https://doi.org/10.69639/arandu.v13i3.2622

Buenas prácticas de navegación segura por Internet para personas de tercera edad y grupos vulnerables

Best Practices for Safe Internet Browsing Among Older Adults and Vulnerable Groups

Mariano Xiu Chan
mariano.xiu@cecyteqroo.edu.mx
https://orcid.org/0009-0004-2666-9877
CECyTE Cancún III
México – Cancún Quintana Roo

Iliana Margarita Medina Zumaya
iliana.medina@cecyteqroo.edu.mx
https://orcid.org/0009-0001-8478-5399
CECyTE Cancún IV
México – Cancún Quintana Roo

David Alejandro Aké Rosado
david.ake@cecyteqroo.edu.mx
https://orcid.org/0009-0008-3230-4726
CECyTE Cancún III
México – Cancún Quintana Roo

Yeimi Cordova de la Rosa
yeimi.cordova@cecyteqroo.edu.mx
https://orcid.org/0009-0006-2894-9578
CECyTE Cancún III
México – Cancún Quintana Roo

Rocío Arceo Díaz
rarceo@utcancun.edu.mx
https://orcid.org/0009-0008-7670-3649
Universidad Tecnológica de Cancún
México – Cancún Quintana Roo

Artículo recibido: 10 agosto 2026- Aceptado para publicación:16 septiembre 2026
Conflictos de intereses: Ninguno que declarar.

RESUMEN

La ciberseguridad en los hogares, con especial consideración para menores de edad y personas de la tercera edad, es de crucial interés hoy en día, ya que las familias están siendo objetivos de frecuentes ataques cibernéticos, en especial menores de edad y adultos mayores, ya que son vulnerables por contar con un conocimiento técnico menor y estar más expuestos a estafas en línea. En esta propuesta, se consideran las herramientas y buenas prácticas enfocadas a este grupo poblacional, para que tengan una navegación segura por internet, proteger su información, datos personales e información financiera. Además, crear una cultura de prevención, permitirá una tranquilidad cuando hagan uso del internet. A diferencia de los menores (niños), en los cuales la vulnerabilidad está ligada a la sobreexposición sin supervisión; Las estafas dirigidas a adultos

mayores por internet son un problema que ha ido en aumento en los últimos años, estas estafas surgen por la buena fe y la disposición de ayudar de los adultos mayores, causando pérdidas financieras significativas y angustia emocional, por lo que al sentirse vulnerables en la navegación en internet, crea incertidumbre, rechazo por la tecnología, a veces la falta de acceso a medios digitales, la falta de habilidades para usar internet, junto con la exposición a fraudes, puede generar ansiedad y aislamiento. La mayoría de los adultos mayores enfrentan dificultades para realizar trámites en línea y acceder a servicios que cada vez se operan mayormente en línea, esto puede afectar su calidad de vida y aumentar su sensación de vulnerabilidad, que los deja intranquilos y sin paz. Por lo anterior se brindó una capacitación rápida y guía de buenas prácticas de ciberseguridad en los hogares, con un enfoque a personas de la tercera edad y algunas recomendaciones del uso de internet para menores.

Palabras clave: Ciberseguridad, delitos cibernéticos, buenas prácticas, navegación segura

ABSTRACT

Cybersecurity in households, with particular consideration for minors and older adults, is crucial for ensuring peace of mind in today's digital environment. Families are increasingly becoming targets of frequent cyberattacks, particularly minors and older adults, who may be more vulnerable due to limited technical knowledge and greater exposure to online scams. This proposal considers tools and best practices aimed at these population groups to promote safe Internet browsing and protect their information, personal data, and financial information. In addition to fostering a culture of prevention, these measures can provide greater peace of mind when using the Internet. Unlike minors, whose vulnerability is often associated with unsupervised overexposure to the Internet, online scams targeting older adults have become an increasingly serious problem in recent years. These scams often take advantage of older adults' good faith and willingness to help, resulting in significant financial losses and emotional distress. Feelings of vulnerability can affect their peace of mind. Furthermore, limited access to digital resources, insufficient Internet skills, and exposure to online fraud may contribute to anxiety and social isolation. Many older adults face difficulties when completing online procedures and accessing services that are increasingly provided through digital platforms. This situation can negatively affect their quality of life and increase their sense of vulnerability and insecurity. Therefore, a brief training session and a guide to cybersecurity best practices for households were provided, with a particular focus on older adults, along with recommendations for the safe use of the Internet by minors.

Keywords: Cybersecurity, cybercrime, best practices, safe Internet browsing

Todo el contenido de la Revista Científica Internacional Arandu UTIC publicado en este sitio está disponible bajo licencia Creative Commons Atribution 4.0 International.

INTRODUCCIÓN

La digitalización nos permite disponer y acceder a trámites y servicios más rápidamente y a veces más eficaces y eficientes. No podemos dejar de contemplar las rupturas, las brechas digitales y la inseguridad que afectan, tanto a las personas adultas mayores, como a los menores con acceso a internet. Los adultos mayores son propensos a delitos cibernéticos, de los que el fraude es el más frecuente, de acuerdo con reportes de la Policía Cibernética de la Secretaría de Seguridad Ciudadana. (Alcalá & Meléndez, 2023).

La vulnerabilidad de los adultos mayores en el entorno digital es un problema que ha ido en aumento, donde la falta habilidades para usar internet, la falta de herramientas de seguridad, hacen que sean blanco para fraudes y delitos informáticos, escuchar estas noticias o tener alguna mala experiencia, provoca que los adultos mayores sientan ansiedad, temor y muchas veces opten por no tener contacto con medios digitales, lo que puede provocar aislamiento e incertidumbre. (Ramírez Mesa, 2020).

Antecedentes Teóricos

En 2018, cada 60 segundos se registraron 3,7 millones de búsquedas en Google, se enviaron 38 millones de WhatsApp, 18 millones de mensajes de texto, 481.000 tweets y 187 millones de email (Desjardins, 2018). Sin contar que la evolución desde la fecha hasta hoy en día de las aplicaciones y servicios, hacen más demandante la evolución digital, tanto para menores como para adultos mayores.

Entre los factores que se han determinado como contribuyentes a la vulnerabilidad digital de niños y adultos mayores:

Sobreexposición sin supervisión: En el caso de los menores, a veces pasan tanto tiempo en aplicaciones, uso de internet sin supervisión, que se van desenvolviendo en el mundo digital sin restricciones y pueden ser blanco de ataques o de algún delito informático y sin darse cuenta son vulnerados.

Brecha digital: Es común que los adultos mayores presenten un rezago al utilizar los nuevos dispositivos y aplicaciones, hablando tanto de hardware como de software, existe una disparidad significativa en el acceso a internet como hoy lo conocemos y como posiblemente la gente mayor actual lo conoció. Actualmente hay un sinfín de dispositivos y de aplicaciones que para muchos adultos mayores los deja rezagados en la adopción de tecnología.

Falta de habilidades digitales: En muchas ocasiones la dificultad para aprender y utilizar nuevas tecnologías, sumada a problemas de visión, audición o motricidad, dificulta el acceso a servicios digitales y la participación en actividades en línea de una manera segura.

Exposición a fraudes y estafas: Los adultos mayores son un blanco frecuente de fraudes en línea, lo que genera miedo y desconfianza hacia la tecnología y para los menores de igual manera es un riesgo ya que dan clic sin saber que pueden ser sujetos de fraudes. (Oxman, 2013).

Dependencia de la tecnología: La digitalización de servicios básicos, como trámites gubernamentales, atención médica, la banca, solicitudes de citas, servicios en general pueden generar dependencia y dificultades para aquellos que no pueden acceder a estos servicios en línea, lo que genera desesperación y a veces el uso de portales o aplicaciones no seguras, acceso indebido o captura de información sensible con tal de obtener el servicio.

Complejidad de las aplicaciones: A veces las aplicaciones y acceso a servicios, representan un reto para los adultos mayores, ya que como se ha mencionado anteriormente hay una brecha digital, el desconocimiento y que no siempre son intuitivas las pantallas puede generar una frustración o el rezago en el uso de alguna tecnología.

Estudios demuestran que, ante la brecha digital y la frustración tecnológica, se presentan situaciones como:

Aislamiento social: Cuando el adulto mayor o incluso los menores, no cuentan con las habilidades o el acceso a internet, pueden limitar su interacción social y aislarse, ya que no se sienten en iguales condiciones que sus pares, muchas veces no solicitan apoyo para estas actividades y prefieren aislarse.

Impacto en la calidad de vida: La dependencia no es cómoda para las personas mayores, con características como aislamiento, brecha digital, acceso limitado a internet, falta de comprensión para el uso de aplicaciones e incluso la interacción social que se da en línea y de la cual no siempre pueden formar parte, va generando un impacto negativo en su calidad de vida.

Dificultad para realizar trámites y acceder a servicios: Muchas dependencias, han modificado su manera de brindar servicios, muchos de los trámites como la solicitud de turnos médicos, pago de facturas o acceso a información se complican cuando solo se ofrecen en línea y no contemplan a los adultos mayores que no siempre tienen las habilidades para acceder a estos de una manera digital.

Aislamiento y pérdida de relaciones: También hay casos, en donde la dificultad para conectarse con familiares y amigos a través de plataformas digitales puede aumentar el aislamiento social y la sensación de soledad. En el caso de los menores son vulnerables al tener habilidades para navegar e interactuar en redes sociales, peor sin tener la madurez emocional para participar en este tipo de plataformas, hay riesgos de seguridad, que, si bien las redes sociales expresamente indican que es para mayores de edad, se puede acceder con datos falsos.

Estrés y ansiedad: La preocupación por fraudes, la dificultad para utilizar la tecnología y la falta de acceso a servicios pueden generar estrés y ansiedad en los adultos mayores, de igual manera en los menores se ha detectado el estrés y la ansiedad por no contar con el acceso a la tecnología o por interrumpir su uso, ante alguna medida de descanso.

Objetivo: El objetivo de este proyecto fue analizar las vulnerabilidades a la que se encuentran expuestos los adultos mayores, referente a su uso cotidiano en internet, después

brindar un taller con las herramientas, buenas prácticas y recomendaciones que permitan reducir estas vulnerabilidades.

MATERIALES Y MÉTODOS

En un estudio realizado a 100 personas adultas mayores, entre 70 a 80 años, con diferentes actividades y necesidades de uso de internet, nos centramos en los tipos de vulnerabilidades que nos comentan o que se deduce que fueron objeto por usar internet en los últimos dos años.

Para ello, se consideró una encuesta con entrevista para recabar información, esto como herramienta de recolección de datos, con el instrumento, se logró identificar la edad, nivel del uso de dispositivo con conexión a internet, experiencia y frecuencia en el uso de internet; este estudio se realizó en dos ocasiones, una antes de brindar la charla y las buenas prácticas, brindarles información acerca de los cuidados y compartirles videos de fraudes y delitos informáticos y como prevenirlos, 3 meses después de la capacitación se realizó la misma encuesta y se logró identificar las mejoras en el nivel de uso de los medios digitales.

Cabe mencionar que estas personas motivo de estudio son personas cercanas a los investigadores, lo que permite conocer a detalle las anécdotas y el actuar. El principal objetivo del acercamiento es conocer a lo que se están enfrentando los adultos mayores en el uso de internet, para el caso de los niños, no se realizó propiamente un estudio, solo se comentan los casos que se referencian por la cercanía y como resultado de la encuesta y entrevista con la familia del adulto mayor.

De acuerdo a la recopilación de información, las vulnerabilidades a la que se han enfrentado las personas mayores son:

Engaños por suplantación de identidad: Los estafadores se comunican con adultos mayores haciéndose pasar por sus nietos o familiares en apuros, solicitando dinero urgentemente, este tipo de engaño también se presenta con menores de edad, que piensan que tienen comunicación con otro menor y en realidad están vulnerables comunicándose con una persona que finge ser otra. (Medero, 2012).

Estafas con tarjetas de regalo: A veces se ven promociones extraordinarias, para acceder a algún servicio, venta de un producto o para cobrar algún premio se solicita el pago con tarjetas de regalo, aprovechando que son fáciles de adquirir y difíciles de rastrear. (González, 2014)

Estafas de soporte técnico: Los estafadores se hacen pasar por técnicos de soporte, contactan a las víctimas para solucionar problemas inexistentes y luego les cobran por servicios inexistentes, esto requiere a veces ingeniería social por parte de los estafadores.

Estafas románticas: Cada vez hay más casos registrados en la policía cibernética de que se crean perfiles falsos en línea y establecen relaciones sentimentales con adultos mayores o con menores para luego solicitar dinero, regalos o para un delito mayor.

Robo de información: Una de las principales vulnerabilidades es el robo de información con fines económicos, los estafadores buscan acceder a la información bancaria de los adultos mayores o que los niños proporcionen esta información de las tarjetas de sus tutores, a veces se realiza el robo de información de una manera automatizada, a través de alguna aplicación maliciosa encargada de recopilar esta información sensible y enviarla a los estafadores, otras veces se obtiene la información persuadiendo al usuario para brindarla vía telefónica, en un chat o a través de un formulario, en ambos casos el objetivo es contar con la información para otro delito. (Arias, 2014).

RESULTADOS Y DISCUSIÓN

Como resultados de la aplicación de la encuesta, revisando los datos se destaca que la edad de los participantes es de 69 a 80; El 92% cuenta con un dispositivo móvil con acceso a internet y el 42% con acceso a una computadora, tableta u otro dispositivo en casa que se conecta a internet, el 100% cuenta con conexión a internet, ya sea por el contrato del proveedor de servicio de internet, a través del modem o a través de datos de su dispositivo telefónico. El 95% admite que el servicio de internet es por la necesidad de una tercera persona como por sus hijos, nietos o que conviven con ellos y no sienten que sea una necesidad primaria de ellos, sin embargo, el 90% admite que realiza al menos una vez al mes alguna transacción vía internet. De los participantes solo el 26% tiene y está consciente de una cuenta de correo electrónica, que si bien no todos consultan, fue necesaria crear la cuenta para algún otro servicio; el 23% cuenta con una red social diferente a una aplicación de mensajería instantánea, en contraste tenemos que hasta el 80% cuenta con una aplicación de mensajería, el 38% tiene acceso a sus aplicaciones de banca electrónica, y el 32% hacen uso de otras aplicaciones por Internet, este constituye un dato muy importante ya que vemos que los adultos mayores si hacen uso de aplicaciones de internet, aunque muchas veces no son del todo conscientes de ello.

Principalmente mencionan que usan el internet para comunicarse, admiten compartir datos y navegar en algunas aplicaciones conforme van requiriendo, muchos indican que han explotado más la tecnología durante la pandemia.

Con base a la información recaba sobre las vulnerabilidades a la que se han enfrentado los adultos mayores, se les diseñaron y compartieron a través de infografías, charlas y videos diferentes estrategias para mejorar su seguridad en el uso del internet y sus aplicaciones, si bien no todos tienen las habilidades del uso de las tecnologías de la información, al menos se logró concientizar de los peligros que existen.

Se presentaron las siguientes estrategias y buenas prácticas:

Acceso a programas de alfabetización digital: Ofrecer programas de capacitación accesibles y adaptados a las necesidades de los adultos mayores para mejorar sus habilidades

digitales, los que tienen posibilidades poder tomar cursos en línea o presencial, al menos documentarse con boletines de seguridad.

Acceder a aplicaciones con diseño de interfaces accesibles: Promover el uso de aplicaciones más intuitivas, claras y fáciles de usar para todos, incluyendo a personas con discapacidades. Muchas veces puede mejorar la experiencia de usuario con mejores colores, personalizado opciones o buscando el uso de herramientas de accesibilidad, que son herramientas que se enfocan en asegurar que las aplicaciones sean perceptibles, operables, comprensibles y robustas para todos los usuarios.

Alternativas no digitales: Es importante no forzar la digitalización, considerar que, si existen opciones no digitales para acceder a servicios como trámites presenciales o atención telefónica, quizá el adulto mayor se sentirá más confiado y cómodo haciendo uso de estos y no forzar a que migre a la opción digital.

Sensibilización sobre fraudes: Informar y educar a los adultos mayores sobre los riesgos de fraudes en línea y cómo protegerse, en este caso indicando sin mayor detalle técnico como saber si es una página segura, buscar sitios con https, considerar el uso del antivirus, el firewall, al menos que no se confíen de todo lo que aparece en internet y no den el clic solo porque se les solicita, sino estar conscientes de adonde y porque se accede a cada espacio en internet. (García, 2019).

Fomento de la inclusión social: Dentro de lo posible, el acompañamiento y nos percatamos que compartir con sus nietos, hijos, puede colaborar para crear espacios y actividades que promuevan la interacción social y el uso de la tecnología de forma segura y beneficiosa.

Educación: Informar a los adultos mayores sobre los tipos de estafas más comunes y cómo identificarlas, una charla como anécdota, puede inspirar para no cometer errores comunes.

Verificación: Verificar la información antes de enviar dinero o proporcionar información personal, los adultos mayores son vulnerables para brindar información, una buena práctica es que no se comparta información con desconocidos o que se identifique cual es la información sensible, como cuentas bancarias, contraseñas. (Muriel Diéguez, 2023).

Comunicación: Fomentar la comunicación abierta y honesta entre los adultos mayores y sus familiares, brindarles el espacio para aprender, preguntar, ayudarles en el uso de la tecnología, que puede ser un reto mayor para ellos.

Apoyo: Brindar apoyo emocional y práctico a las víctimas de estafas, que en alguna minoría han padecido alguna experiencia, pero es mejor estar presentes y acompañarlos para superar la situación.

Denuncia: Denunciar los casos de estafa a las autoridades competentes, como la policía cibernética, en caso de alguna situación que requiera el apoyo de la autoridad, es mejor hacer la denuncia correspondiente.

Explicar los riesgos comunes como phishing, malware, y estafas en línea: Si bien no es necesario el manejo de terminología o jerga informática que puede abrumar al menor de edad o al adulto mayor, es importante que estén conscientes de la existencia de los delitos y de cómo se comportan los estafadores para que estén alertas ante cualquier situación que llame su atención.

Enseñar a identificar correos electrónicos y mensajes sospechosos: Se puede iniciar con algo sencillo como identificar el spam, la publicidad engañosa, revisar ejemplos de correos no seguros.

Informar sobre la importancia de mantener software y sistemas operativos actualizados.

Recomendar no hacer clic en enlaces sospechosos o descargar archivos de fuentes desconocidas.

Contraseñas seguras y autenticación: Utilizar contraseñas complejas y únicas para cada cuenta, es un tema recurrente el uso de las contraseñas, la recuperación y perdida de las mismas, en este caso la concientización del uso de las contraseñas es lo más importante y se puede apoyar a crear una metodología donde escriban y resguarden alguna clave, indicio de la contraseña real.

Revisión de configuraciones de privacidad: Revisar la configuración de privacidad en redes sociales y aplicaciones, es un abuena practica la explicación de las redes y de que no todo es real en ellas, una buena práctica es la búsqueda de un nombre común, para que vean las opciones que salen y como podrían hablar con alguien equivocado.

También es importante, estar atentos a las señales de alerta y concientizar a las personas mayores de estas señales, tales como:

Solicitud de atención o envío de información con urgencia: Siempre que se solicita información de manera urgente hay que desconfiar, los estafadores suelen crear un sentido de urgencia para evitar que las víctimas piensen y valoren la situación o soliciten apoyo con familiares o amigos, por lo que cuando se presente la situación de una solicitud expedita, que requieran compartir información o incluso que les avisen que están siendo objeto de un fraude y que requieren atender de prisa la situación, hay que valorar antes de acceder a la solicitud.

Solicitudes de dinero: De los casos más frecuentes, son las solicitudes de dinero, especialmente si se hacen a través de métodos poco seguros como transferencias bancarias o tarjetas de regalo, son una señal de alerta, incluso por supuestas solicitudes de familiares, para ello es buena práctica establecer palabras claves o determinar que nada se hace por mensaje o llamada.

Solicitud de información personal: Las solicitudes de información personal o financiera, como números de cuentas bancarias o contraseñas, no debería ser una solicitud común, por lo cual no deben de ser atendidas, aunque según provengan de instituciones confiables, al contrario, se debe considerar que las instituciones como las bancarias no suelen hacer solicitudes de información personal y mucho menos se solicitan claves y contraseñas.

Mensajes con errores ortográficos y gramaticales: Al recibirse un mensaje, correo electrónico, validar si viene con errores ortográficos o gramaticales frecuentes pueden ser una señal de que la comunicación no es legítima, si está en otro idioma, con caracteres raros, si viene con adjuntos no solicitados o de un remitente que no se conozca, es mejor no abrir los correos.

Llamadas o contactos de números desconocidos: La recomendación, es incluso no contestar números desconocidos y desconfiar de números con códigos de área extraños. (Astorga-Aguilar, C., & Schmidt-Fonseca, 2019).

CONCLUSIONES

Después de haber brindado los talleres, para personas de la tercera edad y aplicar la segunda encuesta, se aprecian mejores respuestas en cuanto a las buenas prácticas, se validan las aplicaciones que tienen instaladas, se priorizan las aplicaciones que requieren datos personales o los involucran para funcionar, ya se pueden identificar las aplicaciones sensibles de operar y que comprometerían información, tales como la banca electrónica, correo, mensajería instantánea, se aplica seguridad básica como autenticación de dos pasos, contraseñas más seguras, ya no se instalan aplicaciones sin revisar que provenga de un proveedor legítimo y que sea libre de virus, algo muy importante es que ahora no se abren ligas, se da clic a contenido que se comparte o se escanean códigos QR solo por invitación, incluso la información que se comparte vía mensajería ya están conscientes que puede ser sensible, antes podían compartir incluso fotografías de tarjetas bancarias, identificación oficial, las contraseñas eran débiles, actualmente si bien no se puede hablar de uso en un alto nivel de seguridad del internet si han mejorado sus prácticas y se toman más precauciones al usar internet.

En conclusión, la medida más efectiva es el apoyo y acompañamiento en el uso de las tecnologías, tratar de involucrarse activamente en la configuración de dispositivos y la identificación de riesgos, explicar con paciencia y reforzar frecuentemente el tema de la seguridad en el uso del internet, además de fomentar con los adultos mayores un clima de confianza para que puedan preguntar sobre cualquier duda y ejecución de una tarea en internet. Existen algunas organizaciones que ofrecen cursos especializados para adultos mayores que buscan mejorar sus habilidades digitales, fomentar esta capacitación, siempre que el adulto mayor tenga la disposición por aprender.

Mientras más estrategias, herramientas, medidas de seguridad se brinden, el usuario adulto mayor tendrá más confianza, más seguridad y por lo tanto mayor paz.

La ciberseguridad aplicada al uso de internet y dispositivos en usuarios hogareños y personas de mayor edad, es un esfuerzo continuo que requiere estar atentos a las nuevas aplicaciones y nuevas rupturas de seguridad, son importantes las buenas prácticas, la concientización y un enfoque proactivo al navegar en internet.

REFERENCIAS

Alcalá Casillas, M. G., & Meléndez Ehrenzweig, M. Á. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. PAAKAT: revista de tecnología y sociedad, 13(24).

Ramírez Mesa, C., & González López, J. C. (2020). Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes.

Desjardins, J. (2018). What Happens in an Internet Minute in 2018? Visual Capitalist. Recuperado de https://.visualcapitalist.com/internet-minute-2018/

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del" phishing" y el" pharming". Revista de derecho (Valparaíso), (41), 211-262.

Medero, G. S. (2012). Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos. Boletín de Información, (324), 67-88.

García, A. A. (2019). Ciberseguridad: ¿Por qué es importante para todos? Siglo XXI Editores México.

González Suárez, M. (2014). Fraudes en Internet y estafa Informática (Master's thesis).

Muriel Diéguez, J. A. (2023). Estudio de los delitos de estafa continuada a través de internet y su competencia jurisdiccional.

Arias, Á. (2014). Las estafas digitales. IT Campus Academy.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. Revista Electrónica Educare, 23(3), 339-362.