

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

[DOI 10.35381/cm.v12i1.2116](https://doi.org/10.35381/cm.v12i1.2116)

El rol de las redes sociales y aplicaciones móviles en la práctica de la extorsión

The Role of Social Media and Mobile Apps in Extortion

Adelita Zarai Zabala-Ponce
adelitazp57@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador
<https://orcid.org/0009-0005-6023-4671>

Johanna Velarde-Sandy
sandymv17@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador
<https://orcid.org/0009-0005-6023-4671>

Valeria Estefanía Vicuña-Pozo
ur.valeriavp84@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador
<https://orcid.org/0000-0002-1883-8384>

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

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

RESUMEN

El objetivo de la presente investigación fue examinar las redes sociales y aplicaciones móviles en la práctica de la extorsión. La metodología llevada a cabo fue Mixto (cuantitativo y cualitativo), sobre el nivel de confianza que la población seleccionada tiene en diversos medios de difusión, tanto tradicionales como modernos. Los resultados revelaron que una gran parte de los encuestados no utiliza herramientas como la autenticación en dos pasos, la restricción de acceso a su información personal o la configuración de privacidad en sus cuentas. Esto demuestra que, aunque las plataformas digitales han implementado mecanismos de protección, la falta de educación digital sigue siendo un factor determinante en la vulnerabilidad de los usuarios. En conclusión, la prevención sigue siendo la estrategia más efectiva frente a este delito. Se recomienda implementar programas de educación digital desde edades tempranas, integrando la ciberseguridad en los planes de estudio.

Descriptor: Redes sociales; aplicación informática; delito informático; plataforma digital; protección de datos. (Tesauro UNESCO).

ABSTRACT

The objective of this study was to examine the role of social media and mobile apps in extortion. A mixed-methods approach (quantitative and qualitative) was used to assess the level of trust that the selected population has in various media outlets, both traditional and modern. The results revealed that a large proportion of respondents do not use tools such as two-step authentication, restricting access to their personal information, or privacy settings on their accounts. This demonstrates that, although digital platforms have implemented protective mechanisms, the lack of digital literacy remains a determining factor in users' vulnerability. In conclusion, prevention remains the most effective strategy against this crime. It is recommended to implement digital education programs from an early age, integrating cybersecurity into school curricula.

Descriptors: Social media; computer application; cybercrime; digital platform; data protection. (UNESCO Thesaurus).

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

INTRODUCCIÓN

La extorsión en el rol de las redes sociales en la actualidad ha ido evolucionando con el avance de la tecnología. Alrededor del mundo, las organizaciones terroristas han modificado sus actividades para adaptarse a los avances tecnológicos del mundo actual, prueba de ello en la gran adaptabilidad y difusión que han tenido sus acciones violentas a través de las redes sociales.

En el presente artículo ampliaremos esta investigación; mostrando el uso que los grupos extorsionistas han dado a las redes sociales para masificar sus acciones a través del reclutamiento, radicación de la violencia, comunicación segura, formación, ataques, dominio cognitivo, propaganda y financiamiento. A todo esto, se debe añadir el conjunto de acciones emprendidas por las organizaciones de extorsión en el rol de las redes sociales.

Sin embargo, las plataformas como Facebook, Instagram, Tik Tok, Gmail, etc. Son herramientas clave en la práctica de la extorsión, un delito que ha evolucionado junto a avances tecnológicos. A través de este análisis se ha evidenciado como el anonimato, la masividad y la accesibilidad de estas plataformas han facilitado la ejecución de actos ilícitos, afectando a individuos, empresas e instituciones a nivel global.

Se ha demostrado la necesidad de implementar efectivas que permitan combatir este problema de manera integral. Una de las formas más comunes para llevar a cabo la señalada conducta delictiva, consiste en un acercamiento por parte de una persona usuaria respecto de otra, que sin conocerse de forma previa entablan una relación de amistad en un inicio, para posteriormente sostener una relación más íntima y una vez generado este vínculo de confianza, se realiza una solicitud por parte de la persona que planea extorsionar, misma que consiste principalmente en el envío de fotografías o videos íntimos, ante dicha situación y una vez que tienen en su poder dichas imágenes o videos, comienza la extorsión, en donde se le hace saber a la víctima, que en caso de no entregar cierta cantidad de dinero, subirán a

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

las redes dichas fotos e imágenes o bien que las mismas les serán compartidas a su pareja, familiares, amigos o compañeros de trabajo (Martínez Anzures, 2021).

En la práctica de la extorsión los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático, pornografía infantil, entre otros. Para enfrentarlos, no obstante, la dificultad para descubrirlos, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. Colombia avanzó un poco en este tema con la ley 1273 de 2009 la cual implementa un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Sin embargo, este estudio permitió no solo poder comprender cómo operan los extorsionadores en los entornos digitales, sino también destacar la necesidad de políticas públicas y medidas de ciberseguridad que garanticen la protección de los datos y derechos de los usuarios en un mundo cada vez más interconectado. La importancia del estudio radica en identificar y comprender los mecanismos con los que los delincuentes utilizan redes sociales y aplicaciones móviles para extorsionar. Nuestra investigación contribuirá a identificar y comprender estos escenarios, proporcionando un enfoque crítico que facilite el diseño de estrategias para su abordaje efectivo. Si bien es cierto hoy en día las redes sociales juegan un papel importante en la forma en que las personas interactúan con otras, permitiendo que sea más fácil comunicarse con familiares, amigos o conocidos, sin importar la distancia en que se encuentre.

Se analizó la poca importancia que le dan a las redes sociales en general, puesto a que es una manera de incidir a malas acciones de carácter delictivo a través de los medios tecnológicos, que son usados con dos fines, para el bien o para el mal, como pueden ser las amenazas, usurpación de identidad, creación de perfiles que no le corresponde, entre otras (Andrade et al., 2021).

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

Según un análisis policial, el crecimiento de las cifras de extorsiones no es un problema que afecta solo a Ecuador, sino que se replica en varios lugares del mundo. Las características de los países en los que han florecido esta práctica criminal es la presencia de grupos de delincuencia organizada. Estas mafias utilizan las extorsiones como mecanismo para obtener recurso y financiamiento (Primicias, 2023).

El objetivo de esta investigación fue analizar en profundidad el rol de las redes sociales y aplicaciones móviles en la práctica de la extorsión, identificando los mecanismos empleados por los extorsionadores, las consecuencias para las víctimas y las posibles soluciones para mitigar este fenómeno. Además, se buscó proponer estrategias que contribuyan a un entorno seguro en la era digital, donde los usuarios puedan protegerse de estos riesgos y las plataformas asuman un papel activo en la prevención de este delito. Es claro que la solución al problema no es prohibir o restringir su uso, lo que se necesita es crear una cultura responsable para que los usuarios puedan navegar y utilizar sus redes de forma segura.

MÉTODO

En esta investigación se pretende recopilar datos exclusivamente Mixto (cuantitativo y cualitativo), sobre el nivel de confianza que la población seleccionada tiene en diversos medios de difusión, tanto tradicionales como modernos. A través de la recolección y análisis de estos datos pertenecientes a los miembros de la Universidad Regional Autónoma de los Andes, sede Riobamba (a partir de ahora, referida como UNIANDES), se espera obtener una comprensión más profunda de la dinámica entre los medios de comunicación y la confianza del público en el contexto ecuatoriano.

RESULTADOS

Los resultados de la investigación muestran una realidad preocupante en las redes sociales ya que la mayoría de los usuarios no le están dando el uso adecuado de las

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

redes sociales, si bien es cierto la mayoría de las personas que ocupan las redes sociales son los adolescentes, y por eso para los extorsionadores es muy fácil manipularlos, engañarlos a través de links, que los lleva a abrir y a guardar su respectiva información.

Recopilar información para robar datos no es el único motivo para usar las redes sociales para reconocimiento. La información publicada en redes sociales podría usarse para obtener contraseñas o suplantar la identidad de los usuarios empresariales. Muchas cuentas online permiten a los usuarios restablecer las contraseñas si ingresan una pregunta de seguridad. Con la suficiente información de publicaciones en redes sociales, un atacante podría adivinar la respuesta a estas preguntas de seguridad basándose en la información privada publicada por un usuario objetivo.

La investigación reveló que el rol de las redes sociales y aplicaciones móviles en la práctica de la extorsión están reclutando información de los usuarios para así poder guardarse la información y llevar a cabo una estrategia de robo de datos. Los hallazgos de la investigación resaltan la necesidad de implementar más seguridad en las aplicaciones para evitar cualquier tipo de información personal suelta.

Las redes sociales y su papel en la era digital

Las redes sociales han experimentado un rápido crecimiento desde la apareció de plataformas como Facebook, Twitter, Instagram, LinkedIn y Tik Tok. Estas redes se han convertido en lugares virtuales donde las personas pueden compartir fotos, videos y pensamientos, así como mantenerse al tanto de las últimas noticias y tendencias. Además, han permitido que las empresas y marcas se conecten con sus audiencias de manera más directa y efectiva. A medida que las redes sociales han crecido en popularidad, también han surgido preocupaciones sobre la privacidad y la seguridad en línea.

La recopilación de datos y la protección de la información personal de los usuarios han sido temas de debate. Las plataformas de redes sociales se han esforzado por

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

implementar políticas de privacidad y controles de seguridad para proteger la información de sus usuarios. Las redes sociales constituyen plataformas digitales que fomentan la interacción y el intercambio de información entre usuarios a través de Internet. Estas herramientas han revolucionado la forma en que nos comunicamos, permitiendo la creación de comunidades virtuales donde se comparten intereses, noticias y experiencias. Su uso abarca una amplia gama de áreas, incluyendo el entretenimiento, la educación, el comercio y la política, aunque también han habilitado espacios para actividades ilícitas como la extorsión.

Evolución de las redes sociales y las aplicaciones móviles

En las últimas dos décadas, hemos sido testigos de un crecimiento exponencial de las redes sociales, desde la aparición de plataformas como Facebook, Twitter e Instagram, hasta el ascenso de aplicaciones móviles como TikTok, WhatsApp y Telegram. Estos avances han facilitado la conexión entre individuos, al tiempo que han introducido nuevas amenazas. La evolución tecnológica ha propiciado la creación de perfiles falsos, el anonimato en línea y el acceso inmediato a grandes volúmenes de información, elementos que pueden ser utilizados con fines delictivos. El futuro de las redes sociales es emocionante y lleno de posibilidades. Se espera que la realidad virtual y la realidad aumentada se integren cada vez más en las plataformas, lo que permitirá experiencias más inmersivas y colaborativas. Además, las redes sociales seguirán evolucionando para adaptarse a las necesidades cambiantes de los usuarios y las tendencias tecnológicas emergentes.

Cabe recalcar que los dispositivos móviles facilitan el acceso rápido a las redes sociales, haciendo de este un medio de comunicación flexible para ser usado en cualquier momento y lugar, pero así mismo dedican mucho tiempo a estar conectado en las redes sociales olvidando sus obligaciones, y sus padres sin saber que hacen o con quien interactúan o entregan información valiosa, el objetivo principal es evitar que haya víctimas de los delitos anteriormente mencionados, pues mediante estudios se obtuvo que los delitos informáticos actualmente se los realiza por medio

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

de las plataformas antes mencionadas, a través de cuentas falsas, siendo esta como la más vulnerable a datos e información sumamente personal (Andrade et al., 2021).

La Extorsión

La extorsión se define como un delito que busca obtener beneficios ilícitos mediante amenazas o coacción. En el ámbito digital, este tipo de conducta ha experimentado un notable aumento, dado que los delincuentes pueden acceder con facilidad a la información personal de sus víctimas a través de redes sociales y aplicaciones móviles. En Ecuador, En el entorno digital, esta normativa se aplica a situaciones en las que se utiliza información obtenida en redes sociales para coaccionar a las víctimas (Asamblea Nacional del Ecuador, 2014).

Reconocimiento normativo de la extorsión como tipo penal

A nivel global, diversos países han establecido marcos legales con el objetivo de combatir la extorsión digital. Por ejemplo, en Colombia, la Ley 1273 de 2009 protege la información y los datos personales como bienes jurídicos que merecen tutela (Mejía, Hurtado, & Aguirre, 2023; Jara Obregón et al.,2017). En otras naciones, se han endurecido las penas para los ciberdelitos, buscando frenar el uso indebido de las redes sociales para actividades ilícitas. El reconocimiento normativo de la extorsión como tipo penal es el proceso mediante el cual un sistema jurídico identifica, define y sanciona la extorsión dentro de su marco legal. Esto implica la incorporación de este delito en los códigos penales, estableciendo sus elementos constitutivos, las penas aplicables y las circunstancias agravantes o atenuantes (Albuja, 2022; Jara Obregón et al.,2017).

En la sección Sexta del Código Orgánico Integral Penal, menciona sobre Delitos contra el derecho a la intimidad personal y familiar. En el Art 178.- Violación a la intimidad. – La persona que, sin contar con el consentimiento o la autorización legal, acceda intercepte, examine retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (Asamblea Nacional de Ecuador, 2014).

En la sección Novena del Código Orgánico Integral Penal, menciona sobre el delito contra el derecho a la propiedad. En el Art 185.- Extorsión. - La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años (Rocha, Gonzáles, & Ministerio de Justicia, 2014).

Factores en las redes sociales que facilitan la extorsión

Antes, los delincuentes buscaban al azar a sus víctimas. Ahora, con las redes sociales, combinadas con los descuidos de los usuarios, los criminales están ubicando a las víctimas para extorsionarlos telefónicamente o, en los casos más graves, secuestrarlos virtualmente. Entre los métodos de cibercrimen que han experimentado mayor crecimiento destaca la extorsión por plataformas sociales o “doxing”, el cual consiste en una modalidad de acoso, amenaza e intimidación a las víctimas a cambio de dinero en efectivo u otras exigencias, a partir de la difusión de archivos personales de forma pública (La República, 2025).

La extorsión en Internet no es solo una amenaza abstracta. Los informes y operaciones recientes nos muestran la magnitud del problema. En marzo del presente año, la Guardia Civil de Cantabria dismanteló una red de sextorsión, arrestando a tres individuos responsables de extorsionar a 250 personas. Estos delincuentes utilizaban anuncios de índole sexual en sitios web de contactos, obteniendo imágenes privadas de personas a través de redes sociales para luego chantajearlas (REMOVE GROUP, 2025).

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

DISCUSIÓN

Los hallazgos obtenidos en esta investigación confirman que la extorsión a través de redes sociales y aplicaciones móviles es un problema creciente que afecta a distintos sectores de la población. Según los resultados de la encuesta aplicada en la Universidad Regional Autónoma de los Andes (UNIANDES), un porcentaje significativo de los encuestados ha sido víctima de este delito o conoce a alguien que lo ha experimentado. Esto sugiere que la extorsión digital no es un fenómeno aislado, sino una amenaza latente en el entorno digital. Uno de los aspectos más relevantes en la discusión es el papel que juegan las redes sociales en la propagación de este tipo de delitos.

La masividad y el anonimato que brindan estas plataformas han permitido que los delincuentes operen con mayor facilidad, utilizando estrategias como la suplantación de identidad, el envío de enlaces fraudulentos y la manipulación psicológica de las víctimas. Estudios previos han señalado que la ingeniería social es una de las tácticas más utilizadas en los delitos cibernéticos, ya que explota la confianza y la falta de conocimiento de los usuarios para obtener información personal o financiera. Además, se evidenció que muchos usuarios aún desconocen las medidas de seguridad necesarias para proteger su información en redes sociales.

La encuesta reveló que una gran parte de los encuestados no utiliza herramientas como la autenticación en dos pasos, la restricción de acceso a su información personal o la configuración de privacidad en sus cuentas. Esto demuestra que, aunque las plataformas digitales han implementado mecanismos de protección, la falta de educación digital sigue siendo un factor determinante en la vulnerabilidad de los usuarios. Otro punto clave es el rol de las autoridades y la efectividad de las regulaciones existentes.

A pesar de que en Ecuador y otros países de la región existen leyes que penalizan la extorsión digital, la percepción general es que las medidas gubernamentales aún no son suficientes. La falta de denuncias, el miedo a represalias y la dificultad para rastrear a los ciberdelincuentes complican la aplicación de la justicia. Es necesario

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

evaluar cómo pueden mejorarse los procesos de denuncia y persecución de estos delitos, garantizando mayor protección a las víctimas y una respuesta más rápida por parte de las autoridades.

Asimismo, un aspecto a considerar es la responsabilidad de las plataformas digitales en la prevención de la extorsión. Empresas como Facebook, Instagram, TikTok y WhatsApp han desarrollado herramientas de seguridad y políticas contra el acoso y el fraude, pero los resultados de la investigación muestran que estas medidas no siempre son efectivas. Las redes sociales deberían reforzar sus mecanismos de detección de perfiles falsos, mejorar la moderación de contenido y brindar mayor soporte a los usuarios que reportan intentos de extorsión.

Subir imágenes, grabar videos o realizar transmisiones en directo puede parecer inofensivo, pero en realidad puede revelar información sensible sin que el usuario lo note. Según el Instituto Nacional de Ciberseguridad de España (INCIBE), cualquier dato que aparezca en una publicación, como el entorno de una foto, la ubicación o incluso detalles visibles en la pantalla de un dispositivo, puede ser aprovechado por delincuentes. Según el Instituto Nacional de Ciberseguridad de España (INCIBE), cualquier dato que aparezca en una publicación, como el entorno de una foto, la ubicación o incluso detalles visibles en la pantalla de un dispositivo, puede ser aprovechado por delincuentes.

Finalmente, es importante reconocer algunas limitaciones del estudio. La muestra utilizada se centró en la comunidad universitaria de UNIANDES, por lo que los resultados pueden no ser representativos de toda la población ecuatoriana. Además, la investigación se enfocó principalmente en ciertos tipos de extorsión digital, dejando abierta la posibilidad de analizar otras modalidades en futuras investigaciones.

CONCLUSIONES

La investigación demuestra que la extorsión a través de redes sociales y aplicaciones móviles es un fenómeno en constante crecimiento, facilitado por el

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

anonimato que permite el entorno digital y la masificación del uso de estas plataformas. A pesar de la existencia de mecanismos de seguridad, muchas personas siguen siendo vulnerables debido al desconocimiento sobre ciberseguridad y a la falta de educación digital. Es fundamental fomentar una cultura de seguridad digital que capacite a los usuarios para reconocer amenazas, configurar adecuadamente su privacidad y utilizar herramientas de protección como la verificación en dos pasos.

Un hallazgo relevante es la percepción generalizada de ineficacia por parte de las autoridades en el combate contra la extorsión digital. Aunque existen leyes y sanciones establecidas, la falta de denuncias, el temor a represalias y la dificultad de rastrear a los ciberdelincuentes limitan la aplicación efectiva de la justicia. Es necesario fortalecer los mecanismos de denuncia, garantizar el anonimato y la protección de las víctimas, y promover una mayor colaboración entre las plataformas digitales y las entidades judiciales y policiales.

La prevención sigue siendo la estrategia más efectiva frente a este delito. Se recomienda implementar programas de educación digital desde edades tempranas, integrando la ciberseguridad en los planes de estudio. Las plataformas tecnológicas también deben asumir un rol activo, no solo con mejoras en sus sistemas de seguridad, sino con campañas educativas para sus usuarios. De igual forma, futuras investigaciones deberían explorar el impacto de nuevas tecnologías y el comportamiento de diferentes sectores poblacionales frente a estos delitos, para generar respuestas más integrales.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

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

Adelita Zarai Zabala-Ponce; Johanna Velarde-Sandy; Valeria Estefanía Vicuña-Pozo

REFERENCIAS CONSULTADAS

- Asamblea Nacional de Ecuador. (2014). Código Orgánico Integral Penal, Quito: Lexis. <https://n9.cl/s1o44>
- Albuja, B. y. (2022). Áreas de estudio y aplicación de inteligencia artificial en las universidades mejor puntuadas del Ecuador. <https://n9.cl/d7cze>
- Andrade, R., Maldonado Zuñiga, K. ., Anzules Avila, X. L., & Solorzano Alava, W. L. (2021). Redes sociales, un arma empleada a la delincuencia : redes sociales, un arma empleada a la delincuencia .*UNESUM - Ciencias. Revista Científica Multidisciplinaria*, 5(6), 63–68. <https://n9.cl/ovu6m>
- Anzures, R. M. (2021). Extorsión en las redes sociales. <https://n9.cl/0b45j>
- Rocha, L., Gonzáles, Á., & Ministerio de Justicia. (2014). CÓDIGO ORGÁNICO INTEGRAL PENAL. <https://n9.cl/w71g>
- Jara Obregón, L., Ferruzola Gómez, E., & Rodríguez López, G. (2017). Delitos a través de redes sociales en el Ecuador: una aproximación a su estudio. *I+D Tecnológico*, 13(2), 111-122. <https://n9.cl/6k0o5>
- Mejía-Lobo, M., Hurtado-Gil, S. V., & Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista De Ciencias Sociales*, 29(2), 356-372. <https://n9.cl/lo2r6>
- Redacción Primicias. (2023). Ecuador: cada vez hay más víctimas de extorsiones 'clásicas' y virtuales. <https://n9.cl/nu94o>
- REMOVE GROUP. (2025). ¿ Que es la extorsión en el internet?. <https://n9.cl/njrnjb>
- La República. (2025). Evite la extorsión en redes sociales con seis sencillos pasos. *República para decisiones Informadas*. <https://n9.cl/dx4yv>