FRAUDES ELECTRÓNICOS CON TARJETAS DE CRÉDITO Y SU AFECTACIÓN EN LOS JÓVENES UNIVERSITARIOS.

MARTHA MILENA MAGÓN BRAVO

KEYLLA VANESSA BARROS TARAZONA

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS

RECTORÍA CUNDINAMARCA SEDE SOACHA

FACULTAD DE CIENCIAS EMPRESARIALES

SOACHA

2022

FRAUDES ELECTRÓNICOS CON TARJETAS DE CRÉDITO Y SU AFECTACIÓN EN LOS JÓVENES UNIVERSITARIOS.

Trabajo de grado para obtener título de Administrador Financiero

MARTHA MILENA MAGÓN BRAVO

KEYLLA VANESSA BARROS TARAZONA

Asesor:

Leslie Carolina Villamil Escobar

Asesor

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS

RECTORÍA CUNDINAMARCA SEDE SOACHA

FACULTAD DE CIENCIAS EMPRESARIALES

SOACHA

2022

Nota de aceptación.

_____

_____

_____

_____

_____

Firma Jurado

_____

Firma Jurado

AGRADECIMIENTOS

Primeramente, damos gracias, Dios por cada Bendición recibida durante nuestros años de formación, ha sido Él quien ha guiado nuestros caminos hasta este punto y nos ha permitido poder llegar al punto de nuestras vidas en donde nos encontramos, cada prueba, lección y enseñanza nos han permitido crecer en lo personal y profesionalmente siempre de su mano.

A nuestros padres y hermanas quienes siempre nos han apoyado brindando siempre sus saberes, amor, comprensión y paciencia, sin ellos este proceso no hubiera sido igual de satisfactorio, todo este empeño y el acto para la obtención del título es por ellos y para ellos.

A todos y cada uno de los docentes que estuvieron involucrados en nuestro proceso de formación aportando nuevos conocimientos que nos permitieron llevar a cabo el presente proyecto. En especial a la docente Leslie Carolina Villamil quien nos acompañó no solo en el proceso académico todos estos años sino también en la presente investigación, brindando siempre un apoyo incondicional y la disposición de toda su sabiduría y paciencia.

TABLA DE CONTENIDO

TABLA DE CONTENIDO 5

TABLA DE GRAFICOS. 7

TABLA DE IMÁGENES 8

RESUMEN 9

ABSTRACT 9

PALABRAS CLAVES 10

KEYWORDS 10

INTRODUCCIÓN 11

1 PROBLEMA. 12

1.1 Pregunta problema. 13

2 OBJETIVOS 14

2.1 Objetivo general 14

2.2 Objetivos específicos. 14

3 JUSTIFICACIÓN 14

4 METODOLOGÍA. 16

4.1 Diseño 16

4.2 Instrumento. 17

4.3 Muestra. 18

5 MARCO TEÓRICO. 19

5.1 Qué son las tarjetas de crédito. 19

5.2 Qué es fraude. 23

5.3 Que es el fraude financiero. 23
5.4 Comercio electrónico. 24
5.5 Delito electrónico. 25
5.6 Qué es el fraude financiero electrónico. 25
5.7 Ingeniería social. 26
5.8 Modalidades de fraude electrónico. 27
5.8.1 Phising. 27
5.8.2 Vishing. 29
5.8.3 Malware. 29
5.8.4 Smishing. 30
6 RESULTADOS. 32
6.1 Genero. 32
6.2 Edad. 33
6.3 Programa al que pertenece. 34
6.4 ¿Tiene o ha tenido usted una tarjeta de crédito? 35
6.5 ¿Tiene usted clara la debida forma de usar una tarjeta de crédito? 36
6.6 ¿Ha sido víctima o conoce a alguien que haya sido víctima de fraude con tarjeta de crédito? 37
6.7 ¿Cuál de los siguientes tipos de fraude financiero, considera que fue víctima? 38
6.8 ¿Sabe usted que debe hacer si llega a ser víctima de fraude con su tarjeta de crédito? 39
6.9 Cuando realiza un pago, una compra o una verificación de su tarjeta de crédito los hace por: 40
6.10 ¿Cuál es su mejor aliado al momento de realizar una transacción digital con su tarjeta de crédito? 41
6.11 ¿Tiene usted autoguarda la información de tu tarjeta de crédito en sus dispo1tivos personales? 42
6.12 ¿Tiene usted claro que cuidados debe tenerse presente al momento de ingresar a páginas donde deba cargar información de sus tarjetas de crédito? 43
6.13 ¿Cree usted que las tarjetas de crédito atentan contra su estabilidad financiera? 44
6.14 ¿Considera que el uso de las tarjetas de crédito es muy riesgoso? 45
6.15 ¿Cree que los protocolos de seguridad de las tarjetas de crédito no son confiables? 46

6.16 ¿Siente que su información personal esta lo suficiente expuesta como para que ocurras un fraude con este medio de pago? 47
6.17 ¿Considera que la clonación y/o robo de información de una tarjeta de crédito es bastante fácil? 48
6.18 ¿Cree usted que el uso de las tarjeras de crédito en entes (páginas de bancos o almacenes de cadena) conocidos es seguro? 49
6.19 ¿Considera que los cambios tecnológicos que ocurren día a día podrían cambiar su percepción acerca del uso de una tarjeta de crédito? 50
7 CONSIDERACIONES Y RECOMENDACIONES. 51
7.1 ¿Qué se recomienda hacer si es víctima de fraude? 52
7.2 ¿Cómo influye la educación financiera en los fraudes? 53
7.3 Estrategias para evitar el fraude electrónico al usar tarjetas de crédito. 54
7.4 Tipos de fraude. 56
7.4.1 Smishing. 57
7.4.2 Phishing. 58
7.4.3 Vishing 59
7.4.4 Otras modalidades de fraude. 60
8 BIBLIOGRAFÍA. 65

TABLA DE GRAFICOS.

Gráfico 1 - Tarjetas de Crédito vigentes. 21
Gráfico 2 – Genero. 32
Gráfico 3 – Edad. 33
Gráfico 4 – Programa. 34
Gráfico 5 - Uso tarjeta. 35
Gráfico 6 - Manejo tarjeta. 36
Gráfico 7 - Victima de fraude. 37
Gráfico 8 - Tipos de fraude. 38
Gráfico 9 - Que hacer si es víctima de fraude. 39

Gráfico 10 - Canales de pago. 40
Gráfico 11 - Canales digitales. 41
Gráfico 12 - Información en canales digitales. 42
Gráfico 13 - Cuidados al ingresar información. 43
Gráfico 14 - Atentan con estabilidad financiera. 44
Gráfico 15 - Uso de tarjetas es riesgoso. 45
Gráfico 16 - Protocolos de seguridad. 46
Gráfico 17 - Información expuesta. 47
Gráfico 18 - Clonación de tarjetas. 48
Gráfico 19 - Páginas confiables. 49
Gráfico 20 - Tecnología vs tarjetas. 50

TABLA DE IMÁGENES

Imagen 1 - Formula. 18
Imagen 2 - Muestra 19
Imagen 3 - Fraudes 22
Imagen 4 - Correo Smishing. 28

RESUMEN

El presente proyecto tuvo como propósito conocer las percepciones y afectaciones que tiene el fraude electrónico con tarjetas de crédito en los jóvenes universitarios. Se buscó conocer aquellas afectaciones que se han presentado y así mismo poder bridar estrategias con el fin de que las personas comiencen a implementar una mayor educación financiera la cual permita que este tipo de casos no se presente con tanta frecuencia.

Conocer las características de los diferentes tipos de fraude que se pueden presentar en canales electrónicos al hacer uso de tarjetas de crédito analizando las causas que conllevan a estas situaciones; para esto se utilizó un instrumento de recolección de información aplicado a los estudiantes de la Corporaciones Universitaria Minuto de Dios Sede Soacha en modalidad virtual distancia, por medio del instrumento aplicado se conocieron las diferentes apreciaciones que tiene los estudiantes quienes han sido víctimas de este modelo de fraude así como las causas que llevaron hasta dicho punto. Por último, se analizó información teórica ya aceptada de investigaciones previas realizando confrontación con los resultados obtenidos con el fin de indagar en las fallas que se pueden presentar en estas situaciones y cómo actuar ante las mismas.

ABSTRACT

The purpose of this project was to learn about the perceptions and effects of electronic fraud with credit cards among young university students. We sought to know the effects that have been presented and also to provide strategies in order that people begin to implement more financial education which will allow this type of cases do not occur so often.

To know the characteristics of the different types of fraud that can occur in electronic channels when making use of credit cards, analyzing the causes that lead to these situations; for this purpose, an information collection instrument applied to students of the Corporaciones Universitaria Minuto de Dios Soacha Campus in virtual distance mode was used, by means of the applied instrument the different appreciations of the students who have been victims of this type of fraud as well as the causes that led to this point were known. Finally, theoretical information already accepted from previous research was

analyzed and compared with the results obtained in order to investigate the failures that can occur in these situations and how to act in response to them.

PALABRAS CLAVES

Jóvenes, fraude electrónico, tarjetas de crédito, transacciones, digital, riesgo financiero.

KEYWORDS

Adolescents, electronic fraud, credit cards, transactions, digital, financial risk.

INTRODUCCIÓN

Para el presente trabajo se llevará a cabo una investigación respecto a la percepción que tienen los estudiantes universitarios frente al fraude financiero con tarjetas de crédito para dicha investigación es importante tener en consideración el termino fraude; se le denomina aquellas acciones de engaño que tiene un tercero en contra de un individuo o en algunos casos una entidad por medio de las cuales se obtiene un beneficio económico, perjudicando al tercer individuo.

Ahora bien, un fraude financiero se considera como la estafa contra el patrimonio o propiedad de una persona natural o una compañía que terminan ocasionando pérdidas monetarias. En muchas ocasiones las personas o empresas no saben reconocer que son o fueron víctimas de estos fraudes en tempranas instancias dada la falta de controles o educación financiera de la que pueden carecer.

En la actualidad las tarjetas de crédito van tomando mayor fuerza en su participación del mercado, día tras día son más las personas y empresas que solicitan este producto financiero con el fin de tener un recurso económico disponible para financiar sus compras o avances de efectivo, las tarjetas de crédito permiten que los procesos de compra sean más sencillos al contar con el respaldo de una entidad financiera prestadora de dinero para la transacción y luego en el tiempo pactado se podrá ir reintegrando el capital.

Para llevar a cabo esta investigación se pretende realizar una encuesta que evidencie la percepción de la población, si bien se tendrán en cuenta aspectos como el perfil, las edades y ocupaciones de la muestra también se analizar la información que se recopile con la opinión de otros autores frente a los tipos de fraude y como evitarlos.

Finalmente se evaluarán los resultados y se proporcionarán conclusiones y recomendaciones respecto al análisis y los hallazgos evidenciados en la investigación generando la clasificación de la información pertinente obtenida mediante la aplicación de la encuesta.

1 PROBLEMA.

De acuerdo con el Reporte Global de Fraude 2021 el cual entrega la central de información financiera Experian Datacrédito, Colombia ocupo el tercer puesto en Latinoamérica en fraudes y sexto en ataques cibernéticos, afectando en este caso el sistema financiero colombiano teniendo en cuenta que estos fraudes deben ser asumidos por algún ente ya sea la entidad financiera que emite el plástico, el usuario o en su defecto el Estado quien asume la deuda dentro de su PIB.

Es importante tener en cuenta que estos fraudes se pueden realizar tanto de forma online como de forma presencial y que esta modalidad no diferencia entre edad sexo u/o género, hoy en día existen diferentes modalidades de fraude siendo los más usados:

- Cambio de las tarjetas: esta es una de las modalidades de estafa más usadas, en la cual los delincuentes cambian el plástico crediticio bien sea en un cajero electrónico o durante el proceso de pago de una compra; de acuerdo a Datacredito el modus operandi está basado en el poder del engaño, distracción y farsa.
- Clonación de las tarjetas: en este caso los delincuentes utilizan dispositivos electrónicos capaces de copiar la información del plástico; una vez clonada el delincuente podrá realizar compras e incluso avances a nombre del titular de la tarjeta.
- VISHING: en esta metodología los delincuentes usan medios como llamadas o chats ofreciendo promociones con el fin de obtener los datos de los clientes.
- PHISING: en este método los delincuentes usan link enviados por correos electrónicos o mensajes de texto, los cuales una vez se accede extrae del equipo tecnológico toda la información tanto personal como financiera que puede estar almacenada en el mismo.

Si bien las empresas buscan generar siempre una actualización pro de sus clientes en algunos casos la diversificación que se lleva a cabo por medio de la posibilidad de compras online es aprovechada de forma inadecuada, en algunos casos no se cuenta con la suficiente seguridad tecnológica y termina siendo víctima de hackeo por software maliciosos que obtienen información financiera de los clientes o simplemente como usuarios no se

comprueba la legalidad de las plataformas online donde se ingresan datos meramente personales al momento de comprar, pues no siempre se obtiene lo que se ve o pide inicialmente y en algunos casos las páginas web donde se realizan diversas transacciones no son seguras y almacenan los datos con un fin malicioso.

En cada una de las diferentes modalidades mencionadas anteriormente el titular de la tarjeta de crédito al verse afectado acude a su entidad financiera o prestadora del servicio crediticio con el fin de poder recuperar el dinero y no verse afectado al tener que pagarlo, en muchos casos se acogen a la ley de retracto la cual le permite al cliente que su caso sea analizado con el fin de evaluar una posible devolución del dinero. Es aquí, donde se pretende llevar a cabo la presente investigación, se abordarán aquellas percepciones que pueden tener los jóvenes universitarios respecto al fraude financiero, las tarjetas de crédito, y el comercio electrónico, así mismo se analizara el sistema financiero y las pérdidas generadas a raíz de los fraudes ocasionados con el inexperto uso por así decirlo de las tarjetas de crédito.

Cabe resaltar que esta población es una de las más adaptadas a la innovación tecnológica y digital, ya que hoy en día parece que los niños vienen con ese chip incluido. Es por ello que se considera que esta población tiene conceptos y/o deducciones más amplias que una persona con mayor edad, pues ellos vienen en medio de este mundo; de alguna manera lo jóvenes tienden a realizar cualquier tipo de transacción de forma online.

1.1 Pregunta problema.

Según lo descrito y planteado en el problema anterior

¿Cuáles son las percepciones de los estudiantes del campo de ciencias empresariales sobre el fraude en transacciones financiero durante el uso de tarjetas de crédito?

2 OBJETIVOS.

2.1 Objetivo general

Identificar las percepciones de los estudiantes del campo de ciencias empresariales sobre el fraude en transacciones financieras durante el uso de tarjetas de crédito, con la finalidad de recomendar estrategias que mitiguen el riesgo.

2.2 Objetivos específicos.

- Explorar las características y los tipos de fraude financiero con tarjeras de crédito y cuáles son las causas que conllevan a este.
- Describir cuál es el método de fraude financiero más usado según la percepción de los estudiantes de ciencias empresariales.
- Determinar las delimitaciones que aplica la ley en el estatuto del consumidor para las transacciones que sean consideradas fraude.
- Explicar las estrategias que permitan reducir la tasa de fraude financiero con tarjetas de crédito.

3 JUSTIFICACIÓN.

De acuerdo con la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria) con corte al 28 de febrero 2022 en Colombia había 15.761.857 tarjetas de créditos vigentes en el mercado. Lo cual representa una alta cifra en cuanto a tarjetahabientes en el mercado nacional. Es importante recalcar que durante y luego de los periodos de cuarentena impuestos por el gobierno el uso de las tarjetas de crédito se incrementó al cierre del año 2021 según el DANE el uso de tarjetas de crédito registro una cifra de 46,8% según los analistas una de las fuentes para un mayor uso de este método de pago fueron las campañas del Dia sin IVA incentivo al comercio y su reactivación creado en el año 2020. (Sn, Revista Semana, 2022)

Por otra parte, (Alvarez & Mejia, 2021) mencionan que la pandemia y las decisiones tomadas para equilibrar de alguna forma la economía aumentaron el comercio electrónico y en la misma medida los ataques electrónicos; si bien estos

ataques representan un aumento del 59% para el año en que la pandemia había quitado algunas de sus restricciones. (Portafolio, 2020)

Es importante comprender lo que depara el futuro ya que las causas que llevaron a avanzar y dar paso al comercio electrónico fueron radicales y es que de alguna manera se forzó el uso de medios digitales, el aislamiento y no contacto por completo requería de compras y pagos en línea pues era evidente que la sola comida en un momento determinado se iba agotar, así mismo el pago de servicios, sencillamente estos aspecto básicos requerían esta modalidad electrónica así que se creó la necesidad de adaptarse a los medios que facilitaban este tipo de transacciones.

Un artículo reciente de (La republica, 2022) indica que el 50% de los colombianos compra en línea y el 20% de esa población realiza una compra por internet una vez a la semana, evaluando todos estos aspectos se puede deducir que la población creo el hábito del comercio electrónico; lo cual significa que esto es un gran paso y es donde se debe evaluar lo que en el futuro va a representar el dinero pues no se está lejos de digitalizar también el dinero.

Si bien (El portafolio, 2022) indica que las billeteras digitales tuvieron un aumento del 99% en el número de usuarios registrados, un aumento del 122% en las transacciones realizadas digitalmente y un 195% de dinero digital transado. Es por estas cifras que se comprende que el efectivo está siendo usado cada vez menos, y es ahí donde se cuestionan aspectos como los fraudes o robos digitales, en un futuro no muy lejano la mayoría de los intercambios de dinero se realizaran de manera digital y la única manera de verificar ese tipo de transacciones digitales es con información personal de cada uno de los usuarios.

Como usuarios en muchas ocasiones no se toman las medidas necesarias para realizar los procesos de compra ya sean de forma presencial u online puesto que se cree en diferentes ofertas publicitarias; ya sea en días como la estrategia mencionada anteriormente o cualquier otra fecha, no se cuenta con una educación financiera que permita tomar decisiones de compra o precauciones a la hora de hacer uso de las tarjetas de crédito ya sea de forma presencial o en línea; a lo largo de esta investigación

se realizara el análisis de datos referentes a los diferentes tipos de fraudes que se pueden presentar en el uso de las tarjetas de crédito. Por medio del estudio y análisis de la información que brindan las diferentes entidades bancarias nacionales, la Superfinanciera y la Superintendencia de industria y comercio. Se lograrán identificar cuáles son los aspectos que se deben mejorar con el fin de que estos delitos financieros no sigan siendo un tema recurrente y los usuarios puedan obtener un mayor aprovechamiento de sus productos financieros.

Se abordará el tema en el presente trabajo, buscando poder mitigar el desconocimiento del uso adecuado de los productos financieros tanto en los canales digitales de transacción como los corrientes, así mismo poder impartir consejos que permitan adquirir cultura financiera y determinar el impacto negativo que genera a los patrimonios de las personas naturales y jurídicas y el sistema financiero en general.

4 METODOLOGÍA.

4.1 Diseño

Según lo planteado en los objetivos tanto general como específicos, el presente trabajo se llevó a cabo mediante la investigación descriptiva con un enfoque mixto (cuantitativo y cualitativo) así mismo se realizó la recopilación de información documental como libros, portales web, revistas y noticias sobre los fraudes con tarjetas de crédito.

Al implementar la investigación descriptiva en un proyecto de investigación se tiene como fin organizar, sintetizar, caracterizar y ver la información de forma más sencilla permitiendo que tanto el ente evaluador como los lectores tengan una mayor comprensión de la información. Según (Bernal, 2010), “una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de ese objeto (Bernal, 2010)

Siguiendo el concepto de Bernal con lo anterior se identifica que la investigación descriptiva es uno de los procedimientos más usados cuando el

investigador se considera principiante en el tema, es una herramienta ideal para trabajos de grado ya que su principal característica es la narración de carácter descriptivo, mostrando hechos, referencias o rasgos del objeto de estudio. Este modelo de investigación encuentra su soporte en muchas ocasiones en instrumentos como encuestas, entrevistas, la observación e incluso la recopilación documental.

Así mismo el enfoque Cuantitativo caracteriza un método para llevar a cabo la investigación descriptiva, de acuerdo a lo descrito por Bernal (2010) nos define el método cuantitativo como un método tradicional de investigación que se fundamenta en la medición de las características "lo cual supone derivar de un marco conceptual pertinente al problema analizado, una serie de postulados que expresen relaciones entre las variables estudiadas de forma deductiva" (cita) se puede concluir que este método de investigación tiene como punto inicial las teorías ya aceptadas por la comunidad científica y cuya finalidad es demostrar la veracidad del supuesto (Bernal, 2010).

Por otro lado, tenemos la investigación cualitativa la cual se lleva a cabo por medio de la recopilación de información, utilizando herramientas como textos, gráficos o imágenes que permitan comprender y analizar los datos arrojados por medio de la investigación. De acuerdo con Bernal (2010) "los investigadores que utilizan el método cualitativo buscan entender una situación social como un todo, teniendo en cuenta sus propiedades y su dinámica" (Bernal, 2010).

4.2 Instrumento.

Por otro lado, se implementó un instrumento de recolección de información en la población de estudio la cual en el presente proyecto fue la Corporación Universitaria Minuto de Dios sede Soacha tomando como muestra estudiantes pertenecientes a programas virtuales y distancia. El instrumento aplicado tuvo como finalidad identificar las variables de la investigación como lo son el fraude y la percepción del mismo para cada uno de los encuestados, así como sus experiencias con fraudes financieros realizados por medio del uso de tarjetas de crédito; es importante conocer que una encuesta (método de recolección de información usado en la presente investigación) es una técnica que permite mediante la aplicación de un cuestionario a una muestra de

personas ya definidas recolectar información que permita conocer opiniones, conocimientos o actitudes sobre un tema en específico. De esta forma se pude llevar a cabo la comprobación de una hipó tesis, así como identificar de forma metódica un conjunto de testimonios con el fin de cumplir un objetivo o propósito ya establecido.

El instrumento de la presente investigación se planteó desde tres enfoques siendo primero una caracterización del encuestado, luego de esto se realizó un sondeo inicial para determinar si la persona ha sido víctima de fraude financiero con tarjeta de crédito y según la respuesta brindada se desglosan nuevas opciones que permitieron conocer cuál ha sido su experiencia o si por el contrario no ha presentado dicha afectación cual ha sido el motivo y que información tiene para aportar respecto al tema de la investigación.

De igual forma en el instrumento se plantearon preguntas de tipo cerrado contando además con dos preguntas de opción múltiple por medio de las cuales se buscó conocer cuál ha sido el método por medio del cual el encuestado fue víctima del fraude, así como conocer canales transaccionales más usados por los mismos.

4.3 Muestra.

La muestra en la cual se aplicó el instrumento de estudio se tomó de acuerdo con los datos suministrados por parte de los encargados a nivel administrativo y se sustenta de acuerdo con la aplicación de fórmulas basadas en la estadística descriptiva como se explicará a continuación:

Imagen 1 - Formula.

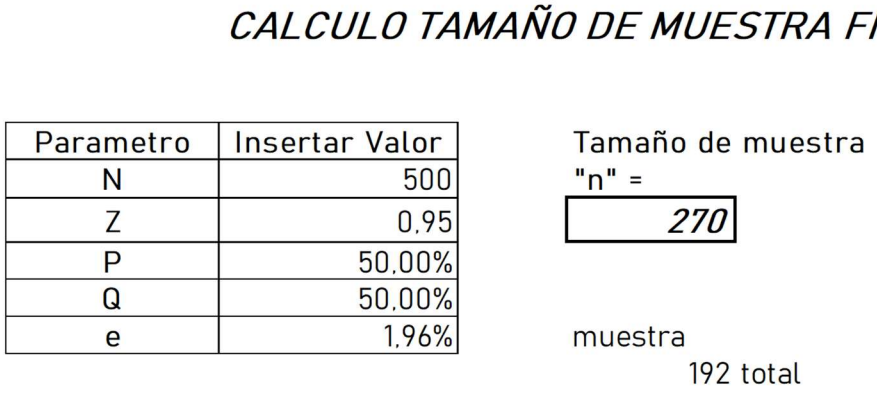
$$\boldsymbol{n} = \frac{N * Z_{\alpha}^{2} * p * q}{e^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

(Morillas, 2007)

Se debe tener presente que cada parámetro le da estructura a la formula, siendo así:

- N: representa el tamaño de la población (Universidad Minuto de Dios).
- n: representa el tamaño de la muestra buscado o deseado: según los cálculos entregados por la fórmula la muestra deseada era de 297 sin embargo, teniendo en cuenta la asistencia al centro académico el instrumento fue aplicado de forma exitosa a 192 personas, aplicación que se llevó a cabo durante los sábados en jornadas de la mañana.
- Z: representa el parámetro estadístico el cual depende del Nivel de Confianza.
- e: El error máximo de estimación aceptado dentro de la investigación y la aplicación.
- p: esta variable determina la probabilidad de que ocurra el evento estudiado (Probabilidad de que ocurra fraude financiero con tarjeta de crédito)
- q: probabilidad de que no ocurra el evento estudiado.

Imagen 2 - Muestra



(Morillas, 2007)

5 MARCO TEÓRICO.

5.1 Qué son las tarjetas de crédito.

Las tarjetas de crédito son un producto financiero que permite realizar compras y avances en efectivo generando el pago de estos valores de forma posterior; con una tasa de

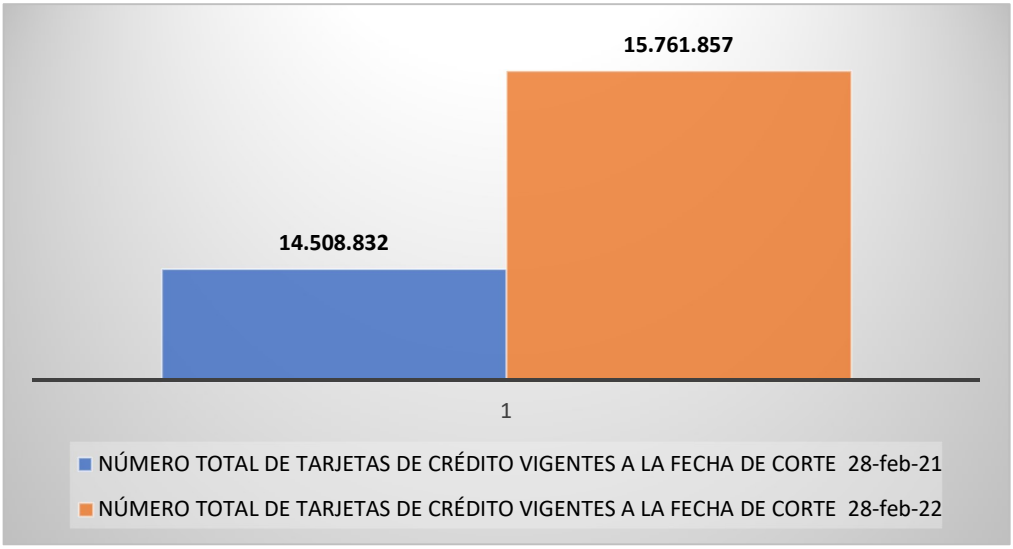
interés pactada con la entidad bancaria que entrega el plástico crediticio. Las entidades financieras mantienen diferentes tasas de interés con el fin de generar una mayor captación de cliente en pro de los beneficios que sus plásticos pueden brindar, beneficios tales como:

- Compras sin pago de intereses si son diferidas a una sola cuota.
- Acumulación y redención de puntos por cada transacción realizada.
- Pagos mínimos pactados de acuerdo con la capacidad económica del titular.
- Cubrimiento a nivel nacional e internacional para el uso de las tarjetas de crédito

Las tarjetas de crédito se usaron por primera vez a comienzos del siglo XX siendo la hoy franquicia Diner's Club pionera en la implementación de lo que se consideraba un título a crédito que permitía a los socios cargar sus compras y comidas a la cuenta de los clientes que tenían el título crédito, cargaban su comida en esté y el restaurante enviaba la factura a Diner's Club quien a su vez enviaba el pago directamente al banco del restaurante, llevándose una pequeña comisión por la transacción. Durante el primer año de esta implementación la empresa Diner's Club logro tener más de 10.000 socios y alrededor de 28 comercios entre restaurantes y hoteles que se acogían a su nueva forma de pago. Para el año 1958 American Express desarrolló su primera tarjeta de crédito la cual lamentablemente termino generando pérdidas en menos de 10 años dado que se daban títulos créditos por máximo 300 dólares a más de 60.000 clientes desembocando en una crisis por tasas de mora de más del 20%. En 1958 se creó BankAmericard la franquicia que hoy conocemos como VISA y la empresa Interbank Card Association conocida en la actualidad como MasterCard. (Sn, Banco BBVA, 2016)

Según datos de Asobancaria (Asociación Bancaria y de Entidades Financieras de Colombia) con corte al 28 de febrero 2022 en Colombia había 15.761.857 tarjetas de créditos vigentes en el mercado, presentando un crecimiento de 8,64% en comparación con el mismo periodo del año anterior como se evidencia en la siguiente gráfica.

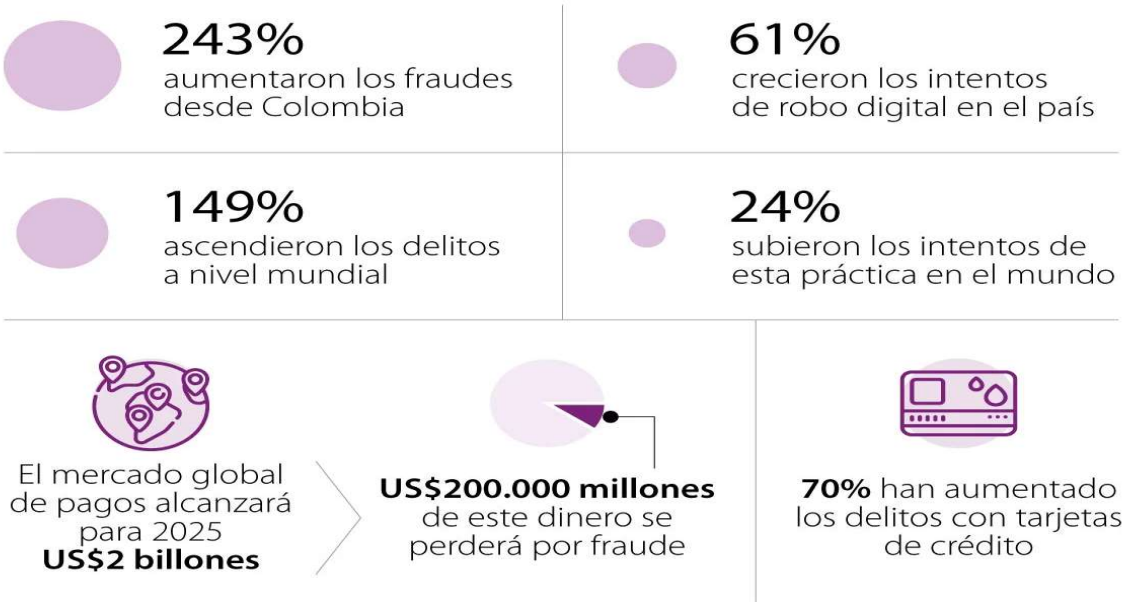
Gráfico 1 - Tarjetas de Crédito vigentes.



(Magon & Barros, 2022)

Según la misma entidad supervisora para septiembre del 2021 cuatro de cada 10 fraudes presentados en el sistema financiero fueron cometidos con tarjetas de crédito por medio de canales digitales concentrado un mayor índice de casos en la banca móvil. Paradójicamente cuando la sociedad busca una forma de acercarnos creando facilidades para procesos de compra y venta así como pagos ejecutados en línea, los delincuentes también se las ingenian para sacar provecho de estas nuevas herramientas afectando la economía de las empresas, según TransUnion entidad encargada de brindar soluciones de información económica y financiera en su informe sobre sobre seguridad financiera y digital entre enero y abril de 2021 las estafas para la industria financiera aumentaron 61% al mismo tiempo que aumentaron 70% los delitos con tarjetas de crédito en el país. A continuación, encontraremos los datos concretos. (Vargas, 2021)

Imagen 3 - Fraudes



Fuente: TransUnion y BPC Banking Tecnologies / Grafico LR-ER.

Para el mes de febrero de 2022 en Colombia se realizaron 24.720.126 transacciones con tarjetas de crédito las cuales correspondieron $5.086.228 millones de pesos según datos brindaron por Asobancaria en su reporte mensual de tarjetas de crédito: transacciones totales por compras teniendo en cuenta que dichas cifras solo recogen las transacciones ejecutadas en comercios nacionales tanto presenciales como online durante el mes.

Como un dato histórico es importante resaltar que para el año 2013 los fraudes electrónicos realizados con medios o productos financieros le costaron al país $3.600 millones de dólares, es decir, el 1% del PIB de dicho año.

La diversificación de las empresas y la forma en la que las personas hoy en día hacen compras no lo han puesto nada fácil para los bancos y los términos legales. En los últimos años se comenzó a ver un mayor auge en lo que a compras en línea o comercio electrónico se refiere, muchas entidades comerciales han comenzado a ver la ventaja de generar sus ventas de forma online puesto que así se evitan gastos como alquileres o infraestructura y a los usuarios les beneficia puesto que pueden acceder a casi cualquier

producto o servicio desde donde estén haciendo pagos en línea y recibiendo los productos en los hogares.

5.2 Qué es fraude.

La palabra FRAUDE proviene de latín FRAUD y hace referencia a un hecho que para nada tiene que ver con lo que se considerar correcto, honesto o verdadero. Este hecho implica el perjuicio de personas u organizaciones, este es considerado un acto de deshonestidad y engaño a fin de beneficiarse sin el propio valor de la ética.

Por otra parte, este acto se considera como un acto con intención ya que involucra aspectos como la manipulación y falsificación de documento y/o información considerada como personal; ahora bien, como se mencionaba antes es una violación a la ética, ética que no solo es de manera profesional sino también humana puesto que el beneficio a costa de terceros es un acto de avaricia, ya que no se tiene conocimiento pleno de lo que el tercero puede enfrentar ante un fraude. (Agudelo, Gallego, Gómez, & González, 2020)

5.3 Que es el fraude financiero.

Como se mencionaba anteriormente el fraude es un acto por el cual se obtiene un beneficio a costa de terceros, pero el fraude financiero se enfoca en el la obtención de beneficio a costa de una organización donde el, la o los individuos que componen las áreas administrativas alteran la información financiera de dicha organización, tales actos como: alteración de los estados financieros; que a su vez involucra falsificación de documentos, el inadecuado uso de recursos, el inadecuado uso de las políticas internas, entre otras.

Así mismo incurre en el acto antiético el cual refleja el comportamiento poco profesional de un individuo, dando por hecho que el engaño, la deshonestidad y falta de compromiso con la organización jamás ha estado en juicio del individuo. Así mismo se considera que el individuo uso sus habilidades en contra y no a favor de la organización.

Es importante tener claro que los fraudes financieros tienen como fin desviar o apropiarse de recursos poseídos por una organización, ya sean monetarios o no. También se

comprende como fraude financiero el soborno a terceros a fin de obtener información de carácter importante con la cual después podría beneficiarse.

El fraude involucra diferentes actos tales como falsificación de documentos pagos ficticios alteración de pagos, alteración de facturas, negociaciones inusuales con proveedores y clientes. Todo acto monetario que dé lugar a la evasión de información sin conocimiento o autorización previa de la organización puede considerarse fraude financiero.

5.4 Comercio electrónico.

También conocido como e-commerce es el canal que indica las transacciones que se realizan en línea y que están soportadas por la tecnología digital, en esta metodología se utilizan las computadoras, celulares, Tablet o demás dispositivos electrónicos incluyendo en este proceso captura, almacenamiento, análisis, presentación logística envió y comunicación de datos.

En el país se llevó a cabo la creación de la Cámara Colombiana de Comercio Electrónico, en la cual es una entidad sin ánimo de lucro y con carácter gremial que busca poder promover y fortalecer la industria del eCommerce en Colombia a través del entendimiento; se debe tener en cuentas que en los pagos realizados en comercios electrónicos el 85% de las transacciones se ejecutan por medio de tarjetas de crédito lo cual le da una ventaja casi total frente a otros métodos de pago usados, esto se debe según los expertos a que se tiene la creencia de que las plataformas implementadas para los pagos online cuentan con parámetros de confianza y calidad los cuales eliminan la información del usuario una vez generada la transacción a menos que el cliente disponga lo contrario, por otro lado también se debe tener en cuenta que el uso de la tarjeta de crédito nos brinda cierto pensamiento de pago póstumo.

De acuerdo con el último Informe de Operaciones en Colombia de la Superfinanciera, los medios digitales han incrementado su participación en las operaciones monetarias y no monetarias realizadas en el país, 52,7 % fueron por el móvil, 20,6 % por Internet, 7,5 % por cajeros automáticos, 6,7 % por datafonos, 4,5 % por corresponsales

bancarios y solo 3,9 % por oficinas físicas. (Sn, Revista Semana, 2022); Esto demuestra que como consumidores hemos comenzado a migrar a la era de la digitalización realizando todo tipo de procesos transaccionales desde la comodidad y a distancia con los móviles, pero es importante destacar que muchos usuarios que realizan estos procesos no tienen una conciencia sobre el uso adecuado de las tecnologías cuando la información financiera se refiere y desconocen cómo pueden ser víctimas de fraudes, así como aquellas normativas que brinda la ley con relación al tema.

5.5 Delito electrónico.

De acuerdo con lo descrito en la página web de la Policía Nacional de Colombia los delitos informáticos son conductas fraudulentas utilizadas por delincuentes quienes con la ayuda de programas informáticos obtienen información para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería. Esto nos lleva a mencionar la normativa de delitos informáticos que rige en Colombia la Ley 1273 de 2009 por medio de la cual se hace una modificación al Código Penal con el fin de crear un nuevo bien jurídico llamado “Protección de la información y los datos” con esto se busca poder tener medidas legales que prevean y sancionen acciones tales como:

- Uso de software maliciosos.
- Suplantación de sitios web con el fin de obtener datos personales.
- Transferencias de activos no consentidos.
- Hurto por medios informáticos.

5.6 Qué es el fraude financiero electrónico.

La tecnología día a día avanza y con ello las diferentes compañías deben innovar, es por ello que los medios electrónicos impactan en gran medida sin embrago, este medio se encuentra en constante riesgo y es ahí donde se presentan los fraudes de tipo electrónico, estos son considerados actos delictivos mediante transacciones online, ese se basa en la obtención de dinero por medio de actos ilícitos, engaños o el aprovechamiento de errores.

Los entes organizadores de estos actos de fraude utilizan diferentes mecanismos por los cuales obtienen información personal como nombres, números de documento, teléfonos, correos; así mismo, información bancaria donde obtienen números de tarjetas de crédito, usuarios, contraseñas, códigos de seguridad que facilitan el acceso a los diferentes aplicativos bancarios para de esta forma planear y organizar la estafa. (Alvarez & Mejia, 2021).

Ahora bien, durante los últimos años se han conocido números casos de fraude electrónico con tarjeta de crédito, se tiene el claro ejemplo de la exdirectora del banco de la república Carolina Soto quien fue víctima de "cambiazo" como así lo menciona un artículo de prensa de El Colombiano. En el mes de marzo del presente año la exdirectora anuncio que su tarjeta de crédito había sido cambiada. Días atrás se presentaron en su residencia anunciando que su tarjeta de crédito tenía una actualización pendiente y por ende debía ser cambiado el plástico de la misma.

Carolina Soto presento una perdida con su tarjeta de crédito de $11.000.000 millones de pesos los cuales se representaron en tres grandes compras en un establecimiento de Bogotá; ella afirmo ante la entidad financiera haber recibido diferentes llamadas para el cambio de su tarjeta de crédito, así mismo indico haber presenciado el momento en el que destruyeron su tarjeta de crédito antigua. Por lo que después de eso non imagino de lo que sería víctima. ((El Colombiano, 2022)

5.7 Ingeniería social.

Es importante reconocer que como seres humanos somos la mente más fácil para manipular cuando a compararse con máquinas se refiere. Es aquí cuando entre a jugar un papel fundamental la ingeniería social herramienta en la cual se valen de técnicas psicológicas con el fin de manipular la mente y el comportamiento de un individuo. Según la empresa de tecnología líder en cuanto al software de protección Avast, la ingeniería social se puede definir como "aprovechamiento del error humano para actuar en contra de sus intereses. En cuanto a seguridad de la información, la ingeniería social se refiere a conseguir que las personas divulguen datos privados en línea, como datos de acceso o información financiera" (Bodnar, 2020)

Los ataques de ingeniera social se realizan en su gran mayoría de forma remota, bien sea de forma online o por medio de teléfonos, los atacantes en muchos casos son personas que pueden llegar a ganar la confianza de la victima de forma rápida y una vez la confianza ya fue obtenida el atacante comienza a generar cuestionamientos que le permiten poder obtener la información personal y financiera de la víctima. Según la información recogida por empresas de seguridad informática como Avast hoy en día la forma más común de generar ingeniería social con el fin de estafas se presente por medio de las redes sociales ya que son aplicaciones en las cuales se suelen compartir momentos o información del día a día las cuales son aprovechadas por los atacantes con el fin de tener información básica antes de comenzar a implementar la ingeniería social.

Los tipos de ingeniería social más usados para el fraude son Phishing, Spear phishing, Vishing, Smishing, Whaling, Baiting, Scareware, Pretexting y Spam en el correo electrónico; todos estos serán tratados en el siguiente ítem.

5.8 Modalidades de fraude electrónico.

Si bien los fraudes electrónicos se han presentado con mayor frecuencia debido a la innovación tecnológica que día a día se presenta es importante tener conocimiento de las diferentes modalidades que existen y como se llevan a cabo, dentro de ellas están:

5.8.1 Phising.

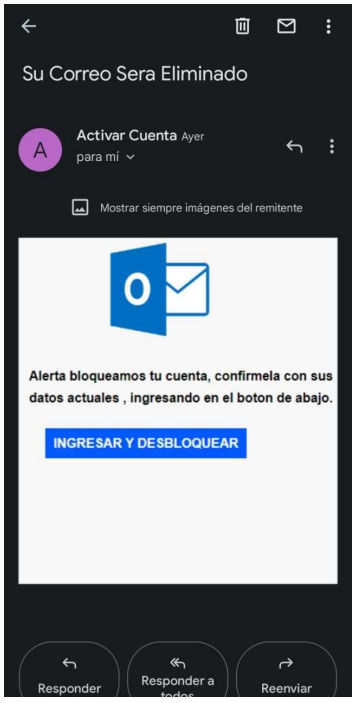
Según (Cumpa, 2021) este se da en un acto de suplantación de identidad, donde se obtienen datos confidenciales de manera ilícita, dichos datos tales como contraseñas de cuentas bancarias o números de tarjetas de crédito. Esta modalidad se da por medio de correos electrónicos con un link que redirecciona a las víctimas a una trampa y por medio de portales web obtiene datos que las victimas según el caso podrían estar actualizando o gestionando una compra con bonos promocionales que supuestamente la entidad financiera les entrega.

Cabe resaltar que una de las características de esta modalidad es hacer creer que el usuario está teniendo contacto con la entidad financiera obteniendo si la confianza de la víctima a fin de obtener información que sea útil.

Por otra parte, un estudio realizado por RZ Redes Zone (Jimenez, 2021), en donde se realizó un estudio de quienes caían más en este tipo de fraude, dicha investigación indico que quienes caen en esta modalidad son jóvenes entre los 18 y 19 años de edad, así mismo se determinó que los jóvenes entre los 20 y 29 años son micha más precavidos con este tipo de situaciones; sin embargo se evidencio que los adultos mayores después de los 60 años de edad son más propensos a caer en este tipo de fraude.

Finalmente, el articulo resalta el hecho de cada persona debe tener sentido común a la hora de encontrarse con este tipo de mensajes pues un link inusual es de dar sospechas.

Imagen 4 - Correo Smishing.



(Magon & Barros, 2022)

5.8.2 Vishing.

Según el artículo del portafolio (2021) este es un mecanismo de estafa en donde el victimario realiza una llamada a la víctima, de tal manera se rigüe por un protocolo tal y como lo haría un ente financiero obteniendo la confianza del individuo haciéndose pasar como funcionario entregando información parcial de los productos financiero o datos personales del mismo. Esta llamada puede implicar promociones exclusivas a la víctima o incluso advertir de algunos riegos a la hora de realizar transacciones con los productos financieros ya obtenidos. De este modo la victima entrega los datos y es en ese momento donde el victimario abre la ventana que lo conduce a realizar el llamado fraude. (Portafolio, 2021).

Ahora bien, es importante que las víctimas de esta modalidad no siempre contestan una llamada por parte de una entidad financiera en algunos casos se ha presentado como el llamado de una empresa prestadora de un servicio como lo es el gas, el agua, entre otros. Estos también pueden ser victimarios de Vishing puesto que con la excusa de revisar un portafolio o bonos promocionales llegan a la información de interés que logra completar su estafa.

Por otra parte, un artículo de Santander (2022) menciona que el Vishing también puede presentarse en una doble llamada lo cual genera más confianza a la víctima. El articulo indica que este método es aún más complejo este consiste en un mensaje grabado como un robot donde se le informa a la víctima de un eventual problema, como un pago o acceso no autorizado en su banca digital (aplicación) dándole un número de teléfono al cual debe comunicare para dar solución a la situación. Y es ahí donde la víctima termina realizando la llamada entregando de manera sencilla los datos todo a din de verificar el movimiento que según eso se había realizado. (Santander, 2022)

5.8.3 Malware.

Para Navarro (2021) esta modalidad de fraude se basa en la instalación de un programa o virus malicioso, esta sin autorización directa de la víctima, este virus genera un error informático, borra o genera inconvenientes ante la accesibilidad a información. El

único propósito de este tipo de fraude es exigir recompensa a la víctima por la recuperación de datos. (Navarro, 2021)

Es muy común hoy en día el teletrabajo pero se debe tener presente que los accesos remotos (Any Desk, teamviewer) pueden representar puertas abiertas a otros dispositivos de los cuales no se tiene seguridad y que de alguna manera un tercero podría estar accediendo a información valiosa en los dispositivos, de esta forma aun y cuando un empleado este gestionando o realizando alguna labor puede existir alguien más con acceso nos solo a uno sino a dos dispositivos de los cuales podría robar información para finalmente pedir de igual forma una jugosa recompensa a cambio de su recuperación.

Ahora bien, Cumba (2021) indica que esta modalidad también se presenta mediante links en donde se le informa a la víctima de un tipoi de cobro o investigación, es en ese momento donde la victima accede a un link y sin saberlo realiza la descarga de un malware y/o virus ocasionando daños en el ordenador permitiendo el acceso para robo de información.

Podría decirse que esta modalidad puede llegar a ser una cadena con modalidades como el Smishing y el Phising ya que estas por su medio de comunicación podría abrir paso al malware con solo acceder al link así fuera por simple curiosidad de la víctima. Es por ello por lo que hoy en día los correos y SMS son tan desprestigiados por parte de la población pues muchos acceden y solo se encuentran con publicidad de diferentes entidades lo que de alguna manera genera desconfianza.

5.8.4 Smishing.

Tarriño (2022) indica en un artículo del banco BBVA que el Smishing es una de las técnicas más usadas por los ciber estafadores con ella roban datos personales e información de los usuarios esto se da suplantando a entidades financieras por medio de mensajes de texto (SMS). Si bien durante los últimos años ha crecido debido a los cambios tecnológicos que con el tiempo se han presenciado existen maneras de, detectar en qué momento se está siendo víctima de esta modalidad de estafa. (Tarriño, 2022).

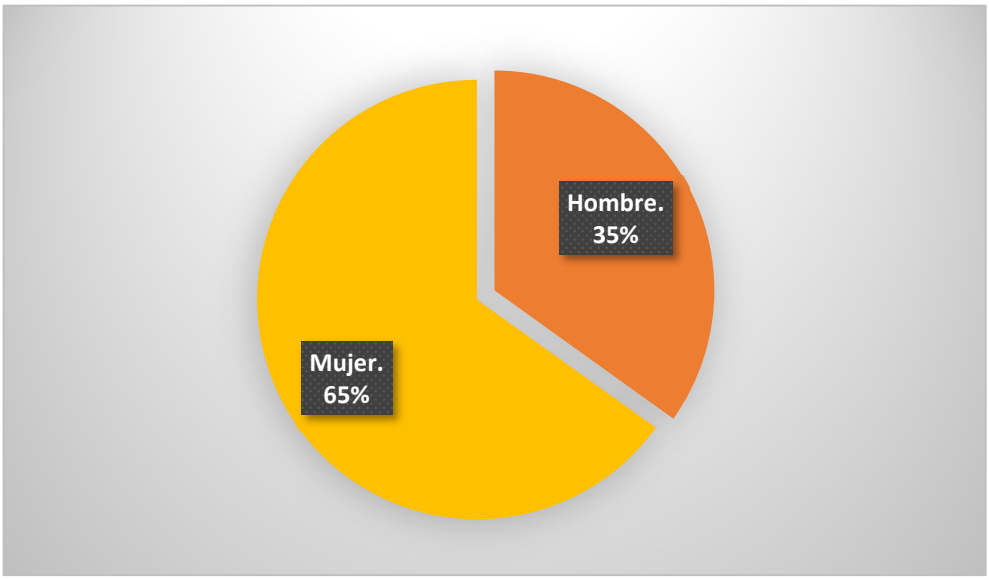
Por otro lado, Cumba (2021) indica que otra de las características de esta modalidad es que mediante el mensaje de texto llega un link le informa a la víctima que ha recibido un premio, descuento o bono y que debe dirigirse al link que eventualmente lo llevara a redimir su premio, pero lo cierto es que el link pide sus datos personales para corroborar según eso la información, pero este solo esta almacenando la información para los victimarios.

Si bien hoy en día la mayoría de la población tiene claro que mensajes de texto con estas características no pueden llegar de un numero de celular común, ya que las entidades cuentan con un código para envió de mensajes de este tipo. Sin embargo, en la actualidad se ha presentado la suplantación por medio de esto códigos resguardados por las entidades financieras sin más los mensajes de texto podrían llegar justo en el momento en el que la víctima realice una transacción justo debajo del mensaje que confirmaría dicho movimiento; es por ello que lo lógico no sería acceder a links que llegan por este medio sino comunicarse con la entidad financiera a fin de validar la información.

6 RESULTADOS.

6.1 Genero.

Gráfico 2 – Genero.



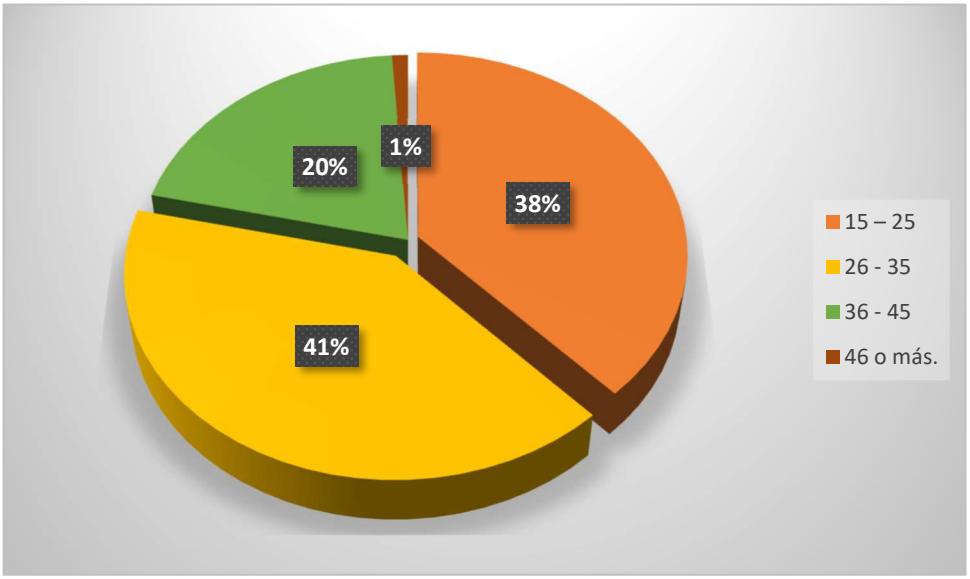
(Magon & Barros, 2022)

Es importante iniciar la implementación de un instrumento de recolección de datos con preguntas que permitan conocer la caracterización de los participantes en la misma; en el presente proyecto la encuesta fue aplicada en una muestra de 192 personas de las cuales 126 fueron mujeres y 66 hombres. Ahora bien, al momento de llevar estos datos a porcentajes como lo recomienda el modelo cuantitativo para dichos casos se puede inferir que del 100% de los participantes el 65% fueron mujeres y 35 % hombres.

Lo anterior permite caracterizar la población y a su vez la muestra con una dominante femenina.

6.2 Edad.

Gráfico 3 – Edad.



(Magon & Barros, 2022)

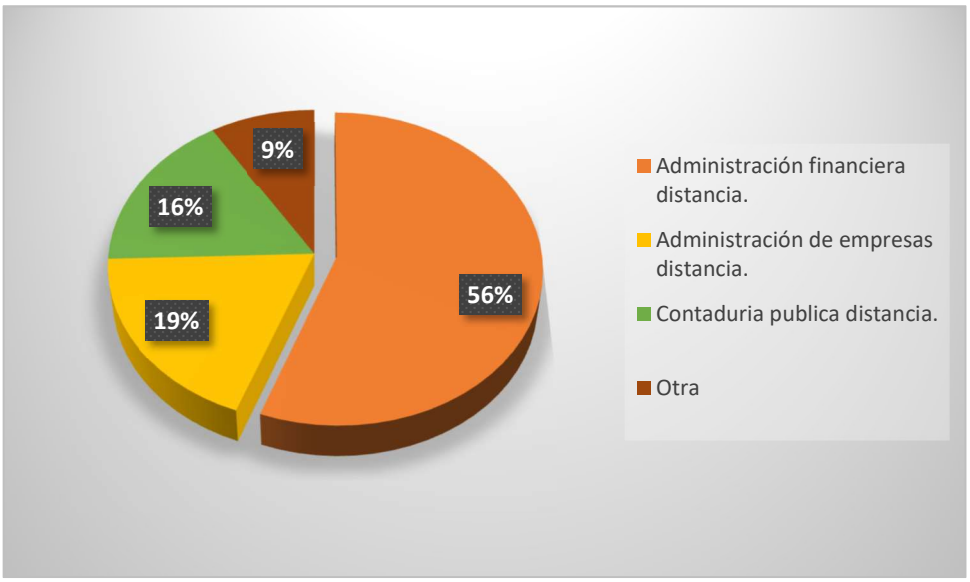
Partiendo desde la premisa de que los encuestados son jóvenes y adultos universitarios a quienes les fue aplicado el instrumento de recolección de datos dentro de las instalaciones de la Sede Soacha de la Corporación Universitaria Minuto de Dios, la edad nos lleva a encontrar otro factor importante en el proceso de la caracterización. En el instrumento de recolección se brindaron 4 opciones de respuesta con rangos de edades de la siguiente forma:

- 15 – 20 años: representaron la segunda mayor población, con 73 personas de las encuestadas lo que fue equivalente al 38%.
- 26 – 35 años: Siendo la mayor población presente en el proyecto con un total de 81 encuestados y equivalente al 41% es la población que más podemos encontrar dentro del centro regional en las jornadas virtual tradicional en las cuales fueron aplicado el instrumento.
- 36 – 45 años: represento el 20% de la población encuestada con un total de 36 respuestas.

- 46 o más: podemos decir que fue la población con mayor minoría en la aplicación del instrumento de recolección representando el 1% de la misma con 2 encuestados.

6.3 Programa al que pertenece.

Gráfico 4 – Programa.



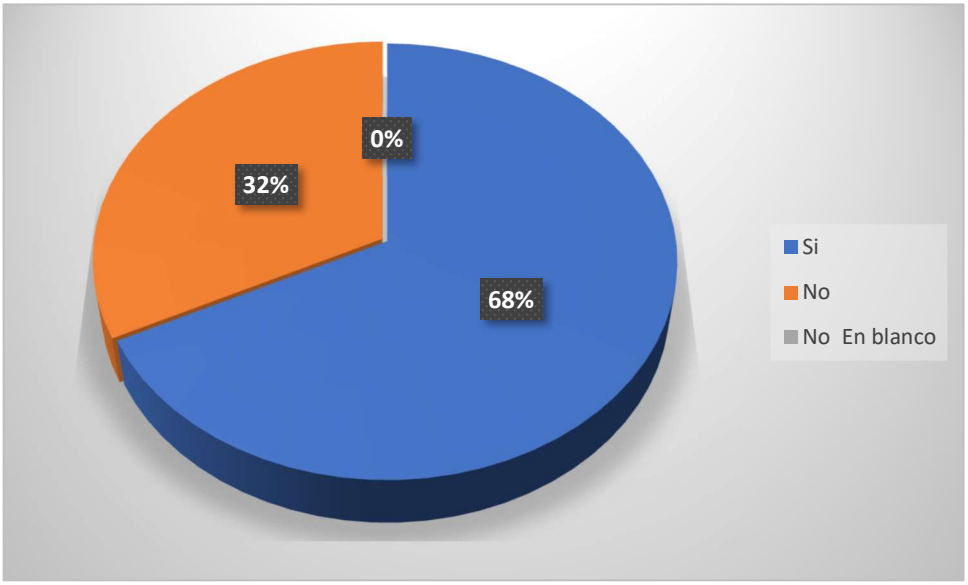
(Magon & Barros, 2022)

Inicialmente el instrumento de recolección de datos fue aplicado a carreras enfocadas en las ciencias empresariales pero siendo testigos de la necesidad de conocer diferentes puntos de vista y contar con testimonios fue abierta a carreras tales como Contaduría Pública y Otra dentro de las cuales tenemos Salud y Seguridad Ocupacional e incluso especialización en mercadeo y gestión organizacional; de esta forma de las 192 encuestas 107 correspondieron a la carrera Administración Financiera Distancia representando el 56% de los encuestados, Administración de Empresas Distancia con el 19% equivalente a 39 encuestados, Contaduría Pública con 16% equivalente a 35 de los encuestados y 20 encuestados perecientes a otras carreras (indicadas anteriormente) lo cual representa el 9% para un total de 100%

Es importante destacar que el estudio tuvo una muestra en su mayoría con estudiantes de carreras orientadas en las ciencias empresariales con el fin de conocer el nivel de educación financiera que tienen los próximos profesionales en campos administrativos educación que se requiere con suma importancia en dichos campos pues serán los encargados de orientar a otros.

6.4 ¿Tiene o ha tenido usted una tarjeta de crédito?

Gráfico 5 - Uso tarjeta.



(Magon & Barros, 2022)

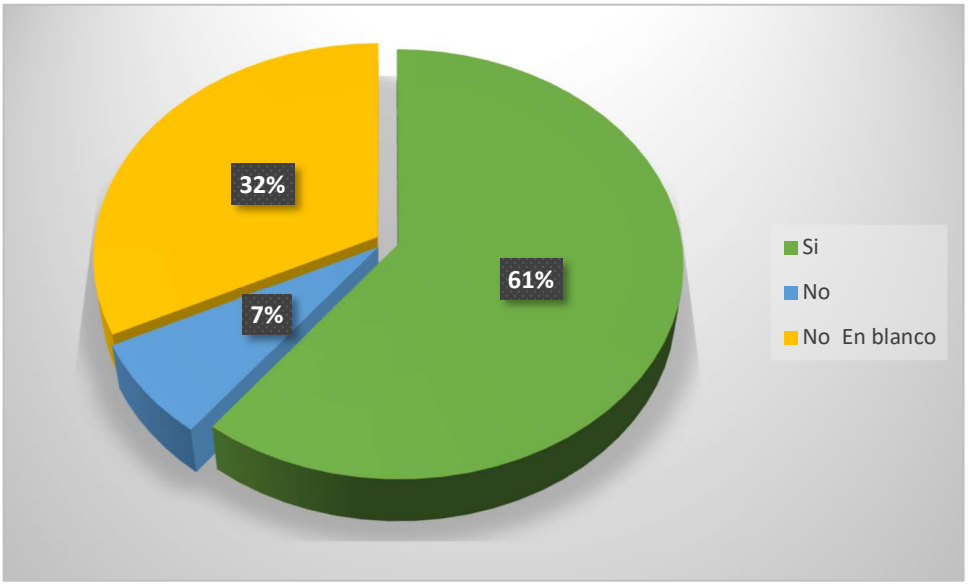
En la presente pregunta comienza el proceso de orientación para determinar el número de encuestados dentro de la muestra que permitieron llevar a cabo los objetivos del presente proyecto, puesto que con esta buscamos poder conocer los encuestados que tienen o han tenido tarjetas de crédito y que por ende han podido llegar a ser víctimas en un fraude durante el uso de esta. Es aquí donde se estructura el conocimiento del que son conscientes los tarjetahabientes sobre los beneficios, pero también la responsabilidad que conlleva tener una tarjeta de crédito.

De esta forma se evidencia que de 192 encuestados 130 informaron que sí han tenido o tiene en el momento un plástico crediticio mientras que 62 responden de forma

negativa; esto convertido en porcentajes nos representa 68% sí tiene tarjeta y 32% no tienen. Es decir que la información en cuanto al uso de la tarjeta, posibilidad de fraude, métodos y demás requerida se basara en esas 130 respuestas afirmativas. Para el caso de que las personas indican que no han tenido o tener tarjetas igualmente se desglosaran preguntas más adelante con el fin de conocer este motivo y determinar si se debe a la falta de educación financiera o certeza de seguridad.

6.5 ¿Tiene usted clara la debida forma de usar una tarjeta de crédito?

Gráfico 6 - Manejo tarjeta.



(Magon & Barros, 2022)

Si bien podemos dar por hecho de que toda persona que tiene una tarjeta de crédito conoce o tiene clara la forma en que la misma debe ser usada no solo en cuanto a compras y pagos si no a protección de información personal que refleja la misma tarjeta dadas las cifras actuales sobre los fraudes podemos inferir en que no es una información del todo clara y que muchas veces se debe a la falta de educación financiera por parte de los usuarios y la negativa a entregarla de forma oportuna por parte de las entidades de financiamiento.

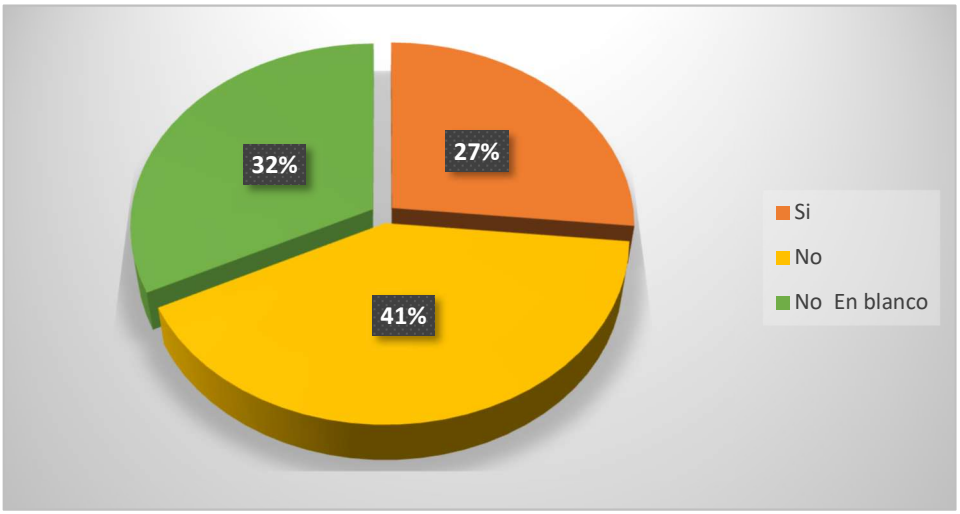
En esta pregunta del presente instrumento de recolección de datos se puedo determinar:

- Del total de encuetados que fueron 192 existe un porcentaje equivalente al 68% (130 encuestados) que informan tener tarjeta y que procedieron a contestar la presente pregunta.
- De estos 130 encuestados 116 indican tener clara la forma adecuada de usar la tarjeta de crédito frente a 14 que indican no conocer dicha información.

En la anterior grafica esto se traduce en porcentajes de 61% para sí y 32% para no; igualmente existe un porcentaje adicional de 7% (para completar el 100%) que registra en blanco el cual es importante aclarar corresponden a las personas que no tuvieron acceso a esta parte de la encuesta pues su respuesta anterior fue negativa pero que se encuentran dentro de la muestra.

6.6 ¿Ha sido víctima o conoce a alguien que haya sido víctima de fraude con tarjeta de crédito?

Gráfico 7 - Victima de fraude.



(Magon & Barros, 2022)

Con esta pregunta se da comienzo a tipificación y conocimiento el objetivo del presente proyecto, teniendo en cuenta que buscamos conocer aquellos casos en donde las

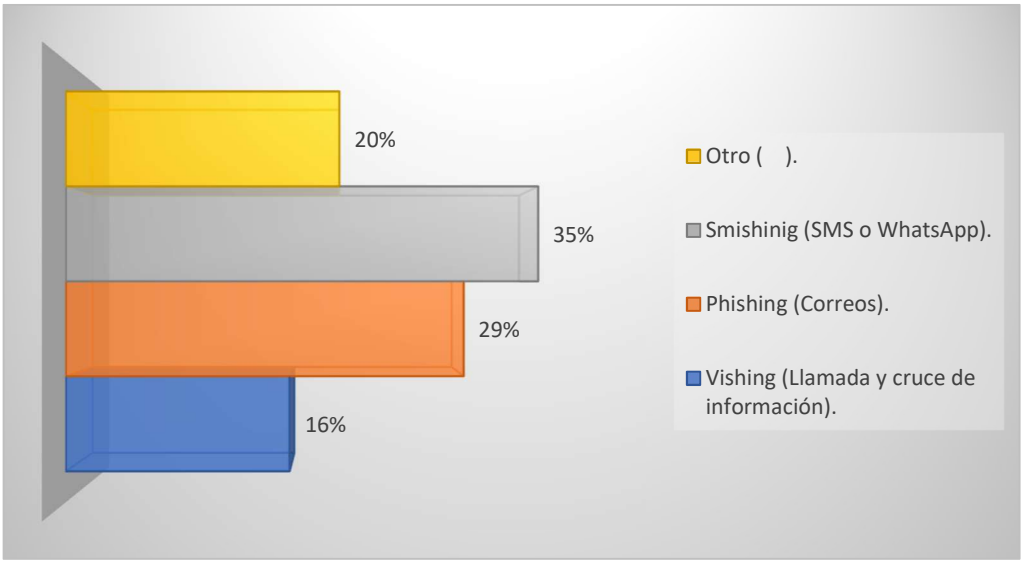
personas han sido víctimas del fraude electrónico por medio del uso de tarjetas de crédito y cuáles son las percepciones que tienen del mismo.

Teniendo en cuenta que del 100% de los encuestados el 32% respondió anteriormente no tener ni haber teniendo tarjetas de crédito en la gráfica se representa como respuestas en Blanco. Por otro las personas que indican si tener tarjetas de crédito o haberlas teniendo en algún momento argumentan que el 27% ha sido víctima o conoce a alguien víctima de fraude financiero con tarjeta de crédito frente a un 41% que informan nunca haber presentado estos problemas.

Si bien a primera vista se observa que el porcentaje de los que indican no haber sido víctimas de fraude es mayor se debe tener en cuenta que aquellos que sí han sido víctimas supera el 50% de los que no lo cual deja un alto porcentaje de afectación y por medio del presente proyecto se buscó conocer esas afectaciones que presentaron.

6.7 ¿Cuál de los siguientes tipos de fraude financiero, considera que fue víctima?

Gráfico 8 - Tipos de fraude.



(Magon & Barros, 2022)

La presente pregunta tuvo como objetivo conocer la información que tienen los titulares encuetados sobre los diferentes tipos de fraude del que pueden ser víctimas y que

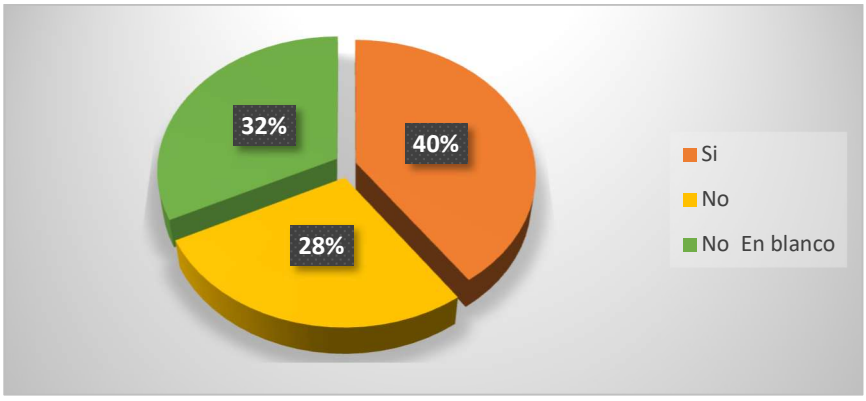
aprendan a identificarlo; así mismo conocer cuál de estos métodos es que mayor presentación está teniendo en la actualidad generando afectación a los tarjetahabientes. La presente pregunta fue aplicada únicamente a las personas que indicaron anteriormente haber sido afectados con fraudes financieros.

Una vez las personas aprendan a identificar los diferentes modelos por los que se puede presentar el fraude sabrán como poder prevenirlo, de esta forma se identificó:

- Smishing fue la modalidad que más argumentan los encuestados que los ha afectado al momento de ser víctimas de fraude con un porcentaje de 35%.
- Phishing fue la segunda mayor modalidad de fraude reportada por los encuestados con el 29%.
- Otro, dentro de este concepto se catalogaron a los encuestados que manifestaron ser víctimas de fraudes electrónico, pero por medio de los canales virtuales que tienen las entidades financieras, dichos canales abarcan cajeros, aplicación móvil, páginas web. A presente categoría ocupo el tercer lugar con un porcentaje del 20%.
- Vishing ocupo el último lugar en cuanto a modalidades de fraude reportada por los encuestados y de la cual han sido víctima; esta modalidad tuvo un porcentaje de afectación de 16%.

6.8 ¿Sabe usted que debe hacer si llega a ser víctima de fraude con su tarjeta de crédito?

Gráfico 9 - Que hacer si es víctima de fraude.



(Magon & Barros, 2022)

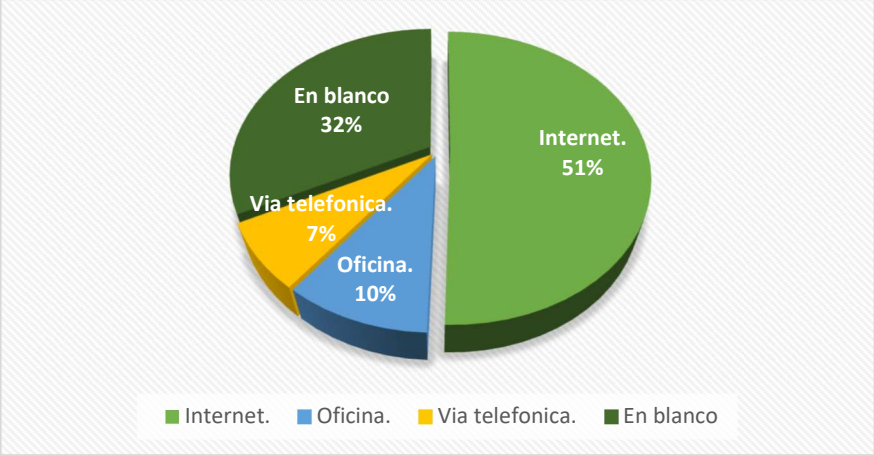
Esta pregunta se consideró de suma importancia para conocer y determinar el estado de la educación financiera que tienen los encuestados y por ende su acción de respuesta ante un posible caso de fraude. De esta forma el proyecto puede abarcar que permitan a los tarjetahabientes conocer diferentes canales y acciones de respuesta para las distintas situaciones que se puedan presentar.

Con la aplicación de la pregunta en el instrumento de recolección de información y teniendo en cuenta la gráfica anterior podemos identificar:

- El 40% de los encuestados aseguran conocer las acciones a seguir una vez se identifican como víctimas en un fraude financiero con tarjeta de crédito en modalidad electrónica.
- El 28% de los encuestados indican no conocer dichos protocolos a seguir, lo cual se traduce nuevamente en un alto índice que corresponde a la falta de educación financiera.
- Por último, en la gráfica se evidencia 32% de encuestas en Blanco, es importante recordar que es el porcentaje correspondiente a las personas que manifestaron no tener tarjeta de crédito.

6.9 Cuando realiza un pago, una compra o una verificación de su tarjeta de crédito los hace por:

Gráfico 10 - Canales de pago.



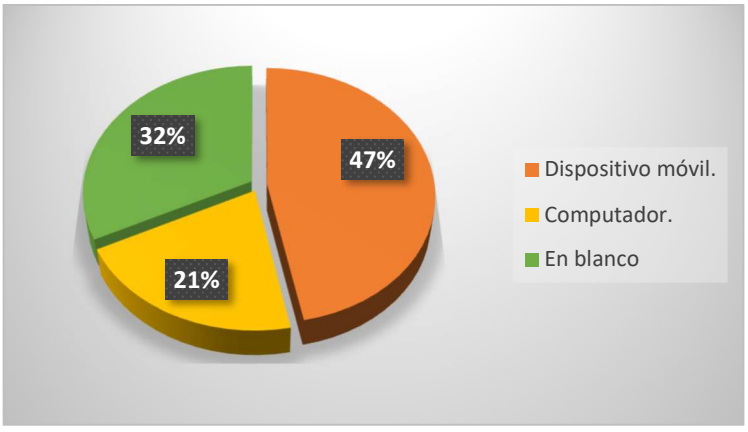
(Magon & Barros, 2022)

En esta pregunta de la encuesta el objetivo era conocer el nivel de uso de canales tanto físico como virtual que realizan los tarjetahabientes y que podría llegar a inferir en las tasas de fraude, teniendo en cuenta que una persona que no usa usualmente los canales digitales en muchos casos no tiene en cuenta las medidas de seguridad que debe tener presente para el uso de este. Una vez finalizado el tiempo de aplicación del instrumento de recolección de información se determinó:

- El 51% de los encuestados indicaron que realizan vía internet procesos tales como pagos, compras e incluso verificaciones de seguridad de la tarjeta de crédito.
- El 10% informo que prefiere hacer estos procesos de forma presencial en una oficina de la entidad financiera.
- El 7% indico que realizan los procesos por medio telefónico.
- Por último, en la gráfica se evidencia 32% de encuestas en Blanco, es importante recordar que es el porcentaje correspondiente a las personas que manifestaron no tener tarjeta de crédito.

6.10 ¿Cuál es su mejor aliado al momento de realizar una transacción digital con su tarjeta de crédito?

Gráfico 11 - Canales digitales.



(Magon & Barros, 2022)

En la actualidad la tecnología avanza a pasos agigantados y es por ello que la mayoría de las transacciones, se realizan por medio de dispositivos tales como el computador o dispositivo móvil, los cuales facilitan la realización de las mismas.

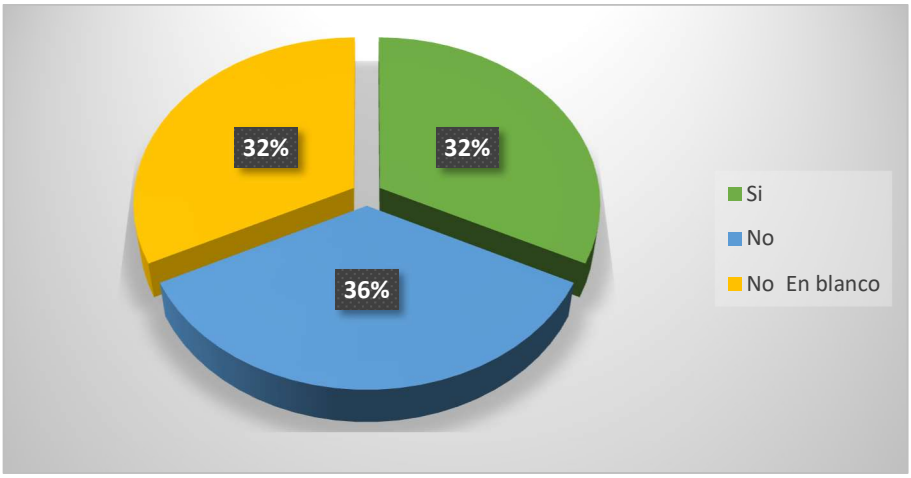
Si bien se identifica, que de los 192 encuestados que hacen referencia al 100% de la muestra; 90 personas que se identifican con el 47% del total de la muestra usan su dispositivo móvil para realizar cualquier tipo de transacción y 40 personas que equivalen al 21% de los encuestados usan un computador para realizar las mismas.

De igual manera se identifica que 62 personas los cuales se identifican con el restante 32% no tiene un producto como lo es una tarjeta de crédito es por ellos que su respuesta es tomada en blanco.

Si bien se comprende que las personas cuyo perfil cuentan mínimo con una tarjeta de crédito en su mayoría usan dispositivos tecnológicos para realizar transacciones de cualquier tipo se encuentran expuestas a ser víctimas de fraude; cabe resaltar que debe plantearse que cuidado tiene este porcentaje de encuestados y si el conocimiento de la manipulación de la información en estos medios es seguro.

6.11 ¿Tiene usted autoguarda la información de tu tarjeta de crédito en sus dispo1tivos personales?

Gráfico 12 - Información en canales digitales.



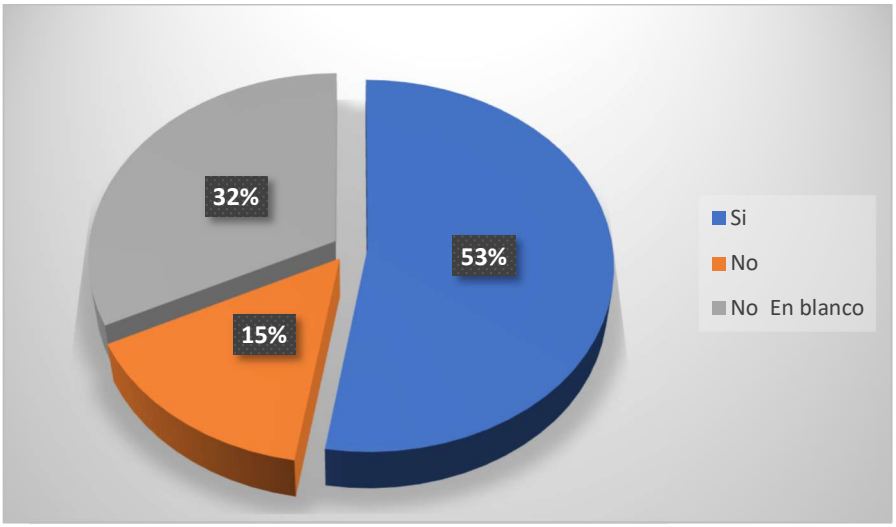
(Magon & Barros, 2022)

Como tarjetahabientes en ocasiones los usuarios no conocen los riesgos que conlleva el tener guardada la información de forma automática en un dispositivo móvil ya sean teléfonos, Tablet, o pc dado que todos estos dispositivos son susceptibles a perdida, robo e incluso a ataques cibernéticos que tienen como fin obtener la información tanto personal como financiera almacenada en el mismo; aun así, en el proceso de recolección de datos la muestra arrojo:

- Del 100% de los encuestados el 32% indico sí tener guardada la información financiera en el dispositivo lo cual se traduce en 62 encuestados.
- Del 100% de los encuestados el 36% indico no tener guardada la información financiera en el dispositivo lo cual se traduce en 68 encuestados.
- El porcentaje equivalente a En Blando dentro de la gráfica corresponde a las personas que al inicio de la encuesta contestaron no tener tarjeta de crédito.

6.12 ¿Tiene usted claro que cuidados debe tenerse presente al momento de ingresar a páginas donde deba cargar información de sus tarjetas de crédito?

Gráfico 13 - Cuidados al ingresar información.



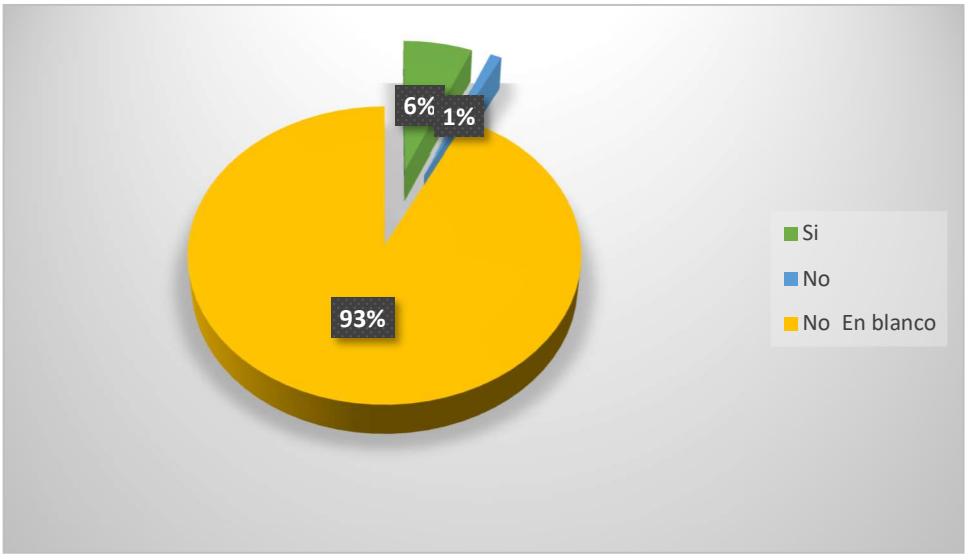
(Magon & Barros, 2022)

Es importante tener claridad de los diferentes movimientos realizados en sitios web y más aun de la información que allí se deposita, es por ellos que se contempló la importancia de analizar qué tan seguros se encuentran los encuestados de los aspectos básicos a tener en cuenta a la hora de ingresar información tan delicada como la de sus productos financieros en este caso las tarjetas de crédito.

De tal manera se aplicó la anterior pregunta a los 192 encuestados de los cuales 101 respondieron que si esto equivale al 53% de la población encuestada; por otra parte 29 de los encuestados respondieron que no siendo este el 15% de la población y finalmente 62 no respondieron esto equivale al 32% de los encuestados, este 32% hace referencia los encuestados cuyo perfil es nulo ya que no cuentan con una tarjeta de crédito. Esta información hace referencia al 100% de los encuestados.

6.13 ¿Cree usted que las tarjetas de crédito atentan contra su estabilidad financiera?

Gráfico 14 - Atentan con estabilidad financiera.



(Magon & Barros, 2022)

Este análisis se llevó a cabo para la población de encuestados cuya respuesta fue no haber tenido ningún producto como lo es una tarjeta de crédito, pero que sin embrago es de

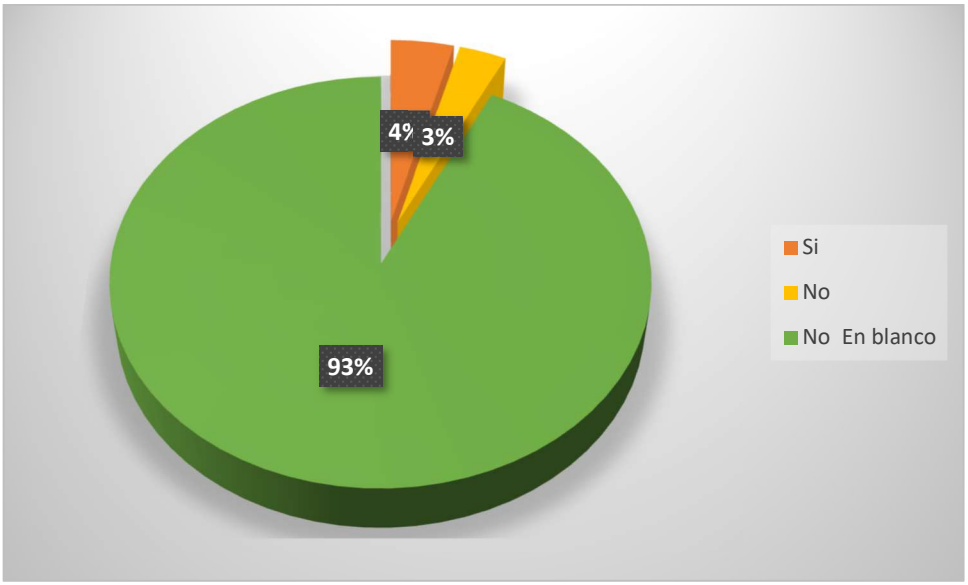
vital importancia tener conocimiento a que se debe que no tengan hoy en día una tarjeta de crédito.

Muchas de las personas hoy en día consideran que productos financieros, aunque necesarias, no son indispensables es por ello, que se requería analizar que parte de la población encuestada no tenían o había adquirido un producto como las tarjetas de crédito y el porqué de esa decisión.

Se denota que de los 192 encuestados que hacen referencia al 100% de la población encuestada 12 personas contestaron que sí lo que equivale al 6% de la población encuestada, lo cual indica que sienten que su estabilidad financiera puede verse afectada por el hecho de tener un producto de este tipo; por otra parte, solo 2 personas tan solo el 1% de los encuestados niegan que el uso de las mismas atente contra su estabilidad financiera simplemente no consideran en su vida financiera un producto de este tipo; así mismo se comprende que las 178 personas restantes que equivale al 93% son los encuestados cuyo perfil es el de contar con una tarjeta de crédito por lo que en este caso no aplican para este tipo de pregunta.

6.14 ¿Considera que el uso de las tarjetas de crédito es muy riesgoso?

Gráfico 15 - Uso de tarjetas es riesgoso.



(Magon & Barros, 2022)

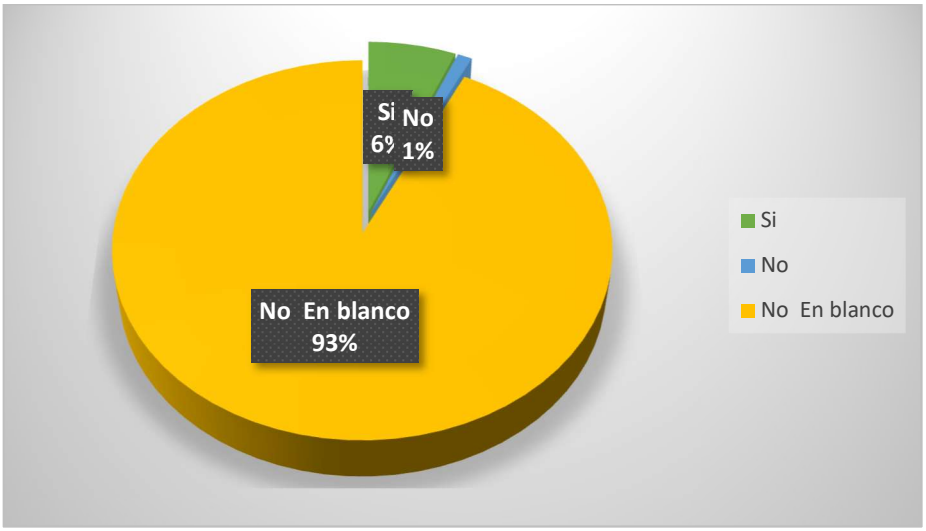
Siempre se ha considerado que una tarjeta de crédito trae consigo diferentes tipos de riesgos, es por ello que se contemplaba conocer la percepción que esta parte de la población encuestada tenía respecto a ello y si es un factor significativo que impedía la adquisición de esta clase de productos.

Se evidencio que de los 192 encuestados que equivalen al 100% del la muestra el 4%, solo 8 persona consideran las tarjetas de crédito un riesgo y por ende no sienten empatía por adquirir un producto de este tipo, así mismo el 3% que equivale a 6 personas no consideran las tarjetas de crédito un riesgo, sencillamente no se inclinan a adquirir un producto de este tipo.

Por otra parte, se identifica que las 178 personas restantes que equivale al 93% son los encuestados cuyo perfil es el de tener al menos una tarjeta de crédito por lo que en este caso no aplican para este tipo de pregunta.

6.15 ¿Cree que los protocolos de seguridad de las tarjetas de crédito no son confiables?

Gráfico 16 - Protocolos de seguridad.



(Magon & Barros, 2022)

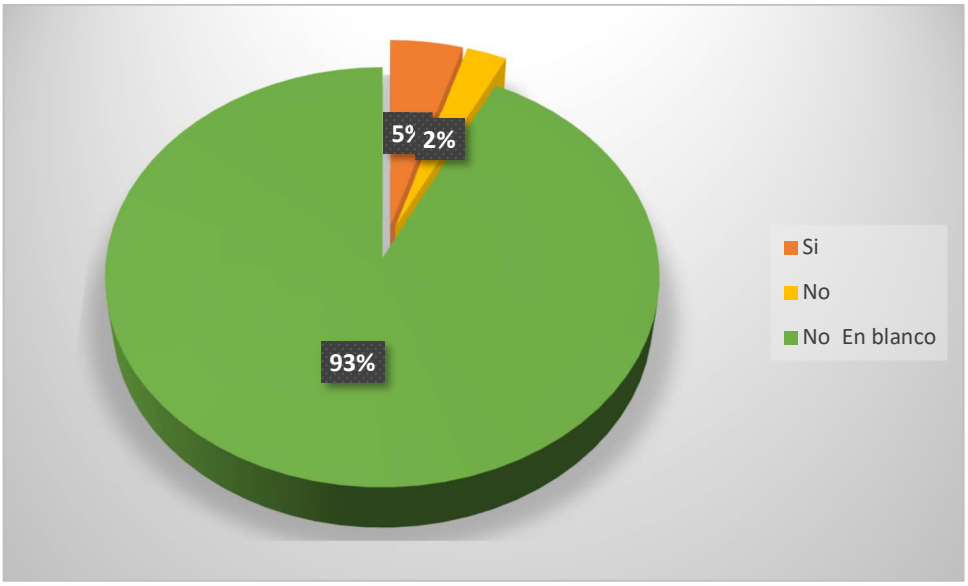
Para muchas personas los protocolos actuales que se implementa para el manejo de transacciones y/o compras con tarjetas de crédito no son lo suficiente para evitar incidentes como lo son los fraudes por medio de estas mismas.

Se comprende que del 100% de la población encuestada la cual indico que no tenía un producto como lo es una tarjeta de crédito 12 personas un 6% indicaron que los protocolos manejados por las entidades financieras no aseguran su confiabilidad para hacer uso de un producto como la tarjeta de crédito; por otra parte 2 personas un 1% de la población encuestada afirma que no consideran que los protocolos de seguridad manejados por entidades financieras sea desconfiable solo no está entre sus percepciones tener un producto como este.

Así mismo, las 178 personas restantes que equivale al 93% son encuestados cuyo perfil es el de tener al menos una tarjeta de crédito por lo que para este análisis no aplica este tipo de pregunta.

6.16 ¿Siente que su información personal esta lo suficiente expuesta como para que ocurras un fraude con este medio de pago?

Gráfico 17 - Información expuesta.



(Magon & Barros, 2022)

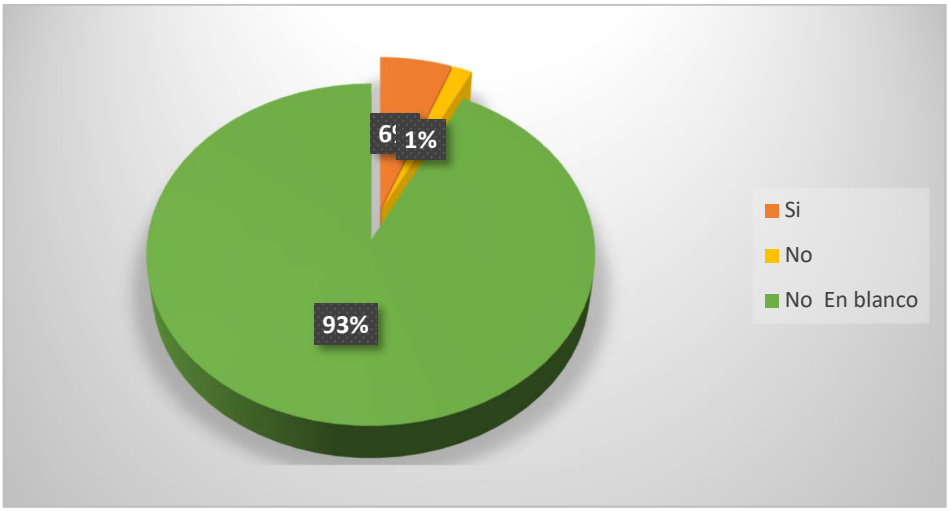
Es importante tener la percepción de aquellos encuestados que indicaron no tener una tarjeta de crédito y su relación con lo que cada página aguarda respecto a su información de carácter personal y lo que esta misma implica para en un futuro ser víctimas de fraude por la exposición que el internet tiene hoy en día.

Analizando que de los 192, el 100% de la muestra; el 5% un total de 9 personas indicaron sentirse inconformes con lo que puede pasar con su información personal dadas las circunstancias que este medio de pago implica y que de laguna manera esto podría ser un factor importante para convertirse en víctimas de fraude; y 2% tan solo 5 personas no contemplan que su información personal y las tarjetas de crédito representen una exposición para ser víctimas de fraude.

Finalmente, las 178 personas restantes que equivale al 93% de los encuestados son aquellos cuyo perfil implica al menos una tarjeta de crédito por lo que para este análisis no aplica este tipo de pregunta.

6.17 ¿Considera que la clonación y/o robo de información de una tarjeta de crédito es bastante fácil?

Gráfico 18 - Clonación de tarjetas.



(Magon & Barros, 2022)

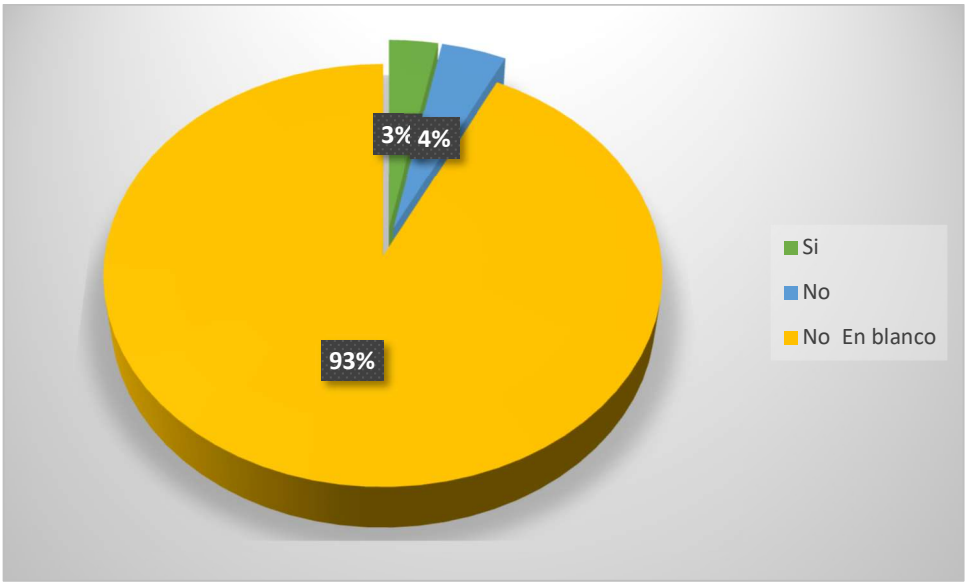
Día a día el uso de medios de pago como las tarjetas de crédito es más recurrente en cierta medida, ya que a nivel global la población a caracterizado este medio de pago como necesario y es que inclusive descuentos y/o promociones se reciben por usar este tipo de productos, sin embargo, el uso continuo de las mismas puede reflejar impaciencia en algunas personas.

Se comprende en el anterior grafico que del 100% de la población encuestada un total de 192 personas, 11 personas un 6% consideran que debito a las circunstancias actuales es muy fácil una clonación y/o robo de información en un producto de este tipo por lo cual se abstienen de adquirir producto como estos, por otra parte un 1% tan solo 3 personas consideran que las tarjetas de crédito tiene medidas suficientes para evitar clonación y/o robo, solo no sienten la necesidad de obtener este producto.

Así mismo, las 178 personas restantes que equivalen al 93% de los encuestados son aquellos cuyo perfil considera por lo menos una tarjeta de crédito por lo que para este análisis no aplica este tipo de pregunta.

6.18 ¿Cree usted que el uso de las tarjeras de crédito en entes (páginas de bancos o almacenes de cadena) conocidos es seguro?

Gráfico 19 - Páginas confiables.



(Magon & Barros, 2022)

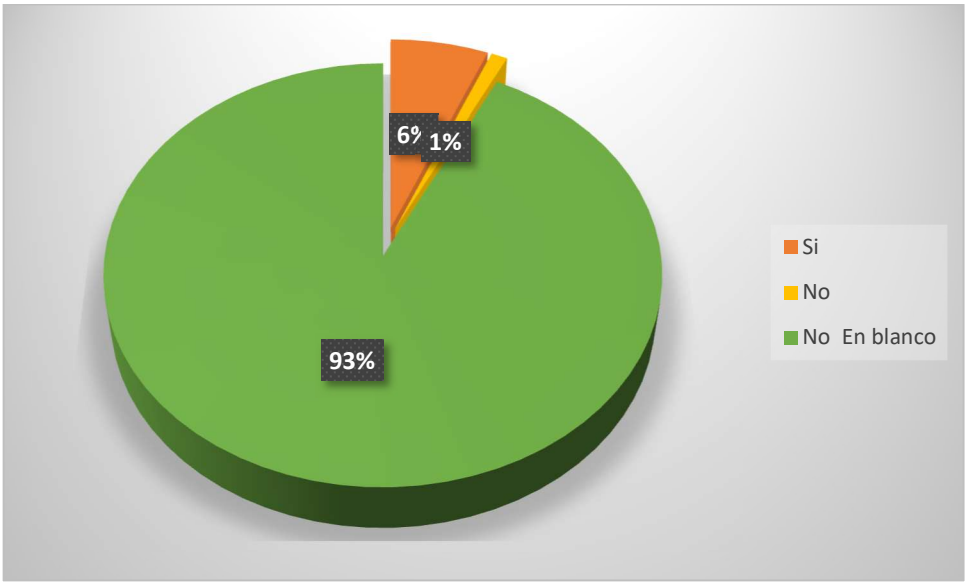
Es importante tener conocimiento de la paginas por la cuales se generan transacciones y más aún si están son usadas de manera regular así que tener conocimiento de lo que los usuarios consideran seguro y no es factor significativo para este análisis o si bien este es uno de los mismos que impiden la adquisición de un producto como este.

En el anterior grafico se identifica de los 192 encuestados que hacen referencia al 100% de la muestra un 3% equivalente a 6 personas consideran que paginas reconocidas o son más seguras que aquellas de las que no se tiene mucho conocimiento; así mismo un 4% que se refiere a 8 personas consideran que este no es un factor de peso para no tener un producto como los son las tarjetas de crédito.

De igual manera las 178 personas restante cuyo porcentaje de la muestra equivale al 93% hacen parte de la población cuyo perfil es al menos contar con un producto financiero como lo es una tarjeta de crédito.

6.19 ¿Considera que los cambios tecnológicos que ocurren día a día podrían cambiar su percepción acerca del uso de una tarjeta de crédito?

Gráfico 20 - Tecnología vs tarjetas.



(Magon & Barros, 2022)

Hoy en día el cambio tecnológico a nivel global crea incertidumbre frente al uso de medios y pagos electrónicos esto crea mayor desconfianza en los consumidores y es que día a día conforme estos avances incrementan los riesgos del uso de los mismos; sin embargo, se identifica que la población que aún no cuenta con un producto financiero como las tarjetas de crédito no refleja tenor en cuanto a los cambios tecnológicos.

El 6% que equivale a 12 de los encuestados que respondieron que no tenían una tarjeta de crédito afirman tener confianza en el futuro y que poco a poco la innovación establecerá niveles de riesgo mínimos, esto contemplando que el dinero digital está tomando cada vez más el mercado.

Si bien se identifica que el 1% tan solo 2 personas consideran que los cambios tecnológicos son un foco aún más fuerte para evitar tener un producto como este; por otra parte, el 93% perteneciente a las 178 personas restantes son encuestados cuyo perfil hace referencia tener como mínimo uh producto financiero como la tarjeta de crédito por lo cual no se toman en cuenta para la opinión respecto a no adquirir una tarjeta de redito.

7 CONSIDERACIONES Y RECOMENDACIONES.

Continuando con el cumplimiento de los objetivos planteados en el presente proyecto de investigación, es importante determinar las delimitaciones que aplica por medio del estatuto del consumidor en cuanto a la ley de retracto con relación a las transacciones en línea realizadas con tarjetas de crédito se refiere. Si bien esta ley se creó con el fin de proteger los derechos del consumidor cuando un producto adquirido vía online por medio de tarjeta de crédito no satisfacía sus expectativas también ha permitido que los usuarios puedan recuperar dineros perdidos por medio de fraudes presentados en las mimas circunstancias.

Se conoce como derecho de retracto aquel que garantiza que el consumidor pueda dar por terminada una transacción y solicitar la devolución del dinero pagado en un contrato de compraventa de forma unilateral (sin necesidad de que el vendedor o la otra parte este de acuerdo) si el producto ya sea un bien o servicio no cumple las expectativas

del cliente, el estatuto del consumidor garantiza este derecho dentro de varias instancias como:

- Ventas o prestaciones de servicios con un método de pago por medio de la financiación.
- Ventas de tiempos compartidos o paquetes turísticos.
- Ventas a distancia las cuales pueden ser vía internet, televisión o telefónicas.

Este último método es el que refiere a la presente investigación, toda vez que permite a una persona que haya sido víctima de fraude por alguno de estos canales electrónicos y teniendo de por medio una tarjeta de crédito podrá solicitar acogerse a la ley de retracto, es importante conocer que para esto debe notar el fraude de forma temprana y así hacer el requerimiento ante la entidad financiera en un tiempo máximo de 5 días hábiles.

7.1 ¿Qué se recomienda hacer si es víctima de fraude?

Es importante que el usuario víctima del fraude reporte el caso ante la entidad de bancaria o financiera que emitió la tarjeta de crédito pues de esta forma dicha entidad podrá a su vez hacer la solicitud al comercio que realiza la transacción con el fin de congelar los fondos de esta y que se pueda dar el reintegro del dinero.

Así mismo se debe recordar que esto no implica una denuncia oficial por tanto y con el fin de que las entidades legales puedan seguir aplicando planes de acción contra estos delitos los usuarios deben generar denuncias por estos casos. Dicha denuncia se realiza directamente ante la Fiscalía General de la Nación por medio de su rama de Delitos Informáticos, es importante que este proceso se realice en la máxima brevedad posible una vez se tenga conocimiento del fraude esto teniendo en cuenta el periodo de tiempo que se tiene disponible para poder hacer la devolución del dinero.

Así mismo es importante que el usuario pueda generar bloqueos preventivos de sus productos financieros dado que pueden ser vulnerables a más ataques o intentos de robo, dependiendo el método de fraude implementando también se recomiendan cambios de claves con el fin de que el delincuente no pueda sustraer más información.

7.2 ¿Cómo influye la educación financiera en los fraudes?

Equivocadamente podemos entender por educación financiera solo lo que al cuidado de nuestras finanzas refiere, es decir, que no se debe hacer uso de las tarjetas de crédito de forma inapropiada con alta frecuencia y a grandes plazos de financiamiento pues esto podría afectar el nivel de flujo de efectivo mensual, también se recomienda que los gastos nunca sobrepasen los ingresos, que se analicen las tasas de interés antes de acceder a un préstamo o producto financiero y otros consejos que se brindan con frecuencia con el objetivo de brindar educación que le permita poder cuidar, mantener y conocer sus finanzas a un individuo.

Tristemente las entidades bancarias o financieras se esfuerzan por cumplir metas de colocación de productos financieros dentro de estos las tarjetas de crédito, pero muchas veces olvidan también brindar información fundamental sobre el cuidado que se debe tener con las mismas.

Cuando se habla de este tipo de educación es importante entender que no solo refiere a que uso debo hacer de la tarjeta con el fin de cuidar las finanzas como se indicó anteriormente, sino que también se debe brindar orientación en cuanto a los cuidados de uso que debe tener el usuario.

Con la llegada de nuevos tiempos y el uso de tecnología de forma más frecuente se puede decir que se han realizado grandes avances en cuanto al acercamiento de las personas, y facilidades en el mundo del marketing, se han ideado nuevas formas de negocios los cuales ahora son 100% digitales pero también se han creado muchas facilidades para el fraude por este medio, si bien se puede decir que hoy en día todos los seres humanos conocemos y hacemos uso de la tecnología, también se debe tener en cuenta que existen personas en su mayoría en un rango de edad superior a los 50 años a quienes se les dificulta más el uso de estas nuevas herramientas y es a ellos a quienes debe ir dirigida principalmente este nuevo modelo de educación financiera la cual se considera una pieza fundamental para promover estabilidad personal y lograr el bienestar monetario en una nación.

Es importante orientar y educar a la población sobre los cuidados que se deben tener al momento de recibir llamadas en donde se informe ser de la entidad bancaria y se solicite información financiera, así mismo educar al cliente sobre como verificar páginas web cuando se van a realizar transacciones en línea y aún más importante teniendo en cuenta que es uno de los métodos más usados, se debe educar a los usuarios sobre los riesgos que conlleva el abrir mensajes (email, mensaje de texto, mensajería instantánea) con links que pueden llegar a contener virus cuyo objetivo es sustraer información financiera que luego será usada con fines delictivos.

Tanto entidades financieras como las personas deben comprender que adquirir nuevos conocimientos y habilidades financieras permitirá hacer mejor uso de los recursos con el fin de proteger la economía de ambas partes.

7.3 Estrategias para evitar el fraude electrónico al usar tarjetas de crédito.

Si bien desde hace varios años el mundo se había visto en una constante evolución en cuanto a tecnología se refiere con la llegada de un evento sin precedente en tiempos modernos como fue la pandemia y a su vez la respectiva cuarentena impuestas por los países muchas actividades diarias que se realizaban de manera presencial comenzaron a pasar del mundo físico al mundo de la digital, actividades básicas y que dábamos por hecho como realizar pagos, ir a estudiar, realizar las compras de la canasta familiar comenzaron a ser delegadas a lo virtual, se comenzó a experimentar planes de estudio virtuales y muchas personas migraron a la era digital para realizar pagos o compras, si bien todo esto se veía como un avance también permitió que se incrementaran los delitos cibernéticos y el robo de datos personales y financieros dado que como se indicó anteriormente muchas personas no contaban y aun al día de hoy no cuenta con la suficiente educación financiera para evitar este tipo de fraudes.

Una vez realizado el proceso de recolección de información por medio de la encuesta aplicada en el presente proyecto se detectaron carencias en cuanto a procesos de cuidado que se debe tener como el hecho de tener autoguardada información como claves, contraseñas y usuarios en los dispositivos móviles los mismos que pueden llegar a ser susceptibles de robo o hackeo de información, es por esto por lo que a continuación se

presentan consejos que buscan evitar ser un blanco fácil en este ámbito. Cabe resaltar que estas estrategias ya existen y lo que se busca con el presente proyecto es generar una divulgación para su mayor entendimiento.

- **Es importante contar con contraseñas seguras tanto en nuestros productos financieros, ingreso a portales web bancarios y correos electrónicos:** se debe evitar tomar como referentes fechas de nacimientos, cumpleaños, aniversarios o números de teléfono para este tipo de claves. Cuanto más compleja sea la contraseña que tengamos más difícil será para un delincuente poder obtenerla y así podremos evitar el robo de datos personales.
- **Siempre cerrar sesión y no autoguardar información:** si bien solemos creer que el celular, computador o dispositivo móvil es de uso propio se debe recordar y tener siempre presente que existen riesgos de robo tanto del dispositivo como de la información que se tiene en el mismo, por esto no se recomienda que las personas tengan autoguardada la información financiera o almacenen archivos para recordar los usuarios y claves de acceso. Una vez más se debe recordar que todos son susceptibles a un hackeo.
- **Nunca brindar datos personales:** lastimosamente hoy en día es normal recibir llamadas o mensajes de texto donde nos informan ser la entidad financiera con la que se tienen productos solicitando confirmaciones de claves, identificación personal e incluso datos de los productos financieros; es importante recordar que los bancos nunca llamaran a solicitar esta información y que al momento de brindarla ya estamos abriendo las puertas al estafador. Así mismo al abrir un enlace recibido por mensajes es posible exponerse a descargar virus o programas silenciosos en los equipos que tienen como finalidad el robo de información.
- **Evitar conectarse a redes públicas:** al momento de realizar transacciones o conexiones a internet fuera del entorno habitual se debe evitar hacer conexiones a redes públicas, si bien estas existen con el fin de garantizar la conectividad a la comunidad son redes que como su nombre lo indica

siempre están abiertas al acceso de todos, por tanto, es posible que otra persona se infiltre en la conexión y así sustraer información.

- **Realizar transacciones en páginas verificadas como seguras**: en este punto es importante que las personas puedan aprender a reconocer y verificar una página para determinar si la misma es segura para realizar transacciones en línea. Algunas pautas que seguir son la verificación del candado verde en la parte superior (al lado de la Url) lo cual significa la verificación de Google, observar si la Url inicia por las siglas HTTPS (Protocolo Seguro de Transferencia de Hipertexto o Hypertext Transport Protocol Secure, en inglés); Confirmar la información legal de la página la cual debe ser visible en la parte superior o inferior de la misma, así mismo se debe contar con información de contacto en caso de presentar algún inconveniente al momento de la transacción.
- **Mantener actualizada la información de contacto ante las entidades bancarias:** este punto permite al usuario obtener alteras de forma inmediata ante cualquier transacción o movimiento en sus productos ya sean realizados por el mismo o no, de esta forma ante cualquier actividad sospechosa podrá tener conocimiento de forma rápida y así mismo actuar y evitar la misma.
- **Instalar antivirus:** se tiene la creencia errada de que los antivirus solo se deben instalar en el equipo pc, sin embargo y dado el uso diario y continuo que se le da a los dispositivos móviles también se recomienda la instalación de estos programas en los celulares pues así al momento de recibir mensajes que lleven a enlaces que posiblemente tienen como finalidad sustraer información que luego podría ser usada de forma delictiva estos programas evitan el ingreso al mismo.

7.4 Tipos de fraude.

Durante la investigación realizada respecto a la percepción que se tiene sobre los fraudes financieros con tarjeta de crédito se identificó que muchos de los encuestado aseguran tener conocimiento de los tipos de fraude que existen y lo que cada uno implica; si bien se evidencio que de los 192 encuestados que equivalen al 100% de la muestra un 68%

representado por 130 personas encuestadas aseguran tener o haber tenido una tarjeta de crédito. Ahora bien, un 27% de esta muestra la cual es representada por 51 personas aseguran haber sido víctimas de fraude y un 32% que equivale a 79 personas quienes indicaron no haber sido víctimas de fraude en ningún momento. Estos resultados están casi en proporción, es inquietante tener la percepción de cuáles son los tipos de fraude usaos por el 27% de la muestra.

Hoy en día existen modalidades de fraude reconocidas no solo por campañas de entidades financieras que han se han visto involucradas por dichos eventos si no por las mismas victimas quienes identifican los medios o canales por los que se han dado los casos. Si bien hace algunos años el miedo de los consumidores adquirientes de este tipo de productos era la clonación de sus tarjetas; con el paso de los años la innovación y digitalización a nivel mundial a obligando a los consumidores a trasladarse consigo a estas novedades puesto que hoy en día es mucho más fácil tanto para entidad financiera responsable como para el consumidor realizar compras, pagos, verificaciones, etc. por páginas que las mismas entidades diseñan a fin de mantener seguros a sus clientes y consigo sus producto.

Es de vital importancia plantearse que si la innovación trae consigo un gran avance los riesgos son mayores pues la misma condición asegura que cuanto mayor es la ganancia mayor será el riego; esto se puede interpretar de la misma manera a mayor agilidad y eficiencia existirá un mayor riego y es que aquellos que diseñan y estructuran la paginas aprenden el arte, pero estos individuos trabajan diferentes campos y así como algunos aseguran estos procesos habrá quienes puedan irrumpir en ellos.

7.4.1 Smishing.

Dentro de los resultados obtenidos se identificó que la modalidad de fraude más usada es el Smishing en esta se ven involucrados los conocidos mensajes de texto o SMS y la nueva modalidad de envió de información vía WhatsApp estas implican mensajes de advertencia o promociones que direccionan al usuario a un link malicioso, este permite el ingreso al dispositivo y a su vez a la información almacenada en correos o cuentas registradas o guardadas en el mismo.

Este método es de los más usados hoy en día, es impactante que aun y con las campañas no solo generales si no de la voz a voz que proviene de las victimas el porcentaje de personas afectadas sea del 35% esto solo para el 100% de la encuesta aplicada la cual equivale a las 192 personas; esta es solo una pequeña muestra de la población a nivel mundial. Cabe deducir que este análisis está enfocado a personas cuyo perfil profesional va enfocado a términos financieros y administrativos deberían ser menos las victimas en estos campos ya que se adquieren conocimientos y experiencias en aspectos que aunque simples relevantes, es insólito detectar que estudiantes en campos como estos caigan en una modalidad de fraude como este teniendo el amplio conocimiento de lo que rodea la seguridad no solo de una compañía sino de sus finanzas, algo tan elemental como un mensaje de texto debe ser signo de sospecha, porque caer en ella si se tiene el conocimiento de cómo detectar una especie de fraude bajo este medio.

7.4.2 Phishing.

Por otra parte el Phishing dentro de los resultados tuvo un enorme impacto pues es acreedor del 29% de la población encuestada esta modalidad está basada en el fraude por medio de los correos electrónicos, esta modalidad impacienta en gran medida y es que los correos electrónicos han sido otro de los canales digitales más evolutivos de los últimos tiempos además se ha convertido en un tema complejo pero de mucho impacto, en la actualidad muchos de los tramites que deben realizarse en la cotidianidad incluyen un correo electrónico a fin de agilizar procesos de claves y contraseñas; bajo estos conceptos debería creerse que estas direcciones de correo electrónico deben ser seguras.

Lo cierto es que cualquier tipo de cambio de contraseña o accesos a un portal aplicativo de entidades financieras requiere una validación o por mensaje de texto o por un correo electrónico donde indican una contraseña o pin para el debido acceso a portales web e inclusive al cambio de contraseñas del mismo, aquí es donde se visualiza que la percepción de los involucrados respecto a determinar si un correo es malicioso o no, es subjetivo ya que un correo electrónico se identifica como no seguro cuando este llega a la bandeja de SPAM.

Sin embargo, cabe determinar que un programador puede activar un correo de carácter malicioso inclusive con una campaña publicitaria de una entidad financiera

pidiendo que simplemente conteste una encuesta que a simple vista es normal el correo es dirigido por la entidad financiera y su dominio en general procede confianza, pero esto puede estar alterado por punto (.) un (-) e inclusive una slash (/) nos símbolos de carácter muy normal en correos electrónicos pero uno solo de estos puede ser la diferencia en el correo. Puede estar programado para direccionar al cliente a la encuesta y a su vez proporcionar el ingreso o descargue de información almacenada en el dispositivo o correo.

Incluso puede estar generando y guardando una copia del correo electrónico, así como también puede crear una cuenta espejo de este, de esta forma el fraude podría generarse de cualquier forma sin que el consumidor se dé cuenta. El usuario puede tener almacena en su correo información muy puntual e inclusive el ingreso a portales de acceso a sus productos financieros.

La evasión de correo es una forma segura de caer en este tipo de fraude por otra parte es importante siempre comunicarse con la entidad financiera y dar lugar a que el correo visualizado en la bandeja de entrada corresponda al emitido por el ente involucrado.

7.4.3 Vishing

Para esta modalidad se evidencio un porcentaje menor comparado con las demás modalidades, sin embrago aun el 16% impacta, posiblemente esto deba que la población sienta la confianza de que se puede realizar un proceso por este medio; ahora bien, se puede determinar que la población propensa a este tipo de fraudes son los adultos mayores quienes no tiene experiencia en aspectos tecnológicos, es por ello que una llamada que indique una actualización de datos o una alerta frente a una posible suplantación puede ser de vital atención para ellos.

Sin embargo, estas medidas indican que también puede ser filtración de información, este proceso hace más fácil la filtración de información pues los encargados de llevar a cabo el robo de información tienen equipos que inclusive si aún se digita la clave a fin de no proporcionarla a voz detectan los números marcados al otro lado del teléfono. Estas personas se encuentran capacitadas para crear la confianza que el usuario necesita para realizar el proceso usan conceptos propios de las entidades financieras a fin de generar confianza y finalmente crear el vínculo que permita la obtención da información.

Si bien con esta información ellos mismos gestionan claves e ingresos a portales web y de esta forma generan una suplantación de la víctima, obteniendo así productos para interés de ellos o haciendo uso de los ya habientes para compras o transacciones que permiten el saqueo de los usuarios originales. En la mayoría de estos casos las víctimas no posen conocimiento de lo sucedido sino hasta que realizan comunicación con los mismo, llevándose la sorpresa de interés por mora y productos que jamás en su vida han manipulado.

Para casos como estos es importante tener presente que las entidades financieras jamás solicitan claves o números de tarjetas puesto que ellos ya adquieren esta información tampoco solicitan información como su cedula solo una confirmación de la misma pues de igual forma ya se posee esta información, este tipo de llamadas son solo para actualizar datos como direcciones o teléfonos. Aun así, hoy en día las entidades ya no realizan estos procesos pues la seguridad de sus clientes es de suma importancia, cuando se tiene un producto con una entidad financiera siempre existe un contacto y es que en validación de compras o transacciones solicitan este tipo de información por lo que la entidad siempre estar actualizada frente a estos datos.

Para esta investigación se tomaron en cuenta las modalidades de fraude más comunes, sus rutas o canales y sus impactos con el consumidor de productos como las tarjetas de crédito sin embargo, existen otras modalidades de fraude que en su defectos son parecidas más non iguales a las ya conocidas y es que este es un campo que conforme se da el avance tecnológico surgen a su paso más modalidades de fraude, es por esto que dentro de la percepción de los estudiantes se quería realizar un análisis de si los encuestados tenían en conocimiento otras modalidades, se determina que el 20% de los encuestados asociaron el tipo de fraude del que fueron víctimas a otras modalidades no especificas o compartidas en la encuesta, es por ellos que se generara información respecto a las otras posibles caudas de fraude.

7.4.4 Otras modalidades de fraude.

El 20% de loa población encuestada aseguro ser víctima de fraude pero el análisis se concentró en que otros tipos de fraude existen y más aún que ocurren con frecuencia; esto debido a que pese a que se relacionaron las modalidades más conocidas y de las que la

mayoría de la población ha sido víctima los resultados de la encuesta aplicada arrogaron que una parte de esa población considerada indica haber sido víctima pero de otra modalidad que aunque identificada no es reconocida por los consumidores, es por ellos que se realizara un análisis con base en otros autores de cuales podrían ser los otros tipos de fraude de los que fueron víctimas los encuestados.

7.4.4.1 Malware.

Esta modalidad es muy peculiar según (Rivera, 2018) el malware es un sistema implementado atacar un sistema software dándole el privilegio de acceder al sistema o red en general este irrumpe en la operación cotidiana del servidor o dispositivo, obteniendo de esta manera información no solo de cuentas sino en sí a la base del servidor, en estos ataques pueden verse involucrados diferentes tipos de malware tales como: virus, gusanos, troyanos, rootkits, backdoors, botnets o spywares.

Ahora bien, esta modalidad puede perjudicar en muchos aspectos al usuario, pero para dar relación al tema este tipo de filtración también da acceso a lo que el servidor tenga guardado y esto involucra consultas e ingresos a diferentes portales web, e inclusive si el acceso al correo electrónico está vinculado al dispositivo el fraude puede llevarse a cabo por ese mismo medio y el usuario notaria esta actividad una vez ingrese a sus portales.

Otra particularidad esta modalidad es que puede este malware puede venir incorporado mediante un correo electrónico, un mensaje de texto o inclusive un mensaje vía WhatsApp por lo que tiene relación con el Smishing, phishing y Vishing.

7.4.4.2 Fraude de negociación o alivio.

Hoy en día las compañías otorgan un tipo de negociación de deudas afirman renegociar, resolver, o de alguna manera, cambiar condiciones de deuda que una persona pueda y aunque se pueda ver como un alivio cuando el usuario se encuentra en el peor momento económico no resulta en nada beneficiario el acuerdo que podría llegar a realizarse.

Ahora bien, esta modalidad de fraude es compleja ya que podría tomarse como fraude, pero a su vez el alivio se vería reflejado de tal manera, esta modalidad es

cuestionable de acuerdo con cada caso y es que muchos de los alivios otorgados por entidades financieras son simplemente eso un alivio mas no una condonación de lo que podría ser capital pues la situación financiera del usuario no determina en nada a la entidad financiera. Para estas entidades el continuo flujo de dinero es ganancia el generar un alivio mientras el usuario sale de aprietos económicos no puede implicar perdida frente al producto obtenido por el cliente.

Según un artículo de (AARP, 2022) esta modalidad de fraude se presentaría según el caso pues existen quienes en verdad afirman renegociar deudas, pero finalmente el usuario o adquirente termina pagando 3 veces más de los había pactado en inicio esto por compras de cartera o refinanciaciones con condiciones exorbitantes.

7.4.4.3 Robocalls de reducción de tasas de interés

Esta modalidad, aunque similar al Vishing involucra una grabación automatizada que afirma generar una reducción de tasa de interés en su tarjeta de crédito y a cambio solicita información para ejecutar dicho proceso.

"Este tipo de estafa, que es similar al fraude con tarjetas de crédito, es relativamente más reciente. Toma la forma de llamadas automáticas, o robollamadas, que afirman garantizar una reducción en la tasa de interés de su tarjeta de crédito por una pequeña tarifa. Este tipo de estafadores a veces también terminan cometiendo robo de identidad después de solicitar información personal. Si recibe una llamada no solicitada de una fuente desconocida o se ve obligado a pagar una tarifa o divulgar datos personales antes de realizar cualquier otra acción, es probable que se trate de una tarjeta de crédito. llamada automática de reducción de tasa de interés." (Adams, 2020).

8 CONCLUSIONES.

Para la presente investigación se plantearon diferentes objetivos que permitieran analizar la percepción que los estudiantes de ciencias empresariales de la corporación minuto de Dios Cundinamarca tenían frente a los fraudes financieros con tarjeta de crédito esto a fin de dar recomendación de las estrategias que podrían ayudar a mitigar en gran medida este tipo de riesgo.

Para ello fue de vital importancia realizar un análisis a los diferentes tipos de fraude y lo que cada uno infiere respecto a su modalidad de ataque.

Para dicho análisis se planteó una encuesta que permitió recopilar información de las diferentes modalidades de ataque frente a las tarjetas de crédito, según los resultados obtenidos en la aplicación de la encuesta se puede concluir que la modalidad de ataque más implementada es el Smishing esta modalidad consiste en el envío de mensajes de texto o vía WhatsApp, estos mensajes tiene como característica un mensaje corto y en su contenido puede indicar al usuario un movimiento inusual, un bloqueo e inclusive una actualización de datos; adjunto al mensaje direcciona al usuario a solucionar el problema mediante un link este en muchos aspecto puede contener un malware o sencillamente dar el acceso que el atacante requiere para filtrar información u obtener acceso al dispositivo y así a toda su información.

Otro resulta resultado que llamó bastante la atención es donde los estudiantes afirman haber sido víctimas de fraude bajo otras modalidades por lo cual, se realizó una investigación final que permitiera identificar que otras modalidades de fraude se presentan hoy en día esto debido a los cambios tecnológicos acelerados a los que se enfrenta la población. Dentro de este análisis fue impactante reconocer que la negociación de alivios financieros en considerada por los consumidores como un fraude y es que las refinanciaciones que otorgan las entidades financieras con los tarje-habientes son símbolo de engaño ya qué es de esperarse que la entidad no tiene por qué perder y sacan provecho de los usuarios que se ven apretados con sus obligaciones financieras. Aquí se concluyó que los tarje-habientes terminan pagando más interés, así como extendiendo el plazo pactado en un inicio. De cualquier forma, el usuario se ve afectado en un furo no lejano.

Otra de las modalidades que causó intriga son las Robocalls esta consiste en una llamada grabada y además en su mayoría deben ser utilizadas bajo autorización previa de entidades de comunicación. Sin embargo, se evidencia que pese a estas autorizaciones y regulación está modalidad tiene un gran impacto puesto que la grabación o en su defecto el robot solicita información para efectuar cambios en los productos de usuario y está queda guardada en una base interna, dando así facilidad para acceder a información que permita llevar a cabo el fraude.

Finalmente, se determinó que tener contacto frecuente con los movimientos efectuados por los productos financieros obtenidos ayuda de tal modo con la identificación temprana de fraude, las notificaciones de los movimientos realizados permiten la verificación del mismo, si el usuario es consciente de que no realizo ese movimiento, en seguida se pone alerta y realiza las validaciones pertinentes para confirmar la transacción notificada y está en efecto fue ejecutada, el usuario puede acogerse a la ley de retracto .

Esta ley acoge al usuario permitiéndole retractarse es un producto que incumple con sus expectativas. Si bien puede generarse el reintegro de la transacción. Por otra parte, estas notificaciones ayudan al usuario alertar también a la entidad financiera para que proceda a tiempo y pueda declinar la transacción efectuada.

Así mismo la educación financiera es carácter importante en la mayoría de los casos las entidades financieras solo se preocupan por cumplimiento y mayor segmentación, olvidando así los consumidores y es que el hecho de que se obtenga un producto como las tarjetas de crédito implica una responsabilidad. El consumismo a llevado a la población a extremos sin tomar medidas frente al uso de este tipo de productos, hoy en día la volatilidad de las tasas de interés, cambios en las monedas extranjeras, inflación y demás afectan bruscamente estos medios de pago pues la mayoría de estos productos dependen de estos cambios y los movimientos realizados durante diferentes periodos, es por ello que los usuarios deben tener previo conociendo que le permita usar este tipo de productos en momentos oportunos.

9 BIBLIOGRAFÍA.

AARP. (30 de Marzo de 2022). *Estafas relacionadas con la reducción de deudas*. Obtenido de https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/reduccion-de-deudas.html

Adams, L. d. (05 de Noviembre de 2020). *Tipos Comunes De Fraude Al Consumidor*. Obtenido de https://parnalladams.com/es/tipos-comunes-de-fraude-al-consumidor/

Agudelo, V. D., Gallego, M. C., Gómez, L. T., & González, C. C. (21 de Noviembre de 2020). *Componentes que influyen en la ejecución de fraudes financieros: percepción de los profesionales contables.* Obtenido de file:///C:/Users/user/OneDrive/Escritorio/3610-Texto%20del%20art%C3%ADculo-17382-2-10-20220718.pdf

Alvarez, S. J., & Mejia, Z. S. (Noviembre de 2021). *FRAUDE ELECTRÓNICO Y CAMPAÑAS DE MITIGACIÓN: ¿EVOLUCIONAN*. Obtenido de file:///C:/Users/user/OneDrive/Escritorio/Trabajo%20de%20grado/22.Trabajo%20final-Alvarez%20y%20Mejii%CC%80a.pdf

Bernal, C. A. (2010). *Metodologia de la investigacion.* Bogotá: Pearson Educacion de Colombia LTDA. Obtenido de ". https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Bodnar, D. (29 de Octubre de 2020). *Avast Academy*. Obtenido de https://www.avast.com/es-es/c-social-engineering

Citibanamex. (26 de Noviembre de 2020). *¿Cómo saber si un sitio es seguro para comprar?* Obtenido de https://www.banamex.com/sitios/capital-y-estilo-citibanamex/entretenimiento/como-saber-si-un-sitio-es-seguro-para-comprar.html

comercio, S. d. (25 de Octubre de 2020). *¿Sabe usted qué es el derecho al retracto?* Obtenido de https://www.sic.gov.co/noticias/sabe-usted-que-es-el-derecho-al-retracto

Comercio, S. d. (06 de Octubre de 2021). *¿Se arrepintió de una compra y no sabe qué hacer?* Obtenido de https://www.sic.gov.co/noticias/%C2%BFse-arrepinti%C3%B3-de-una-compra-y-no-sabe-qu%C3%A9-hacer

Cumpa, Y. C. (2021). *Las actuales modalidades delictivas de los cibercrímenes en el delito de fraude informático.* Obtenido de file:///C:/Users/user/OneDrive/Escritorio/Fraude%20informatico..pdf

El Colombiano. (04 de abril de 2022). *No se salvó: excodirectora del Banco de la República, víctima de "cambiazo" de su tarjeta de crédito*. Obtenido de https://www.elcolombiano.com/colombia/carolina-soto-excodirectora-del-banco-de-la-republica-victima-de-cambiazo-de-su-tarjeta-de-credito-OB17166109

El portafolio. (19 de 03 de 2022). *Las 14 billeteras digitales con mayor crecimiento entre 2020 y 2021*. Obtenido de https://www.portafolio.co/mis-finanzas/las-billeteras-digitales-con-mayor-crecimiento-entre-2020-y-2021-563108

Jimenez, J. (16 de Diciembre de 2021). *RZ Redes Zone,¿Quiénes caen más en la trampa del Phishing? Este estudio lo muestra.* Obtenido de https://www.redeszone.net/noticias/seguridad/victimas-comunes-phishing/

Juridico, L. A. (27 de Julio de 2021). *La SIC recuerda cómo opera el derecho de retracto*. Obtenido de https://www.ambitojuridico.com/noticias/mercantil/la-sic-recuerda-como-opera-el-derecho-de-retracto

La republica. (17 de febrero de 2022). *Ventas de comercio electrónico en Colombia crecieron 40% y llegaron a $40 billones*. Obtenido de https://www.larepublica.co/empresas/las-ventas-de-ecommerce-en-colombia-crecieron-40-y-llegaron-a-40-billones-3305200

Magon, B. M., & Barros, T. K. (17 de Noviembre de 2022). Elaboracion propia. *Graficos e imagenes*. Bogota D.C., Colombia.

Morillas, A. (2007). *Muestreo en poblaciones finitas. Obtenido de Muestreo en Poblaciones Finitas, 20017.* Bogota D.C.

Navarro, D. B. (19 de Septiembre de 2021). *Fraude en el sector asegurador por medios electrónico* . Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/40328/RuizNavarroDerlyBibiana2021.pdf?sequence=1&isAllowed=y

NUÑEZ, P. M. (2021). *IMPACTO DE LOS ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA DESDE*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/42675/pmrinconn..pdf?sequence=3&isAllowed=y

Portafolio. (15 de 09 de 2020). *Delitos informáticos, la otra pandemia en tiempos del coronavirus*. Obtenido de https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

Portafolio. (03 de Agosto de 2021). *Conozca los fraudes financieros más comunes para que no caiga en ellos.* Obtenido de https://www.portafolio.co/economia/finanzas/fraudes-financieros-mas-comunes-sepa-como-son-identifiquelos-y-evitelos-554720

Quijano, M. A. (2021). *"LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020"*. Obtenido de https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

Reig, P. G. (2021). *Ataques y vulnerabilidades web*. Obtenido de https://riunet.upv.es/bitstream/handle/10251/172833/Grau%20-%20Ataques%20y%20vulnerabilidades%20web.pdf?sequence=1&isAllowed=y

Rendón-Macías, M. E.-K.-N. (2016). Estadística descriptiva. *Revista Alergia México*, 63(4), 397-407.

Rivera, G. R. (Septiembre de 2018). *Deteccion y Clasificaci ´ on de Malware con el Sistema de Analisis de Malware Cuckoo*. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/7444/RIVERA%20GUEVARA%2cRICHARD%20PAUL.pdf?sequence=1&isAllowed=y

Santander. (20 de Junio de 2022). *"Vishing": una llamada con mucha trampa*. Obtenido de https://www.santander.com/es/stories/vishing-una-llamada-con-mucha-trampa

Sn. (24 de Octubre de 2016). *Banco BBVA*. Obtenido de https://www.bbva.com/es/salud-financiera/historia-de-las-tarjetas-de-credito/

Sn. (24 de Junio de 2021). *Datacredito Expirian.* Obtenido de https://www.datacreditoempresas.com.co/blog-datacredito-empresas/tipos-de-fraudes-con-tarjetas-de-credito-mas-comunes-en-cajeros-automaticos/

Sn. (08 de Febrero de 2022). *Revista Semana.* Obtenido de Economía: https://www.semana.com/finanzas/credito/articulo/cuanto-usaron-los-colombianos-las-tarjetas-de-credito-en-2021/202202/

Tarriño, A. (06 de Julio de 2022). *BBVA,'Smishing': Cómo protegerse de los nuevos ataques por SMS*.

Vargas, L. (30 de Julio de 2021). *La República*. Obtenido de https://www.larepublica.co/finanzas/el-numero-de-tarjetas-de-credito-cae-7-y-el-de-debito-aumenta-9-en-un-ano-de-pandemia-3209056