VISIÓN ACADÉMICA
ISSN: 3103-1536

Periodicidad: Trimestral, Volumen: 4, Número: 3, Año: 2026 páginas 869-894

DOI: https://doi.org/10.70577/30phrd87

Estrategia para la Detección de Perfiles Potencialmente Falsos en Tiktok: Un Caso Práctico Basado en Técnicas de Análisis Digital y Herramientas Osint.

Silvia Yajaira Sacon Macías
Estudiante de pregrado de la carrera de Tecnologías de la Información y Comunicación
https://orcid.org/0009-0002-6496-9382
ssacon4361@utm.edu.ec
Universidad Técnica de Manabí
Portoviejo

Oscar Alexander López Gorozabel
Docente, Ingeniero de Sistemas Informáticos. Licenciado en Trabajo Social. Máster en Ingeniería de Software. Máster en Intervención Social
https://orcid.org/0000-0002-0640-9953
oscar.lopez@utm.edu.ec
Universidad Técnica de Manabí
Portoviejo

Cómo citar:
Estrategia para la Detección de Perfiles Potencialmente Falsos en Tiktok: Un Caso Práctico Basado en Técnicas de Análisis Digital y Herramientas Osint. (2029). *Visión Académica, 4*(3), 869-894. https://doi.org/10.70577/30phrd87

Fecha de recepción: 2026-07-23

Fecha de aceptación: 2026-08-07

Fecha de publicación: 2026-08-25

Resumen

La proliferación de perfiles potencialmente falsos en redes sociales dificulta la verificación de identidades digitales y requiere integrar diferentes fuentes de evidencia. El estudio tuvo como propósito desarrollar y aplicar una estrategia para identificar perfiles potencialmente falsos en TikTok mediante la combinación de indicadores cuantitativos, análisis OSINT y verificación visual.Se desarrolló un estudio de caso aplicado, con diseño no experimental y enfoque pragmático. Se analizaron intencionalmente 20 perfiles públicos de TikTok. La estrategia comprendió cuatro fases: caracterización inicial mediante Tikmatrix, análisis de coincidencias de identificadores mediante Sherlock, búsqueda inversa de imágenes mediante Google Lens y triangulación de evidencias. Se calcularon tres indicadores: relación entre seguidores y cuentas seguidas, me gusta por video y volumen de publicaciones respecto de seguidores. La clasificación se estableció mediante cuartiles.De los 20 perfiles analizados, nueve fueron priorizados para una segunda valoración. Sherlock identificó 31 coincidencias externas, destacando @pk.cat.fun3 con 12, y @_thiennkimz, @wxdx1015 y @luysacr con cinco cada uno. La verificación mediante Google Lens permitió identificar coincidencias visuales en varios perfiles. La triangulación estableció tres perfiles con nivel de evidencia alto: @footcr7fc, @_thiennkimz, @wxdx1015 y @pk.cat.fun3; cuatro con nivel moderado y uno con nivel bajo.La integración de evidencias cuantitativas, nominales y visuales permitió establecer niveles diferenciados de sospecha y priorizar perfiles potencialmente falsos. Los resultados muestran que la triangulación constituye una estrategia más consistente que el uso aislado de un indicador, aunque la clasificación obtenida representa una valoración de sospecha y no una confirmación definitiva de falsedad.

Palabras clave: Perfiles potencialmente falsos; TikTok; análisis OSINT; triangulación de evidencias; verificación visual.

VISIÓN ACADÉMICA
ISSN: 3103-1536

Strategy for Detecting Potentially Fake Profiles on Tiktok: A Case Study Based on Digital Analysis Techniques and Osint Tools.

Abstract

The proliferation of potentially fake profiles on social media makes it difficult to verify digital identities and requires integrating different sources of evidence. The purpose of this study was to develop and apply a strategy to identify potentially fake profiles on TikTok by combining quantitative indicators, OSINT analysis, and visual verification.An applied case study was conducted, using a non-experimental design and a pragmatic approach. Twenty public TikTok profiles were intentionally analyzed. The strategy comprised four phases: initial characterization using Tikmatrix, analysis of identifier matches using Sherlock, reverse image search using Google Lens, and triangulation of evidence. Three indicators were calculated: the ratio of followers to accounts followed, likes per video, and the volume of posts relative to followers. Classification was established using quartiles.Of the 20 profiles analyzed, nine were prioritized for a second assessment. Sherlock identified 31 external matches, with @pk.cat.fun3 standing out with 12, and @_thiennkimz, @wxdx1015, and @luysacr with five each. Verification using Google Lens allowed us to identify visual matches across several profiles. Triangulation identified three profiles with a high level of evidence: @footcr7fc, @_thiennkimz, @wxdx1015, and @pk.cat.fun3; four with a moderate level; and one with a low level.The integration of quantitative, nominal, and visual evidence made it possible to establish differentiated levels of suspicion and prioritize potentially fake profiles. The results show that triangulation is a more consistent strategy than the isolated use of a single indicator, although the classification obtained represents an assessment of suspicion and not a definitive confirmation of falsity.

Key words: Potentially fake profiles; TikTok; OSINT analysis; triangulation of evidence; visual verification.

Introducción

El crecimiento acelerado de las redes sociales ha generado nuevas formas de interacción digital, pero también ha incrementado los riesgos asociados a la suplantación de identidad y la creación de perfiles falsos. Plataformas de alta viralidad como TikTok permiten la creación rápida de cuentas y la difusión masiva de contenido, lo que ha facilitado el uso indebido de identidades digitales para fines de fraude, desinformación o acoso. Estudios como los de (Orellana y Cotera, 2025; Villavicencio et al, 2025), señalan que las redes sociales presentan vulnerabilidades relacionadas con la verificación de identidad y la gestión de cuentas, lo que favorece la proliferación de perfiles falsos y cuentas automatizadas. Desde el ámbito de la ciberseguridad y la informática forense, la detección de estas cuentas se ha convertido en un tema prioritario debido a su impacto en la confianza digital y en la seguridad de los usuarios.

La identificación de perfiles falsos en redes sociales constituye un desafío técnico significativo debido al volumen de datos, la sofisticación de las estrategias de anonimato y la rápida evolución de las plataformas digitales. Autores como (Campos, Moreno y Jiménez, 2025; Zalazar, 2024), indican que cuando se crea un perfil falso se suelen emplear técnicas de ingeniería social y manipulación de

metadatos para aparentar legitimidad. En el caso específico de TikTok, la naturaleza visual y algorítmica de la plataforma facilita la rápida difusión de cuentas falsas que pueden suplantar a personas reales o crear identidades ficticias para manipular audiencias.

Ante esta problemática, se han desarrollado diversas técnicas para el análisis y la detección de perfiles falsos, (Sarkar y Shukla, 2023; Yadav, Kumar y Singh, 2023) consideran las siguientes: análisis de metadatos, la verificación de imágenes mediante búsqueda inversa, el análisis de patrones de comportamiento y el uso de herramientas OSINT para la correlación de información pública. Estas técnicas permiten identificar inconsistencias en la actividad de los perfiles, así como rastrear evidencias digitales que evidencien posibles intentos de suplantación de identidad. Sin embargo, autores como (Li et al., 2023), reconocen limitaciones importantes, como: el gran volumen de información disponible en internet, lo que puede dificultar la identificación de datos realmente relevantes.

En este contexto, resulta necesario diseñar una estrategia para la detección de perfiles potencialmente falsos en TikTok, esta integra la caracterización de perfiles mediante variables observables, el análisis de relaciones entre entidades digitales y la verificación de la identidad visual, con el propósito de identificar indicadores que, mediante su triangulación, permitan establecer niveles de evidencia asociados a la detección de un perfil potencialmente falso. A partir de este propósito, se plantea la siguiente pregunta de investigación: *¿Cómo pueden las técnicas de análisis digital y las herramientas OSINT contribuir a la detección de perfiles potencialmente falsos en TikTok mediante una estrategia aplicada a un caso práctico?*

Estado del Arte

Redes sociales y ecosistema digital

No cabe duda, que las redes sociales se han convertido en uno de los componentes centrales del ecosistema digital contemporáneo, al facilitar la interacción, la producción de contenidos y la circulación de información entre millones de usuarios conectados globalmente. Desde la perspectiva de (Reyes 2025), las redes sociales son plataformas digitales que conectan a millones de personas en tiempo real y les permite intercambiar información a distancia. En este contexto, las redes sociales no funcionan de manera aislada, sino como parte de un entorno digital interdependiente donde convergen dispositivos, aplicaciones, algoritmos y prácticas sociales.

Por otra parte, para Giménez (2023), las redes sociales han impulsado la economía digital a través de la interacción entre distintos actores: usuarios y empresas que colaboran y compiten en un mismo entorno para generar valor, innovación y visibilidad de productos o servicios. Por lo que podría considerarse que las redes sociales hoy en día son plataformas indispensables para que los individuos y organizaciones produzcan y distribuyan contenido de forma inmediata, lo que transforma las formas tradicionales de comunicación y acceso a la información.

Sin embargo, la masificación de las redes sociales ha traído consigo problemáticas como la creación de perfiles falsos, la suplantación de identidad y diversas formas de ciberdelincuencia que se desarrollan en estos entornos digitales. De acuerdo con Díaz et al. (2025), las redes sociales permiten la propagación de información engañosa, especialmente a través de grupos o comunidades cerradas.

En consecuencia, analizar las redes sociales como parte del ecosistema digital implica también reconocer los riesgos asociados a su uso masivo.

Redes sociales como Facebook, Instagram, X, Kwai, Snapchat, TikTok, entre otras se han convertido en espacios donde coexisten prácticas legítimas de interacción social con actividades delictivas que aprovechan la anonimidad y la rapidez de circulación de la información. Acorde a lo anterior (Moncada y Miranda, 2025) destacan que uno de los principales desafíos en la lucha contra la ciberdelincuencia, es la dificultad en la identificación y sanción de responsables.

TikTok como plataforma social emergente

En los últimos años, TikTok se ha consolidado como una de las plataformas sociales emergentes más influyentes en el ecosistema digital global. Según Jordán, Izaguirre y López (2024), esta plataforma permite que la información se difunda rápidamente a una audiencia global, fomentando el consumismo que ha transformado las prácticas comunicativas tradicionales.

Prado (2025) destaca que TikTok ha superado los mil millones de usuarios activos y ha modificado la manera en que las audiencias consumen información, entretenimiento y tendencias culturales. A diferencia de redes tradicionales basadas en relaciones personales directas, el algoritmo de recomendación que tiene TikTok permite que el contenido llegue a audiencias masivas sin depender exclusivamente del número de seguidores. Según Vintimilla y Erazo (2025), esto ha impulsado nuevas estrategias de comunicación digital, marketing y participación social, especialmente entre jóvenes y estudiantes universitarios.

No obstante, el carácter emergente y masivo de TikTok también ha generado debates sobre sus implicaciones sociales, culturales y psicológicas. Autores como (Zhang, Qiu y Ye, 2025; Meng et al., 2024) señalan que la plataforma influye en diversos ámbitos del comportamiento humano, como el consumo, las decisiones cotidianas y la orientación de tendencias sociales, lo que evidencia su creciente poder dentro de la economía digital y la cultura participativa.

Identidad digital en redes sociales

En redes sociales, hablar de identidad digital es esencial, debido a que las plataformas digitales permiten a los usuarios construir y proyectar representaciones de sí mismos. A través de perfiles, publicaciones, imágenes y comentarios, las personas configuran una narrativa pública que refleja intereses, valores y pertenencias sociales. Según Aguessy y Fandy (2025), las redes sociales funcionan como espacios simbólicos donde la identidad se negocia, se transforma y se reafirma mediante dinámicas de interacción digital.

Para Rubio, González y Olivo (2024), en las redes sociales los individuos reciben retroalimentación inmediata mediante reacciones y comentarios, esto influye en la percepción que tienen de sí mismos y en la manera en que ajustan su comportamiento en línea. De esta forma, se podría manifestar que la construcción de la identidad digital está estrechamente vinculada con procesos de auto-presentación y comparación social.

Acorde a Wang (2025), las redes sociales facilitan la articulación de movimientos sociales, expresiones culturales y narrativas colectivas que fortalecen la identidad grupal y la participación social en el entorno digital. En consecuencia, la identidad digital no solo es individual, sino también relacional y comunitaria.

No obstante, la construcción de identidades en redes sociales también plantea riesgos significativos, en estos casos, la creación de perfiles falsos puede facilitar diversas formas de ciberdelito, como el fraude, la suplantación de identidad o el acoso digital (Laffier y Westley, 2025).

Perfiles falsos y bots

Desde el surgimiento y expansión de las redes sociales, estos perfiles se han creado con identidades ficticias que tienen el objetivo de influir en conversaciones digitales, aumentar artificialmente la popularidad de determinadas cuentas o difundir información de manera masiva. Según Zouzou y Varol, (2024), los perfiles falsos pueden actuar de forma coordinada, siguiendo patrones similares de interacción y publicación con el fin de manipular métricas como seguidores, comentarios o niveles de popularidad en una plataforma. Este tipo de perfil habitualmente se emplea para llevar a cabo actividades ilícitas como: robo de identidad, fraudes financieros, acoso cibernético, entre otros.

Por otra parte, Hayawi et al. (2023) manifiesta que los bots actúan como cuentas automatizadas que pueden publicar contenido, interactuar con otros usuarios y replicar comportamientos humanos dentro de las plataformas digitales. Aunque es evidente que algunos bots cumplen funciones legítimas como difundir noticias o información institucional,

su uso malicioso se asocia frecuentemente con campañas de desinformación y manipulación de la opinión pública.

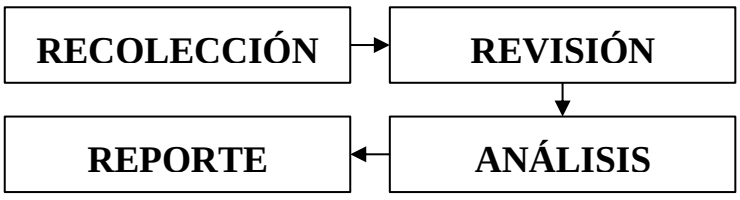
Análisis digital y flujo de trabajo

El análisis digital constituye un proceso sistemático orientado a identificar, preservar, examinar y analizar evidencias digitales con el fin de reconstruir hechos relacionados con incidentes informáticos. De acuerdo a Hargreaves, Nelson y Casey (2024), en la actualidad, el análisis digital se aplica en diversos contextos, como investigaciones de ciberdelitos, fraudes en línea o suplantación de identidad en redes sociales. Vale recalcar que su relevancia radica en la capacidad de transformar datos digitales aparentemente dispersos en evidencia estructurada que permita comprender cómo ocurrió un incidente y quién pudo haber estado involucrado.

Hidalgo et al. (2018), afirma que la National Institute of Standards and Technology ha propuesto un modelo para efectuar análisis digital y está constituido por cuatro fases como: recolección, revisión, análisis y reporte. Este flujo permite a los investigadores garantizar la integridad y trazabilidad de la evidencia. A continuación, se detalla de manera breve en qué consiste cada una de las fases:

Figura 1.

Flujo de trabajo en análisis digital.



- **Recolección:** en esta fase se identifican y obtienen las posibles fuentes de evidencia digital relacionadas con el incidente investigado.
- **Revisión:** consiste en examinar preliminarmente la información recopilada con el fin de identificar aquellos datos que puedan tener relevancia para la investigación.
- **Análisis:** en esta etapa se aplican herramientas especializadas para interpretar los datos, identificar patrones de actividad y reconstruir la secuencia de eventos relacionados con el incidente.
- **Reporte:** se documenta de manera clara y detallada los resultados obtenidos durante la investigación forense.

Técnicas para la detección de perfiles potencialmente falsos

Estas técnicas se basan en metodologías propias de la informática forense y el análisis de evidencia digital, cuyo objetivo es identificar indicios técnicos (registros de conexión, metadatos, direcciones IP y patrones de interacción) que permitan determinar la autenticidad de una cuenta o de su contenido. Según Constantinescu (2025), las principales técnicas para la detección de perfiles falsos, son:

El *análisis de contenido y estilo* constituye una técnica relevante dentro del análisis digital, debido a que permite identificar patrones lingüísticos, semánticos y estructurales presentes en publicaciones o perfiles sospechosos. Para Wu, Guo y Hooi (2023), el estudio del estilo de escritura puede ayudar a diferenciar contenido auténtico de contenido manipulado o generado artificialmente, aunque los avances en inteligencia artificial han permitido que usuarios maliciosos imiten estilos legítimos con mayor precisión.

Otra técnica a destacar, es la *búsqueda inversa de imágenes*, la cual consiste en utilizar una imagen como punto de partida para encontrar su origen o detectar si ha sido reutilizada en diferentes contextos en internet. De acuerdo a Wekesa, DeCusatis y Zhu (2023), en la actualidad, esta técnica ha evolucionado debido a la integración de la inteligencia artificial para el rastreo de imágenes, identificación de su procedencia y verificación de su autenticidad mediante metadatos y análisis de similitud visual. De esta forma, los investigadores pueden detectar inconsistencias entre la imagen de perfil y la identidad declarada, lo que facilita la identificación de cuentas fraudulentas.

Sin duda, el *análisis de comportamiento*, llevada a cabo a través de algoritmos de aprendizaje automático que permiten analizar patrones de interacción, frecuencia de publicaciones, conexiones entre usuarios y comportamiento temporal de las cuentas (Bokolo y Liu, 2024). Si dejar a un lado, la investigación de fuentes abiertas (OSINT) como conjunto de herramientas para la recopilación y verificación de información disponible públicamente en internet, debido a que permite obtener datos provenientes de redes sociales, bases de datos públicas, registros web y otros recursos accesibles sin restricciones legales de acuerdo con (Browne, Abedin y Chowdhury, 2024).

Herramientas OSINT para la detección de perfiles potencialmente falsos en redes sociales

En el desarrollo del proceso investigativo orientado a la identificación de perfiles posiblemente falsos en redes sociales, el enfoque basado en inteligencia de fuentes abiertas (OSINT) constituye una estrategia metodológica eficaz para verificar identidades digitales mediante el análisis de información

pública disponible en internet. A continuación, se presentan algunas de las herramientas OSINT más utilizadas en el proceso de detección:

Tabla 1.

Herramientas OSINT que se emplean para la detección de perfiles falsos en redes sociales.

Aspecto analizado	Herramienta	Enlace oficial
Contenido y relaciones del perfil.	Maigret	https://github.com/soxoj/maigret
	Sherlock	https://github.com/sherlock-project/sherlock
	Maltego	https://www.maltego.com/
	Google Dorks	https://www.google.com/
Foto de perfil.	ExifTool	https://exiftool.org/
	PimEyes	https://pimeyes.com/en
	Google Lens	https://lens.google/intl/es-419/
Correo electrónico.	Holehe	https://github.com/megadose/holehe
Infraestructura digital	Shodan	https://www.shodan.io/

Fuente: Elaboración propia.

Métodos

La investigación adopta un enfoque mixto, debido a que combina procedimientos cuantitativos y cualitativos para analizar las características observables de perfiles de TikTok. El componente cuantitativo permite la medición y el análisis descriptivo de variables observables (Hernández y Klimenko, 2025), entre ellas el número de seguidores, el número de cuentas seguidas, el volumen de publicaciones, la frecuencia de publicación y los indicadores de interacción observable. Estas variables fueron utilizadas para calcular indicadores derivados que permitieron establecer relaciones entre el tamaño de la audiencia, la actividad de publicación y la interacción acumulada de los perfiles analizados.

Por su parte, el componente cualitativo utilizado en la interpretación de evidencias (Martín et al, 2026), permitió analizar características del perfil y del contenido publicado. El estudio se desarrolla bajo un paradigma pragmático, debido a que según (Dube, Nkomo y Apadile, 2024) este permite integrar métodos cuantitativos y cualitativos en función del problema de investigación y de la utilidad práctica de los resultados. En este sentido, el paradigma resulta pertinente para el diseño de una estrategia orientada a la identificación de perfiles potencialmente falsos en TikTok, tomando como unidades de análisis 20 perfiles públicos seleccionados intencionalmente.

Población y muestra

La población de referencia estuvo constituida por perfiles públicos de TikTok susceptibles de ser observados y analizados mediante información disponible públicamente. Al haber muchos perfiles

públicos, se realizó un muestreo no probabilístico intencional, seleccionándose 20 perfiles que presentaban uno o más indicadores preliminares. Los criterios considerados, fueron:

Tabla 2.

Criterios considerados para la selección de los 20 perfiles públicos de TikTok.

Criterios
Inconsistencias en la información del perfil.
Patrones atípicos de actividad e interacción respecto de la audiencia.
Reutilización de imágenes o contenido.

Fuente: Elaboración propia.

Técnicas e instrumentos de investigación

Para la recolección y análisis de la información se emplearon la observación digital estructurada y el análisis OSINT. La observación digital permitió registrar información pública disponible en los perfiles seleccionados, incluyendo nombre de usuario, descripción, vídeos, seguidores, cuentas seguidas y otras variables observables. Por su parte, el análisis OSINT permitió contrastar la información del perfil mediante búsquedas en fuentes públicas de internet y otras plataformas digitales.

Los instrumentos utilizados fueron una ficha de observación digital, una matriz de análisis de perfiles y una matriz de triangulación de evidencias. La ficha de observación digital permitió registrar variables relacionadas con la identidad, audiencia, actividad e interacción del perfil. La matriz de análisis de perfiles permitió organizar y comparar los indicadores obtenidos durante la caracterización inicial. Finalmente, la matriz de triangulación permitió integrar las evidencias cuantitativas, relacionales y visuales obtenidas mediante las diferentes técnicas.

Estrategia propuesta para la detección de perfiles potencialmente falsos en TikTok

Figura 2.

Flujo de trabajo para la detección de perfiles potencialmente falsos en TikTok.

La estrategia fue aplicada a una muestra de 20 perfiles públicos mediante un procedimiento progresivo compuesto por cuatro fases. La primera fase correspondió a la caracterización inicial de los perfiles mediante *Tikmatrix*, herramienta utilizada para recopilar variables observables relacionadas con la identidad, audiencia, actividad e interacción.

La segunda fase correspondió al análisis de relaciones y entidades digitales mediante *Sherlock*, con el propósito de identificar posibles conexiones entre nombre de usuarios, alias y correos electrónicos disponibles públicamente. La tercera fase consistió en la verificación de la identidad visual mediante *Google Lens*, utilizada para identificar coincidencias, reutilización o procedencia externa de fotografías e imágenes asociadas a los perfiles.

Como cuarta fase, se aplicó la *triangulación de evidencias*, fundamentada en la convergencia de los hallazgos obtenidos mediante las diferentes técnicas de análisis. Esta fase permitió integrar las evidencias cuantitativas, relacionales y visuales, establecer niveles de evidencia y priorizar los perfiles que presentaron mayor convergencia de indicadores.

Esta consideración resulta relevante debido a que variables como el número de seguidores, la cantidad de publicaciones, la frecuencia de actividad o la ausencia de una descripción pueden presentarse tanto en cuentas legítimas como en perfiles potencialmente falsos. Por ello, estas variables fueron utilizadas como indicadores preliminares para identificar patrones atípicos que posteriormente fueron contrastados mediante técnicas de análisis relacional y verificación visual.

Tabla 3.

Técnicas y herramientas utilizadas en la estrategia.

Tipo	Técnica de análisis	Herramienta	Función dentro de la estrategia	Indicadores	Naturaleza de la evidencia
Herramientas OSINT	Recopilación y caracterización de información pública.	*Tikmatrix*	Caracterización de perfiles públicos y recopilación de variables observables.	Usuario corto, nombre de usuario, tipo de cuenta, descripción, seguidores, seguidos, videos, frecuencia de publicación, tipo de contenido, me gusta y amigos.	Cuantitativa.
	Análisis de relaciones y entidades.	*Sherlock*	Representación y análisis de relaciones entre entidades.	Relaciones entre nombres de usuarios, alias, correos electrónicos y posibles estructuras de conexión.	Relacional.
	Búsqueda y verificación inversa de imágenes.	*Google Lens*	Verificación de imágenes mediante búsqueda inversa.	Reutilización, coincidencia o procedencia externa de fotografías e imágenes.	Visual.

Fuente: Elaboración propia.

Criterios de operacionalización y valoración de evidencias

La valoración de los indicadores se realizó mediante una escala ordinal de cuatro niveles: 0 = ausencia de evidencia, 1 = débil, 2 = relevante y 3 = fuerte. Para Arias (2022), la escala ordinal se utiliza en la investigación para clasificar variables cualitativas con una jerarquía lógica de menor a mayor gravedad o intensidad. Esta escala no representa una probabilidad de que un perfil sea falso, sino el grado de relevancia de los hallazgos obtenidos respecto de la posible inautenticidad del perfil.

Tabla 4.

Escala general de valoración de evidencias.

Valor	Nivel de evidencia	Detalle de evidencia
0	*Sin evidencia*	No se observa el indicador o no existe información suficiente para establecer posible falsedad del perfil.
1	*Débil*	Cuando los resultados se limitaron a señales provenientes de una sola fuente o cuando las coincidencias encontradas no permitieron establecer una correspondencia suficiente.
2	*Relevante*	Cuando existieron evidencias procedentes de dos fuentes o cuando las coincidencias encontradas presentaron elementos de interés, pero requirieron comprobación adicional.
3	*Fuerte*	Cuando se observó convergencia entre diferentes fuentes de evidencia, particularmente cuando una coincidencia de identificador mediante Sherlock estuvo acompañada por una coincidencia visual mediante Google Lens y/o por características relevantes identificadas durante la caracterización inicial.

Fuente: Elaboración propia.

Resultados

Caracterización inicial de los perfiles mediante Tikmatrix

Mediante Tikmatrix y la observación estructurada de los perfiles se recopilaron las métricas y características observables. La información recopilada comprendió variables relacionadas con la identidad del perfil, tamaño de la audiencia, actividad de publicación, interacción y relaciones sociales visibles. Para cada perfil se registró el identificador que es el nombre de usuario precedido por el símbolo @, número de seguidores, número de cuentas seguidas, cantidad de videos, número acumulado de me gusta y cantidad de amigos. Estas variables fueron agrupadas en cuatro dimensiones:

Tabla 5: Dimensiones e indicadores de caracterización.

Dimensiones	Código	Indicadores
Identidad	T1	Nombre de usuario inusual o genérico.
	T2	Descripción inexistente o inconsistente.
	T3	Identidad declarada poco coherente con el contenido observable.
Audiencia	T4	Relación entre seguidores y seguidos.
	T5	Cantidad de amigos respecto a seguidores.
	T6	Tamaño de audiencia respecto a la actividad observable.
Actividad	T7	Volumen de vídeos.
	T8	Frecuencia de publicación.
	T9	Ausencia de contenido en relación con el tamaño de la audiencia.

Interacción	T10	Relación entre me gusta y número de vídeos.
	T11	Relación entre interacción observable y tamaño de la audiencia.

Fuente: Elaboración propia.

La caracterización permitió identificar patrones preliminares que fueron utilizados para orientar las fases posteriores de análisis. Los resultados de esta primera fase se presentan en la Tabla 6.

Tabla 6.

Caracterización inicial de los 20 perfiles.

N.º	Identificador	Seguidores	Seguidos	Videos	Me gusta	Amigos
1	@evb.edit	3.678	114	8	923.590	51
2	@ user8680834318577	27.510	0	61	321.066	0
3	@fuhui4215	340.104	2	186	8.655,087	0
4	@footcr7fc	165.416	40	32	4.835,762	0
5	@maajid_cade_	97.669	2	60	1.581,977	0
6	@yvfw07909258	19.718	0	126	273.539	0
7	@h205yyh	31.023	77	109	407.919	27
8	@_thiennkimz	2.459	117	126	173.078	55
9	@ luysacr	2.741	3	22	937.341	3
10	@el_libro_de_lo_oculto	86.446	159	582	1.160,626	34
11	@bebot.1234	2.525	22	2	16.180	13
12	@iapiaia	546	319	0	0	309
13	@tio.huesitos2	33.817	137	16	758.583	2
14	@ user5932285756265	123	597	4	65	89
15	@ daya.nara_28	28.114	39	0	170.268	0
16	@soniamoss88	21.027	1,458	99	114.641	390
17	@wxdx1015	31.519	0	219	207.898	0
18	@ pk.cat.fun3	11.669	2	224	234.520	1
19	@an0ther32	415	98	0	2.042	63
20	@ bot45174	1.454	35	0	1.888	32

Fuente: Elaboración propia a partir de los datos obtenidos mediante Tikmatrix.

Indicadores derivados de la caracterización inicial

A partir de las variables recopiladas mediante Tikmatrix se calcularon indicadores derivados orientados a complementar la caracterización inicial de los perfiles. Estos indicadores permitieron establecer

relaciones entre el tamaño de la audiencia, la actividad de publicación y el nivel acumulado de interacción. Su finalidad fue identificar patrones que justificaran una revisión posterior mediante las técnicas de análisis relacional y verificación visual, ver tabla 7:

Tabla 7.

Indicadores derivados.

Indicador	Detalle	Fórmula	Qué mide
Relación entre seguidores y cuentas seguidas.	**S** = Seguidores. **CS** = Cuentas seguidas.	$R_{S/CS} = \frac{S}{CS}$	Relación entre el tamaño de la audiencia y la cantidad de cuentas seguidas.
Me gusta por video publicado.	**MGA** = Me gusta acumulados. **VP** = Videos publicados.	$R_{MGA/VP} = \frac{MGA}{VP}$	Promedio de me gusta acumulados por cada video publicado.
Volumen de publicaciones respecto a seguidores.	**VP** = Videos publicados. **S** = Seguidores.	$R_{VP/S} = \frac{VP}{S}$	Cantidad de publicaciones en relación con el tamaño de la audiencia.

Fuente: Elaboración propia.

En los perfiles que no presentaron cuentas seguidas o vídeos publicados, el indicador correspondiente no fue calculado, debido a que su denominador era igual a cero, se registró como no aplicable (N/A).

Valores individuales de cada indicador por perfil

A continuación, se presenta el procedimiento llevado a cabo para el cálculo de $\boldsymbol{R_{S/CS}}$, $\boldsymbol{R_{MGA/VP}}$, $\boldsymbol{R_{VP/S}}$ tomando como referencia el perfil 1: @evb.edit

$$R_{S/CS} = \frac{3.678}{114} = 32{,}263158 \qquad R_{MGA/VP} = \frac{923.509}{8} = 115.448{,}750000 \qquad R_{VP/S} = \frac{8}{3.678}$$

$$= 0{,}002175$$

El mismo procedimiento se empleó para los 19 perfiles restantes, ver Tabla 8:

Tabla 8.

Cálculo de indicadores derivados: $\boldsymbol{R_{S/CS}}$, $\boldsymbol{R_{MGA/VP}}$, $\boldsymbol{R_{VP/S}}$ *por perfil.*

N.º	Identificador	$\boldsymbol{R_{S/CS}}$	$\boldsymbol{R_{MGA/VP}}$	$\boldsymbol{R_{VP/S}}$
1	@evb.edit	32.263158	115.448,750000	0,002175
2	@user8680834318577	*N/A*	5.263,377049	0,002217
3	@fuhui4215	170.052,000000	46.532,725806	0,000547
4	@footcr7fc	4.135,400000	151.117,562500	0,000193
5	@maajid_cade_	48.834,500000	26.366,283333	0,000614
6	@yvfw07909258	*N/A*	2.170,944444	0,006390
7	@h205yyh	402.896104	3.742,376147	0,003514
8	@_thiennkimz	21.017094	1.373,634921	0,051240

9	@luysacr	913.666667	42.606,409091	0,008026
10	@el_libro_de_lo_oculto	543.685535	1.994,202749	0,006733
11	@bebot.1234	114.772727	8.090,000000	0,000792
12	@iapiaia	1.711599	*N/A*	0,000000
13	@tio.huesitos2	246.839416	47.411,437500	0,000473
14	@user5932285756265	0,206030	16.250000	0,032520
15	@daya.nara_28	720.871795	*N/A*	0,000000
16	@soniamoss88	14.421811	1.157,989899	0,004708
17	@wxdx1015	*N/A*	949.305936	0,006948
18	@pk.cat.fun3	5.834,500000	1.046,964286	0,019196
19	@an0ther32	4.234694	*N/A*	0,000000
20	@bot45174	41.542857	*N/A*	0,000000

Fuente: Elaboración propia.

Rangos para clasificación acorde a indicadores derivados

Para establecer los rangos de clasificación de los indicadores, se emplearon los cuartiles Q1 y Q3 como puntos de referencia estadísticos dentro de la muestra analizada. El primer cuartil (Q1) corresponde al valor por debajo del cual se encuentra aproximadamente el 25 % de las observaciones, mientras que el tercer cuartil (Q3) delimita el 75 % de las observaciones. La mediana (Q2) representa el valor central de la distribución, es decir, el punto que divide la muestra en dos partes iguales. A partir de estos valores se establecieron tres niveles relativos de comportamiento:

Tabla 9.

Criterios de clasificación de los indicadores.

Nivel	Detalle
Bajo	≤ Q1
Moderado	> Q1 y < Q3
Alto	> Q3

Fuente: Elaboración propia.

Cálculo de Q1, Mediana y Q3

Una vez obtenidos los valores individuales de cada perfil, los resultados válidos de cada indicador fueron ordenados de menor a mayor. Posteriormente, se calcularon el primer cuartil (Q1), la mediana (Q2) y el tercer cuartil (Q3), correspondientes a los percentiles 25, 50 y 75, respectivamente. De esta manera, los cuartiles representan puntos de referencia relativos a la distribución de los perfiles analizados y no valores calculados individualmente para cada perfil. Para el cálculo de los cuartiles y mediana se empleó CUARTIL.INC en Excel:

$R_{S/CS}$ = [32.263158, N/A, 170.052,000000, 4.135,400000, 48.834,500000, N/A, 402.896104, 21.017094, 913.666667, 543.685535, 114.772727, 1.711599, 246.839416, 0,206030, 720.871795, 14.421811, N/A, 5.834,500000, 4.234694, 41.542857]

Q1 = CUARTIL.INC(rango;1)

Mediana = MEDIANA(rango)

Q3 = CUARTIL.INC(rango;3)

Tabla 10.

Estadísticos descriptivos: Q1, mediana y Q3.

Variable	Bajo	Moderado	Alto
$R_{S/CS}$	≤ 21,02	> 21,02 y ≤ 4.135,40	> 4.135,40
$R_{MGA/VP}$	≤ 1.900,95	> 1.900,95 y ≤ 45.637,99	> 45.637,99
$R_{VP/S}$	≤ 0,000547	> 0,000547 y ≤ 0,007218	> 0,007218

Fuente: Elaboración propia.

Clasificación de los perfiles

Aplicando los rangos establecidos en la Tabla 9, cada perfil fue clasificado según el comportamiento observado en los tres indicadores derivados. La clasificación no constituye por sí misma una determinación de autenticidad o falsedad, sino un mecanismo de priorización para las etapas posteriores de análisis.

Tabla 11.

Clasificación de los perfiles según indicadores derivados.

N.º	Identificador	$R_{S/CS}$	$R_{MGA/VP}$	$R_{VP/S}$
1	*@evb.edit*	Moderado	Alto	Moderado
2	@user8680834318577	N/A	Moderado	Moderado
3	*@fuhui4215*	Alto	Alto	Bajo
4	*@footcr7fc*	Moderado	Alto	Bajo
5	@maajid_cade_	Alto	Moderado	Moderado
6	@yvfw07909258	N/A	Moderado	Moderado
7	@h205yyh	Moderado	Moderado	Moderado
8	*@_thiennkimz*	Bajo	Bajo	Alto
9	*@ luysacr*	Moderado	Moderado	Alto

10	@el_libro_de_lo_oculto	Moderado	Moderado	Moderado
11	@bebot.1234	Moderado	Moderado	Moderado
12	@iapiaia	Bajo	N/A	Bajo
13	@tio.huesitos2	Moderado	Alto	Bajo
14	@ *user59322857562 65*	Bajo	Bajo	Alto
15	@ daya.nara_28	Moderado	N/A	Bajo
16	@soniamoss88	Bajo	Bajo	Moderado
17	*@wxdx1015*	N/A	Bajo	Alto
18	*@ pk.cat.fun3*	Alto	Bajo	Alto
19	*@an0ther32*	Bajo	N/A	Bajo
20	*@ bot45174*	Moderado	N/A	Bajo

Fuente: Elaboración propia.

La priorización para la segunda valoración se realizó mediante la integración de los resultados cuantitativos de los indicadores derivados y las observaciones cualitativas registradas durante la caracterización inicial. Por tanto, la presencia de un perfil en esta etapa no implica necesariamente que haya obtenido valores extremos en los tres indicadores, sino que presentó una combinación de características que justificó una revisión contextual adicional.

Tabla 12.

Perfiles priorizados para la segunda valoración.

N.º	Identificador	Indicadores relevantes
3	@fuhui4215	S/CS alto; MGA/VP alto; VP/S bajo
4	@footcr7fc	S/CS alto; MGA/VP alto; VP/S bajo
8	@_thiennkimz	S/CS bajo; VP/S alto
9	@luysacr	VP/S alto
14	@user5932285756265	S/CS bajo; VP/S alto
17	@wxdx1015	CS = 0; VP/S alto

18	@pk.cat.fun3	S/CS alto; VP/S alto
19	@an0ther32	S/CS bajo; VP/S bajo
20	@bot45174	VP/S bajo

Fuente: Elaboración propia.

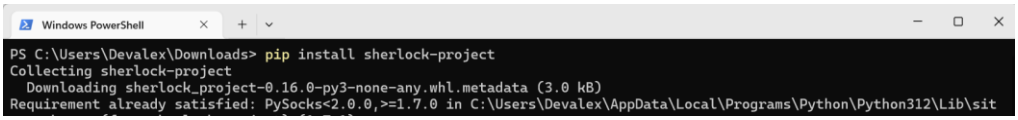
Los indicadores utilizados son señales estadísticas relativas a la muestra y no constituyen evidencia suficiente para establecer por sí solos la autenticidad o falsedad de una cuenta. Por esta razón, los perfiles priorizados fueron sometidos a una segunda valoración mediante análisis relacional y verificación visual.

Verificación de presencia de identificadores en entidades digitales externas

Como segunda etapa de verificación, se realizó una búsqueda de posibles relaciones entre los perfiles priorizados y otras entidades digitales mediante Sherlock, herramienta OSINT orientada a la recuperación de información de usuario mediante nombres o identificadores de usuarios como término de búsqueda, dicha exploración la realiza en una gran base de datos compuesta por diversos sitios web y plataformas de redes sociales. Sherlock está programado en Python por lo que puede ser instalado directamente a través del comando *pip install sherlock* desde la CMD.

Figura 3.

Instalación de Sherlock desde CMD.



Posteriormente para ejecutar un análisis para los nueve perfiles y visualizar las relaciones con otras cuentas en redes sociales, se debe colocar en la misma terminal de comandos, lo siguiente: *sherlock fuhui4215 footcr7fc thiennkimz luysacr user5932285756265 wxdx1015 pk.cat.fun3 an0ther32 bot45174*

Figura 4.

Ejecución de Sherlock para verificar coincidencias de identificadores con redes y sitios web externos.

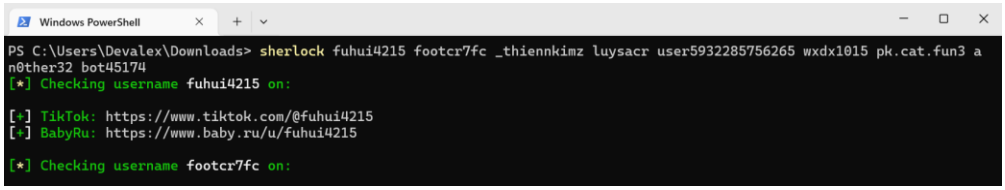


Tabla 13.

Coincidencias de identificadores con redes y sitios web externos mediante Sherlock.

N.º	Identificador	Sitio o plataforma	URL reportada
3	@fuhui4215	TikTok	tiktok.com/@fuhui4215
		BabyRu	baby.ru/u/fuhui4215
4	@footcr7fc	TikTok	tiktok.com/@footcr7fc

		YouTube	youtube.com/@footcr7fc
		BabyRu	baby.ru/u/footcr7fc
8	@_thiennkimz	BoardGameGeek	boardgamegeek.com/user/_thiennkimz
		Chess.com	chess.com/member/_thiennkimz
		TikTok	tiktok.com/@_thiennkimz
		omg.lol	_thiennkimz.omg.lol
		BabyRu	baby.ru/u/_thiennkimz
9	@luysacr	RuneScape	apps.runescape.com/.../luysacr
		Scratch	scratch.mit.edu/users/luysacr
		TikTok	tiktok.com/@luysacr
		Pinterest	pinterest.com/luysacr/
		BabyRu	baby.ru/u/luysacr
14	@user5932285756265	TikTok	tiktok.com/@user5932285756265
17	@wxdx1015	TikTok	tiktok.com/@wxdx1015
18	@pk.cat.fun3	Blitz Tactics	blitztactics.com/pk.cat.fun3
		BoardGameGeek	boardgamegeek.com/user/pk.cat.fun3
		Patched	patched.sh/User/pk.cat.fun3
		TikTok	tiktok.com/@pk.cat.fun3
		Vero	vero.co/pk.cat.fun3
		Mastodon.cloud	mastodon.cloud/@pk.cat.fun3
		Mastodon.social	mastodon.social/@pk.cat.fun3
		Mastodon.xyz	mastodon.xyz/@pk.cat.fun3
		mstdn.social	mstdn.social/@pk.cat.fun3
		mstdn.io	mstdn.io/@pk.cat.fun3
		omg.lol	pk.cat.fun3.omg.lol
		social.tchncs.de	social.tchncs.de/@pk.cat.fun3
19	@an0ther32	TikTok	tiktok.com/@an0ther32
20	@bot45174	TikTok	tiktok.com/@bot45174

Fuente: Elaboración propia a partir de los resultados obtenidos mediante Sherlock.

Los resultados obtenidos mediante Sherlock permitieron identificar posibles coincidencias entre los identificadores de los nueve perfiles priorizados y cuentas o espacios digitales registrados en otras plataformas. En conjunto, se obtuvieron 31 coincidencias, distribuidas de manera desigual entre los perfiles analizados.

El perfil @pk.cat.fun3 presentó el mayor número de coincidencias, con 12 resultados, asociados con plataformas de juegos, comunidades digitales y diferentes instancias de redes sociales descentralizadas. Este resultado representa la mayor presencia externa identificada dentro del grupo analizado. Sin embargo, la cantidad de coincidencias no permite establecer por sí misma que todas las cuentas correspondan al mismo individuo, por lo que su interpretación requiere el contraste con otros elementos de identificación.

Los perfiles @_thiennkimz y @luysacr presentaron cinco coincidencias cada uno. En el primer caso se identificaron cuentas asociadas con BoardGameGeek, Chess.com, TikTok, omg.lol y BabyRu, mientras que en el segundo se encontraron coincidencias en RuneScape, Scratch, TikTok, Pinterest y BabyRu. La presencia del mismo identificador en varias plataformas constituye una evidencia de reutilización o disponibilidad del nombre de usuario en diferentes servicios, pero no permite establecer de forma aislada una relación de identidad entre las cuentas.

El perfil @footcr7fc presentó tres coincidencias, correspondientes a TikTok, YouTube y BabyRu, mientras que @fuhui4215 presentó dos coincidencias, correspondientes a TikTok y BabyRu. Los perfiles @user5932285756265, @wxdx1015, @an0ther32 y @bot45174 presentaron una coincidencia cada uno, todas correspondientes a TikTok.

Un aspecto particularmente relevante es que TikTok aparece como coincidencia en los nueve perfiles analizados. Esto debe interpretarse con cautela, puesto que el identificador utilizado como entrada corresponde precisamente al nombre de usuario de los perfiles analizados en TikTok. Por tanto, esta coincidencia confirma la presencia del identificador en la plataforma de origen, pero no constituye evidencia independiente de una relación con una entidad externa.

En consecuencia, los resultados de Sherlock fueron utilizados principalmente como evidencia de apoyo para la identificación de posibles huellas digitales externas. Las coincidencias obtenidas fueron consideradas señales que requerían una comprobación adicional, especialmente mediante elementos que permitieran establecer una mayor correspondencia entre las cuentas, como fotografías de perfil, nombres visibles, descripciones, contenidos publicados u otros elementos visuales.

Dado que la coincidencia de un identificador no constituye evidencia suficiente para establecer correspondencia entre identidades digitales, se realizó una tercera comprobación orientada a determinar si existían coincidencias visuales entre las imágenes asociadas a los perfiles analizados y otros recursos disponibles públicamente. Para ello se empleó Google Lens.

Verificación de identidad visual mediante Google Lens

El procedimiento consistió en seleccionar las imágenes de perfil y, cuando fue pertinente, otras imágenes representativas disponibles públicamente en los nueve perfiles priorizados. Cada imagen fue introducida individualmente en Google Lens y se revisaron los resultados visualmente similares y las páginas web en las que aparecían imágenes coincidentes o relacionadas, ver tabla 14.

Tabla 14.

Resultados de verificación mediante Google Lens.

N.º	Identificador	Imagen analizada	Coincidencia visual	Observación
3	@fuhui4215		No	Solo aparece como imagen de la cuenta de TikTok.
4	@footcr7fc		Si	Aparece como imagen de una cuenta de TikTok: @daniii6750.

8	@_thiennkimz		Si	Aparece en repositorios de Pinterest, Redbubble, Reddit, Meme Creator y en perfiles de TikTok como: @user870631684730, @jonaisai2. Además, en un perfil de Instagram: xximsomagik.
9	@luysacr		No	Solo aparece como imagen de la cuenta de TikTok.
14	@user5932285756265		No	Solo aparece como imagen de la cuenta de TikTok.
17	@wxdx1015		Si	Aparece en otros perfiles de TikTok como: @golkaxkxy8y, @willowkor6773, @user9856252928, @axzddmmo, @user801794618656, @moviessyyyy0, @lvyduet, @rydn4437lmi.
18	@pk.cat.fun3		Si	Aparece en repositorios de Pinterest, Pexels, MyTv y MN2S. Además, en un perfil de Fiverr: Shadhn.
19	@an0ther32		Si	Aparece en un perfil de LinkedIn: Nur Syamimi. También aparece en Instagram como NurSaidah.
20	@bot45174		Si	Aparece en repositorios de Pinterest y Threads.

Fuente: Elaboración propia a partir de los resultados obtenidos mediante Google Lens.

Triangulación de evidencias

Tabla 15.

Triangulación de evidencias.

N.º	Identificador	Evidencia de caracterización	Sherlock	Google Lens	Convergencia de evidencias	Nivel de evidencia
3	@fuhui4215	S/CS alto; MGA/VP alto.	2 coincidencias: TikTok y BabyRu	No se identificaron coincidencias visuales externas.	Coincidencia nominal externa sin	Moderada

					correspondencia visual.	
4	@footcr7fc	S/CS alto; MGA/VP alto; VP/S bajo.	3 coincidencias: TikTok, YouTube y BabyRu	La imagen aparece asociada a otra cuenta de TikTok (@daniii6750).	Coincidencia de identificador y coincidencia visual, aunque asociadas a identificadores diferentes.	Alta
8	@_thiennkimz	S/CS bajo; VP/S alto.	5 coincidencias: BoardGameGeek, Chess.com, TikTok, omg.lol y BabyRu	Coincidencias en Pinterest, Redbubble, Reddit, Meme Creator, TikTok e Instagram.	Convergencia entre presencia externa del identificador y reutilización de la imagen en múltiples sitios.	Alta
9	@luysacr	VP/S alto.	5 coincidencias: RuneScape, Scratch, TikTok, Pinterest y BabyRu	No se identificó coincidencia visual; imagen correspondiente a Cristiano Ronaldo generada con IA.	Presencia externa del identificador, sin correspondencia visual con una identidad personal.	Moderada
14	@user5932285756265	S/CS bajo; MGA/VP bajo; VP/S alto.	1 coincidencia: TikTok	No se identificaron coincidencias visuales externas.	Evidencia limitada a la plataforma de origen.	Baja
17	@wxdx1015	CS = 0; VP/S alto.	1 coincidencia: TikTok	La imagen aparece asociada a cuentas de TikTok: @golkaxkxy8y, @willowkor6773, @user9856252928, @axzddmmo, @user801794618656, @moviessyyyy0, @lvyduet, @rydn4437lmi.	Evidencia limitada a la plataforma de origen.	Alta

18	@pk.cat.fun3	S/CS alto; VP/S alto.	12 coincidencias en diferentes plataformas	Coincidencias en Pinterest, Pexels, MyTv y MN2S. Además, en un perfil de Fiverr denominado Shadhn.	Amplia presencia externa del identificador y coincidencias visuales en diferentes sitios.	Alta
19	@an0ther32	S/CS bajo; VP = 0.	1 coincidencia: TikTok	Imagen localizada en LinkedIn (Nur Syamimi) e Instagram (NurSaidah).	Coincidencia visual externa sin coincidencia nominal directa.	Moderada
20	@bot45174	VP = 0.	1 coincidencia: TikTok	Coincidencias en repositorios de Pinterest y Threads.	Evidencia limitada a la plataforma de origen.	Moderada

Fuente: Elaboración propia a partir de los resultados obtenidos mediante Tikmatrix, Sherlock y Google Lens.

La triangulación de evidencias permitió establecer diferentes niveles de convergencia entre los indicadores de caracterización, las coincidencias de identificadores obtenidas mediante Sherlock y las coincidencias visuales mediante Google Lens. Los perfiles @footcr7fc, @_thiennkimz, @wxdx1015 y @pk.cat.fun3 alcanzaron un nivel de evidencia alto, debido a la presencia simultánea de indicadores de comportamiento atípico, coincidencias externas del identificador y/o reutilización de imágenes en otras plataformas. En contraste, @fuhui4215, @luysacr, @an0ther32 y @bot45174 presentaron un nivel moderado, mientras que @user5932285756265 mostraron un nivel bajo por la limitada convergencia de evidencias independientes.

En función de la triangulación realizada, se consideran potencialmente falsos los perfiles clasificados con un nivel de evidencia alto, específicamente @footcr7fc, @_thiennkimz, @wxdx1015 y @pk.cat.fun3, debido a que concentran evidencias convergentes provenientes de diferentes fuentes y dimensiones de análisis. Estos resultados indican una mayor probabilidad de que dichos perfiles presenten características incompatibles con una identidad auténtica o un uso original de sus elementos identificativos y visuales.

Discusiones

La caracterización inicial permitió identificar diferencias en las relaciones entre seguidores y cuentas seguidas, me gusta acumulados y videos publicados. Este enfoque coincide con investigaciones recientes que emplean características estructurales, conductuales y de perfil para la detección de cuentas falsas, destacando variables como seguidores, cuentas seguidas y cantidad de me gusta (Chelas et al., 2024).

Los indicadores derivados permitieron establecer señales relativas dentro de la muestra. En particular, la relación entre seguidores y cuentas seguidas, los me gusta por video y el volumen de publicaciones

respecto de seguidores permitieron priorizar perfiles con comportamientos atípicos. Lo que afirma Goyal et al. (2025), sobre la utilidad de combinar variables relacionadas con la actividad y las características del perfil para mejorar la identificación de cuentas potencialmente falsas.

La aplicación de Sherlock amplió la caracterización al identificar coincidencias de los nombres de usuario en diferentes plataformas. Se obtuvieron 31 coincidencias entre los nueve perfiles priorizados, destacando @pk.cat.fun3 con 12 resultados, @_thiennkimz, @wxdx1015 y @luysacr con cinco cada uno. No obstante, la coincidencia de un identificador no demuestra que las cuentas pertenezcan a una misma persona, debido a que los nombres de usuario pueden ser reutilizados o registrados independientemente.

La verificación mediante Google Lens permitió complementar el análisis nominal mediante evidencia visual. Las coincidencias encontradas en perfiles como @footcr7fc, @_thiennkimz, @wxdx1015, @pk.cat.fun3 y @an0ther32 incrementaron la convergencia de evidencias, mientras que la ausencia de coincidencias externas en otros perfiles limitó su nivel de evidencia. La utilidad de la búsqueda inversa para contrastar imágenes asociadas con identidades digitales ha sido documentada en investigaciones sobre verificación de identidades y fraude en línea (Cross & Layt, 2022).

En consecuencia, la triangulación permitió diferenciar los perfiles según el grado de convergencia entre evidencias cuantitativas, nominales y visuales. Los perfiles @footcr7fc, @_thiennkimz, @wxdx1015 y @pk.cat.fun3 alcanzaron un nivel alto debido a la presencia simultánea de señales de comportamiento atípico y evidencias externas y/o visuales.

Conclusiones

A partir de los resultados obtenidos mediante la caracterización inicial, el cálculo de indicadores derivados y la triangulación de evidencias mediante Tikmatrix, Sherlock y Google Lens, se establecieron los principales hallazgos:

La caracterización inicial permitió identificar diferencias en identidad, audiencia, actividad e interacción, generando señales útiles para priorizar perfiles que requerían una revisión adicional. Los indicadores derivados y los cuartiles permitieron clasificar los perfiles en niveles bajo, moderado y alto; sin embargo, estos resultados son relativos a la muestra y no determinan por sí mismos la falsedad de una cuenta.

Sherlock permitió identificar coincidencias de identificadores en plataformas externas, mientras que Google Lens aportó evidencia visual complementaria. Estas fuentes fueron interpretadas como elementos de apoyo y no como pruebas concluyentes de identidad. La triangulación de evidencias permitió identificar cuatro perfiles con nivel alto: @footcr7fc, @_thiennkimz, @wxdx1015 y @pk.cat.fun3, considerados potencialmente falsos debido a la mayor convergencia de evidencias cuantitativas, nominales y visuales.

Recomendaciones

Con base en los hallazgos obtenidos y en las limitaciones identificadas durante el proceso de análisis, se plantean las siguientes recomendaciones:

Aplicar la metodología de forma escalonada, utilizando inicialmente los indicadores cuantitativos para priorizar perfiles y posteriormente Sherlock y Google Lens para profundizar la verificación.

.

Interpretar los resultados como niveles de evidencia o sospecha, evitando considerar un único indicador o coincidencia como prueba definitiva de falsedad.

Ampliar futuras investigaciones mediante muestras de mayor tamaño, con el propósito de obtener puntos de corte estadísticos más robustos y representativos.

Incorporar otras fuentes de evidencia, como antigüedad de la cuenta, patrones de publicación y características del contenido, para fortalecer la triangulación y mejorar la valoración de los perfiles.

Agradecimientos

Expreso mi más sincero agradecimiento a mi tutor de trabajo de investigación por su valiosa orientación, dedicación y constante acompañamiento durante el desarrollo de este estudio. Sus conocimientos, observaciones y sugerencias fueron fundamentales para fortalecer el rigor académico y la calidad del presente trabajo.

Referencias Bibliográficas

Aguessy, A. & Fandy, R. (2025). Identity Construction in the Digital Age: The Impact of Social Media on American Cultural Dynamics. Advances in Social Sciences and Management, 3(6), 55–72. https://doi.org/10.63002/assm.306.1184

Arias, J. (2022). Guía para elaborar la operacionalización de variables. Espacio I+D, Innovación más Desarrollo, 10(28). https://www.espacioimasd.unach.mx/index.php/Inicio/article/view/274

Bokolo, B. & Liu, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 13(9), 1671. https://doi.org/10.3390/electronics13091671

Browne, T., Abedin, M. & Chowdhury, M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. International Journal of Information Security, 23(4), 2911–2938. https://doi.org/10.1007/s10207-024-00868-2

Campos, M., Moreno, R. & Jiménez, B. (2025). Detección de fraudes y estafas basadas en ingeniería social en Ecuador. Revista InveCom, 5(3), e050337. https://doi.org/10.5281/zenodo.14263156

Chelas, S., Routis, G. & Roussaki, I. (2024). Detection of fake Instagram accounts via machine learning techniques. Computers, 13(11), 296. https://doi.org/10.3390/computers13110296

Cross, C. & Layt, R. (2022). I suspect that the pictures are stolen: Romance fraud, identity crime, and responding to suspicions of inauthentic identities. Social Science Computer Review, 40(4), 955–973. https://doi.org/10.1177/0894439321999311

Constantinescu, V. (2025). Cómo detectar un perfil falso en redes sociales. Bitdefender. https://www.bitdefender.com/es-es/blog/hotforsecurity/como-detectar-un-perfil-falso-en-redes-sociales

Díaz, J., Asencio, V., Luzarraga, E. & Tapia, J. (2025). Redes sociales y desinformación en la era digital frente al reto de los algoritmos y la verificación de información. Dominio De Las Ciencias, 11(3), 117–134. https://doi.org/10.23857/dc.v11i3.4452

Dube, B., Nkomo, D. & Apadile, M. (2024). Pragmatism: An essential philosophy for mixed methods research in education. International Journal of Research and Innovation in Social Science (IJRISS), 8(3), 1001–1010. https://doi.org/10.47772/IJRISS.2024.803073

Giménez, S. (2023). Redes sociales: estado actual y tendencias 2023. OBS Business School. https://marketing.onlinebschool.es/Prensa/Informe%20OBS%20Tendencias%20Redes%20Sociales%202023.pdf

Goyal, B., Gill, N. S., Gulia, P., Alduaiji, N., Shukla, P. K., Shukla, P. & J., S. (2025). Instagram fake profile detection using an ensemble learning method. Scientific Reports, 15, Article 26464. https://doi.org/10.1038/s41598-025-03973-x

Hargreaves, C., Nelson, A. & Casey, E. (2024). An abstract model for digital forensic analysis tools: A foundation for systematic error mitigation analysis. Forensic Science International: Digital Investigation, 48, 301679. https://doi.org/10.1016/j.fsidi.2023.301679

Hayawi, K., Saha, S., Masud, M., Mathew, S. & Kaosar, M. (2023). Social media bot detection with deep learning methods: a systematic review. Neural Comput & Applic, 35, 8903–8918. https://doi.org/10.1007/s00521-023-08352-z

Hernández, N. & Klimenko, O. (2025). Metodología de la investigación, enfoque cualitativo, cuantitativo y mixto. Nexus: Multidisciplinary Research Journal (MIR), 2(3), 1–19. https://nexushouseeditorial.com/index.php/nexus/article/view/24

Hidalgo, I., Yasaca, S., Hidalgo, B., Oquendo, V. & Salazar, F. (2018). Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales. European Scientific Journal, 14(18), 40–48. https://doi.org/10.19044/esj.2018.v14n18p40

Jordán, D., Izaguirre, J. & López, A. (2024). La red social Tik Tok y su incidencia en el cambio de comportamiento: un estudio bibliométrico. Intersecciones En Comunicación, 2(18), 1–23. https://ojsintcom.unicen.edu.ar/ojs/article/view/219

Laffier, J. & Westley, M. (2025). Digital Identity Congruence: Exploring the Importance of Congruent Online Identities for Adolescents. En The Evolving Landscape of Online Identity - Recent Studies and Insights. IntechOpen. https://doi.org/10.5772/intechopen.1012336

Li, Y., Zhang, H., Liu, Y. & Wang, X. (2023). Deep learning-based intrusion detection for Internet of Things networks. IEEE Access, 11, 83645–83656. https://doi.org/10.1109/ACCESS.2023.3305568

López Navarrete, A., Cisternas Osorio, R., Díez Somavilla, R. & Cabrera Méndez, M. (2024). La interacción del usuario en TikTok: el engagement según la tipología de contenido. Tsafiqui - Revista Científica En Ciencias Sociales, 14(1). https://doi.org/10.29019/tsafiqui.v14i22.1200

Martín, M., Price, R., Alqunaysi, R., Barrera, A., Macías, E., Ray, D. & Shannon, E. (2026). Características de la investigación cualitativa en comportamiento. Behavior Analysis in Practice, 1–18. https://doi.org/10.1007/s40617-025-01144-y

Meng, L., Kou, S., Duan, S. & Bie, Y. (2024). The impact of content characteristics of short-form video ads on consumer purchase behavior: Evidence from TikTok. Journal of Business Research, 183, 114874. https://doi.org/10.1016/j.jbusres.2024.114874

Moncada, J. & Miranda, A. (2025). La influencia de las redes sociales en los delitos cibernéticos y los desafíos para la Legislación en Ecuador. RICEd: Revista De Investigación En Ciencias De La Educación, 3(5), 15–28. https://doi.org/10.53877/riced3.5-2

Orellana, G. & Cotera, G. (2025). Evaluación de privacidad y seguridad de datos de usuarios en redes sociales. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 7(5), 87–110. https://doi.org/10.59169/pentaciencias.v7i5.1641

Prado, W. (2025). Tik Tok y el periodismo digital: Impacto en el consumo de noticias en Cuenca, Ecuador. Pacha: Revista De Estudios Contemporáneos Del Sur Global, 6(18), e250372. [https://doi.org/10.46652/pacha.v6i18.372

Reyes, A. (2025). Redes sociales: entre la información y la desinformación en la era digital. Universita Ciencia, 13(36), 84–94. https://dialnet.unirioja.es/servlet/articulo?codigo=10108565

Rubio, F., González, E. & Olivo, J. (2024). Adolescentes en la era digital. Desvelando las relaciones entre las redes sociales, el autocontrol, la autoestima y las habilidades sociales. Ciencia y Educación, 8(3), 39–58. https://doi.org/10.22206/cyed.2024.v8i3.3209

Sarkar, G. & Shukla, S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 2, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Villavicencio, C., Rodríguez, A., Vélez, Á. & Zambrano, A. (2025). Riesgo en el uso de las redes sociales. Revista Científica De Informática ENCRIPTAR, 8(16), 109–130. https://doi.org/10.56124/encriptar.v8i16.006

Vintimilla, R. & Erazo, C. (2025). Impact of TikTok interactive content strategies on university engagement. Runas: Journal of Education and Culture, 6(12), e250238. https://doi.org/10.46652/runas.v6i12.238

Wang, Z. (2025). Negotiation, transformation, and reinforcement: The role of social media in shaping collective identity. Proceedings of ICADSS 2025 Symposium, 15–21. https://doi.org/10.54254/2753-7064/2025.BJ26816

Wekesa, E., DeCusatis, C. & Zhu, A. (2023). A Black Box Comparison of Machine Learning Reverse Image Search for Cybersecurity OSINT Applications. Electronics, 12(23), 4822. https://doi.org/10.3390/electronics12234822

Wu, J., Guo, J. & Hooi, B. (2023). Fake news in sheep's clothing: Robust fake news detection against LLM-empowered style attacks. arXiv. https://doi.org/10.48550/arXiv.2310.10830

Yadav, A., Kumar, A. & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 1–32. https://doi.org/10.1007/s10462-023-10454-y

Zalazar, A. (2024). El Uso de Técnicas de Ingeniería Social Integradas a Inteligencia Artificial para Atacar Objetivos. JAIIO, Jornadas Argentinas De Informática, 10(7), 44–52. https://revistas.unlp.edu.ar/JAIIO/article/view/17897

Zhang, Z., Qiu, K. & Ye, Y. (2025). Influence of audiovisual features of short video advertising on consumer engagement behaviors: Evidence from TikTok. Journal of Business Research, 201, 115662. https://doi.org/10.1016/j.jbusres.2025.115662

Zouzou, Y. & Varol, O. (2024). Unsupervised detection of coordinated fake-follower campaigns on social media. EPJ Data Science, 13(1), 62. [https://doi.org/10.1140/epjds/s13688-024-00499-6