

ESTUDIO DE DELITOS INFORMÁTICOS EN LA COMUNIDAD "MOCOCHAL": CAUSAS Y PREVENCIONES**Study of computer crimes in the community "Mocochal": causes and preventions**

Jéssica Johana Montes Vera *, <https://orcid.org/0000-0001-6095-3442>

Karen Barbarita Álava Zambrano, <https://orcid.org/0000-0001-8852-9598>

Willians Eduardo Basurto Vidal, <https://orcid.org/0000-0001-7293-621X>

Aura Dolores Zambrano Rendón, <https://orcid.org/0000-0002-2784-9202>

Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López", Ecuador

*Autor para correspondencia. email jessica.montes@espam.edu.ec

Para citar este artículo: Montes Vera, J. J., Álava Zambrano, K. B., Basurto Vidal, W. E. y Zambrano Rendón, A. D. (2024). Estudio de delitos informáticos en la comunidad "Mocochal": causas y preventiones. *Maestro y Sociedad*, (Número Especial Vinculación Sociedad y Educación), 142-150. <https://maestroysociedad.uo.edu.cu>

RESUMEN

Introducción: Los delitos informáticos son una amenaza creciente en todo el mundo, especialmente en las comunidades rurales, donde los recursos para prevenir y combatir estos crímenes son limitados. En este sentido, el objetivo de este artículo es realizar el estudio de delitos informáticos en la comunidad "Mocochal" de la parroquia Calceta, cantón Bolívar. **Materiales y métodos:** Se utilizó la metodología de investigación cuantitativa, con un alcance descriptivo, un diseño de campo y de tipo documental, aplicando encuestas semipresenciales con una muestra de 104 personas para obtener datos sobre la prevalencia de los delitos informáticos en la comunidad. **Resultados:** Los resultados mostraron que una proporción significativa del 17.3% de las personas encuestadas experimentaron algún tipo de delito informático y que los grupos más vulnerables son los adultos mayores. **Discusión:** Una amenaza común en dichas comunidades es el robo de datos personales y financieros, por lo cual es importante que las comunidades tomen medidas para protegerse de estas amenazas. Esto puede incluir el uso de contraseñas seguras, la protección de la información personal y financiera, la instalación de software de seguridad y la actualización regular de los sistemas informáticos. **Conclusiones:** En función a esto, se concluye que se necesitan medidas de prevención adicionales para combatir la amenaza, asimismo se requiere de capacitación sobre delitos informáticos y seguridad informática.

Palabras clave: Delitos informáticos, Seguridad informática, Comunidad rural, Vulnerabilidad, Prevención.

ABSTRACT

Introduction: Cybercrime is a growing threat around the world, especially in rural communities, where resources to prevent and combat these crimes are limited. In this sense, the objective of this article is to carry out the study of computer crimes in the "Mocochal" community of the Calceta parish, Bolívar canton. **Materials and methods:** Quantitative research methodology was used, with a descriptive scope, a field and documentary-type design, applying blended surveys with a sample of 104 people to obtain data on the prevalence of computer crimes in the community. **Results:** The results showed that a significant proportion of 17.3% of the people surveyed experienced some type of computer crime and that the most vulnerable groups are older adults. **Discussion:** A common threat in these communities is the theft of personal and financial data, which is why it is important that communities take measures to protect themselves from these threats. This may include using strong passwords, protecting personal and financial information, installing security software, and regularly updating computer systems. **Conclusions:** Based on this, it is concluded that additional prevention measures are needed to combat the threat, training on computer crimes and computer security is also required.

Key words: Computer crime, Computer security, Rural community, Vulnerability, Prevention.

Recibido: 19/10/2023 Aprobado: 4/12/2023

INTRODUCCIÓN

La tecnología informática se ha convertido en una herramienta muy importante en nuestra vida cotidiana. El uso de internet y dispositivos móviles ha abierto una puerta a una gran cantidad de posibilidades de conectividad y conocimiento. Sin embargo, también conlleva ciertos peligros que afectan a las personas y comunidades, la violación de la privacidad y el robo de identidad son algunos de estos riesgos. Las personas deben ser conscientes de los peligros potenciales y tomar medidas para minimizar los riesgos en línea. Esto incluye estar al tanto de los últimos avances en la tecnología de seguridad informática, así como tomar las precauciones adecuadas para garantizar la seguridad de los datos.

Desde el 2009, en el Ecuador se han recibido numerosas denuncias por delitos informáticos como el robo de contraseñas, clonación de tarjetas de crédito, ataques a sitios web gubernamentales, falsificación o fraude informático (Toala, 2021). A finales del 2014, se aprobó el Código Orgánico Integral Penal (COIP) que incluye artículos que sancionan específicamente estos delitos informáticos (Enríquez & Alvarado, 2015) (Aparicio, 2022). El problema es que dicha legislación aun no es socializada, aunque es responsabilidad de las personas conocer y acatar las leyes impuestas en el país, hay poco interés en conocer tales disposiciones. Además, el mal uso de la tecnología informática por parte de los usuarios inexpertos, que no emplean ninguna estrategia de seguridad informática, los expone fácilmente a ataques informáticos (Ajila, 2019) (Acosta et al., 2020).

Vélez (2022), menciona un claro ejemplo que se ve reflejado en el caso “Carbanak”, en el año 2016 se descubrió que un grupo de delincuentes cibernéticos había robado más de \$100 millones de dólares de bancos en todo el mundo, incluyendo muchos bancos en áreas rurales. Los delincuentes utilizaron un malware llamado “Carbanak” para infiltrarse en los sistemas bancarios y robar la información financiera de los clientes. En función a todo lo antes mencionado, el gobierno debería generar leyes que garanticen la protección de los datos, tanto en la administración pública como en el ámbito privado, para que la información de los ciudadanos esté disponible únicamente para quienes sean autorizados a usarla (Martínez & Martínez, 2018).

De acuerdo con Aguilar & Fonseca (2019) en la actualidad a través de los medios de comunicación en términos de las redes sociales, se conoce que las personas menores de edad están siendo engañadas, utilizadas en redes de prostitución infantil, secuestradas y violadas por “supuestas” amistades que hicieron en redes sociales y que no son más que perfiles falsos de personas pedófilas y degeneradas (Mendivil, 2019) (Mora et al., 2020). Las noticias del 2017 indican que aún no estamos seguros de cómo educar a nuestros jóvenes y adultos mayores (Alcaraz et al., 2021) (Suárez, 2022). Por esta razón, los grupos de expertos en seguridad informática han aconsejado no aceptar peticiones de amistad de desconocidos, mantener privados los contenidos que se publican en la red, no publicar información personal, no mostrar fotografías de menores que revele su lugar de estudio o hogar, entre otros (Vargas Borbúa et al., 2017).

En consecuencia, a los argumentos previos y la aplicación de una encuesta como medio para realizar un análisis estadístico a la situación actual de la comunidad “Mocochoal” en materia de seguridad informática y delitos informáticos, se han formulado las hipótesis y el objetivo de esta investigación. Ante lo expuesto, el objetivo del presente estudio consiste en realizar un estudio de delitos informáticos en la comunidad “Mocochoal”, sus causas y formas de prevención, para diseñar estrategias de prevención eficaces y minimizar sus efectos en la comunidad.

Este estudio destaca la importancia de la educación sobre seguridad informática y la necesidad de medidas de prevención adecuadas para prevenir delitos informáticos en comunidades rurales. Las recomendaciones del estudio pueden ayudar a las comunidades rurales a tomar medidas para protegerse mejor contra los delitos informáticos y mejorar la seguridad en línea en estas áreas.

MATERIALES Y MÉTODOS

Este estudio se llevó a cabo mediante el uso de la metodología de investigación cuantitativa, partiendo del planteamiento del problema, la descripción del objetivo y las hipótesis, la recopilación y el análisis de datos fundamentadas en datos numéricos y estadísticos (Azuelo, 2019) (Mero et al., 2022). La investigación se desarrolló en la comunidad “Mocochoal” que se encuentra ubicada en la parroquia Calceta en la provincia de Manabí de Ecuador (ver Figura 1, obtenido de Google Maps), donde se aplicaron las encuestas a los residentes que serían seleccionados al azar de entre los habitantes de la comunidad. La finalidad principal de esta investigación está basada en estudiar los delitos informáticos más frecuentes en la comunidad “Mocochoal” y determinar la frecuencia con que se cometen los delitos para evaluar la efectividad de las medidas de prevención y seguridad informática.



Figura 1. Mapa de cobertura satelital.

La investigación tuvo un alcance descriptivo, en la que Alcivar et al. (2022), señala que: “busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis, con el fin de establecer su estructura o comportamiento”. Con base en lo anterior, se tomó en consideración la investigación documental como la revisión bibliográfica, esto sirvió como base para el uso de fuentes electrónicas y otros documentos relacionados con el tema de la investigación. Para esto se consultaron artículos, textos, revistas de editoriales nacionales e internacionales de reconocimiento.

El cuestionario para la encuesta constó de 14 preguntas, de las cuales las primeras 2 son preguntas relacionadas a los datos personales del residente comunitario y las restantes sobre la proyección de los estudios posteriores sobre delitos informáticos en la comunidad “Mocochoal”. Para realizar el análisis de resultados se utilizaron 8 de ellas: ¿Con qué frecuencia se conecta a internet? ¿Con qué finalidad usa usted el servicio de Internet? ¿Qué tan familiarizado/a está usted con el término “delitos informáticos”? ¿Alguna vez ha sido víctima de un delito informático? ¿Cuál es el tipo de delito informático del que usted ha sido víctima? ¿Cuáles cree que son las principales causas de los delitos informáticos en tu comunidad? ¿Con qué frecuencia cambia sus contraseñas de acceso a dispositivos y plataformas? En el caso de existir un delito informático, ¿conoce usted qué acciones tomar?

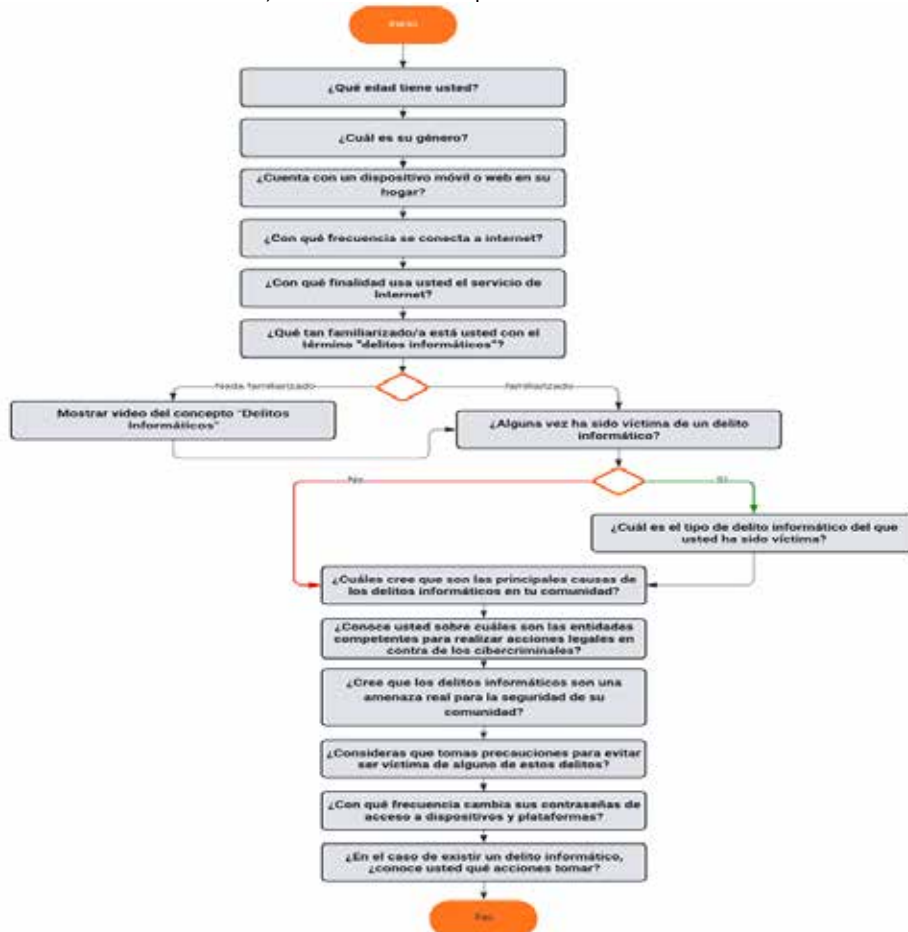


Diagrama 1. Diagrama de flujo de la encuesta

Por consiguiente, se utilizó el tipo de investigación de campo y consistió en obtener los datos de fuentes primarias directamente de la realidad, en la comunidad, esenciales para el logro del objetivo. De este modo, se detalla que hasta el último censo la población está conformada por 800 habitantes, 240 familias, 180 viviendas. Se realizó un muestreo estadístico para la obtención de la muestra, estimándose 104 personas, propiciado de esa manera indagar sobre los delitos informáticos que los residentes de “Mocochoal” han sido víctimas. En función a eso, para la obtención del tamaño de muestra de la población finita se utilizó la siguiente fórmula:

$$n = \frac{Z^2(N)(p)(q)}{[E^2 - (N - 1)] + [Z^2(p)(q)]}$$

$$n = \frac{1.96^2(800)(0.5)(0.5)}{[0.09^2 - (800 - 1)] + [1.96^2(0.5)(0.5)]}$$

$$n = 104$$

Donde:

n = Tamaño de muestra

N = Tamaño de la población

Z = Nivel de confianza = 95%

p = Probabilidad a favor = 50%

q = Probabilidad en contra = 50%

E = Margen de error = 0.09

Para la recolección de la información se aplicaron encuestas, su tabulación se realizó con la herramienta de Google Forms, donde la información se convirtió en datos y gráficos, lo que facilitó la comprensión y el análisis de los datos estadísticos.

Ahora bien, se aplicaron las encuestas para la recopilación de los datos, específicamente a 104 personas residentes de la comunidad “Mocochoal”. Se observó que los residentes de estas comunidades suelen ser menos conscientes de los riesgos de seguridad en línea y, por lo tanto, son más propensos a hacer clic en enlaces maliciosos, compartir información personal y usar contraseñas débiles. También se identificaron la falta de recursos y la falta de acceso a la tecnología de seguridad como un desafío en la prevención de delitos informáticos. Muchas personas en estas áreas no tienen acceso a los mismos recursos que las personas que viven en áreas urbanas, como el acceso a proveedores de servicios de seguridad informática y herramientas de seguridad.



Imagen 1. Visitas a los residentes de la comunidad "Mocochoal" para la aplicación de encuestas. Fuente: Los Autores.

Los autores recomiendan varias medidas de prevención, como la educación de la comunidad sobre los riesgos de seguridad en línea, la implementación de medidas de seguridad básicas como el uso de contraseñas seguras y la autenticación de dos factores, y la colaboración con proveedores de servicios de seguridad informática para garantizar el acceso a recursos de seguridad. También sugieren la necesidad de una mayor

inversión en infraestructura de tecnología de la información para garantizar la disponibilidad de recursos de seguridad informática para las comunidades rurales.

RESULTADOS

En este segmento, se presenta de manera organizada la información obtenida a través de las encuestas aplicadas a los residentes de la comunidad "Mocochal" en la parroquia Calceta del Cantón Bolívar. Los datos recopilados fueron utilizados para crear tablas y gráficos estadísticos y así analizar e interpretar la información. Bajo estas circunstancias, se buscó analizar e interpretar la información, a continuación, se presenta:

¿Con qué frecuencia se conecta a internet?

Tabla 1. Conexión a internet

Alternativa	Frecuencia	Porcentaje
Nunca	15	14.4%
Casi nunca	2	1.9%
Diariamente	70	67.3%
Ocasionalmente	16	15.4%
Cada mes	0	0%
Una vez a la semana	1	1%
Total	104	100%

Según los datos de la Tabla 1, se puede concluir que la mayoría de los habitantes de la comunidad "Mocochal" se conectan a internet diariamente, con un porcentaje del 67.3%. Solo el 14.4% de los encuestados nunca se conectan a internet, mientras que un 15.4% lo hace ocasionalmente. Un porcentaje muy bajo de la muestra, el 1.9% afirmó conectarse casi nunca, y solo un encuestado (1%) dijo que se conecta una vez a la semana.

¿Con qué finalidad usa usted el servicio de Internet?

Tabla 2. Uso del internet

Alternativa	Frecuencia	Porcentaje
Para consultar información	29	28.4 %
Para mantenerse en contacto con amigos y familiares	50	49 %
Para divertirse y pasar el tiempo	39	38.2 %
Para realizar tareas y/o estudiar.	43	42.2 %
Para comprar productos y/o servicios.	8	7.8 %
Para otras actividades	41	40.2 %
Total	104	100%

De acuerdo con la tabla proporcionada, se puede observar que la finalidad principal de los encuestados para usar el servicio de internet es para mantenerse en contacto con amigos y familiares, con un porcentaje del 49%. Un 42.2% de los encuestados afirman que utilizan el servicio de internet para realizar tareas y/o estudiar, mientras que un 38.2% lo utilizan para divertirse y pasar el tiempo. Un 40.2% de los encuestados indicaron que usan el servicio de internet para otras actividades no especificadas. Un 28.4% de los encuestados indicaron que utilizan el servicio de internet para consultar información, mientras que solo el 7.8% lo utilizan para comprar productos y/o servicios.

¿Qué tan familiarizado/a está usted con el término "delitos informáticos"?

Tabla 3. Familiaridad con el término "delitos informáticos"

Alternativa	Frecuencia	Porcentaje
Muy familiarizado	10	9.6%
Familiarizado	12	11.5%
Medio familiarizado	22	21.2%
Poco familiarizado	16	15.4%
Nada familiarizado	44	42.3%
Total	104	100%

Este es uno de los indicadores principales de la investigación da a evidenciar el grado de preparación que tienen los habitantes de la comunidad ante los delitos informáticos. Es aquí donde se puede apreciar que las desinformaciones sobre delitos informáticos equivalen a casi a la mitad de la población en cuestión alrededor de

un 42.3% y otras dos facciones que cuentan con una noción leve al respecto, la primera está poco familiarizada la cual representa un 15.4% de la población y otra que está medio familiarizado representando un 21.2%.

¿Alguna vez ha sido víctima de un delito informático?

Tabla 4. Víctimas de delitos informáticos en la comunidad "Mocochal"

Alternativa	Frecuencia	Porcentaje
Si	86	17.3%
No	18	82.7%
Total	104	100%

De acuerdo con la tabla proporcionada, se puede observar que el 17.3% de los encuestados de la comunidad "Mocochal" indicaron haber sido víctimas de un delito informático. El 82.7% restante indicó que no habían sido víctimas de este tipo de delitos.

¿Cuál es el tipo de delito informático del que usted ha sido víctima?

Tabla 5. Tipo de delito informático del que ha sido víctima

Alternativa	Frecuencia	Porcentaje
Pretexting	9	50%
Sextorsión	1	5.6%
Pharming	4	22.2%
Phishing	0	0%
Acceso no autorizado o Hacking	1	5.6%
Smishing	0	0%
El Sexting	0	0%
El Hostigamiento o Stalking	1	5.6%
Otros	2	11.1%
Total	18	100%

Se puede observar que el tipo de delito informático más comúnmente experimentado por los encuestados de la comunidad "Mocochal" fue el Pretexting, con un 50% de los encuestados que indicaron haber sido víctimas de este tipo de delito. El segundo tipo más común fue el Pharming, con el 22.2% de los encuestados indicando que habían sido víctimas de este delito. Además, hubo un 5.6% de encuestados que indicaron haber experimentado acceso no autorizado o Hacking y Hostigamiento o Stalking. Un 11.1% de los encuestados indicaron haber sido víctimas de otros tipos de delitos informáticos.

¿Cuáles cree que son las principales causas de los delitos informáticos en tu comunidad?

Tabla 6. Causas principales de los delitos informáticos

Alternativa	Frecuencia	Porcentaje
Acceso generalizado a internet y las redes sociales	15	14.4%
La falta de educación sobre el uso seguro de internet y las redes sociales.	55	52.9%
La poca atención que se le presta al tema	25	24%
La existencia de programas y aplicaciones maliciosas	9	8.7%
Total	104	100%

De acuerdo con los resultados de la tabla proporcionada, se puede observar que la principal causa de los delitos informáticos en la comunidad "Mocochal", según los encuestados, es la falta de educación sobre el uso seguro de internet y las redes sociales, con un 52.9% de los encuestados indicando esta como la causa principal.

En segundo lugar, se encuentra la poca atención que se le presta al tema, con un 24% de los encuestados indicando esto como una causa importante de los delitos informáticos en la comunidad. Un 14.4% de los encuestados indicaron que el acceso generalizado a internet y las redes sociales son la principal causa de los delitos informáticos, mientras que un 8.7% de los encuestados indicaron que la existencia de programas y aplicaciones maliciosas es la causa principal.

¿Con qué frecuencia cambia sus contraseñas de acceso a dispositivos y plataformas?

Tabla 7. Cambio de contraseñas de acceso a dispositivos y plataformas

Alternativa	Frecuencia	Porcentaje
Mensualmente	13	12.5%

Trimestralmente	6	5.8%
Semestralmente	16	15.4%
Anualmente	21	20.2%
Nunca	48	46.2%
Total	104	100%

De acuerdo con los resultados de la tabla proporcionada, se puede observar que la mayoría de los encuestados en la comunidad "Mocochoal" no cambian sus contraseñas de acceso a dispositivos y plataformas con regularidad, ya que un 46.2% de los encuestados indicaron que nunca cambian sus contraseñas.

Por otro lado, un 20.2% de los encuestados indicaron que cambian sus contraseñas anualmente, mientras que un 15.4% lo hace semestralmente, un 12.5% mensualmente y un 5.8% trimestralmente.

En el caso de existir un delito informático, ¿conoce usted qué acciones tomar?

Tabla 8. Acciones a tomar en caso de sufrir un delito informático

Alternativa	Frecuencia	Porcentaje
Sí, conozco las acciones a tomar	21	20.4%
No, no conozco las acciones a tomar	16	15.5%
Tal vez, conozco algunas de las acciones a tomar	16	15.4%
Sí, conozco qué acciones tomar en general, pero no en detalle	8	7.8%
No, no tengo idea de qué acciones tomar	31	30.1%
Total	104	100%

El análisis de la tabla muestra que un porcentaje significativo de la comunidad "Mocochoal" encuestada (30.1%) no tiene idea de qué acciones tomar en caso de existir un delito informático. Es preocupante que casi un tercio de la comunidad no esté informada sobre este tema, considerando que los delitos informáticos pueden tener graves consecuencias y afectar tanto a individuos como a empresas o instituciones.

Por otro lado, un 20.4% de los encuestados indicó que sí conoce las acciones a tomar, lo cual es positivo. Sin embargo, es importante destacar que un porcentaje similar (15.4%) indicó que tal vez conoce algunas de las acciones a tomar, lo que sugiere que todavía hay incertidumbre en cuanto a la respuesta adecuada en caso de un delito informático. Además, es interesante notar que un 7.8% de los encuestados indicó que sí conoce qué acciones tomar en general, pero no en detalle. Esto puede significar que tienen una comprensión general del tema, pero necesitan más información o capacitación específica para saber cómo responder de manera efectiva.

DISCUSIÓN

El artículo sobre el estudio de delitos informáticos en la comunidad "Mocochoal" presenta una valiosa contribución al análisis de las amenazas cibernéticas en un contexto local. El estudio aborda un tema muy actual y relevante, ya que los delitos informáticos son cada vez más comunes y afectan a personas, empresas y gobiernos de todo el mundo.

El análisis de los resultados de las encuestas muestra una falta de familiaridad entre los habitantes de la comunidad con los delitos informáticos, lo cual es preocupante dado que esto podría hacer que sean más vulnerables a posibles ataques cibernéticos. Por lo tanto, es importante que se realice una labor de educación y concienciación sobre este tema para evitar posibles riesgos y amenazas en el futuro.

Además, el artículo proporciona una lista de posibles causas de los delitos informáticos en la comunidad "Mocochoal", como la falta de conocimiento y capacitación en seguridad informática, la falta de medidas de seguridad adecuadas en los dispositivos electrónicos y la falta de conciencia sobre la importancia de proteger los datos personales. Estas causas son comunes en muchos contextos y pueden aplicarse a otras comunidades y países.

Una amenaza común en dichas comunidades es el robo de datos personales y financieros, por lo cual es importante que las comunidades tomen medidas para protegerse de estas amenazas. Esto puede incluir el uso de contraseñas seguras, la protección de la información personal y financiera, la instalación de software de seguridad y la actualización regular de los sistemas informáticos.

CONCLUSIONES

En conclusión, el estudio sobre delitos informáticos en la comunidad "Mocochal" es un trabajo valioso y oportuno que destaca la necesidad de prestar atención a la seguridad informática en contextos locales. Los resultados de las encuestas realizadas indican una falta de conocimiento y conciencia entre los habitantes de la comunidad sobre el tema de los delitos informáticos. Esta situación los hace más vulnerables a los riesgos y amenazas cibernéticas.

El artículo también proporciona una lista de posibles causas de los delitos informáticos en la comunidad "Mocochal" y ofrece recomendaciones para prevenirlos. Estas recomendaciones incluyen prácticas de seguridad informática comunes, como el uso de contraseñas seguras, la actualización de los dispositivos y programas, el uso de software antivirus y la educación sobre la seguridad informática.

En general, este estudio sugiere que hay una necesidad de mayor educación y concienciación sobre la importancia de la seguridad informática en sitios rurales como la comunidad "Mocochal". También destaca la importancia de que los individuos y organizaciones tomen medidas preventivas para protegerse contra los delitos informáticos. Este estudio proporciona información valiosa que puede ser útil para prevenir los delitos informáticos en esta y otras comunidades.

En conclusión, la seguridad informática es un tema importante en todas las comunidades, incluyendo las rurales. Es importante que los residentes de estas comunidades tomen medidas para proteger sus dispositivos y datos personales, y que las empresas y organizaciones responsables de la administración de servicios de Internet también tomen medidas para proteger a sus clientes.

REFERENCIAS BIBLIOGRÁFICAS

1. Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 89(89). <https://doi.org/10.37960/revista.v25i89.31534>
2. Aguilar, C., & Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *COMeIN*, 23(6), 1–24. Obtenido de: <https://doi.org/10.7238/c.n6.1132>
3. Ajila, A. (2019). Análisis jurídico de las leyes que amparan a víctimas del delito informático en Santo Domingo. Obtenido de: <http://dspace.uniandes.edu.ec/handle/123456789/10868>
4. Alcaraz, C., Castro, N., & Calvo, G. (2021.). Investigación en ciberseguridad. *Jornadas Nacionales de Investigación en Ciberseguridad*. Obtenido de: <https://ruidera.uclm.es>
5. Alcivar, M., Balseca, P., & Ferrin, H. (2022). La contabilidad y cultura tributaria en los comerciantes de mercados populares. 3, 32–42.
6. Aparicio, V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. *Sapienza: International Journal of Interdisciplinary Studies*, 3(1), 1057–1063. Obtenido de: <https://doi.org/10.51798/sijis.v3i1.284>
7. Azuero, Á. E. (2019). Significatividad del marco metodológico en el desarrollo de proyectos de investigación. *Revista Arbitrada Interdisciplinaria Koinonía*, 4(8), 110.
8. Enríquez, J. V., & Alvarado, Y. C. (2015). Los delitos informáticos y su penalización en el Código Orgánico Integral Penal Ecuatoriano. *Sathiri*, 8, 171. <https://doi.org/10.32645/13906925.404>
9. Martínez, N., & Martínez, R. (2018). Los jóvenes y la ciberseguridad en zonas. *RECAI Revista de Estudios En Contaduría, Administración e Informática*, 7(20), 14–35. Obtenido de: <https://www.redalyc.org/articulo.oa?id=637968308002>
10. Mendivil, E. (2019). Ciberseguridad, Comparativa y Aplicaciones. 1–60. Obtenido de: <http://hdl.handle.net/11531/28934>
11. Mora, D., Agredo, N., & Meneses, R. (2020). Sistema para la gestión y prevención de riesgos de ciberseguridad en la ciudad de Popayán. 8(75), 147–154. Obtenido de: <http://hdl.handle.net/20.500.12494/18429>
12. Mero, U., Baduy, A., & Cárdenas, E. (2022). Producción avícola y su incidencia en el desarrollo económico. 43–61. Obtenido de: https://revistas.uleam.edu.ec/index.php/business_science/article/view/227
13. Suárez, D. (2022). Validación e Implantación de un curso de formación acerca de la competencia digital y la ciberseguridad en el futuro profesorado de la comunidad autónoma de canarias empleando la técnica escape room. Obtenido de: <https://repositorio.grial.eu>

14. Toala, I. (2021). Delitos informáticos frecuentes en el Ecuador: Casos de estudio. Universidad Politécnica Salesiana Sede Guayaquil. Revista EIA, ISSN 1794-1237, Volumen 17, 1–323. Obtenido de: <http://dspace.ups.edu.ec/handle/123456789/10070>

15. Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO- Revista Latinoamericana de Estudios de Seguridad, 20, 31. Obtenido de: <https://doi.org/10.17141/urvio.20.2017.2571>

16. Vélez, E. (2022). Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador. Universidad católica de Santiago de Guayaquil. 1–125. Obtenido de: <http://repositorio.ucsg.edu.ec>

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

Declaración de responsabilidad de autoría

Los autores del manuscrito señalado, DECLARAMOS que hemos contribuido directamente a su contenido intelectual, así como a la génesis y análisis de sus datos; por lo cual, estamos en condiciones de hacernos públicamente responsable de él y aceptamos que sus nombres figuren en la lista de autores en el orden indicado. Además, hemos cumplido los requisitos éticos de la publicación mencionada, habiendo consultado la Declaración de Ética y mala praxis en la publicación.

Jéssica Johana Montes Vera; Karen Barbarita Álava Zambrano; Willians Eduardo Basurto Vidal y Aura Dolores Zambrano Rendón: Proceso de revisión de literatura y redacción del artículo.