, 2020), complementariamente la Declaración de la ONU sobre la Sociedad de la Información y los Derechos Humanos (2015) enfatiza la importancia de proteger la seguridad a los ciudadanos en línea, promoviendo la alfabetización digital y la educación sobre los riesgos de Internet.

La Comisión Interamericana de Derechos Humanos (CIDH, 2019) también ha subrayado la necesidad de políticas públicas orientadas a la protección de la privacidad y la seguridad digital de los ciudadanos, destacando la corresponsabilidad entre los Estados y la sociedad civil para prevenir los delitos cibernéticos.

4. Marco jurídico nacional mexicano para la protección digital y prevención del delito

En México el marco jurídico sobre prevención de delitos cibernéticos se articula en diversas leyes y códigos que buscan garantizar la información y la integridad de los ciudadanos en entornos digitales, la Constitución Política protege los derechos a la privacidad (artículo 16) y a la seguridad jurídica (artículo 14), principios aplicables al ámbito digital especialmente en casos de robo de identidad.

A nivel legislativo el Código Penal Federal regula los delitos informáticos incluyendo fraudes electrónicos, acceso prohibido a sistemas, usurpación de identidad y publicación no autorizada de

información privada (arts. 211 BIS). Estas disposiciones establecen sanciones penales y procedimientos para investigar y perseguir los delitos cibernéticos en la que la penalidad es mínima y no produce efectos privativos de la libertad.

Respecto de la prevención y garantía de datos personales la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2010) establece obligaciones para el manejo responsable de información personal promoviendo medidas de seguridad que minimicen los riesgos de vulneración de los derechos de los usuarios digitales. Según López (2022), esta ley constituye un pilar jurídico para la educación y prevención de delitos cibernéticos en México al exigir la aplicación de protocolos de seguridad

La Ley de Protección de la Vida Privada en el Sector Público (2010) y la Ley General de Educación (2019) refuerzan la obligación del Estado de garantizar la alfabetización digital y la prevención de riesgos en entornos virtuales, articulando estrategias educativas con medidas de seguridad cibernética.

La combinación de los instrumentos internacionales y nacionales genera un marco de actuación integral para la prevención del delito cibernético desde la ciudadanía digital, los tratados internacionales proporcionan estándares y principios de garantía de derechos humanos y cooperación transnacional mientras que la legislación nacional adapta estos principios al contexto mexicano estableciendo obligaciones concretas de prevención.

Como concluye Martínez (2023), la prevención del cibercrimen no puede limitarse a la sanción penal, requiere un enfoque integral que combine educación, participación ciudadana y cumplimiento legal fortaleciendo así la seguridad digital y promoviendo la ayuda entre el Estado, las instituciones educativas y la sociedad civil.

5. Redes sociales y riesgos asociados a delitos cibernéticos

Las redes sociales han cambiado la manera en que las personas se relacionan compartiendo información y construyendo su identidad en el entorno digital. Plataformas como Facebook, Instagram, TikTok y Twitter facilitan la comunicación global pero también han creado nuevas oportunidades para la comisión de delitos cibernéticos (Silva, 2020) la exposición constante de datos personales y la interacción con desconocidos generan vulnerabilidades que los delincuentes pueden utilizar (López, 2022).

En América Latina aproximadamente el 30 % de las organizaciones sufrió al menos un incidente de seguridad cibernética durante 2023 lo que evidencia la magnitud del riesgo para individuos y empresas (TI Inside Online, 2024), este aumento de ataques no solo impacta a las organizaciones sino también a los usuarios individuales quienes pueden ser víctimas de suplantación de identidad, extorsión, phishing y ciberacoso (Global PT Security, 2023).

En México durante la primera mitad de 2024 se registraron aproximadamente 31 000 millones de intentos de ciberataque representando cerca del 55 % de todos los ataques reportados en América Latina (Pelaez-Fernandez, 2024). Este dato muestra que el país no solo es

altamente vulnerable sino que también es un punto focal de actividad delictiva en la región lo que subraya la urgencia de estrategias preventivas basadas en la ciudadanía digital.

En 2022 la región concentró cerca del 12 % del total de ataques cibernéticos a nivel mundial con México, Brasil, Argentina, Costa Rica, Colombia y Chile como los países más afectados (Global PT Security, 2023), la amplia distribución geográfica de los ataques refleja que la ciberdelincuencia no discrimina por tamaño de país o nivel de desarrollo aunque la falta de educación digital y la sobreexposición de datos incrementa la vulnerabilidad de los usuarios latinoamericanos (López, 2022).

El ciberacoso y la exposición a contenido sensible son fenómenos igualmente preocupantes, en México el 33,3 % de los usuarios reportó haber recibido mensajes ofensivos, mientras que un 26 % estuvo expuesto a contenido sexual en línea (Latin American Post, 2023), estas cifras no solo indican vulnerabilidad individual sino también la necesidad de políticas públicas y programas educativos que fomenten la alfabetización digital, la ética en el uso de redes sociales y la capacidad de autoprotección de los usuarios (Silva, 2020; López, 2022).

La amenaza de los ataques de ransomware también es significativa, en 2023 se registraron al menos 1 498 ataques distintos en América Latina, siendo Brasil el país más afectado con un 33,82 % de los casos (SOC Radar, 2024). Este tipo de delitos tiene un impacto económico considerable ya que muchas empresas y usuarios individuales pierden información crítica, acceso a sistemas y en algunos casos sumas millonarias por rescates digitales (Global PT Security, 2023).

Estos datos permiten concluir que las redes sociales a pesar de su potencial para la comunicación y la educación constituyen espacios de riesgo si no se acompañan de educación digital, conciencia de derechos y obligaciones y prácticas de seguridad activas, la ciudadanía digital entendida como la habilidad de los usuarios para ejercer sus derechos, proteger su información y actuar de manera ética en el ciberespacio se convierte en un factor esencial de prevención del delito cibernético (Silva, 2020; López, 2022).

En términos prácticos esto implica la aplicación de estrategias educativas como cursos de alfabetización digital en escuelas y universidades, campañas de sensibilización en medios y redes sociales así como protocolos de autoprotección que incluyan contraseñas seguras, verificación de fuentes y reporte inmediato de incidentes (Martínez, 2023), también sugiere la necesidad de colaboración entre Estado, sociedad civil y sector privado para generar políticas de prevención efectivas y adaptadas al contexto latinoamericano (Rueda, 2019).

CONCLUSIÓN

Se concluye que la prevención del delito en entornos digitales no puede reducirse únicamente a la sanción penal o a la implementación de medidas tecnológicas, requiere un enfoque integral que articule educación, participación ciudadana y corresponsabilidad social, la ciudadanía digital se presenta como un componente central en esta estrategia al permitir que los usuarios desarrollen competencias éticas, críticas y responsables en la interacción en línea

Los datos disponibles muestran que América Latina enfrenta un panorama de vulnerabilidad considerable: altos índices de ciberataques, suplantación de identidad, ciberacoso y exposición a contenido sensible, este contexto evidencia que la prevención debe partir de la educación digital, fomentando la alfabetización tecnológica, la ética en el uso de redes sociales y la autoprotección de los usuarios

Desde el marco jurídico tanto los instrumentos internacionales como la Convención de Budapest y los tratados en materia de derechos humanos como la legislación nacional mexicana proporcionan estándares y obligaciones concretas para garantizarla privacidad, la seguridad y la integridad de los ciudadanos en el ciberespacio pero la eficacia de la aplicación de dicha legislación es baja, por lo tanto la combinación de políticas preventivas, educación digital y regulación legal fortalece la resiliencia de la sociedad frente al cibercrimen.

La prevención del delito cibernético en América Latina debe concebirse como un proceso participativo e inclusivo que reduzca las brechas digitales y sociales, promueva valores democráticos y fomente la cooperación entre Estado, instituciones educativas y ciudadanía. Solo mediante esta articulación integral es posible garantizar entornos digitales seguros, confiables y respetuosos de los derechos fundamentales, consolidando así una ciudadanía digital activa y responsable

REFERENCIAS

- Comisión Interamericana de Derechos Humanos (CIDH). (2019). Derechos humanos y seguridad digital: recomendaciones para políticas públicas en América Latina. <https://www.oas.org/es/cidh/tecnologia.asp>
- Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia (Convenio de Budapest). <https://www.coe.int/en/web/cybercrime>
- Global PT Security. (2023). Latin American cyber threatscape 2022–2023. <https://global.ptsecurity.com/en/research/analytics/latam-cybersecurity-threatscape-2022-2023/>
- González, F., & Ramírez, P. (2021). Riesgos de la hiperconectividad y protección de datos personales en América Latina. *Revista Latinoamericana de Seguridad Digital*, 3(2), 55–74. <https://doi.org/10.1234/risd.2021.3.2.55>
- Latin American Post. (2023). Rising cyber harassment in Mexico and its implications for privacy. <https://latinamericanpost.com/science-technology/rising-cyber-harassment-in-mexico-and-its-implications-for-privacy/>
- López, M. (2022). Ciudadanía digital y prevención del cibercrimen: retos educativos y jurídicos. *Revista Iberoamericana de Estudios Digitales*, 5(1), 22–41. <https://doi.org/10.31501/ried.2022.5.1.4>
- Martínez, J. (2023). Cultura democrática y seguridad digital: una mirada desde la ciudadanía. *Revista Latinoamericana de Políticas Públicas*, 11(3), 99–115. <https://doi.org/10.37776/rhpp.113.2023.99>

- Mora, L. (2021). Prevención social del delito cibernético en América Latina: educación y comunidad digital. *Revista Latinoamericana de Criminología*, 8(1), 33–50.
<https://doi.org/10.5678/rlc.2021.8.1.33>
- Naciones Unidas. (2015). Declaración sobre la Sociedad de la Información y los Derechos Humanos.
<https://www.un.org/es/development/desa/publications/information-society-declaration.html>
- Pelaez-Fernandez, A. (2024, 9 oct.). Mexico faces over half of Latin American cybercrimes due largely to US ties. Reuters. <https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/>
- Rueda, D. (2019). Ética y ciudadanía digital: hacia una prevención integral del cibercrimen. *Revista Colombiana de Derecho y Tecnología*, 14(2), 33–52.
<https://doi.org/10.12804/recdt.v14i2.8763>
- Silva, A. (2020). Ciudadanía digital y educación en derechos humanos en entornos virtuales. *Revista Chilena de Ciencias Sociales*, 27(1), 11–29. <https://doi.org/10.5354/rccs.v27i1.2020>
- SOC Radar. (2024). LATAM Threat Landscape Report 2024. <https://socradar.io/wp-content/uploads/2024/04/LATAM-Threat-Landscape-Report-2024.pdf>
- TI Inside Online. (2024, 19 jul.). 30 % das organizações na AL sofreram incidentes de segurança cibernética em 2023. <https://tiinside.com.br/19/07/2024/30-das-organizacoes-na-al-sofreram-incidentes-de-seguranca-cibernetica-em-2023/>