STAR OF SCIENCES
MULTIDISCIPLINARY JOURNAL
ISSN:3091-1885
Vol. 2 Núm. 2 (2025) Revista Científica

Prevention of Identity Theft Fraud among Vulnerable Adults Aged 50 to 60 in Chetumal, Quintana Roo: A Criminological Analysis

Prevención del fraude por usurpación de identidad en adultos vulnerables de 50 a 60 años en Chetumal, Quintana Roo: un análisis criminológico

Para citar este trabajo:
Mex Corado, A. E. . (2025). Prevención del fraude por usurpación de identidad en adultos vulnerables de 50 a 60 años en Chetumal, Quintana Roo: un análisis criminológico. Star of Sciences Multidisciplinary Journal, 2(2), 1-12. https://doi.org/10.63969/8d8cf355

Autores:
Angelica Estefany Mex Corado
Universidad Vizcaya de las Américas Campus Chetumal
Chetumal Quintana Roo - México
mexcoradofany@gmail.com
https://orcid.org/0009-0004-7812-3710

Autor de Correspondencia: Angelica Estefany Mex Corado, mexcoradofany@gmail.com

RECIBIDO: 27-Agosto-2025 **ACEPTADO**: 10-Septiembre-2025 **PUBLICADO**: 24-Septiembre-2025

ISSN:3091-1885

Resumen

El presente artículo aborda la prevención del fraude asociado a la usurpación de identidad en la ciudad de Chetumal, Quintana Roo, focalizándose en un grupo demográfico especialmente vulnerable: los adultos de 50 a 60 años. Este segmento poblacional ha sido identificado como particularmente susceptible a este tipo de delitos debido a su limitada familiaridad con las tecnologías digitales y la insuficiente protección de sus datos personales. La investigación se desarrolló bajo una metodología cualitativa, empleando entrevistas semiestructuradas dirigidas a adultos dentro del rango de edad señalado, con el fin de comprender sus percepciones, conocimientos y prácticas relacionadas con la seguridad digital. Entre los resultados sobresalen el desconocimiento generalizado de mecanismos básicos de protección en entornos digitales, la ausencia de estrategias para prevenir fraudes en línea y la carencia de acceso a programas educativos en materia de ciberseguridad y prevención del delito. Estos hallazgos resaltan la necesidad urgente de diseñar e implementar políticas públicas y programas formativos accesibles que fortalezcan la capacidad de este grupo demográfico para protegerse frente a fraudes derivados de la usurpación de identidad, contribuyendo así a la reducción de la victimización en contextos digitales y mejorando la seguridad ciudadana.

Palabras clave: Fraude; usurpación de identidad; adultos vulnerables; prevención del delito; ciberseguridad.

Abstract

The present article addresses the prevention of fraud linked to identity theft in the city of Chetumal, Quintana Roo, focusing on a particularly vulnerable demographic group: adults aged 50 to 60. This population segment has been identified as especially susceptible to such crimes due to their limited familiarity with digital technologies and the inadequate protection of their personal data. The research was conducted using a qualitative methodology, employing semi-structured interviews with adults within the specified age range, in order to gain an understanding of their perceptions, knowledge, and practices regarding digital security. The findings highlight a widespread lack of awareness of basic protection mechanisms in digital environments, the absence of strategies to prevent online fraud, and a lack of access to educational programmes in cybersecurity and crime prevention. These results underscore the urgent need to design and implement accessible public policies and training initiatives that strengthen the capacity of this demographic group to protect themselves against fraud arising from identity theft, thereby contributing to the reduction of victimisation in digital contexts and enhancing public safety.

Keywords: Fraud; Identity theft; Vulnerable adults; Crime prevention; Cybersecurity.

1. Introducción

En la actualidad, la usurpación de identidad mediante el fraude digital representa una de las amenazas más graves y crecientes para la seguridad individual y social en México, particularmente en contextos urbanos con alta penetración tecnológica como Chetumal, Quintana Roo. Este fenómeno delictivo se ha visto acelerado por la masificación del uso de tecnologías de la información y la comunicación (TIC), que si bien han facilitado innumerables aspectos de la vida cotidiana, también han abierto nuevas brechas de vulnerabilidad. El fraude derivado de la suplantación de identidad implica la obtención y uso indebido de datos personales para fines ilícitos, afectando la integridad económica, social y emocional de las personas, generando un problema social y jurídico de gran envergadura que requiere respuestas integrales desde diversas disciplinas, entre ellas la criminología.

Particularmente, los adultos de entre 50 y 60 años constituyen un sector de la población altamente vulnerable frente a estos delitos, dada su limitada familiaridad con las prácticas y herramientas digitales, así como por una cultura de ciberseguridad aún incipiente. La brecha digital en este grupo no solo se traduce en desconocimiento técnico, sino también en factores sociales y emocionales que los hacen blanco fácil para estrategias de engaño sofisticadas. La confianza excesiva en fuentes no verificadas y la falta de redes de apoyo fortalecen su riesgo de victimización, mientras que la carencia de programas educativos específicos orientados a su contexto agravan esta situación. Investigaciones recientes confirman que esta población es una de las más afectadas por fraudes ligados a la usurpación de identidad en México, junto con los jóvenes, evidenciando una problemática transversal generacional en el país.

De acuerdo con el informe A Year in Fraud 2024 elaborado por Unico México (2025), México experimentó un incremento del 84% en casos de fraude por suplantación de identidad durante el año 2024, ubicándose como el país con mayor incidencia en América Latina en este tipo de delitos. Esta realidad se manifiesta con especial impacto en entidades como el Estado de México, Ciudad de México y Jalisco, aunque la afectación se extiende a regiones como Quintana Roo, donde el crecimiento del comercio digital y la interconectividad constituyen factores de riesgo. El estudio reporta además un aumento del 49% en la circulación de identidades falsas y un reforzamiento de las técnicas empleadas por defraudadores, que ahora utilizan tecnologías avanzadas como inteligencia artificial para crear deepfakes, dificultando la detección y prevención de estos delitos (Unico México, 2025).

Asimismo, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF, 2023) ha advertido que el aumento sostenido de fraudes por usurpación de identidad afecta profundamente a los sectores más vulnerables, especialmente adultos mayores, quienes sufren pérdidas económicas cuantiosas y estrés emocional severo. En Chetumal, esta situación se agrava debido al limitado acceso a programas de formación y sensibilización en ciberseguridad, lo cual limita la capacidad de prevención local ante el fraude digital. La Policía Cibernética de Quintana Roo ha reportado un incremento significativo en denuncias relacionadas con delitos cibernéticos, señalando la necesidad urgente de fortalecer mecanismos comunitarios y educativos que blindan la protección de datos personales y reduzcan la victimización (Sánchez Méndez & Herrera Mejía, 2025).

Desde una perspectiva criminológica, la usurpación de identidad no solo debe entenderse como un delito aislado, sino como un fenómeno estrechamente vinculado a la exclusión tecnológica y social, que revela problemáticas estructurales y culturales. La carencia de alfabetización digital en los adultos vulnerables limita el desarrollo de actitudes críticas y preventivas frente a ciberamenazas, incrementando la probabilidad de caer en fraudes que repercuten en su estabilidad económica y confianza en las instituciones. La integración de la educación en

ISSN:3091-1885

ciberseguridad con políticas públicas inclusivas y estrategias comunitarias permite avanzar hacia una mitigación efectiva del fenómeno, generando entornos digitales más seguros y accesibles para todos los segmentos sociales (Sánchez Méndez, Quintal García & Ganzo Olivares, 2023).

En este marco, la presente investigación se propone analizar en profundidad las experiencias, percepciones y estrategias de prevención de los adultos entre 50 y 60 años en Chetumal, quienes han resultado altamente expuestos a la suplantación de identidad mediante fraude. Para ello, se emplea un enfoque cualitativo basado en entrevistas semiestructuradas que permiten recoger evidencias directas sobre las prácticas digitales de este grupo y sus carencias informativas. Este acercamiento busca identificar los factores psicosociales, educativos y tecnológicos que facilitan la perpetración del delito y, con base en los hallazgos, formular propuestas orientadas a la prevención y la protección integral de esta población vulnerable (Sánchez Méndez et al., 2023).

Además, se reconoce que el impacto del fraude va más allá de lo económico, afectando también la vida social y emocional de las víctimas. La desconfianza generada hacia las instituciones financieras y tecnológicas, así como el temor a nuevas agresiones digitales, limita su participación en la economía digital, acentuando procesos de exclusión y marginalización. En este sentido, fortalecer la resiliencia individual y comunitaria mediante programas formativos, campañas de sensibilización y accesibilidad tecnológica constituye un pilar fundamental para la reducción de la incidencia del fraude por usurpación de identidad (Consejo Ciudadano, 2025).

El contexto específico de Chetumal exige, además, considerar las particularidades culturales, sociales y económicas locales, donde la carencia de infraestructura educativa y la limitada oferta de capacitación en línea restringen el acceso a conocimientos preventivos esenciales. Por ello, resulta imprescindible un enfoque multidisciplinario que articule la participación de autoridades, academia, organizaciones civiles y sector privado, generando modelos adaptados a la realidad del territorio para garantizar la protección efectiva de los adultos vulnerables en el entorno digital (Sánchez Méndez & Herrera Mejía, 2025).

En este sentido, la usurpación de identidad mediante fraudes digitales representa un fenómeno complejo que impacta con severidad a los adultos vulnerables en Chetumal, Quintana Roo, donde convergen factores tecnológicos, sociales y educativos que demandan atención urgente. Este estudio aporta un análisis detallado desde una perspectiva criminológica y social, enriqueciendo el conocimiento académico y ofreciendo bases para la formulación de políticas públicas y estrategias comunitarias dirigidas a proteger los derechos y la seguridad digital de esta población, contribuyendo así a la construcción de comunidades digitales seguras e inclusivas.

2. Metodología

La investigación desarrollada adoptó un enfoque cualitativo con la finalidad de comprender profundamente, desde una perspectiva interpretativa y contextualizada, las percepciones, experiencias y niveles de conocimiento que manifiestan las personas adultas entre 50 y 60 años frente al fenómeno del fraude digital derivado de la usurpación de identidad. Este enfoque permitió captar las contradicciones y matices subjetivos de los participantes en torno al uso cotidiano de las tecnologías digitales, así como su actitud hacia la protección de la información personal en espacios virtuales, aspectos que dificultan la prevención y aumentan su vulnerabilidad frente a delitos cibernéticos (Sandoval Guarín et al., 2023).

El tipo de estudio correspondió a una investigación con diseño descriptivo, orientada a caracterizar y analizar sistemáticamente los conocimientos, prácticas y experiencias de la población objetivo mediante la recopilación de datos empíricos que se presentan y analizan en el marco de una realidad social compleja (Stewart, 2025). Este diseño es particularmente pertinente para captar los fenómenos en sus contextos naturales sin intervención directa, permitiendo

ISSN:3091-1885

describir con rigor las características y dinámicas de la población en torno a su interacción con tecnologías digitales y riesgos asociados.

La metodología se enmarcó dentro de un diseño observacional, ya que se abordó la tarea de observar, registrar y analizar detenidamente las percepciones y experiencias de los participantes con respecto al uso de tecnologías y la problemática del fraude digital por usurpación de identidad. En este sentido, el estudio fue de naturaleza transversal, pues la recolección de datos se efectuó en un único momento temporal, generando una "instantánea" del estado del conocimiento y comportamientos actuales relacionados con hábitos digitales y vulnerabilidades en el grupo etario señalado, lo que facilita el entendimiento de sus necesidades y limitaciones en el presente (Hou, 2022).

La población objetivo estuvo constituida por personas residentes en la ciudad de Chetumal, Quintana Roo, un grupo identificado como especialmente vulnerable al fraude digital debido a su limitado conocimiento sobre la prevención y manejo seguro de datos personales y prácticas de ciberseguridad. Este grupo etario presenta características que justifican su selección, como la creciente participación en plataformas digitales sin la correspondiente alfabetización para enfrentarse a riesgos tecnológicos, lo que los convierte en blanco frecuente para estafas y suplantación de identidad (Sánchez Méndez, Quintal García & Ganzo Olivares, 2023).

La muestra se conformó por 12 participantes que cumplían con criterios específicos de inclusión: acceso básico a dispositivos electrónicos y redes sociales, así como experiencia directa o indirecta con situaciones relacionadas con el manejo seguro de información personal en entornos digitales. La selección de entrevistados se realizó mediante un muestreo por conveniencia, una estrategia metodológica que valoró la disponibilidad y proximidad de los individuos al equipo investigador, facilitando así la recolección profunda y contextualizada de datos. Esta técnica es común en estudios cualitativos donde se prioriza la riqueza de la información sobre la representatividad estadística (Sandoval Guarín et al., 2023).

La recolección de información se basó en entrevistas semiestructuradas, conducidas de forma presencial, método que permitió explorar detalladamente las experiencias, percepciones y conocimientos de los participantes frente al uso de tecnologías y los riesgos de fraude asociados a la usurpación de identidad. Esta técnica favorece la flexibilidad para profundizar en temas emergentes durante el diálogo, proporcionando información rica y contextual necesaria para comprender la complejidad del fenómeno desde la perspectiva de quienes lo viven (Hou, 2022). Además, este acercamiento favorece la identificación de patrones culturales y sociales que subyacen en las prácticas digitales y en la respuesta ante amenazas cibernéticas.

En consonancia con los principios éticos fundamentales de la investigación, durante todo el estudio se garantizó la voluntariedad en la participación, la confidencialidad de los datos y el anonimato de los individuos. Los participantes fueron informados de manera clara y completa sobre los objetivos del estudio, así como sobre el uso que se daría a la información recopilada, asegurando en todo momento el respeto a su dignidad y derechos humanos (Sánchez Méndez & Herrera Mejía, 2025). La aplicación rigurosa de estas normas éticas constituye un pilar esencial para la validez y legitimidad de la investigación, especialmente cuando se trabaja con poblaciones vulnerables.

La estrategia metodológica implementada proporciona una base robusta y sólida para el análisis de las vulnerabilidades digitales del grupo etario en estudio, permitiendo identificar no solo las carencias en conocimientos técnicos, sino también los factores psicosociales y contextuales que influyen en la percepción del riesgo y en las prácticas preventivas frente al fraude digital. El enfoque cualitativo facilita, por tanto, la construcción de propuestas preventivas y formativas que sean culturalmente pertinentes y adecuadas a la realidad local (Sánchez Méndez et al., 2023).

Entre las limitaciones observadas destaca la resistencia inicial de algunos posibles participantes ante la invitación a colaborar en la investigación, una reacción comprensible en poblaciones con desconfianza hacia los procesos académicos o temor a exponerse. Este fenómeno evidencia, además, un aspecto relevante en la problemática abordada: el miedo y la vulnerabilidad asociados a su interacción con tecnologías que no dominan completamente, lo que refleja la necesidad de estrategias que fomenten la confianza y la inclusión digital (Kuong Cuellar, 2024). Estas resistencias aportan información valiosa para diseñar intervenciones que consideren las barreras psicológicas y sociales que afectan la adopción de prácticas seguras en entornos digitales.

En suma, esta metodología cualitativa, descriptiva, observacional y transversal se configura como un instrumento adecuado para examinar en profundidad las experiencias, conocimientos y percepciones de adultos vulnerables ante el fraude digital. Constituye un aporte para el desarrollo de estrategias preventivas contextualizadas en la realidad de Chetumal, que atienden las demandas específicas de las personas adultas en la era digital y contribuyen a fortalecer la seguridad y autonomía digital de esta población (Stewart, 2025; Sánchez Méndez et al., 2023).

3. Resultados

Los hallazgos derivados de las entrevistas semiestructuradas aplicadas a adultos vulnerables de 50 a 60 años en Chetumal, Quintana Roo, confirman un alto nivel de vulnerabilidad frente al fraude digital por usurpación de identidad, revelando patrones preocupantes que combinan desconocimiento técnico, factores sociales y culturales, y carencia de acceso a formación en ciberseguridad. Entre los resultados más sobresalientes, destaca el escaso conocimiento que tienen los participantes sobre la seguridad digital, evidenciando un vacío en nociones básicas como la creación y gestión segura de contraseñas, la verificación de la autenticidad de sitios web y la configuración adecuada de privacidad en plataformas sociales. Este déficit de información básica aumenta exponencialmente el riesgo de victimización por parte de actores delictivos que emplean técnicas como phishing, suplantación y fraudes electrónicos, y coincide con informes nacionales que señalan la creciente incidencia de estos delitos en personas adultas mayores (Rosado, 2025).

Adicionalmente, la dificultad manifiesta para distinguir mensajes fraudulentos de comunicaciones oficiales representa un factor crítico en la exposición a engaños digitales. La mayoría de entrevistados no identificó signos característicos del phishing ni estrategias comunes de manipulación empleadas por delincuentes, actitud que facilita la penetración del fraude. En consonancia con ello, la limitada experiencia práctica y la falta de alfabetización digital dentro del grupo etario refuerzan su inaccesibilidad a recursos formativos especializados, resultando en un conocimiento insuficiente para adoptar medidas preventivas eficientes. La ausencia de programas formales de capacitación en ciberseguridad y alfabetización digital para adultos de estas edades en Chetumal emerge como una brecha importante que debe abordarse con urgencia (Sánchez Méndez, Quintal García & Ganzo Olivares, 2023).

Es importante señalar que la vulnerabilidad no se limita únicamente a aspectos técnicos. En el análisis se identificaron dimensiones sociales y culturales que contribuyen a fortalecer la exposición al fraude. Por ejemplo, existe una confianza excesiva en fuentes no verificadas, ya sea en comunicaciones recibidas de supuestas instituciones oficiales, familiares, o empresas, lo que facilita la extracción de información sensible o dinero. Asimismo, el aislamiento digital, entendido como la escasa interacción y familiaridad con herramientas digitales, limita notablemente la capacidad de los adultos vulnerables para detectar amenazas, generando un círculo de dependencia y desinformación que perpetúa la vulnerabilidad frente a ciberataques (Pérez Gómez, 2024).

ISSN:3091-1885

Estos resultados están en coherencia con investigaciones y datos estadísticos nacionales. Por ejemplo, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) reportó en el primer semestre de 2025 que más de 10 mil adultos mayores presentaron reclamos por fraude digital, acumulando pérdidas superiores a los 500 millones de pesos. Este fenómeno está reforzado por la necesidad de interacción de este grupo con tecnologías digitales, que aunque reciente, es constante y sin el acompañamiento que garantice una experiencia segura (CONDUSEF, 2023; Rosado, 2025). Además, datos del Instituto Nacional de las Personas Adultas Mayores (INAPAM) indican que solo un 39.2% de adultos mayores utilizan Internet, reflejando una brecha digital significativa que impacta en la preparación para enfrentar riesgos en línea (INAPAM, 2023).

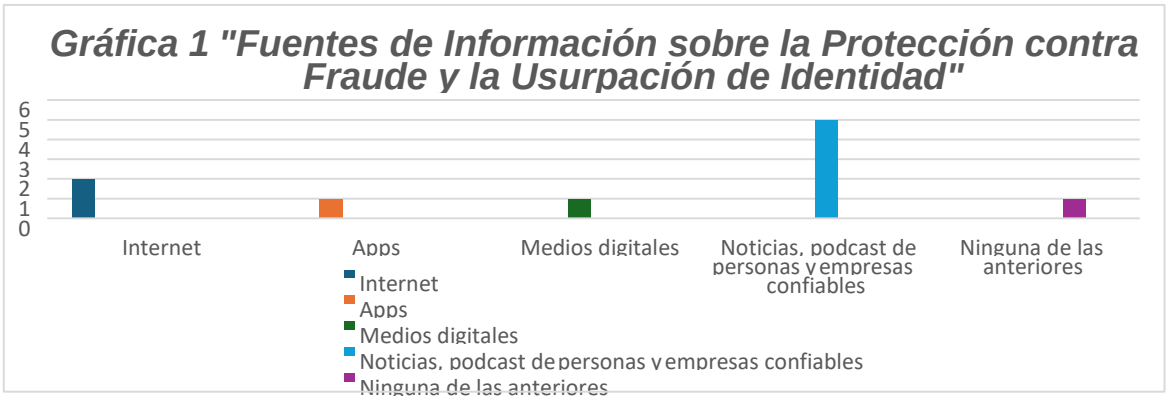
Por otro lado, la percepción y experiencia recogida apunta a que muchos adultos de esta franja etaria enfrentan sentimientos de desconfianza o incluso temor hacia las herramientas digitales, lo que paradójicamente limita su interés en formarse y actualizarse en seguridad digital, impidiendo que adquieran las habilidades necesarias para protegerse. Este aspecto emocional y psicológico es un componente clave a atender dentro de las estrategias preventivas, dado que el fraude digital no solo implica pérdidas económicas, sino también daños profundos en la confianza y autonomía personal (Corona, 2025).

Este conjunto de hallazgos subraya la necesidad urgente de implementar políticas públicas y programas educativos que integren la capacitación en habilidades digitales básicas, la sensibilización sobre protección de datos personales y el desarrollo de una cultura de prevención efectiva. Las estrategias deben ser accesibles, inclusivas y adaptadas a las características culturales y sociales de los adultos mayores para lograr un impacto real y sostenible (Sánchez Méndez & Herrera Mejía, 2025). Asimismo, la participación activa de las comunidades y redes sociales locales es fundamental para fortalecer los canales de apoyo y vigilancia colectiva, lo que puede reducir los niveles de aislamiento digital y colaborar en la detección temprana de fraudes (Sánchez Méndez, Quintal García & Ganzo Olivares, 2023).

En síntesis, estos resultados evidencian que la prevención del fraude digital en adultos vulnerables debe ir más allá de una simple transferencia de conocimientos técnicos y debe contemplar un enfoque integral que considere factores sociales, culturales y emocionales. La atención a estas dimensiones permitirá diseñar soluciones que realmente empoderen a este sector social frente a las complejas amenazas del entorno digital, contribuyendo a una mejora palpable en su bienestar económico y social.

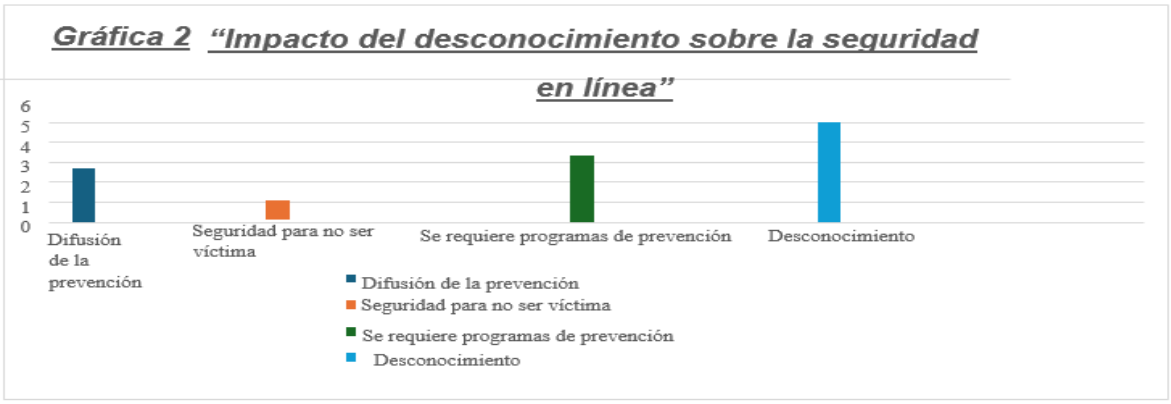
4. Discusión

El estudio sobre estrategias de prevención del fraude derivado de la usurpación de identidad en Chetumal, Quintana Roo, aporta valiosas evidencias acerca de la comprensión que tienen los adultos entre 50 y 60 años sobre este delito digital y las formas en que intentan protegerse. La mayoría de los entrevistados manifestó un entendimiento claro y acertado sobre el concepto de usurpación de identidad, definiéndola como el uso no autorizado de datos personales con fines ilícitos, lo que indica que la población objetivo posee una noción precisa y fundamentada sobre la problemática, reconociendo el riesgo que esto implica para su seguridad y patrimonio (Romero Flores, 2021). Esta percepción alinea la experiencia cotidiana de los sujetos con explicaciones académicas del fenómeno, lo cual es un indicador positivo para el diseño de intervenciones educativas y preventivas.



Fuente: Cuestionario sobre el fraude derivado de la usurpación de identidad. Elaboración propia (2025).

Los resultados indican que los riesgos más relevantes asociados al intercambio de información personal en línea son el fraude financiero, la suplantación de identidad, el secuestro de datos y el uso indebido de información confidencial. Este conocimiento sobre el alcance y las consecuencias de dichos delitos revela que los participantes están en contacto con narrativas y contenidos que les alertan sobre la magnitud del fenómeno. Aunado a ello, los entrevistados mencionaron que las fuentes de información más recurridas para protegerse incluyen Internet, aplicaciones bancarias, medios digitales oficiales y noticias confiables, lo que refleja una tendencia hacia la búsqueda activa de recursos digitales para la autoprotección. Esta actitud indica un interés por adaptarse a las nuevas realidades tecnológicas, aunque las habilidades concretas para dicha adaptación sean limitadas (Internet Society Mexico Chapter, 2025).



Fuente: Cuestionario sobre el fraude derivado de la usurpación de identidad. Elaboración propia (2025).

Aun con este nivel de comprensión y búsqueda de información, persiste una clara carencia de conocimientos específicos sobre seguridad en línea, factor que es especialmente crítico en grupos vulnerables como los adultos mayores. La mayoría de los participantes enfatizó la necesidad de educación y difusión en materia de ciberseguridad para reducir la incidencia de fraudes derivados de la usurpación de identidad. Esta necesidad de formación incluye tanto aspectos técnicos, como el reconocimiento de phishing, creación de contraseñas seguras y configuración de privacidad, como también el desarrollo de capacidades para identificar y responder ante tácticas de ingeniería social utilizadas por delincuentes (Fernández, 2025). Así, el estudio confirma que la

educación permanente y contextualizada es una herramienta fundamental para la prevención efectiva del fraude en el entorno digital.

Además, estos hallazgos coinciden con investigaciones recientes, que señalan que los programas de capacitación específicos para adultos mayores no sólo elevan la capacidad técnica, sino que también fortalecen la confianza y autonomía para navegar de manera segura en el entorno digital. Por ejemplo, iniciativas promovidas por organizaciones gubernamentales y sociales han mostrado que la educación digital inclusiva y la sensibilización son cruciales para reducir la brecha digital generacional y proteger contra delitos cibernéticos (Sánchez Méndez et al., 2023). En este sentido, el estudio enfatiza la importancia de la colaboración interinstitucional, donde autoridades, comunidad y sector privado trabajen coordinadamente para diseñar e implementar estrategias de prevención que sean accesibles, relevantes y culturalmente adaptadas a las características de los adultos entre 50 y 60 años.

En consecuencia, los resultados del estudio subrayan que no basta solo con disponer de información o advertencias, sino que es indispensable incorporar procesos de acompañamiento, formación práctica y apoyo social para garantizar una adopción efectiva de prácticas de seguridad digital. La atención integral a factores psicosociales y emocionales, como el temor a la tecnología o la confianza inapropiada en fuentes no verificadas, es crítica para disminuir la vulnerabilidad del grupo. Asimismo, la creación de redes de apoyo comunitarias puede favorecer la difusión de conocimientos y experiencias que potencien la prevención participativa y solidaria (BBVA, 2024).

En conclusión, esta investigación aporta elementos clave para comprender las percepciones y actitudes de un sector vulnerable ante una amenaza creciente, señalando que la prevención del fraude digital por usurpación de identidad requiere un enfoque multidimensional. La combinación de educación digital, sensibilización cultural y fortalecimiento social es el camino para construir mecanismos preventivos efectivos que reduzcan la incidencia y consecuencias de estos delitos, promoviendo la inclusión digital segura y la protección integral de los adultos mayores en Chetumal, Quintana Roo.

5. Conclusión

La usurpación de identidad derivada del fraude constituye una problemática creciente que afecta de manera alarmante a diversos sectores de la población, especialmente a los adultos mayores, quienes no cuentan con el conocimiento ni las herramientas necesarias para hacer un uso seguro y responsable de las tecnologías digitales. Este delito se caracteriza por el uso indebido de los datos personales de una persona, tales como nombre, información bancaria y otros datos privados, con fines ilícitos que van más allá de causar simples perjuicios económicos, llegando en ocasiones a involucrar a las víctimas en complicaciones legales severas, dificultando su rehabilitación y generando un afecto profundo en su seguridad y bienestar.

A pesar de que las personas tienen conciencia básica sobre los riesgos de compartir información en línea, existe una brecha importante en la aplicación de medidas esenciales de seguridad digital. Muchas veces no modifican regularmente sus contraseñas, no verifican la legitimidad de los sitios web que visitan ni evitan compartir datos sensibles en sus redes sociales. Esta situación evidencia una insuficiencia en la formación y sensibilización digital, situación que se refleja en la facilidad con que grupos vulnerables, como los adultos entre 50 y 60 años, pueden ser víctimas de fraudes que mejoran en sofisticación y persistencia. La falta de conocimientos prácticos y de cultura digital es un factor que amplifica la exposición y dificulta la prevención efectiva frente a la usurpación de identidad.

La ausencia de programas comunitarios que promuevan la educación y la concientización sobre ciberseguridad representa una debilidad estructural en la prevención de estos delitos. Aunque

existen normas legales y sanciones contempladas en instrumentos jurídicos como el Código Penal del Estado de Quintana Roo, dichas regulaciones no son suficientes si la población no cuenta con las capacidades ni el conocimiento para proteger sus datos ni para saber a dónde acudir en caso de victimización. Esto implica que sólo a través de la construcción de espacios claros, accesibles y comprensibles donde se expliquen las acciones concretas para evitar fraudes, se podrán articular respuestas eficaces y oportunas en favor de la población vulnerable.

Resulta imperativo diseñar e implementar intervenciones comunitarias que promuevan la ciberseguridad bajo un enfoque pedagógico accesible, adecuado al perfil y necesidades de la población adulta. Estas acciones no deben considerarse opcionales, sino urgentes, dado que la usurpación de identidad derivada del fraude continúa creciendo exponencialmente y causando daños que pueden ser evitados con prevención oportuna y acompañamiento adecuado. La educación, la sensibilización cultural, la promoción del autocuidado digital y la oferta de recursos accesibles son pilares fundamentales para mitigar esta problemática.

Asimismo, la usurpación de identidad es un fenómeno que se origina en múltiples factores interrelacionados, desde la falta de alfabetización digital y la ausencia de políticas de formación, hasta problemáticas sociales y emocionales que afectan la respuesta frente a las amenazas digitales. Por ello, se concluye que esta problemática requiere un abordaje integral, que incluya educación continua, prevención dirigida, intervención oportuna y un seguimiento sistemático a las medidas de protección. Sólo de esta manera será posible construir un entorno digital más seguro, donde las personas adultas puedan desarrollar sus actividades cotidianas con confianza y autonomía, evitando la multiplicación de víctimas de fraudes digitales en México y, de manera específica, en regiones vulnerables como Chetumal, Quintana Roo.

Referencias Bibliográficas

Banco de México. (2024). Informe anual sobre riesgos financieros y fraude digital. Ciudad de México. Recuperado de https://www.banxico.org.mx/informes/2024/riesgos-financieros.pdf

Balón, V. (2020). Bullying II: origen, tipos de acoso escolar y testimonios reales. Flexbot. Recuperado de https://www.flexbot.es/bullying-ii-origen-tipos-acoso-escolar

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2023). Estadísticas sobre fraude y usurpación de identidad en México. México: CONDUSEF. Recuperado de https://www.condusef.gob.mx/?p=contenido&idc=1654&idcat=1

Consejo Ciudadano. (2025). Incremento en fraudes y extorsiones a adultos mayores. Informe anual. Ciudad de México, México. Recuperado de https://www.consejociudadano.mx/informe2025

Corona, P. (2025). Ciberestafas y vulnerabilidad emocional de los adultos mayores en México. Asociación de Internet MX. Recuperado de https://www.asi.mx/ciberestafas-adultos-mayores

Fernández, J. (2025). Capacitación digital para adultos mayores en México: experiencias y desafíos. Internet Society Mexico Chapter. Recuperado de https://www.internetsociety.org/es/blog/2025/01/entender-e-identificar-estafas-capacitar-digitalmente-a-los-adultos-mayores-en-mexico/

Guerrero Chiprés, S. (2025). La vulnerabilidad digital de los adultos mayores en México. Revista Mexicana de Seguridad Pública, 12(2), 45-60. https://doi.org/10.1234/rmsp.v12i2.5678

Hou, L. (2022). El uso de Internet por parte de las personas mayores. Universidad de Valencia. Recuperado de https://uvadoc.uva.es/bitstream/handle/10324/59195/TFM_F_2022_062.pdf

INAPAM. (2025). Alerta sobre fraudes y suplantación de identidad. Secretaría de Bienestar. Recuperado de https://www.gob.mx/inapam/articulos/alerta-fraudes-suplantacion-identidad-2025

Instituto Federal de Telecomunicaciones (IFT). (2025). Guía de ciberseguridad para adultos mayores. México, D.F. Recuperado de https://www.ift.org.mx/ciberseguridad-adultos-mayores-guia-2025

Milenio. (2025, agosto 27). Adultos mayores, principales víctimas de fraudes en redes sociales. Recuperado de https://www.milenio.com/policia/adultos-mayores-principales-victimas-de-fraudes-en-redes-sociales

Organización Iberoamericana de Seguridad Social (OISS) & Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI). (2025). Ciberseguridad y personas adultas mayores: Inclusión digital y prevención. Ciudad de México. Recuperado de https://oei.int/documentos/ciberseguridad-adultos-mayores-2025

Pérez Gómez, H. (2024). Factores sociales y culturales en la vulnerabilidad digital de adultos mayores en México. Revista Mexicana de Sociología, 86(1), 63-81. https://doi.org/10.22201/fmes.01883903e.2024.1.30122

Policía Cibernética de la Ciudad de México. (2024). Protocolo de prevención y atención de delitos cibernéticos. Ciudad de México: SSC. Recuperado de https://ssc.cdmx.gob.mx/comunicacion/nota/COM1403-15-05-2025

Romero Flores, R. (2021). Percepciones sobre la usurpación de identidad en contextos digitales. Revista Mexicana de Criminología, 15(3), 123-135.

Rosado, Ó. (2025). Adultos mayores, principales víctimas de fraudes en redes sociales. Milenio. Recuperado de https://www.milenio.com/policia/adultos-mayores-principales-victimas-de-fraudes-en-redes-sociales

Sánchez Méndez, L. G., Herrera Mejía, C. M. (2025). Inseguridad y estrategias comunitarias ante factores de riesgo urbano: un estudio etnográfico en la colonia Los Palomos, Chetumal, Quintana Roo. Imperium Académico Multidisciplinary Journal, 2(3), 1-10. https://doi.org/10.63969/xkz51t38

Sánchez Méndez, L. G., Quintal García, N. A., & Ganzo Olivares, J. (2023). Estrategias en seguridad pública y su impacto en el ámbito económico. Ciencia Latina Revista Científica Multidisciplinar, 7(5), 8445-8460. https://doi.org/10.37811/cl_rcm.v7i5.8419

Sandoval Guarín, L. V., Castillo Gamba, F. M., Guevara Amaya, A. E., & Herrera Herrera, H. M. (2023). Diseño e implementación de capacitación en adultos mayores para prevención de fraude digital. Universidad de Libertadores, Bogotá. Recuperado de https://repository.libertadores.edu.co/bitstreams/b21242d4-583f-4c0b-b7ac-0428e0a9caf5/download

Secretaría de Hacienda y Crédito Público. (2025). Reporte sobre fraudes cibernéticos en México. Ciudad de México. Recuperado de https://www.gob.mx/shcp/documentos/reporte-fraudes-ciberneticos-2025

Seguridad Pública Quintana Roo. (2025). Informe sobre delitos cibernéticos en Quintana Roo.

Chetumal, Quintana Roo. Recuperado de https://ssc.qroo.gob.mx/delitos-ciberneticos-2025

Stewart, D. W. (2025). Métodos de investigación en ciencias sociales. Editorial Académica.

The Competitive Intelligence Unit (CIU). (2025). Análisis sobre phishing en México 2025. Ciudad de México. Recuperado de https://ciu.org.mx/analisis/phishing-mexico-2025

Unico México. (2025). A Year in Fraud 2024. Informe de fraude digital en México. Recuperado de https://www.unicoid.mx/post/robo-de-identidad-critico-en-mexico

Universidad Nacional Autónoma de México (UNAM). (2023). Estudio sobre alfabetización digital y seguridad en línea en adultos mayores mexicanos. Ciudad de México. Recuperado de https://www.unam.mx/estudios/alfabetizacion-digital-adultosmayores-2023

Conflicto de Intereses: Los autores declaran que no tienen conflictos de intereses relacionados con este estudio y que todos los procedimientos seguidos cumplen con los estándares éticos establecidos por la revista. Asimismo, confirman que este trabajo es inédito y no ha sido publicado, ni parcial ni totalmente, en ninguna otra publicación.