

Tema: recomendaciones para la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022

Estudiante: Kevin Castillo Ortega¹, Universidad Latinoamericana de Ciencia y Tecnología, ULACIT
2021

Resumen

Debido al incremento de casos por fraudes digitales en el sector bancario privado y la afectación que ha presentado esta situación a la sociedad costarricense, en esta investigación se trata de evidenciar el impacto ocasionado por esta situación y cuáles podrían ser las recomendaciones con base en el análisis realizado para que las personas puedan sentirse más preparadas y seguras.

La problemática planteada es: ¿Cuáles son las recomendaciones adecuadas para la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022? En relación con la metodología, la investigación es de tipo descriptiva con un enfoque cuantitativo. El instrumento de investigación utilizado es un cuestionario, complementándose con una técnica de recolección de datos a través de encuestas, la cual se logró aplicar a un total de 60 personas pertenecientes a la población que fue definida.

En lo que respecta a los resultados, evidencian que el mayor porcentaje de las personas ha recibido algún tipo de fraude digital, lo cual demuestra el gran reto que tienen los usuarios de aumentar aún más las medidas de seguridad para no estar expuestos y vulnerables a escenarios fraudulentos. Por otra parte, se puede entender con base en los resultados, que una mayoría de las personas no tiene un alto conocimiento acerca de los fraudes digitales, lo cual ayuda a que la problemática expuesta siga en crecimiento, al abarcar cada vez más áreas de oportunidad que encuentran por ignorancia de los usuarios y falta de interés por el tema.

Derivado de lo anterior descrito, se recomienda a los usuarios estar más atentos a la información disponible por diferentes medios y buscar aún más la información por cuenta propia, ya que es un tema que depende del comportamiento de cada usuario en cómo se informa y cómo se prepara para evitar ser vulnerable antes los fraudes financieros.

¹ Kevin Castillo Ortega. Bachiller en Administración de Negocios de la Universidad Metropolitana Castro Carazo. Optando por la Licenciatura en Administración de Negocios con énfasis en Finanzas de la Universidad Latinoamericana de Ciencia y Tecnología, ULACIT. Correo electrónico: kcastillo553@ulacit.ed.cr

Palabras clave: prevención, seguridad digital, educación financiera, fraudes, actualización

Abstract

Due to the increase in cases of digital fraud in the private banking sector and the impact that this situation has presented to Costa Rican society, this research tries to show the impact caused by this situation and what the recommendations could be based on the analysis carried out. so that people can feel more prepared and secure.

The problem raised is: What are the appropriate recommendations for the prevention of digital fraud in the private banking sector as part of social innovation during the first half of 2022? Regarding the methodology, the research is descriptive, with a quantitative approach. The research instrument used is a questionnaire, complemented with a data collection technique through surveys, which was applied to a total of 60 people belonging to the population that was defined.

Regarding the results, they show that the highest percentage of people have received some type of digital fraud, which shows the great challenge that users have to further increase security measures so as not to be exposed and vulnerable fraudulent scenarios. On the other hand, it can be understood based on the results, most people do not have a high knowledge about digital fraud, which helps the exposed problem continue to grow by covering more and more areas of opportunity that found by ignorance of users and lack of interest in the subject.

Derived from the above, it is recommended that users be more attentive to the information available by different means and seek even more information on their own, since it is an issue that depends on the behavior of each user in how it is reported and how it is prepared to avoid being vulnerable to financial fraud.

Keywords: prevention, digital security, financial education, fraud, update

Introducción

Los fraudes digitales han sido un problema que afecta a la sociedad en general y que han venido en crecimiento en los últimos años, Costa Rica no ha sido la excepción y no escapa de esta realidad, presentando altos volúmenes de fraudes a través de diferentes tipos de dispositivos electrónicos que son

usados diariamente por los usuarios, aunque la intención de estos últimos no sea ingresar a alguna plataforma bancaria ni realizar ninguna transacción financiera.

Lo que se pretende con el desarrollo de la presente investigación es proporcionar datos que aporten valor para entender y cuantificar la gravedad del problema, que permitan identificar cuáles son las mejores soluciones para mitigar el impacto que este problema genera principalmente al mercado del sector privado bancario. Otro de los alcances de la investigación es identificar la población más vulnerable a este tipo de fraudes con la finalidad de generar alternativas que ayuden a este grupo específico y evitar que sean un blanco fácil de estafas por medios digitales.

Una vez que se hayan entendido las diferentes variantes de la problemática, se pretende generar información de utilidad para las personas que hacen uso de plataformas bancarias del sector privado a través de medios digitales, aportando posibles alternativas que mitiguen el crecimiento de las cifras que van en crecimiento en cuanto al número de personas víctimas de algún tipo de fraude digital. Con base en lo anterior, este proyecto se justifica debido a que está relacionado con una problemática actual a la que está expuesta la sociedad, es un tema fresco que puede generar mucha información, la cual se podría investigar para darle mayor profundidad al tema y que se pretende generar diferentes alternativas para beneficio de la población y disminuir la vulnerabilidad actual que se presenta.

Como beneficiarios del tema a ser desarrollado por la presente investigación, se puede mencionar que va dirigido específicamente los usuarios de plataformas bancarias del sector privado, ya que es justo en este donde se presenta el grueso de los casos del problema de fraudes digitales, consecuentemente al ser el sector bancario privado, el que tiene mayor cantidad de usuarios adscritos a plataformas digitales.

Como beneficio del resultado de la presente investigación se puede citar que la población más vulnerable puede estar mejor informada y preparada para mitigar los fraudes digitales y tratar de disminuir las estadísticas negativas que se observan día con día. Otro de los beneficios que se puede mencionar, es generar una concientización acerca del crecimiento de la problemática, de tal forma que, se pueda crear cambios en las conductas y formas de actuar de la población.

Como resultado de la investigación se pretende generar distintos aportes a la sociedad, específicamente a la población que utiliza plataformas digitales de bancos privados, creando una educación financiera que permita que las personas estén más informadas y puedan evadir actitudes permisivas o de ignorancia ante la amenaza existente. Otro de los aportes que se proyecta conseguir con el desarrollo de la presente investigación es la unión de los esfuerzos de la población y autoridades

correspondientes para generar medidas que permitan mitigar y disminuir los casos de exposición a fraudes digitales.

Considerando que la problemática expuesta en el tema de este proyecto es una amenaza que va en constante crecimiento, se establece la siguiente interrogante: ¿Cuáles son las recomendaciones adecuadas para la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022?

En relación con el objetivo general, se establece analizar las recomendaciones que permitan la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022.

Para atender el objetivo general se plantean tres específicos: describir los criterios que desde las finanzas permiten la prevención de fraudes digitales en el sector bancario privado, descubrir las expectativas del sector bancario privado que desde la innovación social permitan la prevención de fraudes digitales, y sugerir las recomendaciones que prevengan los fraudes digitales en el sector bancario privado en el corto plazo. Seguidamente, se amplían los conceptos claves de la investigación en relación con los objetivos planteados, por medio de la siguiente revisión bibliográfica.

Revisión bibliográfica

El incremento de fraudes financieros está asociado a múltiples factores que se conjuntan en tiempo y forma en contra de un individuo o persona, por lo general, la consecución de un fraude se debe a la falta de controles, medidas de seguridad y por supuesto, una cuota importante de ignorancia o desconocimiento de amenazas por parte de la población. Por lo cual, se estará argumentando a continuación cada uno de los factores que han propiciado el aumento de la problemática en el país, específicamente en el sector bancario privado.

Para comenzar, el fraude se define como una acción contraria a la verdad y a la rectitud que perjudica a la persona contra quien se comete (Real Academia Española, 2020). También se brinda un concepto más amplio como el siguiente: actividad delictiva previa relacionada con el cohecho, tráfico de influencias, malversación, fraudes y exacciones ilegales, negociación y actividad prohibida a los funcionarios públicos y por abusos en el ejercicio de su función, corrupción en las transacciones comerciales internacionales y delitos sobre la ordenación del territorio y el urbanismo, engañar (Real Academia Española, 2020).

Si a las definiciones anteriores se le agregara el término o contexto financiero, se podría obtener una definición más cercana con la problemática de este proyecto, que está dirigido a fraudes digitales en el sector bancario privado. Según Interpol (2021), se refiere a los fraudes financieros con la siguiente definición:

La delincuencia financiera abarca desde el robo o el fraude cometido por individuos malintencionados hasta operaciones a gran escala planeadas por grupos de delincuencia organizada presentes en todos los continentes. Se trata de actividades delictivas graves cuya importancia no debería minimizarse pues, más allá del impacto social y económico, por lo general están estrechamente vinculadas con la delincuencia violenta e incluso el terrorismo.

En complemento con lo descrito, se puede entender que cuando se habla de fraudes financieros, siempre hay una afectación económica de por medio para una persona física o jurídica, la cual ha sido objeto de fraude a través del uso de distintos medios digitales, los cuales son utilizados de forma recurrente por los usuarios. Esto como consecuencia del incremento del uso de la tecnología y el avance que se está teniendo día con día, de tal forma que, se ha ido incorporando aún más en todas las actividades cotidianas que se realizan y que representan una mayor exposición a los fraudes digitales.

Debido al constante crecimiento de la tecnología y al aumento de su uso por parte de los usuarios, hay una tendencia en la sociedad a estar cada vez más expuesto al uso de medios o plataformas digitales. Lamentablemente este desarrollo tecnológico tiene un contexto negativo que está asociado a que los ciberdelincuentes también han avanzado de la mano con la tecnología e implementado cada vez más técnicas novedosas para incrementar el número de sus víctimas.

Ante el escenario adverso descrito anteriormente, surge la necesidad de evaluar diferentes alternativas como medida de mitigación de fraudes digitales, razón por la cual se estarán analizando cada una de ellas. De acuerdo con la Cámara de Bancos y Entidades Financieras de Costa Rica, una de las recomendaciones más básicas es ser cuidadosos de la información personal que se comparte en la red y adoptar una postura defensiva ante cualquier tipo de petición de información, según publicación del diario La República (2021).

Según lo anterior descrito, pareciera ser una recomendación muy básica; sin embargo, no todas las personas son extremadamente cuidadosas con el manejo de su información personal, se podría decir que un mal general de la población es la falta de conocimiento de amenazas en las distintas plataformas digitales, dando lugar a una postura permisiva y de confianza ante cualquier solicitud de información.

Adicionalmente se podría mencionar que un porcentaje muy alto de la población desconoce acerca de la información necesaria relacionada con fraudes digitales y no tienen conocimiento de las medidas preventivas que se debe aplicar para evitar caer en un fraude electrónico.

Para mitigar lo anterior, se podría optar por un cambio de hábitos a nivel general, un cambio de conciencia acerca del manejo de la información personal, para esto el banco BBVA (2021) menciona tener la costumbre de realizar revisiones periódicas de las cuentas bancarias, específicamente los últimos movimientos de la cuenta bancaria, así como de las tarjetas de crédito. Además, es importante realizar un cambio periódico de contraseñas e incrementar las medidas de seguridad que los entes bancarios ponen a disposición de los usuarios.

Se puede rescatar de la citación previa, cómo los entes financieros, específicamente los bancos privados, brindan consejos de valor a sus clientes a través de sus páginas electrónicas y a su vez, proporcionan en sus plataformas digitales, los medios necesarios para supervisar la información personal y que esté en la responsabilidad de cada usuario, la revisión periódica y detección de cualquier anomalía para su oportuna denuncia.

Como parte de las expectativas del sector bancario privado está que los usuarios estén atentos a la información que estas entidades financieras proporcionan como parte de la mitigación de riesgos de ser vulnerables a cualquier tipo de fraude digital, ante esto el Banco Nacional de Costa Rica (2021) sugiere no tener ningún tipo de comunicación con correos electrónicos desconocidos, así como no sostener llamadas telefónicas con ningún tipo de persona, así sean que se hagan pasar por funcionarios bancarios, la recomendación es clara en no brindar ningún tipo de información por ningún medio de comunicación.

Otra atenuante para considerar ha sido el factor pandemia y es que los delincuentes han adoptado nuevas medidas para atacar, sacando provecho de esta situación mundial de salud, realizando estafas por medios electrónicos, ofreciendo todo tipo de información para engañar a la población, es por esto que se ha recibido apoyo de campañas interinstitucionales para informar a la población y alertar acerca de los nuevos métodos de los timadores para vulnerar a los usuarios, según menciona artículo del Ministerio Público de Costa Rica (2020).

La banca privada también contempla dentro de sus expectativas que los usuarios sepan qué hacer en caso de ser víctima de algún tipo de fraude digital, tal y como lo describe Bac Credomatic (2021), estas entidades brindan soporte a sus clientes para orientarlos y tratar de asesorarlos en el proceso, con el fin de mitigar el impacto del fraude lo mayor posible. Como parte de las principales medidas de apoyo está

la comunicación directa por cualquiera de los canales oficiales de las entidades, teniendo interacciones con la persona afectada como parte del seguimiento del caso, para aportar todos los medios de seguridad disponibles para evitar una mayor pérdida.

Uno de los aportes relacionados con la innovación social, es que las entidades financieras están doblgando esfuerzos como parte de ese compromiso de ir adelante de los ciberdelincuentes en temas de tecnología y tratar de mitigar la exposición al fraude a través de las distintas plataformas electrónicas. Según MasterCard (2019), se ha otorgado a disposición de los bancos un nuevo servicio de detección de fraude y sistema de decisión basado en inteligencia artificial. Esta solución permite evaluar el nivel de riesgo de una transacción a beneficio de las entidades financieras para aumentar la precisión de las aprobaciones de pago.

Como parte de las sugerencias para la prevención de fraudes digitales, se encuentra la revisión de los sitios digitales visitados, especialmente de aquellos que resulten desconocidos, según el sitio de BBC (2021), todos los sitios web o también conocidos como “URL” deben de tener en la barra de dirección del navegador un candado cerrado en la parte izquierda, para confirmar que es una página autenticada y por ende, más segura donde no se corra ningún tipo de riesgos de robo de información. En relación con lo mencionado, podemos identificar que los bancos se han visto en la obligación de proveer la mayor cantidad y calidad de recomendaciones ante el constante incremento de casos diarios relacionados con actividades digitales fraudulentas.

Con lo descrito, se puede identificar que el sector bancario privado en conjunto con otras instituciones públicas y financieras están comprometidos con educar a la población, creando una educación financiera y una cultura de más concientización en la población que permita cambiar malos hábitos y costumbres que los usuarios han tenido en el pasado y poniéndolos en contexto de las amenazas actuales en el mundo digital. Es por esta razón que los bancos privados están más comprometidos en invertir en nuevas tecnologías para prevenir los fraudes y hacer sentir a sus clientes no solamente que los están tratando de asesorar con la información que comparten, sino que también están invirtiendo en la seguridad digital de todos los usuarios. Estos esfuerzos por parte de las entidades bancarias se han visto reflejadas como parte de las encuestas globales de fraude bancario mencionadas en la publicación de KPMG (2021).

A continuación, se presenta la metodología de investigación en la que se describe el tipo de investigación, así como su respectivo enfoque, además de la población, muestra utilizada, el instrumento seleccionado como recolección de datos y finalmente, la técnica empleada.

Metodología

La investigación se realiza bajo la modalidad de tipo descriptivo, con la finalidad de analizar la prevención de fraudes digitales en el sector bancario privado y evidenciar que el uso de la información facilitada por estas entidades financieras es de suma importancia para la educación de las personas y que permita la disminución de fraudes.

Con respecto al enfoque de la investigación, se determina que es de tipo cuantitativo consecuentemente al tipo de investigación seleccionado. De acuerdo con Hernández Sampieri (2018), la ruta cualitativa se basa en realizar la investigación, examinando los hechos con el fin de generar una teoría que sea consistente con lo que se está observando que ocurre. La ruta se va descubriendo de acuerdo con el contexto y los eventos que ocurren conforme se desarrolla el estudio. Por lo tanto, se determina que es de más interés conocer y comprender los comportamientos de las personas o usuarios de la banca privada.

En relación con la población, para efectos del presente estudio es finita. Según menciona Hernández Sampieri (2018), la población es el conjunto de todos los casos que concuerdan con una serie de especificaciones. En cuanto a la población finita, se adopta este tipo de población para efectos prácticos, ya que permite ser determinada por la cantidad de individuos que la componen, para el interés de esta investigación, los usuarios de la banca privada son de alrededor de 1 968 139 personas (INEC CR, 2021)

Para la muestra, se entiende como la parte o porción extraída de un conjunto por métodos que permiten considerarla como representativa de él (RAE, 2021). Por otra parte, Hernández Sampieri (2018) menciona que es un subgrupo de la población o universo que interesa, sobre el cual se recolectan los datos pertinentes. Para efectos de la presente investigación, se tendrá el tipo de muestreo no probabilístico de conveniencia. Hernández Sampieri (2018) define esta muestra como un procedimiento de selección orientado por las características y contexto de la investigación, más que por un criterio estadístico de generalización. Para efectos prácticos del presente estudio se determina que la muestra de la investigación será de 60 personas entre los 18 y los 70 años (población ocupada y con edad de trabajar) con cuentas bancarias en el sector privado.

Para concluir, el instrumento de recolección de datos es el cuestionario, el cual se aplicará mediante la técnica de encuesta a través de preguntas que se realizarán a la muestra descrita previamente. Hernández Sampieri (2018) se refiere a los cuestionarios como el instrumento más utilizado para la recolección de datos, consiste en un conjunto de preguntas respecto a uno o más variables a medir, la cual debe ser congruente con el planteamiento del problema y la hipótesis. Para este caso específico, se determina que la recolección de datos será de manera digital, aplicando una encuesta con cuatro secciones, en las que cada sección hace referencia a cada uno de los tres objetivos específicos, más las preguntas de la sección del perfil del encuestado. A continuación, se presentará el apartado de análisis de resultados.

Análisis de resultados

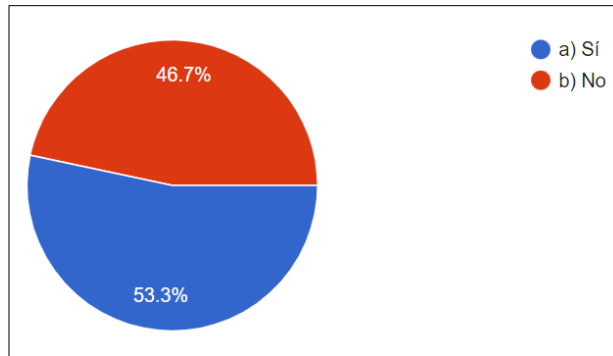
Se estarán evidenciando en la siguiente sección, los resultados obtenidos mediante el uso de encuestas como parte de las técnicas utilizadas para la recolección de datos, de las cuales se obtuvo un total de 60 personas que respondió efectivamente, siendo en su gran mayoría personas entre los 18 y 39 años de edad y que se encuentran laborando actualmente. Los resultados se derivan de preguntas relacionadas con cada uno de los objetivos específicos de este proyecto, los datos recolectados se explicarán con gráficos con la finalidad de generar una mejor interpretación de las respuestas.

En relación con el análisis del primer objetivo específico, el cual indica la descripción de criterios que desde las finanzas permitan la prevención de fraudes digitales en el sector bancario privado, se presentan los siguientes resultados.

Lo primero que se quiso identificar fue el nivel de exposición a fraudes digitales que han tenido los usuarios a través del uso de cualquier medio tecnológico, con el fin de evidenciar el crecimiento de esta problemática en la sociedad. Hay varias atenuantes que han impulsado el crecimiento de los fraudes digitales, una de ellas es la era de la transformación digital que se está dando a nivel global. Entre más uso de nuevas tecnologías, incrementa de igual manera, el riesgo por trampas cibernéticas. Según la Encuesta Global de Fraude de EY, mostró que un 37% de los encuestados consideró que los ciberataques son el mayor riesgo para la sociedad en general, incluso por encima de un 36% relacionado con el fraude y la corrupción (EY, 2019). Es con estos datos que se pone en evidencia la gravedad y complejidad de la situación actual, la cual se estará analizando a continuación.

Gráfico 1

Exposición ante fraudes digitales

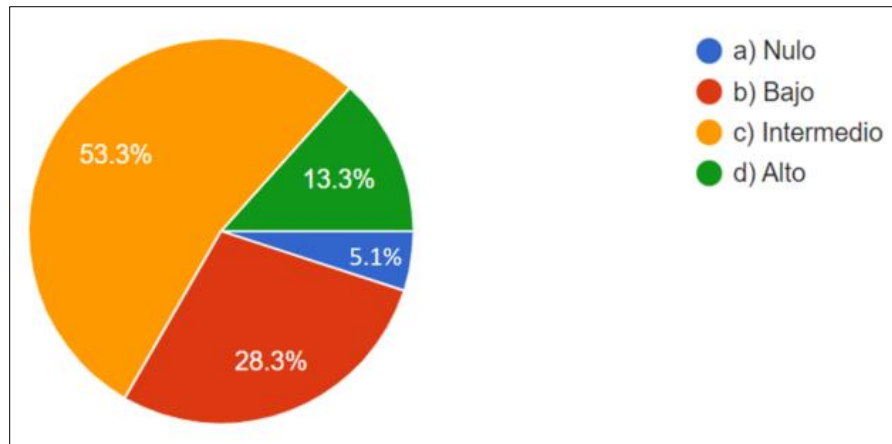


Fuente: elaboración propia, 2021.

Con respecto a los resultados del gráfico 1, se observa que ante la pregunta sobre ¿si han intentado hacerle algún tipo de fraude digital?, se puede evidenciar que la mayoría de encuestados, con un 53.3%, se ha visto perjudicada o al menos le han intentado hacer algún tipo de fraude digital, lo cual confirma que es una situación que está afectando a los usuarios y que hay un gran reto por delante para disminuir estas cifras.

Gráfico 2

Conocimiento acerca de fraudes digitales



Fuente: elaboración propia, 2021.

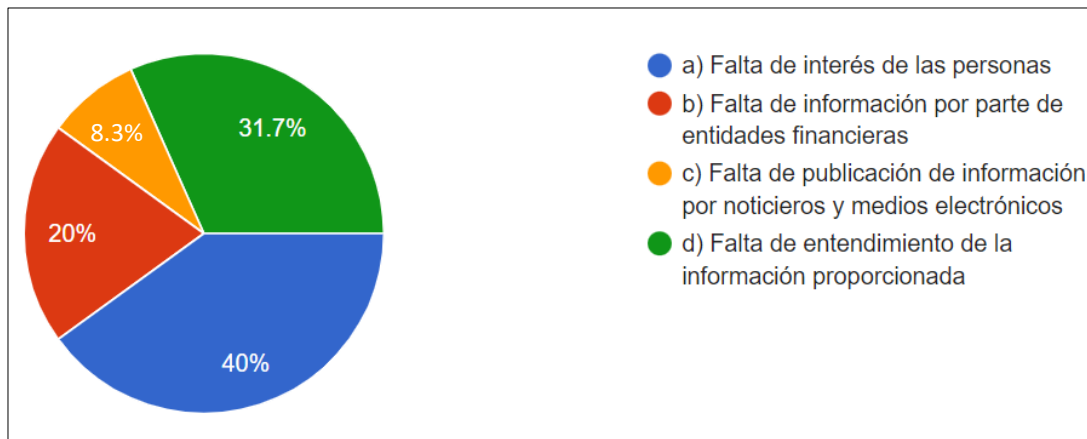
En cuanto a los resultados reflejados en el gráfico 2, se evidencia que la mayoría de los encuestados, con un 53.3% tienen un grado de conocimiento intermedio acerca de información relacionada con los fraudes digitales y lo más preocupante aun es que la segunda opción más elegida con un 28.3% fue que las personas consideran que tienen un grado de conocimiento bajo. Aquí es donde realmente podemos deducir que parte del incremento en los fraudes financieros es porque las personas

no se encuentran informadas y no están lo suficientemente educadas para mitigar la incidencia de situaciones fraudulentas.

Por otra parte, si se viera desde el punto de vista de personas con conocimiento apto acerca de fraudes digitales, solamente un 13.3% de los encuestados tiene un grado alto de información y se encuentra lo suficientemente preparado para no ser víctima de un fraude digital.

Gráfico 3

Principales barreras para prevención de fraudes digitales



Fuente: elaboración propia, 2021.

En relación con el gráfico 3, se observa que un 40% de los usuarios consideró que la principal barrera para prevenir actividades fraudulentas es la existencia de alguna falta de interés por informarse más acerca de los fraudes digitales, lo cual es un factor muy preocupante, ya que ante una situación de aumento de fraudes de manera progresiva conforme pasa el tiempo, no existe un interés por las personas de estar mejor preparadas y de informarse por sus propios medios para aumentar las medidas de seguridad.

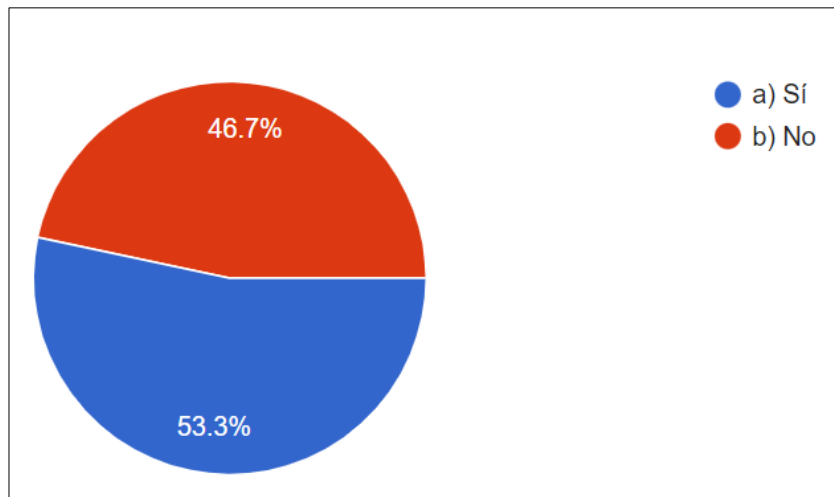
El segundo factor de análisis es que, aun habiendo la existencia de algún tipo de información para prevenir los fraudes, un 31.7% de las personas consideró que también hay una falta de entendimiento de la información que reciben de diferentes fuentes y que, consecuentemente esto ayuda a que se presenten más casos de fraudes. Derivado de estos dos resultados, se identifica principalmente que los mismos usuarios son los responsables de que la situación fraudulenta vaya constantemente en aumento.

Para el análisis del segundo objetivo específico, el cual está asociado con descubrir las expectativas del sector bancario privado que desde la innovación social permitan la prevención de fraudes

digitales. Entendiéndose como innovación social a las nuevas formas de gestión, de administración, de ejecución, nuevos instrumentos o herramientas, nuevas combinaciones de factores orientadas a mejorar las condiciones y de la vida en general de una población o una región (CEPAL, 2021). En relación con la descripción de este objetivo se presentarán los siguientes resultados.

Gráfico 4

Conocimiento de información proporcionada por los bancos privados



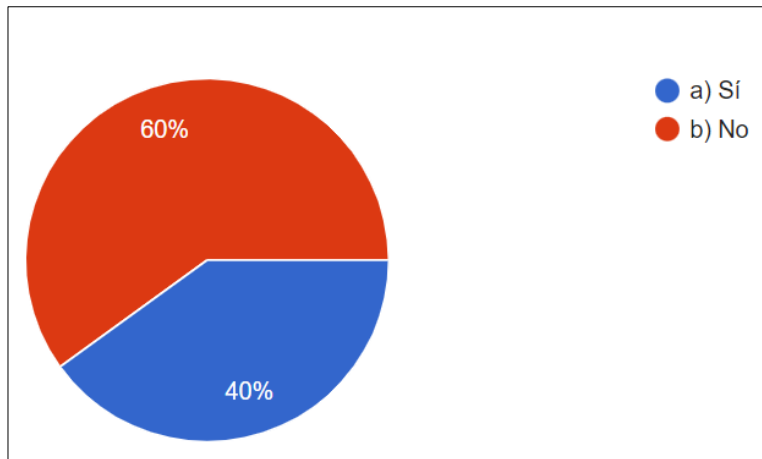
Fuente: elaboración propia, 2021.

Ante la pregunta: ¿Ha leído en algún momento la información que facilitan los bancos privados en cuanto a prevención de fraudes digitales?, el gráfico 4 refleja que la mayoría de los encuestados respondió que sí con un 53.3%, lo cual estaría de acuerdo con la expectativa de que las entidades financieras privadas tienen con respecto al recibimiento de la información por parte de los usuarios; sin embargo, se puede determinar que a pesar de que la mayoría de personas respondió que sí, no es un porcentaje lo suficientemente contundente con respecto al de los que dijeron que no, lo que demuestra que sigue habiendo una cantidad considerable de usuarios (46.7%) que no ha leído en ningún momento la información que generan las entidades bancarias privadas a la población.

Así, se sigue confirmando que hay una gran oportunidad por atacar con respecto al grado de interés que las personas muestran por consumir la información que las entidades bancarias proporcionan a través de diferentes medios, la información es proporcionada; no obstante, no está siendo adquirida por parte de los usuarios, al menos no, con una frecuencia tan alta como lo podrían esperar los bancos privados.

Gráfico 5

Información suficiente proporcionada por los bancos privados

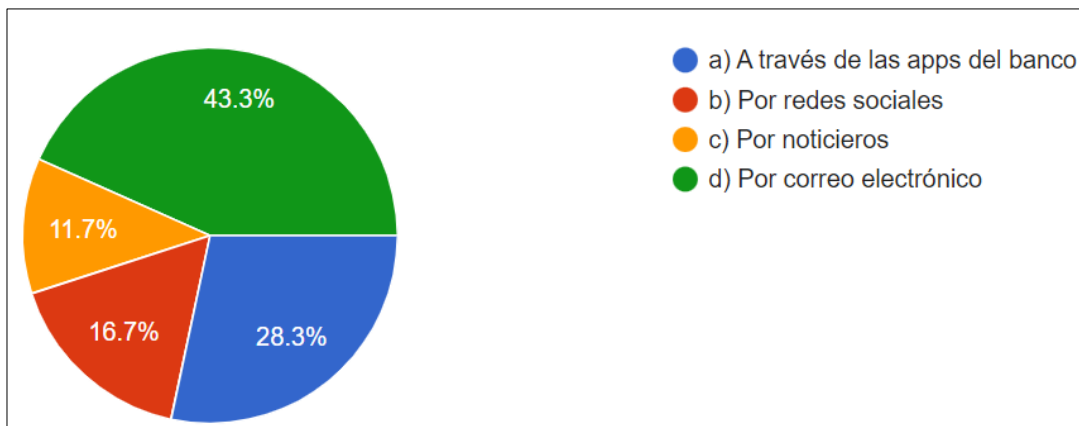


Fuente: elaboración propia, 2021.

Según se muestra en el gráfico 5, un 60% de las personas considera que los bancos privados no proveen la suficiente información para prevenir los fraudes digitales, lo cual se puede interpretar que, la expectativa de los usuarios es que las entidades financieras brinden aún más información de valor, no solamente a nivel de cantidad, sino también de calidad, que sea información lo más actualizada posible que ayude a incrementar la efectividad ante la mitigación de actividades fraudulentas.

Gráfico 6

Medios de preferencia para recibir información



Fuente: elaboración propia, 2021.

En alusión al gráfico 6, se obtiene una contundente evidencia de que los usuarios prefieren recibir la información que los va ayudar a educarse y a prevenir los fraudes digitales a través del correo electrónico, lo cual podría generar la siguiente pregunta: ¿es este el principal medio de comunicación utilizado por los bancos privados para compartir la información con los usuarios?, la respuesta a esta pregunta podría a su vez estar asociada con los resultados reflejados en el gráfico 5, en los que la mayoría de las personas considera que los bancos privados no proporcionan la suficiente información para prevenir los fraudes.

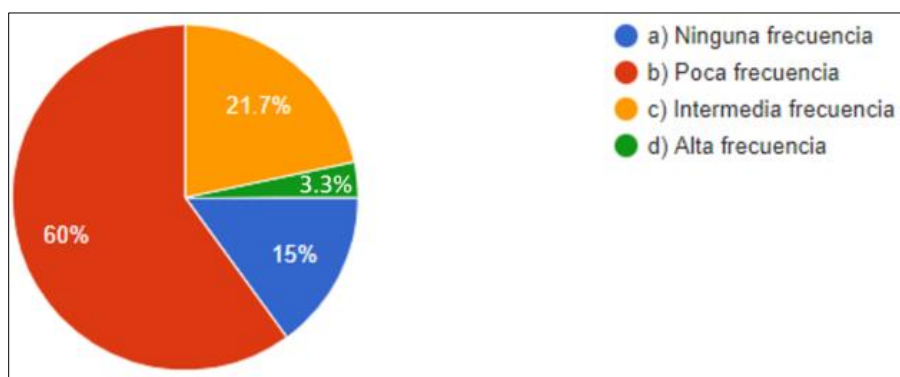
Estos resultados del gráfico 6 podrían presentar un reto más para las entidades financieras que para los usuarios, en el sentido de qué tanto conocen los bancos las preferencias de sus clientes para ser informados y de esta manera, que proporcionen la información respecto de cómo las personas prefieren recibirla y con esto, lograr una efectividad más alta en cuanto a su educación y consecuentemente, disminuir las estadísticas de casos por fraudes digitales.

Finalmente, en relación con el tercer objetivo que hace referencia a sugerir las recomendaciones que prevengan los fraudes digitales en el sector bancario privado en el corto plazo, se presentaron los resultados que se analizan a continuación.

Manteniendo presente el contexto por la pandemia por COVID-19, es una situación que ha beneficiado el incremento de los fraudes, en épocas de crisis y recesiones económicas, el fraude suele ser más extendido, según encuesta mundial sobre delitos y fraudes económicos, un 47% de los encuestados sufrió algún tipo de fraude en los últimos dos años y se espera que aumente significativamente (PWC, 2021). Por esta razón, se hace aún más importante fortalecer las recomendaciones que puedan disminuir estas cifras en el corto plazo.

Gráfico 7

Frecuencia de información preventiva recibida



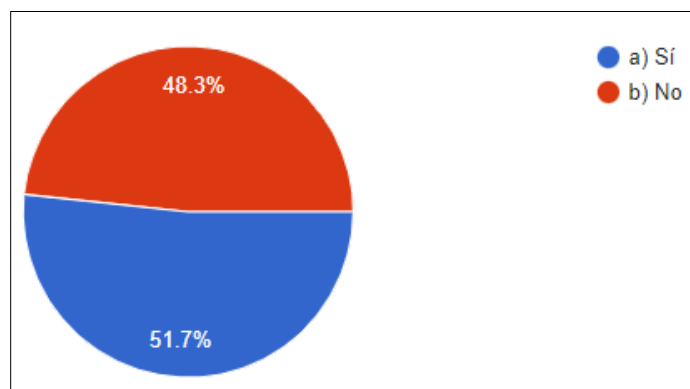
Fuente: elaboración propia, 2021.

El gráfico 7 evidencia que un porcentaje considerable de usuarios con un 60%, considera que reciben con poca frecuencia información preventiva que les ayude a estar más preparados para disminuir la incidencia de estafas, más con la atenuante de la pandemia que se ha prestado aún más para que los ciberdelincuentes hagan de las suyas, engañando a más personas y aprovechándose de sus necesidades ante la presente situación.

Los resultados presentados con este gráfico 7, nos podrían estar confirmando la incógnita que se planteó con los resultados del gráfico 6, la cual corresponde a si los bancos privados estarían considerando como principal fuente de información, los correos electrónicos de sus clientes, ya que de no ser así, los resultados que observamos en el gráfico 7 podrían tener mucha relación y evidenciar que esta entidades bancarias deberían replantear y valorar la forma en que están compartiendo la información con sus usuarios.

Gráfico 8

Capacidad de asesorar a otra persona para prevenir



Fuente: elaboración propia, 2021.

Con respecto a los resultados del gráfico 8, ante la pregunta: ¿Se siente en la capacidad de asesorar a alguna persona cercana como familiar o amistad para brindarle información valiosa que le ayude a prevenir algún fraude financiero?, si bien es cierto, una mayoría de las personas respondió que sí con un (51.7%), no es un porcentaje contundente o con mayor diferencia sobre la respuesta de no, por lo que más bien, un 48.3%, casi la mitad de las personas, no está lo suficientemente preparada y capacitada para asesorar a otra persona cercana y ayudarla a evitar una situación fraudulenta.

Es acá donde todos los resultados previos de los gráficos anteriores se conjuntan en una misma línea, en la que se evidencia que las personas, en general, no tienen el suficiente grado de conocimiento que se espera para disminuir el número adverso de las estadísticas que van en crecimiento por el aumento de fraudes. A esto habría que agregarle un grado importante de encuestados que consideró una clara falta de interés en las personas sobre el tema, ya que como se observó, es responsabilidad de cada usuario

velar por un correcto comportamiento, aplicando medidas de seguridad extremas y siendo muy cauteloso con el manejo de información sensible en la modalidad digital.

Una vez presentado el análisis de los resultados, se compartirá el apartado de conclusiones y recomendaciones que responden a la problemática planteada, así como los objetivos específicos de la presente investigación.

Conclusiones y recomendaciones

Comprender las principales razones que generan el aumento de casos por fraudes digitales en los usuarios de bancos privados, ya que es una situación que ha perjudicado en gran manera a la sociedad.

En cuanto al primer objetivo específico, se concluye que los usuarios de la banca privada siguen viéndose perjudicados ante la problemática de los fraudes digitales, las víctimas continúan en aumento y ha sido principalmente por el desconocimiento de la población ante las medidas de seguridad y cómo actuar al momento de verse expuesto ante una actividad fraudulenta. Se ha determinado como principal causa, la falta de interés por parte de las personas por estar actualizadas en temas de prevención de fraudes.

Con respecto a la recomendación, se tiene que los usuarios de bancos privados estén más preparados, educados e interesados por informarse y así, aumentar las medidas preventivas que puedan aplicar para disminuir las tasas al alza por crímenes digitales por fraude. Esta recomendación va más por que el usuario se haga responsable de su propia seguridad y busque por sus propios medios la información que le ayude aplicar mejores prácticas, en lugar de esperar a recibirla de cualquier otro.

En relación con el segundo objetivo específico, se concluye que hay una gran oportunidad por mejorar la cantidad de información que es consumida por los usuarios, ya que no están adquiriendo en un nivel óptimo, las medidas que les puedan ayudar a estar más seguros. Los bancos privados tienen una gran oportunidad de conocer mejor a sus clientes y sus preferencias con respecto al manejo de la información.

La recomendación relacionada con este objetivo sería para los usuarios de estar más atentos a la información proporcionada por las entidades financieras, tratar de actualizarse y compartir dicha información con familiares y demás seres cercanos. Para los bancos, se recomienda realizar encuestas a sus clientes para obtener datos precisos y actualizados sobre cuáles son los medios preferidos por los usuarios para recibir la información y hacer más efectiva la comunicación entre ambas partes.

Para el tercer objetivo se concluye que, los usuarios no reciben información preventiva con mucha frecuencia por parte de las entidades financieras, lo que puede contribuir a que las personas no están informadas ni preparadas para evitar una situación fraudulenta. En adición, los bancos no podrían estar usando los medios más adecuados para los usuarios, se concluye que las personas no están preparadas para asesorar ni ayudar a otras personas a evitar un fraude digital.

Como recomendación, se puede mencionar la importancia de generar un vínculo más fuerte entre banco privado y cliente para fortalecer las medidas de seguridad y de esta forma, lograr prevenir las actividades fraudulentas en mayor medida.

Finalmente, es a la luz de la investigación que se logra comprender las oportunidades en materia de información preventiva y mejora del flujo de la información entre las entidades financieras y los clientes. Se espera que los cambios puedan ser ejecutados por ambas partes como medida efectiva para mejorar las medidas de seguridad que ayuden a prevenir los fraudes digitales.

Referencias

Bac Credomatic. (2021). <https://www2.baccredomatic.com/>. Obtenido de <https://www2.baccredomatic.com/es-cr/seguridad>

Banco Nacional de Costa Rica. (2021). www.bncr.fi.cr. Obtenido de <https://www.bncr.fi.cr/%C2%BFc%C3%B3mo-evitar-caer-en-fraudes--se-trata-de-aplicar-estas-3-reglas-.html>

BBC. (2021). www.bbc.com. Obtenido de <https://www.bbc.com/mundo/vert-cap-40638275>

BBVA. (2021). www.bbva.mx. Obtenido de <https://www.bbva.mx/educacion-financiera/banca-digital/5-consejos-para-la-prevencion-de-fraudes-digitales.html>

CEPAL. (2021). *Acerca de innovación social*. Obtenido de <https://www.cepal.org/es/temas/innovacion-social/acerca-innovacion-social>

EY. (25 de julio de 2019). *¿Cómo la transformación digital aumenta los riesgos de fraude de los consumidores y retail?* Obtenido de https://www.ey.com/es_bo/assurance/how-digital-transformation-increases-consumer-and-retail-fraud-risks

Hernández Sampieri, R. (2018). *Metodología de la investigación*. Ciudad de México: McGraw-Hill Interamericana Editores, S. A. de C. V.

INEC CR. (19 de octubre de 2021). www.inec.cr. Obtenido de Población Joven y Adulta: <https://www.inec.cr/social/poblacion-joven-y-adulta>

Interpol. (2021). www.interpol.int. Obtenido de <https://www.interpol.int/es/Delitos/Delincuencia-financiera>

KPMG. (2021). <https://home.kpmg/cr>. Obtenido de https://home.kpmg/cr/es/home/tendencias/2019/07/fraude_bancario.html

La República. (19 de octubre de 2021). *www.larepublica.net*. Obtenido de <https://www.larepublica.net/noticia/en-el-mundo-digital-cada-37-minutos-se-comete-un-fraude-electronico-segun-camara-de-bancos-de-costa-rica>

MasterCard. (agosto de 2019). *www.mastercard.com*. Obtenido de <https://www.mastercard.com/news/latin-america/es/sala-de-prensa/comunicados-de-prensa/pr-es/2019/agosto/una-mayor-seguridad-digital-a-traves-de-la-autenticacion/>

Ministerio Público de Costa Rica. (19 de noviembre de 2020). <https://ministeriopublico.poder-judicial.go.cr/>. Obtenido de <https://ministeriopublico.poder-judicial.go.cr/images/2020/NoticiasInstitucionales/19112020.pdf>

PWC. (2021). *COVID-19: El potencial del incremento del fraude y de los delitos económicos*. Obtenido de <https://www.pwc.com/ia/es/gestion-de-crisis/COVID-19-El-potencial-del-incremento-del-fraude.html>

RAE. (2021). *muestra*. Obtenido de <https://dle.rae.es/muestra>: <https://dle.rae.es/muestra>

Real Academia Española. (2020). <https://dpej.rae.es>. Obtenido de <https://dpej.rae.es/lema/fraude>

Anexos

Anexo 1. Encuesta

Encuesta dirigida a: personas entre los 18 y los 70 años (población ocupada y con edad de trabajar) con cuentas bancarias en el sector privado.

Objetivo general del estudio: analizar las recomendaciones que permitan la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022.

Tema de investigación: recomendaciones para la prevención de fraudes digitales en el sector bancario privado como parte de la innovación social durante el primer semestre de 2022.

Presentación de la encuesta: tiene como finalidad obtener el grado de conocimiento de las personas, acerca de los fraudes digitales en el sector bancario privado con el fin de generar recomendaciones y prevenir el crecimiento de este tipo de incidentes.

Objetivo específico 1: describir los criterios que desde las finanzas permiten la prevención de fraudes digitales en el sector bancario privado.

- 1- ¿Han intentado hacerle algún tipo de fraude digital?
 - a) Sí
 - b) No

- 2- ¿Qué grado de conocimiento considera usted que tiene acerca de los fraudes digitales?
 - a) Nulo
 - b) Bajo
 - c) Intermedio
 - d) Alto

- 3- ¿Cuál considera usted que es la principal barrera para que la población sea más consciente del peligro de los fraudes digitales?
 - a) Falta de interés de las personas
 - b) Falta de información por parte de entidades financieras
 - c) Falta de publicación de información por noticieros y medios electrónicos
 - d) Falta de entendimiento de la información proporcionada

- 4- ¿Qué grado de medidas preventivas considera usted que aplica para mitigar los fraudes digitales?
 - a) Nulo
 - b) Bajo
 - c) Intermedio
 - d) Alto

Objetivo específico 2: descubrir las expectativas del sector bancario privado que desde la innovación social permitan la prevención de fraudes digitales.

- 5- ¿Ha leído en algún momento la información que facilitan los bancos privados en cuanto a prevención de fraudes digitales?
- a) Sí
 - b) No
- 6- ¿Considera usted que los bancos privados proveen la suficiente información para prevenir los fraudes digitales?
- a) Sí
 - b) No
- 7- ¿Considera usted que aplica todas las recomendaciones que brindan los bancos privados para evitar fraudes?
- a) Sí
 - b) No
- 8- ¿Por cuál medio preferiría recibir la información más actualizada en cuanto a prevención de fraudes?
- a) A través de las apps del banco
 - b) Por redes sociales
 - c) Por noticieros
 - d) Por correo electrónico
 - e) Otro especifique:

Objetivo específico 3: sugerir las recomendaciones que prevengan los fraudes digitales en el sector bancario privado en el corto plazo.

- 9- ¿Qué tanto se ha visto perjudicado usted o algún cercano (familiar o amistad) por los fraudes digitales?
- a) Nada
 - b) Bajo
 - c) Intermedio
 - d) Alto
- 10- ¿Con que frecuencia cree usted que recibe algún tipo de información que prevenga los fraudes financieros?

- a) Ninguna frecuencia
- b) Poca frecuencia
- c) Intermedia frecuencia
- d) Alta frecuencia

11- Si por infortunio sufriera algún tipo de fraude digital ¿sabe cómo actuar y qué hacer?

- a) Sí
- b) No

12- ¿Se siente en la capacidad de asesorar a alguna persona cercana como familiar o amistad para brindarle información valiosa que le ayude a prevenir algún fraude financiero?

- a) Sí
- b) No

Perfil del encuestado

Edad:

- a) 18-29
- b) 30-39
- c) 40-49
- d) 50 o mayor

Género:

- a) Femenino
- b) Masculino
- c) No binario

Provincia de residencia:

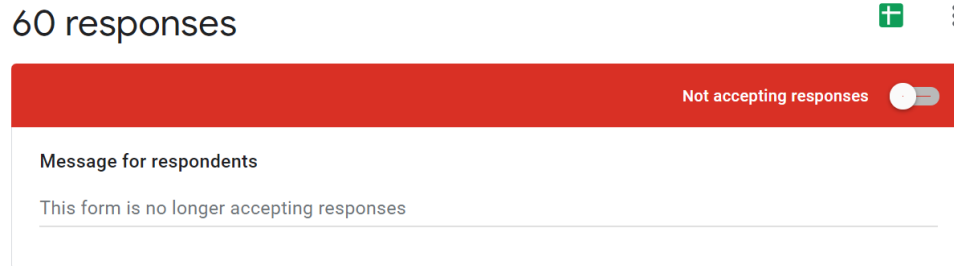
- a) San José
- b) Alajuela
- c) Cartago
- d) Heredia
- e) Limón
- f) Puntarenas
- g) Guanacaste

¡Gracias por su información!

Anexo 2. Resultados de la encuesta

Figura 2.1

Cantidad de encuestas recibidas

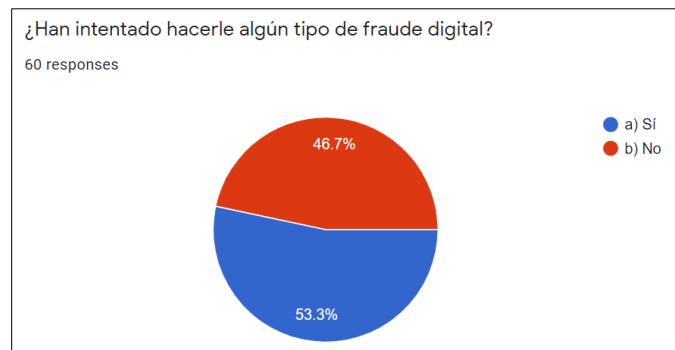


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la investigación.

Fuente: elaboración propia

Figura 2.2

Respuestas recibidas para la pregunta 1

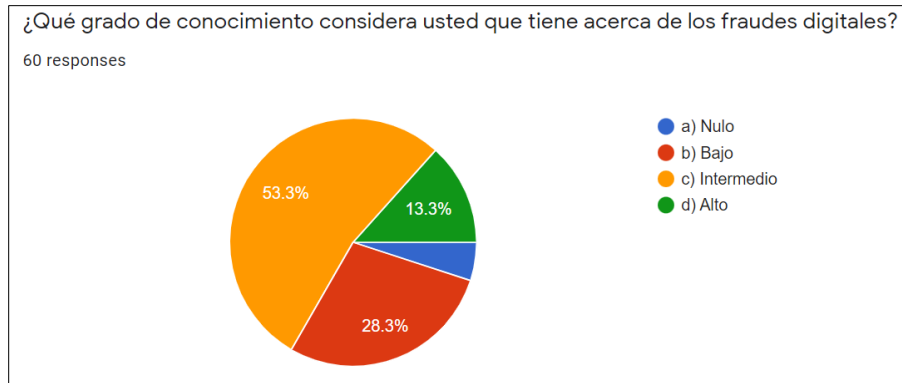


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 1.

Fuente: elaboración propia

Figura 2.3

Respuestas recibidas para la pregunta 2

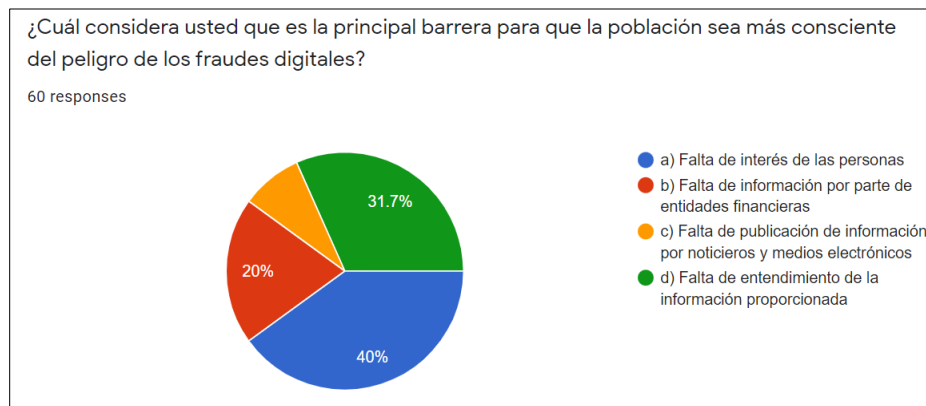


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 2.

Fuente: elaboración propia

Figura 2.4

Respuestas recibidas para la pregunta 3

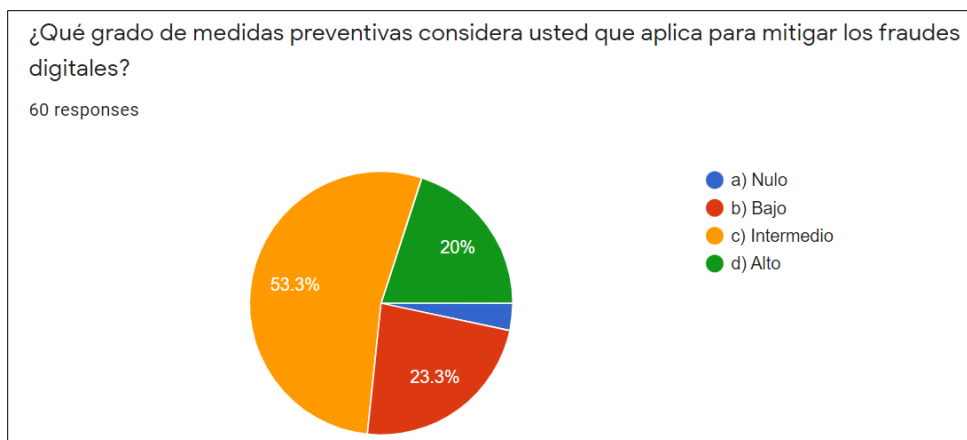


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 3.

Fuente: elaboración propia

Figura 2.5

Respuestas recibidas para la pregunta 4

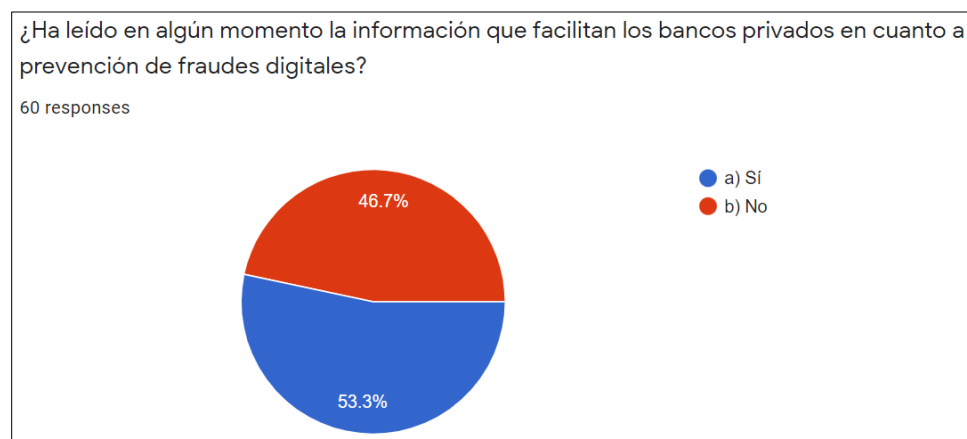


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 4.

Fuente: elaboración propia

Figura 2.6

Respuestas recibidas para la pregunta 5

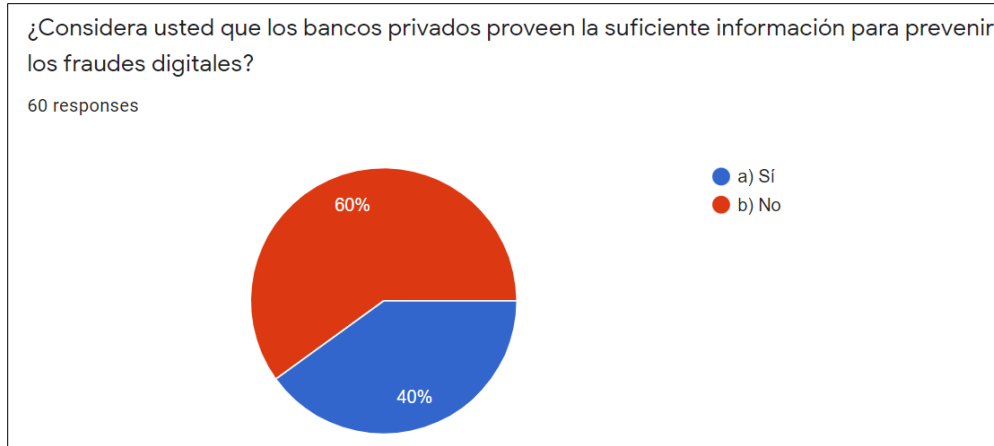


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 5.

Fuente: elaboración propia

Figura 2.7

Respuestas recibidas para la pregunta 6

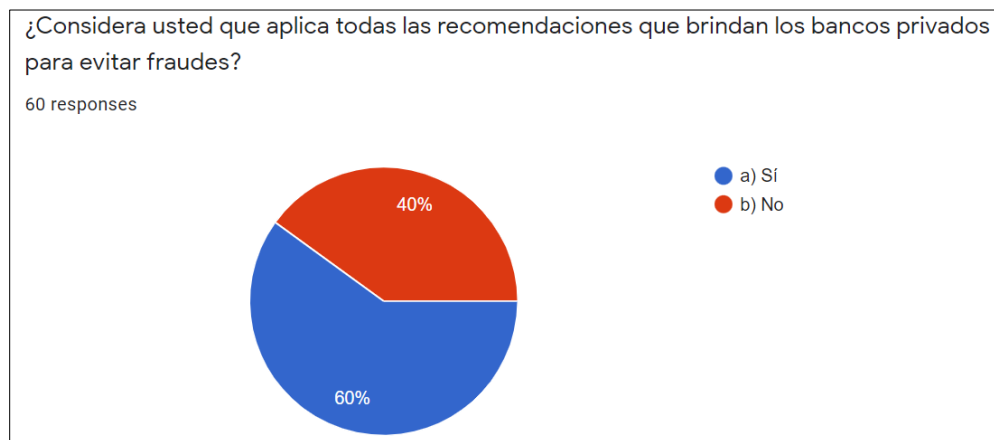


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 6.

Fuente: elaboración propia

Figura 2.8

Respuestas recibidas para la pregunta 7

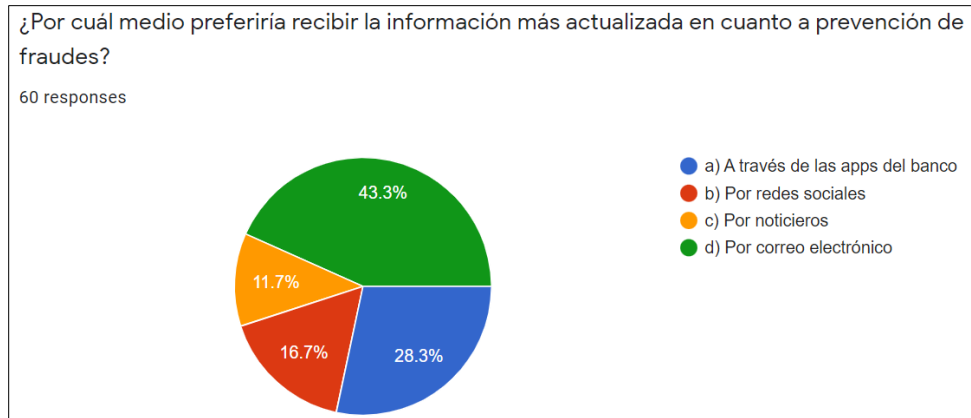


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 7.

Fuente: elaboración propia

Figura 2.9

Respuestas recibidas para la pregunta 8

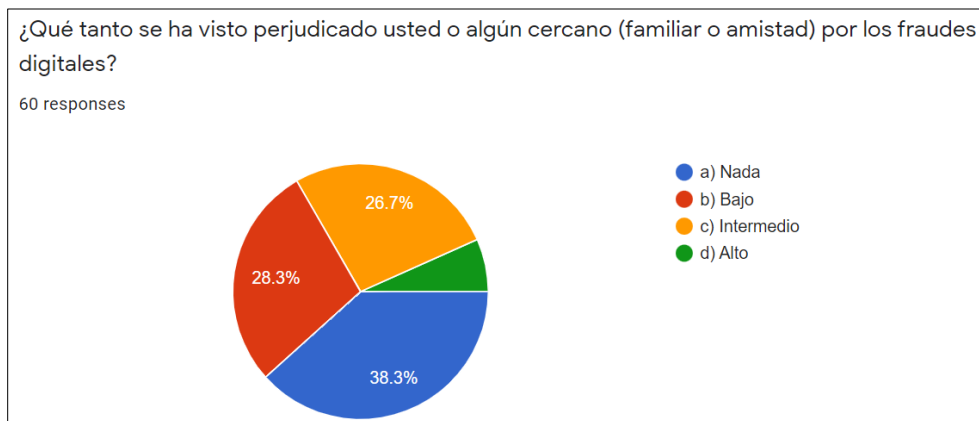


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 8.

Fuente: elaboración propia

Figura 2.10

Respuestas recibidas para la pregunta 9

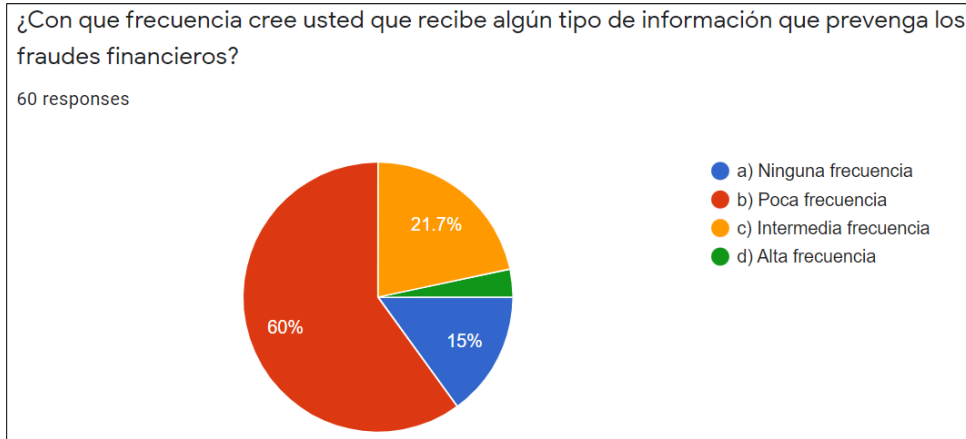


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 9.

Fuente: elaboración propia

Figura 2.11

Respuestas recibidas para la pregunta 10

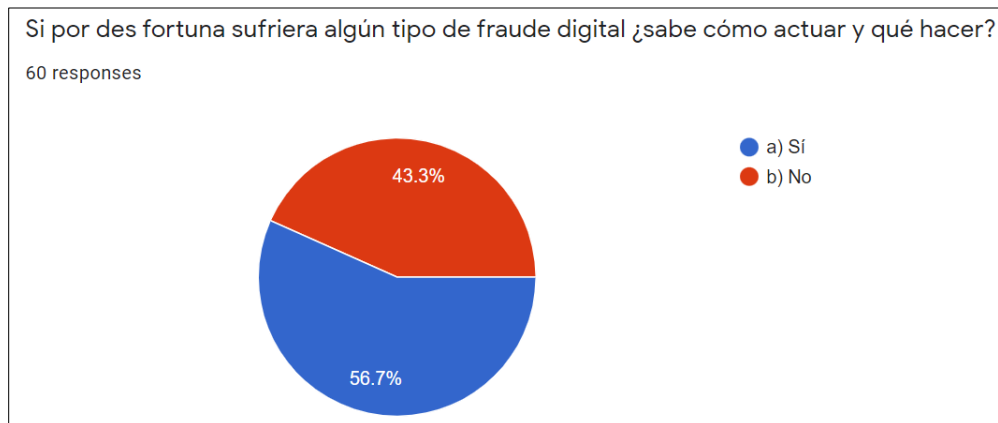


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 10.

Fuente: elaboración propia

Figura 2.12

Respuestas recibidas para la pregunta 11

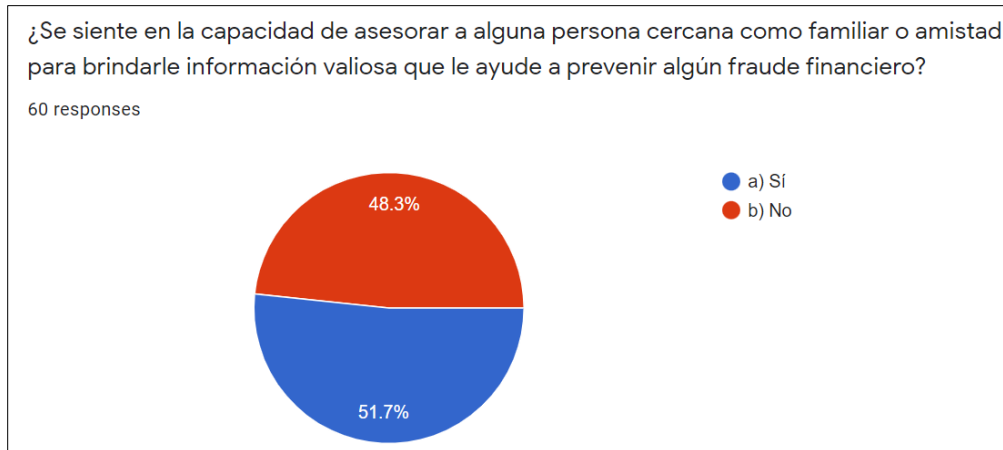


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 11.

Fuente: elaboración propia

Figura 2.13

Respuestas recibidas para la pregunta 12



Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 12.

Fuente: elaboración propia

Figura 2.14

Respuestas recibidas para la pregunta 13

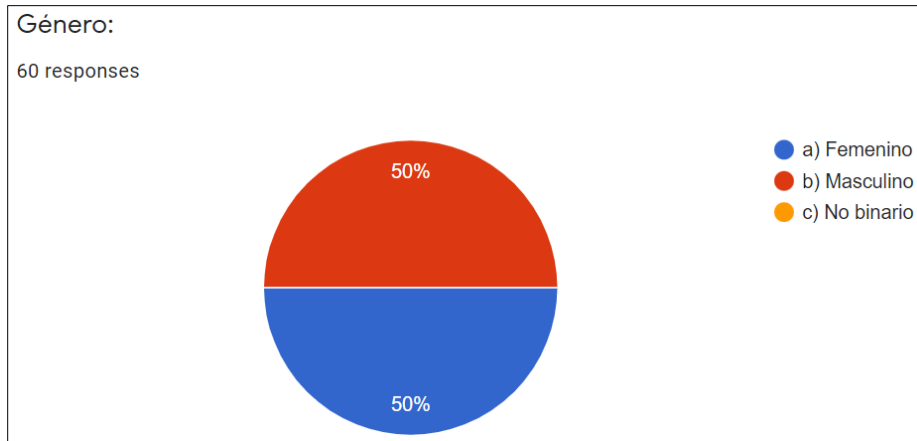


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 13.

Fuente: elaboración propia

Figura 2.15

Respuestas recibidas para la pregunta 14

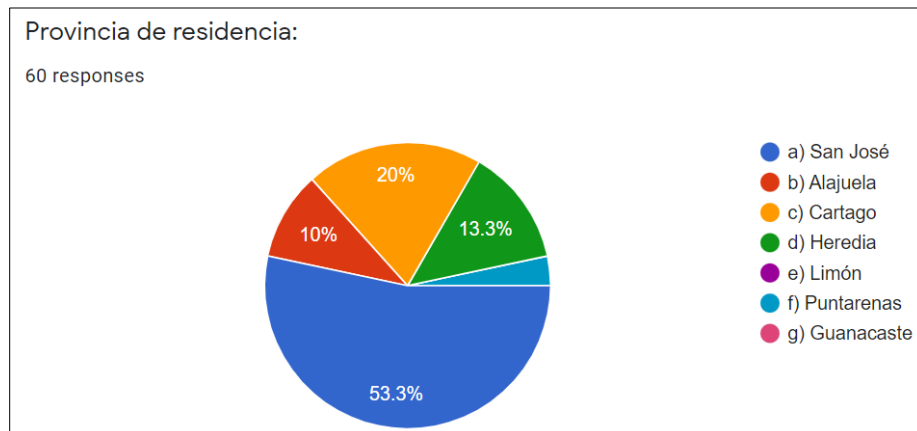


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 14.

Fuente: elaboración propia

Figura 2.16

Respuestas recibidas para la pregunta 15

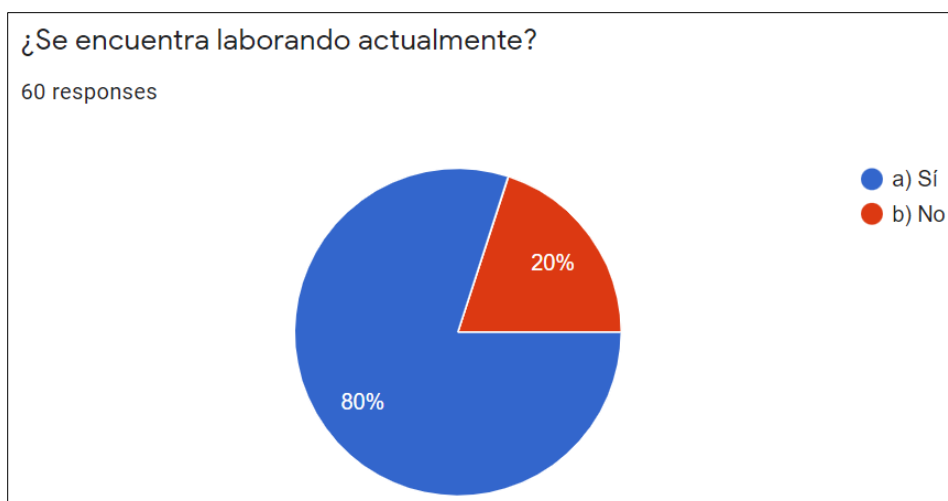


Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 15.

Fuente: elaboración propia

Figura 2.17

Respuestas recibidas para la pregunta 16



Nota: captura de pantalla relacionada con la cantidad de encuestas recibidas para la pregunta 16.

Fuente: elaboración propia

Anexo 3. Carta revisión filológica



M. L. Vilma Isabel Sánchez Castro
Bachiller y Licenciada en Filología Española. U. C. R.



A QUIEN INTERESE

Yo, Vilma Isabel Sánchez Castro, Máster en Literatura Latinoamericana, Bachiller y Licenciada en Filología Española, de la Universidad de Costa Rica; con cédula de identidad 6-054-080; inscrita en el Colegio de Licenciados y Profesores, con el carné N° 003671, hago constar que he revisado el siguiente documento aprobado por el tutor y los lectores. Y he corregido en él los errores encontrados en ortografía, redacción, gramática y sintaxis. El cual se intitula

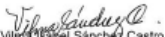
RECOMENDACIONES PARA LA PREVENCIÓN DE FRAUDES DIGITALES EN EL SECTOR BANCARIO PRIVADO COMO PARTE DE LA INNOVACIÓN SOCIAL DURANTE EL PRIMER SEMESTRE DE 2022

DE

KEVIN CASTILLO ORTEGA

**LICENCIATURA EN ADMINISTRACIÓN DE NEGOCIOS CON ÉNFASIS EN
FINANZAS
ULACIT**

Se extiende la presente certificación a solicitud del interesado en la ciudad de San José a los once días del mes de diciembre de dos mil veinte y uno. La filóloga no se hace responsable de los cambios que se le introduzcan al trabajo posterior a su revisión.


M.L. Vilma Isabel Sánchez Castro
Máster en Literatura Latinoamericana. UCR.
Bachiller y Licenciada en Filología Esp. UCR.
Cédula 600540080-Carné 003671

Teléfonos 2227-8513. Cel 8994-76-93 Apartado 563-1011 Y griega
Correo electrónico: vilma_sanchez@hotmail.com-info@chavesysanchezfilologos.com
Página Web: Chaves y Sanchez filólogos
Waze Chaves y Sánchez filólogos