

Efectividad de la Educación Financiera Para Promover el uso Seguro de Herramientas Tecnológicas y Prevenir Estafas en los Clientes Adultos Mayores del Banco Nacional de Costa Rica

Effectiveness of Financial Education to Promote the Safe use of Technological Tools and Prevent Fraud in Senior Clients of the Banco Nacional de Costa Rica

Cristopher Adrián Zúñiga Villalobos¹, Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)
2024

Resumen

La motivación principal para investigar sobre la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y prevenir estafas en clientes adultos mayores del Banco Nacional de Costa Rica radicó en el creciente aumento de estafas dirigidas a adultos mayores y la necesidad de fortalecer sus conocimientos en el uso seguro de tecnologías financieras. El problema expuesto se centró en la vulnerabilidad de los adultos mayores ante fraudes financieros debido a la falta de conocimientos tecnológicos y de seguridad.

El objetivo principal de la investigación fue evaluar la efectividad de los programas educativos del banco en la prevención de estafas y el uso seguro de herramientas digitales entre esta población. Para alcanzar este objetivo, se establecieron objetivos específicos que incluyeron evaluar el conocimiento previo de los clientes sobre seguridad digital, identificar las áreas de mayor vulnerabilidad y medir el impacto de la educación financiera recibida.

La hipótesis planteada fue que una educación financiera efectiva reduciría la vulnerabilidad de los adultos mayores a las estafas y mejoraría su uso de tecnologías financieras. Se utilizó un enfoque cuantitativo y una investigación exploratoria para recolectar datos a través de cuestionarios aplicados a 50 clientes adultos mayores del Banco Nacional de Costa Rica. Los procedimientos incluyeron la elaboración y aplicación del cuestionario, el análisis de respuestas y la interpretación de los resultados.

Las conclusiones principales revelaron que, a pesar de las medidas avanzadas de seguridad implementadas por el Banco Nacional de Costa Rica, los adultos mayores mostraron resistencia a adoptar nuevas tecnologías y carecían de conocimientos prácticos sobre seguridad en línea. La falta de confianza en las

¹ ¹ Licenciado en Administración de Empresas, UCYAR, Auditor para ISO 9001:2015, Yellow Belt Six Sigma, Scrum Master Professional Certificate, actualmente analista de procesos de la Unidad de Planificación y Gestión de Crédito del Banco Nacional de Costa Rica. ORCID (0009-0003-0505-2934). Correo electrónico: czunigav@bncr.fi.cr

herramientas digitales y la insuficiente educación financiera contribuyeron a su vulnerabilidad ante fraudes. Se destacó la necesidad de mejorar la capacitación y la educación práctica para garantizar que los adultos mayores puedan utilizar efectivamente las tecnologías de protección.

Palabras Clave: Educación Financiera, Adulto Mayor, Herramientas Tecnológicas, Ciberseguridad, Fraudes y Estafas.

Abstract (300 words)

The main motivation for investigating the effectiveness of financial education to promote the safe use of technological tools and prevent fraud among senior clients of Banco Nacional de Costa Rica was the increasing rise in scams targeting seniors and the need to strengthen their knowledge in the safe use of financial technologies. The exposed problem centered on the vulnerability of seniors to financial fraud due to a lack of technological and security knowledge.

The primary objective of the research was to evaluate the effectiveness of the bank's educational programs in preventing fraud and the safe use of digital tools among this population. To achieve this objective, specific goals were established, including assessing the clients' prior knowledge of digital security, identifying the areas of greatest vulnerability, and measuring the impact of the received financial education.

The hypothesis proposed was that effective financial education would reduce seniors' vulnerability to scams and improve their use of financial technologies. A quantitative approach and exploratory research were used to collect data through questionnaires administered to 50 senior clients of Banco Nacional de Costa Rica. The procedures included developing and administering the questionnaire, analyzing responses, and interpreting the results.

The main conclusions revealed that, despite the advanced security measures implemented by Banco Nacional de Costa Rica, seniors showed resistance to adopting new technologies and lacked practical knowledge about online security. The lack of confidence in digital tools and insufficient financial education contributed to their vulnerability to fraud. The need to improve training and practical education was highlighted to ensure that seniors can effectively use protective technologies.

Key Words: Financial Education, Senior Client, Technological Tools, Cybersecurity, Frauds and Scams.

Introducción

Descripción del Proyecto

En un contexto donde los adultos mayores estaban cada vez más expuestos a cibercrímenes, la educación financiera se convirtió en una herramienta crucial para su protección. El Banco Nacional de Costa Rica implementó diversas iniciativas para educar a esta población sobre el uso seguro de herramientas tecnológicas y la prevención de estafas. Sin embargo, la efectividad de estos esfuerzos y su impacto real en la reducción de fraudes aún no se había evaluado a profundidad.

Este estudio se centró en analizar cómo el Banco Nacional de Costa Rica abordó las barreras educativas y qué medidas habían sido efectivas para proteger a los adultos mayores. El objetivo se enfocó en proponer mejoras concretas que fortalecieran la protección de los adultos mayores y promovieran un uso más seguro de las herramientas digitales en Costa Rica.

Justificación del Trabajo de Investigación

La creciente vulnerabilidad de los adultos mayores frente al cibercrimen, como reflejaron las estadísticas de estafas y los métodos utilizados por los delincuentes, resaltó la necesidad urgente de mejorar su educación financiera. Las barreras educativas y la falta de conocimiento sobre herramientas tecnológicas contribuyeron significativamente a su exposición a fraudes, como el phishing y vishing, que afectaron su seguridad financiera.

Esta investigación fue crucial para entender cómo las deficiencias en la educación financiera pudieron ser abordadas de manera efectiva para proteger a esta población.

Beneficios del Trabajo de Investigación

Esta investigación permitió identificar las brechas existentes en la educación financiera de los clientes adultos mayores del Banco Nacional de Costa Rica, proporcionando información valiosa para mejorar las estrategias de prevención de estafas. Al abordar estas brechas, la investigación contribuyó a fomentar la inclusión financiera y a mejorar la calidad de vida de los adultos mayores, promoviendo una mayor igualdad de oportunidades.

Además, la investigación ayudó a sensibilizar al Banco Nacional de Costa Rica sobre la importancia de desarrollar programas de capacitación más efectivos. Esto le permitió ajustar sus estrategias y recursos en función de las necesidades específicas de los adultos mayores, promoviendo su bienestar económico y social, contribuyendo a la creación de comunidades más seguras y resilientes, alineándose con objetivos globales para un desarrollo sostenible y equitativo.

Formulación de la pregunta de investigación

¿Cuál es la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y prevenir estafas en los clientes adultos mayores del Banco Nacional de Costa Rica?

Objetivo General

Evaluar la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y prevenir estafas en los clientes adultos mayores del Banco Nacional de Costa Rica.

Objetivos Específicos

- 1) Identificar las principales barreras que enfrentan los adultos mayores clientes del Banco Nacional de Costa Rica, debido a la falta de educación financiera y cómo estas barreras contribuyen a su vulnerabilidad frente a estafas.
- 2) Describir las estafas más frecuentes que afectan a los adultos mayores clientes del Banco Nacional de Costa Rica y cómo estas estafas están relacionadas con deficiencias en la educación financiera.
- 3) Examinar las medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas y su efectividad en la prevención de fraudes.
- 4) Determinar las mejores prácticas internacionales en educación financiera para proponer ajustes específicos que el Banco Nacional de Costa Rica podría adoptar para mejorar la protección de los adultos mayores contra estafas.

Forma de Alcanzar los Objetivos

Hernández (2014) explica que el enfoque cuantitativo, “parte de una idea que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica” (p. 4), por lo tanto, esta investigación presentó un enfoque cuantitativo.

El tipo de investigación es exploratoria ya que, “los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes” (Hernández, 2014, p. 91).

Las fuentes primarias correspondieron a los cuestionarios aplicados y datos internos del Banco Nacional y las secundarias a estudios, informes y publicaciones previos.

Se realizaron los muestreos a conveniencia según Sampieri. Para esto se elaboró un cuestionario, a fin de facilitar la recopilación de los datos. Se aplicaron 50 cuestionarios efectivos a clientes adultos mayores del Banco Nacional de Costa Rica, entre las semanas 4^a a la 7^a de este periodo académico 2024.

Marco Teórico

En el presente apartado se exploraron los conceptos más relevantes para la investigación, los cuales son: la educación financiera, la persona adulta mayor, estafas y ciberseguridad y su relación con las Fintech.

Educación Financiera

La Organización para la Cooperación y el Desarrollo Económico (2005) detalló que:

La educación financiera es el proceso mediante el cual los consumidores/inversores financieros mejoran su comprensión de los productos y conceptos financieros y, a través de la información, la instrucción y/o el asesoramiento objetivo, desarrollan las habilidades y la confianza para ser más

conscientes de los riesgos y oportunidades financieras, tomar decisiones informadas, saber a dónde acudir en busca de ayuda y tomar otras medidas eficaces para mejorar su bienestar financiero. (p. 13)

Aunado a lo anterior, el Banco Nacional (2023) definió la educación financiera de la siguiente manera:

La oportunidad de informar a los clientes y a las comunidades locales sobre cómo tomar decisiones responsables en asuntos financieros. Esto se puede lograr si los clientes del banco comprenden mejor los conceptos y productos del CFBNCR y si se desarrolla una cultura de consumo responsable. (p. 58)

El Banco Central de Costa Rica (2018) destacó que “la Enfiho 2015 también reveló un menor nivel de educación financiera entre las mujeres, jóvenes menores de 20 años y adultos mayores, así como en personas con menor grado de educación y bajos ingresos” (p. 39), por lo tanto, la persona adulta mayor formó parte del segmento de vulnerabilidad a consecuencia de la baja calidad de su educación financiera.

En el apartado de Democratización de la economía, el Banco Nacional apuntó a “aumentar el porcentaje de clientes del CFBNCR que participan de los programas en los siguientes segmentos: adulto mayor, menores de 15 años y mujeres. Diseñar una metodología que mida el impacto de los programas de educación financiera” (Banco Nacional de Costa Rica [BNCR], 2023, p. 49)

Persona Adulta Mayor

La Comisión Interamericana de Derechos Humanos delimitó “la persona mayor como: aquella de 60 años o más, salvo que la ley interna determine una edad base menor o mayor, siempre que esta no sea superior a los 65 años” (Comisión Interamericana de Derechos Humanos, 2022, p. 31).

Ampliando el concepto anterior, Díaz (2019) conceptualizó lo siguiente:

Se denomina persona mayor (PM) o personas mayores (PMs), preferentemente, frente a anteriores denominaciones como adulto mayor, o persona adulta mayor, a partir de la adopción de la Convención Interamericana sobre la Protección de los Derechos Humanos de las Personas Mayores por la Organización de los Estados Americanos (OEA) en junio de 2015. En cuanto a la edad a partir de la cual se considera a una persona, PM, el consenso internacional generado por las organizaciones internacionales del sistema de Naciones Unidas, particularmente la Organización Panamericana de la Salud (OPS), ha establecido los 60 años de edad como límite etario inferior para el grupo de personas mayores. En general, en los países más desarrollados se establece a partir de 65 años y en los países menos desarrollados a partir de los 60 años (Salmerón, Juan et al., Vejez, mujer y educación. Un enfoque cualitativo de trabajo socioeducativo, Madrid, Dykinson, 2014). La mayor parte de los países de la región de América Latina y el Caribe comparten el criterio de los 60 años, salvo Costa Rica y Ecuador. Por su parte, se considera persona muy mayor a la de 75 años y más. (p. 7)

Con respecto a la persona adulta mayor y su vulnerabilidad, el INEC (2022) destacó que:

Al revisar esta carga de gasto financiero entre los hogares de distinto perfil se encuentran algunas diferencias significativas que pueden visibilizar situaciones de mayor vulnerabilidad a sufrir riesgos de dificultades financieras. Entre estas se tiene que los hogares endeudados donde la persona de referencia es adulta mayor (65 años o más), el porcentaje que presenta deudas mayores al 30 % de sus ingresos alcanza el 32,6 %. (p. 18)

Para asegurar un enfoque adecuado de las partes interesadas, en este caso, la persona adulta mayor, el PMBoK (2017) resaltó lo siguiente:

Gestión de los Interesados del Proyecto. Incluye los procesos requeridos para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación eficaz de los interesados en las decisiones y en la ejecución del proyecto. (p. 24)

En el contexto del Banco Nacional de Costa Rica, la educación financiera para adultos mayores se erigió como una estrategia crucial para fortalecer la relación con este segmento de clientes. Para asegurar su éxito en este rol, el banco debía reconocer que "las organizaciones eficientes sobreviven gracias a que escuchan a sus clientes, traducen la información que obtienen de ellos en acciones apropiadas, y alinean sus procesos clave de negocio para respaldar esos deseos" (Summers, 2006, p. 60).

Estafa

En el Código Penal de Costa Rica, se definió la estafa como un delito que involucraba el engaño para obtener un beneficio patrimonial. Así se estipuló en el "Artículo 216.- Quien induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno." Código Penal [CP]. Ley 4573 de 1970. 05 de mayo de 1993 (Costa Rica).

Debido a la aparición de delitos informáticos, se tuvo que ampliar la legislación para incluir este tipo de estafas. En Costa Rica, se estableció en el "Artículo 217 bis.- Estafa informática: Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro." Código Penal [CP]. Ley 4573 de 1970. 10 de julio de 2012 (Costa Rica).

Ciberseguridad

El MICIT precisó la ciberseguridad como un “conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio” (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017, p. 50).

El Banco Nacional (2023) determinó la ciberseguridad de la siguiente manera:

Con el aumento de la banca electrónica y el almacenamiento de datos en la nube, es importante salvaguardar la privacidad de los usuarios y la protección de las operaciones bancarias de las amenazas que se originan tanto desde dentro como desde fuera del CFBNCR, asegurando así el funcionamiento adecuado de los servicios y la confianza de los usuarios. (p. 57)

Relacionado a la ciberseguridad, es relevante detallar el término Fintech que se estableció de la siguiente manera:

Fintech es una palabra que se usa a menudo para describir casi cualquier tipo de startup que utiliza algún nivel de tecnología para crear un producto o servicio financiero. Sin embargo, hay dos tipos distintos de empresas emergentes de tecnología financiera: – Startups Fintech que brindan servicios financieros habilitados por la tecnología en los que el uso de la tecnología permite una mayor eficiencia, escala y velocidad en un producto o proceso industrial existente. Trabajan con instituciones financieras (IF) para reemplazar los procesos y sistemas existentes. – Startups Fintech que aporten soluciones novedosas para una actividad específica de servicios financieros utilizando tecnología. Estas ofertas de servicios financieros impulsados por la tecnología ahora dominan el ecosistema Fintech. (Pranay y Tham, 2018, p. 10).

En el mismo contexto de ciberseguridad, herramientas tecnológicas y Fintech, el Banco Nacional (2023) especificó el concepto de Transformación e innovación Digital de la siguiente manera:

La evolución tecnológica ha permitido al Conglomerado revolucionar su modelo de negocio. Esta transformación se consigue de forma eficiente si las personas internas y externas al Conglomerado tienen el nivel de conocimiento necesario para seguir el proceso de informatización de las operaciones. (p. 56)

Comprender los términos técnicos en ciberseguridad resultó ser de gran valor para esta investigación. Un concepto fundamental de entender fue malware, el cual "hace referencia a todo tipo de software malicioso o dañino cuyo objetivo sea infectar ordenadores, tabletas o teléfonos móviles" (Arroyo, Gayoso y Hernández, 2020, p. 19).

En el estudio de técnicas de fraude, se destacó el concepto de suplantación de identidad, que "consiste en hacerse pasar por otra persona para obtener un beneficio, ya sea económico o de cualquier otro tipo" (Arroyo, Gayoso y Hernández, 2020, p. 30).

Al analizar métodos de ataque, se abordó la ingeniería social, que "consiste en engañar a los usuarios para que faciliten de manera voluntaria información personal confidencial (contraseñas o datos bancarios) que permita el acceso a un equipo e instalar software malicioso" (Arroyo, Gayoso y Hernández, 2020, p. 37).

Metodología de la investigación

Enfoque de la Investigación

La investigación se realizó con un enfoque cuantitativo, adecuado para evaluar la efectividad de la educación financiera en promover el uso seguro de herramientas tecnológicas y prevenir estafas entre los clientes adultos mayores del Banco Nacional de Costa Rica. Este enfoque permitió recopilar y analizar datos numéricos, proporcionando una base sólida para evaluar los resultados y formular recomendaciones.

El enfoque seleccionado detalló que "en una investigación cuantitativa se intenta generalizar los resultados encontrados en un grupo o segmento (muestra) a una colectividad mayor (universo o población). También se busca que los estudios efectuados puedan replicarse." (Hernández, 2014, p. 6).

Tipo de Investigación

La investigación empleada fue de tipo exploratoria, lo que permitió identificar y comprender factores clave, percepciones y desafíos iniciales en la educación financiera de los adultos mayores.

Hernández (2014) explica que este tipo de investigaciones "generalmente determinan tendencias, identifican áreas, ambientes, contextos y situaciones de estudio, relaciones potenciales entre variables; o establecen el "tono" de investigaciones posteriores más elaboradas y rigurosas" (p. 4). Estas características facilitaron la formulación de recomendaciones efectivas para mejorar el uso seguro de herramientas tecnológicas y prevenir estafas.

Tamaño de Población, Muestra y Tipo de Muestreo

En el contexto de esta investigación, se utilizó un modelo de muestreo por conveniencia para la selección de los participantes. Según Battaglia (2008) citado por Hernández et al., (2014), detalló que las muestras por conveniencia "están formadas por los casos disponibles a los cuales tenemos acceso" (p.390).

Se llevó a cabo un cuestionario dirigido a una muestra de 50 clientes adultos mayores del Banco Nacional de Costa Rica para la recolección de datos primarios. El cuestionario constó de 22 preguntas cerradas, diseñadas para evaluar el nivel de educación financiera, el conocimiento sobre la prevención de estafas y el uso de herramientas tecnológicas para servicios financieros. La escogencia del tipo de pregunta "depende del grado en que se puedan anticipar las posibles respuestas, los tiempos de que se disponga para codificar y si se quiere una respuesta más precisa o profundizar en alguna cuestión." (Hernández, 2014, p. 221).

La aplicación del cuestionario se realizó mediante la plataforma digital Microsoft Forms, lo que facilitó la participación de los clientes y garantizó una recolección eficiente de los datos.

Hipótesis

La implementación de iniciativas de educación financiera por parte del Banco Nacional de Costa Rica dirigida a sus clientes adultos mayores resultó en una mejora significativa en el conocimiento sobre el uso seguro de herramientas tecnológicas y en la reducción de estafas, al abordar las principales barreras educativas y aplicar medidas efectivas de protección.

Instrumentos

Se elaboró un cuestionario con el fin de evaluar la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y la prevención de estafas en los clientes adultos mayores del Banco Nacional de Costa Rica. El cuestionario se definió como “un conjunto de preguntas respecto de una o más variables a medir. Debe ser congruente con el planteamiento del problema e hipótesis” (p. 217; Chasteauneuf, 2009; Brace, 2013, como se citó en Hernández, 2014).

Análisis de resultados

En este apartado se detallaron los resultados derivados de los cuestionarios aplicados a 50 adultos mayores, clientes del Banco Nacional de Costa Rica. Estos resultados proporcionaron una comprensión completa de las percepciones de este grupo respecto a su nivel de educación financiera y a las iniciativas del Banco Nacional para educarles en la prevención de fraudes y estafas. El análisis profundo de estos datos permitió abordar los objetivos específicos planteados, aportando una visión más clara del impacto y la efectividad de la educación financiera en la promoción del uso seguro de herramientas tecnológicas y en la prevención de estafas en los clientes adultos mayores del Banco Nacional de Costa Rica.

Principales barreras que enfrentan los adultos mayores clientes del Banco Nacional de Costa Rica, debido a la falta de educación financiera y cómo estas barreras contribuyen a su vulnerabilidad frente a estafas.

Figura 1

Pregunta 1. ¿Con qué frecuencia utiliza herramientas tecnológicas para realizar transacciones bancarias?



En la Figura 1 se observó que el 34% de los encuestados, equivalente a 17 personas, indicó utilizarlas diariamente. Un 28%, correspondiente a 14 personas, mencionó hacerlo semanalmente. Por otro lado, un 14% de los participantes, es decir, 7 personas, afirmó que nunca las utiliza. Finalmente, el 12% de los encuestados, representando 6 personas, utilizaron estas herramientas de manera mensual o rara vez.

Figura 2

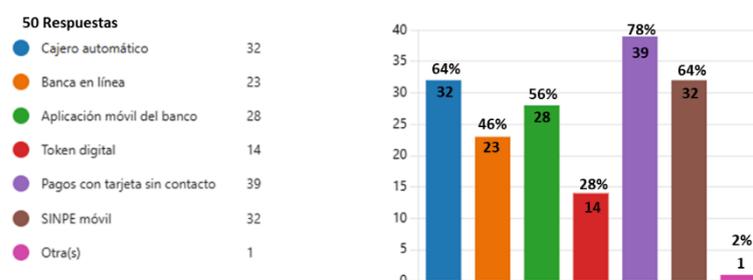
Pregunta 2. ¿Se siente seguro al utilizar herramientas tecnológicas para sus transacciones bancarias?



Según la Figura 2, se observó que el 72% de los encuestados, que corresponde a 36 personas, expresó sentirse seguro. En contraste, un 28% de los participantes, es decir, 14 personas, indicó que no se sentía seguro al utilizar dichas herramientas.

Figura 3

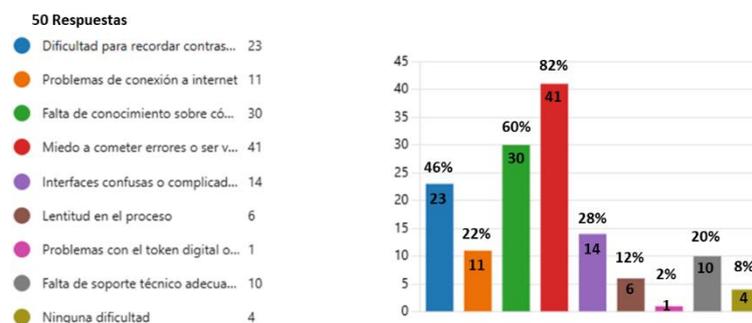
Pregunta 3. ¿Qué herramientas tecnológicas utiliza para realizar transacciones bancarias? (Seleccione todas las que apliquen)



En la Figura 3 se detalló que, de las herramientas tecnológicas utilizadas para realizar transacciones bancarias, el 78% de los encuestados, equivalente a 39 personas, indicó utilizar pagos con tarjeta sin contacto. El 64%, es decir, 32 personas, mencionó emplear tanto cajeros automáticos como SINPE móvil. Además, el 56% de los participantes, correspondiente a 28 personas, señaló que utiliza la aplicación móvil del banco, mientras que el 46%, equivalente a 23 personas, usó la banca en línea. Un 28%, representando a 14 personas, indicó que utiliza el token digital, por último, solo el 2% que corresponde a 1 persona mencionó utilizar otra herramienta.

Figura 4

Pregunta 4. ¿Cuáles son las principales dificultades que enfrenta al utilizar estas herramientas? (Seleccione todas las que apliquen)

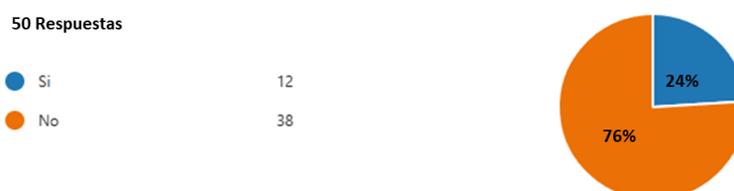


En la Figura 4 se evidenció que, de los 50 encuestados, el 82% manifestó enfrentar dificultades relacionadas con el miedo a cometer errores o ser víctima de estafas, lo que representa a 41 personas. Un 60%, equivalente a 30 personas, mencionó la falta de conocimiento sobre cómo utilizar las herramientas, y un 46%, correspondiente a 23 personas, indicó tener dificultad para recordar contraseñas. Por otro lado, un 28% de los participantes, es decir, 14 personas, señaló que las interfaces son confusas o complicadas, mientras que un 22%, equivalente a 11 personas, reportó problemas de conexión a internet como una dificultad. Además, un 20%, representando a 10 personas, mencionó la falta de soporte técnico adecuado, y un 12%, es decir, 6 personas, indicó la lentitud en el proceso. Un 8%, equivalente a 4 personas, indicó no enfrentar ninguna dificultad y solo el 2% que corresponde a 1 persona reportó problemas con el token digital o físico.

Estafas más frecuentes que afectan a los adultos mayores clientes del Banco Nacional de Costa Rica y cómo estas estafas están relacionadas con deficiencias en la educación financiera.

Figura 5

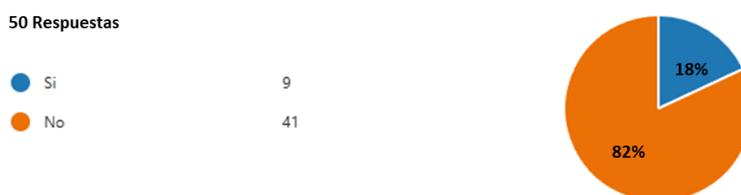
Pregunta 5. ¿Está familiarizado con el término "malware"?



En la Figura 5 se mostró que la mayoría de los encuestados, un 76%, equivalente a 38 personas, no estaba familiarizada con el término "malware". Por otro lado, un 24% de los participantes, es decir, 12 personas, indicó que sí estaba familiarizado con dicho término.

Figura 6

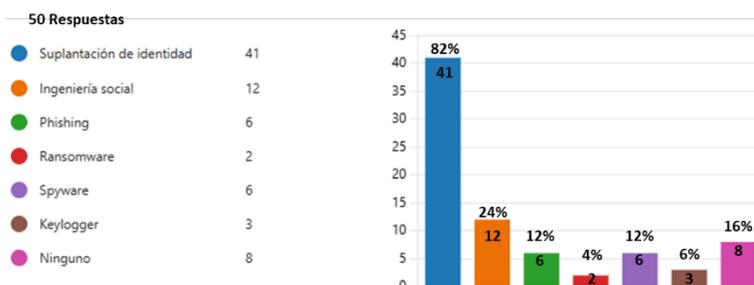
Pregunta 6. ¿Conoce los diferentes tipos de malware, como ransomware, spyware, phishing, keylogger?



En la Figura 6 se observó que la mayor parte de los encuestados, un 82%, equivalente a 41 personas, no conocía los diferentes tipos de malware, como ransomware, spyware, phishing y keylogger. En contraste, solo un 18% de los participantes, es decir, 9 personas, afirmó conocer estos tipos de malware.

Figura 7

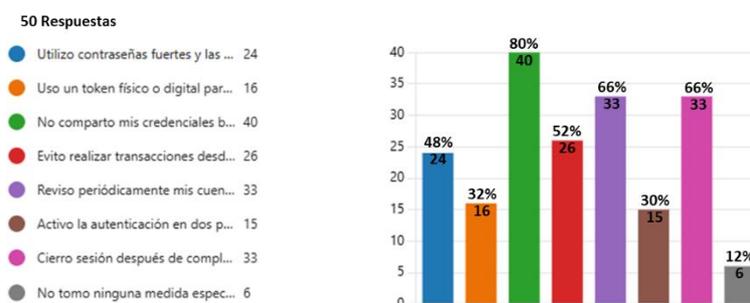
Pregunta 7. ¿Cuál o cuáles de los siguientes conceptos relacionados con estafas y seguridad informática le son familiares? (Seleccione todas las que apliquen)



En la Figura 7 se reveló que el concepto de suplantación de identidad era familiar para el 82% de los encuestados, lo que corresponde a 41 personas. Un 24% de los participantes, es decir, 12 personas, estaba familiarizado con el concepto de ingeniería social. El 16% de los encuestados, es decir, 8 personas, indicó no estar familiarizado con ninguno de estos conceptos. Tanto para phishing y spyware, el 12%, equivalente a 6 personas, conocía su significado. Por su parte, el 6%, representado por 3 personas, estaba familiarizado con el concepto keylogger, y apenas un 4%, correspondiente a 2 personas, conocía sobre los ransomware.

Figura 8

Pregunta 8. ¿Qué medidas de seguridad toma al realizar transacciones bancarias en línea? (Seleccione todas las que apliquen)

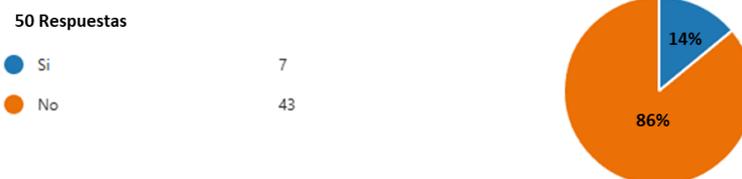


En la Figura 8 se indicó que el 80% de los encuestados, equivalente a 40 personas, no compartía sus credenciales bancarias con nadie al realizar transacciones bancarias en línea. Un 66%, es decir, 33 personas, revisaba periódicamente sus cuentas bancarias para detectar movimientos sospechosos. Con el mismo porcentaje, afirmaron que también cerraban sesión después de completar una transacción. El 52% de los participantes, equivalente a 26 personas, evitaba realizar transacciones desde redes Wi-Fi públicas. Un 48%, representado por 24 personas, utilizaba contraseñas fuertes y las cambiaba regularmente. Además, el 32%, equivalente a 16 personas, usaba un token físico o digital para confirmar transacciones, y el 30%, correspondiente a 15 personas, activaba la autenticación en dos pasos cuando estaba disponible. Finalmente, un 12% de los encuestados, es decir, 6 personas, no tomaba ninguna medida especial de seguridad.

Medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas y su efectividad en la prevención de fraudes.

Figura 9

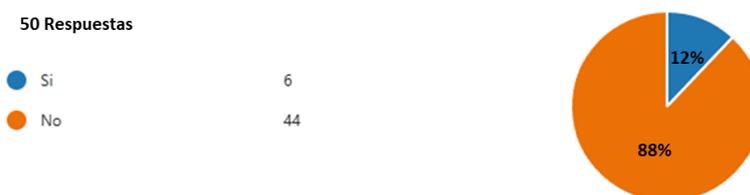
Pregunta 9. ¿Ha participado en algún programa de educación financiera ofrecido por el Banco Nacional?



Según la Figura 9 se evidenció que el 86%, equivalente a 43 personas, no había participado en ningún programa de educación financiera ofrecido por el Banco Nacional. En contraste, solo un 14% de los participantes, es decir, 7 personas, había tomado parte en dicho programa.

Figura 10

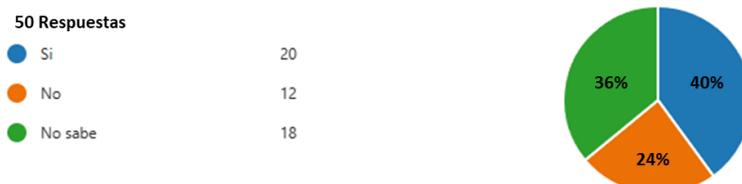
Pregunta 10. Si ha participado en un programa de educación financiera, ¿considera que el programa fue útil para comprender mejor cómo protegerse de estafas?



En la Figura 10 se mostró que gran parte de los encuestados, un 88%, equivalente a 44 personas, consideró que el programa de educación financiera no fue útil para comprender mejor cómo protegerse de estafas. Solo un 12% de los participantes, es decir, 6 personas, encontró que el programa fue útil en ese aspecto.

Figura 11

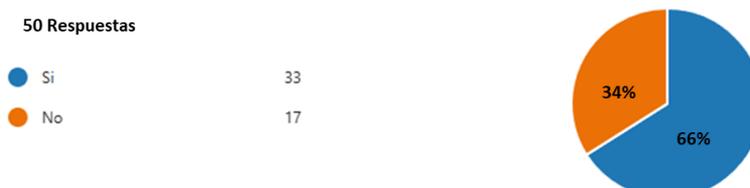
Pregunta 11. ¿Considera que las herramientas tecnológicas ofrecidas por el Banco Nacional son efectivas para prevenir estafas?



En la Figura 11 se observó que el 40% de los encuestados, equivalente a 20 personas, consideró que las herramientas tecnológicas ofrecidas por el Banco Nacional eran efectivas para prevenir estafas. Un 36%, es decir, 18 personas, no sabía si estas herramientas eran efectivas o no. Finalmente, un 24% de los participantes, correspondiente a 12 personas, no creía en la efectividad de las herramientas para prevenir estafas.

Figura 12

Pregunta 12. ¿Confía en las medidas de seguridad implementadas por el Banco Nacional al realizar transacciones en línea?



En la Figura 12 se evidenció que el 66% de los encuestados, equivalente a 33 personas, confiaba en las medidas de seguridad implementadas por el Banco Nacional al realizar transacciones en línea. En contraste, un 34% de los participantes, es decir, 17 personas, no confiaba en dichas medidas de seguridad.

Figura 13

Pregunta 13. ¿Utiliza algún dispositivo inteligente (smartphone, tablet) para realizar sus gestiones bancarias?



En la Figura 13 se mostró que el 62% de los encuestados, equivalente a 31 personas, utilizaba algún dispositivo inteligente (smartphone, tablet) para realizar sus gestiones bancarias. En contraste, un 38% de los participantes, es decir, 19 personas, no usaba dispositivos inteligentes para tales gestiones.

Figura 14

Pregunta 14. ¿Tiene acceso a internet en su hogar o dispositivo móvil?



En la Figura 14 se evidenció que el 98% de los encuestados, equivalente a 49 personas, tenía acceso a internet en su hogar o dispositivo móvil. En contraste, solo un 2% de los participantes, es decir, 1 persona, no contaba con acceso a internet.

Figura 15

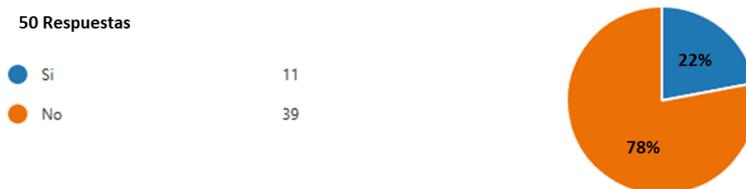
Pregunta 15. ¿Dispone de un token físico para realizar transacciones bancarias?



En la Figura 15 se reveló que el 96% de los participantes, es decir, 48 personas, no contaba con un token físico. En contraste, solo el 4% de los encuestados, equivalente a 2 personas, disponía de un token físico para realizar transacciones bancarias.

Figura 16

Pregunta 16. ¿Está usted enterado de que el token físico dejará de funcionar en Agosto de 2024?



En la Figura 16 se mostró que un 78% de los participantes, es decir, 39 personas, no estaba informado sobre esta medida. El 22% de los encuestados, equivalente a 11 personas, estaba enterado de que el token físico dejaría de funcionar en agosto de 2024.

Figura 17

Pregunta 17. ¿Sabe cómo utilizar el token digital para la autenticación en línea?



En la Figura 17 se observó que el 64% de los participantes, es decir, 32 personas, no sabía cómo utilizar el token digital. Por otro lado, el 36% de los encuestados, equivalente a 18 personas, sabía cómo utilizar el token digital para la autenticación en línea.

Figura 18

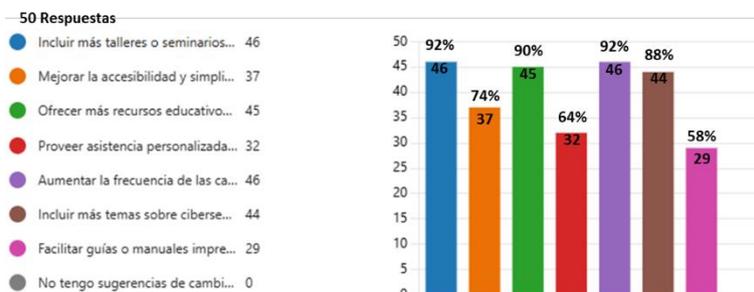
Pregunta 18. Para la autenticación en línea ¿Qué opción prefiere utilizar el token físico o el token digital?



En la Figura 18 se evidenció que el 72% de los encuestados, equivalente a 36 personas, prefería utilizar el token digital para la autenticación en línea. En contraste, un 28% de los participantes, es decir, 14 personas, prefería el token físico.

Figura 19

Pregunta 19. ¿Qué cambios o mejoras sugeriría para los programas de educación financiera o las herramientas tecnológicas del banco? (Seleccione todas las que apliquen)



En la Figura 19 se evidenció que el 92% de los encuestados, equivalente a 46 personas, sugirió incluir más talleres o seminarios prácticos sobre el uso seguro de herramientas tecnológicas y aumentar la frecuencia de las campañas de concientización sobre fraudes y estafas. Un 90%, es decir, 45 personas, propuso ofrecer más recursos educativos en formato audiovisual, como videos y tutoriales. El 88%, equivalente a 44 personas, recomendó incluir más temas sobre ciberseguridad en los programas de educación financiera. Además, el 74% de los encuestados, que correspondió a 37 personas, indicó que se debía mejorar la accesibilidad y simplificar el uso de las plataformas digitales para personas mayores. El 64% de los participantes, es decir, 32 personas, sugirió proporcionar asistencia personalizada en línea o por teléfono para resolver dudas. Finalmente, el 58% de los encuestados, correspondiente a 29 personas, recomendó facilitar guías o manuales impresos para el uso de las herramientas tecnológicas. Ningún encuestado manifestó no tener sugerencias de cambios o mejoras en este momento.

Mejores prácticas internacionales en educación financiera para proponer ajustes específicos que el Banco Nacional de Costa Rica podría adoptar para mejorar la protección de los adultos mayores contra estafas.

Figura 20

Pregunta 20. ¿Qué tan relevante considera que el Banco Nacional se adapte a las mejores prácticas internacionales para proteger a los adultos mayores contra estafas?



En la Figura 20 se mostró que un 78%, equivalente a 39 personas, consideró que era muy importante que el Banco Nacional se adaptara a las mejores prácticas internacionales para proteger a los adultos mayores contra estafas. Un 18% de los

participantes, es decir, 9 personas, lo consideró importante. Solo un 4% de los encuestados, correspondiente a 1 persona, lo consideró poco importante y no importante.

Figura 21

Pregunta 21. ¿Participaría en un taller de simulaciones de estafas, como ejercicios de phishing, para mejorar su capacidad de detectar amenazas cibernéticas?



En la Figura 21 se evidenció que el 86% de los encuestados, equivalente a 43 personas, estaría dispuesto a participar en un taller de simulaciones de estafas, como ejercicios de phishing, para mejorar su capacidad de detectar amenazas cibernéticas. En contraste, un 14% de los participantes, es decir, 7 personas, no participaría en dicho taller.

Figura 22

Pregunta 22. ¿Considera que un taller de simulaciones de estafas, aumentaría su confianza en la identificación de fraudes en línea?



En la Figura 22 se mostró que el 90% de los encuestados, equivalente a 45 personas, consideró que un taller de simulaciones de estafas aumentaría su confianza en la identificación de fraudes en línea. Solo un 10% de los participantes, es decir, 5 personas, no creía que dicho taller tuviera ese efecto.

Discusión

El análisis del estudio sobre la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y prevenir estafas en los clientes adultos mayores del Banco Nacional de Costa Rica proporcionó información valiosa sobre la relación entre la educación financiera, la seguridad tecnológica, el conocimiento respecto a ciberseguridad y la vulnerabilidad de esta población ante fraudes y estafas. Este apartado discute el significado de los resultados obtenidos, evalúa la hipótesis planteada, examina los principales hallazgos y ofrece sugerencias para investigaciones futuras.

Los resultados del estudio indicaron que, a pesar de los esfuerzos del Banco

Nacional de Costa Rica en implementar medidas de seguridad avanzadas, los adultos mayores presentaban una notable falta de conocimiento y habilidades para utilizar adecuadamente estas herramientas. Esta brecha en el conocimiento resalta la importancia de considerar no solo la disponibilidad de medidas de seguridad, sino también la capacidad de los usuarios para comprender y aplicarlas efectivamente. La falta de educación financiera y de capacitación en el uso de tecnologías avanzadas se identificó como un factor crítico que incrementa la vulnerabilidad de los adultos mayores a fraudes y estafas en línea.

Otro hallazgo clave fue la identificación de incongruencias entre la percepción de seguridad de los adultos mayores y la realidad de las medidas de protección implementadas por el Banco Nacional. Aunque las herramientas como la autenticación multifactorial y los tokens digitales fueron introducidas con el objetivo de mejorar la seguridad, su efectividad se vio limitada por la falta de familiaridad y confianza en estas tecnologías por parte de los usuarios. Este fenómeno sugiere que la implementación de medidas de seguridad no puede ser el único enfoque; es necesario garantizar que los usuarios comprendan cómo y por qué usar estas herramientas para que puedan ser realmente efectivas.

Aunado al punto anterior, el análisis reveló que, aunque los adultos mayores estaban expuestos a tecnologías avanzadas, su capacidad para aplicarlas de manera segura seguía siendo deficiente. Este hallazgo es especialmente relevante dado que muestra que la simple familiarización con las tecnologías no es suficiente para proteger a los usuarios contra amenazas cibernéticas y refuerza de que se requiere una educación integral que combine el conocimiento teórico con la capacidad práctica para manejar estas herramientas de manera segura.

Con respecto a la hipótesis planteada en el estudio, que afirmaba que los adultos mayores presentan una mayor susceptibilidad a fraudes debido a la falta de educación financiera en el ámbito tecnológico, fue parcialmente aceptada. Los resultados confirmaron que una falta de educación financiera contribuye significativamente a la vulnerabilidad de los adultos mayores a estafas. Sin embargo, también se evidenció que la efectividad de las medidas de seguridad ofrecidas estaba condicionada por el nivel de comprensión de los adultos mayores sobre el uso de estas herramientas.

Lo anterior sugiere que, aunque la hipótesis inicial era correcta en cuanto a la falta de educación financiera como un factor de vulnerabilidad, también se corroboró un aspecto adicional: la efectividad de las medidas de seguridad es directamente proporcional al nivel de entendimiento y confianza del usuario en estas medidas. Por lo tanto, la aceptación de la hipótesis es válida, pero debe ser combinada con la necesidad de mejorar tanto la educación financiera como la implementación de medidas de seguridad para que sean realmente útiles y efectivas para los adultos mayores.

Uno de los hallazgos más destacados del estudio fue la falta de conocimiento práctico sobre el uso seguro de herramientas tecnológicas entre los adultos mayores. A pesar de estar familiarizados con el uso de dispositivos inteligentes, muchos de ellos no estaban al tanto de las prácticas recomendadas para proteger su información personal y financiera. Esto demuestra que la exposición a la

tecnología no garantiza un comportamiento seguro en línea y resalta la necesidad de una educación más profunda y práctica.

El estudio reveló que las medidas de seguridad como la autenticación multifactorial y los tokens digitales, no estaban siendo utilizadas de manera efectiva. Los resultados indicaron que la falta de confianza y la complejidad percibida de estas herramientas contribuyeron a su bajo uso.

Un resultado sorprendente fue la resistencia de algunos adultos mayores a adoptar nuevas tecnologías de seguridad debido a una falta de confianza en estas herramientas. Este hallazgo resalta una brecha significativa entre la intención del banco de proporcionar una protección robusta y la capacidad de los usuarios para aprovechar estas medidas. La resistencia puede deberse a una combinación de factores, como el temor a cometer errores y la percepción de que las herramientas de seguridad son innecesarias o complicadas.

Para abordar las limitaciones identificadas en este estudio, se recomienda realizar investigaciones adicionales en varias áreas clave. En primer lugar, es fundamental explorar enfoques más efectivos para la educación financiera de adultos mayores que no solo aborden el conocimiento teórico, sino que también proporcionen capacitación práctica en el uso seguro de tecnologías. Esto podría incluir el desarrollo de programas educativos interactivos, talleres prácticos que faciliten una comprensión más profunda y la aplicación efectiva de las medidas de seguridad.

Además, futuras investigaciones deberían evaluar la percepción de los adultos mayores sobre las medidas de seguridad actuales y cómo estas pueden ser adaptadas para mejorar su aceptación y uso. Es importante investigar cómo presentar estas herramientas de manera que sean vistas como accesibles y útiles, en lugar de una barrera adicional. La investigación también podría explorar la eficacia de diferentes métodos de comunicación y soporte técnico en la mejora de la adopción de prácticas de seguridad.

Finalmente, se consideró importante que el Banco Nacional de Costa Rica investigue el potencial de nuevas tecnologías, como soluciones basadas en inteligencia artificial, para ofrecer una protección más robusta y sencilla para los adultos mayores. La inteligencia artificial y el aprendizaje automático podrían proporcionar capacidades avanzadas para detectar y prevenir fraudes en tiempo real, adaptadas a las necesidades específicas de esta población.

Conclusiones

A continuación, se presentan las conclusiones de cada objetivo específico planteado.

Principales barreras que enfrentan los adultos mayores clientes del Banco Nacional de Costa Rica, debido a la falta de educación financiera y cómo estas barreras contribuyen a su vulnerabilidad frente a estafas.

Las principales barreras que enfrentaron los adultos mayores incluían el miedo a cometer errores o ser víctimas de estafas, la falta de conocimiento sobre el uso de

herramientas tecnológicas y la dificultad para recordar contraseñas. Estas dificultades limitaban su uso eficiente y aumentaban el riesgo de fraudes. Aunque muchos se sentían seguros utilizando estas tecnologías, una parte significativa no compartía esta confianza, lo que incrementaba su vulnerabilidad. Las herramientas más utilizadas fueron los pagos sin contacto, cajeros automáticos y SINPE móvil, mientras que el token digital tuvo una adopción limitada. Además, problemas técnicos como interfaces complicadas y falta de soporte adecuado subrayaron la necesidad de mejorar la accesibilidad y el apoyo técnico, así como de fortalecer la educación financiera.

Estafas más frecuentes que afectan a los adultos mayores clientes del Banco Nacional de Costa Rica y cómo estas estafas están relacionadas con deficiencias en la educación financiera.

Los adultos mayores clientes del Banco Nacional de Costa Rica enfrentaban una vulnerabilidad significativa ante estafas debido a deficiencias en su educación financiera. La mayoría no estaba familiarizada con términos y conceptos de seguridad informática, como "malware", y tipos de malware específicos, lo que los hacía susceptibles a diferentes tipos de ataques. Aunque tomaban algunas medidas de seguridad, como no compartir credenciales y revisar cuentas periódicamente, su desconocimiento sobre otras amenazas y prácticas de seguridad avanzadas, como la autenticación en dos pasos o el uso de tokens, indicaba una preparación insuficiente.

Medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas y su efectividad en la prevención de fraudes.

La perspectiva de los encuestados respecto a las medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas resultó insuficientes y poco efectivas. La mayoría de los encuestados no ha participado en los programas de educación financiera del banco, y aquellos que lo hicieron no consideraron que fueran útiles para comprender cómo protegerse de estafas. Aunque algunos confiaban en las herramientas tecnológicas, una parte no las encontraba efectivas o no estaba familiarizada con su uso, especialmente en el caso del token digital. Los encuestados sugirieron mejoras en los programas de educación financiera y herramientas tecnológicas.

Mejores prácticas internacionales en educación financiera para proponer ajustes específicos que el Banco Nacional de Costa Rica podría adoptar para mejorar la protección de los adultos mayores contra estafas.

La mayoría de los adultos mayores consideró fundamental que el Banco Nacional de Costa Rica adopte mejores prácticas internacionales en educación financiera para protegerlos contra estafas. Además, mostraron disposición a participar en talleres de simulaciones de estafas, lo cual indicaba que este tipo de iniciativas podría aumentar su confianza en la identificación de fraudes en línea. Estos hallazgos sugirieron la necesidad de implementar más programas de educación financiera.

Recomendaciones

Principales barreras que enfrentan los adultos mayores clientes del Banco Nacional de Costa Rica, debido a la falta de educación financiera y cómo estas barreras contribuyen a su vulnerabilidad frente a estafas.

Ante las barreras identificadas en los adultos mayores clientes del Banco Nacional de Costa Rica, las recomendaciones estuvieron orientadas a fortalecer la educación financiera y brindar mayor apoyo en el uso de tecnologías. Se sugirió la implementación de talleres de capacitación especializados que abordaran, de manera sencilla y práctica, el uso seguro de herramientas como los cajeros automáticos, pagos sin contacto, SINPE móvil y el token digital. Estos programas debieron incluirse en jornadas de sensibilización dirigidas a disminuir el miedo a cometer errores y a reforzar la confianza en las nuevas tecnologías.

Asimismo, fue fundamental la creación de campañas de concientización sobre la seguridad digital, enfocadas en la protección contra fraudes, lo cual habría reducido la vulnerabilidad de los adultos mayores frente a las estafas y promovido una mayor inclusión financiera segura. Este enfoque incluyó capacitación sobre aplicaciones útiles para detectar posibles estafas, como True Caller ID, y el uso de la huella digital para ingresar de manera más segura a la banca en línea, la relevancia de mantener actualizada su información personal en las plataformas del BNCR y de activar el doble factor de autenticación para una mayor protección.

Estafas más frecuentes que afectan a los adultos mayores clientes del Banco Nacional de Costa Rica y cómo estas estafas están relacionadas con deficiencias en la educación financiera.

Las recomendaciones para enfrentar las estafas que afectaron a los adultos mayores clientes del Banco Nacional de Costa Rica se centraron en el fortalecimiento de la educación financiera, pero con un enfoque más comunitario y cercano. Se sugirió implementar un programa de voluntariado donde el personal del BNCR brindara talleres y capacitaciones presenciales directamente en las zonas de las comunidades, en lugar de limitarlas a las oficinas del banco.

Este enfoque permitió a los adultos mayores acceder a la información en un entorno familiar y cómodo, facilitando la comprensión de conceptos clave de ciberseguridad como "malware", suplantación de identidad e ingeniería social. Estas sesiones comunitarias, además, incluyeron simulaciones de situaciones de riesgo y soluciones prácticas, fomentando el aprendizaje activo. Al acercar estos recursos educativos a las comunidades, los adultos mayores tuvieron una mayor oportunidad de participar, recibiendo apoyo personalizado y constante. A su vez, el voluntariado reforzó el vínculo entre el banco y sus clientes, contribuyendo a una mayor concientización sobre fraudes y mejorando la seguridad digital de este grupo vulnerable.

Medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas y su efectividad en la prevención de fraudes.

Las recomendaciones estuvieron enfocadas en fortalecer las herramientas de seguridad ya disponibles en el Banco Nacional de Costa Rica, como el uso de la huella digital y el reconocimiento facial para el ingreso a la banca en línea, además de fomentar la adopción del doble factor de autenticación. Se propuso que el banco potenciara estas medidas, promoviendo su uso de manera más amplia entre los adultos mayores y brindando capacitaciones prácticas sobre su implementación.

Asimismo, se sugirió que el banco incorporara inteligencia artificial para aprender los patrones de comportamiento transaccional de los usuarios. Este sistema permitiría que, al detectar anomalías, las cuentas fueran bloqueadas automáticamente y se impidieran movimientos hasta que se verificara la identidad del usuario real, añadiendo una capa adicional de protección contra fraudes. Por otro lado, se recomendó que el banco priorizara la actualización de sistemas operativos obsoletos, abordando con urgencia la obsolescencia tecnológica para reducir superficies de ataque que carecieran de soporte de seguridad. Este enfoque integral habría mejorado significativamente la protección de los adultos mayores, minimizando tanto los riesgos tecnológicos como las vulnerabilidades en sus transacciones bancarias.

Mejores prácticas internacionales en educación financiera para proponer ajustes específicos que el Banco Nacional de Costa Rica podría adoptar para mejorar la protección de los adultos mayores contra estafas.

Se recomendó la implementación de programas educativos continuos, que incluyan talleres, videos y guías, para sensibilizar a los adultos mayores sobre fraudes financieros, suplantación de identidad y ciberseguridad. Se sugirió mantener la autenticación multifactorial (MFA) mediante el uso de tokens digitales y biometría, como huella digital o reconocimiento facial, para asegurar el acceso a cuentas y transacciones. También se recomendó continuar utilizando la herramienta KnowBe4 para capacitar al personal y a los clientes en la identificación de amenazas cibernéticas. Además, se propuso colaborar con autoridades para intercambiar información sobre amenazas emergentes y desarrollar políticas de protección más efectivas.

Referencias

- Arroyo, D., Gayoso, V. y Hernández, L. (2020). *Ciberseguridad*. CSIC. <https://web.p.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzI3MzI5MjZfX0FO0?sid=53b9e020-8514-43ed-a34d-e405aa29f838@redis&vid=4&format=EB&rid=1>
- Banco Central de Costa Rica. (2018). Informe sobre el acceso de las micro, pequeñas y medianas unidades productivas, a los servicios financieros. https://www.bccr.fi.cr/publicaciones/DocSectorReal/Informe_acceso_mipymes_servicios_financieros.pdf
- Banco Nacional de Costa Rica. (2023). Reporte de Sostenibilidad BN 2023. https://www.bncr.fi.cr/_cache_a123/content/1609240000255772.pdf
- CIDH (2022). *Derechos humanos de las personas mayores y sistemas nacionales de protección en las Américas*. Organización de los Estados Americanos (OEA). <https://bibliotecacorteidh.winkel.la/Product/ViewerProduct/2091#page=0>
- Código Penal [CP]. Art. 216 y 217 bis. 04 de mayo de 1970 (Costa Rica).
- Díaz, A. (2019). *Derechos humanos de las personas mayores*. Organización de los Estados Americanos (OEA). <https://bibliotecacorteidh.winkel.la/Product/ViewerProduct/842#page=0>
- Gupta, P. y Tham, T. (2018). *Fintech: The new DNA of financial services*. Walter de Gruyter Inc. <https://web.p.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzlwMjY5MDhfX0FO0?sid=e836e0aa-c524-4ee1-a640-d881c8646eea@redis&vid=2&format=EB&rid=1>
- Hernández, R., Fernández, C. y Baptista, M. (2014). *Metodología de la Investigación*. McGRAW-HILL Interamericana Editores, S.A. de C.V.
- Instituto Nacional de Estadística y Censo. (2022). Encuesta Financiera a Hogares 2022. https://admin.inec.cr/sites/default/files/2023-05/Publicacio%CC%81n%20Resultados%20Enfiho%202022_3.pdf
- Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017). Estrategia Nacional de Ciberseguridad de Costa Rica. http://www.conicit.go.cr/sic/biblioteca_virtual/publicaciones/publica_cyt/otros_doc_cyt/Estrategia-Nacional-Ciberseguridad-CR-19-10-17.pdf
- OECD (2005). *Improving Financial Literacy. Analysis of Issues and Policies*. Organization for Economic Co-operation and Development (OECD). <https://doi.org/10.1787/9789264012578-en>
- PMI. (2017). *Guía de los fundamentos para la dirección de proyectos*. Project Management Institute, Inc.

Summers, D. (2006). *Administración de la calidad*. Pearson Educación de México, S.A. de C.V.

Anexos

Anexo 1. Cuestionario sobre Efectividad de la Educación Financiera Para Promover el uso Seguro de Herramientas Tecnológicas y Prevenir Estafas en los Clientes Adultos Mayores del Banco Nacional de Costa Rica

Introducción

Mi nombre es Cristopher Zúñiga Villalobos, estudiante de la Maestría en Gerencia de Proyectos de la ULACIT. Le invito a participar en esta encuesta para evaluar la educación financiera y la prevención de estafas entre los clientes adultos mayores del Banco Nacional de Costa Rica. Su participación es crucial para mi proyecto de integración. La encuesta es anónima y los datos se utilizarán solo con fines académicos. Agradezco su valiosa cooperación.

Propósito

Evaluar la efectividad de la educación financiera para promover el uso seguro de herramientas tecnológicas y prevenir estafas en los clientes adultos mayores del Banco Nacional de Costa Rica.

Uso

La información facilitada será utilizada exclusivamente para propósitos y fines académicos. La misma sirve para evaluar la hipótesis sobre la implementación de iniciativas de educación financiera por parte del Banco Nacional de Costa Rica dirigida a sus clientes adultos mayores para el uso seguro de herramientas tecnológicas y en la reducción de estafas.

Duración

De 7 a 10 minutos, aproximadamente.

Instrucciones

Por favor, lea cada pregunta cuidadosamente y seleccione la(s) respuesta(s) con la(s) que mejor se identifique.

Objetivo Específico 1: Identificar las principales barreras que enfrentan los adultos mayores clientes del Banco Nacional de Costa Rica, debido a la falta de educación financiera y cómo estas barreras contribuyen a su vulnerabilidad frente a estafas.

Pregunta 1. ¿Con qué frecuencia utiliza herramientas tecnológicas para realizar transacciones bancarias?

- Diariamente
- Semanalmente
- Mensualmente
- Rara vez

Nunca

Pregunta 2. ¿Se siente seguro al utilizar herramientas tecnológicas para sus transacciones bancarias?

- Sí
 No

Pregunta 3. ¿Qué herramientas tecnológicas utiliza para realizar transacciones bancarias? (Seleccione todas las que apliquen)

- Cajero automático
 Banca en línea
 Aplicación móvil del banco
 Token digital
 Pagos con tarjeta sin contacto
 SINPE móvil
 Otra:

Pregunta 4. ¿Cuáles son las principales dificultades que enfrenta al utilizar estas herramientas? (Seleccione todas las que apliquen)

- Dificultad para recordar contraseñas
 Problemas de conexión a internet
 Falta de conocimiento sobre cómo utilizarlas
 Miedo a cometer errores o ser víctima de estafas
 Interfaces confusas o complicadas
 Lentitud en el proceso
 Problemas con el token digital o físico
 Falta de soporte técnico adecuado
 Ninguna dificultad

Objetivo Específico 2: Describir las estafas más frecuentes que afectan a los adultos mayores clientes del Banco Nacional de Costa Rica y cómo estas estafas están relacionadas con deficiencias en la educación financiera.

Pregunta 1. ¿Está familiarizado con el término "malware"?

- Sí
 No

Pregunta 2. ¿Conoce los diferentes tipos de malware, como ransomware, spyware, phishing, keylogger?

- Sí
 No

Pregunta 3. ¿Cuál o cuáles de los siguientes conceptos relacionados con estafas y seguridad informática le son familiares? (Seleccione todas las que apliquen)

- Suplantación de identidad
 Ingeniería social
 Phishing
 Ransomware
 Spyware

- Keylogger
- Ninguno

Pregunta 4. ¿Qué medidas de seguridad toma al realizar transacciones bancarias en línea? (Seleccione todas las que apliquen)

- Utilizo contraseñas fuertes y las cambio regularmente.
- Uso un token físico o digital para confirmar transacciones.
- No comparto mis credenciales bancarias con nadie.
- Evito realizar transacciones desde redes Wi-Fi públicas.
- Reviso periódicamente mis cuentas bancarias para detectar movimientos sospechosos.
- Activo la autenticación en dos pasos cuando está disponible.
- Cierro sesión después de completar una transacción.
- No tomo ninguna medida especial de seguridad.

Objetivo Específico 3: Examinar las medidas actuales implementadas por el Banco Nacional de Costa Rica para proteger a los adultos mayores contra estafas y su efectividad en la prevención de fraudes.

Pregunta 1. ¿Ha participado en algún programa de educación financiera ofrecido por el Banco Nacional?

- Sí
- No

Pregunta 2. Si ha participado en un programa de educación financiera, ¿considera que el programa fue útil para comprender mejor cómo protegerse de estafas?

- Sí
- No
- No aplica

Pregunta 3. ¿Considera que las herramientas tecnológicas ofrecidas por el Banco Nacional son efectivas para prevenir estafas?

- Sí
- No
- No sabe

Pregunta 4. ¿Confía en las medidas de seguridad implementadas por el Banco Nacional al realizar transacciones en línea?

- Sí
- No

Pregunta 5. ¿Utiliza algún dispositivo inteligente (smartphone, tablet) para realizar sus gestiones bancarias?

- Sí
- No

Pregunta 6. ¿Tiene acceso a internet en su hogar o dispositivo móvil?

- Sí
- No

Pregunta 7. ¿Dispone de un token físico para realizar transacciones bancarias?

- Sí
- No

Pregunta 8. ¿Está usted enterado de que el token físico dejará de funcionar en Agosto de 2024?

- Sí
- No

Pregunta 9. ¿Sabe cómo utilizar el token digital para la autenticación en línea?

- Sí
- No

Pregunta 10. Para la autenticación en línea ¿Qué opción prefiere utilizar el token físico o el token digital?

- Token Físico
- Token Digital

Pregunta 11. ¿Qué cambios o mejoras sugeriría para los programas de educación financiera o las herramientas tecnológicas del banco? (Seleccione todas las que apliquen)

- Incluir más talleres o seminarios prácticos sobre el uso seguro de herramientas tecnológicas.
- Mejorar la accesibilidad y simplificar el uso de las plataformas digitales para personas mayores.
- Ofrecer más recursos educativos en formato audiovisual (videos, tutoriales).
- Proveer asistencia personalizada en línea o por teléfono para resolver dudas.
- Aumentar la frecuencia de las campañas de concientización sobre fraudes y estafas.
- Incluir más temas sobre ciberseguridad en los programas de educación financiera.
- Facilitar guías o manuales impresos para el uso de las herramientas tecnológicas.
- No tengo sugerencias de cambios o mejoras en este momento.

Objetivo Específico 4: Determinar las mejores prácticas internacionales en educación financiera para proponer ajustes específicos que el Banco Nacional de Costa Rica podría adoptar para mejorar la protección de los adultos mayores contra estafas.

Pregunta 1. ¿Qué tan relevante considera que el Banco Nacional se adapte a las mejores prácticas internacionales para proteger a los adultos mayores contra estafas?

- Muy importante
- Importante
- Poco importante
- No es importante

Pregunta 2. ¿Participaría en un taller de simulaciones de estafas, como ejercicios de phishing, para mejorar su capacidad de detectar amenazas cibernéticas?

- Sí
- No

Pregunta 3. ¿Considera que un taller de simulaciones de estafas, aumentaría su confianza en la identificación de fraudes en línea?

- Si
- No

Agradecimiento

Agradezco su participación en la encuesta. Su opinión ayudará a brindar recomendaciones para mejorar la educación financiera de los clientes adultos mayores del Banco Nacional de Costa Rica.