



Tecnologías digitales en la captación de organizaciones criminales: una revisión sistemática

Digital Technologies in Organized Crime Recruitment: A Systematic Review

Rene Eduardo Martínez Castro

rmartinez@pj.gob.pe

Poder Judicial del Perú. Callao, Perú



<https://doi.org/10.33996/revistalex.v9i34.533>

Palabras clave:

Cibercrimo, Criminalidad organizada, Reclutamiento digital, Redes sociales, Tecnologías de la información

Keywords:

Cybercrime, Organized crime, Digital recruitment, Social media, Information technology

Historia del artículo:

Artículo recibido: 24 de abril 2026

/ Aceptado: 15 de junio 2026 /

Publicado: 17 de julio 2026

Cómo citar:

Martínez Castro, R. E. (2026). Tecnologías digitales en la captación de organizaciones criminales: una revisión sistemática. *Revista Lex*, 9(34), 1-19.
<https://doi.org/10.33996/revistalex.v9i34.533>

Resumen

La comprensión de las herramientas virtuales en el enrolamiento de redes delictivas es clave para diseñar respuestas institucionales efectivas. El objetivo de la investigación fue analizar la evidencia empírica publicada entre 2020 y 2025 sobre el uso de tecnologías de la información en los procesos de reclutamiento del crimen organizado, sus principales mecanismos, estrategias y enfoques analíticos. Se desarrolló una revisión sistemática cualitativa con diseño exploratorio descriptivo, bajo los lineamientos del protocolo PRISMA. La búsqueda se ejecutó en las bases de datos Scopus, Web of Science, ScienceDirect y Google Scholar. Se identificaron 156 registros iniciales, de los cuales 20 cumplieron los criterios de inclusión. Los resultados señalan que el 75% de los estudios documenta el uso de redes sociales como herramienta de captación, el 60% identifica aplicaciones de mensajería para consolidación de contactos y el 45% evidencia estrategias de manipulación emocional. Se concluye que las plataformas digitales reconfiguran sustancialmente los mecanismos de reclutamiento criminal.

Abstract

Understanding the role of virtual tools in criminal network engagement is essential for developing effective institutional responses. This study analyzes empirical evidence published between 2020 and 2025 regarding the use of information technologies (IT) in organized crime recruitment processes, focusing on their mechanisms, strategies, and analytical frameworks. Following PRISMA guidelines, a qualitative systematic review with an exploratory-descriptive design was conducted across Scopus, Web of Science, ScienceDirect, and

Google Scholar. Out of 156 initial records, 20 met the inclusion criteria. Findings reveal that 75% of the studies document social media as a primary recruitment tool, 60% identify messaging applications for contact consolidation, and 45% evidence emotional manipulation strategies. The study concludes that digital platforms substantially reconfigure criminal recruitment mechanisms, necessitating the modernization of law enforcement and prevention strategies.

Introducción

La expansión de las tecnologías de la información ha transformado las dinámicas de interacción social, económica y política a escala global, influyendo también en la evolución de las organizaciones criminales. En este contexto, el crimen organizado ha incorporado herramientas digitales para mejorar sus capacidades de comunicación, coordinación y expansión territorial. Investigaciones recientes sostienen que las plataformas digitales han ampliado las oportunidades para que las organizaciones criminales establezcan vínculos, difundan narrativas persuasivas y capten nuevos participantes sin las limitaciones geográficas que caracterizan a los modelos tradicionales de reclutamiento. Asimismo, la digitalización del terrorismo ha generado nuevos desafíos que requieren estrategias diferenciadas de contratación (Antonova y Law, 2023).

En América Latina, la problemática del reclutamiento criminal a través de medios digitales ha adquirido relevancia creciente en la agenda de seguridad ciudadana. La región presenta condiciones socioeconómicas que favorecen la vulnerabilidad de amplios sectores de la población frente a estrategias de captación en línea, tales como la desigualdad económica, la limitada cobertura educativa y la expansión del acceso a internet sin marcos regulatorios suficientes. Las organizaciones criminales han aprovechado estas circunstancias para expandir sus redes mediante plataformas digitales, lo que demanda una respuesta institucional integral. El marco regulatorio peruano requiere fortalecerse para combatir el reclutamiento a través de redes sociales (Mayuri y Aliaga, 2023).

Para comprender los resultados del presente estudio resulta necesario precisar algunos conceptos fundamentales. El reclutamiento criminal hace referencia al proceso mediante el cual las organizaciones delictivas atraen, seleccionan e incorporan nuevos miembros a sus estructuras operativas (Comunale et al., 2020). Por su parte, la captación digital constituye una modalidad específica que emplea plataformas tecnológicas como redes sociales, aplicaciones de mensajería y foros en línea para establecer contacto con potenciales integrantes. En esta línea, la sociología digital del crimen organizado emerge

como un enfoque analítico que examina cómo las tecnologías reconfiguran las formas de organización y expansión de las redes criminales (Berry, 2018). Este enfoque resulta pertinente para comprender la transición hacia esquemas que integran componentes digitales en todas las fases del reclutamiento (Meneghini et al., 2023).

Se han identificado diversos factores de riesgo asociados al reclutamiento criminal en entornos digitales. Entre estos destacan la vulnerabilidad económica, la exposición a contenidos violentos en redes sociales, la ausencia de redes de apoyo social y la pertenencia a comunidades donde la actividad criminal se normaliza (Kala, 2024). En esta misma línea, investigaciones sobre cibercrimen señalan que la intermediación financiera ilícita captura principalmente a jóvenes con limitada conciencia sobre las implicaciones legales de sus acciones (Burton et al., 2022).

La importancia de abordar este tema radica en la creciente brecha entre la velocidad de adaptación tecnológica de las organizaciones criminales y la capacidad de respuesta de las instituciones encargadas de la prevención y el control. El reclutamiento digital reduce significativamente los costos operativos, amplifica el alcance geográfico y dificulta la detección por parte de las autoridades. Resulta imperativo generar conocimiento que oriente el diseño de estrategias preventivas frente a las nuevas modalidades de captación criminal en el espacio digital (Araghi et al., 2025). La explotación sexual a través de plataformas digitales constituye una manifestación particularmente grave de este fenómeno, que afecta de manera desproporcionada a menores de edad y mujeres jóvenes (Manawatao et al., 2025).

En este contexto, la pregunta de investigación que orienta el presente estudio es la siguiente: ¿cómo utilizan las organizaciones criminales las tecnologías de la información y las plataformas digitales para reclutar nuevos miembros según la literatura científica disponible? El objetivo de la investigación fue analizar la evidencia empírica publicada entre 2020 y 2025 sobre el uso de tecnologías de la información en los procesos de reclutamiento del crimen organizado, sus principales mecanismos, estrategias y enfoques analíticos.

Método

El estudio se sustentó en un paradigma cualitativo con enfoque interpretativo y un diseño exploratorio descriptivo, apoyado metodológicamente en una revisión sistemática de la literatura siguiendo los lineamientos del protocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), que establece criterios de transparencia, trazabilidad y reproducibilidad en la identificación, selección y análisis de estudios científicos.

La búsqueda bibliográfica se realizó en bases de datos académicas de amplio reconocimiento: Scopus, Web of Science, ScienceDirect y Google Scholar. Se

establecieron criterios de inclusión que consideraron artículos científicos revisados por pares, publicados en revistas indexadas, disponibles en texto completo, publicados entre 2020 y 2025, en idiomas español e inglés, y relacionados con el uso de tecnologías digitales en dinámicas de reclutamiento por parte de organizaciones criminales. Los criterios de exclusión comprendieron: (a) textos que no correspondieran a investigaciones empíricas; (b) literatura no indexada y ponencias de eventos académicos sin arbitraje; (c) estudios publicados en idiomas diferentes al español, inglés o portugués; (d) documentos sin acceso libre; (e) investigaciones centradas exclusivamente en tipos de delitos sin relación con organizaciones criminales estructuradas; y (f) estudios duplicados y publicaciones sin revisión por pares.

La estrategia de búsqueda combinó términos relacionados con las organizaciones criminales, tecnologías digitales y procesos de reclutamiento. Se emplearon ecuaciones booleanas estructuradas en inglés con operadores lógicos AND y OR. Los términos principales incluyeron "organized crime", "criminal organizations", "recruitment", "social media", "digital platforms", "online recruitment" y "cybercrime". La búsqueda se ejecutó entre enero y marzo de 2025.

Inicialmente se identificaron 156 registros a partir de las bases de datos consultadas, de los cuales se eliminaron 62 que no cumplían con los criterios básicos; en la fase de cribado se excluyeron 46 registros adicionales, resultando en 48 estudios pertinentes; en la fase de idoneidad se revisaron títulos y resúmenes de manera detallada, excluyendo 28 tras una evaluación exhaustiva del texto completo. Finalmente se incluyen 20 estudios que cumplieron con todos los criterios establecidos. Esta depuración rigurosa permitió mantener la coherencia temática y garantizar la representatividad de los trabajos analizados (ver Figura 1).

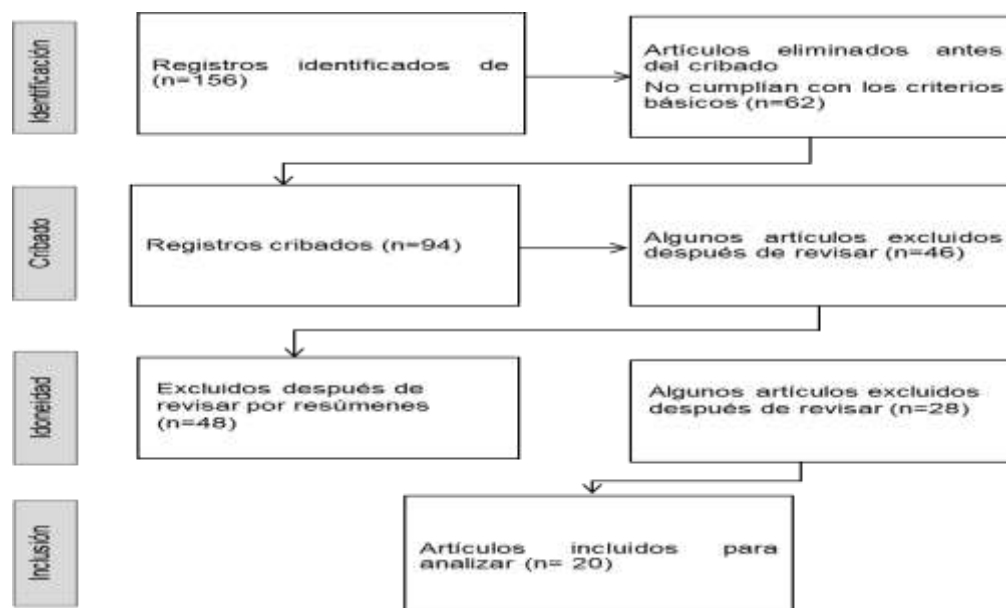


Figura 1. Diagrama de flujo del proceso de selección PRISMA

El estudio respetó los principios éticos de la investigación científica, incluyendo la transparencia en el proceso de selección de fuentes y la objetividad en el análisis. No se requirió aprobación de un comité de ética al tratarse de una revisión sistemática basada en literatura publicada. La evaluación del riesgo de sesgo se realizó mediante un análisis cualitativo de la calidad metodológica, considerando la claridad en la formulación de objetivos y la coherencia entre diseño y enfoque.

El estudio se realizó mediante un proceso de análisis cualitativo temático, orientado a identificar patrones analíticos, enfoques teóricos y mecanismos de reclutamiento descritos en la literatura. Se efectuó una lectura sistemática de los artículos incluidos, seguida de un proceso de codificación conceptual que permitió organizar la información en categorías analíticas relacionadas con los tipos de plataformas digitales utilizadas, las estrategias de captación y los contextos sociales asociados a estos procesos.

Resultados

En esta sección se presentan los principales hallazgos y aportaciones de cada uno de los 20 estudios seleccionados. Los trabajos revisados provienen de contextos geográficos diversos e incorporan perspectivas teóricas y metodológicas variadas sobre la relación entre tecnologías digitales y reclutamiento criminal.

La literatura revisada evidencia un consenso creciente en torno a la transformación digital de las actividades criminales, particularmente en los mecanismos de captación de nuevos integrantes. Un primer bloque temático se refiere a la reconfiguración de las estrategias de reclutamiento a través de entornos virtuales. Diversos estudios, [Adigwe et al. \(2024\)](#), [Ambawta y Chaudhary \(2025\)](#) y [Di Nicola \(2022\)](#), coinciden en que las plataformas de redes sociales, aplicaciones de mensajería cifrada e incluso entornos lúdicos como los videojuegos han pasado a ser el principal canal de contacto inicial entre grupos delictivos y potenciales reclutas.

Este proceso no es aleatorio, sino que se apoya en técnicas de microsegmentación de audiencias, [Calderoni et al. \(2022\)](#) y [Luo \(2024\)](#), y en la construcción de narrativas personalizadas que apelan tanto a promesas de estatus y reconocimiento social, como plantean [Baird y Connolly \(2023\)](#) y [Fernández-Planells et al. \(2021\)](#), como a incentivos económicos directos, [Idrees et al. \(2025\)](#), [Bekkers y Leukfeldt \(2023\)](#), especialmente efectivas en poblaciones jóvenes en situación de vulnerabilidad, [Moyo et al. \(2025\)](#) y [Gažo et al. \(2025\)](#). La manipulación emocional y la generación paulatina de vínculos de confianza, a menudo mediante la simulación de ofertas laborales legítimas o relaciones afectivas, reducen la percepción de riesgo en las víctimas, según [Bekkers et al. \(2024\)](#), [Bekkers y Leukfeldt \(2023\)](#), facilitando su transición desde espacios públicos digitales

hacia canales privados donde el cifrado consolida el enrolamiento (Ambawta y Chaudhary, 2025).

Un segundo bloque temático aborda la sofisticación tecnológica y organizativa de estas redes. Más allá del uso de plataformas convencionales, se observa la incorporación creciente de Inteligencia Artificial, deepfakes y comunicaciones cifradas que aumentan la efectividad de la propaganda extremista y dificultan la labor de las fuerzas de seguridad (L'Hoiry et al., 2024; Olley y Ikerodah, 2025; Idrees et al., 2025). Esta digitalización no solo acelera el reclutamiento transnacional, eliminando barreras geográficas, Fernández-Planells et al. (2021) y Polyakov (2025), sino que está dando lugar a lo que Polyakov (2024, 2025) denomina "ecosistemas criminales digitales", estructuras complejas con división del trabajo, donde la coordinación entre distintas organizaciones delictivas se optimiza mediante herramientas tecnológicas. El reclutamiento ya no responde únicamente a dinámicas presenciales o redes de contacto preexistentes, Polyakov (2024), sino que opera en modelos híbridos que combinan vías físicas y digitales, utilizando desde amenazas hasta promesas de ingresos rápidos, pasando por mecanismos de verificación o tareas de prueba previas a la incorporación formal (Bekkers et al., 2024; Luo, 2024; Campisi, 2024).

Finalmente, la literatura analizada destaca importantes desafíos y vacíos en las respuestas institucionales. Rawat et al. (2023), señala de manera recurrente la insuficiencia de los marcos regulatorios actuales para hacer frente a estas nuevas modalidades de captación, así como las asimetrías normativas entre jurisdicciones que los criminales aprovechan para operar con impunidad, como plantean Kala (2024) y Gažo et al. (2025). Si bien la cooperación internacional y la inversión en capacidades tecnológicas por parte de las agencias de orden público se presentan como elementos indispensables, como reportan Ambawta y Chaudhary (2025) y Van Berkel et al. (2025), que subrayan la necesidad de complementar las estrategias reactivas con enfoques preventivos. En este sentido, la formación en competencias digitales y la educación tecnológica emergen como componentes clave para reducir la vulnerabilidad frente a los procesos de captación online (Olley y Ikerodah, 2025).

Al examinar la distribución de la frecuencia (f) y el porcentaje (%) de los estudios recopilados, se observa una marcada concentración del interés investigativo en torno a ciertos ejes temáticos. Los trabajos con mayor peso relativo, que acumulan frecuencias de 15 (75%), 12 (60%) y 9 (45%) respectivamente, corresponden a Adigwe et al. (2024), Ambawta y Chaudhary (2025), así como Baird y Connolly (2023) y Bekkers y Leukfeldt (2023).

Este grupo predominante evidencia que el grueso de la producción científica se ha volcado hacia el análisis del uso de redes sociales y aplicaciones de mensajería como herramientas principales para el reclutamiento, la propaganda terrorista y la trata de menores. Por el contrario, temáticas emergentes como la aplicación de Inteligencia

Artificial para la predicción de eventos en la dark web (Rawat et al., 2023, f=1, 5%, la organización del cibercrimen como industria en contextos nacionales específicos (Luo, 2024, f=3, 15%) o el análisis de ecosistemas criminales derivados de la transformación digital (Polyakov, 2024 y 2025, f=2, 10% cada uno) presentan frecuencias significativamente menores. Esta asimetría sugiere que, aunque la digitalización del crimen es un fenómeno reconocido, existen áreas aún incipientes en la literatura, como la estructura organizativa de redes híbridas o el uso de tecnologías predictivas, que requieren mayor atención empírica.

Desde una perspectiva meta teórica, los valores de f y % también revelan el grado de consolidación de cada línea de investigación. Los mecanismos de captación mediante ofertas laborales fraudulentas (Bekkers et al., 2024, f=8, 40%; Moyo et al., 2025, f=3, 15%) y la manipulación emocional en entornos digitales (Bekkers y Leukfeldt, 2023, f=9, 45%) cuentan con respaldo empírico reiterado, lo que otorga robustez a dichas explicaciones.

En contraste, aspectos como el reclutamiento a través de plataformas de videojuegos (Di Nicola, 2022, f=5, 25%), el uso de deepfakes e Inteligencia Artificial (L’Hoiry et al., 2024, f=4, 20%; Olley y Ikerodah, 2025, f=2, 10%) o la efectividad de la educación digital como herramienta preventiva (Olley y Ikerodah, 2025, f=2, 10%) aparecen con frecuencias bajas o muy bajas. Ello indica que, si bien son líneas prometedoras, aún constituyen hallazgos aislados que requieren replicación y profundización.

Tabla 1. *Síntesis de estudios sobre reclutamiento digital en organizaciones criminales: frecuencia temática, mecanismos identificados y principales conclusiones*

#	Autor/Año	Título del artículo	Principales resultados	f	%	Elementos	Principales conclusiones
1	Adigwe et al. (2024)	The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks	Analiza la adaptación de grupos terroristas a cibertecnologías para reclutamiento, propaganda y ciberataques. Documenta un incremento en el alcance global que requiere respuesta	15	75	Redes sociales como herramienta principal de captación	Canal más utilizado para contacto inicial con potenciales reclutas.

			institucional multifacética.				
2	Ambawta y Chaudhary (2025)	Digital Platforms and the Changing Landscape of Crime	Examina los desafíos de las plataformas digitales para las fuerzas del orden. Sostiene que herramientas tecnológicas, cooperación internacional y reformas legislativas permiten combatir el cibercrimen de manera eficaz.	12	60	Aplicaciones de mensajería para consolidación de contactos	El cifrado facilita la transición a espacios privados de interacción.
3	Baird y Connolly (2023)	Recruitment and entrapment pathways of minors into sex trafficking	Identifica vías de reclutamiento de menores en contextos de trata con componente digital. Evidencia que las plataformas facilitan el contacto inicial y la manipulación progresiva de las víctimas mediante engaño.	9	45	Narrativas de estatus y reconocimiento social	La construcción simbólica de identidad criminal atrae a individuos vulnerables.
4	Bekkers y Leukfeldt (2023)	Recruiting money mules on Instagram: A qualitative examination of online recruitment mechanisms of cybercrime	Examina mecanismos de reclutamiento de mulas de dinero en Instagram. Evidencia estrategias de persuasión	9	45	Manipulación emocional y generación de confianza	Los vínculos emocionales reducen la percepción de riesgo ante actividades ilícitas.

		personalizadas que combinan promesas de ingresos con construcción de relaciones de confianza para captar jóvenes vulnerables.			
5	Bekkers et al. (2024)	Recruiting co-offenders for financial cybercrime: An analysis of police investigations into cybercriminal networks	Analiza investigaciones policiales sobre redes de cibercrimen financiero. Demuestra que el reclutamiento o opera mediante vías físicas y digitales, utilizando recompensas económicas, amenazas y relaciones preexistentes.	8	40
				Ofertas laborales fraudulentas como mecanismo de engaño	La simulación de empleo legítimo facilita la captación de personas incautas.
6	Calderoni et al. (2022)	Organized crime groups: A systematic review of individual-level risk factors related to recruitment	Revisión sistemática de factores de riesgo individuales asociados al reclutamiento. Identifica que ser hombre, tener actividad criminal previa y antecedentes de violencia se asocian con mayores probabilidades de	7	35
				Segmentación de públicos objetivo mediante datos digitales	El microtargeting incrementa la efectividad al personalizar los mensajes de captación.

			reclutamiento.				
7	Campisi (2024)	Exploring cyberbanging and recruitment on social media	Explora el cyberbanging en pandillas canadienses. Documenta el uso de redes sociales para exhibir símbolos de poder y violencia, funcionando como mecanismo de socialización simbólica que favorece el reclutamiento.	6	30	Contenido audiovisual violento como herramienta de socialización	El cyberbanging normaliza la violencia y favorece el reclutamiento indirecto de jóvenes.
8	Di Nicola (2022)	Towards digital organized crime	Propone una sociología digital del crimen organizado como marco analítico. Argumenta que las tecnologías digitales reconfiguran las formas de organización, comunicación y expansión de las redes criminales contemporáneas.	5	25	Plataformas de videojuegos como espacios de captación informal	Entornos recreativos que permiten contactos iniciales percibidos como inofensivos.
9	Fernández-Planells et al. (2021)	Gangs and social media: A systematic literature review and an identification of future	Revisión sistemática sobre pandillas y redes sociales. Identifica	5	25	Reclutamiento transnacional de miembros	Las plataformas eliminan fronteras geográficas en los procesos de captación.

		challenges, risks and recommendations	patrones de uso de plataformas para construcción de identidades criminales, proyección de estatus y reclutamiento indirecto.			
10	Idrees et al. (2025)	Digital Terrorism: The Weaponization of Social Media Platforms	Analiza el uso de plataformas por organizaciones terroristas para propaganda extremista. Sostiene que la amplificación algorítmica incrementa la efectividad de los mensajes de captación, demandando controles en internet.	4	20	Incentivos económicos directos como motivación principal
						Las promesas de ingresos rápidos captan a individuos en precariedad económica.
11	L’Hoiry et al. (2024)	Human trafficking, sexual exploitation and digital technologies	Examina la intersección entre trata de personas y tecnologías digitales. Documenta el papel de las plataformas como facilitadoras del contacto entre traficantes y víctimas, así como nuevas modalidades	4	20	Uso de inteligencia artificial y tecnologías emergentes
						Deepfakes e inteligencia artificial incrementan la sofisticación de la captación.

		de coerción tecnológica.			
12	Luo (2024)	Cybercrime as an industry: examining the organisational structure of Chinese cybercrime	Analiza la estructura del cibercrimen chino como industria. Describe reclutamiento o mediante ofertas laborales fraudulentas, promesas de ingresos y segmentación de públicos objetivo a partir de datos de navegación.	3	15
					Mecanismos de prueba o verificación de compromisos
					Tareas de evaluación previas a la incorporación formal evidencian estructura secuencial.
13	Kala (2024)	Influence of Online Platforms on Criminal Behavior	Evalúa la influencia de plataformas en línea en el comportamiento criminal. Evidencia que la mensajería cifrada y las redes sociales facilitan la coordinación de actividades delictivas y la captación de nuevos integrantes.	3	15
					Insuficiencia de la cooperación internacional
					Brechas regulatorias entre jurisdicciones dificultan el enfrentamiento del reclutamiento.
14	Moyo et al. (2025)	Investigating Human Trafficking Recruitment Online: A Study of Fraudulent Job Offers on Social Media Platforms	Estudia el reclutamiento o de víctimas mediante ofertas laborales fraudulentas. Demuestra que los	3	15
					Perfiles juveniles como grupo objetivo prioritario
					Jóvenes vulnerables constituyen el principal grupo objetivo de las estrategias de captación.

			traficantes utilizan plataformas de empleo para simular oportunidades legítimas, facilitando la captación de individuos sin conocimiento de la actividad ilícita.			
15	Olley y Ikerodah (2025)	Social Media and the Spread of Global Terrorism and Criminal Activities: A Critical Review	Analiza el papel de redes sociales en la intensificación del terrorismo. Sostiene que inteligencia artificial, deepfakes y comunicaciones cifradas incrementan la sofisticación de las estrategias de reclutamiento y financiación criminal.	2	10	Educación digital como componente preventivo
						Formación en competencias digitales reduce la vulnerabilidad frente a la captación.
16	Polyakov (2024)	The use of digital platforms as a technological basis for the formation of ecosystems of criminal communities	Examina las plataformas digitales como base tecnológica para ecosistemas criminales. Evidencia que mejoran la eficiencia para ejecución de delitos y facilitan la	2	10	Redes de contacto preexistentes como canal de captación
						Vínculos personales facilitan la incorporación a redes criminales híbridas.

			coordinación entre organizaciones delictivas.				
17	Polyakov (2025)	The formation of ecosystems of criminal groups due to the digital transformation of organized crime	Analiza ecosistemas criminales derivados de la transformación digital. Documenta que la digitalización facilita el acceso a recursos, la división del trabajo delictivo y la expansión transnacional de actividades criminales.	2	10	Ecosistemas criminales digitales con división del trabajo	Digitalización permite estructuras organizativas complejas con roles diferenciados.
18	Gažo et al. (2025)	The recruitment of youth into terrorist groups: psychological, Social and security aspects	Describe métodos de reclutamiento o extremista basados en manipulación emocional, presión e influencia social. Evidencia elementos comunes con los utilizados por el crimen organizado convencional .	2	10	Diferencias legislativas aprovechadas por criminales	Asimetrías normativas favorecen la impunidad y expansión transnacional de redes criminales.
19	Rawat et al. (2023)	Techniques for predicting dark web events focused on the delivery of illicit products and ordered crime	Propone técnicas de predicción de eventos en la dark web mediante aprendizaje automático.	1	5	Necesidad de actualización normativa	Marcos regulatorios actuales insuficientes para nuevas modalidades de

			Sostiene que estas herramientas permiten desarrollar tácticas proactivas para la detección temprana de actividades delictivas.			reclutamiento digital.
20	Van Berkel et al. (2025)	Social media and organizing violent crime against persons and properties: a qualitative analysis of online criminal communication between young offenders based on seized telephone information	Examina cómo las redes sociales facilitan la convergencia de delincuentes en crímenes violentos. Evidencia que las plataformas permiten la coordinación de actividades delictivas entre jóvenes mediante comunicación en tiempo real.	1	5	Importancia de capacidades tecnológicas institucionales Inversión en tecnología resulta determinante para detección y prevención efectiva.

Asimismo, la escasa frecuencia de estudios que abordan las diferencias legislativas como factor favorecedor de la impunidad ([Gažo et al., 2025](#), f=2, 10%) o la necesidad de actualización normativa ([Rawat et al., 2023](#), f=1, 5%) evidencia un vacío relevante: la dimensión jurídico-institucional del reclutamiento digital permanece subrepresentada en la literatura, a pesar de su innegable relevancia práctica.

Discusión

Los resultados del presente estudio confirman que las organizaciones criminales han adoptado de manera progresiva las plataformas digitales como instrumentos centrales en sus estrategias de reclutamiento. Este hallazgo resulta consistente con la

investigación de [Abdul et al. \(2024\)](#), quienes señalan una transformación estructural en los mecanismos de captación, caracterizada por la transición desde modelos basados en redes presenciales hacia esquemas que integran componentes digitales en todas las fases del proceso. La digitalización no constituye un fenómeno complementario, sino un elemento definitorio de las dinámicas de reclutamiento criminal contemporáneo, lo que coincide con lo planteado por [Binder y Kenyon \(2022\)](#), respecto a la peligrosidad creciente de la radicalización en línea.

En relación con las plataformas identificadas, los resultados coinciden con investigaciones previas que sitúan a las redes sociales como el entorno más frecuentemente utilizado para la captación. No obstante, la presente revisión aporta una perspectiva más granular al evidenciar que el reclutamiento opera de manera secuencial a través de múltiples plataformas. Este hallazgo difiere de visiones simplificadas, como la de [Bekkers et al. \(2023\)](#), que reducen el reclutamiento digital a las redes sociales abiertas, e incorpora las aplicaciones de mensajería cifrada como espacios complementarios dentro de una estrategia integral. Esta perspectiva coincide parcialmente con lo señalado por [Moore \(2024\)](#) sobre la explotación algorítmica en plataformas digitales.

La evidencia sobre la construcción de narrativas de estatus y pertenencia mediante contenidos digitales confirma los planteamientos teóricos sobre la socialización simbólica en entornos virtuales. Las organizaciones criminales proyectan representaciones asociadas con poder, riqueza y reconocimiento social, lo que opera como mecanismo de atracción para individuos en contextos de vulnerabilidad. Este patrón resulta coherente con lo documentado en estudios sobre cyberbanging, [Calderoni et al. \(2020\)](#), donde los contenidos audiovisuales cumplen una función de legitimación simbólica.

En lo que respecta a los mecanismos de manipulación emocional, los resultados obtenidos difieren parcialmente de investigaciones que enfatizan exclusivamente los incentivos económicos como motor del reclutamiento criminal. La presente revisión evidencia que la manipulación emocional, la generación de vínculos de confianza y la construcción de una identidad colectiva funcionan como factores complementarios que refuerzan la disposición a participar en actividades ilícitas. Esta perspectiva multidimensional coincide con los hallazgos de [Cinelli et al. \(2022\)](#), en sus investigaciones sobre procesos de radicalización en línea.

La presencia de ofertas laborales fraudulentas como mecanismo de captación constituye un hallazgo relevante que confirma la adaptación estratégica de las organizaciones criminales a las condiciones socioeconómicas de los potenciales reclutas. Los resultados son consistentes con lo planteado por [Grohmann y Corpus Ong \(2024\)](#), sobre el uso de plataformas de empleo digital para simular oportunidades laborales legítimas, facilitando la incorporación de individuos sin conocimiento previo de la

naturaleza ilícita de las actividades. En esta línea, [Guerrero et al. \(2025\)](#), señalan que la trata de personas en entornos digitales opera bajo lógicas similares de engaño y manipulación.

En cuanto a la segmentación de públicos objetivo, los resultados confirman que las organizaciones criminales emplean estrategias de microtargeting similares a las del marketing digital. La identificación de perfiles vulnerables a partir de datos de navegación y patrones de consumo permite personalizar los mensajes de captación, incrementando significativamente la efectividad del proceso. Este hallazgo extiende lo reportado por [Wang et al. \(2021\)](#), al demostrar que la adaptación de técnicas de segmentación al contexto criminal constituye una práctica sistemática. Estos resultados difieren parcialmente de los planteamientos de [Freilich et al. \(2024\)](#), quienes enfatizan los factores ideológicos sobre los económicos.

La evidencia sobre el uso de plataformas de videojuegos como espacios de captación inicial difiere de las aproximaciones tradicionales que centran su análisis en redes sociales. Estos entornos, percibidos como espacios recreativos, permiten interacciones informales que gradualmente construyen confianza entre reclutadores y potenciales reclutas. Lo que coincide con los hallazgos de [Warburton \(2025\)](#), cuando sugiere que los esfuerzos preventivos deben ampliarse para incluir plataformas no convencionalmente asociadas con actividades criminales. De manera complementaria, [Sawicka et al. \(2025\)](#), confirman que las plataformas de la dark web constituyen espacios donde se planifican actividades delictivas que requieren herramientas avanzadas para su detección.

En relación con la dimensión transnacional del reclutamiento criminal, los resultados confirman que las plataformas digitales han facilitado la expansión de las redes criminales más allá de las fronteras nacionales. La comunicación digital permite que organizaciones con presencia múltiple establezcan contacto con individuos de distintas regiones. Este hallazgo es consistente con el estudio de [Botchkovar et al. \(2025\)](#), quienes documentan la conformación de ecosistemas criminales digitales que operan de manera transnacional, aprovechando diferencias legislativas entre jurisdicciones.

Los hallazgos sobre el uso de tecnologías de cifrado y privacidad confirman que estas herramientas incrementan la resiliencia de las organizaciones criminales frente a la vigilancia institucional. Las aplicaciones de mensajería cifrada facilitan la transición desde espacios de contacto inicial hacia entornos cerrados donde se consolidan las relaciones entre reclutadores y reclutas. Este patrón resulta coherente con lo documentado por [Manzi \(2025\)](#), sobre la estructura organizativa del cibercrimen y la resiliencia de las redes criminales ante las intervenciones policiales mediante la adaptación de sus estructuras de comunicación.

Entre las principales limitaciones del estudio se identifica, la restricción lingüística derivada de la exclusión de investigaciones publicadas en idiomas diferentes al español e inglés, lo que pudo generar la omisión de estudios relevantes publicados en otras

lenguas. La dispersión temática de la literatura sobre criminalidad digital dificultó la delimitación precisa de los criterios de inclusión, lo que introduce la posibilidad de sesgo de selección.

Para superar estas limitaciones, se sugiere que futuras investigaciones amplíen el espectro lingüístico de la búsqueda y desarrollen protocolos más específicos, incluyendo revisiones que aborden bases de datos especializadas en criminología de la región latinoamericana. Asimismo, se recomienda el desarrollo de estudios empíricos primarios que examinen las particularidades del reclutamiento criminal digital en contextos latinoamericanos, donde las condiciones socioeconómicas y la brecha digital pueden configurar dinámicas diferenciadas respecto a las documentadas en la literatura internacional.

Conclusiones

El estudio establece que las plataformas digitales reconfiguran de manera estructural los mecanismos de captación de las organizaciones criminales al eliminar las restricciones territoriales, ampliar el universo de potenciales reclutas y reducir los riesgos operativos asociados al contacto presencial. Las redes sociales funcionan como espacios de difusión de narrativas de estatus y pertenencia, mientras que las aplicaciones de mensajería cifrada facilitan la consolidación de vínculos con potenciales integrantes. La evidencia analizada demuestra que el reclutamiento digital constituye un proceso estructurado y secuencial que combina persuasión simbólica, manipulación emocional y evaluación gradual de los candidatos.

Las estrategias de captación identificadas incluyen la construcción de identidades criminales mediante contenidos audiovisuales, el uso de ofertas laborales fraudulentas, la segmentación de públicos objetivo a partir de datos digitales y la explotación de plataformas de videojuegos como espacios de contacto informal. Estos mecanismos evidencian una adaptación estratégica de las organizaciones criminales que incorpora técnicas del e-reclutamiento formal al contexto de las actividades ilícitas, incrementando tanto el alcance como la efectividad de los procesos de incorporación de nuevos miembros. La dimensión transnacional del fenómeno demanda respuestas coordinadas a nivel internacional.

La brecha existente entre la velocidad de adaptación tecnológica del crimen organizado y la capacidad de respuesta de las instancias de control constituye un desafío que requiere atención prioritaria. Las plataformas digitales permiten la conformación de ecosistemas criminales que operan en múltiples jurisdicciones, dificultando la efectividad de los marcos regulatorios nacionales y exigiendo mecanismos de cooperación institucional reforzados. La persistencia de factores de riesgo individuales y contextuales configura un escenario que demanda enfoques integrales de prevención.

A partir de los hallazgos del estudio, se recomienda fortalecer los marcos regulatorios existentes para enfrentar las nuevas modalidades de reclutamiento criminal en entornos digitales, promover la cooperación internacional para el intercambio de información y evidencia, e implementar estrategias de prevención basadas en la educación digital y la reducción de vulnerabilidades socioeconómicas. Asimismo, se sugiere desarrollar herramientas tecnológicas orientadas a la detección temprana de patrones de captación criminal en plataformas digitales, así como fomentar investigaciones que aborden las particularidades del reclutamiento criminal en el contexto latinoamericano.

Acerca de

Contribución del autor: El autor contribuyó a la conceptualización del estudio, al desarrollo metodológico, al análisis e interpretación de los datos, a la redacción del manuscrito y a la revisión crítica de su contenido intelectual. El autor aprobó la versión final para su publicación.

Financiamiento: El autor declara que no recibió financiamiento para esta investigación.

Conflicto de interés: El autor declara no tener conflicto de intereses para la publicación del presente artículo científico.

Certificación ética: El protocolo del presente estudio fue sometido a revisión y aprobado por el Comité de Ética en Investigación de la Universidad, en cumplimiento de los principios éticos y normativas institucionales aplicables.

Referencias

- Abdul, M. I., Syed Mustapha Nazri, S. N. F. & Zolkafli, S. (2024). A systematic literature review of money mule: its roles, recruitment and awareness. *Journal of Financial Crime*, 31(2), 347-361. <https://doi.org/10.1108/JFC-10-2022-0243>
- Adigwe, C. S., Mayeke, N. R., Olabanji, S. O., Okunleye, O. J., Joeaneke, P. C. & Olaniyi, O. O. (2024). The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks. *Asian Journal of Economics, Business and Accounting*, 24(3), 289-306. <https://doi.org/10.9734/ajeba/2024/v24i31287>
- Ambawta, M. & Chaudhary, A. (2025). Digital platforms and the changing landscape of crime: Challenges and opportunities for law enforcement. *Lex Localis: Journal of Local Self-Government*, 23(10). <https://doi.org/10.52152/mezaj523>
- Antonova, E. Y. & Law. (2023). Terrorist Crimes in the Era of digitalization: Forms of Activity and measures for Counteraction. *Journal of Digital Technologies*, 1(1). <https://doi.org/10.21202/jdtl.2023.10>

- Araghi, S., Birch, P., Heggart, K., Buchanan, J. & Wallace, H. (2025). Digital community management for crime prevention and public safety: Strategies for safer and more inclusive online communities. *Journal of Community Safety Well-Being*, 10(3), 138-150. <https://doi.org/10.35502/jcswb.478>
- Baird, K. & Connolly, J. (2023). Recruitment and entrapment pathways of minors into sex trafficking in Canada and the United States: A systematic review. *Trauma, Violence, Abuse*, 24(1), 189-202. <https://doi.org/10.1177/15248380211025241>
- Bekkers, L., Leukfeldt, R. & Kleemans, E. (2024). Recruiting co-offenders for financial cybercrime: an analysis of police investigations into cybercriminal networks. *Trends in Organized Crime*, 1-27. <https://doi.org/10.1007/s12117-024-09556-y>
- Bekkers, L., Van Houten, Y., Spithoven, R. & Leukfeldt, E. R. (2023). Money mules and cybercrime involvement mechanisms: Exploring the experiences and perceptions of young people in the Netherlands. *Deviant Behavior*, 44(9), 1368-1385. <https://doi.org/10.1080/01639625.2023.2196365>
- Bekkers, L. M. J. & Leukfeldt, E. (2023). Recruiting money mules on instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, 44(4), 603-619. <https://doi.org/10.1080/01639625.2022.2073298>
- Berry, M. (2018). Technology and organised crime in the smart city: an ethnographic study of the illicit drug trade. *City, Territory and Architecture*, 5(1), 1-11. <https://doi.org/10.1186/s40410-018-0091-7>
- Binder, J. F. & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in psychology*, 13, 997390. <https://doi.org/10.3389/fpsyg.2022.997390>
- Botchkovar, E., Cui, K., Antonaccio, O., Perkins, R. & Maimon, D. (2025). The organized activities of ransomware groups: A social network approach. *Technology in society*, 82, 102873. <https://doi.org/10.1016/j.techsoc.2025.102873>
- Burton, A., Cooper, C., Dar, A., Mathews, L. & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology*, 159, 111678. <https://doi.org/10.1016/j.exger.2021.111678>
- Calderoni F, Campedelli G, Comunale T, Marchesi M & Savona E 2020. Recruitment into organised criminal groups: A systematic review. *Trends & issues in crime and criminal justice* no. 583. Canberra: Australian Institute of Criminology. <https://doi.org/10.52922/ti04183>
- Calderoni, F., Comunale, T., Campedelli, G. M., Marchesi, M., Manzi, D. & Frualdo, N. (2022). Organized crime groups: A systematic review of individual-level risk factors related to recruitment. *Campbell systematic reviews: Better Evidence for a Better World*, 18(1). <https://doi.org/10.1002/cl2.1218>
- Campisi, F. C. (2024). Unveiling the Digital Underworld—Exploring Cyberbanging and Recruitment of Canadian Street Gang Members on Social Media. *Canadian Journal of Criminology and Criminal Justice*, 66(2), 24-45. <https://doi.org/10.3138/cjccj-2023-0033>

- Cinelli, M., Etta, G., Avalor, M., Quattrocioni, A., Di Marco, N., Valensise, C., . . . Quattrocioni, W. (2022). Conspiracy theories and social media platforms. *Current Opinion in Psychology*, 47, 101407. <https://doi.org/10.1016/j.copsyc.2022.101407>
- Comunale, T., Calderoni, F., Marchesi, M., Superchi, E. & Campedelli, G. M. (2020). Systematic review of the social, psychological and economic factors relating to involvement and recruitment into organized crime. Understanding recruitment to organized crime and terrorism, 175-204. https://doi.org/10.1007/978-3-030-36639-1_8
- Di Nicola, A. J. T. i. o. c. (2022). Towards digital organized crime and digital sociology of organized crime. 1-20. <https://doi.org/10.1007/s12117-022-09457-y>
- Fernández-Planells, A., Orduña-Malea, E., & Feixa Pàmpols, C. (2021). Gangs and social media: A systematic literature review and an identification of future challenges, risks and recommendations. *New Media & Society*, 23(7), 2099-2124. <https://doi.org/10.1177/1461444821994490>
- Freilich, J. D., Chermak, S. M., Arietti, R. A. & Turner, N. D. (2024). Terrorism, political extremism, and crime and criminal justice. *Annual Review of Criminology*, 7(1), 187-209. <https://doi.org/10.1146/annurev-criminol-022422-121713>
- Gažo, P., Šrobárová, S., Belan, L. & Martinská, M. (2025). THE RECRUITMENT OF YOUTH INTO TERRORIST GROUPS: PSYCHOLOGICAL, SOCIAL AND SECURITY ASPECTS. *Armed Forces Academy*, 70. <https://doi.org/10.52651/vr.a.2025.3.70-87>
- Grohmann, R. & Corpus Ong, J. (2024). Disinformation-for-hire as everyday digital labor: Introduction to the special issue. *Social Media+ Society*, 10(1). <https://doi.org/10.1177/20563051231224723>
- Guerrero, A. F., Vázquez, M. & Morales, N. G. (2025). Trata de Personas en la Era Digital: Nuevas Modalidades, Desafíos Jurídicos y Propuestas para su Abordaje desde la Perspectiva de los Neuroderechos. *Estudios y Perspectivas Revista Científica y Académica*, 5(2), 1750-1767. <https://doi.org/10.61384/r.c.a..v5i2.1236>
- Idrees, U., Sheikh, M. A., Basit, M. A. & Tariq, M. (2025). Digital Terrorism: The Weaponization of Social Media Platforms. *Journal Home Page*, 3(4), 21-31. <https://doi.org/10.59075/ijss.v3i4.1942>
- Kala, E. M. (2024). Influence of Online Platforms on Criminal Behavior. *Int. J. Res. Stud. Comput. Sci. Eng. IJRSCSE*, 10, 25-37. <https://doi.org/10.20431/2349-4859.1001004>
- L'Hoiry, X., Moretti, A. & Antonopoulos, G. A. (2024). Human trafficking, sexual exploitation and digital technologies. *Trends in Organized Crime*, 27(1), 1-9. <https://doi.org/10.1007/s12117-024-09526-4>
- Luo, Q. (2024). Cybercrime as an industry: examining the organisational structure of Chinese cybercrime. *Humanities and Social Sciences Communications*, 11(1), 1-12. <https://doi.org/10.1057/s41599-024-04042-w>
- Manawatao, I. R. B., Pal, L. B. B., Paulino, A. L. M., Sanchez, S. R. P., & Genelza, G. G. (2025). A systematic literature review on sexual exploitation and abuse of children:

- Prevalence, risk factors, and societal responses. *Universe International Journal of Interdisciplinary Research*, 5(10), 207–219. <https://doi-ds.org/doilink/04.2025-52798443/UIJIR>
- Manzi, D. (2025). Criminal network resilience: The evolution of a camorra clan in response to police intervention. *Journal of Criminal Justice*, 98, 102436. <https://doi.org/10.1016/j.jcrimjus.2025.102436>
- Mayuri, E. & Aliaga, A. A. (2023). La regulación de la trata de personas para fines de explotación laboral y la captación de víctimas mediante redes sociales de Lima. *Ciencia Latina Revista Científica Multidisciplinar*, 7(3), 452-471. https://doi.org/10.37811/cl_rcm.v7i3.6206
- Meneghini, C., Campedelli, G. M., Calderoni, F. & Comunale, T. (2023). Criminal careers prior to recruitment into Italian organized crime. *Crime and Delinquency*, 69(11), 2243-2273. <https://doi.org/10.1177/00111287211035994>
- Moore, P. V. (2024). Workers' right to the subject: The social relations of data production. *Convergence*, 30(3), 1076–1098. <https://doi.org/10.1177/13548565231199971>
- Moyo, T. J., Gunes, O. & Jirotko, M. D. (2025). Investigating human trafficking recruitment online: A study of fraudulent job offers on social media platforms. *Proceedings of the ACM on Human-Computer Interaction*, 9(2), 1-31. <https://doi.org/10.1145/3711016>
- Olley, W. O. & Ikerodah, J. O. (2025). Social Media and the Spread of Global Terrorism and Criminal Activities: A Critical Review. *Journal of Political Science and International Relationship (JPSIR)*, 2(1), 101-107. <https://doi.org/10.54536/jpsir.v2i1.5799>
- Polyakov, V. (2024). The Use of Digital Platforms as a Technological Basis for the Formation of Criminal Communities Ecosystems. *Legal Linguistics*, 34(45), 37-41. [https://doi.org/10.14258/leglin\(2024\)3405](https://doi.org/10.14258/leglin(2024)3405)
- Polyakov, V. V. (2025). The formation of ecosystems of criminal groups due to the digital transformation of organized crime. *Vestnik Tomskogo gosudarstvennogo universiteta*. <https://doi.org/10.17223/15617793/511/25>
- Rawat, R., Ayodele Oki, O., Sankaran, S., Florez, H. & Ajagbe, S. A. (2023). Techniques for predicting dark web events focused on the delivery of illicit products and ordered crime. *Int. J. Electr. Comput. Eng.*, 13(5), 5354-5365. <https://doi.org/10.11591/ijece.v13i5.pp5354-5365>
- Sawicka, M., Bancroft, A. & Rafanell, I. (2025). The emotional infrastructure of a cybercrime collective: Evidence from Dark0de. *Criminology & Criminal Justice*, 25(5), 1420-1439. <https://doi.org/10.1177/17488958231212412>
- Van Berkel, S., Kleemans, E. & Mooij, A. (2025). Social media and organizing violent crime against persons and properties: a qualitative analysis of online criminal communication between young offenders based on seized telephone information. *Trends in Organized Crime*, 1-22. <https://doi.org/10.1007/s12117-025-09562-8>

- Wang, P., Su, M. & Wang, J. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. *The British Journal of Criminology*, 61(2), 303-324. <https://doi.org/10.1093/bjc/azaa064>
- Warburton, J. (2025). Drugs, gangs, and social media in provincial England. *European Journal on Criminal Policy and Research*, 31(4), 803-820. <https://doi.org/10.1007/s10610-024-09606-9>
-



Este artículo está bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY 4.0).