FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

DESARROLLO DE ESTRATEGIA PROACTIVA CONTRA EL FRAUDE CON DE TARJETAS CRÉDITO EN LAS PRINCIPALES INSTITUCIONES BANCARIAS EN HONDURAS

SUSTENTADO POR:

CLINTON MACAULAY JEREZ VILLAMIL
JEYSIE ELIANY SOTO REYES

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
DIRECCIÓN EMPRESARIAL

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

OCTUBRE, 2022

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA
UNITEC

FACULTAD DE POSTGRADO
AUTORIDADES UNIVERSITARIAS

RECTORA
ROSALPINA RODRÍGUEZ

SECRETARIO GENERAL / PRORRECTOR
ROGER MARTÍNEZ MIRALDA

VICERRECTOR ACADÉMICO NACIONAL
JAVIER ABRAHAM SALGADO LEZAMA

DIRECTORA NACIONAL DE POSTGRADO
ANA DEL CARMEN RETALLY VARGAS

DESARROLLO DE ESTRATEGIA PROACTIVA CONTRA EL FRAUDE CON TARJETAS CRÉDITO EN LAS PRINCIPALES INSTITUCIONES BANCARIAS EN HONDURAS

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN DIRECCIÓN EMPRESARIAL

ASESOR METODOLÓGICO

ESTHER MARÍA CLAROS BERLIOZ

ASESOR TEMÁTICO

ANTHONY STEVE BARAHONA ESPINOZA

MIEMBROS DE LA TERNA:

WALTER LOPEZ
JORGE CENTENO
RENE SANTOS

FACULTAD DE POSTGRADO

Desarrollo de Estrategia Proactiva Contra el Fraude con Tarjetas Crédito en las Principales Instituciones Bancarias En Honduras

Clinton Macaulay Jerez Villamil
Jeysie Eliany Soto Reyes

Resumen

El presente trabajo de investigación consiste en la elaboración de una estrategia proactiva contra los casos de fraude en las tarjetas de crédito para ser implementado en las tres principales instituciones bancarias colocadoras de tarjetas en Honduras. El objetivo se orienta en la propuesta de un plan con nuevas iniciativas que permita educar correctamente a los clientes específicamente contra los métodos empleados por los delincuentes para hurtar y robar la información de las personas poseedores de tarjetas. El trabajo se realizó mediante los lineamientos metodológicos, utilizando un alcance de estudio explicativo, de carácter mixto, empleando como muestra a expertos en temas de fraude electrónico en el rubro de las instituciones bancarias en Honduras y tarjetahabientes víctimas de un atentado o fraude con tarjetas de crédito en Tegucigalpa, a quienes se le aplicó una entrevista estructurada y se les solicitó compartir su testimonio de una manera no estructurada, respectivamente, como instrumentos de recolección de datos. Según los hallazgos, más de la mitad de los usuarios de tarjetas habían sido víctima o conocen de alguien que ha sido víctima de fraude. Asimismo, se presenta la propuesta de una estrategia proactiva contra el fraude hacia los tarjetahabientes con el fin de que los tres principales bancos colocadores de tarjetas puedan utilizar eficientemente sus recursos y así mitigar el riesgo del fraude.

Palabras claves: Fraude, Tarjetas de Crédito, Banco Comercial

GRADUATE SCHOOL

Preventive Strategy Development Against Fraud with Credit/Debit Cards in Honduras.

Clinton Macaulay Jerez Villamil
Jeysie Eliany Soto Reyes

Abstract

This research work consists of the elaboration of a proactive strategy against cases of credit card fraud to be implemented in the three main banking institutions that issue cards in Honduras. The goal is to create a plan with new initiatives that allow customers to be properly educated against the methods used by criminals to steal information from cardholders. This research was conducted using an explanatory scope of study, of a mixed nature, having experts in credit card fraud in Honduras and cardholders who were victims of fraud with credit cards in Tegucigalpa as samples. To collect data a structured interview was applied to the experts, and the cardholders were asked to share their testimony in an unstructured manner. According to the results, more than half of card users have been victims or know someone who has been a victim of fraud. Likewise, a proposal is presented for a proactive strategy against fraud towards cardholders so that the three main card placing banks can efficiently use their resources and thus reduce the risk of fraud.

Key words: Fraud, Credit card, Commercial Bank.

DEDICATORIA

Primeramente, le agradezco a Dios por darme la oportunidad y sabiduría necesaria para cumplir un nuevo logro, del cual me siento muy orgullosa y bendecida por estar culminándolo. A mis papás, Adrian Soto y Maira Reyes por el apoyo incondicional en cada etapa de mi vida y en todo lo que hago, ellos son mi inspiración y junto con mi hermano, Diego Soto, mi motivación para continuar superando los retos que me propongo.

Jeysie Eliany Soto Reyes

El presente trabajo es dedicado principalmente a Dios, quien me ha dado la oportunidad de ampliar mis conocimientos y me ha bendecido para poder hacerlo. A mi familia y a mi prometida, quienes han sido el apoyo incondicional y la motivación en los momentos donde más necesite de ellos para poder lograr la meta.

Clinton Macaulay Jerez Villamil

AGRADECIMIENTO

A nuestras familias, por su habernos apoyado incondicionalmente y motivado hasta la recta final de esta maestría.

A mi amigo y compañero de Proyecto, Clinton Jerez, por su alto nivel de compromiso y dedicación con el Proyecto, y su compañerismo, liderazgo y apoyo a lo largo de toda la maestría.

A nuestra asesora metodológica, la Dra. Esther Claros quien nos orientó y motivó hasta el último día de este Proyecto y a nuestro asesor temático, el Ing. Anthony Barahona quien no dudó en ayudarnos y compartirnos de su experiencia profesional.

A todos nuestros amigos, compañeros de maestría, de trabajo y toda persona que aportó un granito de arena para enriquecer nuestro conocimiento y principalmente, fortalecer nuestro proyecto final.

Jeysie Eliany Soto Reyes

A UNITEC y a los catedráticos de la maestría de Gestión Empresarial por habernos compartido las herramientas y conocimientos necesarios para realizar este proyecto.

A mi compañera de Proyecto y amiga, Jeysie Soto, por su perseverancia, tenacidad, resiliencia, determinación y compañerismo mostrado durante la realización de este proyecto y toda la carrera de maestría.

A nuestros asesores Dra. Esther Claros e Ing. Anthony Barahona, quienes con su orientación y apoyo se logró completar este proyecto.

A nuestros compañeros de carrera con quienes compartimos muchas experiencias juntos a lo largo de la maestría.

Clinton Macaulay Jerez Villamil

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

El año 2022 se encuentra en una época tecnológica donde los cambios suceden a un ritmo sin precedentes. Hasta la manera de realizar las compras de víveres es distinta a lo que era hace 10 años. Por ello, las empresas de todos los rubros se ven obligadas a adoptar nuevos métodos, equipos y estrategias para la fabricación de sus productos y la realización de sus servicios. Las instituciones bancarias no están exentas de los cambios tecnológicos y por ende deben acoplarse a las nuevas necesidades que se han creado en esta era. Esto conlleva nuevos riesgos en el entorno externo de los cuales las empresas deben anticipar para no comprometer la información de sus clientes e incrementar la confianza y seguridad percibida de ellos.

El presente trabajo, de enfoque mixto, pretende proponer una estrategia proactiva con el fin de mitigar los riesgos a los que están expuestos los tarjetahabientes que realizan sus pagos por canales digitales. Esta estrategia surge a partir del análisis de las actuales tácticas de fraudes que se utilizan para conseguir la información de los tarjetahabientes de las instituciones bancarias en Honduras.

Se utilizó una metodología investigativa para recopilar la información que sustente la problemática que se ha planteado, como también la solución que se ha propuesto.

Se utilizaron la entrevista, testimonio y la observación como herramientas de investigación que permite la recopilación directa de información de eventos sucedidos a los usuarios de tarjeta de crédito de Tegucigalpa, Honduras. Estos eventos fueron analizados para identificar los

escenarios donde se pueden encontrar expuestos a filtrar su información personal y/o a estafas y las medidas que toman las instituciones bancarias para preparar a sus clientes.

Las transacciones electrónicas en Honduras han incrementado considerablemente a partir de las restricciones que desencadenó la pandemia del COVID-19 para hacer compras en físico, y debido a los cambios que ha incurridos los bancos, muchos nuevos y establecidos tarjetahabientes desconocen tanto los beneficios como los riesgos que implican estos productos.

1.2. ANTECEDENTES DEL PROBLEMA

En los últimos años, la adquirencia (es decir, los POS donde los comercios procesan los pagos con las tarjetas de crédito de sus clientes) han venido a revolucionar la forma en que las personas realizan sus transacciones comerciales, por la rapidez y sencillez con que se efectúa el cobro; esto debido en parte a la globalización mundial que día a día se lleva a cabo con mayor ímpetu. Por tal motivo, la mayoría de las instituciones bancarias a nivel mundial se enfocan en brindar los productos y servicios más innovadores y seguros a sus clientes. Uno de los productos en que las instituciones bancarias invierten recursos para atraer mantener y atraer nuevos clientes diariamente, son las tarjetas de crédito.

La tarjeta de crédito es un instrumento que permite adquirir bienes, servicios y efectuar retiros de dinero en el momento que el titular lo desee, hasta el margen o límite de crédito pre acordado con la empresa emisora de la tarjeta. El emisor de tarjetas de crédito facilita un plástico con el nombre de la persona que ha contratado una línea de crédito con un límite de compra y un límite de crédito En la actualidad existen 11 bancos emisores de tarjetas de crédito en territorio hondureño, con un portafolio variado y dirigido a distintos segmentos. Entre esas instituciones, se encuentran Banco Atlántida, BAC, Ficohsa, Banpaís, entre otros. (CNBS, s.f.).

Como cualquier entidad a nivel nacional e internacional, la crisis global del COVID-19 impactó significativamente la operatividad diaria de estas instituciones. Esto impulsó los pasos agigantados que tuvieron para digitalizar muchas de las gestiones que los clientes realizaban de forma presencial. Debido a que en Honduras se establecieron medidas estrictas de circulación, la población tuvo que familiarizarse con las compras en líneas utilizando de sus tarjetas de crédito para satisfacer sus necesidades del día a día a través de todos los ámbitos de su vida.

Así como las compras en líneas vinieron a facilitarle la vida a la población, de igual forma, aumentaron el riesgo de los fraudes a través de canales digitales. Por este motivo, las instituciones bancarias han tenido que estar extremadamente alertas a las nuevas modalidades de fraudes a los que están expuestos sus clientes y sus empresas, y velar por salvaguardar toda la información de éstos.

Informados por este escenario y con el objetivo que las instituciones bancarias brinden mayor seguridad y confianza a sus tarjetahabientes al momento de realizar compras en línea, se identificó la necesidad de crear nuevas estrategias para mitigar el riesgo del fraude electrónico al que están expuestos los usuarios.

1.3. DEFINICIÓN DEL PROBLEMA

El siguiente espacio detalla el problema encontrado y porque se establece la investigación en las instituciones bancarias emisoras de tarjetas del país:

1.3.1. ENUNCIADO DEL PROBLEMA

A medida que el uso de la tecnología se ha vuelto una herramienta que permite agilizar cualquier proceso de compra y venta de productos y servicios, las tarjetas de crédito se han

convertido en uno de los principales medios de pagos utilizados en dichas transacciones digitales por las distintas facilidades que ofrecen. Una tarjeta de crédito permite al usuario disponer de dinero en tiempo real siempre y cuando haya disponibilidad de fondos en la misma, y así realizar una compra, ya sea de forma presencial o virtual desde cualquier plataforma digital. Sin embargo, se debe tener presente que una tarjeta de crédito no es una extensión del ingreso mensual de la persona o de su salario (CNBS, s.f.).

El COVID-19 ha marcado un antes y un después en el mundo y se ha encargado de resaltar más que nunca la dependencia de las plataformas digitales y el comercio electrónico. Según la CNBS (2020), en un lapso de tres meses, se experimentó una aceleración de la transformación digital que se había anticipado que ocurriría en tres años.

1.3.2. FORMULACIÓN DEL PROBLEMA

El papel que ha jugado la transformación digital en el transcurso de la pandemia del COVID-19, ha sido fundamental para el crecimiento del sistema financiero, muchas instituciones ya contaban con sus plataformas digitales, a fin de ofrecer a sus clientes productos y servicios cada vez más tecnológicos, brindándoles la capacidad de manejar sus finanzas de una manera inmediata y sencilla desde cualquier lugar (CNBS, 2021). Sin embargo, la facilidad del uso de plataformas digitales trae consigo mismo la gran exposición a fraudes electrónicos, motivo por el cual se plantea la siguiente pregunta:

¿Qué estrategias de mitigación de riesgo del fraude digital, que existen actualmente, podrían las instituciones bancarias modificar e implementar aprovechando los recursos y herramientas con las que ya cuentan para brindar mayor seguridad y confianza a los tarjetahabientes?

1.3.2.1. PREGUNTAS DE INVESTIGACIÓN

- ¿Cuáles son los principales riesgos de fraude al que están expuestos los tarjetahabientes al momento de realizar compras en línea?

- ¿Cuáles son las medidas de seguridad que existen actualmente y pueden brindar mayor efectividad y confianza a las instituciones bancarias al momento de monitorear y resguardar las transacciones de sus tarjetahabientes?

- ¿Qué estrategias pueden implementar y modificar las instituciones bancarias para contrarrestar de forma proactiva los fraudes que se presentan en los canales digitales?

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. OBJETIVO GENERAL

Desarrollar una estrategia proactiva que ayude a mitigar los fraudes y estafas en los tarjetahabientes de las principales instituciones bancarias colocadoras de tarjetas de crédito en Honduras que fomente el comercio electrónico.

1.4.2. OBJETIVOS ESPECÍFICOS

1. Conocer los principales riesgos de fraude a los que están expuestos los tarjetahabientes al momento de realizar compras en línea.

2. Identificar las medidas de seguridad efectivas que puedan implementar las instituciones bancarias con el fin de mitigar el riesgo de que sus tarjetahabientes sean víctimas del fraude.

3. Elaborar una estrategia proactiva que pueden poner en práctica las instituciones bancarias para contrarrestar los fraudes que se presentan en los canales digitales.

1.5. JUSTIFICACIÓN DE LA INVESTIGACIÓN

La presente investigación expone los distintos métodos que se han implementado por parte de los criminales y sus redes para poder tomar posesión de la información personal de los tarjetahabientes y utilizar esta información para beneficio personal, ya sea por medio de hurto o extorsión.

Shum (2022) describe que, en Honduras, la población en promedio que tiene una cuenta bancaria en una institución financiera es únicamente del 42.9%, mientras que los que tienen una tarjeta de crédito son un 4.5%. Las personas que tienen una tarjeta de débito son el 16.9%, el 6.2% tiene una cuenta de dinero móvil, el porcentaje que hizo o recibió dinero digital el año pasado es del 37.2%, el 3.6% realizó una compra por internet, el 8.1% utilizó la banca en línea y aquellos que pagaron facturas o cuentas por internet son el 3.7%. La población total de Honduras es de 10.14 millones, de los cuales un 59,6% vive en zonas urbanizadas, mientras que las conexiones móviles totales son 7.61 millones de unidades, lo que representa el 75.1% de la población.

De acuerdo con estos números, Honduras es un país que aún sigue aprendiendo a utilizar los métodos alternativos de pago. Recientemente, tanto los comerciantes como los compradores han tenido que adoptar nuevas herramientas para poder realizar sus transacciones impulsados por las condiciones creadas a partir de la pandemia del COVID-19, y por eso es esencial comprender como funcionan estos recursos para el aprovechamiento de los beneficios y la reducción de las amenazas que ellos traen.

Según las publicaciones estadísticas en Honduras, aproximadamente un 68% de los tarjetahabientes están afiliados a los tres principales bancos del país que son: BAC Credomatic, Banco Ficohsa y Banco Atlántida, respectivamente. Sin embargo, hay 11 instituciones bancarias en el país que ofrecen diversos tipos de tarjetas de crédito (CNBS, 2022).

Al implementar una estrategia dirigida a los clientes de las instituciones previamente mencionadas se puede aumentar la inclusión financiera en el país e impulsar el comercio en línea. Pero primero se debe obligar los a comerciantes y a los gerentes de las empresas a enfocarse en la apropiada administración de las herramientas de pago digital, para anticipar y mitigar las posibles instancias de los casos de fraude y se reducir las estafas en línea.

CAPITULO II: MARCO TEÓRICO

2.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

La crisis sanitaria del COVID-19 afectó la economía a nivel mundial en todos los rubros y puso en riesgo la satisfacción de los consumidores de productos y servicios, ya que uno de los impactos más grandes que detonó la pandemia fue la crisis de la cadena de suministros, que se originó en China. A raíz de esto, los tiempos de entrega de los productos a nivel mundial se fueron extendiendo, generando así incertidumbre a la población y en algunos casos, según la demanda de los productos, hasta la escasez de ellos. La prestación de servicios también se vio afectada debido a que se implementaron medidas estrictas de circulación, por lo que las empresas tuvieron que ingeniárselas para seguir satisfaciendo las necesidades de sus clientes, pero con menos recursos disponibles. Con todo esto, las necesidades de los clientes fueron cambiando según su postura ante la pandemia, por lo que muchas empresas ganaron nuevos clientes y otras los perdieron en el proceso de la adaptación al cambio.

En Honduras, muchas empresas nacionales se vieron en una situación económica precaria que los llevo a cerrar operaciones. Sin embargo, las empresas que sí pudieron adaptarse a los cambios significativos en su operatividad diaria tuvieron que implementar nuevas formas de ofrecer sus productos y servicios. Cabe mencionar que, aunque el comercio electrónico ya venía en repunte en los últimos años, la adaptación de la venta de productos y servicios en medio de una pandemia les aceleró el paso a las empresas que lo tenían contemplado o lo comenzaban a implementar estas nuevas tecnologías.

Es indispensable manifestar que se desconocen las implicaciones que esta pandemia pueda generar a largo plazo en los mercados financieros, pero en el caso de que regrese todo a la

normalidad probablemente estas instituciones habrán aprendido a desarrollar de mejor manera la capacidad de recuperación operativa y así enfrentar futuras pandemias. Uno de los referentes en los últimos años ha sido la migración a canales digitales y conectividad; permitiendo una mayor interacción con los clientes a fin de reducir los costos y los tiempos de espera por parte del usuario y adicionalmente propiciando el no contacto físico en las transacciones (CNBS, 2021).

Es importante recalcar la facilidad que genera a los consumidores realizar sus compras en línea, sin embargo, el fraude electrónico ha aumentado significativamente debido al alza en las transacciones en las compras en línea. Cuando se produce un fraude en el comercio electrónico, la empresa no solo registra pérdidas en la facturación, también, tiene que hacer frente a los gastos por el daño infligido en su reputación y la pérdida de confianza de los clientes (Microsoft Corporation, 2022).

Debido al aumento de los fraudes presentados en el comercio electrónico, se ha identificado la necesidad de potenciar las estrategias que ya existen para hacer uso eficiente de los recursos y crear nuevas estrategias más eficientes mitigar el riesgo de éstos en las instituciones bancarias el fin de que puedan ofrecer a sus tarjetahabientes mayor seguridad, confianza y tranquilidad al momento de realizar sus gestiones en línea.

2.2. ANÁLISIS DEL MACROENTORNO

2.2.1. LA EVOLUCIÓN DE LOS MEDIOS DE PAGO A TRAVÉS DE LA HISTORIA

A lo largo de la historia el comercio ha ido evolucionando en conjunto con los avances tecnológicos, iniciando con el trueque donde Artiedas-Rojas (2017) apunta su concepción del proceso desde la antigüedad cuando varios pueblos empezaron con un intercambio de bienes y

servicios, debido a que el valor de cada producto estaba determinado por las unidades físicas y no por una unidad monetaria. Luego, en el siglo VII A.C. surgió la invención de la moneda que según Valdez (2022) se creó en los mercados con el propósito de agilizar los intercambios mercantiles, primero en la forma de mercancías aceptadas socialmente, y posteriormente, con los metales preciosos, que se convirtieron en la moneda por excelencia. Más adelante, surgió la moneda papel en el sigo VII D.C. sustituyendo a los metales preciosos donde "…el valor del dinero depende del Estado, el cual determina su valor nominal al ser el dinero un simple signo convencional, con lo que puede desempeñar su papel básico que es servir de medio de pago" (Valdez, 2022, p.3).

La tarjeta de crédito como la conocemos se creó en Nueva York, Manhattan en el año 1950, unificando la búsqueda de un sistema de pago a crédito seguro y personal junto con la comodidad de pagar en varios establecimientos con la misma tarjeta (Pérez, 2016). Por ende, Gill (2016) la define como:

> Un documento de material plástico o metal emitido por un banco o institución especializada a nombre de una persona, que podrá utilizarla para efectuar compras sin tener que pagar en efectivo y pudiendo, además, llevar el pago de los productos a períodos futuros (Sección Definición Técnica).

Es hasta en 1994 es cuando se realiza la primera transacción "en línea", cuando un usuario compró una pizza utilizando su ordenador PC por medio de una conexión a internet para compartir sus datos. A este tipo de compras se le denominó E-commerce (González, 2016).

Debido a la popularización de los dispositivos móviles, se ha desarrollado el M-Commerce (Mobile Commerce) que consiste en el uso de un teléfono celular o tableta para realizar las transacciones comerciales (BigCommerce, 2022).

En los últimos años, y especialmente a partir de la pandemia de COVID-19, el comercio electrónico se ha convertido en una parte indispensable del mercado minorista global. Y es que, durante meses, Internet fue el único medio a través del que muchas empresas pudieron seguir generando ingresos. Asimismo, fue la forma que los consumidores tuvieron para acceder a determinados artículos que, por su amplia demanda, no estaban disponibles en los establecimientos que se mantuvieron abiertos. Cerca del 90% de la población mundial admitió haber comprado en Internet en 2020, razón por la que no sorprende que los ingresos procedentes de las ventas online se situaran en alrededor de 4,2 billones de dólares estadounidenses en dicho año. Esta cifra fue aún mayor en 2021 pese a la apertura de los comercios, lo que no hace sino dejar constancia de que este cambio en los hábitos de compra es, con casi toda seguridad, permanente (Orús, 2022, Sección Comercio Electrónico B2C).

En la figura 1 se puede observar que para el año 2022, 2.14 mil millones de personas a nivel mundial han realizado compras en línea:

Figura 1. Número de personas a nivel mundial que han comprado en línea. Fuente: Oberlo|Statista.

Latinoamérica se ha convertido en la región de más rápido crecimiento en cuanto al comercio en línea según el estudio realizado por Ceurvels (2020) sobrepasando a Norteamérica y a Europa centro y occidental. Este crecimiento se puede observar a continuación en la figura 2:

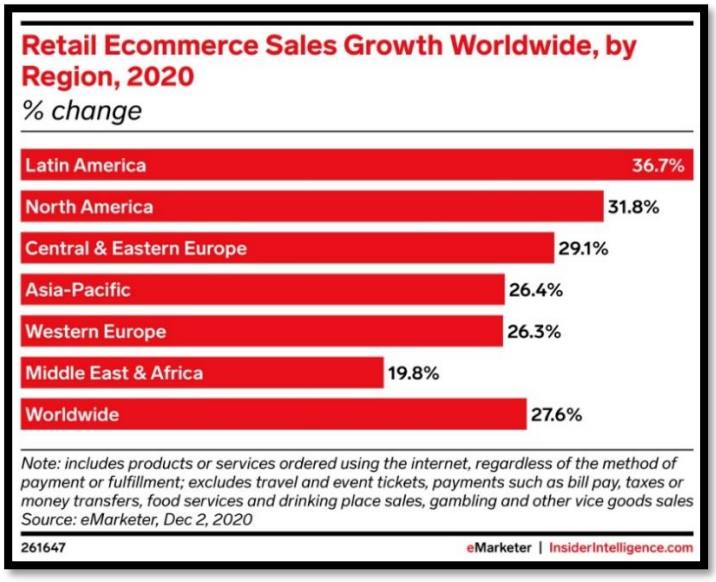

Figura 2. Porcentaje de crecimiento de compras en línea a nivel mundial para el final del año 2022. Fuente: eMarketer.

2.2.2. LA BANCA DIGITAL EN LATINOAMÉRICA

Para no quedarse rezagadas en una era digital, las instituciones bancarias también han tenido que adoptar nuevos canales digitales para poder satisfacer las necesidades de los clientes que, al igual que el comercio electrónico, estas mismas tuvieron un gran crecimiento a partir de la pandemia del COVID-19.

Previo a la pandemia, únicamente el 55% de la población en Latinoamérica tenía una cuenta bancaria y solo el 19% de ellos tenían una tarjeta de crédito (Lehr, 2020); esta región posee cuatro de los 10 países con los índices más altos de la población sin una cuenta bancaria. Estos países resultan ser México (63%) en el quinto Lugar, Perú (57%) en el séptimo, Colombia (54%) en el

octavo y Argentina (51%) en el décimo puesto (Ventura, 2021). Honduras presenta los mismos índices que Perú, pero no fue tomado en cuenta en esta investigación.

Según una investigación realizada por la Agencia EFE (2021) con las restricciones derivadas de la pandemia COVID-19, un 60 % de los consumidores en Latinoamérica abrieron cuentas y realizaron compras en línea en 2020, hasta el punto que los bancos de la región aceleraron sus planes digitales al menos 24 meses. Entre las principales tendencias detectadas por el estudio destaca la "aceleración de la adopción de la banca digital" para comprar y manejar dinero, en momentos en que "el 56 % de los consumidores dijo que prefería abrir una cuenta bancaria en línea en el futuro". Y el aumento de un 60 % de la apertura digital de cuentas entre los consumidores en 2020 indica una "tendencia agresiva hacia la adquisición de clientes en línea". Algunos de los servicios más avanzados que esperan los consumidores son las "transferencias a otros bancos en tiempo real, las transferencias internacionales, los pagos automáticos recurrentes y los pagos a través de una billetera móvil y un código QR"(Sección Economía).

De acuerdo a un estudio realizado por Merchant (2021) durante los primeros meses de la pandemia en el 2020 aumentaron las visitas a la banca en línea en Latinoamérica, siendo Brasil y Argentina los países con el mayor número visitas. En la figura 3 en la siguiente página, se puede apreciar los cambios en el número de visitas a la banca en línea.

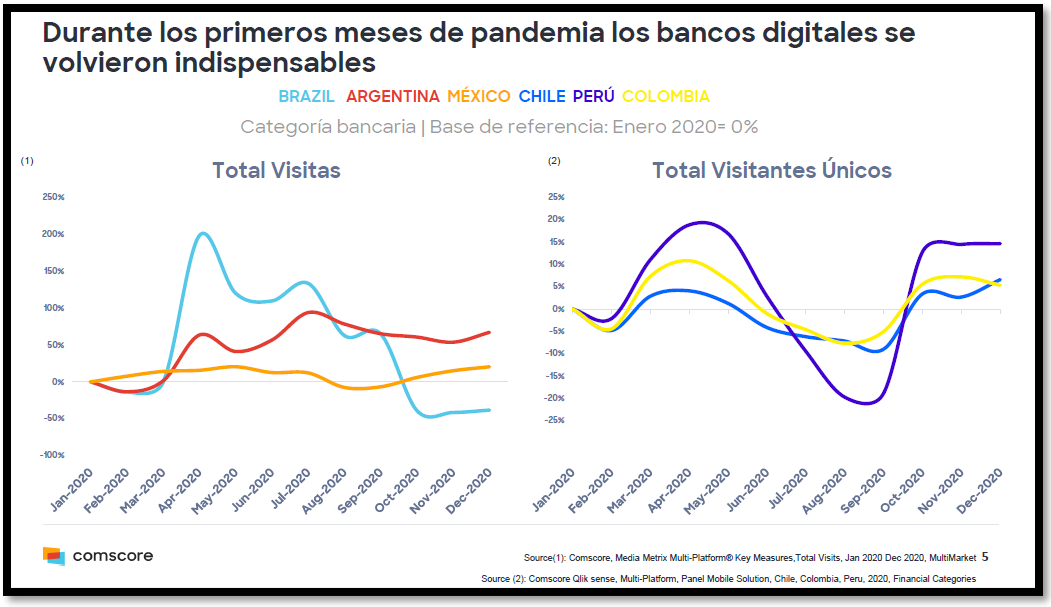

Figura 3. Número de visitas a la banca en línea por país en Latinoamérica en el año 2020. Fuente: Comscore.

En el mismo estudio realizado por Merchant (2021), también se concluyó que Brasil y Argentina fueron los países que lograron tener un mayor alcance de la banca digital en un 73% y un 66% respectivamente, esto se puede observar en la figura 4:

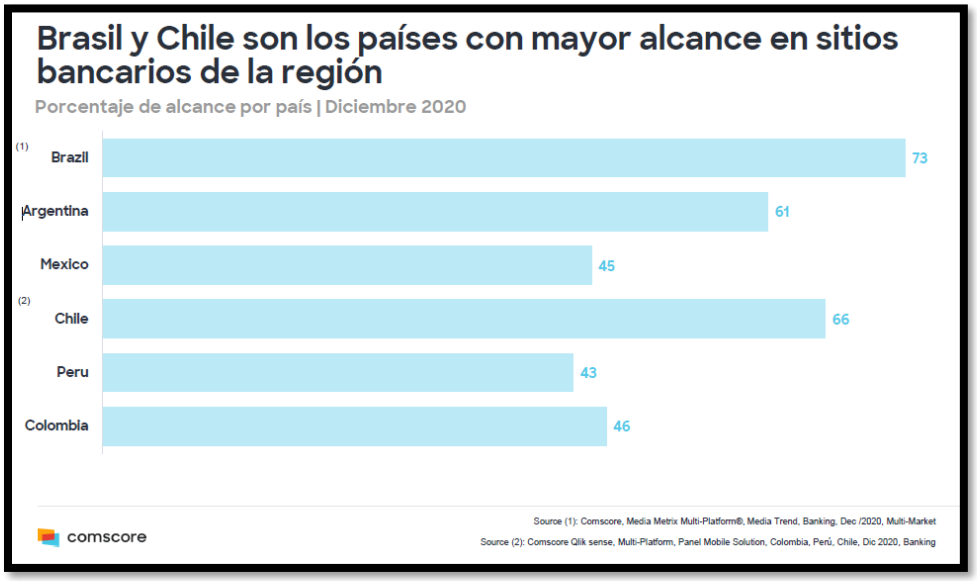

Figura 4. Alcance de la banca en línea por país en Latinoamérica para diciembre 2020. Fuente: Comscore.

2.2.3. USO DE MÉTODOS ALTERNATIVOS DE PAGO EN LATINOAMÉRICA

A pesar de que las compras en línea en Latinoamérica son las de mayor crecimiento a nivel mundial, no todos los países utilizan medios digitales como la manera principal para realizar sus de compras diarias. El efectivo sigue siendo el principal método de pago para la mayoría de las transacciones comerciales, pero fue gracias al aumento del uso de los smartphones que las compras en línea aumentaron de una manera tan considerable. El 70% de la población latinoamericana cuenta con un dispositivo móvil y con una conexión a internet para navegación (Lehr, 2020). Las tarjetas de crédito son las más utilizadas por la región, sin embargo, en parte de Suramérica únicamente utilizan tarjetas domesticas para realizar sus compras debido a que sus instituciones bancarias no les brindan la opción de tener tarjetas internacionales al no contar con canales de pago como VISA o MasterCard y utilizan sus propios canales locales para proporcionarle una tarjeta de créditos a sus clientes, limitando el comercio entre países (PYMNT, 2021).

En Brasil, por ejemplo, las tarjetas de crédito domesticas son el principal medio de pago para operaciones comerciales en línea. En segundo lugar se encuentran los comprobantes de pago, estos consisten en comprar utilizando efectivo un comprobante en las tiendas de preferencia y hacer las compras en línea con estos comprobantes, esto es debido más que todo a hábitos Culturales y desconfianza en las instituciones bancarias del país y en tercer lugar se encuentran las tarjetas de crédito internacional (Rolfe, 2021).

Rolfe (2021) también menciona que, en México, en contraste con Brasil, las tarjetas de crédito internacionales son el principal método de pago para compras en línea. Los comprobantes de pago ocupan el segundo lugar y en tercero se encuentran las tarjetas de débito, que le permiten

al usuario acceder a sus fondos en sus cuentas de ahorra utilizando un plástico similar al de una tarjeta de crédito.

Chile, es el país que posee la mayor penetración de tarjetas de crédito de la región con un 89% de la población utilizando una tarjeta de crédito (Park, 2022). La distribución de los medios de pago para compras en línea es muy similar entre las tarjetas de crédito internacional y domésticas, como también las tarjetas de débito.

2.2.4. FRAUDE CON TARJETAS DE CRÉDITO

Los casos de fraude han existido desde hace más de miles años, siendo el primer caso registrado en el año 300 A.C. en Grecia cuando un comerciante intento hundir su propio barco y reclamar el seguro sobre la mercancía que transportaba en ella cuando él ya la había escondido en un almacén (Goulding, 2018). Este caso no tuvo éxito debido a que encontraron al comerciante en el momento que quiso quemar su barco, pero desafortunadamente murió ahogado intentando huir.

Según Mckenna (2022), el primer caso de fraude con tarjetas de crédito se dio en 1899 en EE.UU. cuando las compañías de transporte le otorgaban un crédito a los ganaderos y granjeros para pagar hasta que sus cosechas rindieran frutos. Uno de estos ganaderos recibió una tarjeta de crédito de transporte, pero no quiso usarla así que la tiro a la basura. Un joven decidió revisar la basura de este señor ganadero y encontró la tarjeta y la utilizó para usar el transporte gratis. Al fin de mes, le llegó una cuenta de $27 al ganadero (en ese entonces era una suma considerada de dinero) y tuvo que pagar la deuda dado que en esos días no existían políticas de protección al consumidor.

Según la Cornell Law School (2008):

> Los sistemas de fraude con tarjetas de crédito se clasifican en dos categorías generales: solicitud fraudulenta de tarjeta y apropiación fraudulenta de cuenta. En el primer caso, los estafadores abren cuentas de tarjetas de crédito a nombre de otra persona. Esto ocurre cuando el delincuente tiene suficiente información sobre la víctima para completar la solicitud de la tarjeta de crédito. Por otro lado, el delincuente puede falsificar documentación. Este sistema representa un grave problema porque el delincuente puede realizar numerosas compras sin que la víctima se entere. El estado de cuenta puede tardar un mes en llegar, si es que llega (Sección Diccionario Digital).

2.2.5. FRECUENCIA DE CASOS DE FRAUDE EN EE. UU.

En los EE.UU. durante el 2020, los casos de fraude con más frecuencia fueron los que involucraban una tarjeta de crédito, sin embargo, los casos que generaron mayores pérdidas fueron los que involucraban transferencias bancarias o transferencias en línea al destinarse más dinero en este tipo de transacciones financieras (Steele, 2021). Los casos más comunes de fraude según su frecuencia fueron:

1. Tarjetas de crédito
    - Número de casos: 91,515 (Mayor número de casos)
    - Monto perdido: $149,000
2. Tarjetas de débito
    - Número de casos: 63,352

- Monto perdido: $117,000

3. Aplicación de pago o servicio.

    - Número de casos: 61,903
    - Monto perdido: $87,000

4. Transferencias en línea

    - Número de casos: 56,811
    - Monto perdido: $311,000

5. Tarjetas de regalo prepago

    - Número de casos: 43,242
    - Monto perdido: $124,000

6. Transferencias bancarias

    - Número de casos: 17,039
    - Monto perdido: $314,000 (Mayor monto perdido)

7. Efectivo

    - Número de casos: 14,630
    - Monto perdido: $146,000

8. Criptomonedas

    - Número de casos: 11,170

- Monto perdido: $129,000

9. Cheques

- Número de casos: 8,142
- Monto perdido: $27,000

10. Orden de dinero

- Número de casos: 3,872
- Monto perdido: $26,000

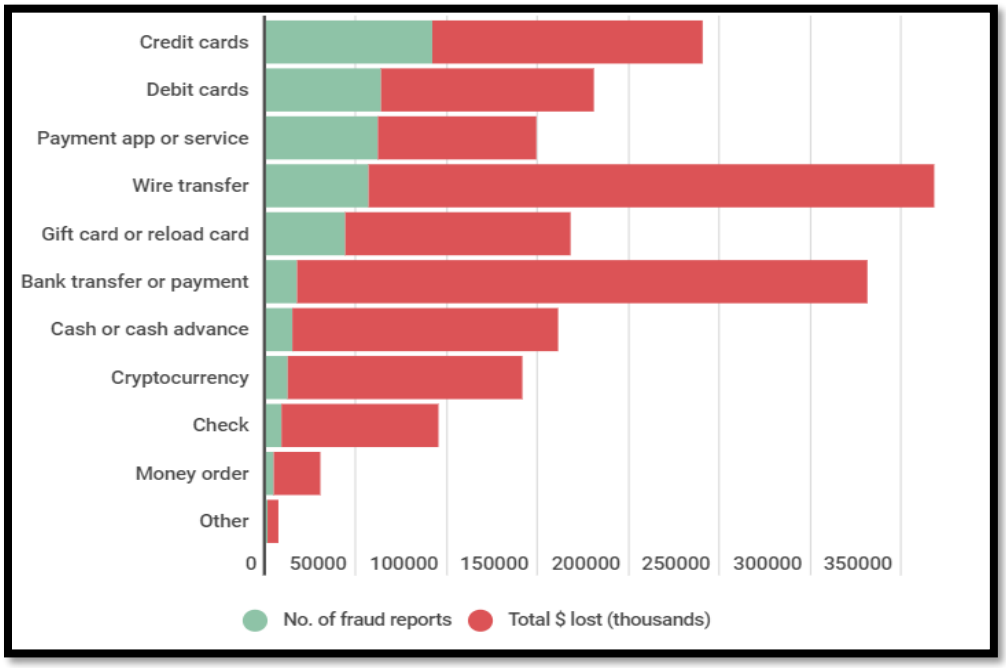

Figura 5. Comparación entre frecuencia y monto total perdido en $ de casos de Fraude en EE.UU. en 2020. Fuente: Federal Trade Commission's Consumer Sentinel Network 2020 Data Book.

2.3. ANÁLISIS DEL MICROENTORNO

Honduras, al igual que muchos países de Centroamérica, ve con buenos ojos las oportunidades de digitalizar su economía, principalmente bajo las modalidades que ofrece la integración financiera entre gobierno y empresas multinacionales (Mastercard, 2022).

En Honduras, los bancos e instituciones bancarias han dado pasos muy importantes en la transformación digital para el sector privado. Según la Consejo Nacional de Inversiones (2020), en las últimas décadas, las instituciones bancarias en Honduras han invertido muchos recursos económicos con el objetivo de brindar a sus clientes mayor flexibilidad al momento de realizar transacciones en canales digitales. Es decir, que el cliente desde cualquier parte del mundo donde se encuentre pueda realizar una compra en el sitio web de su preferencia, con la certeza de que la transacción se efectuará con éxito, por medio de una tarjeta de crédito. Sin embargo, tanta flexibilidad, requiere altas medidas de seguridad para mitigar el riesgo de fraude al que se exponen los tarjetahabientes cuando realizan sus compras en líneas.

Previo al COVID-19 y durante la pandemia, únicamente los Bancos Comerciales y las Cooperativas de Ahorro y Crédito crearon nuevos productos o servicios; hasta en un 25% incrementaron las transacciones por medios digitales en Bancos. Es decir, los Bancos Comerciales están enfocados en digitalizar sus productos y/o servicios, y más aun con las necesidades cambiantes de los clientes, que buscan y desean nuevas soluciones tecnológicas en la palma de sus manos (CNBS, 2020).

El uso frecuente de canales digitales ha provocado el aumento de delitos como, por ejemplo: suplantación de identidad y robo de datos de forma virtual; dentro de los principales controles que se toman, es la restricción de los privilegios administrativos; la cantidad de reclamos

que se obtienen al año, son mayores a 100 en los Bancos Comerciales y se estima que las pérdidas operativas sean mayores a L.1,000,000.00. (CNBS, 2020). Hay diversos tipos de fraudes al que se enfrentan los clientes al momento de realizar sus transacciones en canales digitales. Algunos de esos fraudes son: phishing (suplantación de identidad), captura de datos personales, instalación de software malintencionado, entre otros.

Los casos de fraude en canales digitales cada día son más en Honduras, por lo que las instituciones bancarias tienen que estar al pendiente de las nuevas formas en que buscan los estafadores llevar a cabo los fraudes. Cuando una persona es víctima de fraude en su cuenta de ahorro asume el riesgo de perder el dinero, mientras que en tarjetas de crédito se cuenta con un seguro de robo, fraude y extravío (Rodríguez, 2022). Los bancos recomiendan a los clientes adquirir dicho seguro, sin embargo, queda a discreción del cliente si desea pagarlo o no.

En la siguiente figura se observan las instituciones bancarias colocadoras de tarjetas de crédito en Honduras. Al mes de julio 2022, existían en circulación 813,350 tarjetas de crédito titulares (CNBS, 2022). El primer lugar con el mayor número de tarjetas colocadas es BAC Credomatic con el 35%, seguido por Banco Ficohsa con el 21% y, en tercer lugar, Banco Atlántida con un 11%. Las demás instituciones bancarias tienen una participación en el mercado por debajo del 10% cada una.

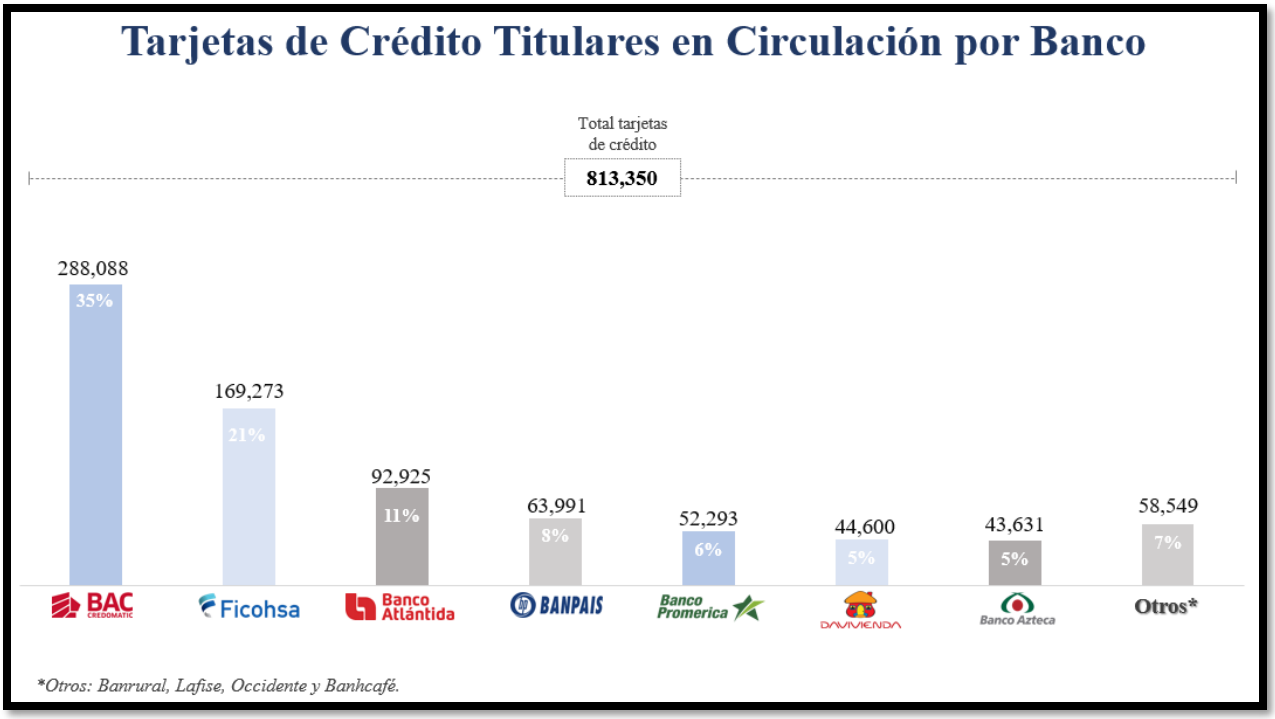

Figura 6. Tarjetas de Crédito Titulares en Circulación por Banco. Fuente: CNBS.

2.4. CONCEPTUALIZACIÓN

A continuación, se detallan los principales conceptos utilizados en este estudio, con el objetivo de brindar mayor claridad y comprensión al momento de la lectura y análisis de este.

- **Banco comercial:** "es un banco cuyo negocio principal es tratar con el público general. Es decir, ofrecen cuentas corrientes, dan prestamos, tienen productos financieros como planes de pensiones y fondos de inversión, etc. Se trata de bancos cuyo negocio se encuentra en la comercialización de estos productos" (BBVA, 2015, Sección Banco Comercial).
- **Digitalización:** "es el procedimiento mediante el cual, ciertas operaciones pueden comenzar a efectuarse a través de los medios digitales, como los ordenadores o los smartphones, normalmente con la ayuda de una conexión a Internet" (Westreicher, 2022, Sección Definición Técnica).

- **Emisor:** La ley de tarjetas de crédito (2006) lo establece como "sociedad mercantil autorizada para emitir tarjetas de crédito, perteneciente o no al sistema financiero, responsable frente a la Comisión y/o terceros por la emisión, operación, procesamiento y comercialización de las mismas, ya sea que estas actividades las realice el emisor o un tercero mediante contratos suscritos a tal efecto y que representan las marcas que ofrecen distintas franquicias" (Decreto No. 306-2006).
- **Mitigación de riesgo:** "es el proceso de desarrollo de opciones y acciones que, al ser implementadas, mejorarán las oportunidades y reducirán el impacto negativo o la probabilidad de ocurrencia de un evento en particular" (Escuela Europea de Excelencia, 2021, Sección ¿Qué es?).

2.5.TEORÍAS DE SUSTENTO

El propósito de las de teorías de sustento es compilar un conjunto de información que sostienen los argumentos y a su vez respaldan la investigación, con el objetivo de proporcionar las herramientas adecuadas para aportar una solución al problema planteado, con perspectivas estratégicas, económicas y administrativas, para fortalecer las bases del estudio.

2.5.1 CONVERGENCIA ENTRE NATIVOS DIGITALES E INMIGRANTES DIGITALES

Los nativos digitales, jóvenes expuestos a las tecnologías de la comunicación e información desde su nacimiento, se vienen integrando a las universidades y encuentran a inmigrantes digitales asumiendo el rol de docentes (Salas Delgado, 2018). Este comparativo se realiza por la diferencia que existe en la forma en cómo ven la tecnología y como su vida gira alrededor de ésta, tanto para los nativos como los inmigrantes.

Según Salas Delgado (2018):

> "La diferencia entre nativos e inmigrantes digitales va más allá de la edad, pero también de la exposición a las tecnologías digitales. La sobreexposición a contenidos en línea no garantiza que los nativos digitales puedan analizar con mayor destreza situaciones conflictivas y proponer soluciones; si bien los estudiantes acceden a información y recursos en mucho menos tiempo; prestan menos atención a los contenidos por la cantidad de datos a los que tienen acceso. Los nativos digitales registran menor tiempo de concentración que los inmigrantes digitales, priorizan la rapidez con que pueden leer los datos frente a la calidad de la información a la que puedan tener acceso (p.6).

Se puede deducir que el uso de las tecnologías es más inherente en las nuevas generaciones, esto apunta a que el uso de las tarjetas de crédito para realizar compras en línea y cualquier tipo de transacciones de forma virtual irán en aumento en los siguientes años. Sin embargo, este segmento, llamado "inmigrantes digitales", seguirá siendo importante mantenerlos actualizado y brindarles las herramientas necesarias para que ellos poco a poco sientan mayor seguridad y confianza al realizar sus gestiones en línea.

2.5.2. TRIÁNGULO DEL FRAUDE

Según López & Sánchez (2012) para que el fraude se materialice:

> Deben existir tres elementos: tener el poder (motivo o presión), percibir la oportunidad de cometerlo y de alguna manera racionalizar que el fraude es aceptable. Estos tres puntos importantes se conocen como el triángulo del fraude desarrollado por el criminólogo estadounidense Donald Cressey. Los componentes del triángulo del fraude surgen cuando una persona tiene altos estándares de moralidad, probablemente tiene dificultad de

cuestionamiento moral cuando está cometiendo un fraude. aquellos que no tienen principios, simplemente encuentran una excusa y se justifican a sí mismos diciendo que no hay nada malo en lo que están haciendo (p.66).

López & Sánchez (2012) describen los factores del triángulo de la siguiente manera:

1. Poder (incentivo, presión)- La administración u otros empleados tienen un estímulo o trabajan bajo presión, lo que les da una razón para cometer fraudes.
2. Oportunidad - Existen circunstancias que facilitan la oportunidad de perpetrar un fraude (por ejemplo, la ausencia de controles, controles ineficaces o la capacidad que tiene la administración para abrogar los controles).
3. Racionalización, actitud - Aquellas personas que son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto (p.69).

2.6. METODOLOGÍAS APLICADAS

En la siguiente sección se presenta una descripción detallada de las metodologías aplicadas para la recolección de datos y análisis de la información relacionada a las teorías anteriormente expuestas para el desarrollo de la investigación planteada.

2.6.1. REVISIÓN DOCUMENTAL #1

Se analizó y utilizó como referencia el proyecto de investigación de la incidencia del uso de tarjetas de crédito como medio de pago en los jóvenes de 18 a 25 años en la ciudad de Santiago de Cali en el año 2020. En él se realizó una investigación del tipo descriptivo con el propósito de

detallar las características y los rasgos de los sujetos sometidos al análisis. El enfoque de la investigación es mixto, recolectando datos cualitativos, las características del comportamiento de la población sujeta a la investigación; y cuantitativos, datos medibles analizados con herramientas estadísticas.

Según Restrepo & Rojas (2021), los jóvenes utilizan la tarjeta de crédito como medio de pago principal. La adquisición de las tarjetas se ha facilitado gracias a la flexibilización de los requisitos establecidos por las instituciones financieras. También se concluyó que los jóvenes prefieren realizar sus compras en línea, a menos que los establecimientos puedan un ofrecer un valor agregado brindando mejores experiencias que sus competidores.

De acuerdo a Sampieri & Fernández (2014) una investigación descriptiva: “Busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis” (p.98). Según Luna y Sierra (2022): “Describen situaciones, eventos o hechos, recolectando datos sobre una serie de cuestiones y se efectúan mediciones sobre ellas, buscan especificar propiedades, características y rasgos relevantes de cualquier fenómeno que se analice. Estos estudios presentan correlaciones muy incipientes o poco elaboradas” (p. 44).

En la investigación se utilizaron como instrumentos de recolección de datos la encuesta, el testimonio y la entrevista para conocer las motivaciones de los jóvenes para utilizar las tarjetas de crédito como medio de pago.

Se utilizó como referencia este trabajo investigativo para sustentar las tendencias mencionadas en los capítulos 2.2.2. y 2.3. en donde se mencionan el crecimiento del uso de tarjetas

de crédito para las transacciones digitales en Latinoamérica y, por consiguiente, también en Honduras.

2.6.2. REVISIÓN DOCUMENTAL #2

Se analizó el estudio por Kr. Kashyap et al. (2016) donde se sintetizó los casos de fraudes con mayor frecuencia en un lapso de 10 años de manera general y las consecuencias que estos actos traen seguido de ser aplicados en un ambiente real.

El enfoque de esta investigación inicia de manera cuantitativa con diseño descriptivo, detallando que es el fraude, los distintos tipos de fraude y las estrategias utilizadas para su descubrimiento; y termina siendo de carácter explicativo, exponiendo las consecuencias que estos casos crean y quienes son los afectados por estas conductas.

"Un enfoque explicativo está dirigido a responder por las causas de los eventos y fenómenos físicos o sociales. Se enfoca en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables"(Sampieri y Fernández, 2014, p. 95). Se utilizó como herramienta de recolección de datos la revisión de literatura de 33 referencias de publicaciones sobre casos de fraude para sintetizar los aspectos relevantes de estos casos en un solo documento. Según Sabates & Roca (2020) la revisión literaria:

> Se trata pues de localizar las aportaciones más relevantes (pasadas y actuales) sobre el tema de estudio, así como definir los principales conceptos y teorías que sirvan para fundamentar y comprender el problema y valorar cómo este encaja en un marco más general de investigación. La revisión de la literatura, además, tiene repercusiones a nivel metodológico, ya que permite ver de qué manera otros autores o autoras han definido y

operativizado las variables objeto de estudio, contribuye al desarrollo de hipótesis, permite identificar limitaciones metodológicas, resultados contrapuestos, etc. (p. 3).

Se utilizó como referencia este trabajo investigativo como soporte para la delimitación de los tipos de fraude en relación a las tarjetas de crédito y, como también quienes son afectados por el fraude y las consecuencias que traen.

2.6.3. DIAGRAMA DE ISHIKAWA

Se diseñó un diagrama de Ishikawa en base a la información obtenida por medio de las herramientas de recolección de datos, con el fin de presentar una visualización de la causa y efecto de los distintos tipos de fraude que pueden ser utilizados con las tarjetas de crédito.

De acorde a Gallo (2021):

> El diagrama de Ishikawa, conocido también como causa efecto o diagrama de espina de pez, es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. Nos permite, por tanto, representar gráficamente el conjunto de causas que dan lugar a una consecuencia, o bien el conjunto de factores y subfactores (en las "espinas") que contribuyen a generar un efecto común (en la "cabeza" del diagrama) (p. 19).

2.7.MARCO LEGAL

2.7.1. PRODUCTOS Y SERVICIOS FINANCIEROS

Para la creación de productos y servicios financieros en canales digitales, es necesario cumplir con una serie de reformas políticas y procesos, no solamente a lo interno de la institución financiera, sino también debe contar con la aprobación de los entes reguladores, en este caso de

la Comisión Nacional de Bancos y Seguros (CNBS), pues es el la institución pública hondureña que formula reglamentos a las leyes del sistema financiero, y de acuerdo a estos parámetros, realiza de forma anual, una auditoria para certificar la correcta aplicación a lo establecido en cada reglamento.

En Honduras se ha implementado la Ley de Tarjeta de Crédito, dicha ley detalla quienes son las entidades capaces de emitir una tarjeta de crédito, quien es el ente encargado de la regulación de los productos de las entidades financieras, sobre el manejo de la documentación necesaria y las condiciones que deben cumplir los clientes para optar a una tarjeta de crédito. Esta ley ha sido reformada en el año 2013 para irse adecuando a los nuevos canales digitales que han surgido gracias a los avances tecnológicos (Ley de Tarjetas de Crédito, 2006, Decreto: 306-2006).

2.7.2. COMERCIO ELECTRÓNICO

La Ley de Comercio electrónico fue creada en 2015 con el propósito de delimitar las condiciones en las que se efectúa un intercambio de manera electrónica. En ella se incluye la conceptualización de los términos generalmente aplicados a este tipo de actividad. Como también mención de las demás leyes ya establecidas que se relacionan directamente, como ser las leyes de protección del consumidor (Ley de Comercio Electrónico, 2014, Decreto: 149-2014).

2.7.3. PROTECCIÓN AL CONSUMIDOR

La Ley de Protección al Consumidor fue aprobada en 2009 con el fin definir las condiciones que los establecimientos comerciales deben cumplir para poder operar de manera legitima en territorio hondureño. Esta ley incluye determinación de precios, garantías de parte de

los proveedores, procedimientos administrativos, prácticas abusivas, acciones y tribunales arbitrales, entre otros (Ley de Protección al consumidor, 2008, Decreto: 014-2008).

CAPÍTULO III. METODOLOGÍA

El presente capítulo consiste en describir las metodologías utilizadas para el desarrollo de la investigación, detalla el enfoque planteado y delimita el alcance del problema. Presenta, además, la congruencia de metodológica, las variables a considerar, como también la hipótesis que proporcionan la estructura necesaria para el posterior análisis de resultados.

3.1. CONGRUENCIA METODOLÓGICA

Con el fin de demostrar la existencia de una cohesión lógica en el tema de investigación, a continuación, se presenta la tabla 6 que contiene la matriz de congruencia metodológica que refleja la correlación entre el problema, las preguntas de investigación, los objetivo y las variables.

3.1.1. MATRIZ METODOLÓGICA

Tabla 1. Matriz Metodológica. Fuente: Elaboración Propia.

Título de la investigación	Problemas de la investigación	Preguntas de la investigación	Objetivos Específicos Específicos
Desarrollo de estrategia proactiva contra el fraude con de tarjetas crédito en las principales instituciones bancarias en honduras	¿Qué estrategias de mitigación de riesgo del fraude digital, que existen actualmente, podrían las instituciones bancarias modificar e implementar aprovechando los recursos y herramientas con las que ya cuentan para brindar mayor seguridad y confianza a los tarjetahabientes?	1. ¿Cuáles son los principales riesgos de fraude al que están expuestos los tarjetahabientes al momento de realizar compras en línea?	1. Conocer los principales riesgos de fraude a los que están expuestos los tarjetahabientes al momento de realizar compras en línea.
		2. ¿Cuáles son las medidas de seguridad en el mercado que pueden brindar mayor apoyo a las instituciones bancarias al momento de monitorear y resguardar las transacciones de sus tarjetahabientes?	2. Identificar las medidas de seguridad efectivas que puedan implementar las instituciones bancarias con el fin de mitigar el riesgo de que sus tarjetahabientes sean víctimas del fraude.
		3. ¿Cuáles son algunas estrategias que puede implementar y modificar las instituciones bancarias para contrarrestar los fraudes que se presentan en los canales digitales?	3. Elaborar una estrategia proactiva que puedan implementar las instituciones bancarias para contrarrestar los fraudes que se presentan en los canales digitales.

3.1.2. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 2. Operacionalización de las variables. Elaboración: Propia.

Variable	Definición		Indicadores	Ítem	Escala	Instrumento
	Conceptual	Operacional				
Fraude	Es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización (como el Estado o una empresa)" (Pérez, 2021, Sección Definición).	Fraudes realizados a tarjetas de crédito	Método de fraude más utilizado. Reducción del fraude con tarjetas de crédito	P. 6, 9	Pregunta abierta	Entrevista estructurada y Entrevista no estructurada.
Estafa	El delito de estafa es un delito patrimonial que comete la persona que emplea el engaño con ánimo de lucro para provocar un error en la víctima, induciéndola a realizar un acto de disposición en perjuicio de sí misma o de un tercero (Escalas, 2019, Sección Derecho Penal)**.**	Materialización del fraude.	Estafas de alto impacto para la institución.	P.8	Pregunta abierta	Entrevista estructurada y Entrevista no estructurada.
Tarjetahabiente	Hace referencia a una persona poseedora de tarjeta de crédito" (RAE, 2021, Sección Definición).	Conocimiento de los tarjetahabientes de prevención contra el fraude.	Nivel de educación contra el fraude de tarjetahabientes. Tipo de tarjetahabientes con mayor exposición al fraude.	P. 1, 11	Pregunta abierta	Entrevista estructurada, Entrevista no estructurada y Observación Participativa.
Bancos	Un banco comercial es una entidad cuya actividad económica es la intermediación financiera. Es decir, capta depósitos del público, dirigiendo esos recursos al otorgamiento de créditos, con el objetivo de obtener un beneficio (Galán, 2017, Sección Definición Técnica).	Manejo del fraude electrónico.	Respuestas de los bancos ante el fraude. Formas de prevenir el fraude a sus tarjetahabientes.	P. 4, 5,7, 10	Pregunta abierta	Entrevista estructurada, Entrevista no estructurada y Observación Participativa.
Comercio electrónico	El e-commerce o comercio electrónico consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet. Conscientes de estar a la vanguardia, las Pymes no se han quedado atrás en este nuevo mercado, por lo que han hecho de los servicios de la red un lugar que permite acceder a sus productos y servicios durante las 24 horas del día (VISA, 2014, Sección Tecnología).	Uso de tarjetas de crédito para compras en línea.	Errores comunes al realizar compras en línea. Transacciones de compras en línea con mayor exposición al fraude.	P.2, 3	Pregunta abierta	Entrevista estructurada y Entrevista no estructurada

3.2. ENFOQUE Y MÉTODOS

La investigación se llevó a cabo mediante un enfoque mixto con el objetivo principal desarrollar una estrategia proactiva para mitigar los fraudes y estafas en los tarjetahabientes en Honduras. Partiendo de este enfoque, el alcance de la investigación serán las principales instituciones bancarias colocadores de tarjetas en Honduras.

El método de estudio aplicado en la investigación es explicativo. Según Sampieri y Fernández (2014), los estudios explicativos buscan encontrar las razones o causas que provocan ciertos fenómenos. Los estudios de este tipo implican esfuerzos del investigador y una gran capacidad de análisis, síntesis e interpretación (p.99). Asimismo, debe señalar las razones por las cuales el estudio puede considerarse explicativo (Hidalgo, 2005). El principal instrumento para la recolección de datos es la guía de entrevistas estructuradas donde se incluyen las preguntas y los aspectos a analizar con expertos en temas de fraude electrónico con tarjetas de crédito en las principales entidades bancarias en Honduras; y, la guía de entrevistas no estructuradas donde se incluye los temas a discutir con tarjetahabientes comunes sin amplios conocimientos financieros en donde relatan sus experiencias con casos de fraude de tarjetas de crédito.

3.3. DISEÑO DE LA INVESTIGACIÓN

3.3.1. POBLACIÓN

Expertos en temas de fraude electrónico en el rubro de las instituciones bancarias en Honduras y tarjetahabientes víctimas de un atentado o fraude con tarjetas de crédito. En este caso, la población de los expertos es desconocida.

La población sujeta a estudio para las víctimas de algún tipo de fraude es elegida a partir de la cantidad de tarjetas de crédito en circulación en Honduras dividida por la mitad debido a que según la CNBS (2021) cada tarjetahabiente tiene 2 tarjetas en promedio. La población sería 813,350 / 2 = 406,675.

3.3.2. MUESTRA

Debido a que la población de expertos en temas de fraude electrónico con tarjetas de crédito en las instituciones bancarias es desconocida. El tamaño de la muestra para nuestra población infinita fue de 385. Se realizaron entrevistas a expertos en Tegucigalpa, Honduras con amplia experiencia laboral y conocimiento en temas de fraude electrónico con tarjetas de crédito en las principales instituciones bancarias de Honduras.

$$n = \frac{Z_{\alpha}^{2} \cdot p \cdot q}{i^{2}}$$

Donde:

Z_a= Nivel de confianza (95%) = 1.96

p = Probabilidad positiva = 0.70

q = Probabilidad negativa = 0.30

i = Margen de error = 0.10

Desarrollo:

$$\frac{1.96^2 * 0.70 * 0.30}{0.10^2}$$

n= 80.6 = 81

Para la selección de la muestra de los tarjetahabientes víctimas de fraude se utilizó el método aleatorio simple debido a que cada uno de los integrantes de la población tiene la misma probabilidad de ser seleccionado para su cálculo se tomó un margen de error del 5%, con un nivel de confianza del 95% y una variabilidad conocida del 50%.

Cálculo del tamaño de la muestra finita y conocida:

$$n = \frac{Z_{\alpha}^{2} \cdot N \cdot p \cdot q}{i^2 (N-1) + Z_{\alpha}^{2} \cdot p \cdot q}$$

Donde:

Z= Nivel de confianza (95%) = 1.96

N= Estimado de tarjetahabientes = 406,675

p = Probabilidad positiva = 0.50

q = Probabilidad negativa = 0.50

i = Margen de error = 0.05

Desarrollo:

$$\frac{1.96^2 * 406675 * 0.50 * 0.50}{0.05^2(406675 - 1) + 1.96^2 * 0.50 * 0.50}$$

n= 383.80 = 384

3.3.3. TÉCNICAS DE MUESTREO

Al ser una investigación mixta, el tipo de muestreo utilizado es por conveniencia, un método no probabilístico.

Esto permite seleccionar aquellos casos accesibles que acepten ser incluidos. Esto, fundamentado en la conveniente accesibilidad y proximidad de los sujetos para el investigador (Otzen y Manterola, 2017). Es decir, el muestreo por conveniencia consiste en seleccionar para la muestra de un estudio estadístico a aquellos individuos que se encuentran más al alcance. Esto permite que la recolección de datos sea menos costosa e implique menor esfuerzo (Westreicher, 2022).

3.4. INSTRUMENTOS, TÉCNICAS Y PROCEDIMIENTOS APLICADOS

3.4.1. TÉCNICAS

La Universidad La Concordia (2020) define las técnicas de investigación como: "Un conjunto de procedimientos metodológicos y sistemáticos cuyo objetivo es garantizar la operatividad del proceso investigativo. Es decir, obtener mucha información y conocimiento para resolver nuestras preguntas".

Las técnicas de investigación utilizadas para la recopilación de datos fueron entrevistas estructuradas, aplicada a expertos en herramientas y procedimientos preventivos en casos de fraude

que involucra tarjetas de crédito; también se utilizó el testimonio en víctimas de atentados o casos de fraude; y se utilizó la observación participativa para analizar los procedimientos de solicitud de tarjetas de crédito en dos de los bancos principales del país Banco Atlantida y BAC, con el propósito de identificar qué formas de educación contra el fraude se les brindan a los tarjetahabientes desde el momento que se les entrega la tarjeta de crédito.

3.4.1.1. ENTREVISTA

Según Universidad La Concordia (2020) en una entrevista estructurada:

Se predetermina un cuestionario específico para la obtención de la información, esta se aplica de manera esquemática y secuenciada. En ella:

- Se plantean preguntas directamente al sujeto o los sujetos de estudio, generalmente en un lugar aislado, para así obtener una aproximación a lo que piensa, siente o ha vivido, que luego podrá ser procesada estadísticamente o mediante otros métodos, para obtener una verdad.
- Se realiza con el fin de obtener información del entrevistado, la cual variará en función del objeto de estudio de la investigación.
- Se hace cuando se considera necesario que exista interacción y diálogo entre el investigador y la persona investigada.
- Es una buena herramienta para utilizar cuando la población que es objeto de estudio es pequeña y manejable, ya sea una persona o un grupo reducido de ellos.

En cambio, en una entrevista no estructurada, la charla es guiada por uno o varios objetivos de la entrevista, se busca ampliar la información lo más posible y no se sigue un orden específico (Sección Entrevista).

3.4.1.2. OBSERVACIÓN

Una observación consiste en "confrontar el fenómeno que se desea comprender y describirlo, tomar nota de sus peculiaridades, de su entorno y detallarlo. Implica observar atentamente el fenómeno, hecho o caso concreto, tomando la información necesaria y registrándola de forma más o menos sistemática" (Universidad La Concordia, 2020, Sección Observación).

3.4.2. INSTRUMENTOS

Según Díaz (s. f.) los instrumentos de investigación son un conjunto de herramientas, procedimientos e instrumentos utilizados para obtener información y conocimiento. Se utilizan de acuerdo con los protocolos establecidos en cada metodología.

Para la presente investigación se utilizaron como instrumentos el guion de entrevista con el propósito de conservar la estructura de las preguntas mientras se realiza la entrevista a los participantes; y, adicionalmente, se utilizó la ficha de contenido para llevar un registro de las notas y observaciones durante la investigación de campo.

Se utilizó la plataforma de "Google Forms" para realizar las preguntas dirigidas a las víctimas de atentados o casos de fraude. En esta se redactaron cuatro preguntas abiertas para y brindar el espacio a las personas entrevistadas para contar su testimonio de situaciones sujetas al fraude de tarjetas de crédito de una manera sin la necesidad de seguir la pauta de algún formato, y; se solicitaron sus respectivos datos demográficos. En esta plataforma se almacena la

información contestada en línea para poder ser analizada una vez se haya recopilado la información por el usuario que creo la entrevista. Esta plataforma permite enviar el enlace en línea para poder ser llenada desde un dispositivo con acceso a internet, y el objetivo de la presente investigación era ser llenado desde un teléfono móvil, una computadora de escritorio o una laptop.

Estas preguntas abiertas aplicadas a víctimas de atentados o casos de fraude fueron analizadas utilizando el software "Microsoft Excel". Las respuestas se transcribieron en una tabla para llevar un registro ordenado y se utilizaron las fórmulas de conteo condicionales para desarrollar una nube de palabras para encontrar las incidencias de las tácticas de fraude utilizadas población entrevistada.

Según Díaz (2018):

> Las nubes de palabras, también conocidas como nubes de tags o nubes de etiquetas, son la representación visual de las palabras más importantes que componen un texto. En el área educativa las nubes de palabras resultan muy útiles para desarrollar la capacidad de síntesis. Las nubes de palabras además permiten visualizar las palabras claves del contenido a tratar o las ideas principales de un tema en un solo vistazo. Mejorando también la compresión (Sección Negocio Online).

3.5. FUENTES DE INFORMACIÓN

3.5.1. FUENTES PRIMARIAS

Las fuentes primarias utilizadas en el presente estudio de investigación son las cinco entrevistas efectuadas a personas con amplia experiencia laboral y conocimiento sobre el fraude electrónico al que están expuestos los tarjetahabientes en las instituciones bancarias en Honduras.

Se utilizaron los testimonios proporcionados por portadores de tarjetas de crédito que han sido víctimas de fraude electrónico. También, se utilizó la observación participativa en el proceso de solicitud de tarjeta de crédito de dos de los bancos de mayor participación en Honduras.

3.5.2. FUENTES SECUNDARIAS

Las fuentes secundarias utilizadas son reportes financieros de la Comisión Nacional de Bancos y Seguros (CNBS), estudios de tesis, artículos virtuales, páginas webs de instituciones bancarias transnacionales, entre otros. Toda esta información obtenida está relacionada muy de cerca con el tema de investigación referente al fraude electrónico, cabe resaltar, que toda la información extraída de las diversas fuentes se encuentra debidamente citada con el fin de salvaguardas los derechos de autor de los terceros.

CAPITULO IV: RESULTADOS Y ANÁLISIS

4.1. INFORME DE PROCESO DE RECOLECCIÓN DE DATOS

4.1.1. ENTREVISTA ESTRUCTURADA

Se programó una sesión de entrevista estructurada individual con especialistas con amplia experiencia en el ámbito de tarjetas de crédito/debito, como también en el ámbito de monitoreo y prevención de fraude financiero, considerando que los miembros de esta población deben enfrentar esta problemática en sus labores profesionales diarias y son capaces de proveer la información confiable y actualizada.

Las preguntas realizadas en la entrevista les permiten a los expertos profundizar sobre la situación actual de la industria financiera de Honduras y les permite ofrecer su opinión profesional de cómo se puede mejorar y mitigar los casos de Fraudes.

Tabla 3. Criterios de Selección de Expertos. Fuente: Elaboración propia

Criterios de Selección de Expertos

Área de experiencia	Monitoreo de sistemas de alertas tarjetas de crédito/Tarjetas de crédito e Inteligencia de Negocios/Seguridad de la información
Áreas de profesión	Ingenieros/Licenciados en Informática/Sistemas/Marketing
Lugar de trabajo	Principales instituciones bancarias colocadoras de tarjetas de crédito en Honduras

Años de Experiencia	Superior a 5 años
Puestos desempeñados actualmente	Supervisores, Jefes, Subgerentes y/o Gerentes

4.1.2. ENTREVISTA NO ESTRUCTURADA – TESTIMONIOS DE ATENTADOS O CASOS DE FRAUDE

Adicionalmente, se realizó una entrevista no estructurada de menor tamaño dirigida hacia tarjetahabientes que han sido víctimas de atentado o de casos de fraude con sus compras de tarjeta de crédito/debito para compartir su experiencia, lecciones aprendidas y retroalimentación de cómo se pudo haber manejado la situación.

Esta herramienta se utilizó para brindar un espacio abierto a los entrevistados de narrar sus experiencias de la forma que se sientan más cómodo sin tener que cumplir con algún requisito en específico.

Se les consultó a 60 personas de la capital de Honduras como había sucedido el intento o caso de fraude, si el banco pudo responder a tiempo y solucionar el caso, su opinión acerca de cómo se pudo haber manejado la situación y que lecciones aprendieron a partir del incidente. Se les consultó los datos demográficos a los entrevistados con el propósito de encontrar alguna tendencia entre las edades o género y los casos de fraude.

4.1.3. OBSERVACIÓN PARTICIPATIVA

También, se realizó una observación participativa en donde se formó parte del proceso de solicitud y adquisición de tarjetas de crédito en Banco Atlántida, Ficohsa y BAC para conocer las

formas que utilizan estas instituciones para educar a sus tarjetahabientes con respecto al fraude en materia de tarjetas de crédito. Al haber 11 instituciones bancarias colocadoras de tarjetas de crédito, no se puede generalizar el sistema bancario solo con estas dos instituciones, sin embargo, BAC, Ficohsa y Banco Atlántida representan el 27% de las instituciones bancarias colocadoras de tarjetas de crédito en Honduras y 67% de las tarjetas de crédito en circulación en Honduras.

4.2. RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

4.2.1. ENTREVISTA ESTRUCTURADA – EXPERTOS EN MATERIA DE PREVENCION DE FRAUDE DE TARJETAS DE CRÉDITO

La entrevista estructurada fue aplicada a cinco profesionales con amplia experiencia en el rubro financiero, específicamente que han estado o están en áreas de Seguridad de la Información y Monitoreo. Se les realizó once preguntas donde cada persona contestó objetivamente basándose en su conocimiento, escenarios que han presenciado y principalmente, en la experiencia adquirida a lo largo de los años.

Cada una de las preguntas fue elaborada con el fin de que las respuestas brindadas por las personas entrevistadas, fuese de mucha utilidad para la realización de la estrategia contra el fraude realizado con tarjetas de crédito. Tomando como un valioso insumo dichas entrevistas, se logró conocer de cerca el tema del fraude en este rubro financiero (ver Respuestas de Entrevistas Realizadas a Expertos, anexo 1).

El primer escenario planteado a los entrevistado fue “Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted que es esencial para que el tarjetahabiente se

anticipe a un fraude al momento que adquiere su primera tarjeta de crédito?". Partiendo de la interrogante y basado en las respuestas obtenidas, es claro que el origen de la prevención contra el fraude con tarjetas de crédito debe ser nacer del lado del Banco, desde el momento que entrega la tarjeta al cliente, tienen la obligación de proporcionarle todas las medidas necesarias que lo eduquen contra la exposición al fraude, con el fin de reducir la posibilidad de ser víctima de éste.

Como segunda pregunta, se consultó "¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?". Expresaron y coincidieron los entrevistados que los errores más comunes que realizan las personas al momento de hacer compras en línea es compartir información confidencial en páginas web que no cuentan con certificados de seguridad porque no son oficiales y son creados con fines maliciosos. Por este motivo, la principal recomendación que ellos brindan es que los tarjetahabientes se aseguren de validar estar comprando en páginas oficiales, que verifiquen los temas de certificados de seguridad y si es posible, dejar una tarjeta de crédito exclusivamente para realizar compras en líneas. En este último caso, más que todo para personas que realizan compras en internet con mucha frecuencia, ya sea por placer o negocio.

La tercera interrogante fue "¿Cuáles son algunas de las transacciones con tarjeta de crédito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?". Los entrevistados respondieron que definitivamente las compras en páginas web son las más expuestas al fraude, esto debido a la gran diversidad de opciones que hay en día donde las personas navegan en internet y muchas veces se dejan llevar por descuentos, ya que los estafadores colocan precios extremadamente bajos en artículos que su precio original es mucho más elevado para atraer sus víctimas. De igual forma, suele suceder que los menores de edad se dejan llevar por

anuncios que tienen que ver con venta de juegos atractivos, ingresando así datos de las tarjetas de sus padres y exponiendo su información sensible en sitios fraudulentos.

En el cuarto inciso, se les consultó "¿Qué considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?". Los expertos respondieron que las instituciones bancarias sin duda alguna tienen mucha responsabilidad ante sus clientes de educarlos contra el fraude al que se exponen al utilizar sus tarjetas y brindarles facilidades en la palma de sus manos donde puedan contrarrestar el fraude de manera rápida. Por ejemplo, que el mismo tarjetahabiente desde su banca en línea pueda inactivar su tarjeta en caso de que haya sido expuesto al fraude, extravío del plástico o cualquier escenario que le genere inseguridad.

En la quinta pregunta, se les consultó "Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?". A lo que los entrevistados mencionaron que, así como las instituciones bancarías invierten en la innovación de sus recursos tecnológicos para facilitarle la vida a sus clientes, igualmente el fraude es cambiante y día a día nuevas formas de estafar son puestas en marcha por malhechores. Lo bancos lastimosamente son entes reactivos, ya que seguirles el paso a los defraudadores es complicado por la manera de operar de ellos. Por ende, deben estar a la vanguardia, tanto de actualizaciones en sus sistemas de monitoreos, como a las nuevas y complejas formas del fraude.

Basado en la experiencia de los entrevistados, se les consultó como sexta interrogante, "En los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?". Los entrevistados mencionaron diversas formas como ser el famoso "phishing", que es la

suplantación de identidad. En los últimos tiempos, de igual forma, la tendencia indica que el fraude se está inclinando por el lado de las billeteras digitales y persiste la venta de números de tarjetas en páginas clandestinas (deep web) en donde se pueden comprar lotes de números de tarjetas y de esa manera probar en cualquier comercio realizar una compra. Por escenarios como este último, las instituciones bancarias resguardan la información de sus tarjetahabientes de forma muy rigurosa, tienen políticas estrictas y procesos documentados para que sus colaborares de igual manera manejen de forma responsable esta información, y evitar al máximo que haya fuga de información.

Considerando la sexta pregunta, la séptima interrogante fue “Según la respuesta anterior, ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?”. Como medida preventiva, los bancos se han enfocado en campañas publicitarias masivas de concientización para la prevención de fraude para sus clientes, con el fin de informarles que hacer ante casos de fraude. Aprovechando de esta forma los canales digitales como correo electrónico y redes sociales, de igual forma, siempre se lanzan campañas por los medios tradicionales, como ser pautas radiales, comerciales en la televisión y publicidad en periódicos impresos. Internamente dentro las instituciones, lo que se hace, es la parametrización de reglas para diferentes patrones de fraude, y así realizar bloqueo de tarjetas según un patrón de fraude identificado.

En la octava pregunta, se buscó que compartieran un poco de lo que han experimentado, se les consultó “¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?”. La siguiente experiencia es basada en un evento real que sucedió en una institución bancaria este año.

"*Hace unos meses un correo phishing ingreso a la bandeja de uno de los colaboradores, en el correo se le pedía ingresar sus credenciales a lo que el accedió pensando que se trataba de un correo interno de la empresa. Cuando los defraudadores ingresaron con sus credenciales enviaron correos a los demás colaboradores pidiendo información con la excusa que se trataba de temas internos. Para que el usuario no se diera cuenta que los correos estaban saliendo de su cuenta los defraudadores crearon una regla en la que los mensajes que le enviaran relacionados al correo en donde pedían información se desviaran. En uno de esos correos que los colaboradores enviaron se divulgaron un set de número de tarjetas que posteriormente los defraudadores usaron para venderlas.*

Este caso pudo haber sido evitado si el usuario simplemente hubiera ignorado el correo que los defraudadores enviaron."

Esta experiencia compartida, es un claro ejemplo de que nadie está exento del fraude, inclusive las personas que laboran dentro de las instituciones bancarias pueden ser víctimas de fraude. Las personas en general podrían creer que por la preparación y medidas de seguridad de las instituciones mantiene, los colaboradores no caerían en estas trampas, sin embargo, las personas dedicadas a realizar fraude aprovechan la mínima debilidad para buscar atacar y lograr el éxito con sus actividades delictivas dentro de cualquier entidad. De igual manera, este caso expuesto sirve como experiencia para la institución y así implementar medidas de seguridad más rigurosas y efectivas.

Ya casi finalizando, en el noveno inciso, se les consultó "¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito para reducir la exposición al fraude?". Coincidieron los entrevistados en que definitivamente las campañas de concientización

para los clientes externos e internos han tenido un apogeo en los últimos años. Así como la adopción de capas de seguridad en correos, y otras plataformas como ser la identificación biométrica, la verificación de dos pasos, notificaciones por correo y mensajes de texto sobre actividades de inicio de sesión y compras. La geolocalización de las compras, para saber dónde se producen las mismas, lo que permite a los sistemas de monitoreo ser más eficientes con las alertas.

Una de las medidas implementadas por las instituciones bancarias, que ha venido a ayudar para mitigar el riesgo de los fraudes, son las nuevas tecnologías de tarjetas chip contacless. Las tarjetas con chip brindan mayor seguridad que las tarjetas de banda y eso ofrece mayor a tranquilidad a los tarjetahabientes.

En la pregunta diez, se consultó "Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?". A esta interrogante respondieron los entrevistados que actualmente es el medio más importante para realizar conciencia de prevención y puede ser aprovechado subiendo las campañas a dichas redes para tener mayor alcance. Ya que con la evolución de la tecnología por medio de las redes sociales es una oportunidad para poder diseñar campañas publicitarias y de prevención por este canal digital que tanto es usado en sus diferentes plataformas, es muy factible porque los costos de propagación son mucho menores que otros medios, pero una notoria igualdad de eficacia.

En la última pregunta, se les consultó "¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué? Considerando que por ejemplo una tarjeta de crédito negra tiene límite alto." Aquí expusieron que los tarjetahabientes están en constante peligro todos en general, ya que muchas veces la suma de pequeñas transacciones

representa una suma de dinero considerable. Sin embargo, cada institución financiera tiene reglas de fraude y límites de compra, diferentes para cada tarjeta, pero definitivamente a mayor limite mayor posibilidad de fraude. De igual forma, también a mayor limite mayor restricción en reglas de compras por el mismo tema, ya que se busca gestionar de forma más segura este tipo de tarjetahabientes, pero definitivamente esto es a criterio de cada institución financiera.

En estos últimos años el término ciberdelincuente, está de moda; y no es para menos, con el avance de la tecnología las empresas grandes, medianas e incluso pequeñas han migrado, o están en el camino, sus procesos para que cada vez más éstos sean soportados por diferentes sistemas tecnológicos, reduciendo tiempos, conectando a sucursales y personas que están en diferentes regiones, automatizando procedimientos entre otras consideraciones.

Las instituciones bancarias son responsables de contar con sistemas efectivos y actualizados para el monitoreo de las transacciones que realizan los clientes con sus tarjetas de crédito, Monitor Plus es un software conocido que usan actualmente algunos de estas instituciones aquí en Honduras. Adicional, contar con medidas de seguridad puedan brindar mayor seguridad a los tarjetahabientes al momento de realizar sus transacciones, como ser, herramientas con varias capas de seguridad, una de ellas es la autenticación de dos pasos (proceso que valida la identidad del usuario mediante dos métodos de confirmación, como ser la solicitud de una contraseña o PIN único para el usuario, y como segundo paso, la confirmación por código enviado a número telefónico o número de token) para el ingreso al correo electrónico. La identificación biométrica para el ingreso a la plataforma digital, notificaciones inmediatas por correo y mensajes de texto sobre compras realizadas, como también la geolocalización de las compras para asegurarse que las compras las está haciendo el propietario de la tarjeta. Estas son otras de medidas de seguridad efectivas que pueden implementarse.

4.2.2. ENTREVISTA NO ESTRUCTURADA – TESTIMONIOS DE ATENTADOS O CASOS DE FRAUDE

La entrevista se les aplicó a 60 personas de distintas edades entre 18 a 65 años, distribuidos en la misma cantidad entre personas del sexo masculino (30) y femenino (30). Entre los entrevistados, el 58% de ellos había sido víctima o conocía de alguien que había sufrido algún tipo de fraude. No se evidenció alguna relación entre el género del tarjetahabiente y la frecuencia de los casos de fraude dado que de los 36 entrevistados que fueron víctimas, 18 hombres y 18 mujeres. La figura 8 muestra el porcentaje de la frecuencia de los métodos de fraude reportados por los entrevistados.

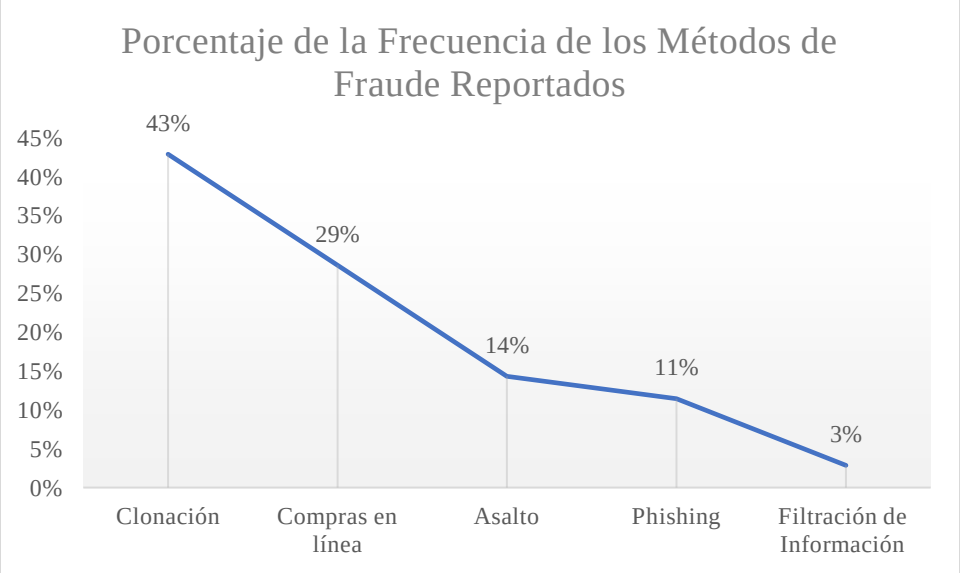

Figura 7. Porcentaje de la frecuencia de los métodos de fraude reportados. Elaboración: Propia.

La primera pregunta realizada fue "¿Ha sido víctima de un atentado o de un caso de fraude con su tarjeta de crédito o conoce de alguien que haya pasado por ello? ¿Qué sucedió?". Al responder, los entrevistados mencionan la facilidad en la que les clonaron su tarjeta de crédito mientras hacían sus compras diarias, que fue la estrategia de fraude más mencionada entre los

entrevistados (42% de los entrevistados de los que han sufrido algún tipo de fraude). La clonación se hizo en gasolineras, tiendas de conveniencia, cajeros automáticos y hasta un hospital público fue mencionado. Los entrevistados se percataron de lo sucedido cuando se notaron en sus estados de cuenta mensuales que se habían realizado compras en tiendas físicas, como ser supermercados o gasolineras en momentos que no concordaban con el horario que ellos tuvieron para los días en que ocurrieron las compras. La segunda estrategia más recurrente es la de robo de datos por compras en línea. Esto ocurrió cuando los entrevistados realizaban compras en páginas web que mostraban productos con jugosos descuentos que pueden considerarse anormales debido a la alta demanda de los productos que estaban siendo ofrecidos.

Los usuarios se percataron de ellas cuando vieron en sus estados de cuenta subscripciones a servicio digitales como “Amazon Prime” y compras realizadas desde Hong Kong en una unidad monetaria distinta a lo que son Lempiras. La tercera estrategia más utilizada es la de asalto a mano armada, que es un suceso de común ocurrencia en la capital. A los entrevistados los despojaron de sus pertenencias y los maleantes fueron inmediatamente a utilizar las tarjetas de crédito, que se encontraban en sus billeteras o carteras, antes de que el tarjetahabiente pueda reportarlo al banco y la tarjeta sea bloqueada. Las estrategias menos mencionadas fueron Phishing, que consistió en enviar mensajes por medio del correo electrónico haciéndose pasar por una entidad bancaria (ejemplo: Banco Atlántida, Ficohsa, BAC, etc.) o por una tienda de compras en línea (ejemplo: Amazon) solicitando la confirmación de una compra o “informando” falsamente sobre un acceso no autorizado sobre la cuenta del tarjetahabiente y es necesario poner los datos del cliente para poder ver que es lo ha sucedido; y, robo de información directamente desde el banco, en donde se filtra los datos de las tarjetas para su uso en línea. Cuando sucedió la filtración de la información, los bancos no informaron a los clientes lo sucedido e intentaron resolver estos problemas sin que

salieran a la luz pública pero estas compras autorizadas se vieron reflejadas en los estados de cuenta y los bancos tuvieron que confirmar lo sucedido cuando sus clientes reportaron las compras hechas de manera ilícita.

La segunda pregunta de la entrevista es "¿El banco le soluciono su problema? ¿Cómo lo hizo o porque no se pudo? Un 83% de los casos de fraude fueron resueltos por parte del banco, pero no todos ellos fueron solucionados fácilmente. La mayoría de los entrevistados contaban con seguro contra hurto, robo o extravío, por lo cual lo único que tuvieron que hacer para que el banco tomara cartas sobre el asunto es reportar lo sucedido. Este proceso demoró entre tres a seis meses. Para algunos entrevistados, los tiempos de respuesta por parte del banco duraron mucho tiempo o no había actualizaciones para que tranquilizar la incertidumbre del caso, por lo que tuvieron que llevar una queja formal o demanda a la CNBS para poder resolver el caso. A unos pocos de los entrevistados, el banco no proporciono una solución a tiempo y no insistieron en el proceso de reembolso, por lo que el banco únicamente se limitó a cancelar la tarjeta, pero no le devolvieron el dinero al tarjetahabiente.

La tercera pregunta fue "¿Cree usted que se pudo manejar mejor la situación?". La mayoría de los entrevistados mencionaron que estaban satisfechos con la manera en la que el banco que ellos utilizan manejó la situación y resaltaron la importancia de contar con el seguro contra hurto o extravío. Una menor porción de los entrevistados mencionó que, aunque ellos estaban contentos de haber recibido un reembolso por las compras inusuales y no tuvieron que pagar de su propio bolsillo, hubieran preferido que el tiempo de respuesta fuera más rápido. Unos pocos entrevistados recomendaron mejorar los sistemas de monitoreo de compras, dado que hay instancias en donde el banco reconoce que las compras son inusuales y proceden a cancelar la compra y a contactar al

tarjetahabiente para confirmar que la compra sea legítima, y en el caso de estos entrevistados, este mecanismo contra el fraude no detectó la actividad sospechosa.

La cuarta y última pregunta de la entrevista fue "¿Qué aprendió de esta situación?". En este espacio, la mayoría de los entrevistados recomendaron que es esencial contar con el seguro de hurto y extravío; también se mencionó que, como buena práctica, se debe revisar minuciosamente el estado de cuenta para cerciorarse que todas las transacciones son las correctas. Otros mencionaron que hay que ser precavido con los lugares físicos en donde realizan sus compras y algunos reiteraron que hay que corroborar la veracidad de las páginas web antes de realizar las compras en línea en sitios que desconocen. Unos pocos se encontraban tan descontentos con los resultados que mencionaron haber cambiado de banco inmediatamente debido a la falta de respuesta y servicio al cliente con su caso de fraude.

4.2.2. OBSERVACIÓN PARTICIPATIVA – PROCESO DE SOLICITUD DE TARJETA DE CRÉDITO

El viernes 19 de agosto de 2022 se realizaron dos solicitudes de tarjeta de crédito, de manera simultánea, a Banco Atlántida y a BAC Credomatic para realizar una comparación en sus procesos de entrega de tarjeta y la manera en la que capacitan a sus tarjetahabientes.

Para realizar la solicitud de una tarjeta de crédito en BAC bastó con llenar la hoja de solicitud y negociar cuanto sería el límite de crédito. En un lapso de tres días hábiles, el 24 de agosto, el banco contactó al solicitante para acordar fecha, hora y lugar para hacer entrega de la tarjeta de crédito. Durante la entrega de la tarjeta, se corrobora la identificación del solicitante, se revisan las condiciones generales del contrato y se le entrega al nuevo tarjetahabiente un folleto de educación financiera sobre las tarjetas de crédito. En este folleto es explica que es una tarjeta de

crédito y se presentan beneficios del uso de ella, se recomiendan buenas prácticas para evitar el endeudamiento y las consecuencias que conlleva caer en mora. En cuanto a estrategias preventivas contra el fraude, el folleto, recomienda revisar el estado de cuenta y llevar un control de los gastos. También se detallan los pasos para hacer un reclamo al banco y en caso de que el banco no responda la CNBS.

Para poder hacer la solicitud en Banco Atlántida, se tuvo que llenar un formulario en línea desde el teléfono móvil estando en el interior de una de sus sucursales. De manera inmediata, al finalizar, un representante del banco procedió a contactar, por medio de WhatsApp, al solicitante para corroborar los datos. Después se contactó un representante de la sucursal para llenar otro formulario y al finalizar, otro representante llamo al teléfono móvil del solicitante para acordar una lugar y fecha para hacer la solicitud formal. El solicitante esperó por 1 hora a que llegase el representante y procedió a llenar la solicitud de la tarjeta de crédito. Tres días hábiles después, el 24 de agosto, el banco contactó al solicitante para notificarle que llamarán a las referencias personales agregadas y que es necesario notificarles de antemano para que contesten las llamadas telefónicas. El banco se demoró 4 días hábiles adicionales y el 30 de agosto, llamó al solicitante para acordar un lugar y fecha para entrega de la tarjeta. Una vez entregada la tarjeta, se revisan los términos generales del contrato y se le entrega un folleto de educación financiera al nuevo tarjetahabiente. En este folleto se detallaban brevemente conceptos financieros relevantes a las tarjetas de crédito, se detallan los beneficios y servicios que otorga el uso de las tarjetas especificas del Banco Atlántida, comparte consejos de seguridad para utilizar el cajero automático y comparte los números a llamar en caso de hurto, robo y extravío. El folleto no detalla cómo hacer reclamos ante la CNBS.

4.3. RESULTADOS Y ANÁLISIS DE LOS DATOS ENCONTRADOS CON OTRAS TÉCNICAS

4.3.1. NUBE DE PALABRAS

En la siguiente figura se realizó una representación visual de la frecuencia de los métodos de fraude mencionados en la entrevista no estructurada:

Figura 8. Nube de palabras de la frecuencia de los métodos de Fraude.Fuente: Elaboración Propia.

4.3.2. DIAGRAMA DE ISHIKAWA

En el siguiente diagrama se puede visualizar los factores que contribuyen a la ejecución de las estrategias de fraude mencionadas por los entrevistados.

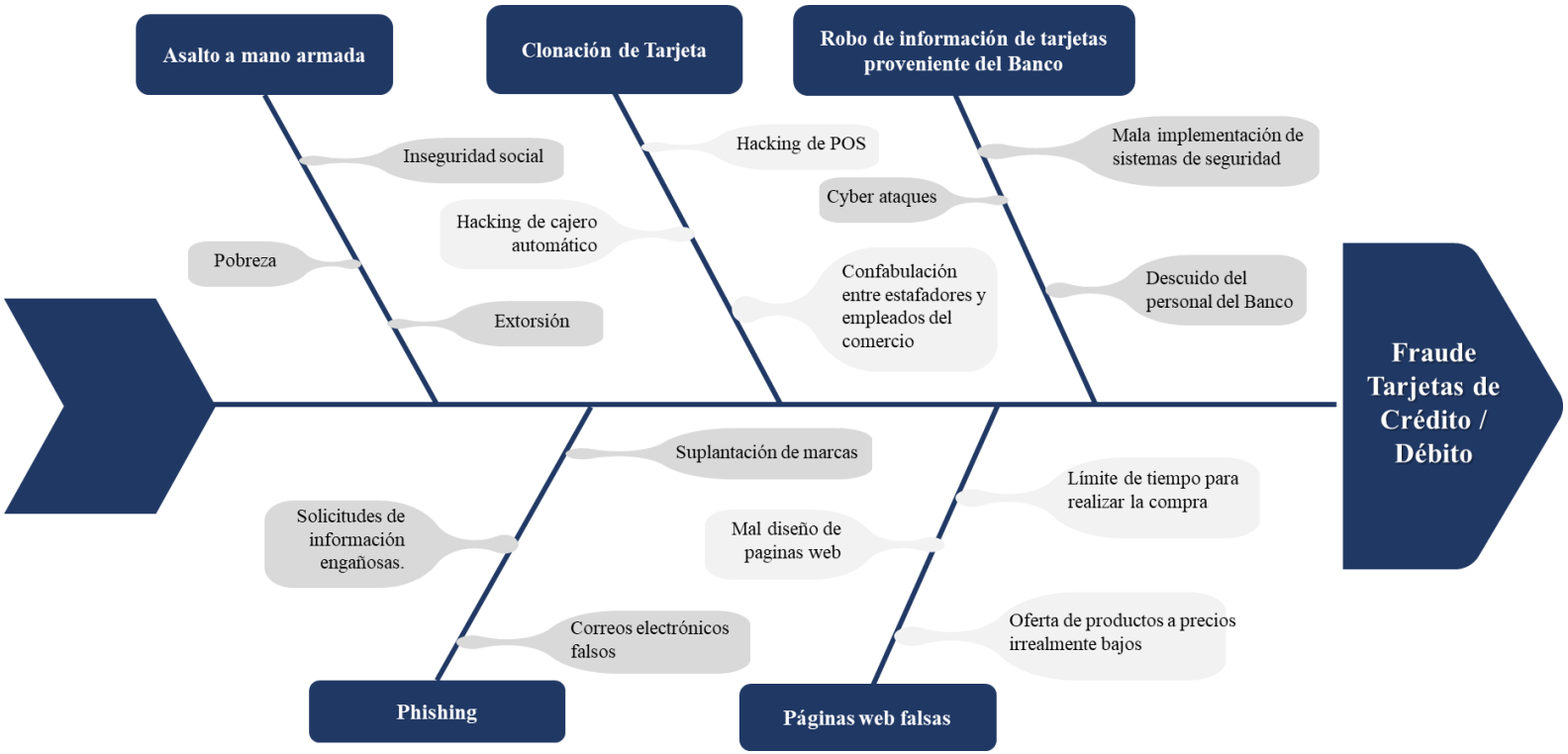

Figura 9. Diagrama de Ishikawa. Fraude de Tarjetas de Crédito en Tegucigalpa. Fuente: Elaboración: Propia

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se presentan las conclusiones y recomendaciones realizados en base a la información obtenida en las entrevistas y en la observación participativa; tomando en cuenta los objetivos específicos establecidos para el desarrollo de la presente investigación.

5.1. CONCLUSIONES

1. Así como los avances tecnológicos ofrecen nuevos métodos más convenientes para realizar los pagos de productos y servicios, además, las transacciones bancarias; también generan nuevos métodos de adquirir la información de las tarjetas de crédito y utilizarlas sin la necesidad de poseer el plástico en físico. La clonación de las tarjetas en puntos de venta no confiables (43%), compras en páginas de internet falsas (29%), correos electrónicos fraudulentos que solicitan información de las tarjetas haciéndose pasar por instituciones respetables (11%) y la filtración de información directamente desde el banco (3%) son los principales riesgos a los cuales los tarjetahabientes en Honduras están expuestos.
2. La confianza en las instituciones bancarias depende de su capacidad de respuesta a las necesidades y problemas de sus clientes, por lo que se utilizan las herramientas de capas de seguridad y la autenticación de dos pasos (proceso que valida la identidad del usuario mediante dos métodos de confirmación, como ser la solicitud de una contraseña o PIN único para el usuario, y como segundo paso, la confirmación por código enviado a número telefónico o número de token) para el ingreso al correo electrónico, la identificación biométrica para el ingreso a la plataforma digital, notificaciones inmediatas por correo y mensajes de texto sobre actividades de inicio de sesión y compras realizadas, como también

la geolocalización de las compras para asegurarse que las compras las está haciendo el propietario de la tarjeta.

3. Se requiere el desarrollo de una estrategia proactiva enfocada en la prevención de estafas y casos de fraude dirigida a los tarjetahabientes para concientizarlos sobre las formas en que pueden ser víctimas de fraude si no se toman medidas precautorias y la seriedad de las consecuencias que implican; de igual forma, enseñará a los tarjetahabientes las herramientas disponibles en la banca digital para contrarrestar las tácticas ilícitas empleadas para la obtención de datos de las tarjetas.

5.2. RECOMENDACIONES

1. Se recomienda a los tarjetahabientes la revisión minuciosa de sus estados de cuenta mensualmente para detectar movimientos inusuales que puedan resultar fraudulentos, independientemente del método utilizado por los delincuentes en estas actividades, y poder realizar los reclamos a tiempo sin temor a perder dinero. Pagar el seguro de tarjeta contra robo, hurto y extravío que protege al tarjetahabiente contra los casos de fraude y así evitar que éste se haga responsable de los gastos incurridos. No realizar compras en tiendas físicas que parezcan sospechosas o informales, tampoco en páginas web de procedencia dudosa, que no sean oficiales o que no muestren cumplir con medidas de seguridad estándares, como también no dejarse llevar por descuentos o promociones extraordinariamente bajas, ya que posiblemente se trate de una estafa.
2. Las instituciones bancarias deben asegurarse de mantener actualizadas sus herramientas de seguridad y monitoreo, debido a que no están exentas de algún malfuncionamiento o que, al estar desactualizadas, no se mitiguen correctamente los distintos escenarios de exposición al fraude. Ocurren instancias que estas herramientas no detectan las

irregularidades a tiempo, por ejemplo, alguna compra en el extranjero es tomada en cuenta como una compra regular, aunque ésta se salga del patrón de consumo del tarjetahabiente. Herramientas mundialmente reconocidas y de alta categoría, como Monitor Plus pueden utilizar los bancos para monitorear de forma efectiva, rápida y en tiempo real y las transacciones de sus tarjetahabientes.

3. Se recomienda a las instituciones bancarias implementar una campaña de publicidad contra el fraude de tarjetas de crédito en sus sucursales, redes sociales a nivel nacional y páginas web; y una estrategia de educación financiera para presentar brindar a los tarjetahabientes las herramientas y canales disponibles para su uso, o enfatizar sobre ellas en el caso de que ya las tengan. Esto con el propósito de actuar de manera preventiva en lugar de solo de forma reactiva como se hace comúnmente hoy en día, y así, mitigar el riesgo de exposición al fraude de sus tarjetahabientes, anticipándose de esta forma a los reclamos que puedan llevar a la insatisfacción de los clientes con la institución.

CAPITULO VI. APLICABILIDAD

6.1. NOMBRE DE LA PROPUESTA

Desarrollo de estrategia proactiva contra el fraude con tarjetas crédito en las principales instituciones bancarias en Honduras.

6.2. JUSTIFICACIÓN DE LA PROPUESTA

La presente investigación pretende desarrollar una estrategia proactiva contra el fraude con tarjetas de crédito en Honduras con el fin de que los bancos puedan implementar y mitigar el riesgo de fraude al momento que sus tarjetahabientes realizan compras en línea o de forma presencial.

En la actualidad el uso de las tarjetas de crédito se ha vuelto esencial en las actividades de consumo de las personas que optan por formas de pagos eficientes, rápidas y seguras. Sin embargo, los portadores de estas tarjetas deben tener presente que siempre existirá exposición al fraude por lo que es de suma importancia educarse para poder protegerse de forma efectiva contra los diversos métodos de fraude. Los bancos, como entidades emisoras de tarjetas, tienen la responsabilidad de brindar seguridad y confianza a sus tarjetahabientes al momento de realizar sus pagos. De igual forma, es necesario que, a través de todos los medios de comunicación posible, se les transmita información útil y relevante sobre medidas que pueden tomar para reducir las posibilidades de ser víctimas de fraude.

6.3 ALCANCE DE LA PROPUESTA

1. Presentar una estrategia proactiva que permita a los bancos y clientes anticiparse contra un intento de fraude al momento de utilizar sus tarjetas de crédito y como contrarrestar un nuevo método de fraude.
2. Aumentar los canales de comunicación al momento que los bancos buscan transmitir a sus clientes la mayor cantidad de información posible contra los diversos tipos de fraude.
3. Fomentar la educación permanente contra el fraude en los tarjetahabientes en Honduras, proporcionándoles información valiosa, actualizada y necesaria que sirva como escudo al momento de utilizar sus tarjetas de crédito.

6.4 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA

6.4.1 PROPUESTA DE ESTRATEGIA PROACTIVA CONTRA EL FRAUDE

Es responsabilidad del banco el cuidar de sus clientes contra cualquier tipo de situación en el cual puedan ser perjudicados al utilizar sus productos y servicios ofrecidos a ellos de terceros individuos con la intención de enriquecerse ilícitamente.

La presente propuesta consiste en un cambio de enfoque con el uso de cinco herramientas utilizadas por los bancos para comunicarse con sus clientes de todos los niveles para la concientización de los peligros del fraude con tarjetas de crédito, estas herramientas destinadas específicamente para la prevención contra el fraude son:

1. Bifolios informativos y educativos sobre la prevención del fraude.
2. Micrositio en página del banco creado específicamente para el tema del fraude.

3. Mensajes de texto a los teléfonos celulares (SMS) con alertas de prevención contra el fraude.
4. Incorporación de código QR e hipervínculo en estados de cuenta para redireccionar al tarjetahabiente hacia el micrositio.
5. Campañas publicitarias en medios tradicionales y redes sociales

Estas se utilizan comúnmente para anunciar a los clientes de nuevos productos lanzados por los bancos al mercado, los beneficios que se obtienen al utilizar los productos o servicios del banco, novedades en cuanto a las leyes financieras, transacciones realizadas en las cuentas de los clientes, promociones disponibles por tiempo limitado, entre otros; y esta estrategia proactiva hará uso de estos canales de comunicación para garantizar la transmisión de información útil contra la prevención del fraude. Aumentando el conocimiento de los tarjetahabientes sobre cuáles son las tácticas y métodos utilizados con mayor frecuencia en Honduras para ejecutar los fraudes a las tarjetas de crédito, y así poder anticiparse para evitar ser víctimas de dichas estafas. Asimismo, se habilitarán nuevas formas de contacto disponibles y de fácil acceso donde los clientes puedan exponer al banco los atentados de fraude.

6.4.2 DESARROLLO DE TODOS LOS ELEMENTOS NECESARIOS

6.4.2.1. BIFOLIO DE PREVENCIÓN CONTRA EL FRAUDE

El objetivo de la creación de un bifolio dedicado específicamente a la prevención contra el fraude es brindar información actualizada sobre dicho tema a los tarjetahabientes. Es oportuno entregar dicho bifolio de forma física al momento que se hace la entrega de la tarjeta al cliente, es decir, como parte del kit de entrega. Para tarjetas de crédito incluye copia del contrato, manual de educación financiera y el plástico como tal.

Por ende, tanto en la entrega de la tarjeta de crédito, se propone incluir el bifolio informativo con recomendaciones sobre la prevención contra el fraude. Considerando que la entrega de un nuevo producto a un cliente significa que el Banco tiene información actualizada de dicho cliente, por medio del correo electrónico debe enviarse el bifolio de forma digital, al momento que la tarjeta es activada. Se desea informar al cliente desde el inicio del ciclo de vida de su producto con el objetivo de que pueda anticiparse al fraude y conozca como protegerse del mismo.

6.4.2.2. MICROSITIO EN PÁGINA WEB

Esta estrategia engloba la creación de un micrositio dentro de la página web del banco, específicamente dedicado a la prevención del fraude. Lo que se pretende, es poner a disposición del cliente un sitio informativo que se mantenga actualizado respecto al tema y que permita a los clientes acceder fácilmente desde la página web oficial del banco, transmitiéndole así seguridad y confianza al cliente respecto a la veracidad de la información publicada.

En dicho micrositio, se pueden publicar artes publicitarios, video tutoriales, links informativos, testimonios de clientes que hayan sido víctimas de fraude y cualquier otro insumo que sirva para la prevención contra el fraude.

Adicional, en este micrositio, debe ponerse a disposición un correo electrónico destinado exclusivamente para el reporte de fraude. Es decir, que los clientes puedan reportar cualquier intento de fraude al que hayan sido expuestos, esto servirá para que el banco esté alerta a las nuevas formas en que los estafadores pretenden adueñarse de lo ajeno. Al conocer estas nuevas técnicas, el banco puede anticiparse para contrarrestar los métodos de fraude más común, implementando medidas de seguridad más efectivas.

6.4.2.3. MENSAJES DE TEXTO ALERTAS

Los mensajes de texto son herramientas que tienen disponibles los bancos para comunicar de forma breve pero concisa cualquier información de forma rápida a los clientes. Para hacer un uso eficiente del envío de los mensajes de texto a los números de celular actualizados, se recomienda que, con el apoyo de la inteligencia de negocios, se pueda extraer la base de los tarjetahabientes que realizan compras en línea. Al extraer esta base, se asegura de llegar a esos clientes que representan mayor riesgo al banco, ya que, basándose en el análisis del comportamiento de consumo de estos clientes, se pretende recordarles consejos básicos que fácilmente pueden ayudarles a prevenir un fraude.

6.4.2.4. ESTADOS DE CUENTA

Un estado de cuenta es un documento enviado mensualmente por las instituciones bancarias a los portadores de tarjetas de crédito con la información detallada sobre los movimientos efectuados con su tarjeta en un período de un mes con el fin de que el tarjetahabiente pueda verificar sus transacciones previo a realizar el pago correspondiente. Aprovechando que esta información ya es enviada al cliente, puede agregarse fácilmente información preventiva contra el fraude. Los estados de cuenta son enviados de forma digital, ya sea al correo electrónico y/o WhatsApp y también de forma impresa, según sea la preferencia del cliente.

Para los estados de cuenta impresos, se propone la incorporación de un arte publicitario con información respecto a la prevención del fraude, así como un código QR que pueda ser escaneado por los tarjetahabientes y los dirija automáticamente al micrositio dentro de la página web, donde puedan acceder fácilmente a toda la información actualizada y útil que es proporcionada por el banco.

Respecto a los estados de cuenta digitales, que son los que reciben los clientes a sus correos electrónicos y/o WhatsApp, mediante la incorporación de hipervínculos dentro del archivo (suele ser un PDF) que redirija a los tarjetahabientes al micrositio informativo en la página web.

6.4.2.5. CAMPAÑAS PUBLICITARAS

Las campañas publicitarias de la prevención contra el fraude son de mucha utilidad porque se logra llegar a un número alto de clientes por los distintos medios de comunicación que son aprovechados para este fin. Respecto a los medios digitales, se propone hacer uso de las redes sociales, como Facebook, Instagram y Twitter, así como también de los correos electrónicos para compartir a los tarjetahabientes toda la información posible. En el caso de las redes sociales, mediante pautas publicitarias pagadas, de forma agresiva se puede lograr concientizar a los tarjetahabientes y crear en ellos un sentido de responsabilidad al momento de utilizar sus tarjetas, con el fin que estén alertas ante cualquier escenario inusual.

WhatsApp puede ser una herramienta muy útil de igual forma, ya que la mayoría de los bancos disponen de cuentas oficiales en donde los clientes pueden comunicarse. Por ende, al momento que el cliente se comunica por este medio, previo a comenzar cualquier gestión, el primer mensaje que le aparezca sea una recomendación como prevención contra el fraude.

Los medios de comunicación tradicionales, como ser la televisión y la radio, siguen siendo canales para atraer la atención de los clientes, por lo que de igual forma deben utilizarse para educar a los tarjetahabientes.

El siguiente cuadro muestra un resumen indicativo de los indicadores que dan sustento a las iniciativas propuestas y que medidas de control de aplicarán con el fin de darle seguimiento mensual con el fin de realizar los ajustes correspondientes al plan propuesto:

Tabla 4. Resumen de indicadores de seguimiento al Plan de Actividades. Elaboración: Propia.

Iniciativas	Indicadores mensuales por iniciativa	Medidas de control de la estrategia	Resultados esperados
Bifolios	Número de bifolios entregados en físico.	• Número de incidentes de fraude • Número de clientes que han sido víctimas de fraude • Método de fraude más utilizado en el mes más reciente. • Monto total de pérdida.	• Aprovechar los canales de comunicación existentes para incorporar información educativa contra el fraude. • Crear nuevos medios para comunicarles información preventiva contra el fraude. • Reducir el número de incidentes de fraude. • Reducir el número de clientes víctimas de fraude. • Prevenir pérdidas originadas por los fraudes.
	Número de bifolios enviados por correo/WhatsApp.		
Micrositio	Número de visitas al micrositio.		
	Número de vistas a los videos tutoriales.		
	Número de visitas a los links.		
Mensajes de texto	Segmento de clientes que realizan compras en línea.		
	Número de mensajes enviados.		
Estados de Cuenta	Número de estados de cuenta enviados por correo.		
	Número de estados de cuenta enviados en físico.		
Campañas publicitarias	Estadística de la publicidad contra el fraude en redes sociales.		
	Actualización de publicidad de forma simultánea en todos los canales de comunicación.		
	Revisión del cumplimiento de las pautas en medios de comunicación.		

6.5. MEDIDAS DE CONTROL

Las siguientes medidas de control presentadas a continuación, serán útiles y necesarias para garantizar el seguimiento mensual de la estrategia con el fin de realizar los ajustes correspondientes a las distintas iniciativas para hacer uso eficiente de los recursos de la institución. El área de

Monitoreo debe asegurarse de extraer los siguientes datos de los sistemas con el fin de presentarlos al área de Imagen Corporativa/Marketing, para que ellos tengan información confiable y actualizada respecto a los fraudes presentados y la efectividad de las estrategias.

- Número de incidencias de fraude

Es el número de casos de fraudes presentados mensualmente.

- Monto total de pérdida

Es el monto total de pérdida que representan los fraudes presentados a la institución bancaria.

- Número de clientes que han sufrido fraudes

Es el número total de clientes que han sido víctimas de fraude mensualmente con el fin de validar si el fraude normalmente se presenta una o más veces en un mismo cliente.

- Método de fraude más utilizado en el mes más reciente

Conocer el método de fraude más comúnmente realizado mes a mes es importante para anticipar al cliente y enfocar la publicidad en contrarrestar este fraude de forma oportuna y eficiente.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

A continuación, se presenta el cronograma de actividades a seguir por iniciativa con el fin de desarrollar e implementar la estrategia de prevención contra el fraude y la estimación del presupuesto:

Tabla 5. Cronograma de Implementación Parte I. Elaboración: Propia.

Iniciativa	Actividades	Área Responsable	Semana I					Semana II					Semana III					Semana IV					Semana V					Semana VI					Semana VII					Semana VIII					Semana IX					Semana X					Semana XI					Semana XII				
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Bifolios	Definición de diseño bifolio e información a incluir	Imagen Corporativa / Marketing																																																										
	Versión final de los bifolios	Imagen Corporativa / Marketing																																																										
	Impresión de bifolios físicos	Imagen Corporativa / Marketing																																																										
	Entrega de bifolios físicos	Sucursales / Mensajerías																																																										
	Envíos de bifolios digitales	Imagen Corporativa / Marketing																																																										
Micrositio	Diseño de micrositio	Imagen Corporativa / Marketing																																																										
	Creación de micrositio	Imagen Corporativa / Marketing / Tecnología																																																										
	Implementación de micrositio	Imagen Corporativa / Marketing / Tecnología																																																										
Mensajes de texto	Definición de información a enviar en SMS	Imagen Corporativa / Marketing																																																										
	Envíos de SMS prevención contra fraude	Imagen Corporativa / Marketing																																																										
Estados de Cuenta	Definición de publicidad en estados de cuenta	Imagen Corporativa / Marketing																																																										
	Implementación de artes en estados de cuenta	Imagen Corporativa / Marketing																																																										
	Envíos de estados de cuenta con información contra fraude (según los cortes)	Imagen Corporativa / Marketing																																																										

Tabla 6. Cronograma de Implementación Parte II. Elaboración: Propia.

Iniciativa	Actividades	Área Responsable	Semana I					Semana II					Semana III					Semana IV					Semana V					Semana VI					Semana VII					Semana VIII					Semana IX					Semana X					Semana XI					Semana XII				
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Campaña publicitarias	Defínción de pauta publicitaria de medios	Imagen Corporativa / Marketing																																																								
	Campaña publicitaria en radio	Imagen Corporativa / Marketing																																																								
	Campaña publicitaria en televisión	Imagen Corporativa / Marketing																																																								
	Campaña publicitaria en redes sociales	Imagen Corporativa / Marketing																																																								
	Campaña publicitaria por correos electrónico	Imagen Corporativa / Marketing																																																								
Seguimiento Campaña	Obtención de resultados indicadores de fraude	Tecnología / Monitoreo																																																								
	Presentación de resultados	Tecnología / Monitoreo																																																								
	Ajustes en campañas publicitarias	Imagen Corporativa / Marketing																																																								

El siguiente presupuesto es una estimación de la inversión aproximada por un período de 3 meses que tendrían que realizar las distintas instituciones bancarias (se toma como referencia el tamaño de las principales instituciones bancarias colocadoras de tarjetas de crédito, como ser BAC Credomatic, Banco Atlántida y Ficohsa) con el fin de implementar las estrategias presentadas anteriormente. Las cantidades y precios pueden variar. Sin embargo, es importante mencionar que en los casos donde materialice un fraude, primero, debe conocerse a detalle el origen del fraude para mitigar el riesgo, es decir, apoyarse en el equipo de auditoría interna para mayor transparencia y veracidad de los hechos. En segundo, a lo interno, con el objetivo de prevenir otro fraude la misma índole, deben aplicarse medidas correctivas eficientes ya sea en los procesos, ajustes en las políticas, restricciones en los permisos de acceso de los usuarios, etc. Por último, debe prevenirse nuevamente un fraude de este tipo, es decir, tanto a los clientes internos como externos, debe educárseles sobre este método fraude empleado por los estafadores y como anticiparse a ser víctimas de éste. Mes a mes, con base en

los resultados obtenidos del área de Monitoreo, la estrategia puede ajustarse siempre con el fin de continuar contrarrestando el fraude de forma eficiente.

Tabla 7. Presupuesto para el desarrollo de la estrategia. Fuente: Elaboración Propia.

Iniciativa	No.	Actividades	Costo unitario	Cantidad	Costo mensual	I Mes		II Mes		III Mes	
						Costo	Observaciones	Costo	Observaciones	Costo	Observaciones
Bifolios	1	Definición de diseño bifolio e información a incluir	L 2.000,00	N/A	L 2.000,00	L -		L -		L -	
	2	Impresión de bifolios físicos	L 2,00	10.000	L 20.000,00	L 20.000,00	*Monto fijo.*	L 20.000,00	*Monto fijo.*	L 20.000,00	*Monto fijo.*
	3	Envíos de bifolios digitales (HTML)	L 1,23	5.000	L 6.150,00	L 6.150,00	*Monto fijo.*	L 6.150,00	*Monto fijo.*	L 6.150,00	*Monto fijo.*
Micrositio	4	Diseño, creación e implementación de micrositio	L 49.200,00	N/A	L 49.200,00	L -		L -		L -	
	5	Mantenimiento micrositio	L 6.150,00	N/A	L 6.150,00	L 6.150,00	*Monto fijo.*	L 6.150,00	*Monto fijo.*	L 6.150,00	*Monto fijo.*
Mensajes de texto	6	Envíos de SMS prevención contra fraude	L 1,48	30.000	L 44.280,00	L 88.560,00	*Monto fijo si se envían 2 SMS a cada tarjetahabiente.*	L 88.560,00	*Monto fijo si se envían 2 SMS a cada tarjetahabiente.*	L 88.560,00	*Monto fijo si se envían 2 SMS a cada tarjetahabiente.*
Estados de Cuenta	7	Definición de publicidad en estados de cuenta	L 3.000,00	1	L 3.000,00	L -		L -		L -	
	8	Implementación de artes en estados de cuenta	L 2.000,00	1	L 2.000,00	L -		L -		L -	
Campaña publicitaria	9	Cuña en radio	L 500,00	60	L 30.000,00	L 30.000,00	*Campaña publicitaria en este medio al 100%.*	L 27.000,00	*Campaña publicitaria en este medio al 90%.*	L 24.000,00	*Campaña publicitaria en este medio al 80%.*
	10	Mención en televisión	L 16.605,00	N/A	L 16.605,00	L 16.605,00		L 14.944,50		L 13.284,00	
	11	Pauta publicitarias en redes sociales	L 36.900,00	N/A	L 36.900,00	L 36.900,00		L 33.210,00		L 29.520,00	
	12	Envío de HTML en correo electrónico	L 1,23	30.000	L 36.900,00	L 36.900,00		L 33.210,00		L 24.000,00	
					L 253.185,00	**L 241.265,00**		**L 229.224,50**		**L 211.664,00**	

Consideraciones del presupuesto:

- Es importante resaltar que los costos unitarios son estimaciones según en lo que oscilan los precios actualmente en el mercado hondureño. Las cantidades son variables y flexibles según el tamaño de la institución bancaria y el número de tarjetahabientes.
- Inciso 1 del presupuesto (diseño del bifolio): el diseño del bifolio es un costo único en el que se incurre al momento de diseñarlo.
- Incisos 2 y 3 del presupuesto (impresión y envíos de bifolios): la cantidad de impresiones, así como de los envíos, son variables dependiendo de la cantidad de tarjetas de crédito que sean entregadas mensualmente, pero se dejan fijas por los primeros 3 meses del desarrollo de la estrategia.
- Incisos 4 y 5 del presupuesto (micrositio): la creación del micrositio es un costo único en el que debe incurrir la institución por su implementación, y el mantenimiento es un costo fijo mensual.
- Inciso 6 del presupuesto (envío de mensajes de textos): se estima que se enviarán 2 mensajes de texto mensuales a treinta mil clientes por los primeros 3 meses de la estrategia.
- Incisos 7 y 8 del presupuesto (estados de cuenta): la publicidad de los estados de cuenta será un costo único para los primeros 3 meses de la estrategia, en caso de que se desee modificarla posteriormente e implementarla en los PDF de los estados de cuenta nuevamente, se incurrirá en dicho costo.
- Incisos 9 al 12 (campaña publicitaria): se iniciará de forma agresiva el primer mes, asumiendo los costos al 100%, para el segundo mes se hará una reducción de las cantidades y costos y se dejará todo al 90% y en el último mes, se dejará todo en un 80% para revisar la efectividad de la campaña al finalizar el primer trimestre.

6.7 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 8. Concordancia de los segmentos de la tesis con la propuesta - Parte 1. Elaboración: Propia.

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título Investigación	**Objetivo General**	**Objetivos Específico**	**Teorías/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
Desarrollo de estrategia proactiva contra el fraude con de tarjetas crédito en las principales instituciones bancarias en Honduras.	Desarrollar una estrategia proactiva que ayude a mitigar los fraudes y estafas en los tarjetahabientes de las principales instituciones bancarias colocadoras de tarjetas de crédito en Honduras que fomente el comercio electrónico.	Conocer los principales riesgos de fraude a los que están expuestos los tarjetahabientes al momento de realizar compras en línea.	Triangulo de Fraude, Convergencia entre nativos digitales e inmigrantes digitales	Fraude	Tarjetahabientes víctimas de un atentado o fraude con tarjetas de crédito	Entrevista no estructurada	Así como los avances tecnológicos ofrecen nuevos métodos más convenientes para realizar los pagos de productos y servicios, además, las transacciones bancarias; también generan nuevos métodos de adquirir la información de las tarjetas de crédito y utilizarlas sin la necesidad de poseer el plástico en físico. La clonación de las tarjetas en puntos de venta no confiables (43%), compras en páginas de internet falsas (29%), correos electrónicos fraudulentos que	Desarrollo de estrategias proactivas contra el fraude con tarjetas crédito en Honduras.	Objetivo general: Presentar una estrategia viable que puedan aplicar las principales instituciones bancarias emisoras de tarjetas de crédito en Honduras con el fin de preparar a sus tarjetahabientes contra el fraude. Objetivos específicos: Implementar una estrategia publicitaria agresiva que de prevención contra el fraude. Aumentar el conocimiento de los tarjetahabientes sobre las medidas
				Estafa	Expertos en temas de fraude electrónico en el rubro de las instituciones bancarias en Honduras	Entrevista estructurada			
				Tarjetahabiente					
				Comercio electrónico					

							solicitan información de las tarjetas haciéndose pasar por instituciones respetables (11%) y la filtración de información directamente desde el banco (3%) son los principales riesgos a los cuales los tarjetahabientes en Honduras están expuestos.		de seguridad que pueden aplicar para reducir la posibilidad de ser víctimas del fraude. Fomentar el uso seguro y consciente de las tarjetas de crédito para compras y demás transacciones en línea.

Tabla 9. Concordancia de los segmentos de la tesis con la propuesta - Parte 2. Elaboración: Propia.

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título Investigación	**Objetivo General**	**Objetivos Específico**	**Teorías/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
Desarrollo de estrategia proactiva contra el fraude con de tarjetas crédito en las principales instituciones bancarias en Honduras.	Desarrollar una estrategia proactiva que ayude a mitigar los fraudes y estafas en los tarjetahabientes de las principales instituciones bancarias colocadoras de tarjetas de crédito en Honduras que fomente el comercio electrónico.	Identificar las medidas de seguridad efectivas que puedan implementar los bancos con el fin de mitigar el riesgo de que sus tarjetahabientes sean víctimas del fraude. .	Triangulo de fraude, Convergencia entre nativos digitales e inmigrantes digitales	Banco comercial Comercio electrónico Estafa	Expertos en temas de fraude electrónico en el rubro de las instituciones bancarias en Honduras	Entrevista estructurada Observación participativa	La confianza en las instituciones bancarias depende de su capacidad de respuesta a las necesidades y problemas de sus clientes, por lo que se utilizan las herramientas de capas de seguridad y la verificación de dos pasos para el ingreso al correo electrónico, la identificación biométrica para el ingreso a la plataforma digital, notificaciones inmediatas por correo y mensajes de texto sobre actividades de inicio de sesión y compras realizadas, como también la geolocalización de las compras para asegurarse que las compras las está haciendo el	Desarrollo de estrategias proactivas contra el fraude con tarjetas crédito en Honduras.	Objetivo general: Presentar una estrategia viable que puedan aplicar las principales instituciones bancarias emisoras de tarjetas de crédito en Honduras con el fin de preparar a sus tarjetahabientes contra el fraude. Objetivos específicos: Implementar una estrategia publicitaria agresiva que de prevención contra el fraude. Aumentar el conocimiento de los

							propietario de la tarjeta.		tarjetahabientes sobre las medidas de seguridad que pueden aplicar para reducir la posibilidad de ser víctimas del fraude. Fomentar el uso seguro y consciente de las tarjetas de crédito para compras y demás transacciones en línea.

Tabla 10. Concordancia de los segmentos de la tesis con la propuesta - Parte 3. Elaboración: Propia.

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI	
Título Investigación	**Objetivo General**	**Objetivos Específico**	**Teorías/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la propuesta**	**Objetivos propuesta**
Desarrollo de estrategia proactiva contra el fraude con de tarjetas crédito en las principales instituciones bancarias en Honduras.	Desarrollar una estrategia proactiva que ayude a mitigar los fraudes y estafas en los tarjetahabientes de las principales instituciones bancarias colocadoras de tarjetas de crédito en Honduras que fomente el comercio electrónico.	Elaborar una estrategia proactiva que puedan implementar las instituciones bancarias para contrarrestar los fraudes que se presentan en los canales digitales.	Triangulo de Fraude.	Banco	Tarjetahabientes víctimas de un atentado o fraude con tarjetas de crédito	Entrevista estructurada	Se requiere el desarrollo de una estrategia proactiva enfocada en la prevención de estafas y casos de fraude dirigida a los tarjetahabientes para concientizarlos sobre las formas en que pueden ser víctimas de fraude si no se toman medidas precautorias y la seriedad de las consecuencias que implican; de igual forma, enseñará a los tarjetahabientes las herramientas disponibles en la banca digital para contrarrestar las tácticas ilícitas empleadas para la obtención de	Desarrollo de estrategia proactiva contra el fraude con de tarjetas crédito en las principales instituciones bancarias en Honduras	Objetivo general: Presentar una estrategia viable que puedan aplicar las principales instituciones bancarias emisoras de tarjetas de crédito en Honduras con el fin de preparar a sus tarjetahabientes contra el fraude. Objetivos específicos: Implementar una estrategia publicitaria agresiva que de prevención contra el fraude.
				Tarjetahabiente	Expertos en temas de fraude electrónico en el rubro de las instituciones bancarias en Honduras	Observación participativa			
				Comercio electrónico.		Entrevista no estructurada			

							datos de las tarjetas.		Aumentar el conocimiento de los tarjetahabientes sobre las medidas de seguridad que pueden aplicar para reducir la posibilidad de ser víctimas del fraude. Fomentar el uso seguro y consciente de las tarjetas de crédito para compras y demás transacciones en línea.

REFERENCIAS BIBLIOGRÁFICAS

Agencia EFE. (2021, octubre 21). *La banca digital acelera su consolidación en América Latina por la covid-19*. www.efe.com. https://www.efe.com/efe/america/economia/la-banca-digital-acelera-su-consolidacion-en-america-latina-por-covid-19/20000011-4657478

Alvarez, M. A. (2001). *Qué es HTML*. https://desarrolloweb.com/articulos/que-es-html.html

Arimetrics. (2020a, enero 29). *Qué es Contactless—Definición, significado y ejemplos*. https://www.arimetrics.com/glosario-digital/contactless

Arimetrics. (2020b, enero 29). *Qué es el Código QR - Definición, significado y ejemplos*. https://www.arimetrics.com/glosario-digital/codigo-qr

Artieda-Rojas, J. R., Andrade, R. I. M., Espinoza, M. S. M., & Tirado, P. S. O. (2017). *El trueque como sistema de comercialización—Desde lo ancestral a lo actual*. https://dialnet.unirioja.es/servlet/articulo?codigo=6756265

BBVA. (2015, agosto 22). Diferencias entre banca comercial y banca de inversiones. *BBVA NOTICIAS*. https://www.bbva.com/es/banca-comercial-banca-inversiones/

BBVA. (2022a, septiembre 23). *Características del titular de la tarjeta de crédito.* https://www.bbva.es/finanzas-vistazo/ef/tarjetas/caracteristicas-del-titular-de-la-tarjeta-de-credito.html

BBVA. (2022b, septiembre 24). *¿Qué es la adquirencia?* https://www.bbva.com.ar/economia-para-tu-dia-a-dia/ef/adquirencia/que-es-la-adquirencia.html

BigCommerce. (2022, agosto 13). *Mobile Commerce 101: M-Commerce Trends + Stats (Updated for 2022)* (https://www.bigcommerce.com/) [Text/html]. BigCommerce; BigCommerce. https://www.bigcommerce.com/articles/ecommerce/mobile-commerce/

CNBS. (s/f). *La tarjeta de crédito*. CNBS - GPUF - Educación Financiera. Recuperado el 18 de agosto de 2022, de https://gpuf.cnbs.gob.hn/educacionfinanciera/prestamos-y-creditos/la-tarjeta-de-credito/

CNBS. (2020). *Proyecto Robo de Datos y Fraude a través de Canales Digitales*. CNBS.

CNBS. (2021a). *Reporte de Inclusión Financiera*. CNBS.

CNBS. (2021b). *Reporte de Inclusión Financiera en Honduras*. Comision Nacional de Bancos y Seguros. https://www.cnbs.gob.hn/wp-content/uploads/2021/05/Reporte-de-Inclusion-Financiera-2021.pdf

CNBS. (2022). *Tarjetas de Crédito en el Mercado y Monto Otorgado*. https://publicaciones.cnbs.gob.hn/boletines/_layouts/15/xlviewer.aspx?id=/boletines/Tarjetas%20de%20Crdito%20Mercado%20y%20Monto%20Otorgado/Tarjetas%20de%20Cr%C3%A9dito.xlsx&Source=https%3A%2F%2Fpublicaciones%2Ecnbs%2Egob%2Ehn%2Fboletines%2FPaginas%2FTarjetas%2Dde%2DCr%25C3%25A9dito%2Den%2Del%2DMercado%2Easpx%23hide2022

CNI. (2020, abril 20). E-commerce: La mejor alternativa para los negocios. *Consejo Nacional de Inversiones - Honduras*. https://www.cni.hn/e-commerce-la-mejor-alternativa-para-los-negocios/

Cornell Law School, G. (2008, octubre 8). *Fraude con Tarjeta de Crédito*. LII / Legal Information Institute. https://www.law.cornell.edu/wex/es/fraude_con_tarjeta_de_cr%C3%A9dito

Díaz, M. (s/f). *Técnicas e instrumentos de investigación.* Universidad de la Costa. https://eduvirtual.cuc.edu.co/moodle/pluginfile.php/618544/mod_resource/content/1/T%C3%A9cnicas%20y%20m%C3%A9todos%20inv.pdf

Díaz, T. (2018, agosto 9). ¿Qué son las nubes de palabras? | Definición de nube de tags | Negocio online. *Economía Simple*. https://www.economiasimple.net/glosario/nube-de-palabras

elEconomista.es. (s/f). *Banca electrónica: Qué es - Diccionario de Economía - elEconomista.es*. Recuperado el 11 de noviembre de 2022, de https://www.eleconomista.es/diccionario-de-economia/banca-electronica

Escalas. (2019, enero 21). Delito de Estafa: Características, elementos del delito y penas. *Conceptos Jurídicos*. https://www.conceptosjuridicos.com/estafa/

Escuela Europea de Excelencia. (2021, junio 1). Mitigación de riesgos: Proceso de 3 pasos para hacer frente al riesgo. *Escuela Europea de Excelencia*. https://www.escuelaeuropeaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/

Galán, J. S. (2017, enero). *Banco comercial—Definición, qué es y concepto*. Economipedia. https://economipedia.com/definiciones/banco-comercial.html

Gallo, M. (2021, noviembre). *Análisis de Procesos* [Explicativo]. Clase Gestion de Operaciones y Logística, Tegucigalpa.

Goulding, S. (2018, marzo). *The Evolution of Fraud*. Transunion. https://www.transunion.co.uk/blog/the-evolution-of-fraud

Hernández Sampieri, R. (2014). *Metodología de la Investigación 6ta edición* (6ta ed.).

Hernández Sampieri, R., & Fernández Collado, C. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

Hidalgo, I. I. V. (2005). *Tipos de estudio y métodos de investigación*. 12.

IBERDROLA CORPORATIVA. (2022). *Ataques cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos?* Iberdrola. https://www.iberdrola.com/innovacion/ciberataques

INCIBE. (2020, junio 17). *Hacker vs. Ciberdelincuente*. INCIBE. https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente

Kapersky. (2021, diciembre 9). *¿Qué es la Deep Web y la Dark Web?* www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/deep-web

Kr. Kashyap, N., B. K., P., H. L., M., & Kumar, A. (2016). *A Comprehensive Study of Various Kinds of Frauds & It's Impact* (SSRN Scholarly Paper Núm. 2838747). https://papers.ssrn.com/abstract=2838747

Lehr, L. (2020). *Digital banking in Latin America: Best practices and the shift toward banking as a service* (A Whitepaper by Mastercard and Americas Market Intelligence). https://newsroom.mastercard.com/latin-america/files/2020/04/AMI_2020_Mastercard_Digital_Banking_in_Latin_America_Best_Practices_English1.pdf

Ley de Tarjetas de Crédito, núm. DECRETO No. 306-2006 (2006).

López, W., & Sánchez, J. (2012). *El triángulo del fraude*. *17*. https://www.redalyc.org/pdf/631/63124039003.pdf

Luna, M., & Sierra, J. (2022). *PROPUESTA PARA IMPLEMENTAR UNA SOLUCIÓN DE INTELIGENCIA DE NEGOCIOS APLICADA AL CANAL CUSTOMER SUCCESS DE TIGO BUSINESS* [Descriptivo]. UNITEC.

Mastercard. (2022, abril 28). *Honduras experimenta un encanto paulatino con la inclusión financiera y digitalización de su economia*. https://www.mastercard.com/news/latin-america/es/sala-de-prensa/comunicados-de-prensa/pr-es/2022/abril/honduras-experimenta-un-encanto-paulatino-con-la-inclusion-financiera-y-digitalizacion-de-su-economia/

Mckenna, F. (2022, julio 22). The Story of the Very First Case of Credit Card Fraud. *Frank on Fraud*. https://frankonfraud.com/fraud-trends/first-credit-card-fraud-case-was-in-1899/

Merchant, I. (2021). *El Estado de la Banca Digital en América Latina | MMA Global*. https://www.mmaglobal.com/research/el-estado-de-la-banca-digital-en-america-latina

Microsoft Corporation. (2022). *Fraude en comercio electrónico online | Microsoft Dynamics 365*. https://dynamics.microsoft.com/es-es/ai/fraud-protection/online-ecommerce-fraud/

Orús, A. (2022, julio). *Tema: Comercio electrónico en el mundo*. Statista. https://es.statista.com/temas/9072/comercio-electronico-en-el-mundo/

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, *35*(1), 227–232. https://doi.org/10.4067/S0717-95022017000100037

Panda Security. (s/f). *¿Qué es el Phishing? - Panda Security*. Recuperado el 25 de septiembre de 2022, de https://www.pandasecurity.com/

Park, S. (2022, marzo 31). *Chile lidera entre los países de América Latina que más utilizan tarjetas para pagos*. AméricaEconomía | AméricaEconomía. https://www.americaeconomia.com/tecnologia-innovacion/chile-lidera-pagos-con-tarjeta

Perez. (2021). *Definición de fraude—Definicion.de*. Definición.de. https://definicion.de/fraude/

PYMNT. (2021, septiembre 24). *Opportunities for PSPs in Latin America*. https://www.pymnts.com/digital-payments/2021/deep-dive-latin-america-payments-ecosystem-psp-opportunity/

RAE. (2021). *Tarjetahabiente | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario. https://dle.rae.es/tarjetahabiente

Restrepo, J., & Rojas, C. (2021). *Incidencia del uso de tarjetas de crédito como medio de pago en los jóvenes de 18 a 25 años en la ciudad de Santiago de Cali en el año 2020* [UNIVERSIDAD LIBRE SECCIONAL CALI]. https://hdl.handle.net/10901/20601

Rodríguez, L. (2022, abril 26). *Los fraudes en la banca: ¿cómo protegerse?* www.laprensa.hn. https://www.laprensa.hn/economia/dineroynegocios/fraudes-banca-como-protegerse-digital-honduras-NB7838168

Rolfe, A. (2021, junio 17). *The payments landscape: How Latin Americans pay for e-commerce*. Payments Cards & Mobile. https://www.paymentscardsandmobile.com/the-payments-landscape-how-latin-americans-pay-for-e-commerce/

Ryte Wiki. (2021). *¿Qué es un Micrositio?* https://es.ryte.com/wiki/Micrositio

Sabates, L., & Roca, J. (2020, abril 23). *La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad* [Explicativo]. https://ddd.uab.cat/pub/recdoc/2020/222109/revliltcie_a2020.pdf

Steele, J. (2021, junio 11). *Credit card fraud and ID theft statistics*. CreditCards.Com. https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/

Universidad La Concordia. (2020, julio 28). Técnicas de investigación para universitarios. *Mundo ULC*. https://universidadlaconcordia.edu.mx/blog/index.php/tecnicas-de-investigacion/

Valdez, F. (2022). *La Concepción del Dinero y las Tarjetas de Crédito como una de las Principales Formas Digitales del Valor en Guatemala.*

Ventura, A. L. (2021). *Global Finance Magazine—World's Most Unbanked Countries 2021*. Global Finance Magazine. https://www.gfmag.com/global-data/economic-data/worlds-most-unbanked-countries

VISA. (2014). *Qué es e-commerce o comercio electrónico*. https://www.visa.com.hn/run-your-business/pymes/notas-y-recursos/Tecnologia/que-es-ecommerce-o-comercio-electronico.html

Westreicher, G. (2022a). *Digitalización—Qué es, definición y concepto*. https://economipedia.com/definiciones/digitalizacion.html

Westreicher, G. (2022b). *Muestreo por conveniencia*. Economipedia. https://economipedia.com/definiciones/muestreo-por-conveniencia.html

GLOSARIO

- Adquirencia:

  Es el proceso que se realiza al pagar con tarjeta. Cuando el comerciante recibe el plástico y se pasa por la terminal POS para concretar la transacción. La terminal se encarga de recoger los datos de la tarjeta y enviarlos a la entidad emisora para comprobar que la operación pueda realizarse y la venta se acredite (BBVA, 2022, Sección ¿Qué es la adquirencia?).

- Ciberataque: “es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas” (IBERDROLA Corporativa, 2022, Sección Ciberataques).
- Ciberdelincuente: “es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware” (INCIBE, 2020, Sección Hacker vs. Ciberdelincuente.).
- Código QR:

  Un código QR (Quick Response por sus siglas en inglés) es un tipo de código de barras bidimensionales que solo se puede leer con teléfonos inteligentes u otros dispositivos dedicados a la lectura de estos códigos. Cuando se lee un código QR, los dispositivos se conectan directamente a mensajes de texto, correos electrónicos, sitios web, números de teléfono, etc (Arimetrics, 2020, Sección Definición).

- Contactless: “es el término que se aplica a la tecnología que permite realizar operaciones “sin contacto” mediante un sistema de comunicación denominado NFC. Se utiliza con

tarjetas de crédito, teléfonos móviles, relojes inteligentes o llaveros" (Arimetrics, 2020, Sección Definición).

- Deep web:

  > Es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales (Kapersky, 2021,Sección ¿Qué es la Dark Web, la Deep Web y la web superficial?).

- HTML: "es el lenguaje con el que se define el contenido de las páginas web. Trata de un conjunto de etiquetas que sirven para definir el texto y otros elementos que compondrán una página web, como imágenes, listas, vídeos, etc" (Alvarez, 2001,Sección Manuales).
- Micrositio: "es un sitio web que extiende o amplía la información y funcionalidades de un sitio web principal. Normalmente un micrositio está vinculado al sitio web principal pero se centra en solo algunos puntos específicos (Ryte Wiki, 2021, Sección Definición).
- Titular de tarjeta: "el titular de la tarjeta de crédito es toda aquella persona física (o particular) que solicita una tarjeta y cuyo nombre aparece grabado en la misma" (BBVA, 2022, Sección Tarjetas).
- Phishing: "es el envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial" (Panda Security, s.f., Sección Seguridad).

ANEXOS

ANEXO 1: RESPUESTAS DE ENTREVISTAS REALIZADAS A EXPERTOS

Experto 1

Datos Generales

Género: Masculino

Edad: 35

Años de experiencia en temas de tarjetas de crédito y fraude: 9

Preguntas

1. Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted que es esencial para que el tarjetahabiente se anticipe a un fraude al momento que adquiere su primera tarjeta de crédito/débito?

Dar a conocer las medidas de seguridad como ser temas de pin de la tarjeta, la explicación del seguro contra fraude, los diferentes métodos de fraude que existen como ser Web skimming, malware, phishing, etc.

2. ¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito/débito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?

El error más común es confiar en cualquier página web, sin verificar los temas de seguridad como ser certificados, la comprobación de protocolos SSL.

Una de las recomendaciones es que se tenga una cuenta asociada a una TD o TC exclusiva para estos temas, así se evitan mayores fraudes, también verificar las “ofertas” si no son creíbles, en las cuales se ven involucrados muchos fraudes

3. ¿Cuáles son algunas de las transacciones con tarjeta de crédito/débito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?

Definitivamente las compras en páginas que no son seguras o de confiabilidad, no son sitios web con especialidad en compras, también proporcionando la más mínima cantidad de información posible.

4. ¿Que considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?

Definitivamente la activación o desactivación de las tarjetas en la banca en línea, creo que actualmente solo BAC tiene esa opción.

5. Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?

Se ha complicado el tema, con el pasar del tiempo se implementan nuevas técnicas sofisticadas de fraude, algunas que no se detectan, por lo cual las empresas deben ir actualizando los componentes de seguridad.

Uno de los factores importantes en el cual se ha dificultado el tema de prevención es la falta de cultura del cliente en no brindar información personal en los temas de phishing.

6. Según su experiencia, en los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?

Sin dudarlo, diría que es el phishing.

7. Según la respuesta anterior ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?

Mas que todas campañas de concientización a los clientes para evitar caer en temas, y reportar para colocar bloqueos de sitios o dominios sospechosos en los sistemas del banco.

8. ¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito/débito para reducir la exposición al fraude?
    - Definitivamente las campañas de concientización para clientes y usuarios, también para empleado interno.
    - La adopción de capas de seguridad en correos, y otras plataformas como ser la identificación biométrica, la verificación de dos pasos, notificaciones por correo y SMS sobre actividades de inicio de sesión y compras.
    - Geolocalización de las compras, para saber dónde se producen las mismas.
    - Implementación del chip en las TC y TD
9. ¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?

    Sin contestar
10. Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?

Actualmente es el medio más importante para realizar conciencia de prevención, subiendo las campañas a dichas redes se tendría un mayor alcance.

11. ¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué? Considerando que por ejemplo una tarjeta de crédito negra tiene límite alto y las de débito del mismo color normalmente disponen un monto elevado de efectivo.

Cada institución financiera tiene reglas de fraude y límites de compra, diferentes para cada tarjeta, definitivamente a mayor limite mayor posibilidad de fraude, pero también a mayor limite mayor restricción en reglas de compras por el mismo tema, definitivamente esto es a criterio de cada institución financiera.

Experto 2

Datos Generales

Género: Masculino

Edad: 35

Años de experiencia en temas de tarjetas de crédito/débito y fraude: 11

Preguntas

1. Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted que es esencial para que el tarjetahabiente se anticipe a un fraude al momento que adquiere su primera tarjeta de crédito/débito?

   A nivel de Sistemas de Información siempre el punto más vulnerable es el factor humano, por eso es de suma importancia que el ente emisor pueda proporcionar al nuevo tarjetahabiente un curso introductorio con el uso correcto de su plástico para la prevención del fraude, con temas como:

   - No comparta la información de su cuenta.
   - Proteja sus cuentas usando un sistema de autenticación de múltiples factores cuando esté disponible.

- Vigile sus cuentas.
- En cuanto a sus tarjetas de crédito, abra y revise enseguida los resúmenes de cuenta.
- Mantenga sus tarjetas, códigos PIN, recibos y boletas de depósito en un lugar seguro y descártelos cuidadosamente.

2. ¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito/débito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?

   El error más común que comete el usuario el compartir su información confidencial recomendaciones como: No dé el número de su cuenta por teléfono, a menos que usted haya efectuado la llamada y conozca el motivo por el que tiene que dar ese dato. Nunca deje la información de su cuenta a la vista de los demás.

3. ¿Cuáles son algunas de las transacciones con tarjeta de crédito/débito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?

   Es muy difícil sacar una media de este tipo de transacciones porque la complejidad de las mismas, pero en aspectos generales se puede decir que:

   - Las compras en “descuentos”.
   - Apuestas de Casino.
   - Apuestas deportivas.
   - Compras de bitcoin.
   - Compra de Videojuegos.

4. ¿Que considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?

A nivel del territorio nacional el sistema bancario sostiene fuertes políticas, procedimientos y procesos de seguridad para la protección antifraude para los clientes, solo sería necesario incluir capacitaciones frente al tarjetahabiente para reforzar el manejo de su información.

5. Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?

   Las técnicas de ataque y los ciberatacantes se han vuelto más complejos con el tiempo esto ha llevado al sistema bancario a poder mejorar a diario sus sistemas de defensa frente al fraude y las estafas, en aspecto general la evolución conlleva mejoras continuas para optimizar los sistemas de defensa.

6. Según su experiencia, en los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?

   - A través de llamadas.
   - Por correo electrónico.
   - Lo más reciente: fraudes a través de redes sociales.

7. Según la respuesta anterior ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?

   Campañas publicitarias de manera masivas para la prevención del fraude:

   - Por correo electrónico-
   - Medios de comunicación radiales, televisamos y escritos
   - Por medio de redes sociales.

8. ¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?

La técnica de sim swapping, los ciberdelincuentes intentan duplicar de forma fraudulenta la tarjeta SIM del dispositivo móvil de una persona. Para ello suplanta su identidad a fin de conseguir un duplicado de esta. Posteriormente, una vez que la víctima se queda sin servicio telefónico, accede a su información personal y toma el control de sus aplicaciones, suplantándole en sus redes sociales, cuentas de correo electrónico o banca digital, utilizando los SMS de verificación que llegan al número de teléfono

9. ¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito/débito para reducir la exposición al fraude?

   Campañas publicitarias de manera masivas para la prevención del fraude:

   - Por correo electrónico-
   - Medios de comunicación radiales, televisamos y escritos
   - Por medio de redes sociales.
   - Implementación de nuevos sistemas de defensa.

10. Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?

    Con le evolución tecnología por medio de las redes sociales es un oportunidad para poder diseñar campañas publicitarias y de prevención por este canal digital que tanto es usado en sus diferentes plataformas, es muy factible porque los costos de propagación son mucho menores que otros medios pero una notoria igualdad de eficacia.

11. ¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué? Considerando que por ejemplo una tarjeta de crédito negra

tiene límite alto y las de débito del mismo color normalmente disponen un monto elevado de efectivo.

En estos últimos años el término ciberdelincuente, está de moda; y no es para menos, con el avance de la tecnología las empresas grandes, medianas e incluso pequeñas han migrado, o están en el camino, sus procesos para que cada vez más éstos sean soportados por diferentes sistemas tecnológicos, reduciendo tiempos, conectando a sucursales y personas que están en diferentes regiones, automatizando procedimientos entre otras consideraciones.

Profesionales de seguridad han notado que existe un común denominador en la mayoría de ellos y han identificado que siguen un proceso que consta de seis fases:

1. Reconocimiento.
2. Escaneo y enumeración.
3. Ganar acceso.
4. Escalamiento de privilegios.
5. Mantener el acceso.
6. Cubriendo rastros y colocar “puertas traseras”.

Con respecto a los tarjetahabientes están en constante peligro todos en general, ya que muchas veces la suma de pequeñas transacciones representa una suma de dinero considerable.

Experto 3

Datos Generales

Género: Femenino

Edad: 29

Años de experiencia en temas de tarjetas de crédito/débito y fraude: 7

Preguntas

1. Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted que es esencial para que el tarjetahabiente se anticipe a un fraude al momento que adquiere su primera tarjeta de crédito/débito?

   Sería esencial que el tarjetahabiente se informe sobre los riesgos a los que se expone, realizar una búsqueda de las practicas más comunes de fraude y sobre todo revisar la protección que ofrece la marca (Visa/MC) ante un posible fraude.

2. ¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito/débito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?

   El error más común de los usuarios es caer en la trampa de los correos phishing que contienen enlaces en donde se les pide las credenciales de la banca en línea y los números de su tarjeta.

   Mi recomendación seria no abrir correos extraños, no contestar a llamadas telefónicas en donde les pida sus datos personales y revisar siempre si el sitio en el que se está realizando una compra es seguro para compras en línea.

3. ¿Cuáles son algunas de las transacciones con tarjeta de crédito/débito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?

   Las transacciones más comunes por las que se podría realizar fraude son por la compra de juegos, trading, criptomonedas. Normalmente son realizadas en páginas falsas es por eso que es importante validar que la página en la que realizamos compras sea real (revisando el nombre del dominio, certificados de seguridad, comentarios, etc.)

4. ¿Que considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?

   En EE.UU. es una tarea obligatoria que todos los bancos y demás instituciones publiquen los ataques cibernéticos y fraudes detectados para que la población tome las medidas necesarias. Honduras deberían por optar esta práctica, lastimosamente las grandes marcas prefieren no hacer públicos sus falencias para evitar daños a su imagen.

5. Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?

   El fraude es cambiante y todos los días nuevas formas de cometer fraudes son aplicadas. Lo bancos lastimosamente son entes reactivos, ya que seguirles el paso a los defraudadores es complicado por la manera de operar de ellos. Las armas que tienen los bancos son herramientas para prevenir el fraude algunas más avanzadas que otras pero el juego del gato y el ratón siempre existirá.

6. Según su experiencia, en los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?

La tendencia indica que el fraude se está inclinando por el lado de las billeteras digitales y persiste la venta de números de tarjetas en páginas clandestinas (Deep web) en donde se pueden comprar lotes de números de tarjetas y de esa manera probar en cualquier comercio realizar una compra.

7. Según la respuesta anterior ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?

   La parametrización de reglas para diferentes patrones de fraude, bloqueo de tarjetas según un patrón de fraude identificado.

8. ¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?

   Hace unos meses un correo phishing ingreso a la bandeja de uno de los colaboradores, en el correo se le pedía ingresar sus credenciales a lo que el accedió pensando que se trataba de un correo interno de la empresa. Cuando los defraudadores ingresaron con sus credenciales enviaron correos a los demás colaboradores pidiendo información con la excusa que se trataba de temas internos. Para que el usuario no se diera cuenta que los correos estaban saliendo de su cuenta los defraudadores crearon una regla en la que los mensajes que le enviaran relacionados al correo en donde pedían información se desviaran. En uno de esos correos que los colaboradores enviaron se divulgaron un set de número de tarjetas que posteriormente los defraudadores usaron para venderlas.

   Este caso pudo haber sido evitado si el usuario simplemente hubiera ignorado el correo que los defraudadores enviaron.

9. ¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito/débito para reducir la exposición al fraude?

Nuevas tecnologías de tarjetas (chip, contacless), plataformas para robustecer la prevención del fraude, capacitación al personal mediante webinars, charlas, cursos, etc.

10. Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?

    Mediante campañas contra el fraude como actualmente se hace en la mayoría de los bancos.

11. ¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué?

    Considerando que por ejemplo una tarjeta de crédito negra tiene límite alto y las de débito del mismo color normalmente disponen un monto elevado de efectivo.

    Podría decir que si, aunque todos los tipos de plásticos están expuestos, los plásticos negros y plateados tienen mayor límite, es decir, mayor dinero disponible para ser consumido.

Experto 4

Datos Generales

Género: Masculino

Edad: 32

Años de experiencia en temas de tarjetas de crédito/débito y fraude: 11 años

Preguntas

1. Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted

que es esencial para que el tarjetahabiente se anticipe a un fraude al momento que adquiere su primera tarjeta de crédito/débito?

En primer lugar, lo esencial seria que la institución bancaria brindara algún tipo de documentación o compartir por medio de correo electrónico un material / tutorial de los fraudes mas comunes para que el tarjetahabiente este consiente del peligro al que se podría enfrentar y puede estar atento a los puntos mas importantes para poder identificar los fraudes más comunes.

2. ¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito/débito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?

El error más común es:

- Ingresan TC/TD en cualquier página no oficial

Lo más recomendable es que se utilicen páginas que estén acorde con las medidas de seguridad de la información (páginas comerciales y populares) y poder determinar las páginas más utilizada y que sean de uso comercial.

3. ¿Cuáles son algunas de las transacciones con tarjeta de crédito/débito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?
    a. Compras de artículos en tiendas en línea como ser: Amazon,Ebay,Alibaba
    b. Colocar las TC/TD en billeteras electrónicas
    c. Colocar las TC/TD en App de Deliverys
    d. Colocar las TC/TD como débitos automáticos.
4. ¿Que considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?

a. Implementar mejores sistemas de monitoreo de las transacciones TC/TD
b. La resolución de conflictos por temas de fraude (reducir el tiempo de respuesta para solventar el fraude)
c. Crear conciencia a los clientes de los fraudes a los que está expuesto ya sea por Correo electrónico, redes sociales de la institución bancaria, WhatsApp etc

5. Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?

   De acuerdo con la experiencia que se vive actualmente en la institución donde laboro me he dado cuenta de que al pasar los años se ha complicado en vista que las técnicas del fraude se van mejorando ya que utilizan plataformas tecnológicas o app que facilitan el robo de identidad y el phishing que hacen que los clientes sean víctimas de fraude y es cada vez más difícil detectar esta problemática.
6. Según su experiencia, en los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?
   a. Es la usurpación de identidad para hacerse pasar por personal de las instituciones o comercios haciendo creer que la entidad le solicita ciertos datos personales y de esta manera tienen acceso a información invaluable y que con dicha información posterior a ello buscan la forma de generar fraudes en línea con la clonación de la información de tarjetas o acceso a su banca en línea para poder debitar sus ahorros.

7. Según la respuesta anterior ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?
    a. Es difícil de mitigar este tipo de eventos, así como lo hemos mencionado en la entrevista cada vez los fraudes al pasar de los años se vuelven más difíciles de detectar y buscan nuevas técnicas, las medidas preventivas son estar realizando campañas de concientización para que los clientes se den cuenta de los fraudes a los que están expuestos para mostrar las diferentes técnicas que aplican los estafadores.
8. ¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?
    a. Los fraudes en donde los estafadores crean páginas con los logos oficiales y aspectos del comercio o institución bancaria que con casi perfectos y hacen que los clientes ingresen información de sus tarjetas permitiendo realizar robo de información y fraudes.
9. ¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito/débito para reducir la exposición al fraude?
    a. Lo que implementan normalmente son campañas de en redes sociales y paginas oficiales notificando que existen casos de fraude y las formas de como mitigar el fraude
    b. Revisan los productos y ven que alternativas pueden implementar para mejorar y hacer que tengan más restricciones a fin de poder proteger al cliente.

10. Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?
    a. Es una vía viable y de bajo costo el tema de las redes sociales y máxime que son de las plataformas que más se utilizan hoy en día, pero de igual forma incurren a spot de televisión, campañas por WhatsApp y anuncios en los periódicos.
11. ¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué? Considerando que por ejemplo una tarjeta de crédito negra tiene límite alto y las de débito del mismo color normalmente disponen un monto elevado de efectivo.
    a. Eso es subjetivo en el caso de las tarjetas negras si es preocupante porque la línea de crédito las cuales tienen aprobadas puede superar fácilmente los 20,000 dólares pero la verdad es que solo tener a disposición una tarjeta de crédito que tengo disponible para realizar compras está sujeto a un fraude y eso es indistinto a su color.

Experto 5

Datos Generales

Género: Masculino

Edad: 43

Años de experiencia en temas de tarjetas de crédito/débito y fraude: 25

Preguntas

1. Dado que un nuevo tarjetahabiente puede ser considerado de los usuarios más vulnerables por su falta de experiencia en el uso de las tarjetas de crédito/debito, ¿que considera usted

que es esencial para que el tarjetahabiente se anticipe a un fraude al momento que adquiere su primera tarjeta de crédito/débito?

Adquirir conocimientos del uso y cuidados que debe tomar al momento de utilizar la tarjeta, los cuales los puede obtener volantes instructivos, redes sociales o gestores financieros.

2. ¿Cuál es el error más común que hacen los usuarios de tarjeta de crédito/débito al realizar compras en línea? ¿Cuál sería su recomendación para reducir el riesgo de fraude en este escenario?

   Validar que el lugar es seguro y que cumpla con las medidas de seguridad requeridas, de igual forma verificar que el comercio tenga un récord de venta positivo.

3. ¿Cuáles son algunas de las transacciones con tarjeta de crédito/débito que considere usted son las más expuestas a realizar fraude al momento de realizar compras en línea?

   Transacciones en comercios que no cumplen con las medidas de seguridad al momento de validar la información de la tarjeta y que esta puede quedar expuesta.

4. ¿Que considera que las instituciones bancarias deben cambiar o implementar en Honduras para una mejor respuesta a los casos de fraude?

   No autorizar un cargo sin haber confirmado con el cliente, dentro de las implementaciones tener las mejores herramientas de fraude y que estén actualizando a las nuevas versiones.

5. Con el paso de los años, ¿diría usted que a las instituciones bancarias se le ha complicado o simplificado el hecho de prevenir intentos de fraude a sus tarjetahabientes tanto en compras en internet y presencial? ¿por qué?

Debido a que los defraudadores están evolucionando y aprendiendo a como solicitar información sensible a los tarjetahabientes, ya sea por correo y redes sociales., al igual ellos cuentan con una red bien organizada incluso con defraudadores dentro de toda institución.

6. Según su experiencia, en los últimos años, ¿cuál es el método de fraude más utilizado por los estafadores en las compras en línea?

   Compras en comercio de entrega inmediata, comercios que son medio de efectivo.

7. Según la respuesta anterior ¿cuál ha sido la medida preventiva o correctiva más eficiente que ha sido aplicada por las instituciones bancaria para contrarrestar este fraude?

   Aplicar políticas más rigurosas apoyándose con las marcas.

8. ¿Cuál ha sido el caso de fraude o estafa que usted considera ha sido el más elaborado y se pudo haber prevenido con base en su experiencia?

   Banca en Línea, donde el defraudador con su ingenio y habilidad solicita datos a los tarjetahabientes para realizar su cometido, se pudo minimizar si se realizaran campañas masivas de seguridad y concientización a los tarjetahabientes, por todos los medios necesarios.

9. ¿Qué han implementado las instituciones bancarias recientemente en las tarjetas de crédito/débito para reducir la exposición al fraude?

   Migrar las tarjetas a la nueva tecnología CHIP o parámetros de compra.

10. Considerando el uso frecuente de las redes sociales ¿cómo considera usted que las instituciones bancarias pueden aprovechar este canal para ayudar a sus tarjetahabientes a prevenir los fraudes?

Tener actualizado a los tarjetahabientes de cómo evoluciona el fraude e instruyendo las medidas de seguridad que se deben de tomar.

11. ¿Hay algún tipo de tarjetahabiente, dependiendo del color del plástico, que esté más expuesto al fraude? ¿Por qué? Considerando que por ejemplo una tarjeta de crédito negra tiene límite alto y las de débito del mismo color normalmente disponen un monto elevado de efectivo.

    Los tarjetahabientes que están en rangos intermedios., por que dan uso de las mismas en diversos comercios.

ANEXO 2: EJEMPLOS DE PROTOTIPOS DE MENSAJES DE TEXTO Y PUBLICIDAD CONTRA EL FRAUDE

- Mensajes de textos

Figura 10. Prototipo mensajes de Texto. Fuente: Elaboración Propia.

- Publicidad HTML

Figura 11. Prototipo Publicidad HTML. Fuente: Elaboración Propia.