UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO

Facultad de Ciencias Jurídicas y Sociales

Carrera: Licenciatura en Seguridad Ciudadana

Título del Trabajo: Ciberdelitos: estafas con billeteras electrónicas.

Autor: Nelson Gustavo López – Email: gustavolop1969@gmail.com

Tutora: Mg. Paula Ariadna Jessurum

Año de presentación: 2024

AGRADECIMIENTOS

El trabajo de investigación y la producción de una tesis, no es posible sin el aporte de conocimientos y, fundamentalmente, de las experiencias brindadas por los actores que participaron desde el comienzo en este proceso. Muchos, incluso sin saberlo, colaboraron en la materialización de este proyecto. Por esto, deseo agradecer en primera instancia a mi directora de tesis, la Profesora Paula Ariadna Jessurum y al Profesor Diego Andrés Pérez Llana, quienes con su confianza y su trabajo académico me enseñaron, mediante sus críticas constructivas, el valor de construir un saber académico. Por todo su trabajo, ¡muchas gracias!

Con el saludo a mi directora, quiero hacer extensivo mi agradecimiento a las autoridades de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Fasta, a los profesores que me brindaron sus conocimientos y a mis compañeros con quienes compartí saberes y aprendizajes de esta hermosa carrera.

Del mismo modo, agradezco a mi amigo y camarada el Licenciado y actual Comisario Mayor de la Policía de la Provincia de Buenos Aires José Segovia, quien me motivó a inscribirme a la carrera de grado, por haberme dado el ánimo para el inicio de esta valiosa experiencia. Sin sus consejos y su confianza, esto no hubiese ocurrido jamás.

También a quienes me brindaron sus conocimientos, experiencias y diferentes puntos de vista sobre la seguridad ciudadana.

A mi familia, soporte fundamental para mantener la llama encendida, para enfocarme en el camino y no parar.

A Dios, al Hijo y al Espíritu Santo por no desampararme jamás, a ellos, mi más sincero agradecimiento.

TRABAJO FINAL

TEMA: Ciberdelitos: estafas con billeteras electrónicas en la ciudad de Miramar, en el primer semestre de 2023.

1. INTRODUCCIÓN

La introducción de la tecnología en la vida cotidiana, acelerada por la pandemia de COVID 19, implicó el pasaje de actividades que se realizaban de manera presencial a la modalidad virtual. Una de las actividades que recibió mayor impacto de esta transformación es el comercio que, en la actualidad, maneja gran volumen de operaciones a través del el e-commerce o comercio electrónico (compra y venta de bienes y servicios a través de internet) potenciado por el incremento de la cantidad de teléfonos celulares en el mundo y la digitalización masiva de ingresos y ayudas sociales durante la mencionada pandemia.

Asegura el Banco Central de la República Argentina (BCRA, 2022b) que, en el segundo semestre de 2022, la tenencia de cuentas de banco alcanzó al 98,5% de los adultos en nuestro país. A su vez, cada adulto realizó, en promedio, 10,8 pagos mensuales a través de diversos medios electrónicos y estrategias digitales.

Los medios de pago más utilizados en las transacciones de comercio electrónico, según CACE (2022) son: tarjeta de crédito a través de una plataforma de pago o un enlace de pago en internet; pago en efectivo contra entrega o a través de medios como Pago Fácil o Rapipago; tarjeta de débito mediante plataformas de pago; billetera electrónica; transferencia bancaria; tarjeta de crédito en el lugar de compra al retirar el producto. Se identifica un avance de las billeteras electrónicas en detrimento del pago en efectivo. Las billeteras virtuales que cuentan con mayor cantidad de usuarios en nuestro país son Mercado Pago, Modo y Cuenta DNI.

Las billeteras electrónicas o billeteras virtuales, según BCRA (2022a) son:

> el servicio ofrecido por una entidad financiera o proveedor de servicios de pago (PSP) a través de una aplicación en un dispositivo móvil o en un navegador web que debe

> permitir –entre otras transacciones– efectuar pagos con transferencia (PCT) y/o con otros instrumentos de pago –tales como tarjetas de débito, de crédito, de compra o prepagas. (p.1)

El incremento de uso de los medios de pago electrónicos en general y de las billeteras electrónicas en particular también fue acompañado por el aumento de ciberdelitos, entre los que se encuentran las estafas con billeteras electrónicas. En primer lugar, diremos que entendemos por ciberdelito, las “conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo” (Acurio del Pino, 2016, p.10). En cuanto a las estafas o fraudes con billeteras electrónicas, definiremos como tales a las artimañas con las que se ataca el patrimonio de los individuos “mediante el despliegue de un ardid o engaño, abusando de su confianza o a través de técnicas de manipulación informática que generan posibles estafas en los términos establecidos en nuestro ordenamiento penal" (UFECI en Risso, 2022).

1.1 Justificación

Pese a que, periódicamente el BCRA refuerza las medidas de seguridad, no se logra detener el volumen de estafas que padecen los usuarios de billeteras electrónicas, las más frecuentes son el robo de los datos de tarjetas de débito y crédito (por la interoperabilidad entre CBU y CVU), hackeos de billeteras virtuales, hurto de los datos del homebanking (también a causa de la interoperabilidad), suplantación de identidad, pagos a individuos u organizaciones que no cumplen con la contraprestación prometida, entre otros.

El Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales de la Universidad Austral (OCEDIC, 2022) manifiesta que las denuncias por ciberfraudes aumentaron un 200% en el primer trimestre de 2022 respecto al primer trimestre de 2021. Las proporciones son similares en todo el territorio aunque muestran mayor incidencia en las capitales de provincia y los centros turísticos. En Argentina se registran, en promedio, 4.800 ciberfraudes mensuales, lo que equivale a una estafa cada diez minutos, es por esto que constituyen una problemática central del campo de la seguridad ciudadana contemporánea.

En lo que atañe a Miramar, territorio donde desplegaremos esta investigación, según Bork (2021) se trata de una ciudad costera de la Provincia de Buenos Aires, cabecera del partido de General Alvarado, cuenta con 34.391 habitantes. La principal actividad económica es el turismo pero, dado que en el partido de General Alvarado se despliegan actividades agrícolas y ganaderas, también cuenta con oficinas y eventos comerciales de ese sector.

Los emprendimientos turísticos y gastronómicos, estimulados por el boom tecnológico de la pandemia, ofrecen sus servicios a través de portales donde reciben el pago mediante diversos medios entre los que se encuentran las billeteras mencionadas. La recepción de múltiples medios de pagos no puede obviarse en una ciudad que compite con otras ciudades de la Costa Atlántica en calidad de receptora turística. Otro tanto ocurre con las ferias, el comercio y la población local que se han visto arrastrados a utilizarlos aunque no siempre los eventuales operadores (compradores y vendedores) cuenten con destrezas digitales para realizar las operaciones ni con recomendaciones básicas de seguridad para prevenir las estafas. Es por esto que se considera pertinente llevar a cabo esta investigación.

1.2 Antecedentes

Entre los antecedentes de esta investigación mencionaremos los trabajos de Sánchez (2019), Bouguet Abiotti (2021) y Iannicelli (2021). En su trabajo titulado “Billetera Virtual ventajas y desventajas de su implementación en Argentina”, Sánchez (2019) analiza la inclusión digital y la creciente inserción de billeteras electrónicas en nuestro país y en el mundo. Algunos de los factores que examina son la confianza de los clientes, la seguridad de los datos y las capacidades tecnológicas de las empresas para brindar una transacción segura.

En su tesis de grado denominada “Ciberdelitos en Argentina: la falta de legislación de ciertas conductas lesivas realizadas a través de tecnologías de la información y comunicación”, Bouguet Abiotti (2021) define y describe los ciberdelitos, enumera los más recurrentes en Argentina (entre los que se encuentran estrategias

criminales que posibilitan el uso fraudulento de billeteras digitales) y explora los vacíos legales en torno a la comisión de estos delitos.

Por fin, en la investigación titulada “Los ciberdelitos y la repercusión de las estafas informáticas durante la cuarentena”, Iannicelli (2021) describe el modo en que las estafas tradicionales se trasladaron a la virtualidad durante la pandemia y los impactos futuros de esta escalada de delitos entre los que menciona la necesidad de aumento de seguridad informática y estrategias de prevención de robo de datos así como la formación de los usuarios.

1.3 Problema

¿Qué características presentan las estafas con billeteras electrónicas que tuvieron lugar en la ciudad de Miramar, en el primer semestre de 2023?

1.4 Objetivo General

Describir y analizar las estafas con billeteras electrónicas que tuvieron lugar en la ciudad de Miramar, en el primer semestre de 2023

1.5 Objetivos Específicos

Determinar modalidades e incidencia del ciberdelito de estafas con billeteras electrónicas en la ciudad y el periodo referidos.

Comparar las diferentes billeteras electrónicas que se utilizan en la ciudad de Miramar en cuanto a seguridad y usabilidad.

Relacionar buenas y malas prácticas de los usuarios de billeteras virtuales con vulnerabilidad al ciberdelito mencionado.

2. MÉTODO

La metodología que utilizaremos es mixta. Por este motivo, trabajaremos con la investigación documental (cualitativa) y la encuesta (cuantitativa). Adherimos a la idea de apelar a la complementariedad de las perspectivas cuantitativas y cualitativas para dar respuesta a los objetivos de la investigación. La articulación de métodos, tal como expresa Sautú (2003) permite integrar y contrastar la información disponible para un abordaje complejo del fenómeno estudiado y, además, para minimizar los sesgos.

El enfoque elegido es descriptivo retrospectivo, para Hernández Sampieri, Fernández Collado y Baptista Lucio (2014) se trata de una investigación que pretende describir situaciones y eventos, a fin de determinar cómo es y cómo se manifiesta el fenómeno en estudio. El diseño es no experimental transversal.

En lo que atañe a los instrumentos mencionados, la investigación documental, según Hernández Sampieri, Fernández Collado y Baptista Lucio (2014) consiste en "detectar, obtener y consultar la bibliografía y otros materiales que parten de otros conocimientos y/o informaciones recogidas moderadamente de cualquier realidad, de manera selectiva, de modo que puedan ser útiles para los propósitos del estudio" (p.50). En esta investigación se utilizarán registros de denuncias de la Policía de la Provincia de Buenos Aires acerca de la problemática en estudio en Miramar durante el primer semestre de 2023, legislación vigente, bibliografía, publicaciones periódicas y publicaciones periódicas online que se refieran de manera específica a la temática abordada.

Respecto a la encuesta, para Achenti (2007) es un método utilizado para recolectar datos con relación a actitudes, creencias u opiniones a través de cuestionarios estandarizados. Las ventajas de las encuestas, según Hernández Sampieri, Fernández Collado y Baptista Lucio (2014) son: costo bajo; información sobre un gran número de personas en un tiempo breve; facilidad para obtener, cuantificar, analizar e interpretar datos; bajos requerimientos de personal; anonimato de los encuestados y eliminación de ciertos sesgos, entre otras.

En este caso, se contactarán 20 (veinte) personas del entorno del investigador (o referidas por el entorno), que hayan sido víctimas de estafas con billeteras electrónicas en la ciudad de Miramar en el primer semestre de 2023, a quienes se proporcionará un cuestionario estandarizado en papel o mediante formulario de Google con link en WhatsApp, a devolver en el día; con preguntas de opción múltiple destinadas a caracterizar el tipo de estafa de la que fue víctima, billetera o billeteras en uso, prácticas de uso, entre otras.

Por último, se pondrán en conversación los datos obtenidos en el análisis documental con aquellos relevados mediante la encuesta y los antecedentes de la investigación. Así, se relevarán conclusiones, hallazgos y recomendaciones si las hubiera.

2.1 Población

Ciudadanos de Miramar afectados por estafas con billeteras electrónicas durante el primer semestre de 2023

2.2 Marco del Muestreo

En lo que atañe a la información documental, se apela a la información disponible en las dependencias policiales de la ciudad de Miramar, prensa y web para el periodo que involucra esta investigación.

En cuanto a la encuesta, se opta por una muestra no probabilística en cadena o bola de nieve. Dado que este tipo de delito, las estafas mediante billeteras virtuales, suelen ser vergonzantes para algunas personas, se elige hacer mención del tema o alusiones en el entorno inmediato para encuestar a los casos positivos y/o a quienes fueran referidas por estas primeras personas.

2.3 Instrumento de Recolección De Datos

Análisis documental: es una operación que, a partir de diferentes fuentes de consulta o documentos primarios, genera un documento secundario que posibilita organizar la información para comunicarla y reutilizarla.

Ficha modelo de análisis documental

Tipo de fuente	Informes – Página web – Registros de Institucionales -Otras
Autor/es	
Título	
Mes – Año	
Palabras clave	
Resumen	

Encuesta. Marque con una X la respuesta correcta. Ésta es una encuesta anónima de uso exclusivamente académico.

1. Edad							
18 a 25		25 a 45		45 a 65		+ de 65	
2. Género							
F		M		Prefiero no decirlo			
3. ¿Qué billeteras virtuales utiliza? (Marque todas las que utilice)							
Mercado Pago		Modo		Ualá		Naranja		Cuenta DNI	
BNA+		Otra		Si respondió otra: ¿Cuál/es?			
4. ¿Cuál es la/s billetera/s con la/s que padeció la estafa? (En el caso de que más de una billetera estuviera involucrada, márquelas también)							
Mercado Pago		Modo		Ualá		Naranja		Cuenta DNI	
BNA+		Otra		Si respondió otra: ¿Cuál/es?			
5. ¿Qué dispositivo estaba usando cuando fue víctima de la estafa?							
Celular		Computadora		Otro. Describa:			
6. ¿Qué tipo de perjuicio sufrió en la estafa? (Marque todos los que correspondan)							
Pedido de préstamos a su nombre		Compras a su nombre		Robo de dinero en cuenta		Robo de dinero a contactos	
Otro. Describa:							
7. ¿Cuál fue la acción que disparó la estafa?							

"Ayuda" o contacto de empresa a través de redes sociales.		Llamadas a través de call centers (diferentes modalidades del cuento del tío).		Duplicación o suplantación de SIM luego de que se le solicitara la clave mediante llamada telefónica o de WhatsApp		Robo de celular.	
Otro. Describa:							

8. ¿Realizó la denuncia policial o ante organismo especializado en ciberdelincuencia?

Sí		No	

9. ¿Se comunicó con la/s empresa/s en la/s que padeció la estafa?

Sí		No	

10. ¿Recuperó el dinero? ¿Logró revertir préstamo o compra? (Lo que corresponda).

Sí. Todo.		Sí. Parcialmente.		No.	

11. Al momento de la estafa ¿contaba con la autenticación de dos factores o dos pasos activa?

Sí		No	

12. Si respondió No. ¿Por qué no la activó?

No sabía hacerlo		Lo creía innecesario		Me resultaba complicado el uso de la aplicación, dispositivo o celular con doble autenticación		Otra	

13. Al momento de la estafa ¿solía brindar datos personales (usuarios, claves, contraseñas, pin, token, DNI original o fotocopia, foto), por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto si creía que quien los solicitaba era confiable?

Sí		No	

14. Al momento de la estafa ¿qué tipo de contraseñas utilizaba en cuentas y dispositivos?

Fuertes (combinación de letras, número y símbolos)		Fáciles (que pueda recordar)		Otra (describa)	

15. Al momento de la estafa ¿solía compartir con otras personas links, ofertas, sorteos, promociones, juegos que solicitaban datos personales?

Sí		No	

16. Al momento de la estafa ¿solía conectarse a internet a través de redes públicas?

Sí		No		A veces	

17. Al momento de la estafa ¿cómo describía sus conocimientos como usuario de internet del 5 al 1? Donde 5 es el nivel más alto y 1 es el nivel más bajo.

5		4		3		2		1	

18. Luego de la estafa, ¿cambiaron sus hábitos de usuario en internet con computadoras y dispositivos móviles?

Sí		Algunos		No	

3. RESULTADOS

La documentación institucional consultada en el partido de General Alvarado asegura que en el cuarto trimestre de 2022, en la localidad de Miramar se consumaron y denunciaron 25 (veinticinco) estafas digitales. Mientras que, en las otras localidades del partido como Comandante Nicanor Otamendi, se cometieron y denunciaron 4 (cuatro) estafas digitales, en Mechongue 1 (una) estafa digital y en Mar del Sud ninguna (cero).

Tabla 1: Estafas comprobadas y denunciadas según ciudad, en el partido de General Alvarado, en el último trimestre de 2022

Ciudad	**Cantidad**
Miramar	25
Comandante Nicanor Otamendi	4
Mechongue	1
Mar del Sud	0
Total	30

Gráfico 1: Estafas comprobadas y denunciadas según ciudad, en el partido de General Alvarado, en el último trimestre de 2022

Fuente: Elaboración propia

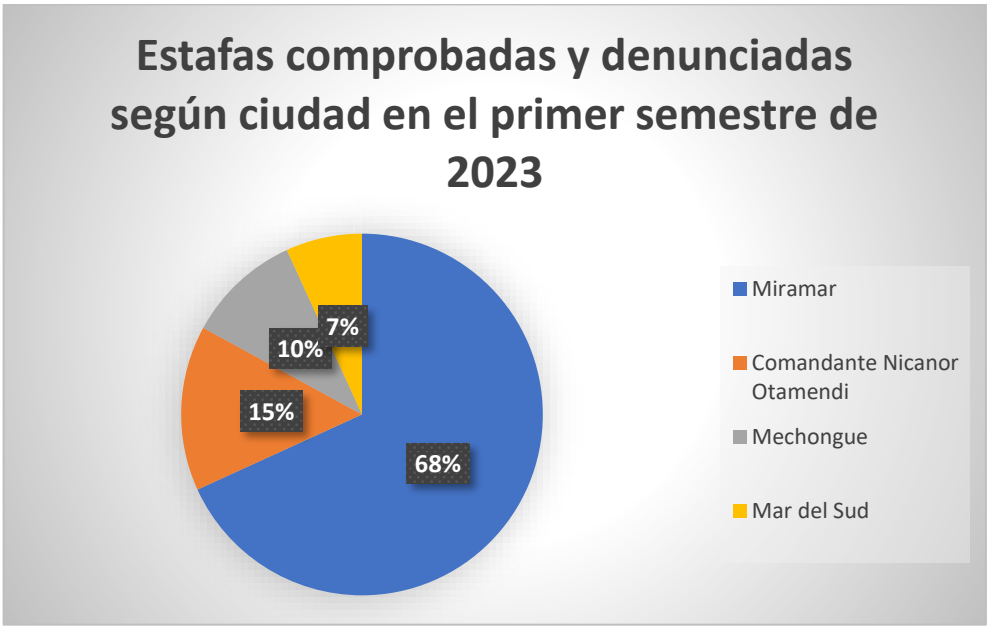
Así, el total de estafas digitales del partido en el segundo semestre de 2022 es de 30 (treinta). De este total, el 83 % ocurren en Miramar por la relevancia de la ciudad como centro comercial y porque concentra la mayor cantidad de habitantes. De ese total, sólo una (1) estafa digital está esclarecida, cuatro (4) están sin esclarecer y 25 (veinticinco) continúan en investigación.

Por su parte, en el primer semestre de 2023, en General Alvarado se consumaron y denunciaron 60 (sesenta) estafas digitales en la localidad de Miramar; 13 (trece) en Comandante Nicanor Otamendi; 9 (nueve) en Mechongue; 6 (seis) en Mar del Sud. La mayoría de estos delitos, el 68,8%, suceden en la ciudad de Miramar.

Tabla 2: Estafas comprobadas y denunciadas según ciudad, en el partido de General Alvarado, en el primer semestre de 2023

Ciudad	**Cantidad**
Miramar	60
Comandante Nicanor Otamendi	13
Mechongue	9
Mar del Sud	6
Total	88

Gráfico 2: Estafas comprobadas y denunciadas según ciudad, en el partido de General Alvarado, en el primer semestre de 2023.



Fuente: Elaboración propia

Entonces, el total de estafas digitales en el primer semestre de 2023 es de 88 (ochenta y ocho) casos. Del mencionado total, 2 (dos) delitos se han esclarecido, 83 (ochenta y tres están en investigación) y 3 (tres) están sin esclarecer.

Nótese el aumento en valor absoluto del primer semestre de 2023 respecto el último trimestre de 2022[1]. No obstante, es preciso tener en cuenta que este periodo contiene al primer trimestre del año que puede presentar variantes estacionales relacionadas con el movimiento de turistas. Como se observa, la ciudad del partido que más delitos digitales denunciados tiene es Miramar por su centralidad y porque allí ocurren numerosas operaciones financieras del partido.

En cuanto a la tipología de estafas documentada por las autoridades locales, la misma incluye una amplia variedad de delitos informáticos que pueden dividirse en dos grupos: (a) informática como objeto del delito, incluye el sabotaje informático, la piratería informática, el hackeo, entre otras; (b) informática como medio del delito, en esta área se encuentra la falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos o a través de redes sociales, hackeo de billeteras virtuales.

[1] Si se divide por dos el semestre (88/2), se obtiene un promedio de 44 delitos trimestrales.

Si bien, el eje de este trabajo se centra en la segunda tipología, pueden combinarse. Al respecto, refiere Perfil (12 de marzo de 2024) que en el primer semestre de 2023, la Policía Federal apresa a una banda involucrada en robo transaccional, estos delincuentes atacaron empresas, entre las que se encuentra Buenbit, a la que le robaron US$ 800000 desviando dinero desde cuentas virtuales asociadas a diferentes billeteras electrónicas afectando la seguridad de la empresa pero también a usuarios. Esto demanda allanamientos en Lanús y Miramar, sedes de estos cripto-hackers[2].

Es preciso enfatizar que el Código Penal (Infoleg, 2023) sanciona las siguientes conductas como delitos informáticos contra la propiedad: (a) la estafa a través del uso de tarjeta magnética o de los datos de la tarjeta; (b) la defraudación con uso de cualquier técnica de manipulación informática que altere el funcionamiento de un sistema informático o el uso de datos; (c) el daño informático como producto de la alteración, destrucción o inutilización de datos, programas o sistemas; la venta, distribución, circulación o introducción en un sistema informático; los programas diseñados para generar daños.

La pena es mayor si el daño afecta a servicios informáticos públicos o sistemas destinados a la prestación de servicios de salud, de comunicaciones, de energía, de medios de transporte u otro servicio público.

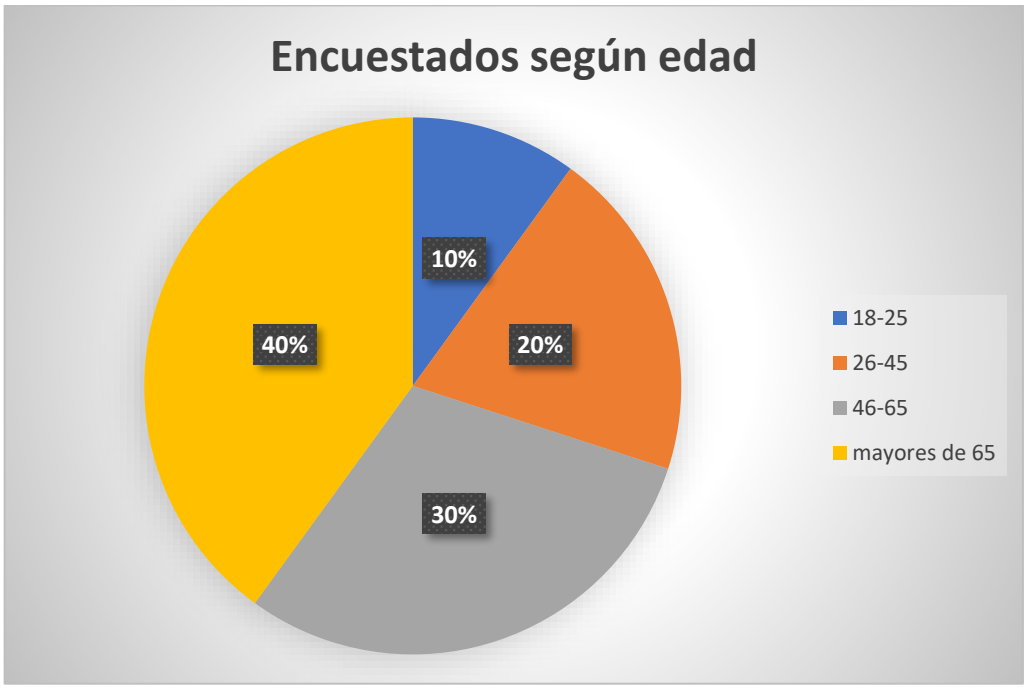
Hasta aquí, lo recabado en fuentes documentales varias. Por su parte, el trabajo de campo arrojó los siguientes resultados.

Tabla 3: Encuestados según edad

Respuesta	**Cantidad**
18-25	2
26-45	4
46-65	6
+65	8
Total	20

[2] Se utiliza este ejemplo porque transcurre en el periodo analizado en esta investigación.

Gráfico 3: Encuestados según edad



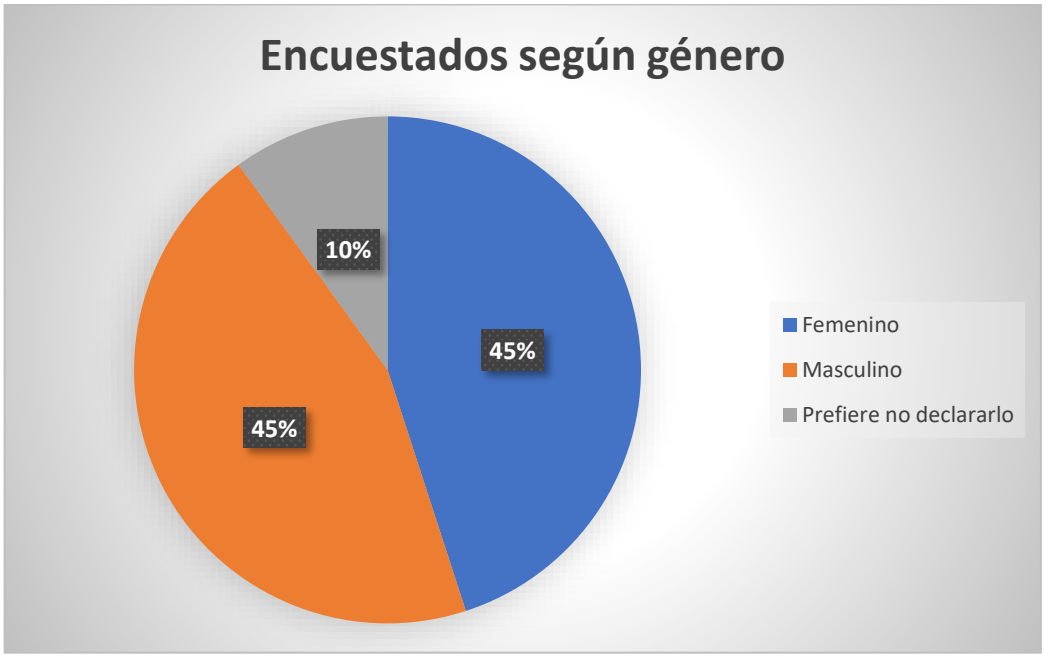
Fuente: Elaboración propia

En la Tabla y el Gráfico 4, la encuesta arroja que la cantidad de estafas (en términos absolutos), aumenta a medida que aumenta la edad, registrando el valor máximo del 40% en personas mayores de 65 años. No obstante, señalaremos que las estafas se producen en todas las franjas etarias.

Tabla 4: Encuestados según género

Respuesta	**Cantidad**
Femenino	9
Masculino	9
Prefiere no declararlo	2
Total	20

Gráfico 4: Encuestados según género



Fuente: Elaboración propia

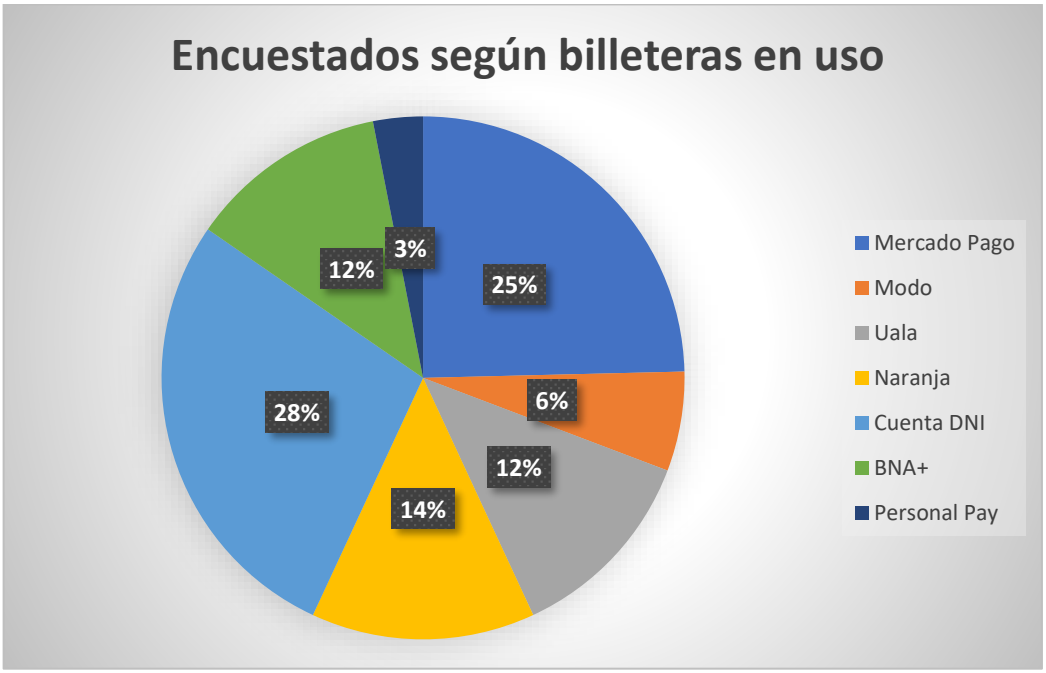
En la Tabla y el Gráfico 4, la encuesta arroja que la cantidad de estafas tiene una incidencia similar entre personas de género femenino y género masculino[3], ambos porcentajes del 40%, las estafas se producen en todos los géneros.

Tabla 5: Encuestados según billeteras en uso

Respuesta	**Cantidad**
Mercado Pago	16
Modo	4
Uala	8
Naranja	9
Cuenta DNI	18
BNA+	8
Personal Pay	2
Total	65

Gráfico 5: Encuestados según billeteras en uso

[3] Es sólo un dato demográfico de la muestra.



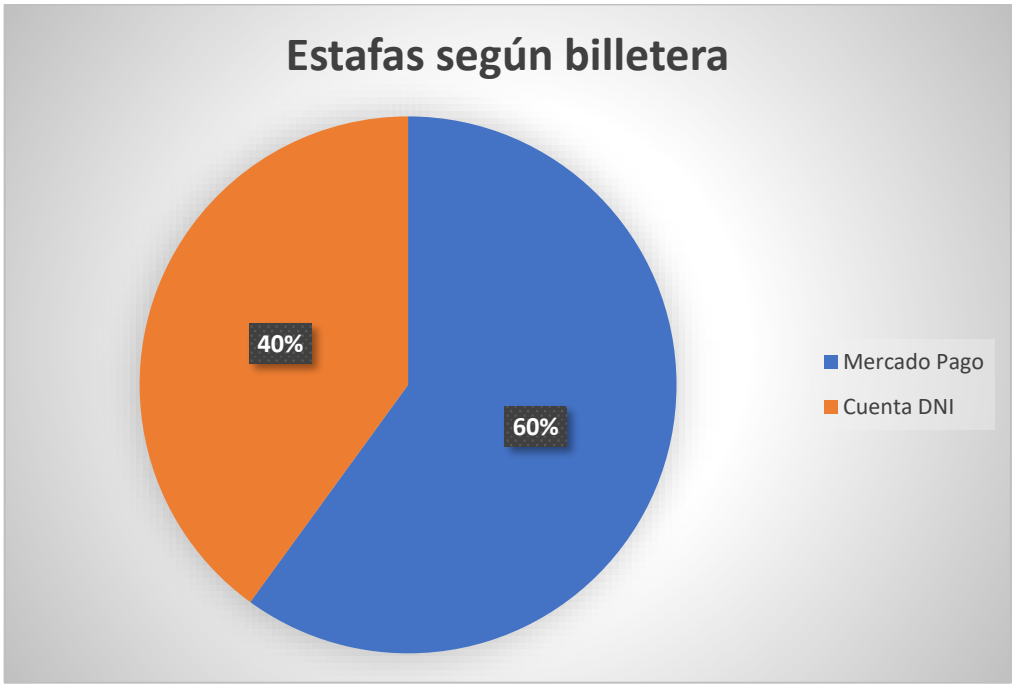
Fuente: Elaboración propia

En la Tabla y el Gráfico 5, la encuesta arroja que la billetera que más se utiliza es la de Cuenta DNI (28%) seguida por Mercado Pago (25%) y Naranja (14%). No obstante, señalaremos que numerosas billeteras están en uso en Miramar y que los usuarios tienen más de una (3,25 promedio por encuestado) lo que refiere una notable inclusión financiera.

Tabla 6: Estafas según billetera

Respuesta	**Cantidad**
Mercado Pago	12
Cuenta DNI	8
Total	20

Gráfico 6: Estafas según billetera



Fuente: Elaboración propia

En la Tabla y el Gráfico 6, la encuesta arroja que la billetera que más estafas recibe es la de Mercado Pago (60%) seguida por Cuenta DNI (40%). Esto se relaciona con el hecho de que son las billeteras de mayor uso en la ciudad y con la familiaridad de los delincuentes con las operatorias de ambas.

Tabla 7: Estafas según dispositivo en uso

Respuesta	**Cantidad**
Celular	20
Computadora	1[4]
Total	21

Gráfico 7: Estafas según dispositivo en uso

[4] Mediante uso de dos dispositivos al mismo tiempo

Fuente: Elaboración propia

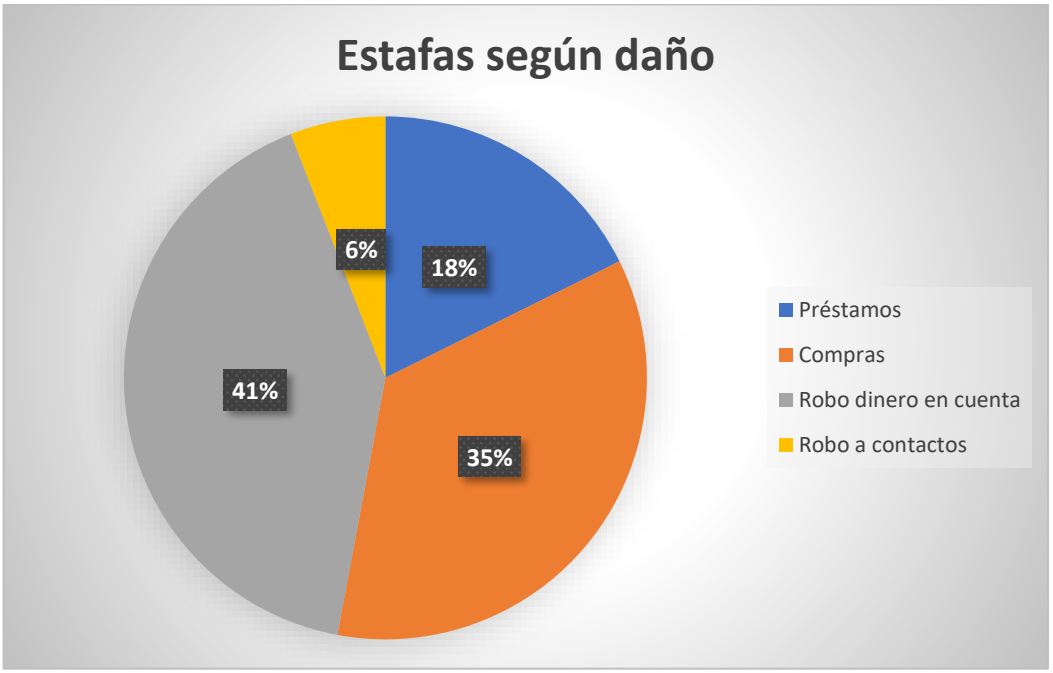
En la Tabla y el Gráfico 7, la encuesta arroja que la mayoría de las personas que padecieron estafas estaban utilizando celular (95%)[5]. Esto se vincula a la masividad de uso de los dispositivos móviles.

Tabla 8: Estafa según daño

Respuesta	**Cantidad**
Préstamos	6
Compras	12
Robo dinero en cuenta	14
Robo a contactos	2
Total	34

Gráfico 8: Estafas según daño

[5] En uno de los casos, la persona fue estafada utilizando ambos al mismo tiempo. Guiada desde el celular a acciones que ejecutaba con la computadora.



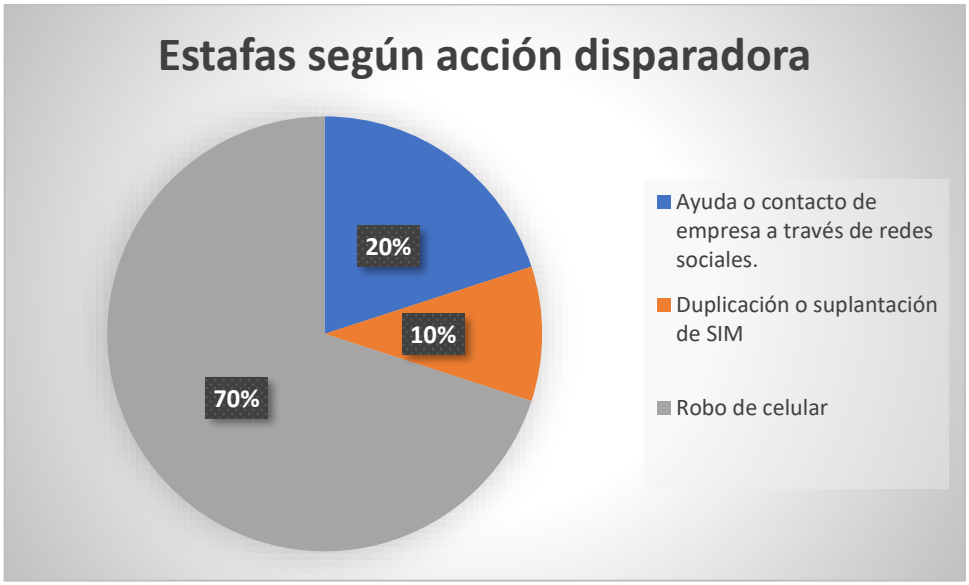
Fuente: Elaboración propia

En la Tabla y el Gráfico 8, la encuesta muestra que el daño más frecuente a las personas que padecieron estafas digitales fue el robo de dinero en cuenta (41%), seguido de compras a su nombre (35%) y toma de préstamos (18%).

Tabla 9: Estafas según acción disparadora

Respuesta	**Cantidad**
Ayuda o contacto de empresa a través de redes sociales.	4
Duplicación o suplantación de SIM	2
Robo de celular	14
Total	20

Gráfico 9: Estafas según acción disparadora



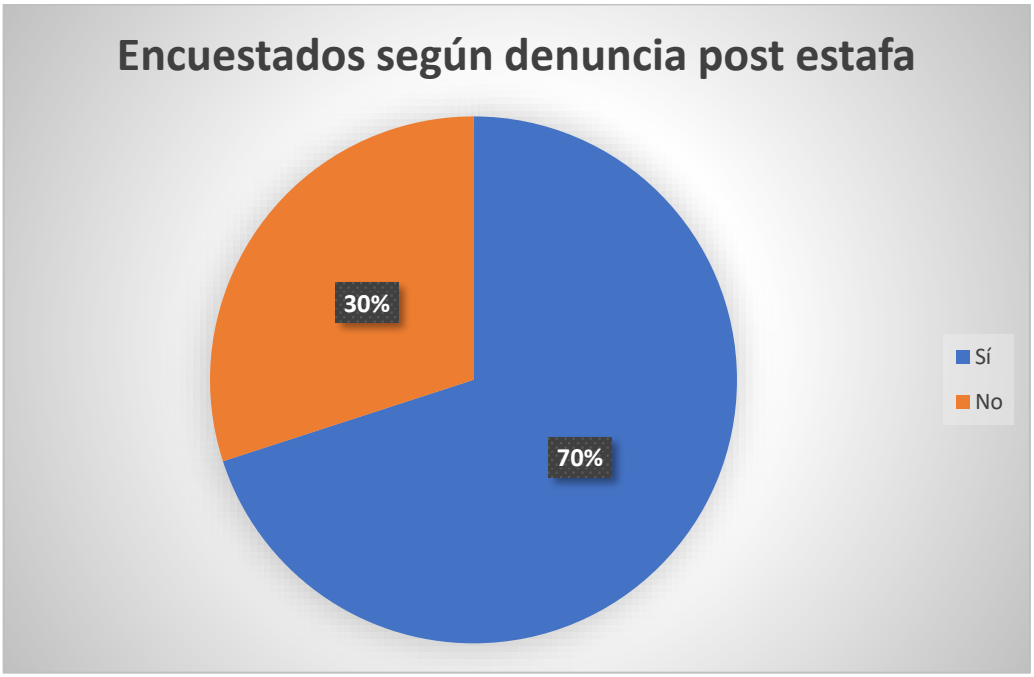
Fuente: Elaboración propia

En la Tabla y el Gráfico 9, la encuesta exhibe que la acción disparadora más frecuente de estafas digitales es el robo del celular (74%), seguida por la supuesta ayuda o contacto de empresa a través de redes sociales (21%) y, por último, la duplicación o suplantación de SIM. Añadiremos que, en este tiempo, el hurto de celular es uno de los más habituales, además, esta situación se vincula con el uso del celular como dispositivo casi excluyente.

Tabla 10: Encuestados según denuncia post estafa

Respuesta	**Cantidad**
Sí	14
No	6
Total	20

Gráfico 10: Encuestados según denuncia post estafa



Fuente: Elaboración propia

En la Tabla y el Gráfico 10, la encuesta arroja que la mayoría de las personas que padecieron estafas digitales hicieron la denuncia (70%). No obstante, no hay que perder de vista el porcentaje de personas que no realizan la denuncia (30%) dado que esto genera subregistros.

Tabla 11: Encuestados según comunicación con la empresa post estafa

Respuesta	**Cantidad**
Sí	18
No	2
Total	20

Gráfico 11: Encuestados según comunicación con la empresa post estafa

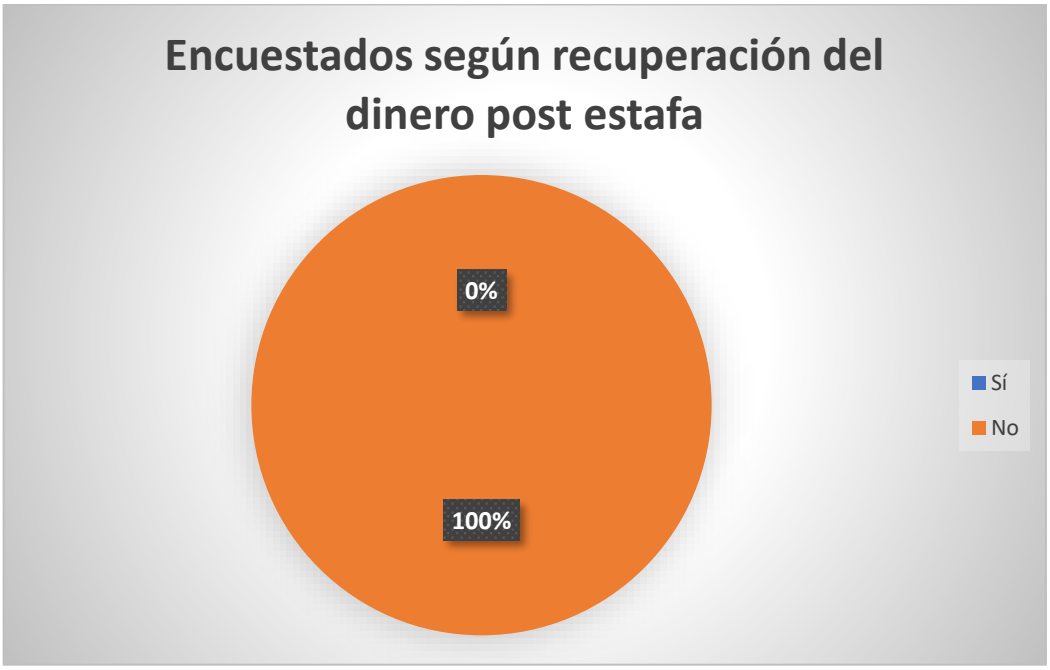
Fuente: Elaboración propia

En la Tabla y el Gráfico 11, la encuesta revela que la mayoría de las personas que padecieron estafas digitales lo comunicó a la empresa proveedora relacionada con la misma (90%). No obstante, es indispensable poner foco en el porcentaje de personas que no realizan la comunicación (10%) dado que esto distorsiona la percepción de seguridad / inseguridad / trazabilidad / mecanismos de mitigación del fraude que las empresas tienen acerca de sus prestaciones.

Tabla 12: Encuestados según recuperación del dinero post estafa

Respuesta	**Cantidad**
Sí	0
No	20
Total	20

Gráfico 12: Encuestados según recuperación del dinero post estafa



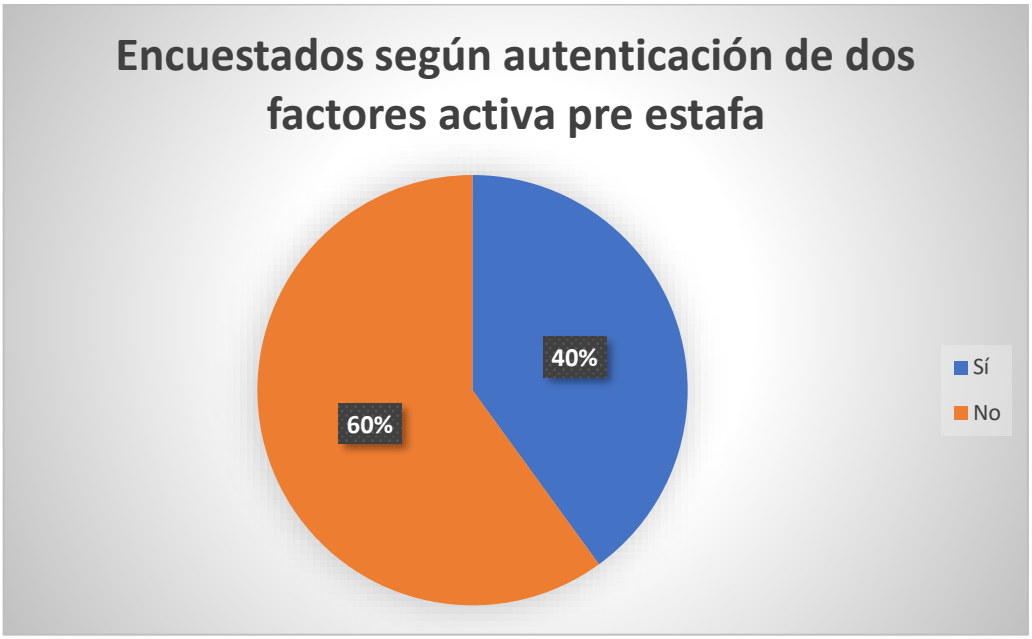
Fuente: Elaboración propia

En la Tabla y el Gráfico 12, la encuesta revela que ninguna de las personas de la muestra, afectadas por delitos digitales, recuperó el dinero (100%). Esto opera como desmotivador de la denuncia aunque se explica en función a la facilidad con la que los delincuentes pueden derivar medianas y pequeñas sumas de dinero. Si lo vinculamos al robo de celulares mencionado en preguntas anteriores, también se trata de un delito subdenunciado.

Tabla 13: Encuestados según autenticación de dos factores activa pre-estafa

Respuesta	**Cantidad**
Sí	8
No	12
Total	20

Gráfico 13: Encuestados según autenticación de dos factores activa pre-estafa



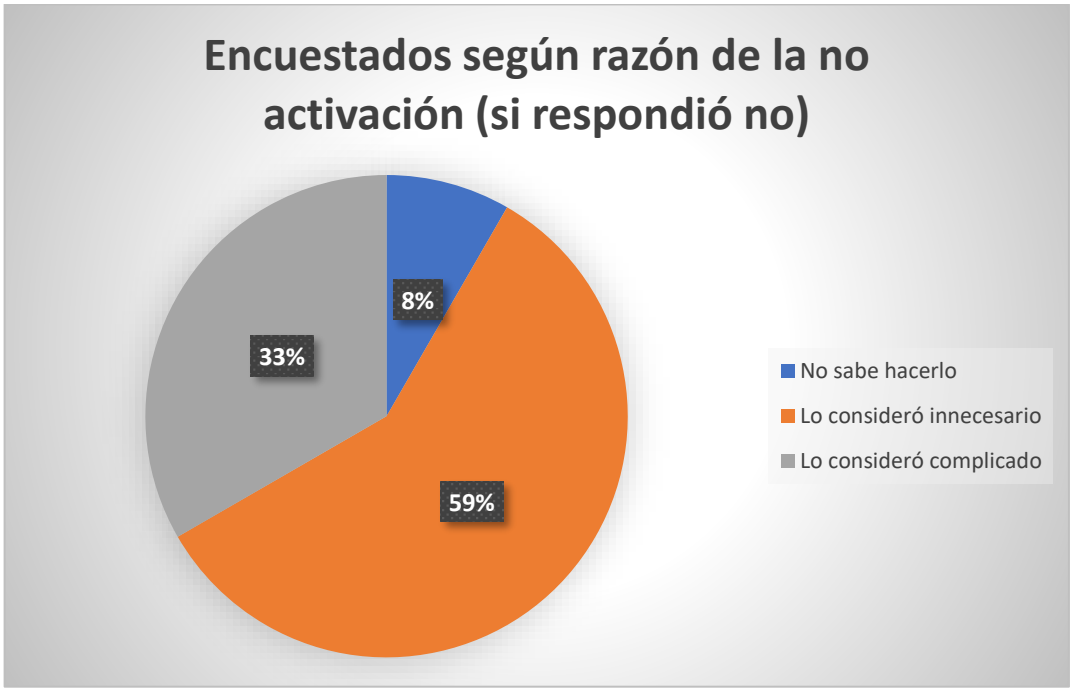
Fuente: Elaboración propia

En el Gráfico y la Tabla 13, la encuesta revela que la mayoría de las personas que padecieron estafas digitales no tenía autenticación de dos factores activa (60%), medida de prevención recomendada por especialistas. Sólo el 40% contaba con la medida activada. Esto potencia la vulnerabilidad de los entrevistados ante el posible robo o pérdida del dispositivo.

Tabla 14: Encuestados según razón de la no activación (si respondió no)

Respuesta	**Cantidad**
No sabe hacerlo	1
Lo consideró innecesario	7
Lo consideró complicado	4
Total	12

Gráfico 14: Encuestados según razón de la no activación (si respondió no)



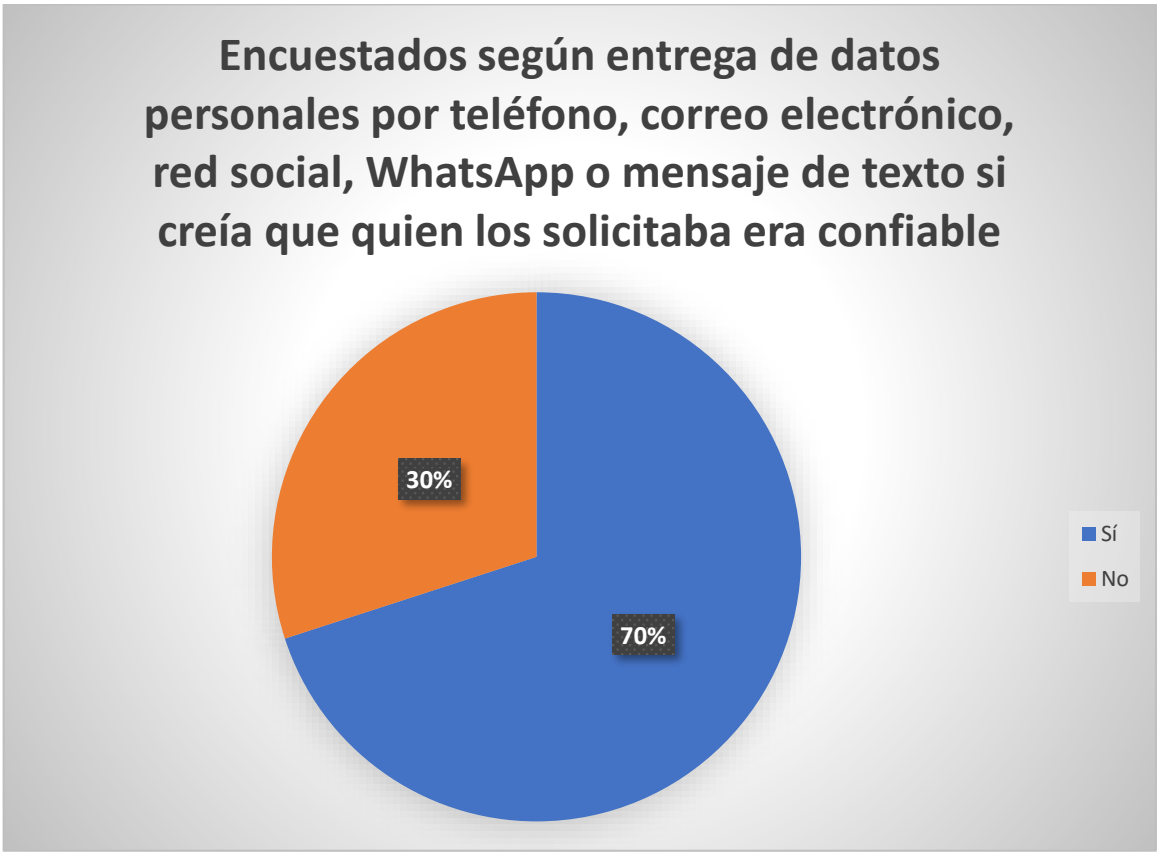
Fuente: Elaboración propia

En el Gráfico y la Tabla 14, la encuesta expresa que la mayoría de las personas que padecieron estafas digitales no realizaron la autenticación en dos pasos porque lo consideraron innecesario (59%). Esta respuesta es seguida por quienes lo percibieron complicado (33%). En último lugar se encuentran quienes no saben hacerlo (8%).

Tabla 15: Encuestados según entrega de datos personales (usuarios, claves, contraseñas, pin, token, DNI original o fotocopia, foto), por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto si creía que quien los solicitaba era confiable

Respuesta	**Cantidad**
Sí	14
No	6
Total	20

Gráfico 15: Encuestados según entrega de datos personales (usuarios, claves, contraseñas, pin, token, DNI original o fotocopia, foto), por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto si creía que quien los solicitaba era confiable



Fuente: Elaboración propia

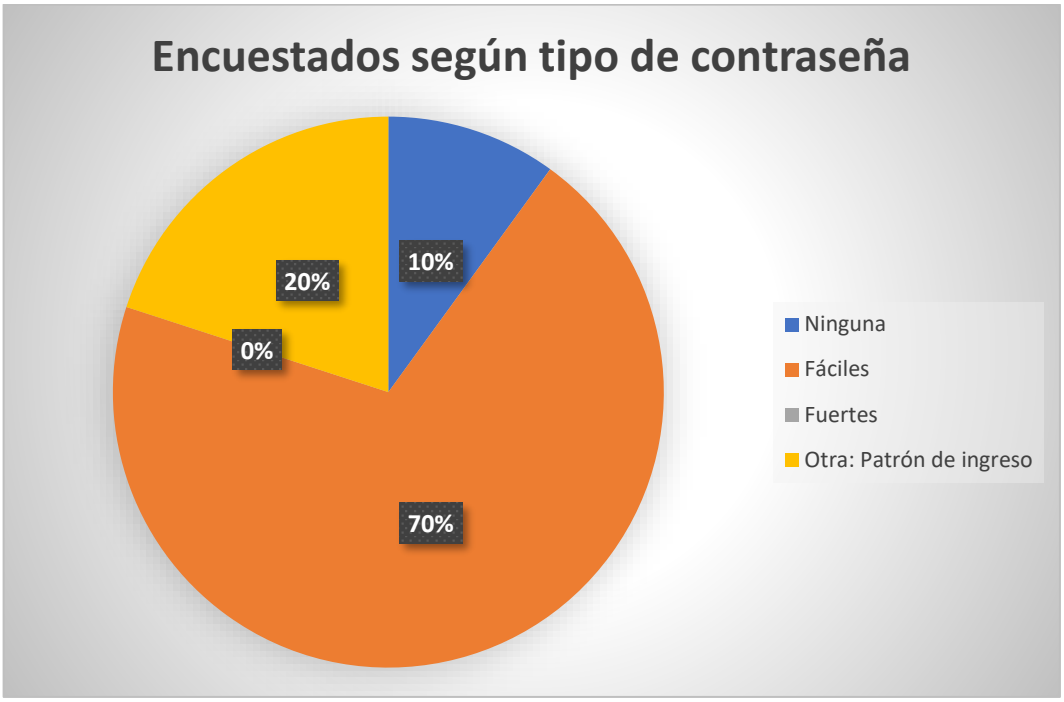
En el Gráfico y la Tabla 15, la encuesta evidencia que la mayoría de los individuos que padecieron estafas digitales revelaba datos a personas que suponía confiables (70%) mientras que sólo la minoría (30%) no lo hacía. Esto pone en riesgo la privacidad de los datos[6] y facilita las estafas digitales aumentando la vulnerabilidad de estos individuos.

Tabla 16: Encuestados según tipo de contraseña

Respuesta	**Cantidad**
Ninguna	2
Fáciles	14
Fuertes	0
Otra: Patrón de ingreso	4
Total	20

[6] Las medidas de seguridad recomendadas son básicas y no constituyen una lista definitiva sino ilustrativa.

Gráfico 16: Encuestados según tipo de contraseña



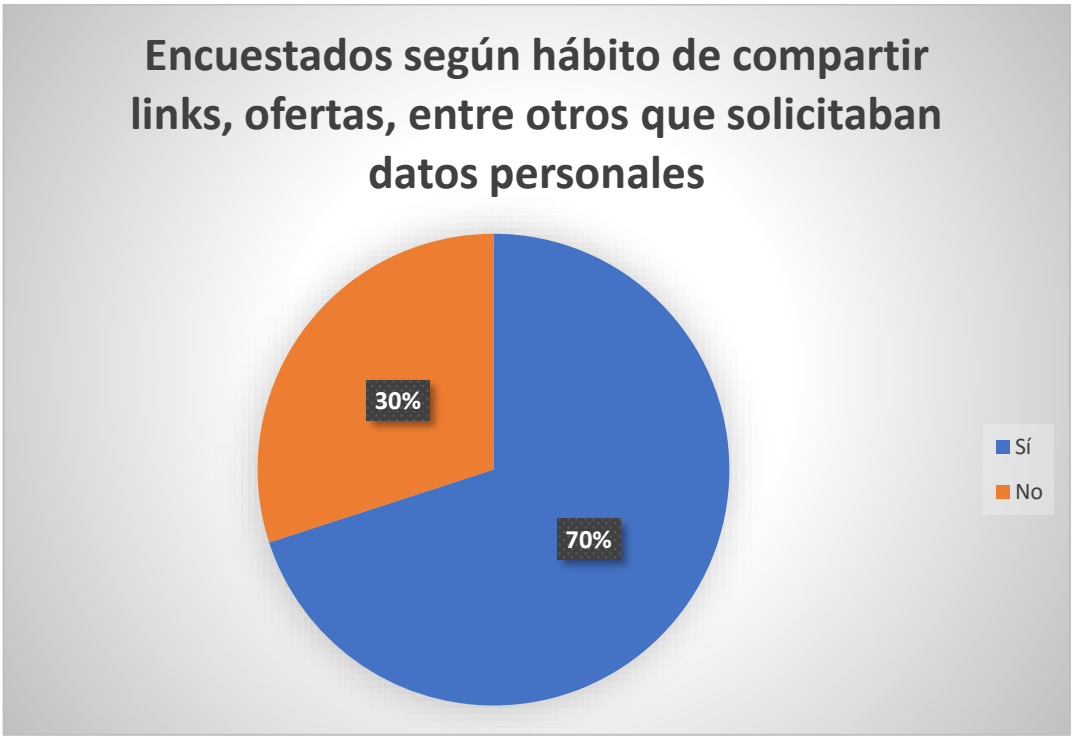
Fuente: Elaboración propia

En el Gráfico y la Tabla 16, la encuesta devela que la mayoría de las personas que padecieron estafas digitales utilizaba contraseñas fáciles para poder recordarlas (70%). Esta respuesta es seguida por quienes utilizaban un patrón de ingreso (20%), a posteriori continúan quienes no tienen ninguna contraseña en uso (10). Ninguno de los encuestados afirma utilizar una contraseña fuerte (0%). Esto incrementa el peligro de estafa virtual de los encuestados.

Tabla 17: Encuestados según hábito de compartir links, ofertas, entre otros que solicitaban datos personales

Respuesta	**Cantidad**
Sí	14
No	6
Total	20

Gráfico 17: Encuestados según hábito de compartir links, ofertas, entre otros que solicitaban datos personales



Fuente: Elaboración propia

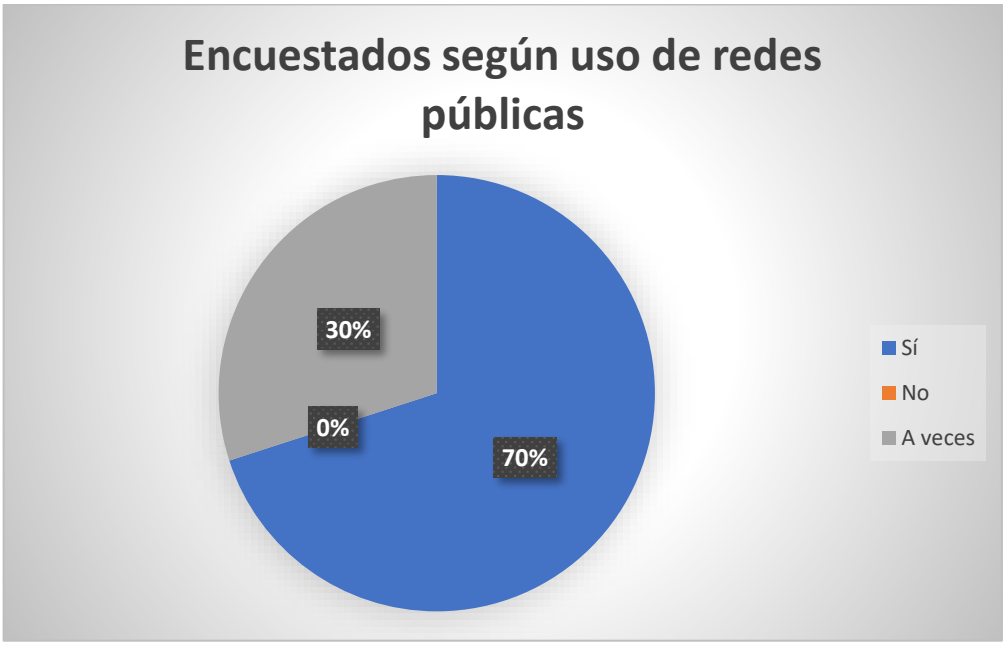
En el Gráfico y la Tabla 17, la encuesta revela que la mayoría de las personas, al momento de la estafa, compartía links con datos personales (70%), sólo la minoría de los encuestados no lo hacía (30%). Esto pone en riesgo la privacidad de los datos y la seguridad de las transacciones aumentando la vulnerabilidad de estos individuos al phishing[7].

Tabla 18: Encuestados según uso de redes públicas

Respuesta	**Cantidad**
Sí	14
No	0
A veces	6
Total	20

[7] Los cibercriminales fingen ser cuentas legítimas.

Gráfico 18: Encuestados según uso de redes públicas



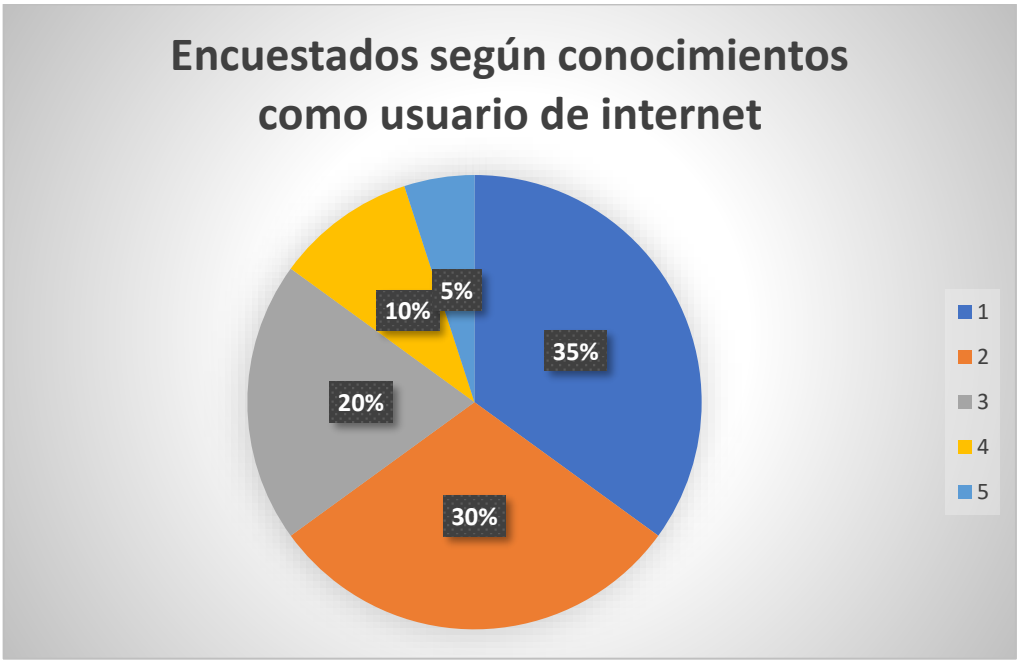
Fuente: Elaboración propia

En el Gráfico y la Tabla 18, la encuesta expresa que la mayoría de las personas, al momento de la estafa, utilizaba redes públicas (70%) o lo hacía eventualmente (30%) mientras que nadie afirma no haberlas utilizado (0%). Esto pone en riesgo, la privacidad y la seguridad de las transacciones electrónicas de las personas encuestadas.

Tabla 19: Encuestados según conocimientos como usuario de internet

Respuesta	**Cantidad**
1	7
2	6
3	4
4	2
5	1
Total	20

Gráfico 19: Encuestados según conocimientos como usuario de internet



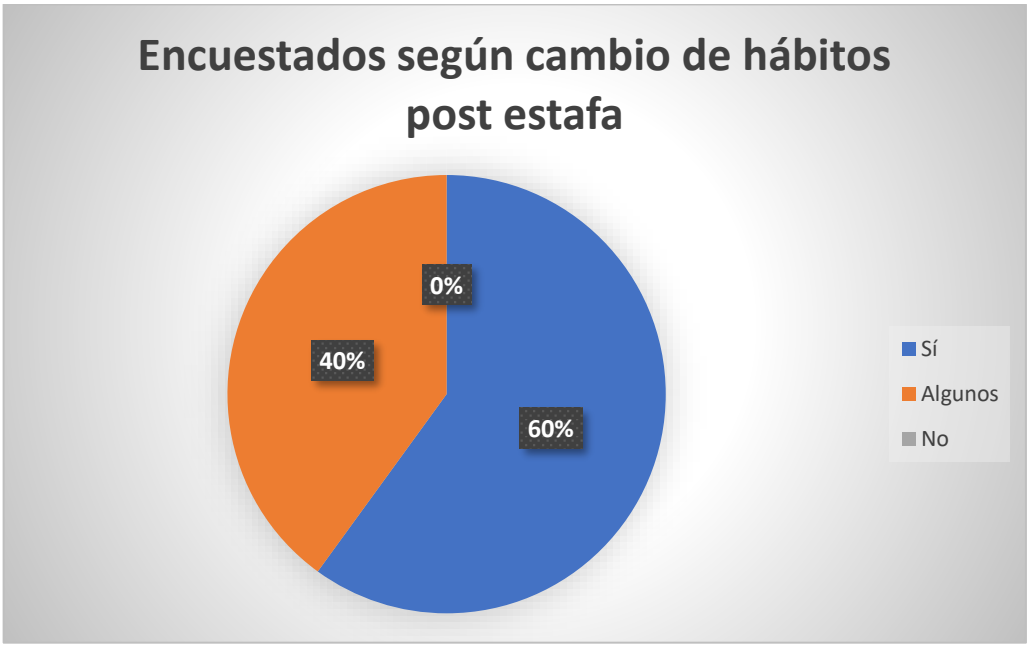
Fuente: Elaboración propia

En el Gráfico y la Tabla 19, la encuesta revela que la mayoría de las personas, al momento de la estafa digital, consideraba tener un conocimiento como usuario de internet de nivel 1 (muy bajo, el 35%), seguidas por los niveles 2 (bajo, el 30%) y 3 (medio, el 20%). Pocos encuestados definen sus conocimientos como 4 (altos, el 10%) o 5 (muy altos, el 5%). Esto llama a la reflexión respecto a la necesidad de que, al mismo tiempo que la inclusión financiera, se promueva la educación en el uso de dispositivos electrónicos con énfasis en los riesgos que estos implican para la seguridad de las personas y sus bienes.

Tabla 20: Encuestados según cambio de hábitos post estafa

Respuesta	**Cantidad**
Sí	12
Algunos	8
No	0
Total	20

Gráfico 20: Encuestados según cambio de hábitos post estafa



Fuente: Elaboración propia

En el Gráfico y la Tabla 20, la encuesta muestra que la mayoría de las personas, después de la estafa digital, asegura haber cambiado sus hábitos como usuario de internet (60%). Estas personas son seguidas por quienes cambiaron algunos de sus hábitos (40%), ningún entrevistado manifiesta no haberlos cambiado (0%). Esto implica que los cambios actitudinales respecto al uso de internet, en numerosas personas, recién se producen una vez que han sufrido una estafa virtual.

4. DISCUSIÓN Y CONCLUSIONES

La pandemia de COVID 19 aceleró un proceso de inclusión financiera que, de todos modos, ya estaba avanzando a la par del aumento del comercio electrónico. Coincidimos con Sánchez (2019) respecto a que los datos son el nuevo oro de esta etapa de las transacciones comerciales del mundo global.

Subrayamos, junto a Iannicelli (2021), que la razón por la que las estafas digitales se disparan en pandemia obedece a que grandes masas de usuarios inexpertos pasan muchas horas conectadas.

Conforme a lo investigado, acordamos con Sánchez (2019), en que la educación en seguridad cibernética, a toda la población, debe ser continua dado el potencial de daño del cibercrimen. Es por esto que los ciudadanos tienen que estar preparados para proteger sus bienes y su información y tomar buenas decisiones en tiempo real.

Como se desprende de este trabajo, Miramar es la ciudad con mayor incidencia de estafas en el partido de General Alvarado. Esta cifra se encuentra en aumento conforme a los periodos comparados. En cuanto a la condición demográfica de las personas estafadas, afecta por igual a hombres y mujeres aunque los casos se incrementan cuando aumenta la edad. Esta última cuestión destaca la relevancia del rol pedagógico que deben ejercer quienes pretendan incursionar en la economía plateada[8].

Asimismo, adherimos a Sánchez (2019) cuando manifiesta la importancia de que las empresas inviertan en seguridad informática convencional y en seguridad contextual. Esta última es un análisis, a cargo de las empresas proveedoras, destinado identificar posibles amenazas, a partir del comportamiento de cada usuario, a fin de brindarle un aprendizaje personalizado.

Al respecto, retomando la cuestión de Miramar, diremos que según Info Blanco Sobre Negro (10 de junio de 2023), la jueza Grahl falla contra Banco Provincia de Buenos Aires en un caso de estafa digital, aludiendo problemas en su sistema de seguridad, indiferencia a los reclamos de los usuarios y obligatoriedad en el uso de

[8] Venta de bienes y servicios orientados a la tercera edad,

los canales electrónicos. Esto implica que los clientes son empujados a digitalizar sus vidas sin entrenamiento en seguridad y, además, suelen ser culpabilizados cuando padecen una estafa[9].

Como hemos visto, dado que en el siglo XXI no es posible prescindir de los dispositivos digitales que facilitan la vida social, laboral y económica de las personas, es preciso encarar la problemática con enfoque preventivo tanto en la referida formación en tecnología de los individuos como en la mejora de la experiencia de los usuarios de las plataformas y aplicaciones.

Por otra parte, las empresas proveedoras de portales y billeteras digitales, además de aumentar la inversión en ciberseguridad (expertos, software, certificados de seguridad, entre otros) deben brindar alguna instancia de atención humana con amplia disponibilidad horaria para garantizar el acceso seguro y responsable.

Conforme a nuestro trabajo, la billetera que más se utiliza en Miramar es la de Cuenta DNI, seguida por la de Mercado Pago (entre una inúmera variedad de billeteras); mientras que la billetera que más estafas recibe es la de Mercado Pago, seguida por Cuenta DNI. Por ende, observamos que la incidencia se vincula a una mayor tasa de uso, dado que los ciberdelincuentes se inclinan por éstas.

El dispositivo más usado por quienes fueron estafados es el celular que es el dispositivo más común en la población, el que utilizan para la comunicación, compras y aplicaciones bancarias, la mayoría de los ciudadanos. El daño al patrimonio más frecuente es el robo de dinero en cuenta, seguido de compras a nombre del damnificado y toma de préstamos.

Señalaremos que el disparador de estos delitos es el robo de celular. También observaremos que, según el periódico Ámbito (23 de octubre de 2023), en nuestro país se roban 10.000 celulares por día, alrededor de 7 celulares por minuto. Destacaremos entonces la importancia que adquieren, tanto el combate a organizaciones delictivas que cometen este tipo de ilícitos, como las medidas de seguridad que deben implementar los damnificados (bloqueo, comunicación a la empresa proveedora, denuncia a las autoridades).

[9] Lo traemos a la discusión dado que sucedió en el periodo estudiado por este trabajo.

Las personas estafadas se caracterizan por las malas prácticas, en cuanto a las medidas preventivas para usuarios de celular, dado que carecen de contraseñas fuertes, la mayoría no utiliza la autenticación en dos pasos, comparten datos personales a través del dispositivo (con personas que creen conocer), comparten links sin estar seguros de su procedencia (posible phishing), usan redes públicas y tienen bajo conocimiento de internet[10] aunque aseguran que mejoraron sus habilidades después de la estafa. Esto se vincula a la digitalización compulsiva sin la formación ya mencionada.

Además, respecto a la reacción ante la estafa, diremos que la mayoría de las personas estafadas, aunque no todas, realiza la denuncia y/o se comunica con la empresa proveedora (banco, billetera) aunque no recuperan el dinero.

A su vez, Bouguet Abiotti (2021) se centra en los vacíos legales que facilitan el aumento de la ciberdelincuencia y en la lentitud que caracteriza las investigaciones. Al respecto, diremos que las penas por suplantación de identidad digital orientada a la comisión de una estafa son bajas y no desalientan el accionar criminal.

Igualmente, la batalla contra el cibercrimen no se restringe a la creación o modificación de tipos penales (aunque es indispensable) sino que requiere de un trabajo pertinente, ininterrumpido y riguroso por parte de las fiscalías especializadas a cargo junto a las fuerzas policiales.

Sobre este particular, enfatizaremos la importancia del primer paso de este circuito que es la denuncia en la comisaría u oficina receptora (a la que algunos de los encuestados de Miramar son reticentes) seguida del resguardo de la prueba (chats, capturas de pantalla) del modo en que lo determinen los investigadores.

Por su parte, Iannicelli (2021) manifiesta que la Ley Nacional 26.388 coloca a la Argentina junto a los estados que reconocen la omnipresencia de las TIC (Tecnologías de la Información y la Comunicación) en la sociedad dado que sustituye e incorpora figuras típicas para complementar los medios de comisión de los delitos previstos en el articulado del Código.

[10] La lista es sólo ilustrativa.

Coincidimos con Iannicelli (2021) respecto a que los principales damnificados de estas estafas son los usuarios comunes, dada la baja seguridad que tienen en sus dispositivos y la cantidad de información que portan a diario en estos (nombres de usuario, claves bancarias, números de tarjetas de crédito).

También acordamos con Iannicelli (2021) cuando asegura que la estrategia más habitual a la que apelan los delincuentes es la ingeniería social dado que generan ardides como una comunicación a través de WhatsApp o un phishing rudimentario en el que fingen que se trata de una comunicación oficial.

Pese a los diagnósticos y recomendaciones, los tiempos de la justicia no satisfacen las necesidades de los usuarios digitales que, en ocasiones, quedan desprovistos de todo su capital financiero en pocos minutos, este es un posible factor desmotivador para la radicación de la denuncia.

Por fin, no podemos ignorar que la ciberdelincuencia es un negocio a gran escala cuya desarticulación requiere compromiso de los usuarios así como capital y recursos humanos destinados a la pedagogía y prevención así como a la investigación en el área. Esto junto al férreo compromiso de los gobiernos y las agencias estatales.

PROPUESTAS

Incrementar la difusión de campañas informativas convocando a todos los sectores de la población comprometidos con la seguridad ciudadana, instituciones bancarias proveedoras de billeteras electrónicas, instituciones financieras proveedoras de billeteras electrónicas, empresas de telefonía celular, entre otras.

Recomendaciones para las campañas adaptadas de organismos varios (BCRA, 2023; Argentina, 2024):

Comunicarse telefónicamente con el banco si existieran dudas ante una operación. El cliente debe generar la llamada, el banco debe disponer de una línea sólo a estos efectos.

No acceder al cajero, home banking ni billeteras virtuales siguiendo instrucciones desde una llamada que el usuario no originó.

No compartir datos personales mediante celular, correos electrónicos, redes sociales o servicios de mensajería.

No compartir códigos de activación de la cuenta de WhatsApp. Dejar visible la foto de la aplicación sólo para los contactos.

No seguir enlaces que el usuario recibe mediante correos electrónicos, redes sociales o servicios de mensajerías.

Seleccionar contraseñas fuertes, mezclando mayúsculas, minúsculas, números y símbolos. Crear un acrónimo para recordarlas, no escribirlas en papeles ni libretas que se transportan con documentos o en billetera o cartera. No dejarlas en la memoria de los dispositivos ni utilizar dispositivos de otras personas para realizar operaciones que requieran contraseñas.

No usar redes abiertas para acceder a portales, bancos o billeteras que requieran contraseñas.

Utilizar la doble autenticación en los equipos aunque esto conspire contra la velocidad de algunas operaciones.

Mantener actualizado el equipo, los sistemas y las aplicaciones. No instalar aplicaciones de dudosa procedencia.

Aprender a diferenciar perfiles verdaderos y perfiles falsos, también urls verdaderas y urls falsas. No ingresar si se presentan sospechas o se cree que se trata de spam.

Leer con atención los mensajes dado que los perfiles y cuentas falsas suelen tener faltas de ortografía, errores de redacción, demasiadas mayúsculas o propuestas excesivamente tentadoras. Redoblar la atención cuando la supuesta oferta / promoción se corresponde con promociones o noticias que se dieron a conocer por otros medios (aniversarios de entidades o supermercados).

Chequear las medidas de seguridad recomendadas por las instituciones bancarias y financieras.

Prestar atención a las nuevas recomendaciones respecto a delitos con inteligencia artificial como duplicación de voz, usar palabras de seguridad para instrucciones financieras que procedan de familiares y conocidos a través de dispositivos.

Es indispensable tomarse tiempo antes de actuar.

Por fin, si la estafa se produjo, es necesario comunicarlo a los proveedores relacionados además de denunciar y seguir las instrucciones y recomendaciones para conservar las pruebas. Las denuncias pueden hacerse en comisarías, en fiscalías o mediante la línea 137, sin importar el flujo de trabajo las diferentes dependencias deben estar receptivas a esta modalidad delictiva que afecta el patrimonio, los bienes y el bienestar de las personas.

BIBLIOGRAFÍA

Acurio del Pino, S (2016): *Delitos informáticos: generalidades*. Quito: PUCE:

Ámbito (13 de octubre de 2023). Alerta por ciberdelitos: ¿cómo funciona el robo de datos bancarios en celulares Android? En: *Ámbito*. Disponible en: https://www.ambito.com/tecnologia/alerta-ciberdelitos-como-funciona-el-robo-datos-bancarios-celulares-android-n5843785 Última consulta: 1/03/2024

Archenti, N. (2007). El sondeo. En A. Marradi, N. Archenti y J.I. Piovani (Eds.), *Metodología de las Ciencias Sociales* (pp. 203-2014). Buenos Aires: Emecé.

Argentina (2024). Recomendaciones para evitar fraudes informáticos a través de WhatsApp. *Argentina*. Disponible en: https://www.argentina.gob.ar/seguridad/ciberdelito/para-pensa-conectate-argentina/recomendaciones-para-evitar-fraudes Última consulta: 18/04/2024

BCRA (2022a). Comunicación A7462. Normas sobre Proveedores de servicios de pago. Adecuaciones. Servicio de billetera digital. Registro de billeteras digitales interoperables. *BCRA*: Disponible en: https://www.bcra.gob.ar/pdfs/comytexord/A7462.pdf Última consulta: 9/03/2023

BCRA (2022b). Informe de Inclusión Financiera - Síntesis Ejecutiva. *BCRA*: Disponible en: https://www.bcra.gob.ar/PublicacionesEstadisticas/informe-inclusion-financiera-012022.asp Última consulta: 9/03/2023

BCRA (2023). Cómo prevenir estafas. *BCRA*. Disponible en: https://www.bcra.gob.ar/bcrayvos/Como-prevenir-estafas-virtuales.asp

Bork, I. (2021). *Diversificación de la oferta turística de Miramar a través del Turismo Rural.* [Tesis de Grado] Universidad Nacional del Sur. Buenos Aires. Disponible en: https://repositoriodigital.uns.edu.ar/bitstream/handle/123456789/5769/TESIS%20BORK.pdf Última consulta: 9/03/2023

Bouguet Abiotti, G. (2021). *Ciberdelitos en Argentina: la falta de legislación de ciertas conductas lesivas realizadas a través de tecnologías de la información y comunicación.* [Tesis de Grado] Universidad de Belgrano. Ciudad Autónoma de

Buenos Aires. Disponible en: http://repositorio.ub.edu.ar/handle/123456789/9847 Última consulta: 9/03/2023

CACE (2022). Medios de pago. *CACE.* Disponible en: https://cace.org.ar/educacion_categoria/medios-de-pago/ Última consulta: 9/03/2023 Última consulta: 9/03/2023

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación*. México D.F.: McGraw-Hill.

Info Blanco Sobre Negro (10 de junio de 2023). Dictaron otro fallo contra el Banco Provincia, esta vez por una ciberestafa que sufrió una docente de Miramar. En: *Info Blanco Sobre Negro*. Disponible en: https://www.infoblancosobrenegro.com/nota/96711/dictaron-otro-fallo-contra-el-banco-provincia-esta-vez-por-una-ciberestafa-que-sufrio-una-docente-de-miramar/ Última consulta: 19/03/2024

Infoleg (2023). *Código Penal de la Nación Argentina.* Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm Última consulta: 19/03/2024

OCEDIC – Austral. (2022). *Ciberfraudes: criptoactivos y blockchain.* Buenos Aires: Editorial Universidad Austral.

Perfil. (12 de marzo de 2024). Cayó una banda argentina de "cripto-hackers" que robó US$ 800 mil a una empresa británica. En: *Perfil*. Disponible en: https://www.perfil.com/noticias/economia/cayo-banda-cripto-hackers-que-robo-us-800-mil-empresa-britanica.phtml Última consulta: 9/03/2023

Riso, N. (23 de mayo de 2022). Cuáles son las estafas digitales más comunes. En: *Página12.* Disponible en: https://www.pagina12.com.ar/422319-cuales-son-las-estafas-digitales-mas-comunes Última consulta: 9/03/2023

Sánchez, M. (2019). *Billetera Virtual ventajas y desventajas de su implementación en Argentina.* Buenos Aires: Universidad de San Andrés. [Tesis de Maestría] Disponible en: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16752/1/%5BP%5D%5BW%5D%20T.%20M.%20Ges.%20S%C3%A1nchez%2C%20Mar%C3%ADa%20Jimena.pdf Última consulta: 9/03/2023

Sautú, R. (2003). *Todo es teoría. Objetivos y métodos de investigación*. Buenos Aires: Lumiere.

ANEXOS

GRÁFICOS.