FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES ESPECIALIZACIÓN
EN SEGURIDAD DE LA INFORMACIÓN

CAÑAS QUIROGA MARTA CECILIA
CUELLAR SOSA ANGIE LORENA
MARÍN AGUIRRE ANDREA PAOLA

DELITOS INFORMÁTICOS QUE AFECTAN A LOS CONSUMIDORES FINANCIEROS DEL BANCO DAVIVIENDA

Bogotá D.C., 2021

DELITOS INFORMÁTICOS QUE AFECTAN A LOS CONSUMIDORES FINANCIEROS DEL BANCO DAVIVIENDA

Proyecto de grado presentado con el fin de recibir el título de Especialista en Seguridad de la Información.

Orientador: Jaimes Fernández Wilmar

Bogotá D.C., 2021

Nota de aceptación

_____

_____

_____

_____

_____

Dirección de Investigaciones

_____

Firma del Jurado

_____

Firma del Jurado

RESUMEN

A la par de la evolución tecnológica, la cual ha sido impulsada por la innovación, la transformación digital y acelerada por la pandemia por Covid-19, el sector financiero ha afrontado un aumento en los índices de delitos informáticos. Esta situación ha obligado a las entidades financieras a adoptar, implementar o reforzar sus sistemas de gestión de seguridad informática, teniendo en cuenta no solo que la información es el activo empresarial más importante sino en ofrecer a sus clientes niveles de seguridad adecuados que generen confianza y experiencias positivas al momento de usar los canales digitales.

Tanto los entes reguladores como las entidades financieras han invertido una gran cantidad de recursos y esfuerzos para minimizar el riesgo de ser víctimas de delitos informáticos, en buena parte orientados a diseñar e implementar campañas enfocadas en sensibilizar a los usuarios acerca de las modalidades delictivas y la forma en que pueden prevenir ser víctimas de estas.

Con el presente trabajo se realizará recolección de información a través de una encuesta a 180 consumidores del banco Davivienda, con el objetivo de determinar el índice de conocimiento de los encuestados sobre las modalidades delictivas, existencia de la campaña de sensibilización “La Tía Segura” y que tan efectiva es esta campaña.

Palabras clave: Ciberdelitos, delitos informáticos, fraudes financieros, ingeniería social.

TABLA DE CONTENIDO

INTRODUCCIÓN 8
1. PLANTEAMIENTO DE LA INVESTIGACIÓN 12
2. OBJETIVOS 13
2.1 Objetivo General 13
2.2 Objetivos Específicos 13
MODALIDADES DE CIBERDELITOS MÁS COMUNES QUE AFECTAN A LOS USUARIOS DEL SECTOR FINANCIERO. 13
3.1 Modalidades Delictivas 17
3.2 Smishing Estafas basadas en mensajes de texto y llamadas 18
3.3 Vishing - Llamadas y/o mensajes telefónicos grabados 19
3.4 Phishing -correos electrónicos fraudulentos que dirigen a los clientes a páginas web falsas 19
3.5 Pharming – Sitios web falsos. 20
3.6 El Cambiazo 21
ÍNDICE DE ADOPCIÓN DE LA CAMPAÑA DE PREVENCIÓN "LA TÍA SEGURA" REALIZADA POR DAVIVIENDA 22
4.1 Instrumentos - Fuentes y técnicas para la recolección de la información 23
4.2 Encuesta 24
EFECTIVIDAD DE LA CAMPAÑA LA TÍA SEGURA 28
CONCLUSIONES 30
RECOMENDACIONES 32
REFERENCIAS 33

ÍNDICE DE ILUSTRACIONES

Ilustración 1 - Usuarios de Internet Vs Popularidad por Región..... **¡Error! Marcador no definido.**
Ilustración 2 Ciberseguridad en Colombia ..... **¡Error! Marcador no definido.**
Ilustración 3 Fuente: Davivienda - Smishing..... 18
Ilustración 4- Fuente: Davivienda - Vishing. 19
Ilustración 5 Fuente: Davivienda - Phishing. 19
Ilustración 6 Fuente: Davivienda – Pharming..... 20
Ilustración 7 Fuente: Davivienda - El Cambiazo..... 21
Ilustración 8 Fuente: Autoras - Conocimiento general sobre las campañas de sensibilización 24
Ilustración 9 Fuente: Autoras Conocimiento de la campaña la "tía segura 25
Ilustración 10 Fuente: Autoras Víctimas de algún ciberdelito. 25
Ilustración 11 Fuente: Autoras - Modalidades Delictivas 26
Ilustración 12 Fuente: Autoras - Conocimiento de la Campaña Antes o Después del Suceso Fraudulento 27
Ilustración 13 Fuente: Autoras - Importancia y Utilidad de la Campaña..... 27

ÍNDICE DE TABLAS

Tabla 1 Delitos informáticos ley 1273 de 2009 16

INTRODUCCIÓN

Internet ha evolucionado en todo el mundo y así mismo ha cambiado la forma en que interactuamos con nuestro entorno. En América Latina, el 72 % de la población está en línea y la tasa de crecimiento de usuarios de Internet es una de las más altas del mundo. (Marketing4ecommerce.net, 2021)

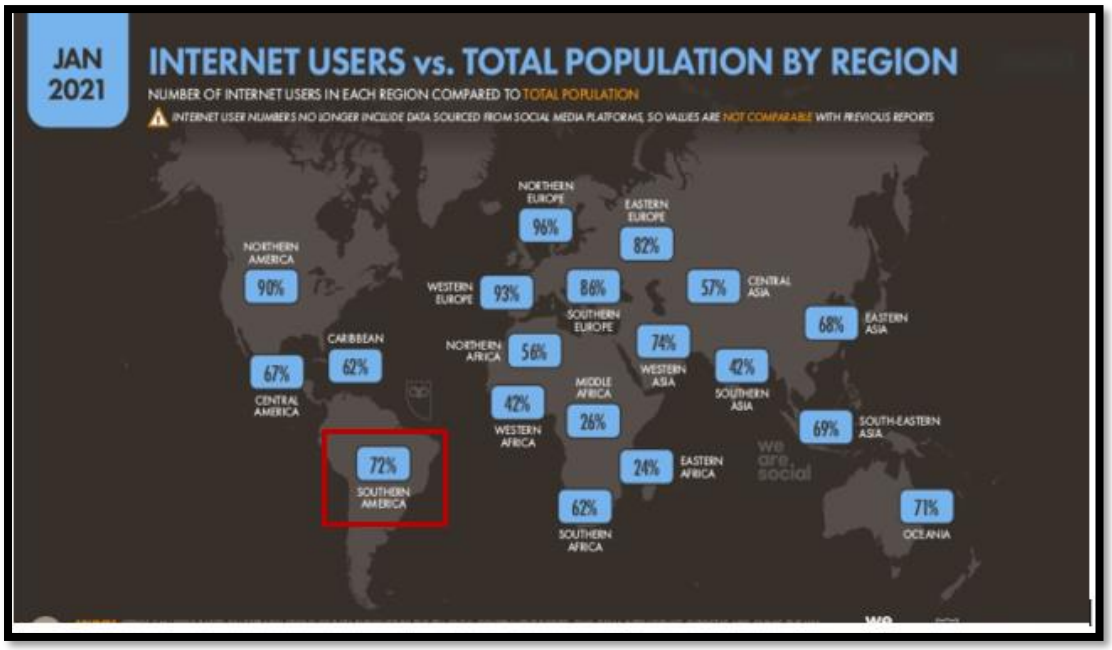

Ilustración 1 Fuente: Marketing4ecommerce-Usuarios de Internet Vs Popularidad por Región

El sector financiero fue uno de los primeros en adoptar las TIC para ponerlas al servicio de sus clientes ofreciéndole canales digitales que les faciliten realizar transacciones bancarias. De acuerdo con la conferencia sobre Retos de Ciberseguridad en el sector Financiero Jacob González nos informa que e*n "…Colombia la población bancarizada es del 81 % y el 79,4 % de esta la población ha consultado o*

hecho transacciones bancarias en línea" (Jacobo A. González C., 2021), también encontramos según estudio de la OEA que "*…el 92 % de las entidades bancarias identificaron algún tipo de evento de seguridad y el 37 % de entidades bancarias manifestaron que fueron víctimas de ataques materializados"* (OEA, 2018).

Colombia es el 3er país de Latinoamérica en el ranking de cibercrimen y el 6º con más ataques cibernéticos (Cali, 2021), durante la pandemia debido al virus Covid-19 la gran mayoría de los consumidores financieros se vieron en la necesidad de hacer uso de los canales digitales para realizar transacciones electrónicas u operaciones bancarias, esto tuvo injerencia en que el primer trimestre del año 2020 se presentará un aumento del 37% de ciberdelitos respecto al año 2019, (Argote, 2021). Esto evidencia que los bancos han implementado medidas para asegurar la protección de la información de sus clientes, este sector sigue siendo uno de los principales objetivos de los ciberdelincuentes quienes aprovechan el alto volumen de usos de canales digitales, así como el desconocimiento de los usuarios en medidas básicas de ciberseguridad para convertirlos en su blanco principal de ataques como lo son Vishing, Smishing, Phishing y el Cambiazo.

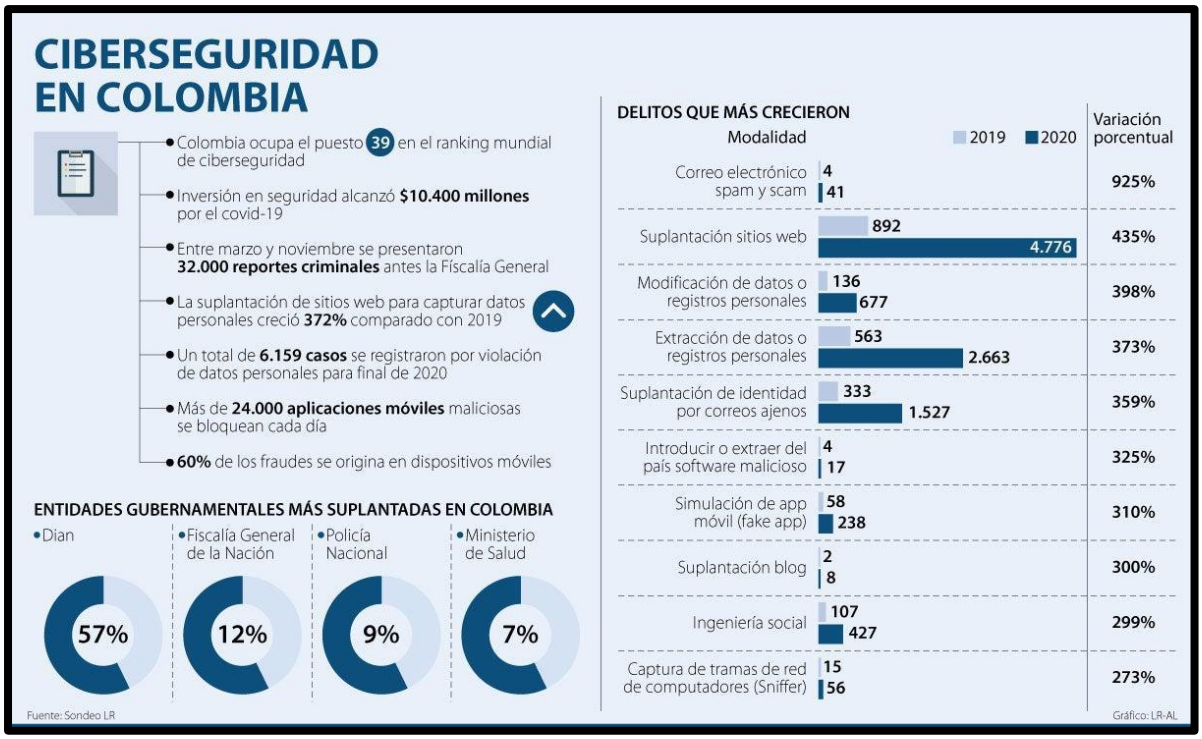

Ilustración 2 Fuente: Asuntos legales.com -Ciberseguridad en Colombia

Las entidades bancarias hacen grandes inversiones en seguridad a nivel de sus aplicaciones e infraestructura tecnológica y algunas campañas de sensibilización a usuarios, sin embargo, se considera que aún falta invertir en educar y concientizar a los usuarios, ya que si ellos saben identificar los ataques y las modalidades delictivas hay menos probabilidades de que sean víctimas de fraude.

Davivienda es uno de los bancos en Colombia que ha presentado mayor afectación por la ciberdelincuencia según lo informado por la revista semana (Semana, 2021).

"… De los 49 millones de transacciones que la entidad bancaria lleva a cabo en promedio al mes a través de todos sus canales, el 0,068 % corresponde a una reclamación por una actividad presuntamente fraudulenta y de los 16,6 millones de

clientes que acumulan Davivienda y Daviplata el 0,042 % son los que reclaman" (Revista Semana, 2021).

Es decir que alrededor de 7 mil clientes reclaman cada mes por actividades fraudulentas. Las modalidades más utilizadas por los ciberdelincuentes son el Vishing, Smishing, Phishing y el Cambiazo, cada una de estas es perpetrada a través de técnicas de ingeniería social y se dan en ambientes externos, es decir no se generan por explotación de vulnerabilidades de seguridad de la entidad.

Por ello, es que Davivienda hace énfasis en que la seguridad es una responsabilidad conjunta entre proveedores de servicio y consumidores, teniendo en cuenta que los últimos son el eslabón más débil en la cadena de seguridad de la información y deben ofrecérseles herramientas que les permitan permanecer atentos ante las diferentes modalidades de ciberdelincuencia.

Como parte de la estrategia de protección contra ciberdelitos y sensibilización a usuarios, Davivienda implementó en abril del año 2020 la campaña llamada "La Tía Segura" esta campaña es caracterizada por un personaje familiar y se enfoca en brindar recomendaciones para evitar ser víctima de fraude financiero. El objetivo de esta investigación se enfoca en determinar la efectividad de esta campaña en la reducción del índice de delitos informáticos de los cuales son víctimas los clientes del banco.

Es así, que para recolectar información que permita conocer el índice de adopción y efectividad de la campaña "La Tía Segura" de Davivienda, se realizó a una encuesta a 180 usuarios con edades entre 18 y 56 años residentes en la ciudad de Bogotá.

A nivel general, el resultado de la encuesta arroja un alto índice de desconocimiento acerca de la campaña: Solo el 17 % de los encuestados manifiestan conocer la

campaña y los usuarios que manifiestan conocerla aseguran que esta trae recomendaciones muy importantes para la protección de la información de sus productos y servicios financieros como lo son el manejo seguro de claves, seguridad en la conexión a Internet para el uso de los canales digitales del banco, desconfiar de mensajes donde se solicite la entrega de información personal y claves de acceso a los productos financieros, entre otras.

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

El Banco Davivienda ha presentado un alto número de casos relacionados con fraude cibernético que atentan contra los usuarios que realizan transacciones en línea. Debido a esto, la experiencia de los usuarios al realizar transacciones por medios digitales no es satisfactoria porque sienten la inseguridad de utilizar estos canales digitales.

Esta situación afecta la reputación de Davivienda, poniendo en duda la seguridad de su infraestructura, canales y aplicaciones Web. Como consecuencia, podría sufrir pérdida potencial de clientes y también el banco tendrá una considerable pérdida en los rubros cobrados por transacciones realizadas en línea, además de exponerse a demandas jurídicas.

Pregunta de la Investigación

¿Por qué los controles implementados en los medios electrónicos de Davivienda no son suficientes para evitar la materialización de delitos informáticos y en qué medida afecta el desconocimiento de los usuarios sobre las campañas de sensibilizaciones enfocadas en prevenir ser víctimas de estos?

2. OBJETIVOS

2.1 Objetivo General

Analizar la efectividad de la campaña de sensibilización “La Tía Segura” creada por Davivienda para prevenir que sus consumidores sean víctimas de delitos informáticos.

2.2 Objetivos Específicos

- Analizar las modalidades de ciberdelitos más comunes que afectan a los usuarios del sector financiero.
- Evaluar el índice de adopción de los consumidores financieros respecto a la campaña de prevención y concientización “La Tía Segura” realizada por Davivienda.
- Identificar la efectividad de la campaña de sensibilización “La Tía Segura” implementada por Davivienda en abril de 2020, con el fin de prevenir y concientizar a sus consumidores sobre las modalidades de delitos informáticos.

MODALIDADES DE CIBERDELITOS MÁS COMUNES QUE AFECTAN A LOS USUARIOS DEL SECTOR FINANCIERO.

La habilidad de los ciberdelincuentes para adquirir información haciéndose pasar por fuentes confiables en diferentes circunstancias, es una de las principales razones por las que aún se presentan este tipo de fraudes. Ejemplo de ello son los mensajes de texto y correos electrónicos falsos que fueron recibidos durante el periodo de la pandemia a causa del Covid-19, en estos se hacen pasar por servidores de las diferentes organizaciones de Salud ofreciendo ayuda. De acuerdo con esto, se evidencia que los cibercriminales han sabido detectar y aprovechar las circunstancias para engañar a las víctimas (Salud, Ministerio de, 2021).

En Colombia los delitos informáticos son descritos a través de la ley 1273 de 2009 por la cual se cambia el Código Penal, se crea un nuevo bien jurídico nombrado "*de la protección de la información y de los datos*" y se salvaguardan completamente los sistemas que utilicen las tecnologías de la información y las telecomunicaciones, entre otras prácticas. Dentro de esta ley se tipifican los delitos contra la confidencialidad, la integridad y la disponibilidad de la información.

En la tabla 1, se sintetizan los delitos informáticos contemplados en el ámbito jurídico colombiano, el momento en el que se considera la materialización del delito y las penas o sanciones que acarra la comisión de estos.

Delito	**Se materializa Cuando**	**Pena - Sanción**
Acceso abusivo a un sistema informático (269A)	Quien sin autorización acceda a un sistema informático esté o no con medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.	48 a 96 meses de encarcelamiento y en multa de 100 a 1000 salarios mínimos (SMLV)

Delito	Se materializa Cuando	Pena - Sanción
Obstaculización ilegítima de sistema informático o red de telecomunicaciones (269B)	Se bloquea de manera ilegal un sistema o impide su ingreso de forma normal, sin el consentimiento de la persona autorizada.	48 a 96 meses de encarcelamiento y en multa de 100 a 1000 salarios mínimos (SMLV)
Interceptación de datos personales. (269C)	El que sin autorización legal intercepte datos informáticos en su origen, destino o en el interior de un sistema informático	Encarcelamiento 36 a 72 meses.
Daños informáticos (269D)	El que sin autorización legal modifique, dañe, altere, borre o destruya o suprima	Encarcelamiento 48 a 96 meses y sanción de 100 a 1.000 (SMLV)

Delito	Se materializa Cuando	Pena - Sanción
	datos que se encuentran en el programa o documentos electrónicos.	
Uso de software malicioso (269E)	El que, sin tener autorización legal, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso	Encarcelamiento 48 a 96 meses y sanción de 100 a 1.000 (SMLV)
Violación de datos personales (269F)	El que sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales, almacenados en medio magnéticos.	Encarcelamiento 48 a 96 meses y sanción de 100 a 1.000 (SMLV)

Delito	Se materializa Cuando	Pena - Sanción
Suplantación de sitios web para capturar datos personales (269G)	El que sin autorización legal diseñe desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes	Encarcelamiento 48 a 96 meses y sanción de 100 a 1.000 (SMLV)

Tabla 1 Delitos informáticos ley 1273 de 2009

3.1 Modalidades Delictivas

Entre las modalidades de ciberdelitos más comunes identificados por el banco Davivienda están: Smishing, Vishing, Phishing y el Cambiazo, donde los ciberdelincuentes aplican técnicas de ingeniería social para engañar a las personas y obtener de manera fraudulenta información confidencial.

A continuación, se describe en qué consisten están modalidades delictivas.

3.2 Smishing Estafas basadas en mensajes de texto y llamadas

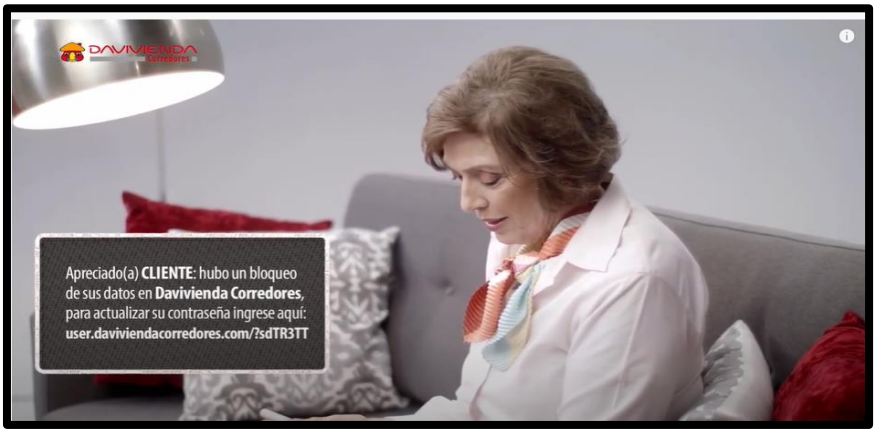

Ilustración 3 Fuente: Davivienda - Smishing

Esta modalidad está basada en correos, mensajes de texto y llamadas realizadas por los ciberdelincuentes para engañar a los usuarios financieros y obtener información valiosa, como los datos de usuario y clave de acceso a las plataformas virtuales, haciéndose pasar por agentes de la entidad bancaria.

Con esta modalidad de estafa los ciberdelincuentes se apropian de todos los datos necesarios para poder realizar movimientos bancarios a nombre de las víctimas.

3.3 Vishing - Llamadas y/o mensajes telefónicos grabados

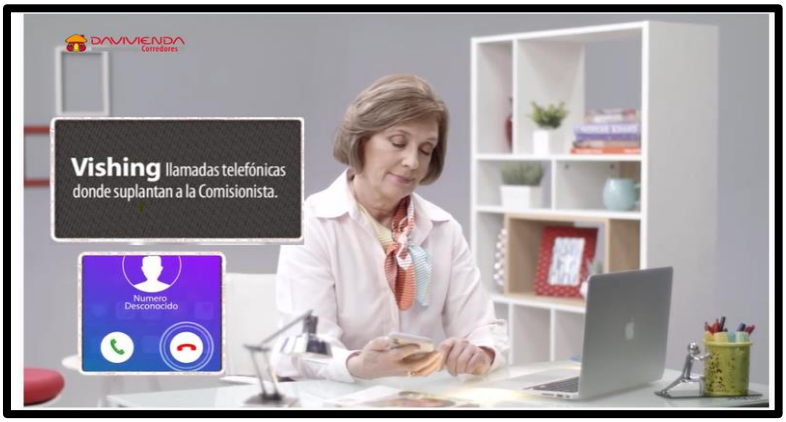

Ilustración 4- Fuente: Davivienda - Vishing.

El Vishing son llamadas y/o mensajes telefónicos grabados, que informan al usuario que el banco ha bloqueado sus cuentas y que es necesario actualizar la información. Para esto piden llamar a un número de teléfono, en el que le pedirán confirmar cierta información para reactivar las cuentas o actualizar la información. (BBVA, El vishing, una nueva modalidad de fraude, 2019).

3.4 Phishing -correos electrónicos fraudulentos que dirigen a los clientes a páginas web falsas

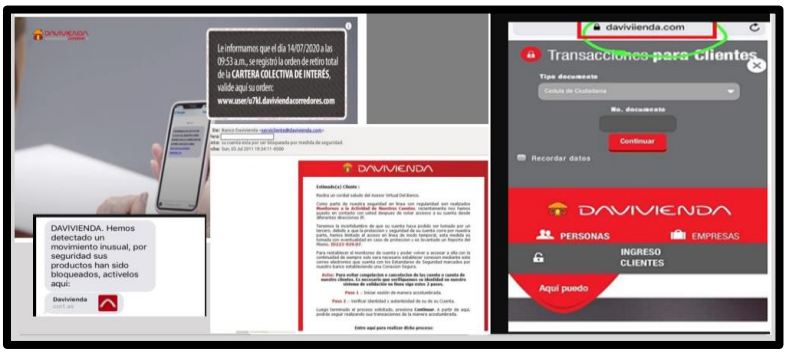

Ilustración 5 Fuente: Davivienda - Phishing.

Probablemente sea el método más utilizado por los ciberdelincuentes, y consiste en el envío de correos electrónicos fraudulentos que dirigen a los clientes a páginas Web falsas que aparentan ser de la entidad bancaria. Esta modalidad también puede presentarse en Facebook con 'fan page' falsas que postean contenido fraudulento y solicitan información confidencial de los usuarios.

3.5 Pharming – Sitios web falsos.

Ilustración 6 Fuente: Davivienda – Pharming

El Pharming se produce cuando un ciberdelincuente dirige a un usuario de Internet hacia un sitio web falso, no hacia uno legítimo. Estos sitios falsificados pueden capturar información confidencial de la víctima, como nombres de usuario, contraseñas y datos de tarjetas de crédito, o bien pueden instalar malware en el dispositivo electrónico.

3.6 El Cambiazo

Ilustración 7 Fuente: Davivienda - El Cambiazo

Practica fraudulenta que consiste en engañar a las personas fingiendo ser amables y aprovechándose de las dificultades de manejo con elementos electrónicos, con esto aprovechan y realizan el cambio de la tarjeta de la víctima para poder duplicar la información y así poder realizar su acto delictivo.

A continuación, algunas recomendaciones para minimizar el riesgo de fraude:

- No suministrar información personal o bancaria en páginas web a las que haya accedido desde un enlace incluido en un email o SMS.
- Revisar cuidadosamente el enlace que contiene el SMS y observar si tiene palabras o caracteres extraños.
- Los códigos de un solo uso (One Time Password) son secretos y el banco nunca los pedirá por correo, llamada o SMS.
- Desconfiar de todos los mensajes alarmantes que tengan tono de urgencia y contengan faltas de ortografía.

- Recordar que las páginas web seguras comienzan siempre por https.
- Omitir los mensajes que solicitan llamar o hacer alguna operación.
- De tener alguna duda con la legitimidad de la llamada o mensaje recibido, llamar directamente al banco y confirmar la veracidad de la información.
- Tener presente que el banco nunca se contactará por ninguna vía para solicitar información sensible y confidencial sobre números de tarjeta, clave y/o contraseñas.
- En los cajeros no acepte ayuda de extraños.
- No pierda de vista su tarjeta mientras hace pagos.
- Evite entablar conversaciones con personas desconocidas cuando estés esperando en la fila del cajero.
- Al ingresar la clave, cubre el teclado con la mano o el brazo para que nadie la vea. (Davivienda, 2021)

ÍNDICE DE ADOPCIÓN DE LA CAMPAÑA DE PREVENCIÓN "LA TÍA SEGURA" REALIZADA POR DAVIVIENDA

Debido a la pandemia Covid-19, Davivienda se enfrentó al reto de continuidad operacional y capacidad de negocio, basado en la transformación digital e implementó los diferentes canales y aplicaciones de atención virtual. En ese sentido el Banco Davivienda trabaja continuamente en mejorar los canales de comunicación y mantener a salvo la información confidencial de todos sus clientes, y así minimizar los riesgos que pongan en peligro la seguridad de la información de sus clientes. En abril del año 2020 fue lanzada la campaña de sensibilización llamada "La Tía Segura" que tiene como objetivo ayudar a proteger la información sobre los productos

financieros de los clientes, a través de un personaje familiar que brinda consejos ante situaciones sospechosas que ponen en riesgo el bienestar financiero de las personas y enseña a tomar las medidas necesarias de seguridad para evitar ser víctima de fraude.

4.1 Instrumentos - Fuentes y técnicas para la recolección de la información

Para conocer el índice de adopción de la campaña “La tía segura” de Davivienda, se tomó la encuesta como herramienta para la recolección de información , ya que por medio de esta podemos obtener y elaborar datos de forma rápida y eficaz sobre temas específicos de ciberdelitos financieros más usuales, según la frecuencia del uso de los canales virtuales y físicos del banco, conocimientos de las campañas de prevención ofrecidas por la entidad, nivel de seguridad, satisfacción de los usuarios entre otros, esto nos da una estadística de la cantidad de personas vinculadas al banco y que se han visto afectadas por las diferentes modalidades de fraude.

Con esta investigación se plantea obtener el índice de efectividad de la campaña la “Tía Segura” dentro de la población encuestada teniendo en cuenta las siguientes características:

1. Recolectar la información mediante la observación indirecta teniendo en cuenta las quejas que tienen los usuarios financieros al haber sido víctimas de fraudes financieros.
2. El interés como investigadoras es conocer si la campaña la “Tía Segura” realizada por Davivienda es conocida entre sus usuarios financieros, concientiza y evita que realmente estos sean víctimas de los delincuentes.
3. Permitir la obtención de una gran variedad de productos porque consideran que la campaña sirve para prevenir fraudes financieros.

4.2 Encuesta

Se realizó el cuestionario a 180 usuarios financieros del Banco Davivienda, entre diferentes rangos de edades desde los 18 años hasta más de 56 años, Mas del 60% de los encuestados son profesionales y el 55% de esta población desempeña cargos en nivel profesional, jefatura y analista.

Al indagar entre la población seleccionada, si conocían alguna campaña de seguridad de la información de Davivienda, se encontró que las campañas emitidas por el banco no son muy conocidas por los usuarios encuestados, como lo muestra en la ilustración 8.

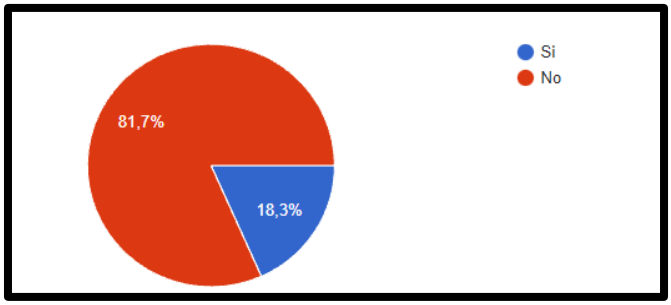

Ilustración 8 Fuente: Autoras - Conocimiento general sobre las campañas de sensibilización

Pero si bien, espontáneamente las campañas en general no son muy conocidas, para los que conocen algún tipo de campaña de seguridad de la información la “tía Segura” es la campaña más recordada entre ellos, a presar del desconocimiento como se puede observar en la ilustración 9. Donde los usuarios de Davivienda no han sido participes de esta información.

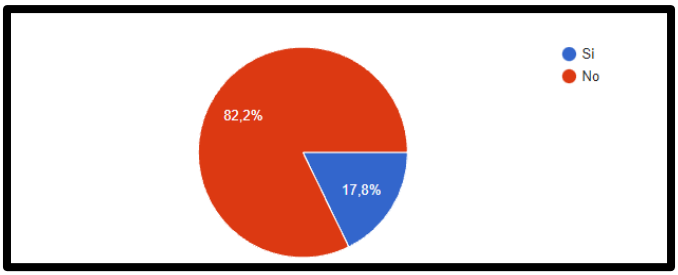

Ilustración 9 Fuente: Autoras Conocimiento de la campaña la "tía segura

Según los usuarios encuestados que dicen conocer la campaña la “tía segura”, manifiestan que esta deja el siguiente aprendizaje:

- No entregar sus claves a terceros.
- Usar conexiones seguras para transaccionar a través de canales virtuales la deben realizar por medio de equipos y redes seguras nunca abiertas.
- No ingresar a links que causan desconfianza y puedan ser usados para robo de información.
- No creer en mensajes o llamadas donde ofrecen premios o piden actualizar datos personales.

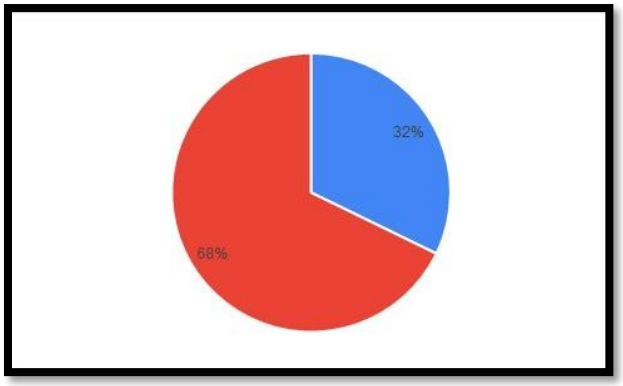

Ilustración 10 Fuente: Autoras Víctimas de algún ciberdelito.

Se encontró que el 32% de los encuestados han sido víctimas de alguna modalidad de ciberdelitos financieros.

Una de las modalidades más utilizadas para cometer los ilícitos de los que han sido víctimas los usuarios es Phishing (correos que solicitan ingresar a un link donde los redirige a una página de suplantación a la del banco), seguido continuando con el Malware (software que se infiltra o daña un dispositivo sin el consentimiento de su propietario) y en tercer lugar, está el Pharming (Infecta el dispositivo del cliente por medio de un malware que modifica algunos archivos del sistema operativo) y en último lugar el cambiazo de tarjetas (intercambio de la tarjeta original por una falsa) como lo muestra en la ilustración 10.

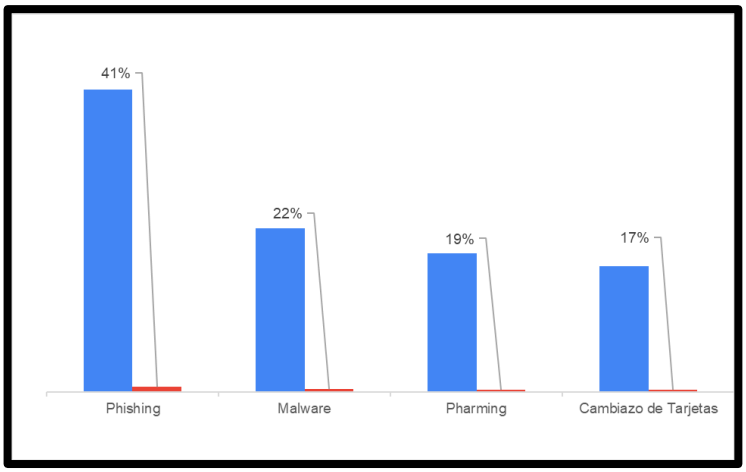

Ilustración 11 Fuente: Autoras - Modalidades Delictivas

Los usuarios que fueron afectados por algún ciberdelito manifiestan que conocían la campaña “La Tía Segura” antes de sufrir el suceso fraudulento como se muestra en la ilustración 12.

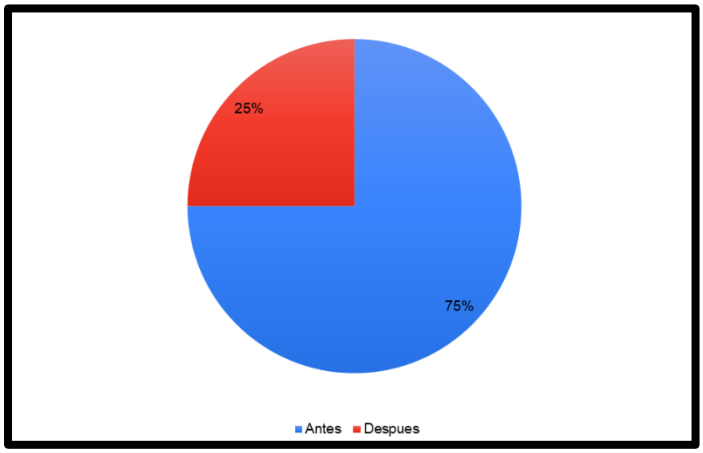

Ilustración 12 Fuente: Autoras - Conocimiento de la Campaña Antes o Después del Suceso Fraudulento

Cuando se pregunta a los encuestados porque consideran importante la implementación y conocimiento de las campañas de sensibilización y si estas sirven de alguna manera para mitigar la probabilidad de ser víctima de fraudes cibernéticos, la respuesta más común es “SI” como se muestra en la ilustración 13, se consideran importantes ya que promueven el ciber cuidado, crean conciencia, previenen, informan y alertan; Sin embargo, los medios de divulgación no son los más visitados y efectivos.

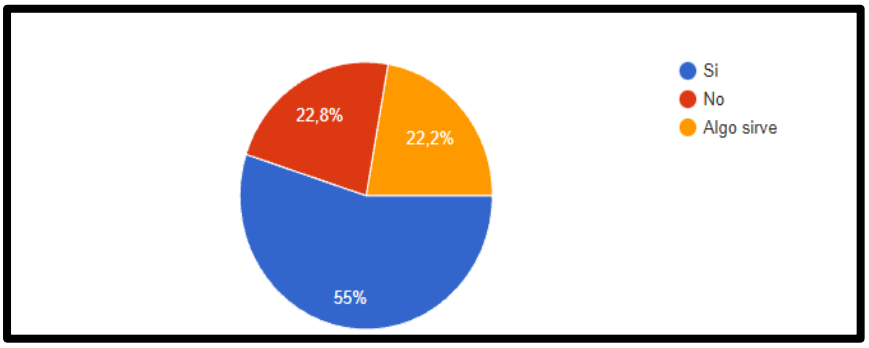

Ilustración 13 Fuente: Autoras - Importancia y Utilidad de la Campaña

EFECTIVIDAD DE LA CAMPAÑA LA TÍA SEGURA

La campaña “La Tía Segura” lanzada en abril del año 2020, ha sido una de las campañas de Davivienda con mayor énfasis en la prevención delitos informáticos, sin embargo, hay una cantidad significativa de usuarios que hace caso omiso a este tipo de información bien sea por falta de tiempo, falta de conocimientos ante la evolución tecnológica o porque no sienten seguridad al abrir cierto tipo de contenido o enlaces ya que no es fácil identificar si viene del banco o de un atacante haciéndose pasar por la entidad financiera.

La “Tía Segura” se ha ido replicando mediante videos y como canal de comunicación por medio de su página web, SMS y YouTube, para así llegar a todos los tipos de usuarios financieros, pero aun así no es tan conocida dentro de los clientes del banco a pesar que la información de la campaña es actualizada cada mes y comunicada a sus clientes vía mensaje de texto con un hipervínculo para poder ver su contenido, también es enviada por medio de correos electrónicos, pero por la inseguridad en general que existe entre los usuarios; Actualmente por el aumento en los delitos informáticos no todos acceden a estos links a ver la información.

Sin embargo, los usuarios financieros consideran que es importante estar actualizados en temas de prevención de fraudes cibernéticos debido al incremento que se ha presentado sobre esta modalidad de estafa.

Los adultos mayores son las personas que menos están informadas sobre dichos delitos y son las menos afectadas, ya que ellos siguen prefiriendo hacer sus trámites

bancarios de manera presencial trasladándose hasta la oficina ya que para ellos *"si no tiene el sello del banco no se formalizó el pago o la transacción no se realizó"*, las compras y demás actividades de su día a día también son realizadas de forma presencial ya que no están habituados al comercio electrónico y son los que en la mayoría de los casos está menos actualizados e interesados en el tema tecnológico ya que son muy susceptibles de engaños y estafas, esto a pesar que los teléfonos inteligentes están al alcance de todos y el acceso a Internet no tiene límites en su uso cotidiano.

La población más afectada por la ciberdelincuencia está en los rangos de edad de 25 a 45 años de edad, ya que esta generación vio llegar el Internet a los hogares, posteriormente a la vida cotidiana y con ella la tecnología que nos ha facilitado la vida como lo son los disipativos como smartphones, laptops y tabletas siendo más confiados en el uso personal de estas herramientas al momento de navegar en la red y realizar sus actividades diarias en línea ya que esta se realiza de forma inmediata debido a que les facilita el día a día evitando trasladarse de un lugar a otro sin tener que llevar efectivo y/o hacer largas filas en el banco o establecimientos comerciales.

La población más "responsable" al momento de realizar sus transacciones y usar los medios tecnológicos son los usuarios financieros entre 18 y 25 años, ya que son nativos digitales, ellos nacieron con la tecnología de la mano y son menos complicados y más cuidadosos a la hora de ingresar a las plataformas financieras y/o comerciales, la comunicación con ellos se debe realizar a través de plataformas con un contenido específico para mantenerlos interesados, saber qué nueva plataformas con información actualizada disponen que utilizan y para qué.

CONCLUSIONES

La virtualidad y la tecnología han avanzado al pasar de los días, con ello logra facilitar la cotidianidad de los seres humanos en el mundo digital, paralelamente a esto ha aumentado el índice de delitos informáticos.

Los entes reguladores en conjunto con las entidades bancarias han realizado grandes esfuerzos para minimizar el riesgo de ser víctimas de ciberdelitos, sin embargo, el mayor número de sucesos en los que se materializan estos delitos se dan por fuera de los canales del banco. En la actualidad se puede denominar que el factor humano tiene un porcentaje muy alto de responsabilidad frente a estos sucesos, ya que la mayoría de las personas son vulnerables a través de la ingeniería social, la concientización en ciberseguridad es una de las principales "armas" para detener estos ciberataques.

A pesar de los avances tecnológicos y mejoras en seguridad que ha implementado Davivienda, la delincuencia busca nuevas formas de atacar, por este motivo para lograr un alto nivel de seguridad, se requiere de renovación continua en las estrategias de seguridad tanto en la infraestructura de la entidad como en la concienciación a los usuarios.

Davivienda y Daviplata cuentan con aproximadamente 16,6 millones de clientes, los videos de la campaña la tía segura tienen un tiempo de duración entre 35 segundos y 1 minuto, a pesar de ser tan cortos, didácticos e informativos su registro de visualizaciones es muy baja según los estadísticas de YouTube, ya que corresponden a 16.092 visitas es decir que la información de la campaña está llegando por este medio únicamente al 0,097% de los usuarios del banco y de la población encuestada solo el 17% tiene conocimientos sobre dicha

campaña. (Revista Semana, 2021).

El 55% de esta población la considera la campaña importante y útil, porque con ella pueden evitar, prevenir, ayudar a culturizar, detener y bajar el índice de delitos.

De acuerdo con lo anterior la campaña “la tía segura” no alcanza un buen nivel de efectividad, ya que los medios de divulgación no son los adecuados y no logra llegar al 100% de los consumidores financieros de Davivienda.

Lo anterior se puede evidenciar en la población encuestada ya que solo el 17% tiene conocimientos sobre la campaña “La Tía Segura” y el 55% de esta población la considera importante y útil, porque con ella pueden evitar, prevenir, ayudar a culturizar, detener y bajar el índice de delitos. La campaña “la tía segura” no alcanza un buen nivel de efectividad, ya que los medios de divulgación no son los adecuados y no logra llegar al 100% de los consumidores financieros de Davivienda.

Por lo tanto, los usuarios financieros deberían “invertir más tiempo en informarse, adoptar e implementar los métodos de prevención y autocuidado, y no que por un simple descuido terminen siendo un blanco fácil para el delincuente”. Pero solo esto se puede realizar si se concientiza a todos los consumidores y así previene no solo para Davivienda si no para las otras entidades financieras.

RECOMENDACIONES

Invertir en seguridad es indispensable, ya que la virtualidad está cada vez más presente en nuestra vida cotidiana, los cambios de esta nueva realidad pueden dejar de manera obsoleta una tecnología que se pensaba era muy segura, por lo tanto, es necesario innovar constantemente para así poder dar la continuidad al negocio en este caso el proceso funcional de los canales virtuales implementados por Davivienda y la banca móvil, debido a que los usuarios pueden llegar a ser muy vulnerables a causa de su desconocimiento, acerca de las medidas de seguridad, los bancos deben invertir más en la concientización de sus usuarios sobre el autocuidado cibernético.

Davivienda lleva a cabo una campaña de concientización que brinda a sus usuarios consejos básicos para cuidarnos del fraude a la hora de hacer transacciones a través de sus canales, al recibir llamadas o mensajes "sospechosos". En comparación de otras entidades financieras se puede decir que es una de las mejores campañas de prevención que se han visto, debido a su dinámica y el personaje usado para las mismas, ya que con esto puede llegar a los diferentes usuarios, desconociendo su edad, nivel socioeconómico y conocimiento digital, pero lamentablemente los medios usados para divulgar a " la Tía segura" no son los más frecuentados por los consumidores financieros; Por lo que se debería evaluar hacerlo de manera diferente para poder llegar a cada una de las generaciones ya que todas tiene formas diferentes en cuanto al utilización de la información.

Los adultos mayores de 76 años por ejemplo, prefieren las suscripciones a periódicos, televisión tradicional y noticias, a ellos se les puede informar por medio de los populares folletos, los baby boomers generación entre los 57 y 75 años quienes tienen buena adaptación a la tecnología ya que les gusta compartir información de

interés a través de ciertas redes sin verificar su contenido, con ellos se puede trabajar por medio del Facebook y se encargarían de ayudar a compartir la campaña, continuando con la generación X que son entre los 41 y 56 años quienes prefieren consumir contenido a través de las plataformas digitales ya que las necesidad de informarse sobre ciertos temas los lleva a explorar en internet, generación Y o millennias su rango de edad esta entre los 25 y 40 años esta generación fue la que vio llegar el Internet a los hogares y posteriormente a la vida cotidiana junto con la tecnología que nos ha facilitado la vida con los diferentes dispositivos, los centennials son altamente influenciables por las redes sociales ya que sus edades están entre los 10 y 24 años (primicias, 2021), dentro de las campañas se debería empezar a culturizar desde los pequeños ahorradores para ir creando conciencia desde una temprana edad; tomando como referencia esta información las entidades financieras deberían pensar en personalizar las campañas según los rangos de edades de sus clientes y su manera de utilización de la información para así lograr la concientización y culturización sobre los peligros y riesgos que hay al navegar en la red y no creer en cualquier llamada o mensaje fraudulento, esto con el fin de disminuir el índice de denuncias que se han venido presentando.

REFERENCIAS

ACIS. (2019). *Benchmark de tecnología antifraude.* From Benchmark de tecnología antifraude: https://acis.org.co/portal/content/NoticiaInternacional/reducir-los-niveles-de-fraude-prioridad-de-las-instituciones-financieras-y-empresas-para-el

Almagro, Luis. (2019). *Desafios del Riegos Cibernetico en el Sector Financiero.* OEA. Washington D. C.: Prologo OEA. From https://www.minsait.com/sites/default/files/newsroom

Argote, C. A. (2021, 02 17). *asuntos:legales*. From asuntos:legales: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

Banco BBVA. (n.d.). *Banco BBVA*. From Tips' de seguridad para usar mejor la tarjeta de crédito: https://www.bbva.com/es/ar/tips-de-seguridad-para-usar-mejor-la-tarjeta-de-credito/

BBVA. (2019). *¿Qué es el CVV o CVC de las tarjetas de crédito?* From ¿Qué es el CVV o CVC de las tarjetas de crédito?: https://www.bbva.com/es/que-es-el-ccv-o-cvc-en-las-tarjetas-de-credito/

BBVA. (2019). *El vishing, una nueva modalidad de fraude*. From El vishing, una nueva modalidad de fraude: https://www.bbva.com/es/el-vishing-una-nueva-modalidad-de-fraude/amp/

BBVA. (2019). *El vishing, una nueva modalidad de fraude*. From El vishing, una nueva modalidad de fraude: https://www.bbva.com/es/el-vishing-una-nueva-modalidad-de-fraude/amp/

Cali, E. (2021). *Cibercrimen en Colombia: somos el tercer país con más fraudes en Latinoamérica*. From Cibercrimen en Colombia: somos el tercer país con más fraudes en Latinoamérica: https://www.enteratecali.net/2021/07/cibercrimen-en-colombia-somos-el-tercer-pais-con-mas-fraudes-en-latinoamerica/#.YYBlP2DMLIU

Castro Gómez , Santiago. (2020, Octubre 26). Asobancaria. *Banca y economia*, 3. From Impacto económico y social del phishing y Smishing en Colombia: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

Corrales, J. C. (2019, 12 1). *revelock.* From revelock: https://www.revelock.com/es/blog/los-tres-tipos-principales-de-fraude

Davivienda. (2021, octubre 12). *La tia segura*. From https://comunicaciones.Daviviendacorredores.com/La-Tia-Segura/

economia, Banca. (2020). *Asobancaria.* From Asobancaria: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

Editorial La República S.A.S. (2021, febrero 17). From https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

El tiempo. (2021, Octubre 14). *El tiempo*. From https://www.eltiempo.com/tecnosfera/novedades-tecnologia/robo-por-internet-ojo-a-las-modalidades-de-fraudes-bancarios-en-linea-624873

Jacobo A. González C. (2021, 07 15). *https://acis.org.co/*. From https://acis.org.co/portal/content/los-retos-de-la-ciberseguridad-de-la-informaci%C3%B3n-en-el-sector-bancario

Marketing4ecommerce.net. (2021, 01). From https://marketing4ecommerce.net/usuarios-de-internet-mundo/

minsait, I. C. (2018). *tendenciasmediosdepago_2018.* From tendenciasmediosdepago_2018: https://www.minsait.com/sites/default/files/newsroom_documents/tendenciasmediosdepago_2018.pdf

OEA. (2018). *sectorbancariospa.* From sectorbancariospa: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Pinto, Alejandro. (2021, 01 23). Davivienda recibe 33 mil reclamaciones al mes por fraude. *El Espectador*.

Portafolio. (2020). From El fraude electrónico, el principal problema del sistema financiero: https://www.portafolio.co/economia/finanzas/fraude-electronico-el-principal-problema-del-sistema-financiero-511655

Portafolio. (2021, Octubre 14). *portafolio*. From portafolio: https://www.portafolio.co/economia/colombia-se-destaca-en-educacion-financiera-y-billeteras-digitales-557384

primicias. (2021). *primicias*. From primicias: https://www.primicias.ec/noticias/tecnologia/silenciosa-hasta-alpha-estas-son-generaciones-digitales/

Revista Semana. (2021). ¿Cuántos reclamos por fraude recibe Davivienda al mes? *Semana*.

Salud, Ministerio de. (2021, 10 18). *minsalud*. From minsalud: https://www.minsalud.gov.co/Paginas/No-se-deje-confundir-con-los-mensajes-falsos.aspx

Santiago Castro Gómez. (2019). *Ciberdelitos en el Sector Financiero.* From ASOBANCARIA: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Semana. (2021). ¿Cuántos reclamos por fraude recibe Davivienda al mes? *Semana*, 1. From https://www.semana.com/economia/finanzas-personales/articulo/cuantos-reclamos-por-fraude-recibe-davivienda-al-mes/202147/

Velásquez Durán , Ana María . (2019). *El Tiempo*. From https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096