

Javier Alejandro Ochoa-Vallejo; Brayan Gabriel Taday-Guamán; Michell Stefanya Zurita-Delgado

[DOI 10.35381/cm.v12i1.2143](https://doi.org/10.35381/cm.v12i1.2143)

## **Estafas en redes sociales y su relación con el delito cibernético. Ecuador**

### **Social Media Scams and Their Link to Cybercrime. Ecuador**

Javier Alejandro Ochoa-Vallejo  
[javierov39@uniandes.edu.ec](mailto:javierov39@uniandes.edu.ec)  
Universidad Regional Autónoma de los Andes; Riobamba, Chimborazo  
Ecuador  
<https://orcid.org/0009-0001-6534-896X>

Brayan Gabriel Taday-Guamán  
[brayantg95@uniandes.edu.ec](mailto:brayantg95@uniandes.edu.ec)  
Universidad Regional Autónoma de los Andes; Riobamba, Chimborazo  
Ecuador  
<https://orcid.org/0009-0006-3578-2809>

Michell Stefanya Zurita-Delgado  
[us.michellezd90@uniandes.edu](mailto:us.michellezd90@uniandes.edu)  
Universidad Regional Autónoma de los Andes; Riobamba, Chimborazo  
Ecuador  
<https://orcid.org/0009-0000-3193-8024>

Recepción: 15 de diciembre 2025  
Revisado: 26 de febrero 2026  
Aprobación: 15 de marzo 2026  
Publicado: 01 de abril 2026

## **RESUMEN**

El objetivo general de la investigación fue analizar las estafas en redes sociales y su relación con el delito cibernético. Ecuador. El planteamiento realizado por los investigadores para el desarrollo del método, es mediante la indagación, recolección y análisis crítico documental y referencial bibliográfico, basándose en la exploración metódica, rigurosa y profunda de diversas fuentes documentales conformadas por artículos arbitrados, leyes e instituciones. Se empleó como técnica la revisión documental. Se recurrió, además, al método inductivo-deductivo. Además, se realizó una serie de entrevistas, estas permitieron obtener perspectivas diversas sobre las estafas en redes sociales y su relación con el delito cibernético. En conclusión, los fraudes digitales representan un serio desafío contemporáneo para la sociedad ecuatoriana. Al tener un mayor acceso a medios digitales, las personas están más vulnerables que nunca a caer en trampas y fraudes. Por esta razón, es urgente que las plataformas digitales actualicen sus sistemas de protección.

**Descriptores:** Plataforma digital; protección de datos; ley. (Tesauro UNESCO)

## **ABSTRACT**

The overall objective of the research was to analyze scams on social media and their relationship to cybercrime in Ecuador. The researchers' approach to developing the methodology involved inquiry, data collection, and critical analysis of documents and bibliographic references, based on a methodical, rigorous, and in-depth exploration of various documentary sources, including peer-reviewed articles, laws, and institutional documents. A literature review was employed as the primary research technique. The inductive-deductive method was also employed. Additionally, a series of interviews was conducted, which provided diverse perspectives on social media scams and their relationship to cybercrime. In conclusion, digital fraud represents a serious contemporary challenge for Ecuadorian society. With greater access to digital media, people are more vulnerable than ever to falling into traps and scams. For this reason, it is urgent that digital platforms update their protection systems.

**Descriptors:** Digital platform; data protection; law. (UNESCO Thesaurus)

## **INTRODUCCIÓN**

Los engaños en plataformas sociales son delitos en el ámbito digital que intentan estafar a personas a través de internet, con el objetivo de obtener dinero, información personal o acceso no autorizado a cuentas y sistemas. Las cifras precisas registran 10. 678 noticias de delitos (NDD) y afectados por fraudes entre los meses de enero y mayo de 2024. De este total, hay 3. 262 en la ciudad capital, 1. 757 en Guayaquil, 539 en Cuenca, y el resto se distribuye a lo largo del país. Las señales preocupantes son cada vez más visibles y, aunque en las plataformas digitales y en la comunidad se busca mejorar la capacidad para identificarlas, el índice sigue siendo elevado, sin contar los casos no denunciados. (Primicias, 2023).

El uso masivo de aplicaciones móviles y plataformas de pago en Ecuador ha superado la velocidad con la que los usuarios aprenden a protegerse, dejando una brecha de seguridad que los estafadores aprovechan mediante herramientas digitales automatizadas. Los delincuentes utilizan la información pública de los perfiles de los usuarios para personalizar las estafas y hacerlas más creíbles. (Campos Gallegos et al.,2025).

Por ello, en las últimas décadas, la digitalización ha cambiado significativamente la manera en que nos relacionamos tanto social como comercialmente, lo que ha llevado a un aumento en el uso de plataformas sociales como Facebook, Instagram y WhatsApp. No obstante, este progreso también ha abierto la puerta a nuevas formas de delitos. En Ecuador, se ha detectado un aumento en las quejas por estafas en línea, especialmente durante la crisis sanitaria del COVID-19. (Fiscalía General del Estado del Ecuador, 2020).

Las personas afectadas enfrentan pérdidas económicas, falta de privacidad y desconfianza al utilizar plataformas digitales, lo que lleva a los criminales a emplear tácticas más avanzadas, como el phishing y el hacking de alta complejidad. Hay una carencia en la formación digital de la sociedad, lo que la vuelve más susceptible a las

estafas. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

En Ecuador, se dispone de leyes para enfrentar crímenes cibernéticos, como el Código Orgánico Integral Penal (2014), que en sus artículos 178 y 232 castiga el ingreso no permitido a sistemas.

Se identifica a las redes sociales no solo como medios de comunicación, sino como herramientas de precisión para el delito. La facilidad para crear perfiles falsos y el acceso a datos personales compartidos voluntariamente por los usuarios permiten a los delincuentes diseñar engaños personalizados que tienen una alta tasa de éxito. (Sánchez Salazar et al., 2025).

Los fraudes electrónicos no siempre es sencillo señalar a un culpable. La "imputación objetiva" sirve para determinar si el resultado (el fraude) puede atribuirse legalmente a una acción específica que creó un riesgo no permitido. En el mundo digital, esto es complejo porque intervienen usuarios, bancos, plataformas y delincuentes. (Collantes Rodríguez, 2025).

Mayer Lux, & Oliver Calderón. (2020), definen el fraude informático como una modalidad donde el engaño no se dirige a una persona, sino a un sistema de procesamiento de datos, a diferencia de la estafa convencional, donde una persona engaña a otra para que esta le entregue dinero voluntariamente, en el fraude informático el delincuente manipula directamente el software o los datos para obtener un beneficio económico ilícito.

En tal sentido, la evidencia digital es volátil (puede borrarse en segundos) y fácil de alterar. Los autores destacan que la fiscalía y los jueces enfrentan retos para garantizar la "cadena de custodia" de los datos informáticos, lo que a menudo provoca que los procesos se caigan por falta de pruebas técnicas sólidas. (Enríquez-Chapi et al., 2024).

Se plantea como objetivo general de la investigación analizar las estafas en redes sociales y su relación con el delito cibernético. Ecuador.

## **MÉTODO**

El planteamiento realizado por los investigadores para el desarrollo del método, es mediante la indagación, recolección y análisis crítico documental y referencial bibliográfico, basándose en la exploración metódica, rigurosa y profunda de diversas fuentes documentales conformadas por artículos arbitrados, leyes e instituciones, describiendo los hallazgos encontrados. En la investigación, se ha empleado como técnica la revisión documental, la cual permite obtener información valiosa para encuadrar los acontecimientos, problemas y reacciones más usuales de personas y culturas que son objeto de análisis. (Sánchez et al, 2021). Se recurre, además, al método inductivo-deductivo, el cual propone que para hallar una verdad se deben escudriñar los hechos y no basarse en meras especulaciones, igualmente a partir de afirmaciones generales para llegar a las específicas. (Dávila, 2006). Además, se realiza una serie de entrevistas, estas permiten obtener perspectivas diversas sobre las estafas en redes sociales y su relación con el delito cibernético en Ecuador.

## **RESULTADOS**

Se presentan a continuación las entrevistas formuladas.

1. ¿Podría contarnos su experiencia en redes sociales en cuanto a la estafa que usted sufrió?

(Entrevista 1): “Uso redes sociales a diario y compré un celular en una página con muchas recomendaciones se veía muy confiable, pero nunca me llegó el producto y cuando fui donde las autoridades a reclamar no se procedieron a hacer nada talvez para ellos no represente mucho, pero para mí que solo soy un estudiante es dinero que me costó conseguir.” (Eddy Molina, 19 años)

Javier Alejandro Ochoa-Vallejo; Brayan Gabriel Taday-Guamán; Michell Stefanya Zurita-Delgado

(Entrevista 2): “Me escribió una cuenta de mi hermano que vive en Estados Unidos parecía muy real porque tenía incluso los mismos amigos en común, me pedía que le depositara 300 de urgencia porque había llegado al aeropuerto y se le habían perdido sus cosas entonces le di pues mi plata sacando de donde sea pidiendo prestado porque es familia decía, pero después de depositarle mi hermana le ha llamado y me dice que no ha sido el entonces ya ahí perdí mi plata mijo” (María Zapata, 46 años).

2. ¿Cómo percibe usted la seguridad en cuanto a las redes sociales para evitar las estafas?

(Entrevista 1): “Siento que por ejemplo Facebook o tik tok al ser una redes sociales tan globalizadas no toman en cuenta este tipo de estafas porque imagínate cuantas personas deben haber que sean estafadas a diario, también que hay mucha libertad en estas redes sociales cualquiera puede vender, emprender hacerse un perfil falso con la cara de algún famosos y escribir para pedir dinero, entonces de ese lado no creo que deberían limitar esa libertad sino que poner medidas cautelares para evitar mejor este tipos de estafas porque aunque pareciera poco es mucho a largo plazo” (Eddy Molina, 19 años).

(Entrevista 2): “Yo veo que no hay nada para evitar que a las personas que a veces no sabemos cómo funcionan o no sabemos identificar cuando nos están estafando, yo creo que tanto las redes sociales como el mismo gobierno debería dar capacitaciones para decirle a la gente cómo saber cuándo a uno le estafan no y uno a veces ni siquiera sabe qué hacer en ese tipo de casos” (María Zapata, 46 años).

3. ¿Cómo percibe usted el sistema legal ecuatoriano actual ante este fenómeno?

(Entrevista 1): “Sé que hay leyes que en teoría nos defienden, pero también yendo a la práctica en mi caso sé que el ladrón debe robar más del sueldo básico unificado para poder tomar medidas en contra de él y tener que estar buscando a qué personas

Javier Alejandro Ochoa-Vallejo; Brayan Gabriel Taday-Guamán; Michell Stefanya Zurita-Delgado

nomas a robado o estafado para una persona común es muy difícil tanto por el tiempo como por los recursos que se necesitan, en mi caso cuando fui a denunciar mi caso pues hasta ahí quedó” (Eddy Molina, 19 años).

(Entrevista 2): “Yo no sé qué podría hacer en caso de que me estafen cuando yo perdí mi plata lo único que quería era llorar porque había quedado endeudada, yo veo que, aunque acudiera a denunciar que podrían hacer si la cuenta después de eso desapareció viendo eso mejor no hago nada, pero sí debería haber como denunciar eso digo yo porque no he de ser solo yo sino mucha gente más” (María Zapata, 46 años).

Los participantes describieron distintos tipos de fraudes sufridos en redes sociales, por lo cual se identificaron dos modalidades que predominaron: Suplantación de identidad y ventas falsas los estafadores clonaron un perfil de conocidos para solicitar dinero, también falsas ventas y comercio engañoso: Se ofrecieron productos (electrodomésticos, celulares, ropa, vehículos) o servicios inexistentes a través de páginas fraudulentas en redes sociales.

Suplantación de Identidad en el Artículo 212 del Código Orgánico Integral Penal(2014I), se refiere al uso no autorizado de la identidad de otra persona con el fin de cometer un delito o causar daño. Los entrevistados coincidieron en que antes de la estafa tenían poca o ninguna información sobre cómo detectar fraudes digitales lo cual evidencia la falta de políticas públicas que puedan ayudar a prevenir estafas. Sin embargo, también se considera que las plataformas de redes sociales no hacen lo suficiente para prevenir estas estafas lo cual se debe a la poca regulación que tienen las mismas. Aunque existen leyes como el Código Orgánico Integral Penal que sancionan la estafa (Art. 186), en la práctica el control sobre redes sociales es difícil. Los hallazgos evidencian la creciente vulnerabilidad de los usuarios ecuatorianos ante estafas digitales en redes sociales. La falta de educación en ciberseguridad y la limitada acción de las autoridades contribuyen a la repetición de estos fraudes.

## **DISCUSIÓN**

Los hallazgos de este estudio muestran que los fraudes en redes sociales han incrementado de manera notable en años recientes, motivados por la mayor utilización de servicios como Facebook, Instagram y WhatsApp después del auge necesario que tuvo internet durante la crisis sanitaria de 2019, la sencillez con la cual los delincuentes digitales pueden generar cuentas falsas y la credibilidad que los usuarios otorgan a estas redes han promovido la difusión de timos por la vía virtual.

Uno de los descubrimientos más importantes de la investigación llevada a cabo es que las plataformas sociales, al carecer de una regulación más estricta que la impuesta por ellas mismas, no logran evitar que se produzcan delitos en línea, ya que los delincuentes utilizan este entorno para llevar a cabo fraudes digitales. Además, a pesar de las peticiones realizadas para que estas redes colaboren con las fuerzas del orden, las políticas de las compañías simplemente impiden esta cooperación, y por estas causas, resolver estos problemas se convierte en algo muy difícil y exige una gran inversión. Igualmente, las personas que fueron entrevistadas en esta investigación suelen ser individuos que no tienen un contacto frecuente con la tecnología en su vida cotidiana, así como los riesgos que esta conlleva. Además, es común que los estafadores intentan apelar a las emociones de sus víctimas, utilizando ya sea promesas tentadoras o creando perfiles falsos que aparentan ser de familiares. Tras ser víctimas de fraude, todos los participantes expresan una sensación de abandono por parte del sistema de justicia actual, lo que indica que hay aspectos que no funcionan bien y que es necesario modificar o actualizar las leyes. Esto es especialmente relevante en un país donde la crisis económica persiste y más personas enfrentan este fenómeno, generalmente ignorado a lo largo de estos años.

Es importante considerar los factores que contribuyen al aumento de este fenómeno, tales como la pobreza, el desempleo, la ausencia de políticas públicas adecuadas y la falta de seguridad además un incremento del uso de las redes sociales y el internet en sí después de la pandemia del 2019. Esto revela no solo una falta de atención hacia ciertas áreas de la población, sino también una grave crisis que Ecuador enfrenta actualmente además de la poca atención que se le da a dicho fenómeno a la hora de atender estas necesidades.

Se evidencia que La suplantación de identidad, venta de productos y ofertas de trabajo dando como resultado que los estafadores usan las necesidades de las personas además de aprovechar la deficiencia de seguridad en las plataformas, así como de las autoridades competentes para cometer estafas por otro lado el modus operandi de este tipo de estafas por lo general apuntan al lado sentimental como suplantación de identidad o necesidades que tengan las personas como productos o servicios.

Aunque este estudio proporciona información útil sobre cómo operan los estafadores y cómo las víctimas perciben estos fraudes, hubo una limitación importante: no se pudo analizar casos en tiempo real debido a las políticas de privacidad de las redes sociales. Para futuras investigaciones, sería ideal crear herramientas que detecten automáticamente perfiles falsos y desarrollar programas educativos enfocados en las personas más propensas a ser engañadas.

## **CONCLUSIONES**

Los fraudes digitales representan un serio desafío contemporáneo para la sociedad ecuatoriana. Al tener un mayor acceso a medios digitales, las personas están más vulnerables que nunca a caer en trampas y fraudes. Por esta razón, es urgente que las plataformas digitales actualicen sus sistemas de protección. Además, es fundamental establecer nuevas medidas de seguridad para los usuarios. Las entrevistas indican que, aunque este fenómeno es significativo, también es bastante subestimado por las

instituciones de protección correspondientes.

## **FINANCIAMIENTO**

No monetario.

## **AGRADECIMIENTO**

A la Universidad Regional Autónoma de los Andes, en el desarrollo de la investigación.

## **REFERENCIAS CONSULTADAS**

- Asamblea Nacional (2014). Código Orgánico Integral Penal. Registro Oficial N° 180. <https://url2.cl/53c6h>
- Campos Gallegos, M., Moreno Dillon, R., & Jiménez Espín, 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>
- Collantes Rodríguez, K. (2025). La imputación objetiva frente a los fraudes electrónicos: evidencia de reformas normativas en un estudio de revisión sistemática. *Aula Virtual*, 6(13), e571. <https://doi.org/10.5281/zenodo.17443011>
- Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. *Laurus*, 12(Ext),180-205. <https://n9.cl/nx847>
- Enríquez-Chapi, B. J., Muñoz-Chulde, D. A., Guerrón-Bracero, M. S., & Santander-Moreno, J. J. (2024). La estafa electrónica en el Sistema Penal Ecuatoriano. *IUSTITIA SOCIALIS*, 9(1), 336–345. <https://doi.org/10.35381/racj.v9i1.3581>
- Fiscalía General del Estado de Ecuador. (2023). Unidad Nacional Especializada en Investigación de Ciberdelito. <https://n9.cl/zhhvb>
- Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, 9(1), 151-184. <https://dx.doi.org/10.5354/0719-2584.2020.53447>

Javier Alejandro Ochoa-Vallejo; Brayan Gabriel Taday-Guamán; Michell Stefanya Zurita-Delgado

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). Política de Ciberseguridad. <https://n9.cl/qdrpi>

Primicias. (2023). El 8,2% de ecuatorianos son analfabetos digitales y eso los hace vulnerables a ciberdelitos. <https://n9.cl/5djh>

Primicias. (2023). Incremento de fraudes digitales en Ecuador: haga un 'checklist' de protección. <https://n9.cl/6c2cv>

Sánchez Salazar, P., Araujo Arízaga, A., & Salinas Herrera, F. (2025). Responsabilidad penal por manipulación digital con fines delictivos: Una mirada desde el derecho digital comparado en América Latina. *Cuestiones Políticas*, 43(83), 42-55. <https://doi.org/10.5281/zenodo.17756519>