

Ciberseguridad y banca digital en los bancos Bancolombia y Scotiabank Colpatría

Cesar David Pérez

Brandon Arias Rodríguez

Sebastián Flórez Maya

Tecnológico de Antioquia - Institución Universitaria



Resumen

La evolución es un proceso constante, todo aquello cuanto existe es afectado siempre por este cambio inmutable y permanente en el mundo, así mismo, la forma en que el hombre ha cambiado sus necesidades, procesos y hábitos se reflejan en la historia de manera continua y palpable. La globalización y la evolución de la tecnología, hace que la evolución se acelere a pasos acrecentados donde la ciberseguridad toma un rol vital en un mundo digital donde nos encontramos, en nuestra área de enfoque, las finanzas en Bancolombia y Scotiabank-Colpatria buscamos entender la percepción de clientes y usuarios en un marco definido, la ciudad de Medellín, identificando cómo funciona y caracterizando los conocimientos de los servicios bancarios a través del conocimiento recopilado, logramos identificar estrategias y alternativas que dejan ver como en esta era digital se facilita y se acoge un nuevo método para hacer más ágil y seguras las operaciones financieras adaptándonos a un modelo alejado de la banca clásica, que muestra seguridad y se impone en una sociedad más moderna y más demandante; tener la facilidad de poder entender y estudiar a profundidad la ciberseguridad en la banca digital nos acerca un paso más a una economía moderna y globalizada, que se ajusta más a un mercado volátil y cambiante.

Palabras clave: ciberseguridad, percepción, informática, seguridad, servicios, banca, fraude.

Introducción

Entender la vida cotidiana actual sin ningún indicio de la tecnología propia de las dos últimas décadas, se plantea como un ejercicio mental difícil de concebir y más para las más recientes generaciones en donde estas tecnologías han estado presentes todas sus vidas y se han naturalizado. Por lo tanto, la tecnología y el avance del mundo actualmente van ligadas. Esto incide de forma directa en nuestra cotidianidad y en las diferentes formas de hacer y solucionar las incontables operaciones que son demandadas por el consumidor contemporáneo.

Cada una de las esferas y actividades humanas se han visto, en mayor o menor medida, incididos por la tecnología. La educación, la producción, el consumo, la publicidad, el turismo, el transporte, la banca, entre muchas otras esferas. De forma particular con el sistema financiera, se observa aún una relación, a veces antagónica, entre la banca tradicional y la moderna; una amalgama muy marcada, lo tradicional y lo contemporáneo es ahora algo que se enmarca en la diferencia de edades, las generaciones se habituaron al uso y consumo de diferentes servicios que ahora entran a generar controversia, ya sea por el correcto uso o el miedo a ser víctima de un abuso.

En ese orden de ideas, la presente investigación tiene por objetivo general: Analizar como la ciberseguridad bancaria, en Medellín genera diferentes percepciones en los clientes y usuarios de las organizaciones Bancolombia y Scotiabank-Colpatria. Con el fin de dar cumplimiento a este objetivo, se plantean una serie de específicos: i) Identificar el funcionamiento de la seguridad informática aplicada a la banca colombiana en la última década. ii) caracterizar el uso de servicios bancarios y conocimiento sobre la ciber seguridad en la ciudad de Medellín. iii) identificar algunas de las estrategias y alternativas para evitar fraudes bancarios cibernéticos.

Se estructura en cinco partes. La primera de ellas se delinea y caracterizan aspectos que dan cuenta de la existencia del problema de investigación en torno a la percepción de la ciber seguridad. Posterior a esto, se revisa los fundamentos teóricos y conceptuales necesarios para la investigación. En la tercera parte se especifica la metodología e instrumentos empleados. La cuarta sección presenta el análisis y discusión de los datos. Finalmente se presentan una serie de conclusiones y reflexiones sobre lo investigado.

Materiales y métodos

El presente artículo cuenta con un nivel de profundización a nivel descriptivo, toda vez que procura identificar la aceptación referente la ciber seguridad bancaria, por parte de los usuarios. En ese orden de ideas cuanta, con una naturaleza de tipo cuantitativa, que como instrumento principal de recolección de datos se hace uso de encuestas a la población de interés. Sin embargo, también se hace uso de información secundaria, especialmente documental con el fin de sustentar y comprender los resultados.

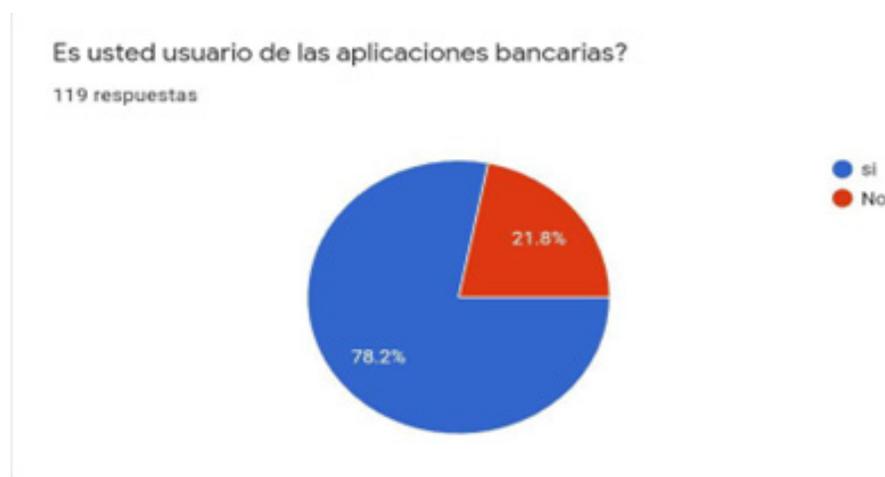
Análisis y discusión de resultados

El presente apartado tiene por finalidad presentar, de forma sintética los resultados y análisis de la información, los cuales se encuentran orientados hacia el cumplimiento del objetivo general propuesto.

Caracterización de uso de servicios bancarios y conocimiento sobre la ciber seguridad

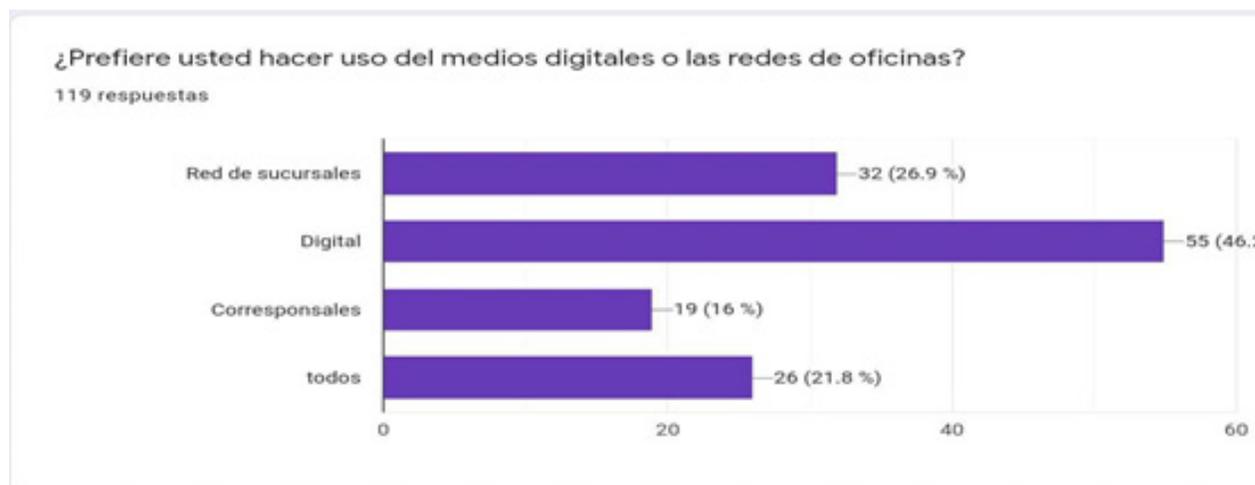
Los resultados obtenidos a través de esta encuesta de caracterización ofrecen un panorama que da la facilidad de analizar y entender el pensamiento, manejo, preferencias, y sentir de los usuarios y clientes dentro de las entidades, con el objetivo de caracterizar los servicios y entender más sus funcionalidades, para entender las alternativas y estrategias que nos ofrecen mientras hacemos un uso adecuado de los productos y servicios financieros.

Figura 1: Población usuaria de servicios bancarios



Nota: Elaboración propia con base en datos recolectados en la encuesta

Dentro de la primera pregunta en el cual se pretende analizar la cantidad de personas que utilizan los medios virtuales, se puede inferir que una gran parte utiliza medios digitales para realizar operaciones o consultas lo cual es equivalente al 78.2 % de la población, mientras que el 21.8 % dice no utilizar medios digitales para realizar transacciones o consultas.

Figura 2: Preferencias en uso de servicios bancarios

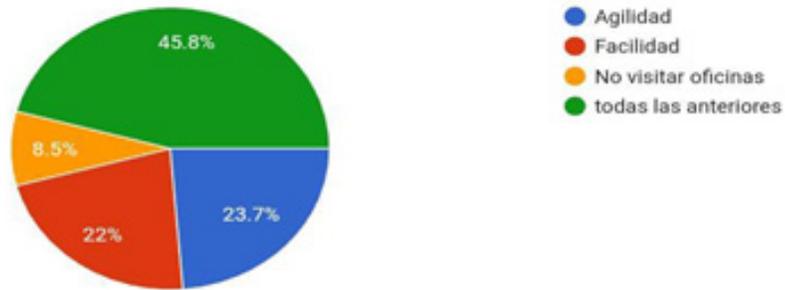
Nota: Elaboración propia con base en datos recolectados en la encuesta

En la siguiente pregunta se realizó un cotejo de los canales que prefieren las personas encuestadas entre el canal digital o los canales físicos en las que las personas han contestado en un gran porcentaje el cual equivale al 46.2 % un poco más de la mitad de las personas prefieren este medio digital ya que se entiende que tienen más tiempo que pueden invertir en otras cosas el cual no lo tendrían visitando un canal físico y un 26.9 % de las personas contestaron estar a gusto en visitar la red de sucursales el cual les gusta tener más contacto con los asesores y comprobantes físicos, mientras que el resto de los encuestados 21,8 % esta prefiere utilizar todos los medios.

Figura 3: Preferencias medios digitales bancarios

¿Qué es lo que más le gusta de usar los medios digitales?

118 respuestas



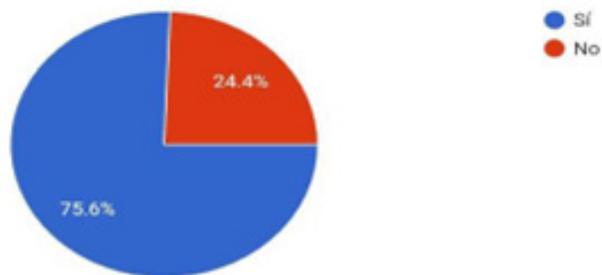
Nota: Elaboración propia con base en datos recolectados en la encuesta

Les pregunta a las personas sobre qué es lo que más le gusta de los medios y canales digitales para realizar transacciones y consultas y la mayoría de las personas 45.8 % contestaron entre agilidad facilidad y no visitar oficinas el estar de acuerdo con todas las anteriores mencionadas y los que da pie a entender en la anterior pregunta por qué las personas prefieren los canales digitales con el fin de ganar tiempo.

Figura 4: Confiabilidad de medios digitales

¿Considera usted que el canal digital es confiable?

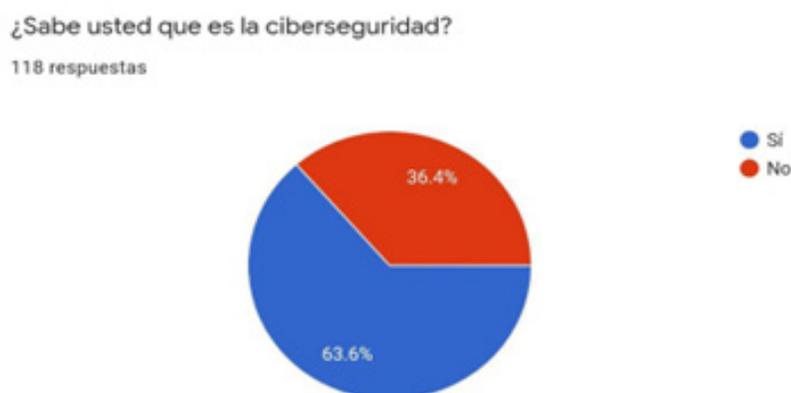
119 respuestas



Nota: Elaboración propia con base en datos recolectados en la encuesta

Las personas encuestadas dicen que los canales digitales del sector financiero son confiables en el cual un 75.6 % está conforme con la seguridad de los canales digitales ya que les proporciona confianza y fácil de utilizar, mientras el 24.4 % manifiesta que los canales digitales del sector financiero no son confiables.

Figura 5: Conocimientos sobre la ciberseguridad



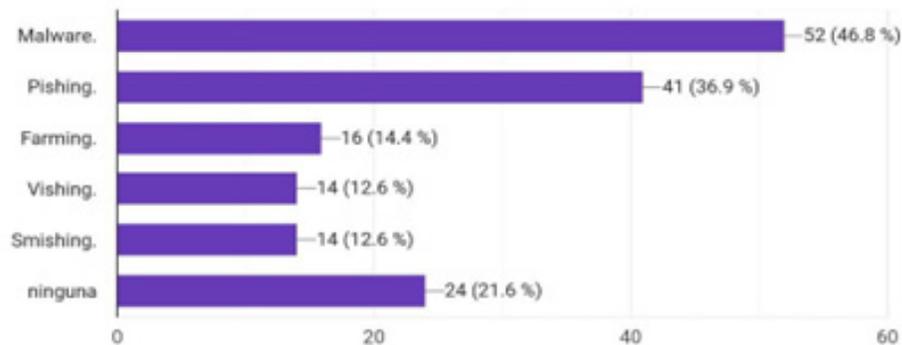
Nota: Elaboración propia con base en datos recolectados en la encuesta

Según en los datos recolectados se puede determinar que el 63.6 % de las personas encuestadas determinan conocer algo acerca de que es ciberseguridad y el autocuidado de sus productos financieros, por otra parte el 36.4 % del resultado de la muestra dice no conocer sobre que es ciberseguridad lo que puede inferir en que no tenga productos financieros por un lugar, por otra parte se puede decir que es un porcentaje de la muestra que no está interesados en realizar transacciones o consultas a nivel digital, por el hecho que han tenido malas experiencias no se los han recomendado o porque simplemente no saben utilizar los canales digitales en el sector financiero y por lo tanto evitan utilizar estos medio digitales y seguir visitando los medios físicos como es la red de sucursales.

Figura 6: Conocimientos sobre métodos de fraude bancario

¿Cuál de las diferentes maneras usadas para hacer fraude conoce usted?

111 respuestas



Nota: Elaboración propia con base en datos recolectados en la encuesta

El resultado de las encuestas sobre el conocimiento de las diferentes maneras de hacer fraude digital y de cuáles son los más conocidos en el entorno digital y el cual en la toma de la muestra en una de la manera de hacer fraude es el malware con un 46.8 % como ese ataque por aplicaciones o programas maliciosos en los dispositivos el cual viola la seguridad informática, phishing con un resultado 36,9 % como la técnica de ciber ataque en el que los delincuentes ganan la confianza de las personas con el fin que estos mismos revelen sus contraseñas y datos personales y así cometer el delito y este mismo es muy conocido por las personas encuestadas, mientras que un 14,4 % de la muestra manifiesta el farming en el cual muy similar al phishing trata a través de páginas vulnerar las aplicaciones de las entidades financieras con el fin de lograr atacar clientes, por otro lado con un mismo porcentaje el 12.6 % de las personas encuestadas afirman en el vishing y smishing.

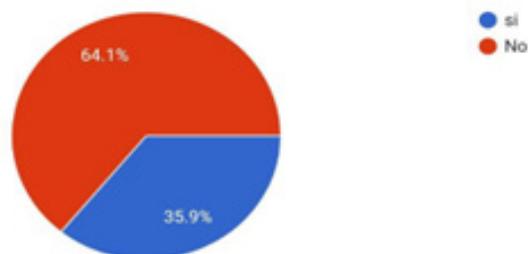
La frecuencia con la que se presentan los fraudes electrónicos dentro de las operaciones habituales de los clientes no es algo común, los casos son esporádicos y existen medidas que ayudan a mitigar y prevenir situaciones que generen impactos negativos en cliente y dentro de las entidades, por ello las compañías financieras acoplan a sus portafolios productos como los seguros, que ofrecen garantías en cada situación y se moldean a los perfiles y necesidades transaccionales de cada persona, al momento de realizar las ventas se hacen ejemplos y asesoramiento continuo a través de los diferentes formas en que se hacen los fraudes y cómo funcionan los comportamientos

delictivos. Los canales de información de las entidades son la principal alternativa de prevención donde constantemente se repiten las medidas de seguridad y protocolos de uso saludable de sus productos sin necesidad de acogerse a garantías adicionales como los seguros, el buen uso y adecuado manejo de la información personal es la principal alternativa a la que siempre se recurre, al fin y al cabo, la protección de la información personal es responsabilidad de cada individuo.

Figura 7: Víctimas de fraudes cibernéticos bancarios

¿Si usted fuera víctima de un fraude por ciberseguridad, ¿lograria identificar como o porque medios fue vulnerado?

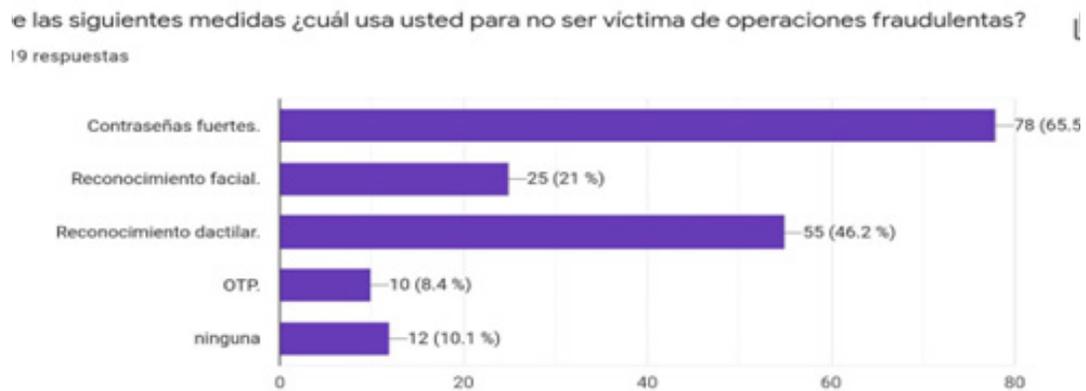
117 respuestas



Nota: Elaboración propia con base en datos recolectados en la encuesta

Un gran porcentaje de las personas encuestadas las personas no identifican porque medio les cometieron violación a sus productos financieros por lo cual puede ser un índice de falta de conocimiento de ciber ataque existentes por lo cual las personas no logran identificar porque medio fue que han sido vulnerados, ya que por la falta de conocimiento de todas las posibles formas y violación en temas de ciber seguridad las personas han perdido credibilidad.

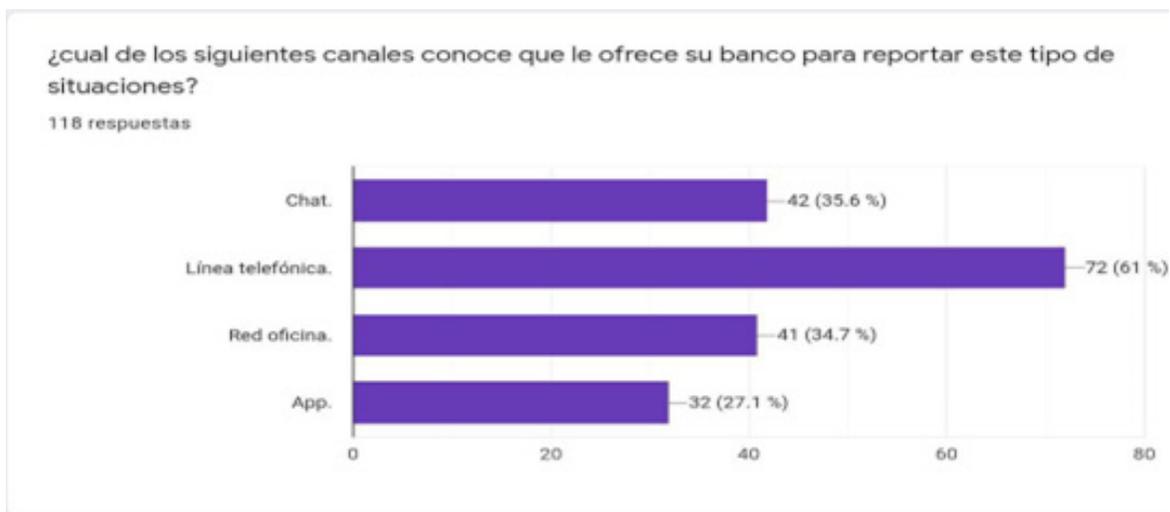
Figura 8: Medios de protección para evitar fraudes



Nota: Elaboración propia con base en datos recolectados en la encuesta

En los demás aspectos las personas mencionan como la forma más acertada dentro de la toma de la muestra como la forma más segura para que no ser víctima de un ciberataque serían las contraseñas fuertes y reconocimiento dactilar para cotejar niveles de seguridad más alto y cuidar sus productos financieros.

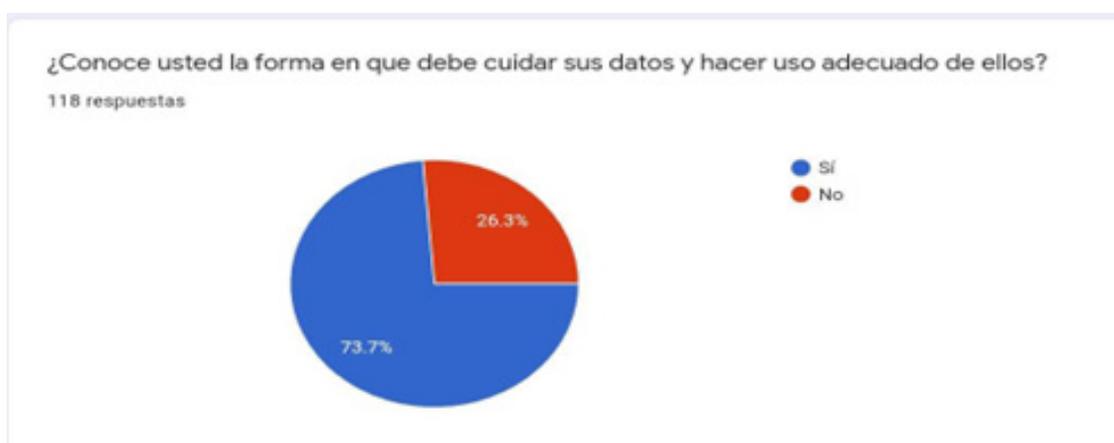
Figura 9: Canales y medios de reporte de fraudes



Nota: Elaboración propia con base en datos recolectados en la encuesta

En esta pregunta como resultado de la muestra se conocen los medios por los cuales las personas encuestadas realizan el reporte de las situaciones como ataques cibernéticos y los cuales la mayoría de las personas el 61 % encuestadas infieren que el lugar donde se realizara el reporte es por la línea telefónica mientras el 35.6 % mencionan que otro lugar por donde se realizaría el reporte de dicho fraude se haría por chat un 34.7 % prefiere ir a la red de sucursales y tener la posibilidad de montar la reclamación con un agente, por otra parte un 27.1 % prefieren reportar por la aplicación.

Figura 10: Prevención personal de fraudes bancarios



Nota: Elaboración propia con base en datos recolectados en la encuesta

Según el análisis de la recolección de los datos en esta pregunta un porcentaje alto que constituye al 73.7 % de los encuestados afirman estar de acuerdo en proteger sus datos personales y hacer uso adecuado de los canales digitales tomando las medidas pertinentes para evitar fraudes de los productos financieros a través de los medios digitales, mientras que el 26.3 % de los encuestados responden no estar de acuerdo en cuidar sus datos personales lo que indica que pueden ser personas que no utilizan los canales digitales.

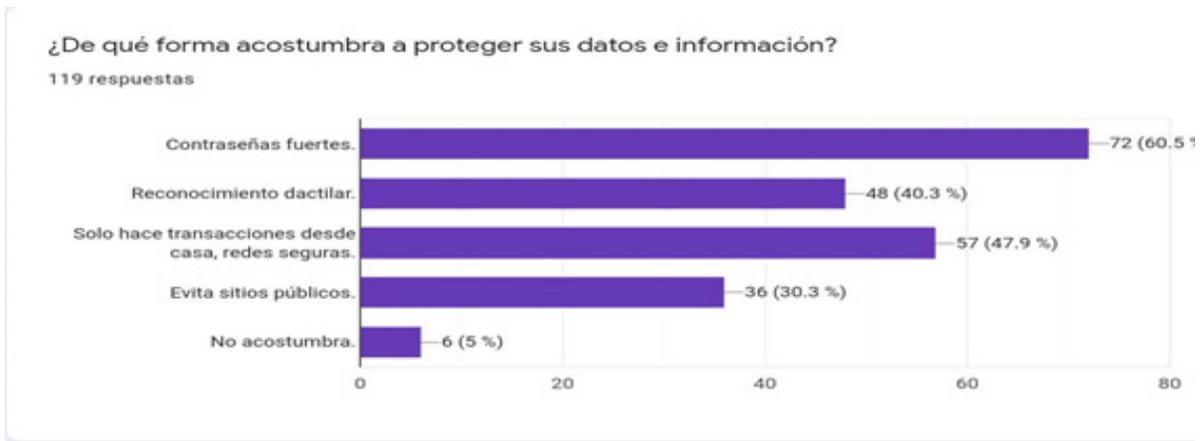
Figura 11: Identificación y detección personal de posibles fraudes



Nota: Elaboración propia con base en datos recolectados en la encuesta

En la pregunta en donde se hace referencia si se logra identificar operaciones fraudulentas frente a sus productos financieros en los resultados fue muy equilibrado frente a las respuestas de los encuestados un 52.1 % afirma en conocer cuando están por hacer fraude a sus productos financieros mientras que 47.7 % de la muestra dice no conoce cuando estén cometiendo un fraude directo que afecte su integridad financiera.

Figura 12: Estrategias de protección de datos



Nota: Elaboración propia con base en datos recolectados en la encuesta

En esta pregunta las personas encuestadas coinciden en el que la mejor manera de proteger sus productos financieros es con contraseñas fuertes y seguras que tengan un nivel de dificultad para los ciberdelincuentes mientras que otros quieren utilizar solo los dispositivos del hogar y evitar sitios públicos, y en un porcentaje mínimo las personas no acostumbran ningún tipo de estrategia para proteger sus productos en el sector financiero.

Se puede determinar en la toma de resultados que las personas a medida que han conocido las aplicaciones en sus entidades financieras y mientras más interactúan con los medios digitales estos se acostumbran más a utilizarlos y por ende pretenden lograr más transacciones con el fin de ganar tiempo y agilidad, por otra parte hay un público reacio a manejar las aplicaciones y los medios digitales ya sea por lo difícil y poco amigable que sean estas aplicaciones o por que han tenido malas experiencias, o simplemente han escuchado noticias donde han ocurrido fraudes digitales por ende prefieren utilizar los canales físicos para realizar sus operaciones financieras, por otra parte la falta de conocimiento y educación financiera en los cuidados de sus datos personales hacen que los canales digitales para este tipo de personas no sea tan apetecido.

Conclusiones

Por esto podemos decir que, si bien los servicios bancarios en línea generan una mayor rapidez, comodidad, y solución es hiperactivo para todas las personas que utilizan los servicios tener un mayor cuidado con la protección de sus datos personales a la hora de realizar cualquier tipo de operación por estos medios.

La percepción que tienen las personas con el uso de las aplicaciones bancarias en los últimos tiempos demuestra que cada vez se tiene una mejor aceptación de las mismas y que así como todos estos procesos evolucionan nos vemos a la tarea de estar cada día mejor informados con este tipo de operaciones dado que es un mundo que avanza aceleradamente, se debe tratar de estar a la vanguardia, como además contemplar la idea que las operaciones bancarias han cambiado y que estos nos lleva a tener una constante relación con los sistemas de información que nos ayudan en los procesos cotidianos como lo son los movimientos y transacciones que realizamos en los bancos.

Durante la investigación se pudo encontrar diferentes amenazas a los cuales los clientes y usuarios de la banca están expuestos en el día a día en la utilización de los medios y canales digitales, es decir que los clientes de uso habitual se definen en agentes individuales o grupos que atacan a las personas implementando diferentes estrategias para cometer los diferentes delitos cibernéticos en los cuales atacan los

sistemas para obtener beneficios financieros y causar daños o interrupciones en el sector financiero. Se ha logrado caracterizar dentro del proyecto de investigación algunos de los métodos más utilizados por los ciberdelincuentes que nos indican que el ciber espacio es aún muy vulnerable a estos ataques y también se puede mencionar que por una parte también hay responsabilidad de los clientes que utilizan la banca al momento de utilizar estas aplicaciones con un compromiso propio de auto vigilancia y capacitación en el uso de estos canales digitales por ende este muchos de las personas que realizan transacciones por medio de los canales digitales han optado por minimizar la utilización de los canales de la banca por miedo a que los ciberdelincuentes afecten sus productos financieros.