# 20

Recibido: 25/9/24 Aceptado: 10/11/24

## Estafas informáticas en una comunidad agrícola del interior de Ecuador

Computer scams in an agricultural community in the interior of Ecuador

Jairo Mauricio Puetate Paucar[1]*
E-mail: ut.jairopuetate@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-9904-1897
Vanessa Lisseth Montenegro Altamirano[1]
E-mail: vanessama23@uniandes.edu.ec
ORCID: https://orcid.org/0009-0002-1677-4185
Rene Estalin Portilla Paguay[1]
E-mail: ut.renepp25@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-7227-747X

[1]Universidad Regional Autónoma de Los Andes, Ecuador.
*Autor para la correspondencia

**Cita sugerida (APA, séptima edición)**

Puetate Paucar, J. M., Montenegro Altamirano, V. L., y Portilla Paguay, R. E. (2024). Estafas informáticas en una comunidad agrícola del interior de Ecuador.. *Revista Científica Agroecosistemas, 12*(3), 141-147. https://aes.ucf.edu.cu/index.php/aes

**RESUMEN**

La importancia de adoptar un enfoque multidisciplinario y colaborativo para proteger a las comunidades rurales ecuatorianas frente a las estafas informáticas, permite el fortaleciendo tanto las capacidades tecnológicas como legales del país. El objetivo de la investigación es evaluar el impacto y la vulnerabilidad de las comunidades agrícolas del interior de Ecuador frente a las estafas informáticas. El enfoque utilizado es mixto, que combinó encuestas cuantitativas y entrevistas cualitativas, se analizó cómo el bajo acceso a la tecnología, la falta de conocimiento en ciberseguridad y la insuficiencia de la legislación ecuatoriana actual han dejado a estas comunidades expuestas a los fraudes electrónicos. Los resultados revelaron una alta incidencia de desconocimiento en torno a las medidas de protección frente a estafas digitales. La mayoría de los encuestados, aunque utilizan tecnología en sus actividades diarias, no saben cómo prevenir fraudes, lo que pone en riesgo tanto sus datos personales como su economía. Asimismo, las entrevistas con líderes comunitarios y expertos legales destacaron que la legislación vigente no es adecuada para abordar la creciente amenaza de los delitos informáticos en zonas rurales, lo que impide una respuesta efectiva ante estos crímenes. Además, se identificaron importantes deficiencias en la infraestructura de seguridad digital y en la capacidad de las autoridades locales para investigar y sancionar estos delitos. La necesidad urgente de una serie de reformas: desde la actualización del marco legal hasta la implementación de programas educativos y preventivos, pasando por la capacitación de las autoridades locales en el uso de herramientas tecnológicas avanzadas.

**Palabras clave:**

Fraude, Ciberseguridad, Comunidad rural, Tecnologías.

**ABSTRACT**

The importance of adopting a multidisciplinary and collaborative approach to protect Ecuadorian rural communities against computer scams allows for strengthening both the technological and legal capabilities of the country. The objective of the research is to evaluate the impact and vulnerability of agricultural communities in the interior of Ecuador against computer scams. The approach used is mixed, which combined quantitative surveys and qualitative interviews, analyzing how low access to technology, lack of knowledge in cybersecurity and the insufficiency of current Ecuadorian legislation have left these communities exposed to electronic fraud. The results revealed a high incidence of ignorance regarding protection measures against digital scams. The majority of respondents, although they use technology in their daily activities, do not know how to prevent fraud, which puts both their personal data and their finances at risk. Additionally, interviews with community leaders and legal experts highlighted that current legislation is inadequate to address the growing threat of cybercrime in rural areas, impeding an effective response to these crimes. In addition, significant deficiencies were identified in the digital security infrastructure and in the capacity of local authorities to investigate and punish these crimes. The urgent need for a series of reforms: from updating the legal framework to the implementation of educational and preventive programs, through the training of local authorities in the use of advanced technological tools.

**Keywords:**

Fraud, Cybersecurity, Rural community, Technologies.

## Introducción

La evaluación de las estafas informáticas en las comunidades agrícolas del interior de Ecuador presenta un desafío creciente en el contexto de la digitalización global y la proliferación de tecnologías de la información (López y López, 2018). Estas comunidades, tradicionalmente apartadas de los avances tecnológicos, han comenzado a adoptar dispositivos electrónicos y plataformas digitales para gestionar sus actividades comerciales y acceder a servicios públicos (Villarreal, 2023). Sin embargo, esta transformación también ha expuesto a sus habitantes a nuevos tipos de delitos, entre los cuales la estafa informática se destaca como una de las principales amenazas (Vera et al., 2024).

La estafa informática, entendida como la manipulación fraudulenta de sistemas electrónicos para obtener beneficios económicos ilícitos, afecta no solo a grandes corporaciones y entes gubernamentales, sino también a pequeñas empresas y agricultores locales que, en su mayoría, carecen de formación en ciberseguridad y protección de datos (Hernández, 2022). Estas comunidades rurales, donde la agricultura es el principal motor económico, están particularmente expuestas a este tipo de fraude debido a su limitada infraestructura tecnológica y su falta de acceso a programas de educación digital que podrían mitigar los riesgos (Sadjadi y Fernández, 2023).

A nivel nacional, la legislación ecuatoriana ha hecho esfuerzos para abordar los delitos cibernéticos, incluyéndolos en el Código Orgánico Integral Penal (COIP) (Ponce Tubay, 2024). Sin embargo, estas normativas no han demostrado ser lo suficientemente efectivas, especialmente en las zonas rurales, donde persisten dificultades para la recolección de evidencia digital y la persecución de los delincuentes (Castañeda y Feijóo, 2021). Según estudios recientes, los profesionales del derecho en Ecuador coinciden en que la legislación vigente presenta importantes lagunas que permiten la impunidad en muchos casos de estafa informática, particularmente cuando los perpetradores operan desde fuera del país (Ponce Tubay, 2024).

Otro factor que incrementa la vulnerabilidad de estas comunidades es la falta de recursos y personal especializado para prevenir, investigar y sancionar los delitos informáticos. Los agricultores, en su mayoría, no cuentan con los conocimientos necesarios para identificar estafas electrónicas, y las instituciones locales carecen de los medios tecnológicos para ofrecer una protección adecuada (Kshetri, 2017). Como resultado, se generan escenarios de incertidumbre y desconfianza hacia el uso de la tecnología, afectando no solo la economía local, sino también el desarrollo social de estas regiones (Ongadi, 2024).

La prevención de este tipo de fraudes es vital para garantizar la seguridad económica de los pequeños agricultores y emprendedores en las zonas rurales. Por ello, es crucial implementar una estrategia integral que incluya tanto el fortalecimiento de la legislación actual como la promoción de la educación digital entre los ciudadanos de estas comunidades (Arisukwu et al., 2020). De igual forma, es necesario fomentar la cooperación entre las autoridades nacionales e internacionales, con el fin de desarrollar herramientas tecnológicas avanzadas que permitan identificar y sancionar a los responsables de estos delitos de manera eficaz (Smith, 2020).

Por lo antes expuesto se plantea como objetivo de la investigación la evaluación de las estafas informáticas en las comunidades agrícolas del interior de Ecuador. Esto no solo implica un análisis jurídico y técnico, sino también un esfuerzo conjunto para empoderar a estas comunidades a través de la educación digital y la adopción de mejores prácticas de ciberseguridad. Esto permitirá mitigar los riesgos actuales, y también asegurar que la creciente digitalización en las áreas rurales sea una herramienta para el progreso, y no una fuente de vulnerabilidad.

## Materiales y métodos

La investigación adopta un enfoque mixto, utilizando tanto métodos cualitativos como cuantitativos para obtener una visión más completa del fenómeno:

- Investigación Cuantitativa: El objetivo de la investigación cuantitativa será recolectar datos estadísticos sobre la frecuencia y el impacto de las estafas informáticas en la comunidad agrícola seleccionada.

Esto incluye:

1. Encuestas estructuradas: Se aplicarán a los miembros de la comunidad, incluyendo agricultores, comerciantes y líderes locales, para entender su nivel de exposición a estafas electrónicas, su familiaridad con la tecnología y su conocimiento sobre ciberseguridad.
2. Variables a medir: Frecuencia de uso de dispositivos electrónicos, acceso a internet, tipos de estafas experimentadas, impacto económico y personal.
3. Muestra: Se seleccionará una muestra representativa de la comunidad agrícola, utilizando un muestreo no probabilístico por conveniencia, priorizando la diversidad en términos de género, edad y nivel de acceso a la tecnología.
4. Análisis de Datos: Los datos recolectados se analizarán utilizando herramientas estadísticas con el software SPSS para identificar patrones, correlaciones y la magnitud del impacto de las estafas en la comunidad.

- Investigación Cualitativa: Complementando el enfoque cuantitativo, se utilizará un enfoque cualitativo para obtener una comprensión más profunda de las experiencias personales, percepciones y desafíos enfrentados por los miembros de la comunidad.

Esto incluye:

1. Entrevistas semiestructuradas: Se realizarán con agricultores, líderes comunitarios, expertos en tecnología local y autoridades, para explorar sus experiencias y percepciones sobre las estafas informáticas. Se abordarán temas como la vulnerabilidad, las medidas de seguridad adoptadas y la efectividad de las políticas locales.

2. Grupos focales: Se organizarán grupos de discusión con miembros de la comunidad para identificar de manera colectiva las principales preocupaciones y posibles soluciones a las estafas informáticas.
3. Temas clave: Percepción de seguridad en el uso de tecnología, obstáculos en la denuncia de fraudes, efectividad de las campañas educativas o preventivas.

Para esta evaluación, se seleccionará una comunidad agrícola específica del interior de Ecuador, que represente las características comunes de las zonas rurales, como limitaciones tecnológicas, baja conectividad a internet y una economía basada en la agricultura. La comunidad deberá ser una que tenga acceso a dispositivos electrónicos, pero con una penetración de conocimiento tecnológico aún en desarrollo.
La recolección de datos será llevada a cabo en varias fases:

4. Fase de Preparación:

- Identificación de informantes clave: Se identificará a los líderes comunitarios, representantes de asociaciones de agricultores y comerciantes locales, quienes facilitarán el acceso a la comunidad y ayudarán en la recolección de datos.
- Diseño de instrumentos: Se diseñarán encuestas, guiones de entrevistas y dinámicas de los grupos focales adaptadas al nivel de conocimiento tecnológico de la comunidad. Las encuestas se desarrollarán en un lenguaje sencillo, accesible para las personas con menor educación formal.
- Recolección en Campo
- Aplicación de encuestas: Un equipo de encuestadores capacitados visitará a las familias y comercios locales para recolectar los datos mediante encuestas en formato papel o digital, dependiendo de los recursos disponibles.
- Entrevistas y grupos focales: Se realizarán en lugares accesibles de la comunidad, utilizando un enfoque participativo que incentive la apertura y la confianza.

Se realizará una revisión crítica de la legislación ecuatoriana aplicable a los delitos informáticos, especialmente en el contexto de comunidades rurales, para identificar las brechas y deficiencias en la protección de los ciudadanos frente a las estafas. Esto incluirá:

- Análisis de la legislación vigente: Se examinarán las leyes relacionadas con la ciberseguridad y la protección de datos en Ecuador, identificando su aplicación en áreas rurales.
- Entrevistas a expertos legales: Se consultará a abogados y fiscales locales para conocer sus experiencias en la persecución de delitos informáticos y sus sugerencias para mejorar el marco legal y operativo en estas comunidades.

## Resultados-discusión

La Tabla 1 muestra el uso de tecnología y estafas informáticas. En ella se puede apreciar que el un 65 % de los encuestados utiliza tecnología en sus actividades agrícolas, lo que demuestra una tendencia creciente hacia la digitalización, aunque su uso está limitado a tareas básicas como la comunicación.

En cuanto al desconocimiento sobre ciberseguridad el 80 % no conoce cómo protegerse de estafas informáticas, lo que sugiere la necesidad de programas de capacitación urgentes. Mientras que la percepción de las autoridades, el 85 % siente que las autoridades locales no brindan suficiente apoyo o protección contra el fraude digital, destacando una brecha entre las necesidades de la comunidad y las respuestas institucionales.

Tabla 1: Uso de tecnología y estafas informáticas.

| Pregunta | Respuesta Mayoritaria | Porcentaje | Observaciones |
|---|---|---|---|
| ¿Utiliza dispositivos electrónicos (celulares, tablets, etc.) para sus actividades agrícolas? | Sí | 65 % | La mayoría usa dispositivos electrónicos, aunque en tareas limitadas. |
| ¿Ha sido víctima de alguna estafa informática? | No | 75 % | Aunque un 25% sí reporta haber sido víctima, la mayoría no lo ha sido o no lo identifica. |
| ¿Sabe cómo protegerse ante posibles fraudes electrónicos? | No | 80 % | Gran parte de la comunidad desconoce medidas básicas de ciberseguridad. |
| ¿Considera que las autoridades locales le brindan suficiente protección frente a fraudes informáticos? | No | 85 % | Existe una percepción generalizada de insuficiente apoyo gubernamental. |
| ¿Confía en el uso de la tecnología para mejorar su negocio agrícola? | Sí, pero con reservas | 60 % | La desconfianza en la tecnología es alta, especialmente en temas de seguridad. |

**Fuente:** Elaboración propia.

Según Mphatheni y Maluleke (2022), las comunidades agrícolas se encuentran en una posición precaria, ya que son notablemente vulnerables a diversas formas de estafas electrónicas, una situación que se atribuye principalmente a su comprensión insuficiente de los principios de ciberseguridad y a su acceso restringido a recursos y herramientas tecnológicas avanzadas que podrían ayudar a proteger sus entornos digitales.

Un número considerable de personas encuestadas en el estudio realizado por Kshetri (2013; 2017) en estas comunidades muestran una falta de conciencia con respecto a las precauciones y medidas fundamentales que deben adoptarse para protegerse eficazmente de las amenazas generalizadas del fraude informático, lo que las convierte en objetivos particularmente susceptibles y atractivos para las nefastas actividades perpetradas por los ciberdelincuentes que explotan estas vulnerabilidades con una facilidad y frecuencia alarmantes.

La entrevista realizada a líderes comunitarios y expertos legales (Tabla 2 ) arroja que la comunidad agrícola está significativamente expuesta a estafas informáticas debido a la falta de formación y recursos tecnológicos adecuados. La legislación ecuatoriana sobre delitos informáticos, aunque ha mejorado, no es efectiva en áreas rurales, lo que requiere reformas para incluir especificidades de estas zonas. La ausencia de campañas educativas y programas preventivos es preocupante. Es fundamental la inversión en capacitaciones específicas para la población agrícola. Las autoridades locales no están suficientemente preparadas para investigar y sancionar este tipo de delitos, resaltando la necesidad de crear unidades de investigación especializadas.

**Tabla 2:** Entrevistas a Líderes Comunitarios y Expertos Legales**.**

| Tema | Opiniones de los Entrevistados | Conclusiones |
|---|---|---|
| Vulnerabilidad de la comunidad | La comunidad está poco preparada para afrontar ciberestafas. | Falta de conocimiento sobre ciberseguridad y baja capacidad de respuesta. |
| Eficacia de la legislación actual | La legislación actual es insuficiente y no abarca las particularidades de las zonas rurales. | Urge una actualización del marco legal que contemple las realidades rurales. |
| Colaboración de autoridades locales y nacionales | Existe poca coordinación entre las autoridades locales y nacionales para combatir este tipo de delitos. | Necesidad de mejorar la coordinación interinstitucional y las capacidades locales. |
| Medidas preventivas en la comunidad | No hay campañas educativas ni programas preventivos en la comunidad sobre estafas informáticas. | Recomendación de iniciar campañas educativas a nivel local. |
| Posibilidades de persecución de estos delitos | La falta de recursos técnicos y de personal especializado dificulta la persecución de los delitos informáticos. | Se requiere la creación de unidades especializadas en ciberseguridad. |

**Fuente:** Elaboración propia.

La cooperación internacional emerge como un elemento crucial en la lucha contra la estafa informática. Dado que estos delitos no se limitan a las fronteras nacionales, se reconoce la importancia de colaborar con otras jurisdicciones para investigar y procesar a los perpetradores. Sin embargo, se señala la necesidad de mejorar los mecanismos de cooperación y compartir información de manera efectiva entre países para lograr resultados más significativos (Demestichas et al., 2020).

En términos de capacidades y recursos, se destaca la necesidad de una mayor especialización y capacitación entre los profesionales del derecho y las autoridades encargadas de hacer cumplir la ley (Ticona et al., 2024). Esto incluye el desarrollo de habilidades técnicas y forenses específicas para investigar delitos informáticos, así como el acceso a herramientas y tecnologías avanzadas para recopilar y analizar evidencia digital de manera efectiva.

El impacto de las estafas informáticas se ilustra en la Tabla 3. En relación entre educación y exposición a estafas, existe una fuerte correlación entre el nivel educativo y la exposición a estafas, lo que sugiere que mejorar el nivel de educación en ciberseguridad podría reducir significativamente el riesgo de fraude. El acceso a internet y seguridad suelen implementar más medidas de seguridad, pero aún existe un porcentaje considerable que no aplica medidas básicas de protección, lo que refleja la necesidad de promover la ciberseguridad. Las estafas informáticas generan un impacto económico significativo en aquellos agricultores que dependen más de la tecnología, lo que subraya la importancia de proteger los sistemas digitales utilizados en las actividades agrícolas.

**Tabla 3:** Impacto de las Estafas Informáticas**.**

| Variable | Correlación | Significado Estadístico (p-valor) | Observaciones |
|---|---|---|---|
| Nivel de educación vs. exposición a estafas | 0.75 | $p < 0.01$ | A mayor nivel de educación, menor es la exposición a estafas informáticas. |
| Acceso a internet vs. uso de medidas de seguridad | 0.42 | $p = 0.03$ | Quienes tienen mejor acceso a internet suelen aplicar más medidas de seguridad. |
| Uso de tecnología vs. impacto económico de las estafas | 0.58 | $p = 0.02$ | El impacto económico de las estafas es mayor en aquellos que dependen más de la tecnología. |

**Fuente:** Elaboración propia.

La evaluación cualitativa de las medidas Gubernamentales y propuestas de mejora se presenta en la Tabla 4. La percepción de que la legislación actual es insuficiente es predominante. Las reformas deben enfocarse en las particularidades del ámbito rural y en la prevención de estafas informáticas. En cuanto a la falta de campañas educativas son casi inexistentes, lo que afecta negativamente la preparación de la población para protegerse de fraudes electrónicos. La capacitación de los funcionarios locales es deficiente, lo que limita la capacidad de las autoridades para prevenir y responder ante estos delitos. Se recomienda un enfoque en la formación continua en ciberseguridad y nuevas tecnologías.

**Tabla 4:** Evaluación de las medidas Gubernamentales y propuestas de mejora**.**

| Medida Gubernamental | Percepción de Eficacia (Escala 1-5) | Propuesta de Mejora |
|---|---|---|
| Legislación actual sobre ciberseguridad | 2 (Baja) | Revisión y actualización del COIP para incluir zonas rurales. |
| Campañas de concienciación | 1 (Muy baja) | Implementar campañas educativas en las comunidades agrícolas. |
| Capacitación de funcionarios locales en ciberseguridad | 2 (Baja) | Capacitación urgente en tecnología y ciberseguridad a nivel local. |
| Cooperación internacional | 3 (Moderada) | Fortalecer la cooperación para el intercambio de información y herramientas de investigación. |

**Fuente:** Elaboración propia.

Los resultados de la investigación subrayan la necesidad imperiosa de adoptar una estrategia holística y sinérgica para combatir eficazmente el problema generalizado del fraude informático que ha estado afectando cada vez más al panorama socioeconómico rural de Ecuador. Este enfoque multifacético requiere no solo reformas significativas en los marcos legales existentes, sino también la mejora de la formación profesional y la asignación de recursos, al tiempo que fomenta un espíritu de colaboración que trasciende las fronteras nacionales para hacer frente a esta amenaza en constante evolución (Campos, 2019).

A la luz de los rápidos avances de las tecnologías digitales, es evidente que quienes participan en actividades fraudulentas están innovando y perfeccionando al mismo tiempo sus métodos e instrumentos para perpetuar sus actividades ilícitas (Acuña-Gamba y Sotelo-Vargas, 2016). En consecuencia, resulta absolutamente vital asignar inversiones sustanciales a la exploración y el desarrollo de metodologías novedosas destinadas a mejorar la detección y la prevención del fraude informático, junto con la creación de soluciones tecnológicas de vanguardia que permitan a las fuerzas del orden y a otras partes interesadas contrarrestar de manera más eficaz estos delitos sofisticados (Villacís, 2022). Al navegar por este complejo panorama, es fundamental reconocer que la batalla contra el fraude informático requerirá un esfuerzo concertado y sostenido por parte de varios sectores, incluidas las entidades gubernamentales, las organizaciones privadas y las instituciones académicas (Coila, 2018). En última instancia, solo a través de un frente unido y un compromiso con la mejora continua podemos esperar mitigar el impacto del fraude informático y salvaguardar la integridad de nuestros ecosistemas digitales (Mera y Gallegos, 2023).

## Conclusiones

- Las comunidades agrícolas del interior de Ecuador están significativamente expuestas a estafas electrónicas debido a su bajo nivel de conocimientos en ciberseguridad y el limitado acceso a recursos tecnológicos. La mayoría de los encuestados desconocen las medidas básicas de protección frente a fraudes informáticos, lo que los convierte en blancos fáciles para los delincuentes cibernéticos.
- A pesar de que Ecuador ha implementado normativa sobre delitos informáticos en el Código Orgánico Integral Penal (COIP), esta no es suficiente para proteger eficazmente a las comunidades rurales. Las leyes actuales no contemplan las particularidades de estas zonas, donde el acceso a tecnología es más limitado y los recursos para la persecución de estos delitos son escasos.
- Las autoridades locales carecen de la capacitación y los recursos necesarios para enfrentar los delitos informáticos en zonas rurales. La investigación reveló que no existen unidades especializadas en ciberseguridad ni programas formales para educar a los ciudadanos sobre cómo protegerse de estafas electrónicas.
- Aunque un porcentaje significativo de la comunidad utiliza tecnología para actividades agrícolas, la confianza en el uso seguro de la misma es baja debido a la falta de protección efectiva contra fraudes. Esto afecta tanto al desarrollo económico local como a la adopción de tecnologías que podrían mejorar las actividades agrícolas.
- La cooperación entre instituciones locales, nacionales e internacionales es vista como un elemento clave para combatir las estafas informáticas, debido a la naturaleza transnacional de muchos de estos delitos. Sin embargo, esta cooperación es actualmente insuficiente y necesita ser fortalecida, especialmente en lo referente al intercambio de información y la adopción de nuevas tecnologías de investigación.
- Se recomienda un enfoque integral que incluya la actualización de la legislación, la capacitación de las autoridades locales, y la implementación de campañas

educativas sobre ciberseguridad dirigidas específicamente a las comunidades rurales. Además, es crucial mejorar la cooperación entre instituciones a todos los niveles para combatir eficazmente este fenómeno.

## Referencias bibliográficas


Acuña-Gamba, E. J., & Sotelo-Vargas, D. A. (2016). Ley 1273 de 2009:¿ Los jueces del cibercrimen?. *Iter Ad Veritatem*, *14*, 181-193. http://revistas.ustatunja.edu.co/index.php/iaveritatem/article/view/1339/1242

Arisukwu, O., Igbolekwu, C., Oye, J., Oyeyipo, E., Asamu, F., Rasak, B., & Oyekola, I. (2020). Community participation in crime prevention and control in rural Nigeria. *Heliyon*, *6*(9), 1-7. https://www.cell.com/heliyon/pdf/S2405-8440(20)31858-2.pdf

Campos, N. J. O. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. https://dialnet.unirioja.es/descarga/articulo/7148227.pdf

Castañeda, M. M., & Feijóo, C. (2021). La ciberseguridad alimentaria en China y sus implicaciones internacionales. *Análisis del Real Instituto Elcano (ARI)*, (50), 1-7. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari50-2021-martinez-fiejoo-ciberseguridad-alimentaria-en-china-y-sus-implicaciones-internacionales.pdf

Coila, M. E. (2018). El derecho penal informático humano como cautela frente al poder punitivo en la sociedad de control. *Revista de Derecho*, *3*(2), 233-245. https://www.redalyc.org/pdf/6718/671871279002.pdf

Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on security threats in agricultural IoT and smart farming. *Sensors*, *20*(22), 1-17. https://www.mdpi.com/1424-8220/20/22/6458/pdf

Hernández, M. (2022). Situación de los servicios financieros digitales, la seguridad de la información y ciberseguridad en el Sector Financiero Popular y Solidario. *X-pedientes Económicos*, *6*(14), 18-32. https://ojs.supercias.gob.ec/index.php/X-pedientes_Economicos/article/download/100/91

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, *13*, 41-69. https://core.ac.uk/download/pdf/345078785.pdf

Kshetri, N. (2017). The economics of the Internet of Things in the Global South. *Third World Quarterly*, *38*(2), 311-339. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Economics_2016.pdf

López, N. M., & López, R. M. (2018). Los jóvenes y la ciberseguridad en zonas rurales del Estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. *RECAI Revista de Estudios en Contaduría, Administración e Infomática*, *7*(20), 14-35. https://www.redalyc.org/journal/6379/637968308002/637968308002.pdf

Mera, J. M. R., & Gallegos, M. J. V. (2023). La categoría dogmático penal de la tipicidad, el principio de legalidad y los delitos informáticos en la legislación ecuatoriana: Ciberseguridad y criminalidad informática. *Desafíos Jurídicos*, *3*(4), 24-37. https://desafiosjuridicos.uanl.mx/index.php/ds/article/download/63/28

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(4), 384-396. https://www.ssbfnet.com/ojs/index.php/ijrbs/article/download/1714/1310

Ongadi, P. A. (2024). A comprehensive examination of security and privacy in precision agriculture technologies. *GSC Advanced Research and Reviews*, *18*(1), 336-363. https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2024-0026.pdf

Ponce Tubay, M. A. (2024). Desafíos y respuestas legales ante los delitos informáticos en Ecuador. *Revista San Gregorio*, *1*(58), 111-118. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072024000200111

Sadjadi, E. N., & Fernández, R. (2023). Challenges and opportunities of agriculture digitalization in Spain. *Agronomy*, *13*(1), 1-23. https://www.mdpi.com/2073-4395/13/1/259/pdf

Smith, K. (2020). Desolation in the countryside: How agricultural crime impacts the mental health of British farmers. *Journal of Rural Studies*, *80*, 522-531. https://hau.repository.guildhe.ac.uk/id/eprint/17614/1/Kreseda%20Smith%20Desolation%20upload.pdf

Ticona, J. C. A., Calcina, K. M. C., Lipe, J. J. L., Valero, M. L., Cabrera, R. M. M., García, H. L. T., & Parí, N. C. (2024). Causas y consecuencias del incremento de los delitos informáticos en la ciudad de Puno 2023. *Revista de Derecho*, *9*(1), 1-19. https://www.redalyc.org/journal/6718/671876168004/

Vera, J. J. M., Zambrano, K. B. Á., Vidal, W. E. B., & Rendón, A. D. Z. (2024). Estudio de delitos informáticos en la comunidad "Mocochal": causas y prevenciones. *Maestro y Sociedad*, 142-150. https://maestroysociedad.uo.edu.cu/index.php/MyS/article/download/6426/7161

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*, *6*(1), 50-62. https://revista-edwardsdeming.com/index.php/es/article/download/88/158

Villarreal, M. B. (2023). Elementos para la conceptualización de la ciberseguridad nacional. *Trabajo Social UNAM*, (34), 30-44. https://revistas.unam.mx/index.php/ents/article/download/88025/77112