Licenciatura en Seguridad Pública

TESINA

“Ciberdelito y vulnerabilidad del Sistema Bancario en la provincia de Mendoza”

Estudiante: Teixido, Guillermo

Director de Tesina: Lic. Carlos Tomás Puebla

Coordinación de Tesina: Lic. Graciela Matricani

Mendoza, diciembre 2021

Agradecimientos

A mi familia, a mi esposa y mis hijas que me han acompañado en este proceso de estudio, durante tantas horas. Las amo.

A mi director de tesis que estuvo en todo momento a mi lado

A la Licenciada Graciela Matricani y a Mónica Ferreyra por su dedicación y acompañamiento durante todo el trabajo.

Especialmente a mis compañeros de grupo, Claudio, Pablo, Alfredo, Lorena, Tucho, al más chiquito, Leonel, que le dio energía al grupo, y todos los que comenzamos juntos en la carrera, y seguimos apoyándonos hasta el día de hoy

A mis camaradas de Seguridad Bancaria que aportaron sus conocimientos y me ayudaron a buscar información

A Maricel Martín, comisario de la Policía de Córdoba que tantos aportes me ha brindado, guiándome en los temas de tesis en forma incondicional.

A todos ellos muchas gracias por todo el compromiso que me han brindado.

Introducción

El año 2020 marcó un punto de inflexión trascendente en Argentina y el mundo con la aparición de la pandemia de Covid-19 la cual generó cambios coyunturales en la vida cotidiana de todos los ciudadanos. Las comunicaciones vía utilización de herramientas electrónicas con el acceso a Internet, marcaron las nuevas formas de comunicación que los seres humanos debieron adoptar a fin de evitar un posible contagio con una enfermedad desconocida. Frente a esto, los sistemas bancarios, como otros sistemas, debieron incrementar sus servicios online a fin de evitar que la gente concurriera a las sucursales bancarias y pudiera realizar sus trámites mediante Online Banking, ya sea, a través de diferentes dispositivos electrónicos como pueden ser una notebook, una PC, una tablet o celular.

Los medios más utilizados por los clientes se han convertido en un campo particular para el incremento de otros delitos que, si bien ya se venían registrando con anterioridad como el fraude, la extorsión o la suplantación de identidad, entre otros, durante el año de pandemia se incrementaron, adquiriendo nuevas modalidades. El *phishing* ya no solo consiste en mandar correos y vincular link, sino que esto además, se realiza utilizando WhatsApp y así obtener los datos privados necesarios para vaciar cuentas bancarias.

Indiscutiblemente la delincuencia informática bancaria se ha incrementado en los últimos años, aunque desde la aparición de la pandemia de Covid-19, el crecimiento de estos delitos, tanto a nivel mundial como nacional y provincial, ha crecido rápidamente no solo en cantidad de hechos, sino que además, se ha ido adaptando a la tecnología, elaborando nuevas formas delictivas. En consecuencia, el ambiente virtual e intangible de esta forma de delito origina confusión además, en su tipificación, como también complejiza las investigaciones que se llevan a cabo para su identificación.

Si bien en la gran mayoría de ataques bancarios los clientes son las víctimas preferidas, el espacio informático y el incremento de las comunicaciones, ha generado una mayor vulnerabilidad en algunos ciudadanos como son las personas mayores y los jubilados. Estos últimos eran los preferidos al momento de cobrar para los delincuentes, sin embargo, con el incremento del uso de la banca virtual, la vulnerabilidad de este grupo creció, haciéndolos víctimas de mayores estafas, incluso con una mayor complejidad en la constitución del hecho delictivo.

La modalidad destacada de estos ciberdelitos económicos se vincula con sustracción de identidad en cuentas bancarias, compras online, información falsa sobre el acceso a subsidios y/o ayudas estatales como producto de la pandemia, cambios de códigos de seguridad bancario para acceder a servicios falsos, información sobre cuenta inexistentes, utilización de sitios web clones que ofrecen préstamos rápidos, o la utilización de sitios web asociados a cuentas bancarias, todas estas modalidades implican la extracción de dinero de cuentas bancarias, generando fraude bancario con débito y tarjetas de créditos.

En definitiva, el uso masivo del sistema online por la pandemia, mostró la vulnerabilidad del Sistema Bancario frente al delito económico, o sea, lo que se denomina ciberdelito.

En el presente trabajo se ha partido de realizarse interrogantes que han permitido elaborar la investigación, con la finalidad de conocer en qué situación se encuentra la provincia de Mendoza, respecto al ciberdelito de fraude y estafa bancaria, como también observar cuáles han sido las medidas que se llevaron a cabo para dar respuesta a los usuarios, partiendo de preguntarse cómo ha impactado el uso masivo de la banca on line en el sistema bancario de la provincia de Mendoza, durante los años 2020 y 2021, como producto de su uso casi exclusivo, a fin de evitar o disminuir, los contagios de Covid-19. Para esto se han fijado los siguientes objetivos:

Objetivo general

Analizar el impacto del uso masivo de la banca online sobre el ciberdelito económico en el Sistema Bancario de la provincia de Mendoza en el contexto de pandemia de Covid-19, durante el período 2020 y 2021.

Objetivos específicos

Visibilizar el uso masivo del sistema de banca on line en el ciberdelito económico registrado en las entidades bancarias de nuestro país, en el contexto de pandemia de Covid-19.

Conocer el funcionamiento de la banca online, sus características particulares, y los instrumentos mediante los cuales funciona.

Definir los conceptos de ciberdelitos y su vinculación con los delitos económicos.

Estudiar las estrategias de prevención y control del Sistema de Seguridad Pública respecto a los ciberdelitos económicos.

Tomar como marco de análisis el funcionamiento del Sistema de Seguridad Bancario de la provincia de Mendoza y las estrategias de prevención y control del ciberdelito económico, en el contexto del Sistema de Seguridad Pública.

Planteamiento de la hipótesis

El uso masivo de la banca online en el contexto de pandemia, en el período 2020 y 2021, en la provincia de Mendoza, evidenció la vulnerabilidad del Sistema de Seguridad Bancario frente al ciberdelito económico.

Metodológicamente esta investigación es de campo con un diseño flexible, ya que combina diferentes tipos de técnicas. El alcance es descriptivo dado que pretende dar cuenta de los eventos que corresponden al ciberdelito económico, y cómo este se ha desarrollado en la provincia de Mendoza durante el período de estudio. Los estudios de alcance descriptivo, buscan describir, como su nombre lo menciona, los eventos o las circunstancias en que se dan determinados fenómenos, en este caso los ciberdelitos económicos que han vulnerado los sistemas. Por otro lado, estos estudios buscan especificar las propiedades y características de los grupos de personas y/o fenómenos estudiados y sometidos al análisis del investigador.

Además, el estudio es de alcance explicativo, ya que pone de manifestó cuáles son las causas que permiten que este tipo de hechos delictivos, se produzcan en el ámbito bancario. A partir del análisis, se podrá realizar una explicación respecto a las circunstancias en que estos fenómenos se manifiestan, luego de haber descripto las características particulares del objeto de estudio. Los trabajos con alcance explicativo buscan encontrar una explicación del porqué ocurren los fenómenos y en qué circunstancias se dan los mismos. Estas investigaciones dirigidas a responder sobre las causas de los eventos sociales, permiten proyectar predicciones que sostengan que, en iguales condiciones sobre objetos similares, ciertas causas pueden provocar otros efectos.

El trabajo de campo analiza el funcionamiento del Sistema Bancario de Mendoza, el cual se constituye en una de las unidades de análisis de la investigación, junto con las estrategias de prevención y control del ciberdelito económico. Para ello, se analizan las fuentes secundarias y fuentes primarias. En cuanto a las fuentes secundarias, estas están compuestas por los datos obtenidos de la Asociación Argentina de Lucha Contra el Ciber Crimen (AALCC); Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y Defensa al Consumidor. Estas instituciones recopilan el conjunto de denuncias e intervenciones que realizan las policías de todo el país, incluyendo la provincia de Mendoza. La UFECI, es la encarga de agrupar las denuncias de la provincia, las cuales son investigadas por el personal policial de Ciberdelitos Económicos. Mientras que la Dirección de Defensa al Consumidor agrupa los datos estadísticos correspondientes a las denuncias que llegan a esta institución y que luego son derivadas a la UFECI, en caso de que se constituyan en hechos delictivos.

Para la obtención de fuentes primarias se realiza una guía de entrevista la cual se aplica a los actores sociales involucrados en el tema de los ciberdelitos económicos que se observan en el ámbito bancario.

Esta investigación ha sido organizada en los siguientes capítulos:

Capítulo I se presenta la situación del Sistema Bancario Argentino y su funcionamiento durante el contexto de pandemia de Covid-19. Además, se muestra cómo ha evolucionado el mismo hasta la digitalización de la banca, detallando la implementación de las medidas extraordinarias que se debieron adoptar a partir del año 2020 como consecuencia de la aplicación de las medidas de A.S.P.O. y D.I.S.P.O.

En el Capítulo II se presenta la constitución del Sistema Bancario Argentino y la relación que se establece con los clientes. Para esto se describen las conceptualizaciones de clientes, funcionamiento de la modalidad presencial de atención a los clientes, y las características que a lo largo del tiempo, ha ido adquiriendo la atención on line, hasta llegar a las aplicaciones móviles. Por otro lado, incluye el ciberdelito económico como la modalidad delictiva particular en el ámbito bancario.

En el Capítulo III se explicitan las estrategias de prevención y control del ciberdelito económico desde la Seguridad Pública, en el marco de la Ley 6721/1999 y la normativa

legal vigente destinada al abordaje del ciberdelito económico. Además, se incluyen las medidas que ha llevado adelante el Banco Central de la República Argentina a fin de incentivar al Sistema Bancario a adoptar las medidas preventivas de seguridad correspondientes.

En el Capítulo IV se desarrolla el trabajo de campo en el cual se presentan los datos estadísticos obtenidos, como también las entrevistas realizadas a los actores que intervienen, desde diferentes espacios, en la problemática. En el mismo se realiza la discusión de los resultados a la luz de los aspectos teóricos obtenidos.

Finalmente se presentan las conclusiones y aportes al tema.

Marco contextual

Capítulo I

Funcionamiento del Sistema Bancario en Argentina, en el contexto de pandemia

Durante el año 2020 se produjo a nivel mundial, la pandemia de Covid-19, lo que generó que se produjeran un conjunto de cambios coyunturales en diferentes esferas de la vida cotidiana de todos los habitantes del mundo.

Como consecuencia de esta situación, el mundo entero recurrió al confinamiento para evitar o disminuir los contagios. Una vez adoptada esta medida, se debió recurrir al uso de Internet, como medio de comunicación exclusivo, utilizado tanto en todos los ámbitos, más allá de las comunicaciones personales. La educación, el trabajo, incluso la atención en salud, comenzaron a adquirir nuevas modalidades de contacto, evitando la aglomeración de personas en espacios comunes. Entre ellos el sistema bancario.

En el presente capítulo se describen las acciones que debieron desarrollarse en la atención bancaria a fin de evitar que las personas concurrieran a las instituciones bancarias. Sin embargo, como veremos, muchas fueron las dificultades que se debieron afrontar.

1.1 Situación del Sistema Bancario

En el sistema bancario, las medidas de confinamiento, llevaron a que se debiera recurrir a la adquisición de nuevas formas de relaciones con los usuarios. Se potenció así la utilización de sistemas virtuales como la banca electrónica, la creación de aplicaciones específicas bancarias que les permitieron a los usuarios acceder a su información y realizar todo tipo de transacciones, desde sus casas a través de computadoras, *tablets* y/o *smartphone*.

Este aumento de conectividad que debieron generar los sistemas bancarios permitió a su vez, crear un nuevo campo para el ciberdelito, incrementando las acciones delictivas que ya se venían registrando y perfeccionando las metodologías delictivas.

La PwC Argentina realizó una encuesta, durante el mes de mayo de 2021, en la que midieron los impactos del Covid-19 en la industria bancaria. La misma arrojó resultados interesantes, que se detallan:

> "El 62% de las entidades considera que el COVID-19 tuvo un impacto de medio a alto en la continuidad de su negocio. Sus principales dificultades estuvieron relacionadas con: Entrega de productos, la gestión de consultas y reclamos, la gestión de claves y la gestión de cheques". (PwC, 2021).

PwC Argentina, sostiene que se ha incrementado la utilización de la tecnología mediante los canales digitales como *home banking* y apps propias de los bancos. Lo que a su vez llevó a aumentar la migración de canales alternativos como la utilización de aplicaciones y tecnología, y se perfeccionó el capital humano en tanto se fomentó el trabajo remoto. "El 81% de las entidades considera que podrá continuar con trabajo remoto en las áreas de IT y de soporte, en un 56% en las áreas centrales tanto comerciales y de operaciones y en *call center*" (PwC, 2021).

El presente trabajo de investigación, realizado en función de las modificaciones surgidas como producto del confinamiento por el Covid-19, ha permitido identificar algunos de los ciberdelitos más frecuentes que se han producido en entidades bancarias. Por otro lado, ha puesto de manifiesto que los *smartphones* se han convertido en un blanco masivo para los delincuentes, mediante el uso de redes sociales, pero especialmente de *WhatsApp*, plataforma por la cual se han iniciado la mayoría de este tipo de delitos.

1.1.1 Modificaciones en el Sistema Bancario Argentino durante la pandemia de Covid-19

En el marco de la cuarentena obligatoria dispuesta por el gobierno nacional y los gobiernos provinciales, desde el 20 de marzo del año 2020, el Banco Central de la República Argentina (BCRA) realizó una serie de comunicados en los cuales estableció las nuevas normativas que entrarían en vigencia para dar respuesta, desde los bancos, a las necesidades de la sociedad usuaria de estos sistemas.

En primer lugar, se debió garantizar la disponibilidad de efectivo en los cajeros automáticos, a fin de que las personas concurrieran lo menos posible a las entidades financieras, lo que evitó la propagación del virus. Posteriormente se establecieron sistemas de turnos por finalización de documentos a fin de que se resolvieran los problemas que pudieran surgir por la utilización de medios electrónicos, y otros que ya se encontraban en proceso de resolución con anterioridad al período de confinamiento

Las operaciones de forma remota fueron las que se mantuvieron en vanguardia y requirieron que se ampliaran las operatorias, muchas de las cuales ya se venían realizando bajo esta modalidad.

Por otro lado, la aparición del teletrabajo para los empleados, implicó también una comunicación más fluida en forma telefónica, a fin de evitar que se produjeran problemas para los usuarios.

La realización de rápidas respuestas, sumado a un conjunto de estrategias que llevaron adelante, les permitió a los bancos y a todo el sistema financiero en general, sortear la crisis que se presentó atendiendo a las dificultades, pero logrando brindar respuesta a gran parte de la población.

La rápida respuesta coordinada de las autoridades monetarias, pero también fiscales, ha sido clave para abordar las consecuencias que podría producir la crisis desatada por Covid-19. Si bien estas medidas fueron heterogéneas, dependiendo de los diferentes países y dentro de estos, cada particularidad, el sistema financiero encontró en las regulaciones gubernamentales, respuestas que favorecieron el funcionamiento, y permitieron a su vez, brindar respuestas adecuadas a las demandas de la sociedad. Uno de los mayores retos fue el sistema de atención y las estrategias que debieron crear para atender al público, principalmente.

1.2 Digitalización del sistema bancario internacional

Los bancos, centralizados en las necesidades de los clientes, brindaron respuestas a nivel de digitalización, e incluso con la agilización del sistema de créditos bancarios. Mantuvieron los acuerdos pactados y, a su vez, ofrecieron nuevas formas de pago de créditos o refinanciamiento. Claro está que esta situación no sólo se debía a la necesidad de dar respuesta a sus clientes, sino también a la necesidad propia de garantizarse el cobro de créditos otorgados con anterioridad.

La aceleración de los procesos de digitalización, indican que desde el sistema financiero se han mejorado los esfuerzos tecnológicos. Para esto debieron recurrir a lo que

Fine, (2019) ha denominado "*fintech*, término genérico que reúne múltiples clases de tecnologías aplicadas al sector financiero" (Fine, 2019), las cuales son creadas por grandes empresas internacionales que se han convertido en impulsoras de las formas en que se ofrecen los servicios financieros, abriendo grandes oportunidades de negocios.

Apoyados en el gran desarrollo tecnológico de *smartphones* y computadoras, se ha convertido en una ventaja de oportunidades para la oferta de servicios financieros, siendo las *fintech* las empresas que más han ganado con estas modificaciones (Vives, 2019). Los pagos móviles han permitido que empresas como Visa, MasterCard, y en el caso de Argentina Mercado Libre, a través de su billetera virtual de Mercado Pago, haya generado un gran desarrollo en pagos móviles, impulsando la utilización de la digitalización para todas las operaciones y transacciones económicas. Lo principal de esta industria es que las personas ya no necesitan contar con una cuenta bancaria tradicional, es decir una cuenta que hayan debido gestionar en forma presencial en una entidad bancaria, para crearla.

Las aplicaciones móviles que se han potenciado durante el tiempo de pandemia, permiten a los usuarios crear sus propias cuentas bancarias con solo introducir un número de documento, o Clave Única de Identificación Tributaria o Laboral (CUIT/CUIL), para que la interconexión que se establece con instituciones estatales, permita obtener los datos completos del usuario nuevo. De esta forma cualquier persona, mayor de 18 años, puede abrir sus propias cuentas bancarias, desde un *smartphone*, *tablet* o computador.

Esto puede ser un gran servicio para los consumidores, sin embargo, es también un gran problema para la seguridad pública, ya que los ciberdelitos de fraude y estafa, se producen con gran celeridad en el mundo, cuanto más digitalizado este se encuentre.

Durante el año 2020 y gran parte del 2021, la no utilización del dinero físico, fue una gran ayuda para mitigar los contagios de Covid-19, ampliando las funciones del cajero automático a las aplicaciones móviles. Esta ampliación de la digitalización ha ofrecido también una gran oportunidad al sistema bancario para mejorar su eficiencia y ampliación de servicios, optimizando los productos que el sector posee, pero además, interconectándose entre sí y permitiendo que se acceda a un conjunto de bienes y servicios

a los que no se accedía con tanta facilidad con anterioridad. Así lo expresa el titular del Banco BBVA, Martín Zarich (2021):

> "El sector bancario es parte de los servicios esenciales dentro de este contexto. Debimos adaptar todos los sistemas y los equipos con rapidez para adecuarnos a las normativas que se dieron en este entorno. En este sentido, fue relevante la organización y la flexibilidad de los equipos, para dar respuesta y garantizar la atención en una situación tan inusual para todos". (p. 1).

Los bancos debieron realizar grandes inversiones también para la digitalización, las que redituaron en la captación de mayor cantidad de clientes, tanto minoristas como mayoristas y empresarios. Las operaciones hoy pueden hacerse en su totalidad, *on line*, incluso la solicitud de préstamos. El sistema financiero ha realizado grandes inversiones en *hardware*, *fintech*, robótica y biometría, que les permitieron mejorar los servicios y acercarse a sus clientes.

Cecilia Valleboni (2021) escribe un artículo para la revista Forbes, de Argentina, en el que sostiene que el sistema financiero se mantiene en un proceso de transformación constante, sin embargo, la coyuntura actual ha generado que esta transformación se de en forma acelerada, obligando a las instituciones bancarias a ofrecer respuestas rápidas, eficaces y eficientes. Respecto al desempeño bancario durante el año 2020 explica que:

> "Pero la pandemia fue implacable: aceleró todos los planes que las entidades tenían para el próximo lustro. Y lo más importante: hizo más digitales a los clientes. Innovaciones a la medida de las necesidades, desarrollos en tiempo récord y la rápida adaptación de los usuarios fueron los puntos altos de un año movido" (Valleboni, 2021. P.1).

Las respuestas de la banca argentina reflejan un comportamiento impecable, como sostiene Valleboni, creando soluciones en las ayudas financieras.

1.3 El Sistema Bancario Argentino durante la pandemia

La ayuda financiera a la que accedieron los usuarios bancarios argentinos, fue un gran aporte a los problemas que se presentaron durante la pandemia, sobre todo aquellos vinculados con los cierres de comercio y con ello la disminución de demanda de bienes y servicios.

La economía argentina ya estaba sufriendo crisis y los bancos debieron salir a dar respuestas "La economía se contrajo un 10,5%, hubo una inflación del 36% y el déficit primario llegó al 6,5% del PBI. Es un año que nos obligó a dar mucho apoyo" (Valleboni, 2021).

Los principales problemas se vincularon con la entrega de productos, la gestión de claves y cheques, y la entrega de tarjetas. La firma digital fue otro inconveniente, que debió resolverse, la cual AÚN estando legislada, muchos bancos no la habían implementado. Esto llevó además, A que la población argentina, adquiriera nuevas conductas bancarias.

El sector de jubilados fue el más complejo de atender. Este grupo de personas que se encuentran bancarizadas, tuvieron serias dificultades para acceder a cobrar sus jubilaciones, ya que un gran número de ellos no utilizaba los servicios digitalizados. Luego de varios esfuerzos los bancos lograron que este grupo comience a acercarse más a la digitalización.

Los datos que presenta Valleboni (2021), respecto a la digitalización bancaria, ponen en evidencia que el uso de las aplicaciones ha crecido entre un 200% y un 300% en el año 2020, ya que por canales digitales se pueden realizar transferencias, inversiones, plazos fijos, solicitud de préstamos, gestión de cuentas corrientes, entre otras.

Por otro lado, esta digitalización ha permitido también incrementar el contacto con los usuarios a través de la aplicación de WhatsApp, la cual les permite a los clientes comunicarse con operadores que responden en línea rápidamente. En relación con este tema, Valleboni (2021) amplía:

> "Hay un componente muy fuerte que es el cambio de hábitos. Los niveles de penetración de los canales digitales rondan el 80% y crecieron un 20% en 2020", destaca. En su caso, el nivel de digitalización estaba encaminado. El

> 80% de los plazos fijos y el 55% de la venta de préstamos personales se hacen por canales digitales. "Lo que abordamos es un proceso de transformación más integral y con una evolución cultural que ayude a lograr esos objetivos", explica. Uno de los ejes de este año fue el ICBC Mall, la plataforma de *e-commerce* que, según Martínez Álvarez, es la página número 10 en facturación de la Argentina (p. 1).

Lo explicado pone de manifiesto que la digitalización bancaria ha llegado a los usuarios para mantenerse por mucho tiempo. Sin embargo, como se ha mencionado, la vulnerabilidad ha aparecido en estos sistemas. En el caso de Mendoza, lo explicado a nivel nacional por los expertos, se ha mantenido de igual manera que en el resto del país. Hoy, la banca digitalizada ha logrado una menor afluencia de público a las entidades bancarias, aunque muchos usuarios continúan con el retiro de efectivo en cajeros automáticos.

En referencia a este punto, los delitos que antes acontecían se llevaban a cabo mediante la modalidad denominada *skimming*, delito que consiste en extraer datos de la tarjeta de debido y/o crédito en el punto de venta y utilizar los mismos para fabricar tarjetas falsas, o bien comprar artículos utilizando esos datos. La modalidad delictiva consistía en colocar un dispositivo en el cajero automático, el cual permitía la clonación de la tarjeta. Para esta clonación es necesario contar con un software que posibilite realizar la clonación de la banda magnética. Además, se requiere cámaras pequeñas, y muy bien ocultas, que posibiliten obtener los datos de las claves de seguridad de las víctimas.

Otra modalidad delictiva fue la que se denominó "viejos pescadores". Esta consiste en insertar una varilla de metal en la ranura donde se entrega el dinero, y cuando la víctima accedía a retirar los billetes, estos quedaban trabados en la boca de salida del cajero automático. Luego, quien había colocado el "anzuelo", rescataba el dinero de su víctima.

Si bien esta modalidad delictiva continúa, es en menor medida, dado que el ciberdelito económico ha adquirido nuevas modalidades, las que no requieren de la presencia física. Ya no alcanza con un metal en la boca del cajero, o la clonación de

tarjetas, sino que hoy la modalidad denominada *spear phishing*, mediante la cual se realiza un contacto con la víctima vía correo electrónico, *WhatsApp* o llamadas telefónicas, es la que prevalece.

Estas avanzadas modalidades delictivas utilizadas por los delincuentes, buscan engañar a los usuarios seduciéndolos para que entreguen información personal, y luego poder modificarla. Quien concurre a los cajeros en estas ocasiones, ya no es el delincuente sino la misma víctima.

1.3.1. Consecuencias sobre la seguridad en el sistema operativo de los bancos

Los bancos fueron parte de la solución para enfrentar los problemas económicos ya que debieron brindar accesibilidad a todos los usuarios por igual. Sin embargo, algunas de estas respuestas resultaron vulnerables para los usuarios y muchos de ellos fueron víctimas de las nuevas modalidades delictivas.

Durante el período de pandemia, los usuarios bancarios sufrieron una gran cantidad de ciberdelitos. En "2020 hubo un 140% más de denuncias que en el acumulado de los tres años anteriores en el país", sostiene Horacio Azzolin en una entrevista brindada al diario La Nación, agregando que en los últimos meses (del año 2020) se duplicó el acceso indebido a "las cuentas de los bancos, fraudes de reclutamiento por empleo y compras por internet" (Poleri, 2021).

La modalidad delictiva preferida fue a través de *WhatsApp* y correos electrónicos, enviando contactos que parecen provenir de una institución confiable y ofrecen enlaces, que luego sirven a los delincuentes para acceder a sitios web, en los que roban los datos que requieren para ingresar a las cuentas bancarias. Mucha de esta información, como e-mail o números de teléfono personales, fueron obtenidos de redes sociales donde los usuarios suelen compartirlos. O bien, de aquellos que han sido comentados en las mismas publicaciones bancarias de las redes sociales, en las cuales los usuarios realizan sus quejas. De esta forma el estafador accede a una información que es proporcionada por el propio usuario, por lo que luego si la estafa

se logra, muchas veces no pueden reclamar a los bancos ya que los datos han sido propiciados por los usuarios.

Las consecuencias de muchas acciones de este tipo sobre los bancos, resultaron en algunos casos, sumamente negativas, tal como ha sucedido con la gran estafa de la cual fueron víctimas los usuarios del Banco Nación y que se presentará en el capítulo 4. Frente a estos delitos debieron afrontar presentaciones judiciales de usuarios por la vulnerabilidad del sistema.

Por otro lado, es destacable que algunos usuarios que han recibido mensajes por WhatsApp o e-mail o llamadas telefónicas, no han presentado demandas.

Estas acciones llevaron a un incremento en las medidas de seguridad que, desde el Banco Central de la República Argentina (BCRA), se debieron articular a fin de evitar mayores víctimas.

Frente a esto, los bancos desarrollaron un conjunto de medidas preventivas, que incluyeron los procesos específicos que permitieron mitigar los riesgos del uso de canales digitales que utilizan en forma periódica, además, de instalar medidas de monitoreo y control de fallas. En consonancia con estas acciones, y en acuerdos con el BCRA, se realizaron campañas de prevención y concientización orientadas al cliente, entre las que se mencionan #VosSosLaClave, la cual se desarrolló íntegramente a través de redes sociales.

El BCRA a su vez difundió en las entidades bancarias los “Lineamientos de Ciberseguridad” consistente en material que planteó los lineamientos para brindar rápidas respuestas frente al crecimiento del ciberdelito.

Los bancos incrementaron rápidamente las claves de acceso a *homebanking* y aplicaciones, mediante la creación de los denominados “Alias” los que consisten en una combinación de palabras y símbolos que son únicos para cada cuenta bancaria. De esta forma hoy la seguridad bancaria de los usuarios está protegida por: claves numéricas, claves alfa numéricas, CBU, CVU y Alias. Además, de exigir en muchos

smartphones, la utilización de acceso de seguridad, como claves numéricas, patrones y/o huellas digitales.

De diversas formas el sistema bancario fue aportando soluciones para digitalizar la población, y evitar que se propagaran los contagios de Covid-19. Pero a su vez, desde el BCRA en conjunto con todos los representantes bancarios, se debieron ajustar las medidas de protección de seguridad, a fin de preservar a sus usuarios y sus bienes. Esto fue configurando un conjunto de nuevas formas de atención al público, prestación de servicios, y operaciones bancarias que se conceptualizan en el capítulo siguiente. En el mismo se explican, además, las formas más comunes de estafa y fraude bancario preexistentes y que en la actualidad se han ido perfeccionando a partir de la creciente digitalización bancaria.

Marco Conceptual

Capítulo II

Constitución del Sistema Bancario Argentino y su relación con los clientes. Banca on-line. Aplicaciones móviles.

El presente capítulo desarrolla los conceptos que guían la investigación, referentes al Sistema Bancario, sus componentes y las prestaciones de servicios que realizan a los clientes. En el mismo se describen los delitos que vulneran el sistema como también aquellos que se han perfeccionado sobre todo durante el año 2021, y el marco legal que protege a los clientes bancarios en relación con los delitos que pueden convertirlos en víctimas.

2.1. Conformación del sistema bancario

Está conformado por un conjunto de instituciones financieras que se dedican a la intermediación económica "Su actividad consiste en captar el ahorro del público y, con ese capital, solventar el otorgamiento de créditos y realizar inversiones" (Westreicher, 2020).

Estas entidades captan el dinero de sus clientes y lo administran de diferentes maneras, con el objetivo de generar ganancias para sí o para sus clientes, aplicando diferentes tasas de interés, las que son abonadas por otros clientes que solicitan créditos a quienes se les aplica una tasa de interés superior. Dentro de estas entidades se encuentran no solo los ahorros de muchos de sus clientes, sino que se administra el dinero que perciben por sus prestaciones laborales, jubilaciones, beneficios sociales entre otros.

Los elementos que componen este sistema son:

- *Banco*: Entidades financieras cuyo fin es el control y administración de dinero.
- *Productos bancarios:* son los servicios que ofrece el banco que pueden ser ahorro, depósitos a plazo fijo, alternativas de financiamiento como tarjetas de crédito entre otros.
- *Entidades supervisoras:* son las entidades gubernamentales que se encargan de recoger la información del sistema bancario.

- *Autoridad monetaria:* es el organismo que dictamina la política monetaria de cada país fijando valores y tasas de interés de referencia. Es el encargado de la emisión de billetes y monedas (Westreicher, 2020).

Las operaciones que en ellos se realizan, son variadas, y se conforman por las acciones de captación, recepción y recolección de dinero, con la finalidad de redistribuirlo. Estas operaciones tienen tres grandes categorías que se describen a continuación.

2.1.1 Sistema Bancario Argentino

2.1.1.1. Elementos que lo constituyen, sus componentes

El Sistema Bancario en nuestro país se compone del Banco Central de la República Argentina (BCRA) quien rige las normas bajo las cuales operan diferentes bancos dentro del país, y los colocadores y tomadores de fondo. El principal objetivo del BCRA es mantener el valor de la moneda nacional, tal como lo estipula el Artículo 3º de su Carta Orgánica (BCRA, Carta Orgánica, s.f.).

Son funciones del BCRA las de publicar al principio de año su objetivo de inflación, el cual debe ser reafirmado cada tres meses. En dichos informes debe referenciar las causas que han llevado a un aumento, o no, inflacionario. Debe vigilar el buen funcionamiento del sistema financiero y de cambio de moneda, y el desempeño de los bancos y entidades financieras, las cuales se encuentran catalogadas en función de lo establecido por la Carta Orgánica.

En referencia a los colocadores y tomadores de fondos, estos son quienes reciben las tasas de interés a su favor por realizar determinados depósitos, mientras que los tomadores son quienes solicitan préstamos y pagan una determinada tasa de interés para la devolución del dinero. Esta tasa aplicada es siempre mayor para quien solicita préstamos que para quien invierte.

Está integrado por:

Entidades financieras: Son aquellas intermediarias comprendidas dentro de la Ley de entidades financieras, y se encuentran bajo el control del BCRA. También existen cooperativas de crédito y cajas de ahorro.

Entidades no financieras: Son aquellas empresas que se consideran como auxiliares del mercado financiero y no están autorizadas por el Banco Central para operar como entidad financiera, por lo que los depósitos que en ellas se realizan no están garantizados por el BCRA. Pueden realizar todas las actividades que realizan los bancos, pero carecen de garantías.

Fintech: estas empresas, combinan la tecnología con las funciones financieras a fin de solucionar diferentes necesidades de personas y/o empresas. Se trata de plataformas electrónicas que permiten realizar transacciones financieras, interactuar con el sistema desde cualquier dispositivo electrónico y pueden realizar acciones como otorgar préstamos, realizar pagos y transferencias y recibir inversiones (Fernández, Victor, Lauxmann, Carolina & Tealdo, Julio, 2012).

2.2 Formas de funcionamiento bancario

Las formas del funcionamiento bancario en la actualidad se conforman de la modalidad presencial, la cual ha sido la que ha prevalecido desde la creación del sistema, hasta la modalidad *on line* que es la forma más novedosa de atención.

2.2.1. Modalidad presencial

Esta modalidad de atención ha sido la clásica forma de acceder al sistema bancario implica la atención simultánea de los clientes. La gran cantidad de afluencia de público lleva, muchas veces, a despersonalizar la atención y con esto muchos usuarios comenzaron a migrar hacia bancos que ofrecían atención más personalizada. Sin embargo, la demanda de público lleva a un aumento en el tiempo de espera para acceder a diversos servicios.

Las sucursales deben contar con espacios suficientes y lugares disponibles para las largas colas que se producen en los ingresos ya sea que se busque pagar un servicio o

solicitar un préstamo, los tiempos de espera siempre fueron un problema para el cliente bancario, sobre todo en épocas cercanas a fiestas como fin de año.

Los servicios, en su gran mayoría eran personalizados antes de la pandemia, y el cliente concurría al sistema bancario cuando era citado, y aún sin cita para realizar diversos trámites. Muchas veces observando como otros grandes clientes accedían al sistema de manera más rápida y dinámica. Poco a poco muchas de estas acciones fueron migrando hacia la utilización de la tecnología, demostrada en primera instancia, con los cajeros automáticos los que además, de permitir retirar dinero, también empezaron a recibir depósitos para otras cuentas y pagos a servicios, buscando disminuir la atención presencial. Sin embargo, muchos usuarios continuaron concurriendo a los bancos a realizar sus trámites, sobre todo quienes no deseaban realizarlos en forma digitalizada. Un gran grupo de estos clientes lo conforman los jubilados, quienes encuentran graves dificultades para acceder al sistema digitalizado. Durante el período de pandemia, esto cambió en forma drástica y llevó necesariamente a un ordenamiento digitalizado de los clientes que podrá mantenerse en el tiempo.

Los trámites que se pueden realizar en forma presencial en los bancos consistentes en cobros, pagos, transferencias, envíos de dinero entre otros, son los mismos que hoy pueden ser realizados en forma digitalizada. Salvo algunas transacciones de mayor magnitud, la gran mayoría de los usuarios puede hoy, realizar todas sus actividades bancarias bajo la modalidad *on line*, la que se describe en el siguiente apartado.

2.2.2. Modalidad *on line*

Esta modalidad de vinculación entre clientes y entidades bancarias, recibe diferentes denominaciones las que se diferencian entre sí. Ellas son la banca electrónica, banca en línea, banca digital o la más conocida de todas el *home banking*.

Sus orígenes se remontan a la utilización de la telefonía para las transacciones bancarias, las que surgen en los años 90 en nuestro país, iniciando un proceso de cambio en la atención al cliente, que se amplió hasta la utilización de diversos dispositivos

electrónicos que pueden soportar la utilización de internet para el acceso a estos sistemas. Cada una de estas denominaciones presenta una definición que le es particular:

- *Banca electrónica:* se refiere a las acciones que los clientes llevan a cabo mediante la utilización de elementos electrónicos como por ejemplo los cajeros automáticos o las llamadas telefónicas. Comprende a todo servicio bancario y/o financiero, ofrecido por una entidad y basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros, con mínima o ninguna asistencia o -6- participación de un operador humano. La Banca Electrónica incluye pero no se limita a la implementación de Canales Electrónicos con las características indicadas en esta norma (BCRA Circular 1208/16).

- *Banca por internet:* son los espacios en internet, que ofrecen los bancos mediante la utilización de esta red, en la que se encuentran diferentes servicios que pueden ser utilizados por los clientes. Esta conexión con el cliente se realiza mediante la utilización de la *World Wide Web* (www) permitiendo generar *link* que sirven para que los clientes efectúen sus operaciones financieras dentro de un espacio virtual. Comprende las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros que se basan en la utilización de programas informáticos diseñados para su operación mediante el acceso a sitios publicados en internet, bajo administración de una entidad u operador y el uso de motores de navegación instalados en dispositivos propios del usuario que se comunican con un centro de procesamiento de la entidad (propio o de un tercero), mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de datos bajo administración de un operador público o privado (BCRA Circular 1208/16).

- *Banca virtual:* en este grupo se incluyen todos aquellos bancos que no cuentan con espacios físicos para establecer contactos con sus clientes. El intercambio de información se realiza en forma exclusiva mediante la utilización de Internet (Martínez, 2021).

- *Cliente - usuario de servicios financieros - usuario*. Los términos "cliente" y "usuario de servicios financieros" son equivalentes y se refieren a la persona física o jurídica que se encuentra identificada y suscrita a los servicios de una o más entidades financieras. El término "usuario" es una denominación genérica aplicable a clientes y no clientes (BCRA Circular 1208/16).

Todas estas formas de vinculación entre los bancos y sus usuarios, implican también los cambios de conducta de los consumidores y con ello, su adaptación, o no, a estos sistemas.

Esto también llevó a que muchos clientes debieran aprender a utilizar tanto computadoras como *tablets* y/o *smartphones* dependiendo del dispositivo por el cual ingresan a los servicios bancarios.

2.2.2.1 Home Banking

El BCRA define al *home banking* como:

> "Se llama home *banking*, banca online o *e-banking*, a los servicios bancarios a los que se puede acceder a través de internet por medio de computadoras, *tablets* o teléfonos celulares. Para poder operar mediante esta modalidad es necesario ser titular de una cuenta bancaria". (BCRA, s.f.)

Se trata de un servicio con el que cuentan todas las entidades financieras en la actualidad. Permite administrar el dinero, por parte del cliente, a través de la utilización de internet, mediante el acceso con diferentes dispositivos como computadoras, tablet y/o smartphone.

En ella se puede operar las 24 h., los 365 días del año. Quedan registradas todas las operaciones que se llevan a cabo hasta la última fecha de acceso del cliente, excepto aquellas que se realizan fuera del horario bancario, las que serán acreditadas el siguiente día hábil en horario de atención. Sin embargo, la mayoría de las entidades hoy funcionan con horarios más amplios y las transacciones suelen ser, en su mayoría, inmediatas.

Para operar en estas plataformas se requiere ser cliente bancario, disponer de dispositivos adecuados, gestionar un usuario y clave para operar en *home banking*. Se

requiere que el usuario haya realizado una serie de pasos previos a fin de garantizar las máximas medidas de seguridad. Estos pasos dependerán de cada banco en particular.

Los pasos consisten en:

- Ingresar la tarjeta y PIN en el Cajero Automático de la Red que corresponda.
- Seleccionar la opción Claves del menú principal y en la siguiente pantalla elegir *home banking* gestión de claves, o *Link* Celular, dependiendo también del banco
- Crear una clave y posteriormente reingresarla. Esta clave puede ser sólo numérica o alfanumérica (compuesta por números y letras).
- El cajero entrega un ticket de la operación con un número de usuario que deberá conservar todo usuario pues le será requerido posteriormente en su ingreso por el dispositivo móvil.

Una vez realizados estos pasos en el cajero, se le solicitarán otros datos que pueden incluir nuevas claves, fotos de perfil, comprobación por fotos de reconocimiento, fotos del DNI, claves alfanuméricos, usuarios, generación de *token*, entre otros. Cada banco establece sus propios sistemas de seguridad (Banco Nación, 2021).

2.2.2.2 Aplicaciones móviles

Las aplicaciones bancarias conforman parte de los servicios digitalizados bancarios que permite a los clientes realizar toda clase de transacciones financieras, en forma remota, mediante la utilización de dispositivos móviles. Son diferentes de la utilización del *home banking*, en tanto estas pueden ser descargadas al celular, tablet y/o computadora y el ingreso del usuario puede hacerse sin necesidad de ingresar a la página web bancaria.

A través de estas aplicaciones los usuarios pueden acceder a sus estados de cuenta, obtención de saldos, lista de transacciones más recientes, pagos de facturas electrónicas, transferencia de fondos, y algunas permiten la solicitud de créditos bancarios.

Estas aplicaciones reducen costos bancarios en relación con la necesidad de que el cliente se dirija a la sucursal para realizar estas consultas y/o transacciones, lo que para el banco significa un ahorro de personal, entre otros.

Con la pandemia de Covid-19 durante el año 2020, la creación de aplicaciones bancarias para dispositivos, se incrementó notablemente, permitiendo que cada entidad financiera creara la suya propia.

La descarga de la misma se realiza desde las tiendas de Google Play (disponible para dispositivos Android), o la tienda de Apple (disponible para IPhone e IPad) y todas son gratuitas, sin costo de mantenimiento.

Las aplicaciones móviles son versiones más pequeñas que las páginas web, ya que solo requieren la combinación entre HTLM, CSS y Javascript para su desarrollo. Requieren el uso de las API, sino que su ejecución se lleva a cabo mediante el browser. Un ejemplo de ello es una aplicación web, que puede acceder a la información del GPS a través del browser del dispositivo, pero no podrá hacer un almacenamiento de mensajería (Rojas Poblete, 2016, p 20). Las aplicaciones pueden utilizar el browser para almacenar mensajería ya que cuentan con la extensión de *Javascript*.

Las aplicaciones utilizadas por el sistema bancario son las denominadas aplicaciones nativas, las cuales aprovechan todas las funciones de las API incorporadas en el sistema operativo del dispositivo en el cual se instalan. “Los desarrolladores de cada plataforma ponen SDK’s a disposición de los desarrolladores de aplicaciones, los cuales permiten que estos últimos puedan crear aplicaciones las cuales pueden acceder a recursos del aparato mediante un modelo de permisos definido” (Rojas Poblete, 2016, p. 23).

Actualmente en Argentina las aplicaciones móviles deben solicitar al usuario que permita acceder a la privacidad personal y del equipo móvil en el que se instalan, como fotos, cámara, GPS, contactos, entre otros. Esto a fin de evitar que obtengan información mediante el cruce de datos que efectivizan cuando ingresan en los datos privados de nuestros dispositivos. Los datos que pueden ser utilizados para el *linkability* son generalmente identificadores como el DNI de la persona, su correo electrónico, el IMEI (Rojas Poblete, 2016).

Cada aplicación es adecuada al Sistema operativo en el que funcionará, el cual puede ser Android o iOS, cada uno tiene sus propias características de hardware y software particulares, pero son iguales para la entidad que las origina, como en este caso los bancos.

2.3 Clientes

Los clientes bancarios son aquellas personas que participan en las relaciones comerciales, y establecen diferentes contratos con las entidades bancarias, adquiriendo derechos y obligaciones propias del sistema financiero.

Las operaciones bancarias presentan grandes complejidades, y no resulta fácil para los clientes conocer la totalidad de las responsabilidades que le caben. Por esto los bancos cuentan con contratos estándar que son firmados por los clientes al momento de conformar diferentes transacciones. Dado que en todo sistema financiero la base de la relación se encuentra en la confianza entre el cliente y la entidad, es fundamental que estas les entreguen a los clientes toda la información que necesitan a fin de que no se violen derechos de los clientes. Por esto el asesoramiento que ofrecen las entidades bancarias debe ser siempre el adecuado y debe estar supervisado por organizaciones no gubernamentales, como en Argentina es Defensa al Consumidor (Mazzinghi, 2015).

2.3.1 Marco legal que ampara a los clientes bancarios

Los clientes bancarios se encuentran protegidos por el nuevo Código Civil y Comercial (CCC), el cual dedica a los contratos bancarios un conjunto de normativas que les garantizan el goce de sus derechos. A propósito de esto legisla sobre seis tipos diferentes de contratos bancarios: depósito bancario, cuenta corriente bancaria, préstamo y descuento bancario, apertura de crédito, servicio de caja de seguridad y custodia de títulos.

En el Capítulo 12 del Título IV referido a los Contratos en particular, en función de los Derechos Personales, el CCC abarca 42 artículos desde el 1.378 hasta el 1.420. En ellos rigen las acciones que deberán llevar a cabo tanto el cliente como la entidad bancaria o financiera, en referencia a los depósitos bancarios, las cuentas corrientes, los préstamos bancarios, las aperturas de líneas de crédito, los servicios de cajas de seguridad y la custodia de títulos.

El ámbito de aplicación de las disposiciones es todo el territorio nacional argentino, y las entidades financieras reguladas por la Ley 21.526/77 de Entidades Financieras, y además, se aplica a los contratos celebrados con las entidades públicas y/o privadas y/o Organizaciones No Gubernamentales.

Los artículos citados regulan en materia de publicidad y tasas de interés, refiriendo que las mismas deben ser coherentes entre sí; la forma que adquieren los contratos, los que deben ser por escrito, firmados, y también mediante la constatación de cualquier soporte electrónico con el cual opere la entidad financiera. Los clientes deben recibir información periódica de sus movimientos y también de las acciones que la entidad financiera lleve a cabo, los beneficios y costos de sus servicios como también las innovaciones en atención.

Respecto a la rescisión del vínculo contractual, el artículo 1.383 le garantiza al cliente bancario la facultad de rescindir en cualquier momento los contratos, vigentes a tiempo indeterminado, sin penalidad, ni gastos a su cargo, salvo los que estuvieran devengados al momento en que el cliente ejerza este derecho.

En referencia a las operaciones *on line* o mediante el denominado *home banking*, el CCC (art. 1396) prevé expresamente que "…los créditos y débitos pueden efectuarse y las cuentas pueden ser llevadas por medios mecánicos, electrónicos, de computación u otros en las condiciones que establezca la reglamentación, la que debe determinar también la posibilidad de conexiones de redes en tiempo real y otras que sean pertinentes de acuerdo con los medios técnicos disponibles, en orden a la celeridad y seguridad de las transacciones". Permitiendo que el manejo de la cuenta se realice en forma virtual (Mazzinghi, 2015).

2.4 Ciberdelito económico en el ámbito bancario

En referencia al ciber delito, el Ministerio de Justicia y Derechos Humanos (2021) lo ha definido como:

> "Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas. Son estafas, robo de datos personales, de información comercial

> estratégica, robo de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos".

Este tipo de delitos adquiere diferentes formas de expresión. Pueden ser realizados mediante la utilización de malwares desarrollados para dañar, deteriorar o hacer inaccesibles diferentes programas informáticos, como también utilizar diferentes herramientas informáticas y de comunicación, a fin de cometer otros delitos. Requieren de un hardware que puede estar ubicado en una computadora o cualquier tipo de dispositivo electrónico con diferentes niveles de tecnologia, y de un software como sistema que puede realizar las acciones necesarias. Ambos requieren de la utilización de medios como internet, para hacer posible un delito informático basado en las TICs (Tecnologías de la Información y la Comunicación). Estos deltios van desde el espionaje industrial, hasta pornografía infantil, incluyento el grooming y diferentes tipos de acciones que se llevan a cabo mediante la utilización de las TICs. En este sentido los ciberdelitos vinculados a fraudes económicos, adquieren diferentes caracteristicas, y conforme a esto se tipifican, teniendo en cuenta la complejidad que cada uno de ellos presenta.

2.4.1. Tipos

Dentro de los delitos bancarios el *fraude*, como la *estafa*, han sido los más comunes, además, de ser muy analizados a lo largo de la historia. A partir de la aparición de internet y con el crecimiento de la tecnología y la incorporación de nuevos dispositivos electrónicos, estos delitos han adquirido una complejidad mayor.

Los ciberdelitos que interesan a la presente investigación son aquellos que se realizan mediante la utilización de las herramientas tecnológicas y que han debido ser nuevamente tipficados por la legislación. Los fraudes y estafas con dispositivos informáticos, se emnarcan en conductas delictivas que derivan de metodologías vinculadas a modificar, manipular, ocultar o alterear datos, sistemas y programas infomáticos, tales como los que se describen a continuación. Entre ellos se encuentran los siguientes:

2.4.1.1. Robo de indentidad

Este tipo de delito se lleva a cabo mediante la utilización de tarjetas de crédito que son obtenidas a nombre de terceros. A través de esta operación se realizan diferentes estafas.

2.4.1.2. Phishing

Mediante la utilización de “cebos”, como mensajes fraudulentos logran atraer a sus víctimas hacia sitios falsificados. La metodología de estafa consiste en obtener información personal, la cual muchas veces es proporcionada por el propio usuario a quien le solicitan realizar cambios de claves de seguridad, cambios de usuarios y/o contraseñas, entre otros, para posteriormente vaciar las cuentas personales. Es utilizado comunmente para acceder a cuentas bancarias, tratando de copiar o replicar el mismo diseño de la web de la entidad financiera o similar, a fin de que la víctima confie en la ifnormación que se envía y acceda de esta manera, al link que se ha enviado, el cual es un “espejo” de la página web original. (Techlandia, s.f.).

2.4.1.3. Pharming

Un delito que requiere mayor grado de complejidad que el anterior ya que utiliza malware para redirigir usuarios deprevenidos hacia versiones falsificadas de sitios web. Se caracteriza por crear páginas web exactamente iguales a las que ha plagiado. Una vez que la víctima ingresa ya ha obtenido los datos personales como también las contraseñas (Techlandia, s.f.).

2.4.1.4. Keylogging

Se trata de la utilzación de spyware que registra en secreto todo lo que alguien escribe a fin de obtener información de sus cuentas y otros datos personales. Se utilizan programas denominados *Keyloggers* los que realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario.

Un *keylogger* puede estar basado en hardware o software, y se puede usar como herramienta lícita de control de tecnología, tanto profesional como personal (Ministerio de Justicia y Derechos Humanos, 2021). El usuario, una vez que ingresa a cualquier página web como a su computadora, esté esta conectada o no, podrá ser visto en forma remota por otras personas que aprovechan la oportunidad para robar identidad. Al existir diferentes programas como *Keyloggers* inalámbricos o asociados a software espías, pueden acceder de cualquier manera a los dispositivos en los que fueron instalados.

2.4.1.5. Sniffing

Requiere de la conexión a una red Wi-Fi pública y no protegida, mediante la cual los hackers pueden robar datos observando el tráfico de Internet, mediante la utilización de herramientas especiales. Es una aplicación especial para redes informáticas (un software) que se encarga de capturar y analizar paquetes en tránsito (entrada y/o salida) en una red de comunicaciones entre dispositivos (Techlandia, s.f.).

2.4.1.6. Ciberextorsión

Se trata de extorsionar víctimas mediante la utilización de medios electrónicos e internet (AALCC, 2021).

2.4.1.7. Robo de datos: databreach y dataleaks

Con el uso diario y permanente de los dispositivos y miles de millones de usuarios en planeta, se disparó el riesgo y la exposición. El teletrabajo y las decenas de apps que descargamos en nuestros smartphones, que se vuelven aparentemente necesarias para sobrevivir en cuarentena, se convirtieron en una mina de oro para los cibercriminales y estafadores que toman información laboral y profesional.

2.4.1.8. Fraude bancario

Es la acción dolosa que provoca un perjuicio a un tercero, con la información obtenida hacen traspasos bancarios, venden información y hasta extorsionan a los propietarios de las claves.

> En el caso de los hechos on-line, los autores del fraude, con las claves en su poder, suelen abrir de modo simultáneo una cuenta bancaria a la que remiten el dinero mediante transferencias on-line. Estas cuentas se situarán normalmente en sucursales bancarias de terceros países adonde acceden para retirar el dinero. Para ejecutar estafas de importantes partidas de dinero, los autores suelen fraccionar las transferencias a diferentes entidades bancarias, aunque muy próximas geográficamente, de manera que el cobro se pueda materializar en un breve espacio de tiempo (Ronquillo, 2011)

2.4.2 Sistemas electrónicos

Los medios electrónicos que utilizan con mayor frecuencia son los correos electrónicos, comúnmente conocidos como e-mail. Estas herramientas utilizadas en manera frecuente por millones de personas, destinadas al trabajo o la comunicación en la vida cotidiana, se han convertido en un medio de comunicación también para hechos delictivos. "Algunos de los proveedores de servicios gratuitos de correo electrónico más conocidos, tienen millones de usuarios en todo el mundo, lo que refuerza la dimensión transnacional del delito cibernético" (12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2010, p.4).

La utilización de este medio electrónico se encuadra en la violación de correspondencia y forma parte de los delitos contra la intimidad de la persona. Las TICs han generado nuevas oportunidades para que se cometan este tipo de delitos complejos. "La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia" (Acurio Del Pino, 2015, p. 50). Otra forma de acceso es mediante mensajería de texto o aplicaciones como WhatsApp, Telegram, Messenger o Redes Sociales.

2.5 Medidas adicionales gubernamentales

La DirecciónNacional de Defensa del Consumidor y Arbitraje en Consumo, estableció que las entidades bancarias han incumplido las obligaciones de proteger sus usuarios y no han garantizado la seguridad, en referencia a la protección de datos personales y la protección de ocurrencia de estafas y fraude, con el incremento del uso de internet para la banca.

En este punto ha emitido una doble sanció para los bancos Santander y BBVA, por haber incumplido con la protección de datos, como también con la protección de lo bienes. Estas multas ascienden a $5 millones a cada entidad bancaria, en función de lo establecido en la Ley de Defensa al Consumidor (Ministerio de Desarrollo Productivo, 2021).

En el siguiente capítulo se desarrollan las estrategias que se llevaron a cabo, desde el sistema bancario y el BCRA, para disminuir la ocurrecncia de ciberdelitos y aumentar la seguridad bancaria en lo referente a la oferta de servicios de los usuarios.

Capítulo III

Estrategias de Prevención y Control de la Seguridad Bancaria, desde el contexto de la Seguridad Pública

En el presente capítulo se explicitan las estrategias de prevención y control del ciberdelito económico desde el contexto de la Seguridad Púbica que se debieron adoptar, a lo largo del tiempo, para controlar los ciberdelitos que fueron apareciendo en sus diferentes modalidades. Para dar respuesta a las necesidades de la sociedad y los bancos, el legislador ha creado un corpus legal que ha permitido tipificar estos delitos.

Por otro lado, ardua ha sido la tarea que ha debido desarrollar el Banco Central de la República Argentina (BCRA) durante el año 2020 y 2021 para dar respuesta a los usuarios bancarios y proteger sus intereses económicos, para lo cual ha formulado un conjunto de normas que aún se encuentran vigentes. Estas estrategias requieren, además, de un trabajo continuo de concientización social y distribución de información, tendiente a comunicar a los grupos más vulnerables del sistema bancario, sobre las estafas que circulan por las diferentes redes sociales. En el siguiente apartado se explica la seguridad bancaria y posteriormente se presentan las diferentes estrategias que se han llevado a cabo.

3.1 Seguridad Bancaria

El término seguridad procede de las palabras latinas "*securitas*" o "*securus*", éstas a su vez derivan de "sine cura" lo cual significa sin cuidado, sin preocupaciones o sin problemas. Por lo tanto "seguridad" quiere decir libre de preocupaciones, amenazas o problemas (Garibaldi, 2006).

La seguridad bancaria se refiere a la institución de tipo financiero que administra el dinero que le dejan en custodia sus clientes, pero también utiliza este dinero en concepto de préstamos para otras instituciones, personas físicas, o empresas aplicándoles un interés. Esto significa que se presenta en su interior, un constante movimiento de dinero que circula de diferentes formas.

Reisz y Zeballos (2012) definen a la seguridad bancaria como aquella que abarca una serie de seguridades entre las que se encuentran:

- *La seguridad básica:* constituida principalmente por los planteamientos arquitectónicos (cerramientos y elementos constructivos), los medios de protección

física y mecánica (blindajes, cajas fuertes, cerraduras, cámaras acorazadas, etc.) y los medios de prevención y protección activa o electrónica (sistemas de detección, control, registro, etc.).

- *La seguridad operativa y funcional*: constituida por los procesos administrativos y de control de riesgos, informaciones y datos confidenciales, formación y capacitación del personal, control de accesos y circulación de personas, control de las instalaciones de gestión y seguridad.
- *La seguridad informática*: constituida por los sistemas de protección de la información, control de las comunicaciones, transmisión de datos, control y protección de los procesos operativos.
- *La seguridad especial:* constituida por los sistemas y operativos especiales correspondientes para la protección de personas, de informaciones y valores específicos, así como por los dispositivos necesarios ante situaciones de riesgo o amenaza no habituales (agresiones terroristas, amenaza de bomba, catástrofe, etc.). (Reisz y Zeballos, 2012)

3.1.1. Principales amenazas a la seguridad bancaria

La digitalización ha creado nuevos espacios de riesgo para el sistema bancario, los que se detallan a continuación:

- *Ataque de denegación de servicio distribuido*: consiste en la creación de diferentes accesos a los servidores bancarios, los que pueden ser bloqueados o saturados por una sobre utilización de los mismos. Es decir, los denominados "piratas informáticos" generan una sobre utilización de los servicios bancarios y con esto logran burlar algunos sistemas de seguridad y realizar el delito de robo. Frente a esto los bancos recurren a la utilización de software de monitoreo de tráfico de datos que permite resguardar datos y redirigir peticiones, evitando la caída de los servidores.
- *Ingeniería inversa de las aplicaciones*: las aplicaciones presentan muchas vulnerabilidades. Al ser unas herramientas novedosas, los sistemas de protección pueden no ser siempre los más seguros. Vernengo (2020) afirma que "estas

herramientas pueden ser utilizadas como maquetas para la ingeniería inversa". Esto se logra al encontrar los puntos débiles que pueden existir en las estructuras de los códigos internos de las aplicaciones. Una vez identificados se puede clonar la aplicación y utilizar el *phishing*, robando la identidad de los usuarios.

- *Ransomware*: estos ataques son los más comunes, ya que se produce un ataque cada 15 segundos en el mundo (Vernengo, 2020). Consiste en un malware cuyo objetivo es el de obtener el control de computadoras o cualquier dispositivo, ganando acceso al mismo y sus archivos, buscando datos que puedan ser utilizados con fines espurios. Esta es la forma más compleja de ingreso, la más frecuente y la que más acciones de seguridad han obligado a desarrollar por parte del sistema bancario para su protección.

La complejidad de la tecnología cibernética actual, mantiene una escalada que parece no tener fin, lo que genera la necesidad constante de innovar en nuevos dispositivos de seguridad para evitar que se vulneren los sistemas y con ellos, la economía de la familia.

3.1.2 Métodos de protección bancaria

Una vez identificados los riesgos bancarios frente al crecimiento de la utilización de tecnología, las nuevas medidas de seguridad que se llevaron a cabo consistieron en diferentes formas de identificación de los usuarios. Por otro lado, los bancos recurrieron a la adquisición de software de seguridad que permiten bloquear las amenazas de *hacker*.

Entre los métodos de protección bancaria se reforzaron las claves de seguridad alfanuméricas, la creación de Alias, el uso de la firma electrónica, ya explicadas con anterioridad, pero además, se incorporó la autenticación en dos pasos, consistente en la elaboración de un conjunto de preguntas de seguridad que pueden ser realizadas por los bancos, una vez ingresadas las claves o el número que se haya generado por un *token*.

En referencia a las aplicaciones, se solicitan datos de los documentos de identidad específicos, además, de fotos que debe tomar el usuario. Esto permite identificar con claridad al usuario del sistema bancario.

Las instituciones llevaron a cabo un conjunto de medidas preventivas y concientizadoras destinadas a sus usuarios mediante campañas de seguridad cibernética, tanto en medios de comunicación como en redes. Entre estos consejos informan las medidas que se toman para solicitar información a los clientes entre las que mencionan las siguientes:

- No se solicitan datos personales a los clientes por correo electrónico, redes sociales, teléfono, SMS o WhatsApp.
- Se aseguraron las URL de los bancos, las cuales son identificadas como sitios seguros.
- No se mantienen conversaciones privadas ni de amistad con sus clientes a través de las redes sociales, ya sea por privado como por espacios públicos.
- Creación de alertas en las páginas de *home banking* que informan sobre los movimientos de las tarjetas bancarias.
- Sitios de información y prevención para los usuarios.
- Seguir los dictámenes del BCRA en materia de seguridad bancaria.

Estas medidas de seguridad fueron acordadas por la Asociación de Bancos de Argentina, la Asociación de Bancos Públicos y Privados de la República Argentina y la Asociación de la Banca Especializada, la Asociación de Bancos Argentinos, induciendo a los bancos y financieras a realizar campañas de concientización y prevención del ciberdelito mediante la difusión de mensajes simples a toda la población.

La Seguridad Pública, cumple un rol fundamental dentro de la Seguridad Bancaria, y se enmarca en el plexo normativo vigente que se detalla a continuación.

3.2 Políticas públicas de Seguridad Bancaria en Argentina y Mendoza

Las políticas públicas, en materia de Seguridad Bancaria, son definidas por las directrices que establece el BCRA, el cual va adoptando diferentes directivas, en función de las necesidades bancarias que se presentan en forma cotidiana, pero sobre todo, en relación

con la ocurrencia de nuevas formas delictivas, las que se van tomando a medida que aparecen nuevas medidas de seguridad.

A través de la ley 19.130/71, en su artículo Nº2, se crean los organismos provinciales a los fines que realicen el contralor de las entidades que operan bajo la órbita del BCRA, y cuyos controles deberán ser remitidos a esta entidad para su evaluación. Además, el Banco Central de la República Argentina, envía las directrices sobre los requisitos mínimos e indispensables para la apertura de las instituciones bancarias, en materia de seguridad. Las últimas comunicaciones emitidas, se refieren a los ciberdelitos económicos, y estas medidas se ven reflejadas en las comunicaciones denominadas de tipo "A".

Para entender las medidas mínimas de seguridad en entidades Financieras, debemos remontarnos a la Ley 19130/71 la cual da origen en su artículo N°2 a la creación de organismos provinciales a los fines de que realicen el contralor de las entidades que operan bajo la órbita del BCRA, y cuyos controles deberán ser remitidos a esa entidad para su evaluación.-

En nuestra provincia nace como División Seguridad Bancaria en el año 1973 dependiente de la Dirección Comunicaciones, con el trascurso de los años y la incorporación de nuevas tecnologías ésta Dirección fue reemplazada por Informática y Telecomunicaciones y en el año 2009 es creado en forma independiente el Departamento de Seguridad Bancaria, funcionando como tal hasta nuestros días.

La función específica del Departamento de Seguridad Bancaria es verificar que las entidades financieras cumplan con las medidas mínimas de seguridad ordenadas por el BCRA, ésta medidas son publicadas periódicamente por el ente regulador bajo el nombre de COMUNICACIÓN "A" y el número que corresponda.

Si bien han sido modificadas con la incorporación de las nuevas tecnologías, se considera como ley madre a la Comunicación "A" 3390, ésta comunicación es considerada como la Constitución Nacional, todas las nuevas directivas se encuentran subordinadas a ella. La presenta comunicación establece todos los requisitos que debe tener una entidad financiera pero incorpora nuevas medidas mínimas de seguridad que hasta el momento no

se tenían en cuenta. Surge a raíz de una ola de asaltos a sucursales bancarias en todo el país entre los años 1998 y 2000 donde en nuestra provincia llegaron a ser asaltadas 3 sucursales en una semana.

Mediante la Resolución Nº 558-S del 9 de marzo de 2009, se creó el Departamento de Seguridad Bancaria, el cual antes funcionaba como división. Este cambio de categoría, en el Ministerio de Seguridad de Mendoza, respondió a la imperiosa necesidad de brindar soluciones dinámicas al contexto cambiante que se observa en las políticas de Seguridad Bancaria.

Como puede observarse, no existe una política de seguridad bancaria establecida en forma definitiva, ya que las mismas deben mantenerse adecuadas al contexto. En tanto las situaciones de riesgo van cambiando, las políticas de seguridad que establece el BCRA son dinámicas, y se adaptan en tiempo y forma, al contexto en el cual se desarrollan. Estas políticas de seguridad, se amparan en el marco normativo legal que se detalla a continuación.

3.3 Marco normativo legal de la Seguridad Pública

Desde el punto de vista de la Seguridad Pública, el accionar policial se enmarca en las normas que regulan su actuación, la cual es una parte fundamental para garantizar la seguridad del Sistema Bancario.

3.3.1 Ley Nº6721/1999 Bases jurídicas, políticas, institucionales del Sistema Provincial de Seguridad Pública. Principios. Organización. Funcionamiento Policía de Mendoza

El objeto de esta ley es el de "Sentar las bases jurídicas, políticas e institucionales del sistema provincial de seguridad pública, estableciendo sus principios fundamentales, los elementos que lo integran, su organización y funcionamiento.

Los principios fundamentales de esta reglamentación son los de asegurar las condiciones de seguridad pública a todos los habitantes de la provincia, para el pleno goce

de sus derechos, entendiendo que la Seguridad Pública es responsabilidad primaria e irrenunciable del Estado provincial.

Crea el Sistema Provincial de Seguridad Púbica, conformado por "el conjunto de componentes públicos, privados y comunitarios" y que tiene por finalidad "propender a la unidad y coordinación en la formulación, diseño, planificación, ejecución, conducción, control y evaluación de las Políticas de Seguridad Pública que se apliquen en la provincia de Mendoza, con especial referencia al sistema de policías" (Art. 3).

Esta ley, además, crea el Consejo Provincial de Seguridad Pública, integrado por el Ministerio de Justicia y Seguridad, el director de la Inspección General de Seguridad, los legisladores integrantes de la Comisión Bicameral de Seguridad Pública del Poder Legislativo y un representante del Poder Judicial.

En su Artículo 9º la ley establece que se implementan los Consejos de Seguridad Departamentales y de Foros Vecinales a fin de acercar las fuerzas policiales a la comunidad.

El Capítulo VIII de la Ley desarrolla la Junta de Disciplina la cual se encuentra bajo la dependencia del Ministerio de Justicia y Seguridad. Sus funciones son las de resolver sumarios administrativos por faltas e infracciones cometidas por el personal policial; conocer y decidir sobre los recursos de apelación; denunciar a la autoridad competente hechos delictivos advertidos en el ejercicio de sus funciones. Esta junta está integrada por tres miembros que representan al Ministerio de Justicia y Seguridad, el Subsecretario del área y las seis Policías de la Provincia o del Servicio Penitenciario, alternativamente.

Esta norma jurídica ha sido modificada en el año 2007, mediante la Ley 7.813, momento en el que se agrega el artículo 26 y se le otorga a la Inspección General de Seguridad, el carácter de organismo descentralizado. El organismo estará a cargo de un directorio conformado por un director presidente designado por el Poder Ejecutivo Provincial y un mínimo de dos directores vocales que deben ser propuestos por la primera y segunda minoría de la oposición.

Sustituye el inciso 1) del artículo 29 de la Ley 6.721, el que quedará redactado de la siguiente manera:

"Inciso 1) Instruir sumario administrativo y designar a sus instructores quienes serán personal civil de la Inspección General de Seguridad y/o personal policial y/o penitenciario, transferidos al mismo por el Poder Ejecutivo Provincial y seguirán revistando en sus respectivos escalafones bajo la dependencia orgánica y funcional del Directorio de la Inspección General de Seguridad".

3.4 Marco normativo del Sistema de Seguridad Bancaria

La primera obligación de la seguridad bancaria surge del Artículo 42 de la Constitución Nacional en el que se enumeran los derechos básicos de los consumidores "la protección de su seguridad e intereses económicos". Ha reconocido expresamente que todos/as los/as consumidores/as y usuarios/as (entre ellos, claro está, los/as usuarios/as de servicios financieros) tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección; y a condiciones de trato equitativo y digno, a cuyo respecto las autoridades públicas deben proveer a la protección de esos derechos (Defensoría del Pueblo, 2021).

En el marco de la Constitución Nacional y la incorporación de los Tratados Internacionales, se tienen en cuenta las "Directrices para la Protección del Consumidor" de las Naciones Unidas, aprobadas por la Asamblea General de su Resolución Nº 70/186 de septiembre de 2015. Este documento internacional de suma importante, sirve de guía y marco de referencia a los Estados Miembros para implementar políticas activas de defensa a los consumidores.

Posteriormente un conjunto de leyes y normas del BCRA conforman el plexo normativo de seguridad bancaria.

3.4.1 Ley 19.130/71 Seguridad Bancaria. Medidas de seguridad para las entidades financieras de todo el país

Establece que será el Poder Ejecutivo el que determina los requisitos mínimos de seguridad tanto en los edificios donde funcionen los bancos, como en las medidas de seguridad que se aplican en materia de transporte de valores.

Art. 2°.- EL BANCO CENTRAL DE LA REPUBLICA ARGENTINA dispondrá la verificación sobre el cumplimiento de los dispositivos de seguridad por parte de las entidades financieras comprendidas. A este fin, contará con el asesoramiento técnico de la Policía Federal tratándose de casas ubicadas en el ámbito de la Capital Federal y con el de los organismos de seguridad competentes, cuando funcionen en jurisdicción provincial. Los organismos de seguridad mencionados verificarán como mínimo semestralmente el correcto funcionamiento de los sistemas de prevención implantados.

> "Art. 2°.- EL BANCO CENTRAL DE LA REPUBLICA ARGENTINA dispondrá la verificación sobre el cumplimiento de los dispositivos de seguridad por parte de las entidades financieras comprendidas. A este fin, contará con el asesoramiento técnico de la Policía Federal tratándose de casas ubicadas en el ámbito de la Capital Federal y con el de los organismos de seguridad competentes, cuando funcionen en jurisdicción provincial. Los organismos de seguridad mencionados verificarán como mínimo semestralmente el correcto funcionamiento de los sistemas de prevención implantados."

3.4.2 Ley 24.240/93 Ley de Defensa del Consumidor

Esta ley, en su Artículo 5º establece la obligación de seguridad, en sentido estricto, y obliga a las entidades financieras a advertir los riesgos, pero además, los responsabiliza por el riesgo de la cosa. ARTICULO 5º — Protección al Consumidor. Las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios.

En este sentido, la responsabilidad de los bancos ante las estafas electrónicas es relativa y solo se vincula con aquellos casos en los cuales se haya comprobado que dicha estafa haya sucedido como parte de la vulnerabilidad del sistema bancario. Para que esto ocurra, el sistema informático del banco debe haber sido vulnerado, siempre que las medidas de protección de los usuarios hayan sido establecidas en su máximo nivel disponible al momento que ocurra el delito (Abad, 2021).

3.4.3 Ley 25.326/2000 de Protección de los datos personales

Se caracteriza por definir principios generales relativos a la protección de datos. Esto abarca desde derechos de los titulares hasta las figuras de usuarios y responsables de archivos, registros y bancos de datos. El control, las sanciones, la acción de protección de los datos personales e inclusive el spam están vinculados a esta Ley.

El artículo establece que se protegerán los datos personales "asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".

En su artículo Nº9 establece que

> "El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".

En este sentido, la norma establece que "queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan las condiciones técnicas de integridad y seguridad".

3.4.4 Ley Nº 26.388/2008 Código Penal. Modificación

Modificación del Código Penal que permitió incorporar diversos delitos informáticos, tales como la distribución y tenencia, de material con fine de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Esta no es una ley especial que regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código.

En el artículo 1º sostiene que: Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Artículo 2º — Sustituye el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Principalmente incluye temas como:

- Distribución y tenencia con fines de distribución de pornografía infantil
- Violación de correos electrónicos
- Acceso ilegítimo a sistemas informáticos

3.4.5 Ley 26.637/2010 Entidades Financieras

Medidas mínimas de seguridad que deben adoptar las entidades bancarias y financieras nació como consecuencia de los altos índices delictivos que se produjeron durante el año 2010 en bancos del país.

El artículo 1° establece que las medidas de seguridad contenidas en su cuerpo revisten carácter obligatorio para las entidades enmarcadas bajo la Ley n° 21.52615, como así en sus modificatorias y complementarias.

De acuerdo al artículo 2 de dicha ley las medidas a implementar para mejorar la seguridad consisten en 3 ejes fundamentales:

- La instalación de mamparas divisorias entre el salón de espera y la línea de cajas que aseguren el suficiente nivel de reserva a efectos de impedir la observación por parte de terceros de las operaciones realizadas por el público.
- El reforzamiento o recambio de los recintos destinados al resguardo de valores propios o de cajas de seguridad de alquiler.
- La instalación de inhibidores o bloqueadores de señal de celulares.

3.4.6 Ley 26.904/2013 Incorporación del Art. 131 al Código Penal.

Plantea el *grooming* en Argentina como delito. Incorpora en el Código Penal el artículo 131, el que sostiene que "será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma"

3.4.7 Resolución Nº 139/2020 del Ministerio de Desarrollo Productivo, Secretaría de Comercio Interior de la Nación

En referencia a la extrema necesidad de acentuar la prevención del ciberdelito y proteger a usuarios y consumidores que por diferentes motivos se encuentra en situación de mayor vulnerabilidad o con una vulnerabilidad agravada, se establece en esta Resolución que

> "… a los fines de lo previsto en el Art. 1º de la Ley 24.440 se consideran consumidores hipervulnerables a aquellas personas que sean personas humanas y que se encuentren en otras situaciones de vulnerabilidad en razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales que provoquen especiales dificultades para ejercer con plenitud sus derechos como consumidores".

En su artículo 2º describe los factores que se constituyen en causas de vulnerabilidad para el consumidor, entre los que semana las personas mayores de 70 años, personas con discapacidad, pertenencia a pueblos originarios, ser jubilado/pensionado/trabajador en relación de dependencia con un salario menor a dos Salarios Mínimos Vitales y Móviles, Monotributista social, entre otros.

3.4.8 Comunicaciones del Banco Central de la República Argentina

Las Circulares del BCRA son herramientas que contienen diferentes temas, los que a su vez están subdivididos en capítulos. “A estos se les asigna, además, de su denominación, su abreviatura” (BCRA, 2021).

Las actualizaciones ser efectúan mediante comunicaciones “A”, “B” y “C”, en las que se dan a conocer las sucesivas modificaciones y/o rectificaciones que se producen en cada tema. Las comunicaciones “A” llevan doble numeración secuencial: de la propia comunicación y del ordenamiento”. A continuación, se presentan las comunicaciones vinculadas con la seguridad bancaria referentes a la modalidad *on line*.

3.4.8.1 Comunicación “A” 3390/2001

La presente comunicación establece todos los requisitos que debe tener una entidad financiera, incorporando nuevas medidas mínimas de seguridad que hasta el momento no se tenían en cuenta.

Independientemente de las normas de atesoramiento del dinero, construcción de recinto privado de seguridad (bunker) o uso de castillete, ésta Comunicación modifica el sistema en las líneas de caja, ordenando que deben tener 2.20 mts. de alto los vidrios blindados, ya que los asaltantes saltaban la línea de caja y se apoderaban del dinero, pero como novedad incorpora la prohibición de uso de aparatos de telefonía móvil o similar dentro de las sucursales, como así también establece pautas sobre el uso de anteojos oscuros sombrero o gorras.

3.4.8.2 Comunicación “A” 6017/2016

En esta comunicación el BCRA especifica las características de seguridad que deben tener en referencia a la integridad, registro, monitoreo, el control, la gestión de incidentes, control de acceso y de la matriz de Escenarios y Control de Riesgo Operacional de Tecnología. Define que es responsabilidad de las entidades financieras preservar no solo

la privacidad de sus usuarios, sino además, arbitrar todas las acciones correspondientes para disminuir los riesgos de vulnerabilidad tecnológica.

Establece la responsabilidad de los canales electrónicos definiendo que los directorios de las entidades financieras son los responsables primarios de la gestión de seguridad informática y de la operatoria de los Canales Electrónicos.

3.4.8.3 Comunicación "A" 6853/2019

Tiene por finalidad agilizar los trámites bancarios en referencia a la creación de la banca on-line, autorizando la utilización de estos dispositivos, en el interior de los recintos bancarios, pero bajo la supervisión de personas autorizadas por la entidad.

3.4.8.4 Comunicación "A" 6878/2020

Establece en su normativa la imposición a "las entidades bancarias que deberán tener implementados mecanismos de seguridad informática que garanticen la genuinidad de las operaciones".

3.4.8.5 Comunicación "A" 6942/2020

En el marco de la emergencia sanitaria se establecen las formas de atención las que quedaron configuradas como:

- Continuar prestando los servicios que usualmente prestan en forma remota, como ser: constitución de plazos fijos, otorgamiento de financiaciones y los servicios relacionados con el sistema de pago.
- Adoptar las medidas necesarias, incluyendo los recursos humanos, para garantizar la suficiente provisión de fondos en cajeros automáticos y la continuidad de la operatoria relacionada con la extracción de efectivo en puntos de extracción extra bancarios. El BCRA garantizará la provisión de efectivo para este fin.

3.4.8.6 Comunicación "A" 7370/2021

Establece los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

Refuerza las autorizaciones de créditos estableciendo que:

Para la autorización de un crédito pre aprobado la entidad debe verificar fehacientemente la identidad de la persona usuaria de servicios financieros involucrada. Esta verificación debe hacerse mediante técnicas de identificación positiva, de acuerdo con la definición prevista en el glosario y en el requisito técnico operativo específico (RCA040) de estas normas. Asimismo, se deberá constatar previamente a través del resultado del proceso de monitoreo y control, como mínimo, que los puntos de contacto indicados por el usuario de servicios financieros no hayan sido modificados recientemente. Una vez verificada la identidad de la persona usuaria, la entidad deberá comunicarle –a través de algunos de los puntos de contacto disponibles– que el crédito se encuentra aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de los 2 (dos) días hábiles siguientes. El citado plazo de acreditación podrá ser reducido en el caso de recibirse la conformidad del usuario de servicios financieros de manera fehaciente.

La entidad financiera quedará exceptuada de implementar lo previsto precedentemente, en la medida de que dé cumplimiento a alguna de las siguientes condiciones:

- Que para la autorización de un crédito pre aprobado la entidad financiera verifique fehacientemente la identidad de la persona usuaria de servicios financieros involucrada, mediante soluciones biométricas con prueba de vida.
- Que la entidad financiera cancele el crédito pre aprobado, asuma la devolución de las sumas involucradas y anule los posibles efectos sobre la situación crediticia de la persona usuaria de servicios financieros afectada, ante la denuncia policial presentada por esta persona usuaria de acuerdo con el modelo de acción "asumido" definido en el requisito RMC004, siempre

que la denuncia se presente en un plazo máximo de 90 (noventa) días corridos desde el vencimiento de la primera cuota del crédito.

En ambos casos, el crédito solicitado podrá acreditarse de manera inmediata en la cuenta del usuario. La actividad que se realice para el cumplimiento de este requisito debe ser trazable y auditable.

En este período de pandemia se ha puesto de manifiesto, en referencia a las entidades bancarias, que, en su carácter de especializados en servicios financieros, poseen una responsabilidad mayor a partir del crecimiento de la banca *on line*, ya que los cambios producidos como consecuencia de la aparición del Covid-19, generaron también un conjunto de cambios en las características de los delitos que fueron sucediendo en este período. Esto llevó no solo a crear nuevas formas de atención, sino a profundizar notablemente las medidas de seguridad. Sin embargo, la pregunta que gira en torno a esto, es si han sido suficientes. Para dar respuesta a lo expuesto precedentemente, en el siguiente capítulo se desarrolla el trabajo de campo, en el cual se va a contrastar empíricamente esta problemática en el Sistema Bancario de la provincia de Mendoza.

Capítulo IV

Trabajo de campo

“Ciberdelito económico y vulnerabilidad del Sistema Bancario en la provincia de Mendoza”

4.1 Entrada en contexto

La presente investigación parte de analizar el impacto del uso masivo de la banca online sobre el ciberdelito económico en el Sistema Bancario de la provincia de Mendoza, en el contexto de pandemia, durante el período 2020 y 2021. Como se ha mencionado, el Sistema Bancario, tanto a nivel mundial como en Argentina y en Mendoza, debió adaptarse rápidamente a los cambios producidos por la situación de riesgo generada por la pandemia de Covid-19.

A partir de la aparición de la pandemia de Covid-19 se generaron un conjunto de cambios que fueron paulatinamente creciendo en la búsqueda de disminuir la circulación de la población en el territorio. En este contexto, el Sistema Bancario sufrió un conjunto de modificaciones en la atención a sus clientes, que se detallan a continuación.

4.1.1 Constitución del Sistema Bancario de Mendoza

Está constituido por bancos del sector público y privado los que se conforman por 175 unidades financieras habilitadas en todo el territorio mendocino, de las cuales solo el Banco de la Nación Argentina corresponde al sistema público, mientras que las restantes 174 unidades financieras bancarias corresponden al sistema privado.

En el territorio se dispone de 668 cajeros automáticos, distribuidos estratégicamente en la provincia, y 333 bocas de expendio de efectivo habilitadas. Estas últimas, se refieren a las terminales ubicadas en estaciones de servicios o negocios habilitados para entregar dinero en efectivo.

De acuerdo a los datos obtenidos por el BCRA (2021), en este sistema bancario operan 9.521.761 cuentas, las cuales corresponden a diversos propietarios como jubilados, empresas públicas y privadas, ONG, entre otras.

4.1.2 Organización del Sistema de Seguridad Bancaria

En la provincia de Mendoza la institución de seguridad encargada de la Seguridad Bancaria es el Departamento de Seguridad Bancaria, el cual se encuentra en funcionamiento desde el año 2009.

Su función principal es la de verificar que las entidades financieras cumplan con las medidas mínimas de seguridad ordenadas por el BCRA, estas medidas son publicadas periódicamente por el ente regulador bajo el nombre de COMUNICACIÓN "A" y el número que corresponda.

Si bien han sido modificadas con la incorporación de las nuevas tecnologías, se considera como ley madre a la Comunicación "A" 3390, la cual presenta las nuevas directivas que se encuentran subordinadas a ellas, las que consisten en:

- Modificación de la seguridad en las líneas de caja, las cuales deben presentar divisiones por vidrios blindados de 2,2 mts de alto.
- Seguridad Privada en el interior del recinto bancario y Seguridad Pública en el exterior de los mismos.
- Prohibición de utilización de aparatos de telefonía móvil o similar dentro de las sucursales.
- Establecimiento de pautas sobre el uso de anteojos oscuros, sombreros o gorras.
- Incorporación de nueva tecnología en los Circuitos Cerrados de Televisión (CCTV) como centros de monitoreo, en los que se debe realizar un monitoreo permanente, sobre todo en los ingresos a las entidades bancarias, donde se debe observar el rostro del cliente.
- Incorporación de CCTV para monitorear a los clientes en los cajeros automáticos.
- Comunicación "A" 6894 en la que se establece un Monitoreo Remoto a Distancia que reemplaza al policía de castillete
- Se deja solo como custodia al personal de seguridad del banco dentro de la sucursal.
- Incorporación de personal de la Seguridad Privada.
- Centro de Monitoreo tiene como objetivo observar el CCTV estableciendo como obligatorio el ingreso a la entidad, línea de caja, tesoro móvil o bóveda, cajas de seguridad si las hubiere, pero principalmente lobby de ingreso con el fin de poder grabar el rostro de las personas que ingresen al mismo.
- A partir de la incorporación de la banca on line, existen, de alguna forma, posibilidades de utilizar la telefonía celular dentro de las instalaciones bancarias, lo que representan una de las mayores fallas de seguridad presentes.

4.1.2.1 Medidas excepcionales de seguridad desde el mes de marzo 2020

A partir de la adopción del período de Distanciamiento Social Preventivo y Obligatorio en el mes de marzo de 2020, se llevaron a cabo las siguientes medidas de seguridad para proteger a la ciudadanía:

- Restricción del personal al 50% incluyendo al personal de Seguridad Privada o Seguridad Pública policial.
- Uso obligatorio de barbijo o tapa boca.
- Uso de telefonía celular o similar, solo con supervisión del personal designado por la entidad financiera.
- Atención del público mediante un sistema de turnos y por terminación de documento.
- Priorización de la atención virtual.

4.1.2.2 Centro de monitoreo privado

Todos los bancos cuentan con un Centro de Monitoreo Privado, el cual se encuentra interconectado con los Sistemas de Alarma que son monitoreados por el personal policial. Las alarmas de estos centros surgen tanto en el sistema policial como en el Sistema de Seguridad Bancaria pero son vigilados por el personal policial.

4.1.2.3 Seguridad cibernética

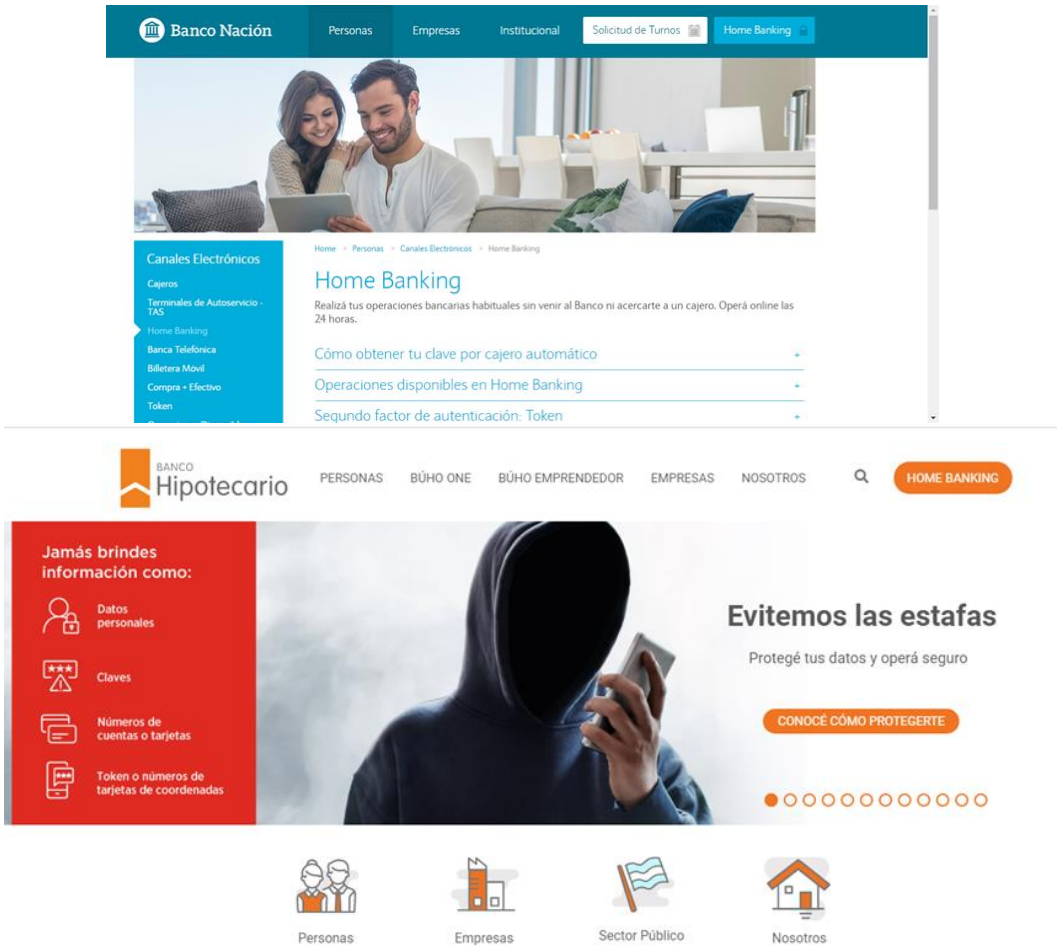
La seguridad cibernética de los bancos es absolutamente privada. Cada banco cuenta con su propio personal especializado en informática el cual debe mantener actualizados sus cortafuegos, los cuales son programas preventivos de invasión externa a los circuitos digitalizados bancarios. Su misión es evitar el fraude cibernético. Las intervenciones de la Seguridad Pública se dan cuando, desde la Fiscalía, se solicitan las investigaciones pertinentes sobre hechos delictuales puntuales, sólo cuando estos han sido ejecutados.

4.1.2.4 Organización de la banca on-line en la provincia de Mendoza

La organización de la banca on –line es la que corresponde a cada banco en particular y la misma se conforma de los dispositivos electrónicos y programas digitales diseñados para sus clientes. Estos diseños se corresponden con lo que cada banco, en su

particularidad, sea este nacional o internacional, haya creado para el acceso de usuarios. Al no existir un banco provincial, no hay una diferenciación entre provincias sobre el diseño de la banca on-line.

Imagen 1 Banco Nación y Banco Hipotecario vistos desde una computadora



Fuente: imágenes recuperadas de: https://www.bna.com.ar/Institucional y https://www.hipotecario.com.ar/ (Consultado 02/12/2021)

En las capturas de pantalla precedentes se observan los formatos de la banca on line tal como es el acceso de usuarios a través de la web en una computadora. En las mismas se observan puntos comunes como el acceso de usuarios, y las diversas prestaciones de servicios que se realizan en forma continua. Las diferencias son de diseño, aunque la mayoría tiene las mismas ubicaciones de ingreso. Estos diseños se han ido modificando con el tiempo.

Las aplicaciones móviles tienen diseños similares para ingresar y, una vez en su interior, cada banco en particular ha creado su propio diseño para la aplicación:

Imagen 2 Aplicación Banco Patagonia

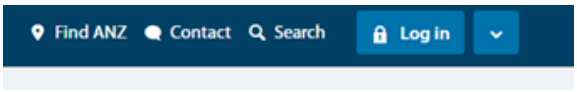
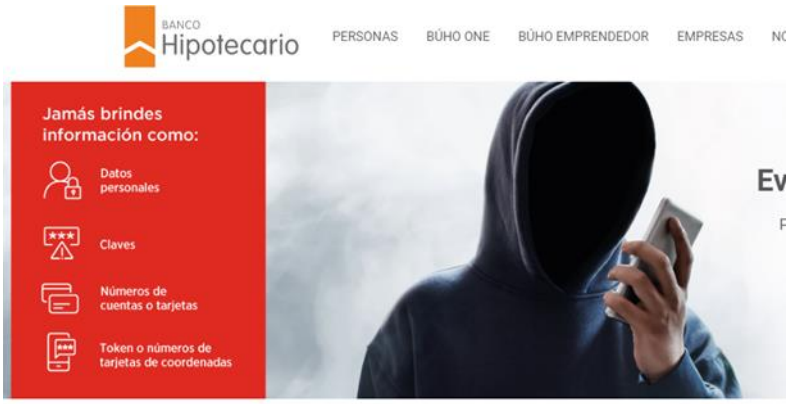
Fuente: Imagen recuperada de e-mail por home banking personal. (2021)

Imagen 3 Aplicación Banco Credicoop

Fuente: Imagen obtenida de Aplicación móvil de cuenta personal del banco Credicoop (2021)

Como puede observarse, en las imágenes precedentes, cada banco tiene sus propias características de diseño ya sea que se trate del ingreso por computadoras, o por las aplicaciones propias de cada uno de los bancos en particular. Sin embargo, presentan características comunes, especialmente en el ingreso por computadora:

Tabla 1 Identificación de información en la banca on-line

El ingreso por usuario se ubica en el ángulo derecho de las pantallas	
Los servicios con los que cuentan los clientes se encuentran a la izquierda de la pantalla	
El acceso a los diferentes clientes se encuentra en el plantel desplegable	
Información preventiva en los espacios de mayor visibilidad, con imágenes destacables.	

Fuente: Elaboración propia en base a capturas de pantalla de Banco Nación y Banco Hipotecario (2021)

Como ha quedado demostrado, la organización de la banca on-line presenta canales de accesibilidad que son similares en todos los bancos, independientemente si estos pertenecen al ámbito privado o público.

En el ingreso a cada una de las partes que componen las páginas web como las aplicaciones, los usuarios encontraran la siguiente información sobre sus cuentas:

- Acceso a las cuentas personales con los movimientos correspondientes al período del banco que haya dispuesto, el cual generalmente se divide cada 30 días.
- Acceso a créditos.
- Acceso a tarjetas de crédito.
- Acceso a pagos de servicios e impuestos.
- Acceso a inversiones
- Acceso a descuentos y beneficios.
- Acceso a compra y/o venta de divisas.
- Acceso a seguros asociados
- Sistema de descuentos y beneficios
- CBU y Alias

Habiendo presentado las descripciones de la banca on- line en sus diferentes versiones digitalizadas, se analiza la problemática de inseguridad, la cual refleja la vulnerabilidad que presenta el Sistema Bancario en la provincia de Mendoza.

4.2 Desarrollo metodológico

Metodológicamente esta investigación es de campo con un diseño flexible ya que combina diferentes tipos de técnicas. El alcance es descriptivo dado que pretende dar cuenta de los eventos que corresponden al ciberdelito económico, y cómo este se ha desarrollado en la provincia de Mendoza durante el período de estudio. Los estudios de alcance descriptivo, buscan describir, como su nombre lo menciona, los eventos o las circunstancias en que se dan determinados fenómenos, en este caso los ciberdelitos económicos que han vulnerado los sistemas. Por otro lado, estos estudios buscan especificar las propiedades y características de los grupos de personas y/o fenómenos estudiados y sometidos al análisis del investigador.

Además, el estudio es de alcance explicativo, ya que pone de manifestó cuáles son las causas que permiten que este tipo de hechos delictivos, se produzcan en el ámbito bancario. A partir del análisis, se podrá realizar una explicación respecto a las

circunstancias en que estos fenómenos se manifiestan, luego de haber descripto las características particulares del objeto de estudio. Los trabajos con alcance explicativo buscan encontrar una explicación del porqué ocurren los fenómenos y en qué circunstancias se dan los mismos. Estas investigaciones dirigidas a responder sobre las causas de los eventos sociales, permiten proyectar predicciones que sostengan que, en iguales condiciones sobre objetos similares, ciertas causas pueden provocar otros efectos (Montbrún Ruggiero, 2013).

4.2.1. Unidades de análisis

Las unidades de análisis son aquellas de las cuales se saca información sobre el estudio, a continuación, se mencionan:

- Sistema de Seguridad Bancaria de la provincia de Mendoza.
- Sistema de Seguridad Pública de la provincia de Mendoza.
- Ciberdelitos económicos.
- Medidas de prevención y control del delito
- Personal bancario, especialistas en seguridad bancaria y especialistas en ciberdelitos.

4.2.2. Fuentes de información

Las fuentes de información son aquellas de las cuales se extrae la información para luego ser analizada y tener el dato correspondiente. A continuación, se mencionan.

4.2.2.1. Fuentes secundarias

Estas se componen de la información estadística obtenida de hechos de ciberdelitos económicos a entidades bancarias, registrados durante el período 2020 – 2021 las mismas son:

- Asociación Argentina de Lucha Contra el Cibercrimen.
- Unidad Fiscal Especializada en Ciberdelincuencia (UFECI).
- Dirección de Defensa al Consumidor del Gobierno de Mendoza

4.2.2.2. Fuentes primarias

- Personal bancario
- Jefes de seguridad de entidades bancarias
- Asesor de seguridad bancaria
- Analista de seguridad del BCRA
- Subcomisario analista de sistemas y diplomado en Cibercrimen y Evidencia Digital
- Subcomisario a cargo de la Delegación del Departamento de Seguridad Bancaria Zona Sur
- Subcomisario especialista en seguridad bancaria.

4.2.3. Técnicas de información

4.2.3.1. Técnicas de observación documental

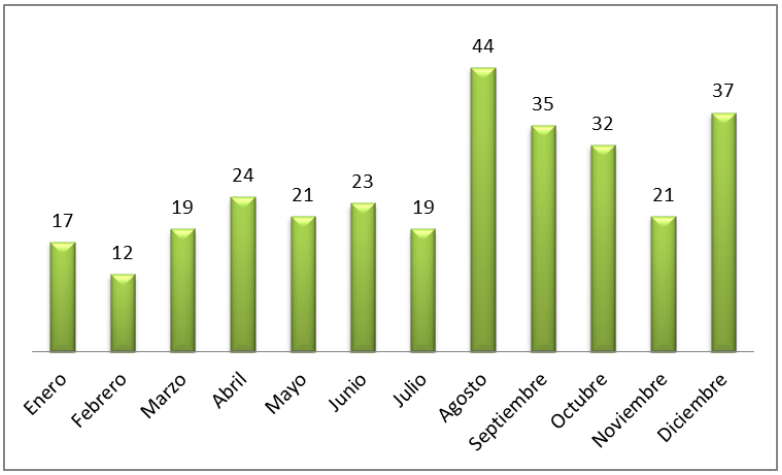
Consiste en la búsqueda, identificación, recolección y análisis de documentos que se relacionan con el tema de investigación, en este caso, los ciberdelitos económicos registrados en Argentina y Mendoza de los que fueron víctimas los usuarios de entidades bancarias, durante los años 2020 y 2021. Respecto a este último período solo se toman en cuenta los primeros 6 meses del año ya que no se cuenta con datos estadísticos del segundo semestre.

4.2.3.1.1 Análisis de la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC)

La Asociación Argentina de Lucha Contra el Cibercrimen, es una institución conformada por personal policial y expertos en cibercrimen. Esta institución se ocupa de contabilizar los ciberdelitos, realizando investigaciones permanentes, elaborando estadísticas y brindando capacitación a profesionales de todo el país. Cuenta con una vasta trayectoria en el abordaje de estos delitos, compartiendo con toda la comunidad de profesionales dedicados al abordaje de la seguridad, los resultados de sus múltiples investigaciones. A continuación, se presentan los datos estadísticos correspondientes.

4.2.3.1.1.1 Ciberdelitos de estafa y fraude bancario año 2020

Gráfico Nº1 Evolución de los ciberdelitos de estafa y fraude bancario durante el año 2020, expresado en miles

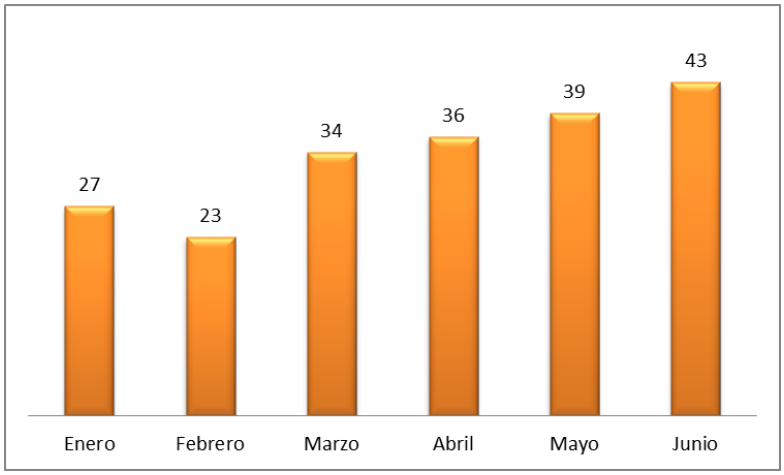


Fuente: Elaboración propia en base a datos obtenidos de AALCC, (2021).

El gráfico Nº1 de la AALCC, permite observar cómo se han incrementado este tipo de delitos a lo largo del año 2020. El mes de agosto ha sido el período durante el cual se ha producido mayor cantidad de ciberdelitos, seguidos por el mes de diciembre y septiembre. Si realizamos la comparación con los meses enero y febrero, podemos observar que los ciberdelitos económicos, presentaban un crecimiento tan elevado.

4.2.3.1.1.2 Ciberdelitos de estafa y fraude bancario año 2021

Gráfico Nº 2 Evolución de los ciberdelitos de estafa y fraude bancario durante el primer semestre del año 2021, expresados en miles

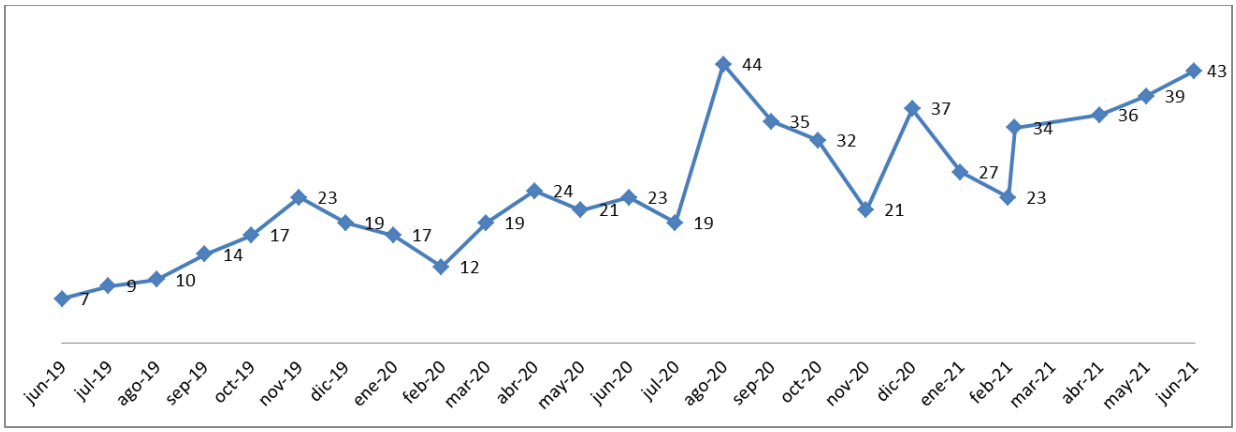


Fuente: Elaboración propia en base a datos obtenidos de AALCC, (2021)

El gráfico Nº2 de la AALCC, muestra el incremento de los ciberdelitos durante el primer semestre del año 2021. Como puede observarse, los mismos han ido creciendo en forma paulatina, siendo el mes de junio el más significativo.

4.2.3.1.1.3 Evolución de los ciberdelitos de estafa y fraude bancario

Gráfico Nº 3 Evolución de los ciberdelitos de fraude y estafa bancaria desde junio de 2019 hasta junio 2021, expresado en miles



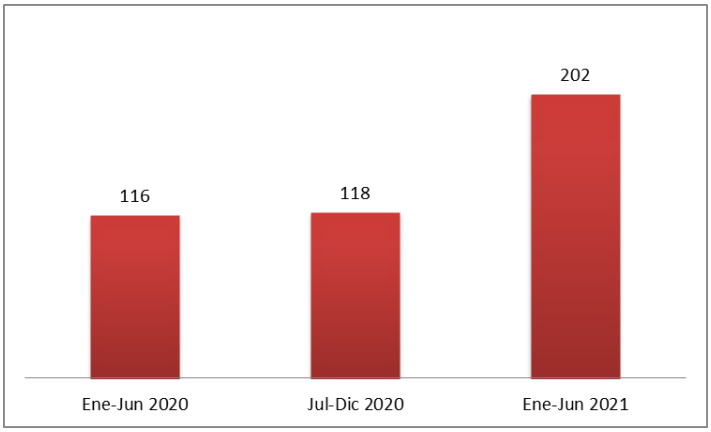
Fuente: Elaboración propia en base a datos obtenidos de AALCC, (2021) Nota: el valor corresponde a miles.

El gráfico Nº 3 muestra el incremento de ciberdelitos de fraude y estafa bancaria registrados desde el mes de junio del año 2019, momento en que se producían menos delitos, hasta el mes de junio de 2021. Se observa que en mes de agosto 2020 se produjo un incremento notable de este tipo de delitos, momento en el cual se habían incrementado las ayudas económicas que el Estado brindaba a la sociedad, con motivo de las dificultades económicas producto del confinamiento de la cuarentena. Si bien con posterioridad se

observa que han disminuido levemente estos hechos, durante el primer semestre del año 2021 se ha vuelto a incrementar y no se ha regresado a los valores del año 2019.

4.2.3.1.1.4 Crecimiento de los delitos de estafa y fraude bancario semestres 2020-2021

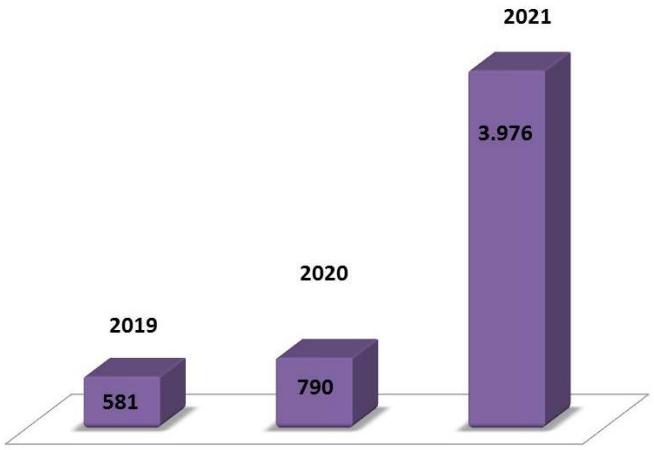
Gráfico Nº 4 Evolución de los delitos de estafa y fraude bancario por semestres 2020-2021, expresado en miles



Fuente: Elaboración propia en base a datos obtenidos de AALCC, (2021) Nota: el valor corresponde a miles.

El gráfico Nº4 muestra la evolución que estos delitos han presentado durante los 3 períodos semestrales correspondientes al año 2020 y 2021. Teniendo en cuenta la comparativa del período enero-junio 2021, respecto al mismo período del año anterior, los delitos han presentado una importante variación, que se sitúa en el 74,14% de incremento durante el año 2021.

Gráfico Nº 5 Evolución interanual de los ciberdelitos generales desde 2019 hasta el primer semestre 2021, expresado en miles



Fuente: Elaboración propia en base a datos obtenidos de AALCC, (2021)

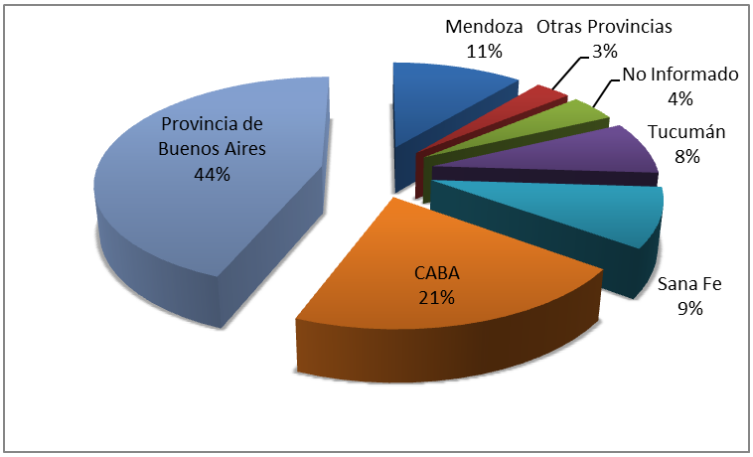
El gráfico Nº 5 presenta la evolución de los delitos cibernéticos (expresados en miles, que incluye todos los delitos que se producen dentro de esta modalidad) desde el año 2019 hasta el primer semestre del año 2021. Los delitos han aumentado 35,97% en el año 2020, respecto al año 2019. Diferente es el caso del comparativo del año 2020 respecto al año 2021, momento en el cual los ciberdelitos se han incrementado en un 403%. Estos datos se refieren a los delitos denunciados en forma presencial y vía e-mail en todo el territorio argentino. Incluyen los acosos, la difamación (generalmente en redes sociales), la circulación de las denominadas fake news, el ciberbuling, phishing, extorsión, ciber odio, pornografía infantil, tráfico de drogas, entre los más comunes.

4.2.3.1.2 Análisis de la Unidad Fiscal Especializada en Ciberdelincuencia (UCEFI)

Es la Unidad Fiscal Especializada en Ciberdelincuencia, creada mediante la Resolución PGN Nº 3743/15, con el fin de robustecer la capacidad de respuesta del organismo en materia de detección, persecución y represión de la criminalidad organizada y de los delitos que más menoscaban la Seguridad Pública. En ella se concentran todos los ciberdelitos del país. Los mismos se encuentran desglosados por provincia y por tipología delictiva. A continuación, se presentan los datos obtenidos sobre ciberdelitos económicos.

4.2.3.1.2.1 Distribución por provincia de los ciberdelitos de fraude y estafa bancaria

Gráfico Nº 6 Porcentaje de ciberdelitos de fraude y estafa bancaria, según provincia correspondientes al año 2021

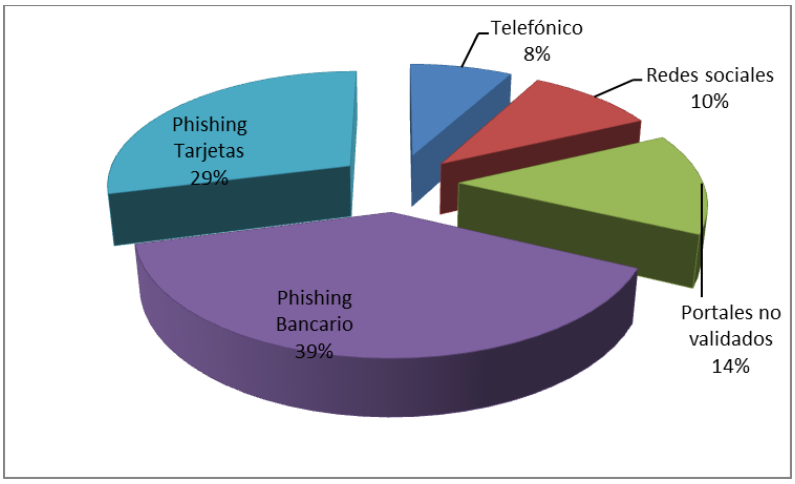


Fuente: Elaboración propia en base a datos obtenidos de UFECI, (2021)

El gráfico Nº6 permite observar que la provincia de Buenos Aires es donde mayor cantidad de delitos se han producido, seguidas por CABA (Ciudad Autónoma de Buenos Aires), con un 21% del total. En tercer lugar, se encuentra la provincia de Mendoza con un 11% del total de ciberdelitos de fraude y estafa, posteriormente le siguen Santa Fe y Tucumán.

4.2.3.1.2.2 Modalidades más comunes dentro del fraude bancario

Gráfico Nº 7 Modalidad más frecuente de delitos de fraude y estafa bancaria año 2020



Fuente: Elaboración propia en base a datos obtenidos de la UFECI (2021)

- *Compras en portales no validados o redes sociales*. Esta modalidad delictiva se caracterizó por buscar a las víctimas a través de las redes sociales, donde éstas expresan sus preferencias. Se ofrecen diversos productos y/o servicios que el cliente ve en una plataforma perfectamente conformada, donde puede adquirirlos. Una vez ingresados los datos de sus tarjetas de crédito y/o débito, los delincuentes aprovechan para retirar el dinero de los bancos. Durante el año 2020, esta modalidad ha representado el 14% de los hechos de ciberdelito.
- *Robo de información de llamadas telefónicas.* Durante el año 2020, el Estado ha brindado un conjunto de ayudas sociales a los más vulnerables. Esto posibilitó que los delincuentes aprovecharan para crear mensajes, con imágenes y logos oficiales, y ofrecer al usuario la posibilidad de cobrar con anticipación un beneficio o acceder al mismo. Para esto se les solicita que cambien la contraseña de ingreso a su cajero automático o al *home banking*. Una vez realizado esto, el delincuente procede a retirar los fondos. Además, se han registrado pedidos de préstamos bajo esta modalidad, la cual representa el 8% del total.
- *Phishing*, con la modalidad más frecuente de envío de e-mail. Esta modalidad ha crecido: 39% a nivel bancario; 29% a nivel de tarjetas de crédito y 10% por datos obtenidos a través de redes sociales. En la Figura Nº1 se presenta un ejemplo de e-mail fraudulento
- *Redes sociales*: esta modalidad delictiva ha sido otra de las más frecuentes durante el período de estudio. Mediante el uso de WhatsApp, la circulación de información falsa se ha incrementado a cifras de las que no se tienen registros, esto es porque muchas de ellas no son denunciadas. Sin embargo, ha sido la red más utilizada para la estafa o fraude bancario, representando el 10% del total de los hechos de ciberdelito.

Figura 1 Ejemplo de e-mail fraudulento

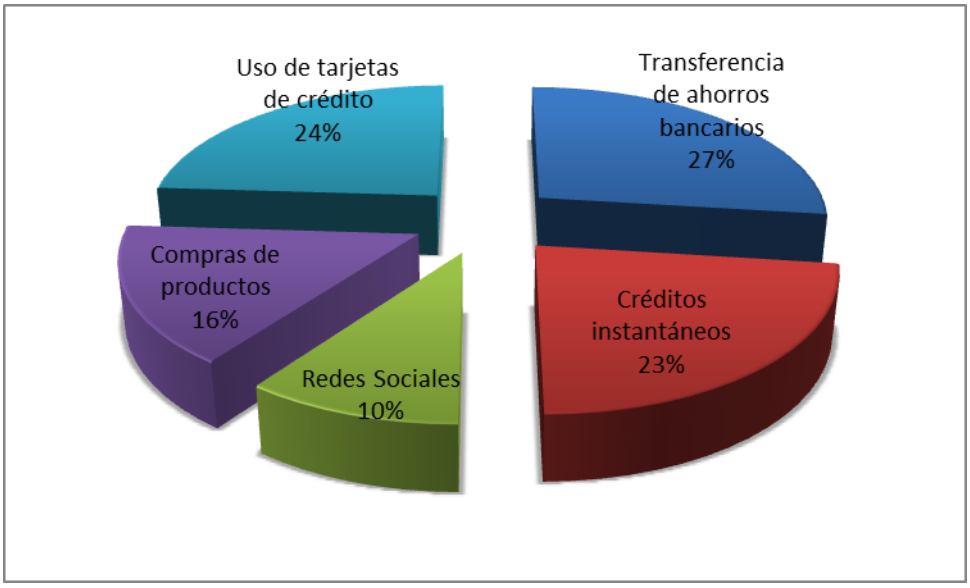
Fuente: Captura de pantalla de e-mail personal recibido bajo la modalidad del delito de phishing. (2021)

En la figura Nº1 se observa cómo le llega el e-mail al usuario, el cual procede de una cuenta de servicios de correo comunes a todos los usuarios de internet (mercyok@hotmail.com), pero se realiza con copia al e-mail alerta@bancohipotecario.com.ar con una extensión http[1] del banco hipotecario.

4.2.3.1.2.3 Operatoria utilizada

Gráfico Nº 8 Tipo de operatoria de delitos de fraude y estafa bancaria año 2020

[1] Hypertext Transfer Protocol (**HTTP**) (o Protocolo de Transferencia de Hipertexto en español) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML



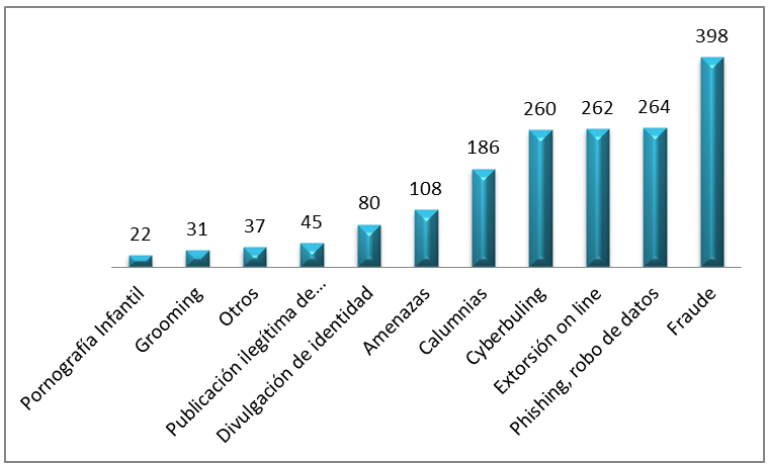
Fuente: Elaboración propia en base a datos obtenidos de la UFECI, (2021)

El gráfico Nº8 expone el porcentaje de ciberdelitos registrados en el año 2020, según la operatoria que se ha utilizado para llevarlos a cabo. Las transferencias de ahorros bancarios, se corresponden con el 27%, seguido por el uso de tarjetas de créditos y los créditos instantáneos. Posteriormente aparecen las compras de productos y finalmente la utilización de redes sociales.

4.2.3.1.2.4 Ciberdelitos económicos en Mendoza

En este punto se debe destacar que la provincia de Mendoza no cuenta con datos estadísticos actualizados, por lo que se ha recurrido a las fuentes de la UCEFI y el Informe de Reclamos de Defensa al Consumidor a nivel nacional, el cual presenta datos desagregados por provincia en función de los reclamos que se realizan en las oficinas de Defensa al Consumidor provinciales.

Gráfico Nº 9 Delitos de mayor frecuencia en Mendoza. Primer semestre año 2020



Fuente: Elaboración propia en base a datos obtenidos de la UFECI, (2021)

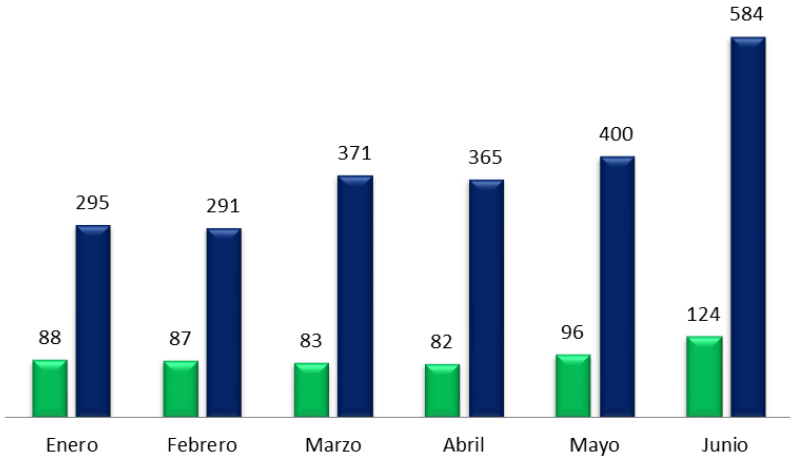
El gráfico Nº9 muestra que los delitos que más se han denunciado a las fiscalías durante el primer semestre del año 2020 en la provincia de Mendoza, son los de fraude, los que corresponden a 398 casos, seguidos por *phishing*, con un total de 264 casos y la extorsión *on line* correspondiente a 262 casos. Posteriormente sigue el delito de *cyberbulling*, calumnias, amenazas, divulgación de identidad, publicación ilegítima de imágenes, otros (no especificados), *grooming* y pornografía infantil.

4.2.3.1.3 Análisis de datos de la Dirección de Defensa al Consumidor Gobierno de Mendoza

La Dirección de Defensa al Consumidor, dependiente del Ministerio de Economía de la Provincia de Mendoza, es la entidad encargada de recibir, en primera instancia, gran parte de las denuncias por estafas o fraudes bancarios, de víctimas que no encuentran respuestas en sus reclamos en el banco. Una vez ingresada la denuncia en esta institución, los profesionales las procesan y las derivan hacia la fiscalía, en el caso que se considere que se requiere el inicio de una investigación judicial. A continuación se presenta el comparativo que esta institución, ha elaborado correspondientes a los años 2020 y 2021.

Gráfico Nº 10 Comparativa 2020-2021 denuncias de reclamos de Fraude o Estafa cibernética

Mes	2020	2021
Enero	88	295
Febrero	87	291
Marzo	83	371
Abril	82	365
Mayo	96	400
Junio	124	584
Total	560	2306



Fuente: Defensa al Consumidor (2020)

El gráfico Nº10 presenta los datos comparativos por mes y año, en base a las denuncias que se han recibido en Defensa al Consumidor (2020). En este punto se observa que el año 2021 (representado por el color azul), muestra un considerable aumento de denuncias por fraude o estafa respecto de los mismos meses del año 2020 (representado por el color verde), siendo el mes de junio 2021, donde se han recibido mayor cantidad de denuncias de fraude o estafa.

4.2.3.1.4 Análisis de fuentes secundarias

La mayor dificultad a la que se ha debido enfrentar en este trabajo ha sido la obtención de datos actualizados, esto se debe a que los mismos aún no son cargados en ninguna base de datos estadísticos sobre todo de la provincia de Mendoza. Por este motivo, se ha recurrido al conjunto de datos disponibles en la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), la Unidad Fiscal Especializada en Ciberdelincuencia y el último informe de Defensa al Consumidor.

Los datos presentados han puesto en evidencia que el ciberdelito, bajo la modalidad de fraude y estafa bancaria, han presentado un notable incremento desde el año 2020 como producto del aumento de la utilización de internet, ya sea para realizar operaciones bancarias, como para realizar otro tipo de transacciones comerciales en las que se

incluyeron estafas mediante la utilización de redes sociales, aprovechando claramente la oportunidad de intercambio de información de múltiples usuarios.

De igual manera, los bancos han aumentado el contacto con sus clientes utilizando las redes sociales, con páginas que tienen acceso público y en las cuales, muchos usuarios han volcado datos personales inocentemente como números telefónicos y/o números de documento. En la era digital, donde todo es fácilmente rastreable, estos datos pueden ser de vital importancia para los ciberdelincuentes.

Sin ninguna duda, tal como lo refleja el gráfico Nº3, los delitos de este tipo han aumentado notablemente desde junio de 2019. Si bien este período de estudio no corresponde a la presente investigación, sirve como referencia para demostrar el rápido aumento delictivo.

Dentro de estos delitos, las formas más comunes de delincuencia son el *phishing* bancario y *phishing* de tarjetas. Esta separación se realiza para diferenciar aquellos delitos que se realizaron con tarjetas de crédito, respecto de las tarjetas de débito o la violación del *home banking*. De todos modos, las modalidades de las que se trate, han puesto en evidencia que la vulnerabilidad de los usuarios por el uso de internet, es elevada en tanto se refleja de igual manera en las redes sociales y los fraudes en los portales no validados. Esto permite inferir que existe una falta de concientización en la población respecto de la vulnerabilidad que presenta el uso de internet.

De acuerdo al gráfico Nº6, Mendoza se encuentra en tercer lugar en relación al resto del país en referencia a los ciberdelitos de fraude y estafa bancaria, lo que significa que se requiere urgentemente que se realicen estadísticas suficientes que den cuenta de los mismos, pero sobre todo que permitan inferir la modalidad más usada, así como las instituciones bancarias más vulnerables.

El gráfico Nº10 muestra la comparativa del crecimiento de los ciberdelitos de estafa y fraude en la provincia de Mendoza, y estos datos son alarmantes al observar que por ejemplo, el mes de junio de 2021 arrojó 584 denuncias en Defensa al Consumidor, lo que significan 460 casos más respecto al mismo período del año anterior en el cual se

registraron, durante el mes de junio 124 denuncias por estafa y/o fraude bancario a los usuarios.

Estos datos secundarios, serán contrastados con los obtenidos de las entrevistas realizadas, que se presentan a continuación.

4.2.4 Fuentes primarias

Las fuentes primarias provienen de entrevistas a personal bancario, especialistas en seguridad bancaria, especialistas en cibercrimen, y analistas de seguridad bancaria.

La población de estudio se compone de:

- Profesionales que se desempeñan en el ámbito del cibercrimen.
- Profesionales que se desempeñan en el ámbito de Seguridad Bancaria.
- Personal bancario.
- Personal policial de investigaciones que indaga sobre ciberdelitos bancarios.

Se realizó una muestra teórica, voluntaria e intencional, compuesta de las personas que decidieron participar de la investigación y que además, conocen la problemática de estudio. Dadas las características sensibles de la misma, se tuvo en cuenta especialmente el respeto por la privacidad de quienes no desearon brindar sus datos personales, por lo que se garantizó absoluta reserva sin volcar esos datos. La muestra teórica se compone de ocho personas:

- Personal bancario
- Jefes de seguridad de entidades bancarias
- Asesor de seguridad bancaria
- Analista de seguridad del BCRA
- Subcomisario analista de sistemas y diplomado en cibercrimen y evidencia digital
- Subcomisario a cargo de la Delegación del Departamento de Seguridad Bancaria Zona Sur

- Subcomisario especialista en seguridad bancaria.

4.2.4.1 Categorías de análisis

El objetivo de la realización de estas entrevistas consistió en conocer las opiniones y experiencias de los actores que poseen más conocimientos sobre la problemática, a partir de indagar sobre las siguientes categorías:

- *Conocimiento sobre ciberdelitos económicos en entidades bancarias*. En esta categoría se busca identificar el conocimiento que los especialistas tienen sobre los ciberdelitos económicos que se produce en las entidades bancarias.
- *Ciberdelitos económicos más frecuentes en la provincia de Mendoza*. Se refiere a los ciberdelitos económicos que se han dado con mayor frecuencia.
- *Factores de riesgo en el ámbito bancario*. En esta categoría se busca conocer cuáles son los factores de riesgo que se presentan en el ámbito bancario, en relación a la protección que los bancos poseen para proteger a sus clientes del ataque de ciberdelincuentes.
- *Actuación policial y/o bancaria en esclarecimiento de hechos delictivos de ciberdelitos*. Esta categoría indaga sobre las acciones policiales que se llevan a cabo en materia de ciberdelitos económicos en el ámbito bancario.
- *Procedimientos para el esclarecimiento*. Se investiga sobre cuáles son los procedimientos que cada uno de los actores lleva a cabo a fin de esclarecer los hechos de ciberdelitos económicos.
- *Medidas de seguridad para evitar el ciberdelito*. En esta categoría se busca conocer cuáles son las medidas de seguridad vigentes tanto en los sistemas de seguridad policiales, como en los sistemas de seguridad bancarios.
- *Medidas de protección de usuarios y sus datos*. Se busca identificar si los bancos poseen suficientes cortafuegos, programas y demás medidas de protección para los usuarios, como también si se protegen los datos privados de los clientes.

Categorías emergentes

- *Preparación previa de los bancos para enfrentar la virtualidad*. Se indaga respecto a si los bancos cuentan con suficientes medidas preventivas para

afrontar los cambios que se produjeron como consecuencia del incremento de la utilización de la banca virtual.

- *Admisión de la vulnerabilidad bancaria/información de ciberdelitos*. En esta categoría se busca conocer si los bancos admiten que existe una vulnerabilidad bancaria.
- *Acciones preventivas desde los bancos*. Se identifican las medidas preventivas que los bancos aplican a fin de evitar la comisión de hechos delictivos del cibercrimen.
- *Soluciones a los usuarios*. Esta categoría se refiere a las soluciones que los bancos, dan a la problemática de los usuarios cuando estos han sido estafados mediante la modalidad de ciberdelito económico.

4.2.4.1.1 Técnicas de conversación: entrevista semiestructurada

Los datos recolectados de la guía de entrevista se organizaron en función de las categorías de análisis propuestas y aquellas que emergieron de las respuestas obtenidas. Se van a realizar las entrevistas a:

- Personal bancario
- Jefes de seguridad de entidades bancarias
- Asesor de seguridad bancaria
- Analista de seguridad del BCRA
- Subcomisario analista de sistemas y diplomado en Cibercrimen y Evidencia Digital
- Subcomisario a cargo de la Delegación del Departamento de Seguridad Bancaria Zona Sur
- Subcomisario especialista en seguridad bancaria

4.2.4.1.2 Guía de entrevista

Se aplicó la guía de entrevista a ocho personas que participan, desde diferentes instituciones, cargos y funciones, en la seguridad bancaria. La misma se encuentra en el Anexo I (pág. 98 a 123).

4.2.4.1.2.1 Primera categoría: conocimiento sobre ciberdelitos en entidades bancarias

Todos los entrevistados identifican los ciberdelitos que se cometen en las entidades bancarias, mencionado el phishing, smishing, skimming y spoofing.

Los mismos "se encuentran descriptos por la Ley 26388/2008, en los que se mencionan aquellos delitos que son cometidos, en primer lugar, contra un medio informático, en segundo lugar, utilizando un medio informático para su comisión y en tercer lugar contra la información que el medio informático contiene".

"En el primer caso, el objetivo sería realizar acciones que perjudiquen de alguna manera el medio, lo deje fuera de servicio o deteriore su funcionamiento, como por ejemplo, ataques de denegación de servicio, exigiendo a cambio de la liberación del servicio el pago de algún bien económico. En este caso las entidades bancarias invierten gran cantidad de recursos para evitar ser víctimas de este tipo de delitos por lo que difícilmente puedan ser llevados a cabo, además, de ser cometidos, ninguna entidad dará a conocer esa situación debido a que resultaría contraproducente para su confiabilidad".

"El más común es este segundo caso, donde las personas aprovechándose de la poca experiencia en los sistemas informáticos, sobre todo de adultos mayores, y de algunas debilidades de en los procesos de adquisición y validación de identidad, utilizan llamados engañosos donde se hacen pasar por diferentes situaciones, como el secuestro de algún familiar, o por parte del círculo de confianza, haciéndose pasar por algún agente de la entidad bancaria le solicitan las claves y de acceso y diferente información que le permite al victimario apropiarse de los valores que se encuentran en las cuentas bancarias y contraer préstamos a nombre del damnificado por medios tecnológicos".

"Y finalmente, software que tiene el fin de engañar a las víctimas como el phishing o ramsonware que produce el secuestro de la información como medio para dejarla de alguna manera secuestrada o inaccesible".

4.2.4.1.2.2 Segunda categoría: ciberdelitos más frecuentes

Los entrevistados, consideran que el ciberdelito más frecuente que se ha producido durante la pandemia de Covid-19, es el phishing, mediante la modalidad de llamados telefónicos, haciéndose pasar por diferentes instituciones, como por ejemplo "ANSES donde le iban a otorgar los beneficios de los $10.000, lograban que la gente fuera a un cajero automático y de allí obtenían los números secretos y claves de acceso. Lo más común era que se hiciera cambiar las contraseñas y así poder ingresar a sus cuentas y producían el vaciamiento de las mismas".

Otra modalidad del phishing se logra a través de la comunicación por e-mail, con logos bancarios y apariencias que asemejan un mail oficial. En esta modalidad ofrecen un préstamo al que el usuario puede acceder si ingresa a un link, donde obtienen los datos personales de las cuentas bancarias, y de esta forma obtienen el dinero de las cuentas reales.

Los llamados telefónicos ofreciendo el acceso a la ayuda económica, donde se le solicitaba a la víctima que concurrieran al "cajero automático y los iban guiando y así accedían a su cuenta y sacaban el dinero que tenían".

El skimming, el cual ha disminuido con la pandemia. Se trata de "la clonación de tarjetas, a través de un lector de banda magnética en la boquilla del cajero y de un dispositivo de grabación en la parte superior para obtener la clave alfanumérica…" "El skimming fue pionero en la provincia ya que tuvimos varios hechos denunciados por las entidades bancarios y clientes. La modalidad está basada en adquirir datos personales para finalmente clonar la tarjeta y luego hacer usufructúo de la misma".

El smishing, el cual "va dirigido a usuarios de telefonía móvil ya que es una variante del Phishing, pero este se realiza mediante mensaje de texto".

"El spoofing se manifiesta a través de la falsificación de datos en una comunicación. Por ejemplo, se hacen pasar por una entidad distinta (suplantación de identidad) enviando

un correo electrónico para así acceder a datos personales o confidenciales, de forma maliciosa".

En menor medida la colocación de dispositivos físicos conocidos como "pescadores".

4.2.4.1.2.3 Tercera categoría: factores de riesgo en el ámbito bancario

Los factores que se enumeran a continuación, son los que han identificado como los de mayor riesgo:

- "La gente cree que le llaman del banco y le pasan los datos que requieren los ciberdelitos".
- "durante la pandemia la gente necesitó dinero y ya no podían concurrir al banco como era habitual, muchos de nuestros clientes no estaban acostumbrados a usar la banca on-line, los delincuentes aprovecharon eso y la necesidad e ignorancia de la gente".
- "Al informarle a la gente que no debía concurrir al banco y que debían llamar por teléfono, los ciberdelicuentes, haciéndose pasar por el personal nuestro, lograban convencer a la gente y estos aportaban los datos que le pedían".
- La gente creía que había sido seleccionado para el cobro de una ayuda del gobierno
- Desconocimiento del uso de tecnología.
- "El problema surge cuando la extracción no se realiza en un cajero, como por ejemplo estaciones de servicios, supermercados, farmacias, en aquellos locales no bancarizados".
- "Los adultos mayores que por lo general asisten solos a los cajeros automáticos o solicitando ayuda de un tercero".
- Desconocimiento de las personas respecto a la preservación de su información confidencial.
- Complicado para las personas que están en poco contacto con la tecnología.

- Falta de atención de los usuarios al momento de operar o interactuar con los presuntos operadores de bancos, vendedores, etc.
- "…poca inversión, desde el punto de vista bancario, en evolucionar para evitar este tipo de delitos".
- "Desconocimiento o exceso de confianza que existe en el común del púbico…"
- "…seguridad y accesibilidad, son características casi excluyentes, por lo tanto mientras más fácil es acceder a un servicio, más fácil podría ser vulnerado y en contraposición mientras más seguro, más engorroso será su acceso. Desde esta perspectiva una entidad complejiza sus sistemas de seguridad cuanto más hechos de inseguridad ocurran, ya que no invertirá recursos en mejoras de sistemas que funcionan de manera correcta o no generan inconvenientes a los clientes".

4.2.4.1.2.4 Cuarta categoría: actuación policial y/o bancaria en el esclarecimiento de hechos delictivos de ciberdelitos

El personal bancario solo se limita a atender los reclamos de "aquellas personas a las cuales han sido afectadas por este tipo de delito, pero intervenir directamente no".

El personal policial de seguridad, ha participado de algunos eventos como el skimming, "donde habían colocado dispositivos para clonar tarjetas de débito en una de nuestras sucursales, donde fuimos advertidos por monitoreo del banco y al llegar a la sucursal estaban los clonadores colocados en uno de los cajeros automáticos y llamamos a la policía pero eso fue en el año 2019".

En los hechos de clonadores de tarjetas, que es una modalidad que ha dejado de prosperar, si se llama al personal de seguridad. Pero "a lo que respecta a ciberdelito no hay participación física, por así decirlo, de personal del banco". En la modalidad del skimming han participado en eventos del Banco Patagonia, Banco Macro en San Rafael, Banco Macro de calle San Martín y Alem de Ciudad, entre otros. En estas oportunidades han secuestrado material necesario para la clonación de tarjetas de crédito y débito.

Han participado además, en el caso del Banco Nación de Villa Nueva, Guaymallén, en una investigación que ha demandado "más de dos meses para poder establecer que el

autor de los hechos (le vaciaban las cuentas bancarias de abuelos y jubilados) sin que quedaran rastros de las maniobras. La investigación, permitió conocer que de forma remota y desde otro punto del país, personas idóneas en informáticas, accedían a los archivos bancarios y extraían dinero o realizaban compras por internet".

4.2.4.1.2.5 Quinta categoría: procedimientos para el esclarecimiento

El personal bancario sostiene que se debe realizar la denuncia en la fiscalía. Luego, en caso de que los fiscales o jueces lo requieran, se entrega, oficio judicial mediante, la información correspondiente a los números de cuentas a las que ha sido transferido el dinero para seguir su camino, a nombre de quien estaban las mismas, a que sucursal bancaria fue transferido, en qué provincia fue retirado o se llevó a cabo la operación de extracción, y todos los datos que consideren necesarios.

El personal de seguridad bancaria sostiene que son diferentes procedimientos. En el caso que el cliente, "en forma engañosa aporta sus datos y se comete el delito, no hay sistema de seguridad que ayude a identificar a la persona, si bien se determina el número de cuenta a la que fue trasferido el dinero o si es una billetera virtual. Pero si alguien concurre a una sucursal a retirar el dinero a través del CCTV (Circuito Cerrado de Televisión) se pueden aportar imágenes que se hacen circular en todo el país y en caso de observarlo nuevamente se alerta a la policía".

Esta es una tarea muy compleja, cuando están bien organizados ya que son difíciles de rastrear. Para el procedimiento sostienen que "No hay una receta única, sino que debe ser dinámica y adaptarse a la modalidad detectada, ya que la tecnología les permite rápidamente borrar sus huellas, las distancias le brindan anonimato y privacidad por lo cual se precisa de personas con alta capacidades y conocimiento para ejecutar el rastreo antes de que el delincuente se dé cuenta o mute la modalidad".

El experto en ciberdelincuencia y cibercrimen y evidencia digital, sostiene que se deben seguir los siguientes pasos:

"Resguardar la información existente en los medios informáticos, mediante actas de Notariales en los procesos civiles y mediante orden de juez competente en el caso de causas

penales. Puede darse también la situación que la víctima se presente de manera espontánea en una dependencia policial (que pueda realizar la medida) en cuyo caso se dará aviso a la autoridad judicial competente"

- "Una vez realizada el resguardo o extracción de la información; se procederá con la orden de la autoridad competente a realizar el análisis de los datos, con el objeto de determinar el origen y la identificación del autor de las comunicaciones y/o acciones realizadas para la comisión del hecho investigado".
- "Se le solicita por medio de oficio de la autoridad judicial competente, a las empresas prestadoras de los servicios analizados (servicio de e-mail, de Internet, de telefonía, de redes sociales, de televisión, o cualquier otro similar) que aporte los datos de registros que se vinculan al hecho a fin de validar o refutar los elementos encontrados en la extracción y análisis anterior".
- "Tareas de Explotación de fuentes abiertas de información y verificación de los datos obtenidos en el terreno (con la colaboración de las Unidades Investigativas de jurisdicción) a fin de verificar domicilios, personas y vehículos".

4.2.4.1.2.6 Sexta categoría: medidas de seguridad para evitar el ciberdelito

- Medidas de seguridad para evitar el ciberdelito.
- Se trabaja en forma permanente para evitar estos casos.
- Se coloca la cartelería preventiva en las sucursales y cajeros automáticos, informando que "desde el banco no le van a solicitar cambios de claves ni contraseñas, no aporte sus datos personales, evite se víctima de una estafa virtual y todo tipo de información preventiva".
- "…enviar e-mail a todos los clientes del banco detallando cuales son los links falsos, cuales son los correos oficiales del banco y toda información preventiva".
- "…nuestra asociación bancaria limitó los montos de trasferencias de dinero de una cuenta a otra, siempre y cuando no fuera de la misma persona, o pagos habituales de servicios en caso de las empresas, aunque el BCRA no nos autorizaba a restringir este tipo de operaciones todavía".

- "…los préstamos pre adjudicados, ya no son de forma inmediata, hay una demora de 48 horas y el cliente deberá certificar en ese lapso que está seguro de la operación realizada ya sea en forma personal o por e-mail al banco.
- "Capacitar al personal de la división informática intensificando los cortafuegos para evitar un hackeo a nuestro sistema informático".
- Colocación de cartelería en todos los cajeros automáticos.
- Créditos on line requieren de un tiempo de espera de 48 horas para acceder a los mismos, y se incrementan las notificaciones al cliente.
- Se les solicita a los clientes que concurran a la sucursal.
- "Desde ABA (Asociación de Bancos de Argentina) también solicitaron al BCRA un mayor control en los retiros o circulación de dinero en forma virtual hacia las billeteras electrónicas como Mercado Pago, Ualá o Naranja X entre otras, cuando la suma de dinero es considerable".
- "En la provincia de Mendoza, afortunadamente, el sistema de seguridad bancaria, es altamente efectivo. Si tenemos en cuenta la cantidad de bocas de expendio de dinero (cajeros automáticos y entidades bancarias, en comparación con otras latitudes".
- "…el banco tampoco va a invertir en seguridad sobre un sistema que funciona sin problemas, ya que no podes complicarle aún más a la gente el uso de la banca on-line cuando el 80% de las funciones bancarias desde marzo del año paso se hace en forma remota, incluso los empleados bancarias trabajan en forma remota, entonces te llaman a cualquier hora y las personas accedían".
- Utilización de seguridad biométrica como huella dactilar, facial, etc. Se han incrementado los sistemas de control como doble validación alfanumérica, diferencia de pin de ingreso, pin de compra, y pin de extracción de efectivo. "He notado un gran incremento de los sistemas de control y validación de las operaciones".

4.2.4.1.2.7 Séptima categoría: medidas de protección de usuarios y sus datos

- Recomendaciones a usuarios que no pasen datos por coreos, WhatsApp o cualquier otro medio.

- Las tarjetas de débito con chip, más la cinta magnética
- Cajeros inteligentes con huella dactilar
- Comunicación "A" 6894, el BCRA emplazó a los bancos a que cambien sus equipos de modo teclado al uso de huella dactilar.
- Campañas activas de información.
- Pin de acceso al sistema
- Sistemas biométricos de validación.
- Limitación de montos máximos de transferencia.
- Sistema de validación de operaciones por mail o vía telefónica.

4.2.4.1.2.8.1 Categorías emergentes

4.2.4.1.2.8.2 Primera categoría emergente: preparación previa de los bancos para enfrentar la virtualidad

Personal bancario sostiene que "nosotros no estábamos preparados para la virtualidad bancaria, pero fuimos obligados por el Banco Central de la República Argentina a trabajar de ésta forma, sin tener los cortafuegos necesarios en nuestros sistemas informáticos, independientemente de que nunca fuimos hackeados y en todos los casos la gente aportaba los datos que necesitaban para ingresar a sus cuentas por ende a nuestro sistema".

"…recibimos capacitaciones y se nos ordenó colocar cartelería informativa en todos los ATM y sucursales bancarias alertando a los usuarios de que no deben realizar tales maniobras engañosas ya que el banco nunca les va a solicitar ese tipo de información, por algo es secreta".

"…si tenemos en cuenta que el ciberdelito se disparó durante la pandemia, te puedo decir que el BCRA nos ordenó de la noche a la mañana trabajar on-line y no teníamos los soportes necesarios de seguridad para hacerlo".

4.2.4.1.2.8.3 Segunda categoría emergente: admisión de la vulnerabilidad bancaria/información de ciberdelito

Los bancos ocultan la información. "… no hay campañas en los medios masivos de comunicación porque ninguna entidad bancaria va a admitir que sus clientes son vulnerables, ya que es muy mala publicidad".

"…en dos oportunidades sacamos este tipo de dispositivos de nuestras sucursales (dispositivos destinados al skimming) y nunca llamamos a la policía ya que desde Buenos Aires no ordenan no hacerlo por la mala publicidad".

Durante un tiempo los bancos han ofrecido los créditos sin tomar las medidas necesarias, lo que llevó a que se produjeran muchos ciberdelitos, que, aunque denunciados no fueron publicados por los bancos: "…creo necesario recalcar, que durante un buen periodo de tiempo, los bancos brindaron una opción de préstamos pre aprobados que podían ser tramitados por el titular de la cuenta bancaria o por personas que se apropian de una identidad o que de algún modo manipulan a la víctima para realizar esta tarea, incrementándose los hechos de este modus operandi", sostienen expertos en seguridad bancaria.

4.2.4.1.2.8.4 Tercera categoría emergente: soluciones a los usuarios

"En la mayoría de los casos el banco se hace cargo a través de los seguros que tenemos contratados, pero han aumentado tanto que se empezó a estudiar cada caso en específico, pero por temor a mala publicidad, como te decía recién, en la mayoría de los casos se responde en forma inmediata".

"…depende del tipo de delito, por ejemplo si el cliente aportó las claves secretas, a través de la sección Investigación de Fraude se decide si es responsabilidad del banco que haya sido víctima o si es responsabilidad del cliente, ahora en la mayoría de los casos con el fin de evitar una mala publicidad el banco va a responder. Te pongo como ejemplo lo que pasó en la sucursal del Banco Nación de Guaymallén, las compras fueron on-line con el uso de tarjetas de crédito, y tarjetas de débitos de los jubilados, en esos casos el banco no

responde, pero como salió en televisión, el banco ahí nomás salió a decir que se harían cargo de la devolución del dinero. Si la estafa es por Mercado Libre o Whatsapp donde se ve involucrada la cuenta bancaria, el banco no tiene que responder ya que no fue un hackeo a su sistema sino un error del usuario en la transacción económica que realizó".

4.2.5 Análisis e interpretación de los resultados

A partir de los datos obtenidos se puede poner en evidencia que el ciberdelito se encuentra en pleno crecimiento. Es destacable el aumento importante que ha tenido en el período de estudio en referencia, especialmente, al fraude y estafa bancaria.

Si bien no se cuenta con datos estadísticos registrados de la provincia, los que se han presentado resultan clarificantes de la situación a nivel país y el crecimiento que esta modalidad tuvo durante el año 2020 y el primer semestre del 2021, posicionando a la provincia de Mendoza en el tercer lugar dentro del país detrás de Buenos Aires y CABA.

El gráfico Nº3 (pág. 51) elaborado por la AALCC, muestra un elevado y rápido crecimiento del ciberdelito en sus diferentes modalidades. El *skimming* es ahora un viejo delito cibernético que ha dado lugar a nuevos modelos delictivos que, no solo obligan a tomar otras medidas de seguridad bancaria, sino que además, llevan al personal policial y miembros del derecho, a una constante actualización de las nuevas formas delictivas como el *phishing* o el *spoofing*, generando que las instituciones elaboren más respuestas, como el caso del BCRA que ha debido elaborar circulares cada vez más específicas.

La situación de pandemia, con su aparición repentina y rápida propagación, obligó a todas las instituciones de los países, a tomar medidas extraordinarias, muchas de las cuales no habían sido planificadas. Para enfrentarlas se debieron adoptar nuevas formas de comunicación, siendo internet el campo de mayor interacción social. De esta forma, las instituciones bancarias debieron expandir su atención virtual, y los usuarios, muchos de ellos resistentes a la atención virtual, debieron adaptarse. Nadie estaba preparado para esto, ni para la enfermedad ni para la atención "nosotros no estábamos preparados "pero fuimos obligados por el Banco Central de la República Argentina a trabajar de ésta forma, sin tener los cortafuegos necesarios en nuestros sistemas informáticos, independientemente de que

nunca fuimos hackeados y en todos los casos la gente aportaba los datos que necesitaban para ingresar a sus cuentas por ende a nuestro sistema". La gente aportaba los datos no solo al personal bancario, sino que muchas veces lo hicieron con delincuentes, que aprovechando esta coyuntura, rápidamente idearon nuevas formas de intervenir. Aprovechando además,, las necesidades económicas que la sociedad estaba atravesando producto del confinamiento, sobre todo los más vulnerables "Al informarle a la gente que no debía concurrir al banco y que debían llamar por teléfono, los ciberdelicuentes, haciéndose pasar por el personal nuestro, lograban convencer a la gente y estos aportaban los datos que le pedían". "La gente creía que había sido seleccionado para el cobro de una ayuda del gobierno…"

Frente a esta nueva situación los bancos han incrementado sus medidas de seguridad a través de reforzar el contacto con las redes sociales, sin embargo, esto puede ser contraproducente ya que, como se ha observado, las redes sociales han sido un terreno para el ciberdelito y lo continúan siendo. Observando el gráfico Nº7, estos espacios cibernéticos de interacción, representan un 10% de la modalidad más frecuente de los delitos de fraude y estafa bancaria. Esto es así ya que el desconocimiento en el uso de la tecnología y la confianza de las personas en las transacciones, los ha llevado a entregar información confidencial la cual, aprovechada por el ciberdelincuente, es utilizada para sus fines espurios.

La evolución del ciberdelito, es un punto a tener en cuenta en estas intervenciones, ya que como se ha observado, la creación visual de e-mail enviado a los usuarios, con falsas promesas o informando que las cuentas serán bloqueadas, tienen una presentación similar a las enviadas a clientes bancarios. Esto hace que la víctima confíe en la presentación, e ingrese al link que adjunta ingresando a una página similar a la bancaria, con iguales características pero que no pertenece al banco. Esto demuestra la capacidad organizativa que tienen los ciberdelincuentes para obtener su cometido.

Así como han sostenido los especialistas, cuando se produce un ciberdelito en el que el usuario brinda sus datos, bajo un engaño, "… no hay sistema de seguridad que ayude a identificar a la persona, si bien se determina el número de cuenta a la que fue trasferido el dinero o si es una billetera virtual. Pero si alguien concurre a una sucursal a retirar el dinero

a través del CCTV (Circuito Cerrado de Televisión) se pueden aportar imágenes que se hacen circular en todo el país y en caso de observarlo nuevamente se alerta a la policía". Esta compleja tarea, cuando están bien organizados, hace que sea difícil de rastrear, lo que lleva a que las actividades que desarrollan los expertos en seguridad bancaria o en ciberdelito, deban adoptar medidas estratégicas de carácter "…dinámica y adaptarse a la modalidad detectada, ya que la tecnología les permite rápidamente borrar sus huellas, las distancias le brindan anonimato y privacidad por lo cual se precisa de personas con alta capacidades y conocimiento para ejecutar el rastreo antes de que el delincuente se dé cuenta o mute la modalidad".

Las medidas preventivas que los bancos adoptaron, al igual que el BCRA, incluyen brindar información al usuario mediante e-mail informativos, comunicaciones por WhatsApp, información en cajeros automáticos, disminución de los montos de transferencia de dinero, alargar el tiempo de obtención de los préstamos pre adjudicados los que ya no son de transferencia inmediata, sino que se presenta una demora de 48 horas, induciendo al cliente a certificar el pedido del mismo, incluso haciendo que se dirija a la sucursal. Además, se ha capacitado al "personal de la división informática intensificando los cortafuegos para evitar un hackeo a nuestro sistema informático". Se ha solicitado "al BCRA un mayor control en los retiros y circulación de dinero en forma virtual hacia las billeteras electrónicas como Mercado Pago, Ualá o Naranja X entre otras, cuando la suma de dinero es considerable". En este punto es importante destacar que esta modalidad que llevó a la ocurrencia de la estafa a miles de jubilado y clientes en el Banco Nación de Guaymallén, Mendoza, la investigación policial es fundamental a fin de poder identificar el recorrido del dinero. A estas medidas de seguridad se está incorporando la utilización de seguridad biométrica y la doble validación alfanumérica, a fin de evitar, o al menos disminuir, la ocurrencia de ciberdelitos.

Los bancos, como entidades financieras que reciben sus clientes en función de su trayectoria y confiabilidad, tampoco muestran su información real en referencia a los ciberdelitos que impliquen la violación de su seguridad interna, "… no hay campañas en los medios masivos de comunicación porque ninguna entidad bancaria va a admitir que sus clientes son vulnerables, ya que es muy mala publicidad". El hecho de haber otorgado

créditos sin medidas de seguridad más fuertes hizo que muchos ciberdelincuentes tomaran los préstamos bancarios a nombre de sus titulares, y se quedaran con este dinero. Sin embargo, poco se ha informado de estos hechos delictivos que muy probablemente, como ha sostenido otro experto en seguridad, se solucionan con los seguros del banco o el mismo se hace cargo.

La mayor dificultad radica en aquellos hechos en los cuales, mediante mentiras, los ciberdelincuentes obtienen los datos de los usuarios aportando claves secretas. "…a través de la sección Investigación de Fraude se decide si es responsabilidad del banco que haya sido víctima o si es responsabilidad del cliente, ahora en la mayoría de los casos con el fin de evitar una mala publicidad el banco va a responder. Te pongo como ejemplo lo que pasó en la sucursal del Banco Nación de Guaymallén, las compras fueron on-line con el uso de tarjetas de crédito, y tarjetas de débitos de los jubilados, en esos casos el banco no responde, pero como salió en televisión, el banco ahí nomás salió a decir que se harían cargo de la devolución del dinero. Si la estafa es por Mercado Libre o Whatsapp donde se ve involucrada la cuenta bancaria, el banco no tiene que responder ya que no fue un hackeo a su sistema sino un error del usuario en la transacción económica que realizó".

El conocimiento de expertos, como también del personal bancario, demuestra que las estadísticas que se han presentado se corresponden con las vivencias y experiencias de los entrevistados ya que manifiestan claramente, las modalidades de *phishing* como la más frecuente, en sus dos versiones: tarjetas de crédito y débito, y/o transacciones bancarias.

Los profesionales de la seguridad bancaria, al igual que los especialistas en cibercrimen, coinciden en que se deben reforzar y ampliar las medidas de seguridad que se aplican en el sistema bancario, sin embargo, esto debe ir acompañado de estrategias que complejicen la utilización del servicio.

A continuación, se presentan las conclusiones a las que se ha arribado en la presente investigación.

Conclusiones

El presente trabajo de investigación ha partido de analizar el impacto del uso masivo de la banca on line sobre el ciberdelito en el sistema bancario de la provincia de Mendoza en el contexto de pandemia, durante el período 2020 y 2021. Para alcanzar este objetivo se partió de explicar que el sistema bancario ha debido enfrentar cambios bruscos a partir de marzo del año 2020, dejando de lado la atención presencial, para pasar casi en forma exclusiva, a una atención virtual. Esto llevo a incrementar los servicios de banca electrónica y la creación de aplicaciones específicas bancarias, que permitieron a los usuarios realizar todas sus transacciones desde sus hogares a través de computadoras, tablets y/o smartphone.

En este nuevo escenario, el crecimiento del ciberdelito ha desbordado las capacidades de control y las medidas de seguridad que se habían tomado con anterioridad, "el 62% de las entidades (bancarias)…tuvieron dificultades con la entrega de productos, la gestión de consultas y reclamos, la gestión de claves y la gestión de cheques" (PwC, 2021). El aumento del uso del *home banking*, y las aplicaciones propias de los bancos llevo a perfeccionar el capital humano, fomentando el trabajo remoto, con el cual se ha presentado continuidad de atención. Esto llevó a una modificación del cibercrimen en su modus operandi a fin de poder obtener beneficios de esta nueva normalidad en la que nos encontramos en la actualidad.

Frente a esto, se realizaron modificaciones en el sistema bancario, las cuales fueron establecidas por el BCRA, buscando garantizar el funcionamiento de los cajeros automáticos, en primer término, pero además, estableciendo turnos de atención, y posteriormente incrementando algunas medidas de seguridad. De esta forma se brindó una rápida respuesta a los usuarios, sobre todo el sector de jubilados quienes debieron modificar sus formas de actuación y relación con el sistema bancario, aprendiendo a utilizar la banca digital. Como sostiene Valleboni (2021), "la pandemia fue implacable: aceleró todos los planes que las entidades tenían para el próximo lustro", digitalizando a los clientes y llevando a los bancos a generar innovaciones en tiempo récord, sumado a una rápida adaptación de los usuarios. Además, debieron responder con ayudas financieras excepcionales.

Las consecuencias sobre la seguridad del sistema operativo de los bancos han sido notables, ya que el incremento de los ciberdelitos ha sido muy elevado, pero no bajo la misma modalidad que ocurrían anteriormente, sino que adoptaron nuevas estrategias para captar víctimas, y lamentablemente con mucho éxito, ya que en el 2020 se produjo un 140% más de denuncias, en comparación con los tres años anteriores en el país, sostiene Azzolin. En este punto, los datos aportados por la AALCC, demuestran que en el año 2019 se produjeron 581mil llamados, consultas y denuncias por fraude y estafa, mientras que en el año 2021 esta cifra ha aumentado en un 403% como se ha demostrado en el gráfico Nº5. Teniendo en cuenta que muchas de estas consultas no han llegado a constituirse en denuncias, de todos modos, no son datos menores.

Como se ha expresado en el capítulo I del presente trabajo, y se ha podido corroborar en los datos obtenidos, la modalidad delictiva de contacto preferida ha sido el WhatsApp y el correo electrónico, medios mediante los cuales obtienen la información personal del usuario. Sin embargo, en este punto, es necesario reflexionar sobre la importancia de realizar la denuncia, ya que esto contribuye a mejorar las intervenciones a fin de prevenir la ocurrencia de estos hechos delictivos.

La atención *on line* del sistema bancario ha debido incrementarse en este período, tal como ha mencionado Valleboni (2021), adoptando medidas extraordinarias que permitieran brindar mejores y más servicios. En este punto es importante destacar lo que han mencionado los expertos consultados, quienes sostienen que las acciones que se llevan a cabo en los bancos, deben, además,, contemplar la población más vulnerable que se constituye en los mayores factores de riesgo como son la población de jubilados, quienes no siempre están adaptados a la tecnología. La aparición de aplicaciones móviles, ha facilitado la comprensión del movimiento de la banca digital, sin embargo, también es un campo potable para el cibercrimen. Las mismas, al utilizar la privacidad personal y del equipo móvil, mediante conectores como las API, las cuales permiten la interconexión con otros servidores. Muchas veces en estos puntos las aplicaciones son vulneradas y se pueden obtener los datos privados para fines delictivos. Los clientes, muchas veces vulnerados, se encuentran amparados en el nuevo Código Civil y Comercial, el que dedica a los contratos bancarios un conjunto de normativas que les garantiza el goce de sus derechos, y lleva a los

bancos a afrontar los daños que puedan devenir de estas fallas en sus aplicaciones, páginas web e incluso en los cajeros automáticos.

Como se ha observado, el ciberdelito adquiere diferentes formas de expresión, las cuales coinciden con las mencionadas por los expertos en sus diferentes intervenciones, y partiendo de sus experiencias, algunas de estas formas son difíciles de rastrear ya que los hackers cada vez perfeccionan más su forma delictual.

A fin de dar seguridad a la población, las medidas adoptadas por el BCRA se basaron en la elaboración de un conjunto de disposiciones que debieron ser implementadas por las entidades bancarias, a fin de evitar nuevas sanciones como las multas impuestas al Banco Santander y el BBVA, por violar la ley de defensa al consumidor.

Si bien el plexo normativo de Argentina es extenso y se basa fundamentalmente en el artículo 42 de nuestra Constitución Nacional, los cambios vertiginosos, obligan a las instituciones de control, como el BCRA, a adoptar medidas de seguridad expresadas en nuevas disposiciones. Entre las múltiples que se llevaron a cabo, se destacan aquellas que buscaron complementar el cumplimiento de la ley de defensa al consumidor y las normas jurídicas que regulan el uso de tecnologías como medios de comisión de delitos, los cuales ya se encuentran previstos en el Código, en referencia a los delitos de estafa y fraude, pero debiendo incorporar en la normativa los términos de “documento”, “firma”, “suscripción”, “firma digital”, a fin de dar respuesta a las nuevas modalidades.

El Estado, incorporó la Resolución Nº 139/3030 de la Secretaría de Comercio Interior de la Nación para acentuar la prevención del ciberdelito y proteger a usuarios y consumidores, lo que se reforzó mediante la creación de diferentes comunicaciones del BCRA, las cuales estuvieron destinadas específicamente a definir las formas de atención al público y fijar todas las medidas adecuadas para incrementar la prevención de situaciones de ciberdelito.

Tanto la revisión bibliográfica como la investigación de campo realizada, han demostrado que el Estado argentino ha articulado medidas de prevención para la seguridad bancaria, instando a las instituciones privadas a llevar a cabo un conjunto de acciones que protejan a sus usuarios, especialmente a aquellos considerados como más vulnerables. En

este punto es necesario aclarar que, si bien muchas de estas medidas fueron vertiginosas y no permitieron una preparación previa, es indiscutible que la situación de carácter extraordinario que se vivió a partir de la aparición de la pandemia, no solo afectó a los bancos locales, sino que a nivel mundial todos fueron afectados en mayor o menor medida.

En referencia a las entidades financieras, es destacable mencionar que la seguridad bancaria siembre ha sido un tema de discusión en todos los ámbitos, ya que en muchos aspectos puede ser vulnerable y alterada por los delincuentes. Sin importar al año al que hagamos referencia, es necesario, en todo momento que, ante la oferta de un servicio, los bancos tengan en cuenta las condiciones de riesgo y vulnerabilidad que estos deben respetar. El hecho de no comunicar los problemas de vulnerabilidad que puedan aparecer, no debería ser ocultado en función de la mala publicidad, sino que, por el contrario, debe ser observado a fin de evitar que se produzcan más estados de vulnerabilidad.

Por último, es importante destacar el trabajo de inteligencia que desarrollan las fuerzas de seguridad ya que, gracias al mismo, logran encontrar y describir los caminos que los delincuentes siguen a fin de dar con los botines que persiguen. Pero además, se considera de carácter imprescindible que se lleven adelante campañas masivas de información a fin de prevenir a la comunidad en su conjunto, sobre las acciones delictivas que se realizan en materia de cibercrimen, y cuáles son las medidas más importantes que deben tener en cuenta para realizar transacciones digitales. Consideramos que las mismas no son suficientes si solo se llevan adelante por los bancos.

Se considera de vital importancia obtener datos fehacientes y que correspondan con la realidad de la provincia en su particularidad, ya que con esto se podrán defender las medidas preventivas necesarias para disminuir la ocurrencia de este tipo de delitos.

En síntesis, la hipótesis de la cual hemos partido para la presente investigación consistente en afirmar que “El uso masivo de la banca online en el contexto de pandemia, durante el período 2020 y 2021, en la provincia de Mendoza, evidenció la vulnerabilidad del Sistema de Seguridad Bancario frente al ciberdelito económico”, ha quedado comprobada. Esta conclusión se desprende de lo que hemos observado a partir de los datos estadísticos obtenidos, que demuestran un incremento en esta modalidad delictiva, como

también en la percepción de los entrevistados, quienes ponen de manifiesto que las condiciones de seguridad bancaria mostraron niveles de vulnerabilidad, frente a la inteligencia del cibercrimen económico.

La comprobación de esta hipótesis, puso de manifiesto que las políticas públicas que se llevan adelante en el país y la provincia, en materia de Seguridad Bancaria, deben ser dinámicas, adaptándose en forma cotidiana a las nuevas modalidades delictivas que van surgiendo del cibercrimen, lo que evidencia, además, que no siempre se puede contar con programas estáticos en materia de Seguridad Pública, sino que estos deben evolucionar en forma constante.

Para finalizar con este análisis, consideramos que es importante destacar que la provincia de Mendoza, ha solicitado al Banco Central de la República Argentina, independencia en el análisis de riesgo de las instituciones bancarias, teniendo en cuenta el contexto particular de la provincia. Esto permitiría emitir nuestras propias leyes en relación a la Seguridad Bancaria, toda vez que cada región y cada provincia, presentan sus propias problemáticas que, si bien pueden ser comunes al resto del país, cada lugar tiene la particularidad de su idiosincrasia y el contexto en el cual, las acciones, suceden. Un antecedente relevante de esta experiencia, se encuentra reflejado en CABA, gobierno que en la actualidad está comenzando a diseñar sus propias leyes en materia de seguridad bancaria.

Anexos

ANEXO I

MODELO DE LA GUÍA DE ENTREVISTA

Edad

Cargo que ocupa

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

2. ¿Podría numerar cuáles son los más frecuentes?

3. ¿Podría decirnos cuales con los casos más frecuentes en los cuales han sido víctima los clientes del banco?

4. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

5. ¿Ha debido intervenir en algún hecho delictivo de este tipo?

6. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

7. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

8. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger a los usuarios y sus datos?

ANEXO II

CONTENIDO DE ENTREVISTAS REALIZADAS

ENTREVISTA Nº1

Edad 57 años

Personal bancario

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

Sí

2. ¿Podría numerar cuales son los más frecuentes?

Los más frecuentes son con las transferencias.

3. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

Que lamentablemente la gente cree que le llaman del Banco, y le pasan los datos que requieren los ciberdelitos

4. ¿Ha debido intervenir en algún hecho delictivo de este tipo?

En una oportunidad me quisieron estafar mediante el Instagram, creando una página adulterada.

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

En los casos de hechos delictivos, se debe realizar la denuncia en la fiscalía. Ellos son los encargados de seguir el /los casos.

6. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

En el caso de Seguridad Bancaria, se trabaja en forma permanente para evitar éstos casos.

7. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger a los usuarios y sus datos?

El Banco en forma permanente, recomienda a todos los usuarios que no pasen datos solicitados mediante correos, WhatsApp u otros medios. Y aclara cada Banco que nunca le va a pedir claves a los usuarios.

ENTREVISTA Nº2

Edad: 49 años

Personal bancario

En la actualidad, tengo a mi cargo el análisis de los casos de fraude electrónico o ciberdelito, en donde nuestros clientes hayan sido víctimas.

1. Entonces podemos decir que ¿conoce los ciberdelitos que se producen contra las entidades bancarias?

Si los conozco, es más, hemos recibido capacitaciones a los fines de poder ayudar a nuestros clientes a prevenir el robo de clave secretas, pin de seguridad, robo de identidad entre otros.

2. ¿Podría decirnos cuales con los casos más frecuentes en los cuales han sido víctima los clientes del banco?

Lo más común desde el comienzo de la pandemia, con el crecimiento de la bancas on-line, es lo que denominamos PHISHING, donde en muchos casos, con llamados telefónicos haciéndose pasar por personal del ANSES, donde le iban a otorgar los beneficios de los 10.000 pesos, lograban que la gente fuera a un cajero automático y de allí obtenían sus números secretos y claves de acceso, lo más común, era que les hicieran cambiar las contraseñas, y así poder ingresar a sus cuentas y producían el vaciamiento de las mismas.

Otros casos que aumentaron, fueron a través de un e-mail donde se le ofrecía un crédito bancario, y al ingresar estos obtenían los datos, se apoderaban del monto del crédito y lo hacían saltar de una cuenta a la otra, o a una billetera virtual como Mercado Pago o similar, y de allí extraían el dinero.

También con engaños logran obtener los números de la tarjeta de crédito realizando compras on-line.

Otros casos que he tenido que atender, se lo llama PHARMING, donde a través de una página web exactamente igual a la del banco, estos ingresan y cargan sus números claves y contraseñas y los ciberdelincuentes acceden a todo su home banking, y de allí, bueno, desde préstamos hasta extracciones de dinero.

3. Para Uds. ¿Cuáles cree que son los factores de riesgos más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?-

Si tenemos en cuenta que durante la pandemia la gente necesitaba dinero, y del día a la noche no podían concurrir al banco como era habitual, y muchos de nuestros clientes no estaban acostumbrados a usar la banca on-line, los delincuentes aprovecharon esta situación

y la necesidad e ignorancia de la gente. Si a esto le agregamos que se les decía que debían llamar por teléfono al banco, no concurrir, los ciberdelincuentes, haciéndose pasar por personal nuestro, lograban convencer a la gente y estos aportaban los datos que le pedían. Si me pedís una opinión personal, te digo que incluso nosotros no estábamos preparados para la virtualidad bancaria, pero fuimos obligados por el Banco Central de la República Argentina a trabajar de ésta forma, sin tener los cortafuegos necesarios en nuestros sistemas informáticos, independientemente de que nunca fuimos hakeados, y en todos los casos la gente aportaba los datos que necesitaban para ingresar a sus cuentas, y en consecuencia, a nuestro sistema.

Por otra parte, el ocultamiento de la información, que quiero decir con esto, no hay campañas publicitarias en los medios masivos de comunicación porque ninguna entidad bancaria va a admitir que sus clientes son vulnerables, ya que es muy mala publicidad. Si se alerta a los clientes a través de e-mail, cartelería en nuestras sucursales, incluso por whatsapp pero si un nuevo cliente ingresa a una página que parece oficial del banco como te decía anteriormente es presa de éstos ciberdelincuentes o lo contactan por cualquier otro medio.

4. Por tu trabajo dentro de la entidad bancaria ¿has debido intervenir en algún hecho delictivo de este tipo?

Mi trabajo consiste en atender los reclamos de aquellas personas que han sido afectadas por este tipo de delito, pero intervenir directamente no. Si recuerdo un caso de SKIMMING donde habían colocado dispositivos para clonar tarjetas de débito en una de nuestras sucursales, donde fuimos advertidos por monitoreo del banco, y al llegar a la sucursal estaban los clonadores colocados en uno de los cajeros automáticos y llamamos a la policía. Pero eso fue en el año 2019 antes de la pandemia, que también habían colocado clonadores en otras entidades bancarias donde vos participaste y lograron detener a una persona de nacionalidad brasilera, creo que esto también está dentro del ciberdelito, es más, en dos oportunidades sacamos este tipo de dispositivos de nuestras sucursales y nunca llamamos a la policía, ya que desde Buenos Aires nos ordenan no hacerlo por la mala publicidad.

5. Desde la entidad bancaria ¿Cuáles son los pasos que se siguen para identificar a los autores de los hechos delictuales?

Nosotros actuamos conforme la solicitud de las Fiscalías que soliciten algún tipo de información mediante un oficio judicial, como por ejemplo, número de cuentas a las que fue transferido el dinero, a nombre de qué persona, si lo tuviéramos, o a que sucursal bancaria fue transferido, o en qué provincia fue retirado o se llevó a cabo la operación de extracción. Pero la identificación de los mismos, estimo que está a cargo de la policía (sonríe).

6. Desde su lugar en el banco ¿Cómo observa la seguridad bancaria para evitar que estos tipos de hechos sucedan?

Complicada para responder tu pregunta, empecemos por la colocación de cartelería, que no fue un gasto menor, colocar en todas las sucursales y cajeros automáticos cartelería preventiva informando al usuario que desde el banco no le van a solicitar cambios de claves ni contraseñas, no aporte sus datos personales, evite se víctima de una estafa virtual y todo tipo de información preventiva.

Por otra parte, enviar e-mail a todos los clientes del banco detallando cuales son los links falsos, cuales son los correos oficiales del banco, y toda información preventiva.

Por otra parte, nuestra asociación bancaria limitó los montos de trasferencias de dinero de una cuenta a otra, siempre y cuando no fuera de la misma persona, o pagos habituales de servicios en caso de las empresas, aunque el BCRA no nos autorizaba a restringir este tipo de operaciones todavía. También en los casos de los prestamos pre-adjudicados, ya no son de forma inmediata, hay una demora de 48 horas y el cliente deberá certificar en ese lapso que está seguro de la operación realizada, ya sea en forma personal o por e-mail al banco, y éstas medidas recibimos la autorización desde casa central en CABA antes que saliera la comunicación del BCRA ya que nosotros atendíamos los reclamos de la gente.

7….**Entonces podemos decir que las entidades bancarias ¿han llevado a cabo distintas medidas para proteger a sus usuarios y sus datos?**

Sí, como te decía anteriormente, se realizó una campaña interna y si vos sos usuario de nuestro banco, vas a recibir correos con los consejos de cómo prevenir el ciberdelito, casi en forma permanente. La colocación de cartelería en las distintas sucursales, bueno lo que veníamos hablando. También se procedió a dar capacitación a nuestro personal de la división informática, intensificando los cortafuegos para evitar un hackeo a nuestro sistema informático.

8. Por último y si te comprometo más de lo debido, no hace falta que respondas a ésta pregunta ¿Cómo responde el banco a las víctimas del ciberdelitos, se hace cargo de ese dinero, lo devuelve, o por ejemplo en caso de un crédito, anula las cuotas?

Si me comprometes bastante con esta pregunta, pero te puedo decir que en la mayoría de los casos el banco se hace cargo a través de los seguros que tenemos contratados, pero han aumentado tanto que se empezó a estudiar cada caso en específico, pero por temor a mala publicidad, como te decía recién, en la mayoría de los casos se responde en forma inmediata.

Muchas Gracias.

ENTREVISTA Nº3

EDAD: 52 años.

Jefe de Seguridad de entidad bancaria

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

Si bien la función específica mía es la seguridad física de las distintas sucursales bancarias, a raíz del aumento de casi un 300 % de los fraudes electrónicos o ciberdelitos, también nos afecta de lleno, ya que en muchos casos las personas concurren a los ATM (cajeros automáticos) guiados por el engaño de otras personas y cambian las contraseñas y los números secretos, y es allí que nos solicitan a nosotros las grabaciones del CCTV (Circuito Cerrado de Televisión) para verificar si verdaderamente ha sido así. Además,, desde los principios de la pandemia cuando esto se disparó por las nubes, recibimos capacitaciones y se nos ordenó colocar cartelería informativa en todos los ATM, y sucursales bancarias, alertando a los usuarios de que no deben realizar tales maniobras engañosas ya que el banco nunca les va a solicitar ese tipo de información, por algo es secreta. No obstante ello, nuestra entidad bancaria tiene dos secciones que se ocupan de lleno de este tipo de delitos, que son Prevención de Fraude e Investigación de Fraude.

2. ¿Nos podrías enumerar cuales son los ciberdelitos más frecuentes que hayan afectado a la entidad bancaria que representa?

Los más comunes son los que denominamos phishing, entre los que se encuentra la utilización del correos electrónicos utilizando los logos del banco anunciando engañosamente que tiene un préstamo pre-aprobado y de este forma obtienen la información necesaria para ingresar a sus cuentas y producir el vaciamiento de la misma, también ofreciendo la banca on-line en especial durante la pandemia y obtenían la información necesaria no solo de sus cuentas sino también de sus tarjetas de crédito.

También los llamados telefónicos donde les manifestaban que para acceder a la ayuda económica que otorgaba la presidencia debían concurrir al cajero automático y los iban guiando y así accedían a su cuenta y sacaban el dinero que tenían.

Por otro lado, tenés el skimming pero este con la pandemia disminuyo que es la clonación de tarjetas, a través de un lector de banda magnética en la boquilla del cajero y de un dispositivo de grabación en la parte superior para obtener la clave alfanumérica, pero sabemos que disminuyó porque la gente no podía circular por la calle y los delincuentes encontraron otra forma de engañar a la gente. En todos los casos logran suplantar la identidad del verdadero cliente bancaria.

3. ¿Cuáles cree que son los factores de riesgos más recurrentes para que ocurra este tipo de delito en el ámbito bancaria?

Para mí la crisis económica, que lleva a la gente a creer lo que escucha diciéndole que ha sido seleccionado para el cobro de una ayuda del gobierno, después del desconocimiento del uso de la tecnología y que el común de la gente no sabe usar las bancas on-line, y como te decía recién la crisis económica llevó a la gente a un estado de stress tal que nunca pensó que el banco jamás te va a pedir un cambio de clave o contraseña y si hacemos un meaculpa el banco tampoco va a invertir en seguridad sobre un sistema que funciona sin problemas, ya que no podes complicarle aún más a la gente el uso de la banca on-line cuando el 80% de las funciones bancarias desde marzo del año paso se hace en forma remota, incluso los empleados bancarias trabajan en forma remota, entonces te llaman a cualquier hora y las personas accedían. Y si tenemos en cuenta que el ciberdelito se disparó durante la pandemia, te puedo decir que el BCRA nos ordenó de la noche a la mañana trabajar on-line y no teníamos los soportes necesarios de seguridad para hacerlo.

4. ¿Ha tenido que intervenir en algún hecho delictivo de este tipo?

Directamente no, actuamos una vez que la denuncia ingresa al banco y conforme nos solicite información la sección que se ocupa de la investigación del fraude, o en caso de que monitoreo nos llame por alguna actitud sospechosa en un ATM, en todo caso la gerencia de la sucursal afectada es la que concurre a la entidad si fuera un hecho fuera de hora como por ejemplo la colocación de clonadores de tarjetas, pero a lo que respecta a ciberdelito no hay participación física por así decirlo de personal del banco.

5. Desde el Banco ¿Qué pasos siguen para identificar a los autores de los hechos delictivos?

Acá tenemos que dividir los distintos procedimientos de seguridad del banco y conforme el tipo de metodología o clase de ciberdelito que se cometa. Si hablamos de aquellos donde el cliente en forma engañosa aporta sus datos y se comete el delito, no hay sistema de seguridad que ayude a identificar a la persona, si bien se determina el número de cuenta a la que fue trasferido el dinero o si es una billetera virtual. Pero si alguien concurre a una sucursal a retirar el dinero a través del CCTV se pueden aportar imágenes que se hacen circular en todo el país y en caso de observarlo nuevamente se alerta a la policía. Ahora si son delitos como la clonación de tarjeta que requiere la presencia física del estafador para colocar los dispositivos, se pueden obtener imágenes que sirven para su identificación como prueba del delito cometido. En todos los casos se aportan los datos a requerimiento del tribunal que intervenga, previa anuencia de la gerencia general del banco.-

6. Desde la entidad bancaria ¿Qué medidas se toman para evitar que éstos tipos de hechos sucedan?

Desde nuestro banco en primera instancia se alertó a toda la cartera de clientes a través de correos electrónicos con power point y recomendando en todo momento que el banco nunca le va a pedir cambio de contraseña, ni es necesario concurrir a un cajero automático para introducir códigos específicos para el cobro de algún beneficio etc. Por otra parte, la colocación de cartelería disuasoria en todas las sucursales y ATM del país, no solo de Mendoza, esto si hablamos solo de los ciberdelitos que últimamente se da a conocer. En el caso de la clonación de tarjetas, la red Banelco tiene un sistema de alarma que en caso de que la misma tarjeta opere en dos provincias distintas el mismo día dispara una alerta para el bloqueo de la misma, por ejemplo, si tu cuenta es de Mendoza y realizaste una operación a las 10;00 hs de la mañana y a las 14;00 hs realiza una operación en Tucumán, automáticamente se bloque y te notifican al cliente que debe concurrir a la sucursal del banco más cercana ya que se estima una clonación de tarjeta, el problema surge cuando la extracción no se realiza en un cajero automático, como por ejemplo estaciones de servicios, supermercados, farmacias en aquellos locales no bancarizados. En cuanto a los créditos on-line, también se les colocaron trabas como por ejemplo un lapso de 48 horas para acceder a los mismos, de esta manera se lo notifica al cliente a través de un correo o llamado telefónico o de whatsapp de que ha efectuado exitosamente la operación y en un lapso de 48:00hs será acreditado el préstamo solicitado, como así también se le solicita que concurra a la sucursal. Se procedió a limitar el monto de las transferencias bancarias a no ser que sean movimientos habituales de la cuenta o pago de servicios. Desde ABA (Asociación de Bancos de Argentina) también solicitaron al BCRA un mayor control en los retiros o circulación de dinero en forma virtual hacia las billeteras electrónicas como Mercado Pago, Ualá o Naranja X entre otras, cuando la suma de dinero es considerable.

7. ¿Qué otras medidas se llevan a cabo en los bancos para proteger a los usuarios y sus datos?

A parte de las que te mencioné, podemos agregar en el caso de SKIMMING, las tarjetas de débito con chip aparte de la cinta magnética, la colocación de cajeros inteligentes con lectores de huella dactilar, pero esto sirve únicamente para la clonación de tarjetas.

8. Por último y si te comprometo demasiado con la pregunta no hace falta que la responda. ¿Cómo responden los bancos cuando un cliente realiza la denuncia de que ha sido víctima de un fraude o de los ciberdelitos que hemos enumerados?

Todo depende del tipo de delito, por ejemplo, si el cliente aportó las claves secretas, a través de la sección Investigación de Fraude se decide si es responsabilidad del banco que haya sido víctima o si es responsabilidad del cliente, ahora en la mayoría de los casos con el fin de evitar una mala publicidad el banco va a responder. Te pongo como ejemplo lo que pasó en la sucursal del Banco Nación de Guaymallén, las compras fueron on-line con el uso de tarjetas de crédito, y tarjetas de débitos de los jubilados, en esos casos el banco no responde, pero como salió en televisión, el banco ahí nomás salió a decir que se harían

cargo de la devolución del dinero. Si la estafa es por Mercado Libre o Whatsapp donde se ve involucrada la cuenta bancaria, el banco no tiene que responder ya que no fue un hackeo a su sistema sino un error del usuario en la transacción económica que realizó.

Muchas Gracias.

ENTREVISTA Nº4

CABO 1° P.P. (R. C.) Víctor Jorge Contrera. Asesor de Seguridad Bancaria

Edad: 63 Años

Actualmente me desempeño como Asesor del Departamento de Seguridad Bancaria, Titulo otorgado por el Banco Central de la República Argentina (BCRA), desde hace veintiocho años aproximadamente.

1 ¿Conoce los Ciberdelitos que se producen en las Entidades Bancaria?

Si los conozco, los ciberdelitos más comunes en el ámbito bancario son: phishing, smishing, skimming, spoofing.

2. ¿Podría enumerar los más frecuentes?

Por ejemplo el phising es un término informático, que busca mediante el engaño a una víctima ganarse su confianza y haciéndose pasar por una persona "X" o empresa, para manipularla y hacer que realice actividades que no debería (por ej. otorgar datos confidenciales).

El smishing va dirigido a usuarios de telefonía móvil ya que es una variante del phishing, pero este se realiza mediante mensaje de texto.

El spoofing se manifiesta a través de la falsificación de datos en una comunicación. Por ejemplo se hacen pasar por una entidad distinta (suplantación de identidad), enviando un correo electrónico para así acceder a datos personales o confidenciales, de forma maliciosa.

El skimming fue pionero en la provincia, ya que tuvimos varios hechos denunciados por las entidades bancarias y clientes. La modalidad está basada en adquirir datos personales para finalmente clonar la tarjeta y luego hacer usufructo de la misma. Se desarrolla colocando una mini cámara en un lugar casi imperceptible del cajero automático, ya sea en la parte superior de la pantalla o en algún lateral, esto es para poder acceder a los datos de la persona que se encuentra realizando la transacción, y se guarda en una tarjeta de memoria (se instala por lo general en la boquilla por donde ingresa la tarjeta para ser procesada).

3. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurra este tipo de delito en el ámbito bancario?

El Principal factor de riesgo son los adultos mayores, que por lo general asisten solos a los cajeros automáticos o solicitando ayuda de un tercero. A su vez, son desconocedores de términos y acciones informáticas, y quizás esto deriva en una aceptación de proveer datos personales o aprobar un crédito sin siquiera ellos saberlo.

4. ¿Ha debido intervenir en algún hecho de delito de este tipo?

Sí, he tomado conocimiento por denuncias al 911, como ser Banco Macro de Calle San Martin y Alem de Ciudad, donde habían colocado un Skimming en el cajero automático, quedándome en el lugar y el Comisario se dirigió a controlar los otros cajeros automáticos encontrando otro Skimming en el Banco Patagonia de Calle Gutiérrez N° 72, Cdad y por último fue descubierto en el Banco actualmente BBVA de Calle España N° 1342, Ciudad donde el Comisario observa un movimiento raro de un ciudadano que estaba cruzando la plaza y al darle la voz de alto se da a la fuga , al alcanzarlo se lo reduce tratándose de una persona de nacionalidad brasilera, siendo trasladado todo el procedimiento a Oficina Fiscal N° 1 de Comisaría 3° .

Otro caso, fue en el año 2020, para el mes de Mayo, cerca de las 18:00 hs es alertado personal de la Delegación de la zona sur que en el Banco Macro de Calle Chile N° 173, San Rafael habían instalados Skimming, en la recorrida por los cajeros automáticos y teniendo las fotos de las personas que habían colocado los dispositivos que le brindó el monitoreo al personal de Bancaria Zona Sur, que esto a su vez a través del WhatsApp le brindan las fotografías al personal policial que estaba colaborando en la búsqueda de los mismos; los cuales a posterior fueron detenidos.

Al día siguiente, salgo en comisión en la movilidad 2941, a cargo del Comisario, a la Delegación de Zona Sur para realizar un allanamiento en el Hotel que se encontraban hospedados estas dos personas de nacionalidad argentina y brasilera. Se procedió al secuestro de una notebook, una máquina para hacer las cintas magnéticas de las tarjetas, varias tarjetas de red bus y otras tarjetas similares.

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

Solicitamos imágenes a las entidades bancarias, para así transmitirle los datos y fotos a personal de Delitos Tecnológicos.

6. ¿Cómo observa la seguridad bancaria para que estos hechos sucedan?

Para mi ver, monitoreo remoto debe estar atento a las cámaras, y en caso de observar algún movimiento extraño, por parte del cliente, debe comunicarse de forma inmediata al 911.

7. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger los usuarios y sus datos?

Una de las medidas es que en el Banco Central emplazó a las entidades en la Comunicación "A" 6894, a que cambiasen sus equipos, de modo teclado al uso de huella dactilar, esto lo deberían aplicar las sucursales a más tardar en diciembre de 2021.

También las propagandas que realizan por todos los medios de que no brinden sus datos personales (usuarios, claves, contraseñas y PIN).

Otra medida que se ha dispuesto es que las tarjetas de débito posean chip

MUCHAS GRACIAS.

ENTREVISTA Nº5

NOMBRE: Gustavo Espinosa. Analista de Seguridad en el Banco Central de la República Argentina

EDAD: 50

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

Existen muchos tipos y variantes de cada uno, entre ellos, puedo mencionar (así mismo se puede ampliar en los links de abajo):

Phishing / suplantación de identidad: Se hacen pasar por una entidad Financiera, posteriormente solicitan los datos para apoderarse de las cuentas

Robo de tarjetas bancarias: el delincuente realiza la estafa por llamadas telefónicas o email, consigue los datos de la tarjeta de la víctima y realiza compras reiteradas veces en sitios online.

Fraudes en páginas, páginas que anuncian ventas con descuentos importantes de diversas entidades y la finalidad es obtener los datos bancarios de la victima

Virus: son una variante llegan por correo o por compartir archivos infectan la máquina y roba el almacén de claves, o por ejemplo instalan un keylogger que luego en segundo plano trasmiten todo lo que se tipeó y las página que ingresó.

2. ¿Podría numerar cuales son los más frecuentes?

Los más frecuentes son la suplantación de identidad y el robo de datos de las tarjetas bancarias.

3. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

El desconocimiento de las personas sobre como preservar su información confidencial. Como así también, qué medidas adoptar o donde deben ingresar para comprobar la veracidad de un sitio, desconocen las medidas básicas para no caer en tramas del pishing. Por otro lado, están las entidades que no preservan adecuadamente los datos personales de sus clientes, Como lo demuestra la multa que aplicó Comercio Interior a entidades bancarias.

El entorno virtual resulta complicado para las personas que están en poco contacto con la tecnología o tienen escasos conocimientos, presentando de esta forma un abanico de posibilidades a los ciberdelincuentes que son muy hábiles en explotarlas

4. ¿Ha debido intervenir en algún hecho delictivo de este tipo?

No

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

Los delitos informáticos, son muy complejos, cuando están bien organizados son muy difíciles de rastrear, no hay una única receta, sino que debe ser dinámica y adatarse a la modalidad detectada, ya que la tecnología les permite rápidamente borrar sus huellas, las distancias le brindan anonimato y privacidad, por lo cual se precisa de personas con altas capacidades y conocimientos para ejecutar el rastreo, antes de que el delincuente se dé cuenta o mute la modalidad.

6. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

La seguridad para la prevención de fraudes por canales electrónicos se encontraba en un estándar muy bajo a comienzo de la pandemia, la cual hizo que el ciberdelito aumentara considerablemente hasta un 3000% durante el 2020 como lo describe una nota de Telam: https://www.telam.com.ar/notas/202104/551902-estafas-bancarias-ciberdelito.html

En general y cómo podemos observar al pie en los gráficos, en la República Argentina no se ha avanzado demasiado en materia de ciberseguridad entre los 2016 y 2017 de acuerdo al informe realizado por el Banco Interamericano de Desarrollo (BID), a través del Observatorio de Ciberseguridad, titulado “Ciberseguridad Riesgos avances y el Camino a seguir en América Latina y el Caribe”.

7. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger a los usuarios y sus datos?

Actualmente los bancos han iniciado una campaña activa de información, y con ejemplo, donde los usuarios pueden aprender al respecto

Muchas gracias

ENTREVISTA Nº6

SUBCOMISARIO P.P.

Edad 48 años

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

En lo que respecta los ciberdelitos que se producen en las entidades bancarias, podemos decir que la clonación de tarjetas de débito y/o crédito, son las más comunes. Cuando decimos ciberdelitos, debemos aclarar que, como tal, se entiende por ciber, al espacio no determinado, o sea que si decimos ciber crimen, sería el crimen cometido en un espacio virtual. En este caso, vamos a decir ciberdelitos, a los que se cometen en espacios virtuales como son las cuentas bancarias o los accesos a estas

2. ¿Podría numerar cuales son los más frecuentes?

Los delitos más frecuentes, son las estafas virtuales en las que se tiene como denominador común, la llamada telefónica. Con esta llamada, y luego de entablar una conversación extensa, en la que se confunde a la víctima, se logra acceder a datos de cuentas bancarias como clave token, usuario y contraseña etc. Y poder disponer del dinero que las cuentas tengan.

3. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

Los factores de riesgo más frecuentes, son sin dudas, la falta de atención que los usuarios tienen al momento de operar o interactuar con los presuntos operadores de bancos, vendedores, etc. Aportan datos como claves, sin saber con quién están hablando, o en su caso, transfieren dinero por alguna compra son ver el producto o conocer a la persona

4. ¿Ha debido intervenir en algún hecho delictivo de este tipo?

Con la experiencia en la División Delitos Económicos, se ha intervenido en varios procedimientos de los cuales se tiene como resultados, el secuestro de elementos que hacen a la clonación de tarjetas de crédito y debido, como así se ha podido obtener elementos que hacen a otras investigaciones importantes que han impactado en nuestro medio de forma relevante. Sobre este punto, podemos citar el caso del Banco Nación de Villa Nueva, Guaymallén, investigación que demandó más de dos meses para poder establecer que el autor de los hechos (le vaciaban las cuentas bancarias de abuelos y jubilados) sin que quedaran rastros de las maniobras. La investigación, permitió conocer que de forma remota y desde otro punto del país, personas idóneas en informáticas, accedían a los archivos bancarios y extraían dinero o realizaban compras por internet.

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

Como venimos reseñando anteriormente, es complicado poder identificar a los autores, dado que todos sus movimientos son en el plano virtual, en espacios atemporales. Sin embargo, podemos referir que en ocasiones, se tiene que todo dispositivo deja un registro como puede ser la IP, que no es más que una dirección electrónica a la cual se la puede ubicar en un determinado lugar. Esto como es ampliamente conocido por estos idóneos, utiliza programas que ocultan o deformar esas IP, haciendo más complicado el trabajo policial.

6. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

En la provincia de Mendoza, afortunadamente, el sistema de seguridad bancaria, es altamente efectivo. Si tenemos en cuenta la cantidad de bocas de expendio de dinero (cajeros automáticos y entidades bancarias, en comparación con otras latitudes, vamos a poder apreciar que estamos en una muy buena ubicación. Para referir alguna situación sobre este punto, debemos recordar que recientemente se han llevado a cabo dos procedimientos en los cuales se logró el secuestro de material para clonar tarjetas, (San Rafael y Casino Clandestino en Lujan) y otra intervención de la que surge un aprehendido con elementos que colocaba en los cajeros para poder hacerse de dinero (pescadores).

7. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger a los usuarios y sus datos?

No solo las entidades bancarias aportan para proteger a los usuarios, Existen casas de envío de dinero con alcance nacional e internacional, que ante la posibilidad que una persona esté por enviar dinero a otra persona que puede ser un estafador, le consultan si conoce a esa persona, sin antes ha operado con ella. O si tiene en cuenta que podría estar siendo estafada.

En el caso de los bancos, estos han colocado en las pantallas de los cajeros, indicaciones y recomendaciones para evitar ser estafados. Colocan folletería de prevención en los locales, entre otras cosas. A ello hay que agregar que se trabaja en conjunto con otras entidades para difundir medidas de prevención que apunten a evitar ser estafados.

Muchas gracias

ENTREVISTA Nº7

SUBCOMISARIO PP JUAN ANDRÉS RÍOS

Edad: 41 años

Jerarquía: Subcomisario PP

Actualmente estoy a cargo de la Delegación del Departamento de Seguridad Bancaria Zona Sur, desde hace 9 años aproximadamente, en ese tiempo he recibido capacitación del Banco central de la República Argentina, lo cual me fue preparando para ser asesor del Departamento en el ámbito de seguridad bancaria, también estoy a cargo del sistema de alarma bancario con jurisdicción en todo el sur mendocino.

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

Si los conozco, los ciberdelitos más comunes en el ámbito Bancario son: el phishing, smishing, skimming, spoofing.

2. ¿Podría enumerar los más frecuentes?

Por ejemplo el phishing, que es cuando el delincuente, utilizando ingenio social para obtener datos personales de las personas atreves del engaño, suplanta la identidad del mismo enviando un correo electrónico falso y de esta forma obtener los datos necesarios para ingresar a su cuenta y retirar dinero que posee, y si la cuenta no tiene dinero, sacan un préstamo otorgado en forma inmediata por la entidad bancaria en forma on line, y después vacían la mismas realizando transferencias o bien retirándola por caja con una identificación falsa, existen varios casos con este modo operandi. También este tipo de delito se empezó a ver con más frecuencia debido a la pandemia, por motivo que los bancos fueron apostando a realizar más operaciones a través de lo digital, ampliando este concepto y a modo de ejemplo antiguamente lo común era para sacar un préstamo, se debía presentar una serie de documentación en la sucursal bancaria y esperar a que fuese aprobado y con suerte en los días restantes era depositado en su cuenta, después retiraba el dinero por la ventanilla, eso con el tiempo fue desapareciendo, y ahora lo común es, a través del celular con una aplicación o bien utilizando una pc accedes al homebanking, solicitas un préstamo en forma on line, te lo aprueban casi de forma inmediata, y en minutos tenés el dinero depositado en tu cuenta.

En cuanto al smishing es igual al anterior, salvo que obtiene lo hacen a través de un mensaje de texto o cualquier aplicación de mensajería.

El spoofing es el uso de técnicas de suplantación de identidad. Hay diferentes tipos, entre ellos el envío de correos electrónicos o páginas fraudulentas, falsificación de dispositivos o de direcciones IP. Independientemente del tipo, los ataques de spoofing son maliciosos. Es decir, quienes realizan este tipo de fraudes buscan hacerse pasar por otras personas,

organizaciones o empresas para acceder a datos personales, distribuir malware o generar algún tipo de perjuicio.

Otro tipo de esta clase de delito es el skimming , que se trata de cuando un delincuente utilizando la ingeniería, y conocimiento informático, ya exponiéndose un poco más, estos delincuentes se acercan a una entidad bancaria, una que sea concurrida por los usuarios, fuera del horario de atención al cliente, donde el vigilador y/o personal bancario no se encuentra, ya una vez en el interior del lobby(lugar donde se encuentran los cajeros automáticos) coloca cámaras sobre la superficie del cajero, casi siempre en la parte superior del teclado o bien en el costado de la pantalla, depende también del modelo de cajero, de esta forma obtiene las claves de acceso a la cuenta de la víctima, también colocan en el interior de la boquilla, un lector de tarjetas, de tamaño diminuto, lo cual utilizan para clonar la información de la banda magnética de la tarjeta, dejan trabajar los dispositivos, unas horas y ya cuando el público deja de concurrir, ingresan al lobby nuevamente y retiran los dispositivos, para ilustrar un poco más lo enunciado, las cámaras no suelen ser reconocidas por las victimas debido a que utilizan materiales muy similares al que normalmente posee los cajeros y ocultan las cámaras de alta definición y solo se observa un pequeño orificio que es por donde toma las imágenes la cámara, con respecto al clonador, va dentro de la boquilla donde se introduce la tarjeta y no se visualiza desde el exterior, salvo que se posea conocimiento y utilizando un tipo de gancho se logra extraer, es un delito muy difícil de detener al delincuente mientras está en su comisión, porque normalmente, una vez que el autor logra sacar los elementos del lobby, se retira a donde pernota, ya por la noche, trabaja los datos tanto la tarjeta clonada, la cual pasa esos datos a una tarjeta que posea una banda magnética, pude ser por ejemplo un tarjeta de alguna compañía telefónica, una de videos juegos etc., luego trabaja sobre las imágenes y así obtiene las claves de ingreso y a veces las alfanuméricas, entonces repite el procedimiento con cada tarjeta clonada, una vez finalizada estos trabajos, en la madrugada del día siguiente salen de la ciudad con destino a una nueva, que es donde ya con los datos que obtuvieron la noche anterior, se dirigen a la sucursal bancaria elegida, esperan cierra de la jornada, ya una vez retirada los empleados, ingresan al lobby y comienzan aprobar las tarjetas clonadas, finalizada la faena, antes de retirarse, vuelven a colocar cámaras y clonadores, retirándose y así continúan con la pesca de nuevas víctimas, por cuando la víctima nota que hay una operación de extracción que no han realizado, ya los delincuentes de se encuentran a kilómetros de distancia y con al menos dos días de ventaja, también es de resaltar que las sumas de dinero que extraen no son de grandes cantidades, inclusive hay clientes que ni siquiera nota lo ocurrido, pero que realizar varias operaciones por días, se llevan grandes cantidades de dinero, a modo de ejemplo en una semana pueden recaudar millones de pesos, es un delito que se observa muy frecuente en los países limítrofes, como Chile y Brasil, donde posee una estadística elevada de estos ciberdelitos, y es más, todo lo que necesitan, clonadores, cámaras, lectores son adquiridos en mencionados países, otro dato para aportar en lo que respecta a clonación de tarjetas, ya fuera del ámbito bancario, es el skimming pero ya no es necesario desplazarse a

las sucursales bancarias, lo hacen en una estación de servicio o en un comercio como puede ser un restaurant, donde el lector de tarjetas para clonar funciona por bluetooth, con solo arrimar este dispositivo a la tarjeta, ya la clonan y luego observan la clave que introduce el cliente, cerrando de esta manera la estafa.

3. ¿Cuáles cree que son los factores de riesgos más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

El factor de riesgo más alto, es el desconocimiento de este estos tipos de delito, en las personas y aún mayor en los adultos mayores, que poseen poco o escaso conocimiento de la materia, apenas saben colocar la tarjeta y la clave, no son precavidos en por ejemplo ocultar la clave que introducen al teclado del cajero automático, también existe poca inversión desde el punto de vista bancario en evolucionar para evitar este tipo de delitos, otra herramienta sería un proceso judicial penal diferente a los delincuentes que son detenidos por estos hechos, dado que son procesados por estafa, un hecho que es excarcelable, pagando una fianza, lo cual el dinero en este caso no es un problema para ellos.

4. ¿Ha debido intervenir en algún hecho de delito de este tipo?

Si, en el año 2012 me toco trasladarme a la ciudad de Malargüe, donde personal policial había detenido la marcha de un vehículo de alta gama y le llamada la atención al personal la cantidad de tarjetas magnéticas que poseían. Al llegar a la ciudad de Malargüe me hice presente en la comisaria 24, donde al pedir ver el secuestro, observa los elementos habituales para el delito de skimming, cámaras, clonadores y lectores de tarjeta, hasta el momento no se sabía nada más, por lo cual inicie una investigación por el lugar y al consultarle a varios vecinos de la zona, logramos dar con el lugar donde pernotaron, lo cual le habían pagado a la casera dinero extra para que no los registraran en el libro, todo quedó plasmado en las actuaciones y de esta forma logramos establecer el circuito recorrido por los autores, dando el conocimiento a las policías vecinas para que asistieran a las víctimas de esta estafa, y también evitamos que los vecinos de Malargüe que le fueron clonadas las tarjetas no llegaran a ser estafados.

Otro caso fue en el año 2020, en el mes de mayo. Corría un día normal, a las 18 horas soy alertado por el Monitoreo del Banco Macro que posiblemente los autores de skimming estarían trabajando en mi zona, me desplazo al lugar en compañía de mi segundo al mando, Sargento PP Carlos Quiroga, y constato fehacientemente que en la sucursal del banco macro de Calle Chile 173 de San Rafael, poseía instalados dispositivos compatibles con Skimming, por este motivo hablé con el jefe de la comisaría y el Ayudante de Fiscal. La zona se encontraba con demasiada presencia policial, y les solicite que no abandonaran ese lugar y nos dejaran trabajar en el resto de las entidades para poder lograr la aprehensión de los malvivientes, por lo que el Ayudante de fiscal me dio unos minutos y como pertenezco al grupo de WhatsApp creado por el BCRA, poseía información de los presuntos autores. Y

otro dato que utilizamos era la clase de cajeros automáticos que estaban utilizando, por lo cual nos dividimos para cubrir las entidades, a los pocos minutos ya sobre la avenida Hipólito Irigoyen, en la verada del Banco Patagonia, mi sub alterno observa a uno de los delincuentes y me avisa por teléfono, por lo cual espera mi apoyo y se logra la aprehensión del sujeto cuando este iba caminando pasando por la vereda de la comisaría 32º, personal de comisaria miraba sin entender aun lo que pasaba, seguramente por la vestimenta del delincuente, ya una vez aprehendido y el suscripto con el conocimiento de que se trataba de los dos ciudadanos advertido por el BCRA, por frecuencia radial ordeno y solicito al personal de calle, que busque con las características físicas que poseía y que el mismo tenia acento portugués debido a que era oriundo de Brasil, lo cual el personal de operativo, es cual es de destacar, procede a la aprehensión del ciudadano que faltaba y al secuestro del vehículo que utilizaban, luego de una larga investigación y tarea en conjunto, se logra dar con el hotel donde estaban pernotando, se dejó consigna policial y en horas de la mañana, ya con luz solar, también con el apoyo del Titular de la Dependencia Comisario PP Guillermo Teixido, y personal a cargo, personal de investigaciones, como así la presencia del Jefe Distrital dos, se procedió al allanamiento y al secuestro de los elementes que se encontraban en el interior de la habitación que habían alquilado, los cuales fueron muchos y que sirvieron para procesar a los detenidos, como así se facilitó lo necesario a las policías como las provincias de Córdoba y Neuquén.

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

Por lo general, si el delito es phishing, smishing o spoofing se trata de dar con el autor de la llamada telefónica, mensajería o cualquier otra dato que nos lleve a la identificación del mismo, y se le da intervención al área de delitos tecnológicos, en el caso de skimming al ser más presencial este tipo de delito, se trata de recabar datos a través de los sistemas de Circuitos cerrados de televisión de las entidades Bancarias, donde ya interferimos de manera más activa para dar con los autores o bien para alertar a las provincias vecinas.

6. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

Desde nuestra óptica la forma de evitar como sucedió por ejemplo en las dos oportunidades que se dieron en el sur, es a través de primero tener personal policial con conocimiento y preparados para actuar de forma rápida, dado que son tipos de delitos muy difíciles de lograr la aprehensión de mismo, también es importante contar con el apoyo del resto del personal policial que realiza la misma tarea en el resto del país, lo cual nutre y proporciona datos muy significativos para llevar adelante un procedimiento de esta magnitud, es muy importante, no es un dato menor contar con el apoyo del BCRA.

7. ¿Qué acciones a observado que llevan a cabo las entidades bancarias para proteger los usuarios y sus datos?

Debido a los múltiples hechos no solo en nuestra provincia como decía en el párrafo anterior, si no en el resto del país, el banco central ha dispuesto una serie de medidas para tratar de revertir estas situaciones, emitiendo en una de las últimas comunicaciones, la cuales actúan de forma inmediata en el cumplimiento de los bancos, por lo que se está en estudio de tratar de endurecer y tratar de corroborar la identidad de una persona al momento de extraer ciertas cantidades de dinero o bien al momento de solicitar un préstamo, también he observado que desde la página del BCRA difunden una serie de recomendaciones para evitar este tipo de delitos, la cual si me permite voy a citar textualmente:

Recomendaciones para proteger tu información personal

El desafío en este escenario es proteger tu información personal y adoptar buenas prácticas para el uso de redes sociales, sitios y plataformas digitales.

- Activá la autenticidad de dos factores en cuentas de redes sociales y WhatsApp o las plataformas digitales que utilices. Esta herramienta es una capa adicional de seguridad que ayuda a verificar que solo la persona usuaria de la cuenta pueda acceder a sus redes sociales y plataformas digitales. Se activa ingresando al menú de ajustes o configuración de la cuenta que se quiere proteger, opción "Autenticación en dos pasos".
- No brindes ningún dato personal (usuarios, claves, contraseñas, pin, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato), por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto.
- No ingreses datos personales en sitios por medio de enlaces que llegan por correo electrónico, podrían ser fraudulentos.
- Usá contraseñas fuertes mezclando mayúsculas, minúsculas y números. Tienen que ser fáciles de recordar pero difíciles de adivinar por otras personas. No uses la misma clave para distintas aplicaciones, cuentas, plataformas o sitios.
- Leé cada correo electrónico recibido con cuidado. Verificá que los sitios remitentes sean legítimos.
- Tené cuidado con los enlaces sospechosos y asegurate siempre de estar en la página legítima antes de ingresar información de inicio de sesión.
- No uses equipos públicos o de terceras personas para acceder a aplicaciones, redes sociales o cuentas personales.
- No uses redes de wi-fi públicas para acceder a sitios que requieran contraseñas.
- Mantené actualizado el navegador, el sistema operativo de tus equipos y las aplicaciones (borrá las que no uses)

- Siempre hay que tomarse un minuto antes de actuar. Quienes realizan este tipo de estafas apelan a las emociones, descuidos y urgencias.

Muchas Gracias

ENTREVISTA Nº 8

SUBCOMISARIO P.P. Lic. Omar Darío Raguasi

Edad: 43 años

Soy Licenciado en Seguridad Pública de la Universidad de Cuyo; Soy Diplomado en Cibercrimen y Evidencia Digital de la Universidad Champagnat; además, soy Idóneo en Informática Forense con 10 años de experiencia en investigaciones de delitos informáticos y actualmente soy Jefe de la Oficina Observaciones Tecnológicas y cumplo funciones de Perito Informático en causas judiciales del fuero penal provincial y federal.

1. ¿Conoce los ciberdelitos que se producen en las entidades bancarias?

Los comúnmente llamados ciberdelitos son aquellos hechos típicos que se encuentran descriptos por la Ley 26388/2008, en los que se mencionan aquellos delitos que son cometidos, en primer lugar contra un medio informático, en segundo lugar utilizando un medio informático para su comisión y en tercer lugar contra la información que el medio informático contiene.

De esta manera en el primer caso, el objetivo sería realizar acciones que perjudiquen de alguna manera el medio, lo deje fuera de servicio o deteriore su funcionamiento, como por ejemplo ataques de denegación de servicio, exigiendo a cambio de la liberación del servicio el pago de algún bien económico. En este caso las entidades bancarias invierten gran cantidad de recursos para evitar ser víctimas de este tipo de delitos por lo que difícilmente puedan ser llevados a cabo, además, de ser cometidos, ninguna entidad dará a conocer esa situación debido a que resultaría contraproducente para su confiabilidad.

El más común es este segundo caso, donde las personas aprovechándose de la poca experiencia en los sistemas informáticos, sobre todo de adultos mayores, y de algunas debilidades de en los procesos de adquisición y validación de identidad, utilizan llamados engañosos donde se hacen pasar por diferentes situaciones, como el secuestro de algún familiar, o por parte del círculo de confianza, haciéndose pasar por algún agente de la entidad bancaria le solicitan las claves y de acceso y diferente información que le permite al victimario apropiarse de los valores que se encuentran en las cuentas bancarias y contraer préstamos a nombre del damnificado por medios tecnológicos.

Y finalmente, software que tiene el fin de engañar a las víctimas como el phishing o ramsonware que produce el secuestro de la información como medio para dejar de alguna manera secuestrada o inaccesible.

2. ¿Podría numerar cuales son los más frecuentes?

Actualmente los más frecuentes son:

- La obtención por medio de llamados telefónicos engañosos, de datos de tarjetas de crédito y de cuentas bancarias para extraer dinero o contraer préstamos.
- Phishing por medio de correos electrónicos suplantando la identidad de autoridades de entidades bancarias con el objeto de obtener las credenciales de acceso a los servicios de banca online para apropiarse de los valores.
- En menor medida la colocación de dispositivos físicos conocidos como "pescadores" que tiene el objeto de copiar la información de las tarjetas y la obtención de la claves de validación por medio de teclados falsos, cámaras de filmación, etc; para lograr acceder a las claves del cajero automático conocido como ATM (Automated Teller Machine).

3. ¿Cuáles cree que son los factores de riesgo más recurrentes para que ocurran este tipo de delitos en el ámbito bancario?

En primer lugar, el desconocimiento o exceso de confianza que existe del común del público, cuando recibe una comunicación que dice ser y que en muchas ocasiones aportan información cierta, como nombre, apellido y DNI, y por tanto, por defecto se asume que verdaderamente es esa persona.

En segundo lugar, es importante entender que seguridad y accesibilidad, son características casi excluyentes, por lo tanto mientras más fácil es acceder a un servicio, más fácil podría ser vulnerado y en contraposición mientras más seguro, más engorroso será su acceso. Desde esta perspectiva una entidad complejiza sus sistemas de seguridad cuanto más hechos de inseguridad ocurran, ya que no invertirá recursos en mejoras de sistemas que funcionan de manera correcta o no generan inconvenientes a los clientes.

4. ¿Ha debido intervenir en algún hecho delictivo de este tipo?

Si, en varios hechos de estafas, por medios informáticos, en algunos casos de phishing por correo y últimamente tome conocimiento del incremento de hechos de suplantación de identidad por llamados engañosos y secuestro de la aplicación Whatsapp para pedir dinero en algunos casas y otros para (supuestamente) vender dólares a los contactos de la aplicación de la víctima.

5. ¿Cuáles son los pasos que se siguen para identificar los autores de los hechos delictivos?

Los pasos a seguir son los siguientes:

1- Resguardar la información existente en los medios informáticos, mediante actas de Notariales en los procesos civiles y mediante orden de juez competente en el caso de causas penales. Puede darse también la situación que la víctima se presente de manera espontánea en una dependencia policial (que pueda realizar la medida) en cuyo caso se dará aviso a la autoridad judicial competente quien dispondrá que se presente en sede judicial o que se realice el resguardo de la información, mediante acta que contendrá descripción de los elementos que fueron objeto del procedimiento, los elementos y/o herramientas utilizadas, el resultados de las medidas y los datos que fueron resguardados con su validación correspondientes. Todo ello, con la firma de los presentes.

2- Una vez realizada el resguardo o extracción de la información; se procederá con la orden de la autoridad competente a realizar el análisis de los datos, con el objeto de determinar el origen y la identificación del autor de las comunicaciones y/o acciones realizadas para la comisión del hecho investigado.

3- Se le solicita por medio de oficio de la autoridad judicial competente, a las empresas prestadoras de los servicios analizados (servicio de e-mail, de Internet, de telefonía, de redes sociales, de televisión, o cualquier otro similar) que aporte los datos de registros que se vinculan al hecho a fin de validar o refutar los elementos encontrados en la extracción y análisis anterior.

4- Tareas de explotación de fuentes abiertas de información y verificación de los datos obtenidos en el terreno (con la colaboración de las Unidades Investigativas de jurisdicción) a fin de verificar domicilios, personas y vehículos.

6. ¿Cómo observa la seguridad bancaria para evitar que estos hechos sucedan?

Con la utilización de seguridad biométrica (huella dactilar, facial, etc.) se han visto incrementados los sistemas de control, como la doble validación alfanumérica, la diferencia de pin de ingreso, pin de compra y pin de extracción de efectivo y otras muchas combinaciones; he notado un gran incremento de los sistemas de control y validación de las operaciones. Recientemente se implementaron dos medidas que me resultan interesantes; la primera más flexible, que consiste en realizar una llamada o enviar un mail de validación al correo definido por el usuario, para autorizar una transferencia determinada. Y la segunda, consiste en evitar que determinados usuarios, como los jubilados y otros sectores más vulnerables, puedan realizar operaciones al menos dudosas, como transferencia de grandes volúmenes de dinero y la utilización de algunas tarjetas para compras en línea.

Por otro lado, creo necesario recalcar, que durante un buen periodo de tiempo, los bancos brindan una opción de préstamos pre aprobados que podían ser tramitados por el titular de

la cuenta bancaria o por personas que se apropian de una identidad o que de algún modo manipulan a la víctima para realizar esta tarea, incrementándose los hechos de este modus operandi.

7. ¿Qué acciones ha observado que llevan a cabo las entidades bancarias para proteger a los usuarios y sus datos?

A criterio personal, sin conocimiento técnico específico sobre las tareas realizadas por los responsables del área, puedo mencionar:

- Tarjeta de débito que permite al usuario operar.
- Pin de acceso al sistema.
- Sistemas biométricos de validación de usuario.
- Limitación de montos máximos de transferencias.
- Sistema de validación de operaciones, por mail o por vía telefónica.
- Desde el punto de vista físico, prohibición del uso de telefonía celular en el interior de entidades bancarias.
- Colocación de biombos para impedir la exposición de claves de acceso, etc.

Glosario

Alias: Permite a los usuarios identificar cada una de sus cuentas de manera más sencilla que el CBU. Este Alias puede ser modificado cuando desee el usuario.

API: Significa interfaz de programación de aplicaciones. Las API permiten que sus productos y servicios se comuniquen con otros, sin necesidad de saber cómo están implementados. Esto simplifica el desarrollo de las aplicaciones y permite ahorrar tiempo y dinero.

CBU: Clave Bancaria Única

Cortafuegos: Programas destinados a funcionar como sistema de seguridad para blquear accesos no autorizados a un ordenador, mientras sigue permitiendo la comunicación con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales. Se trata de una de las primeras medidas de seguridad que empezó a implementarse en los ordenadores tras el nacimiento de Internet.

CSS: Cascading Style Sheets, Es lo que se denomina lenguaje de hojas de estilo en cascada y se utiliza para estilizar elementos en un lenguaje de marcado como HTML

CVU: Clave Virtual Uniforme

Fintech: Industria naciente en la que las empresas usan la tecnología para brindar servicios financieros de manera eficiente, ágil, cómoda y confiable. Es una palabra en inglés formada por la contracción de los términos “finance y technology” en inglés.

GPS: El Sistema de Posicionamiento Global (GPS) es un servicio propiedad de los EE. UU. ... El segmento del usuario consiste en el equipo receptor del GPS que recibe las señales de los satélites del GPS y las procesa para calcular la posición tridimensional y la hora precisa.

HTLM: Lenguaje de Marcad de Hipertexto. Es el código que se utiliza para estructurar y desplegar una página web y sus contenidos.

IMEI: International Mobile Station Equipment Indetity (IMEI) es un número que funciona como identificador único de un aparato de telefonía celular.

iOS: Sistema operativo de Apple

JavaScript: es el único lenguaje de programación que funciona en los navegadores de forma nativa (lenguaje interpretado sin necesidad de compilación). Por tanto, se utiliza como complemento de HTML y CSS para crear páginas webs.

Keylogging: Acción de realizar seguimientos en dispositivos móviles mediante la instalación de software o hardware malicioso.

Linkability: Capacidad de rastrear y encontrar

Phishing: Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios.

Pharming: El pharming consiste en disfrazar sitios web falsos como si fueran auténticos para obtener así la información que se introduzca en ellos.

SDK: es el acrónimo de "Software Development Kit" (Kit de desarrollo de software). El SDK reúne un grupo de herramientas que permiten la programación de aplicaciones móviles. Este conjunto de herramientas se puede dividir en 3 categorías: SDK para entornos de programación o sistemas operativos (iOS, Android, etc.)

Skimming: Robo de información de tarjetas de crédito y/o débito utilizado en el momento de la transacción a fin de clonar la información de las tarjetas, para su posterior clonación y uso fraudulento.

Sniffer: Un sniffer es una herramienta de software o hardware que permite al usuario supervisar su tráfico en Internet en tiempo real y capturar todo el tráfico de datos que entran y salen de su equipo.

Spear phishing: Estafa mediante la utilización de correo electrónico, u otro medio de comunicaciones directas, dirigidas a personas, organizaciones o empresas. Roban datos para fines maliciosos o bien se utiliza para la instalación de malware en los dispositivos de las víctimas.

Token: Elemento de seguridad adicional que sirve para confirmar la identidad cuando se realiza una operación a través de la app Móvil o el home banking. La clave cambia

cada 30 segundos y es una clave válida por única vez y para una operación. No genera ningún costo.

URL: Uniform Resource Locator (Localizador de Recursos Uniforme). Dirección de un recurso único en la Web

Bibliografía

Abad, G. (2021). *Análisis de la responsabilidad bancaria en casos de estafas electrónicas mediante redes sociales desde la óptica del derecho de consumo*. Obtenido de Doctrina cosumo: https://www.abogadovergara.com.ar/2021/05/analisis-de-la-responsabilidad-bancaria.html

BCRA. (2021). *Comunicados A, B, C, comunicados de prensa (P) y circulares.* Obtenido de Banco Central de la República Argentina: http://www.bcra.gob.ar/SistemasFinancierosYdePagos/Buscador_de_comunicaciones.asp#:~:text=Tipos%20de%20comunicaciones%20o%20comunicados,P%E2%80%9D%20%7C%20Comunicados%20de%20prensa.

BCRA. (2021). *Entidades financieras de Mendoza.* Obtenido de Banco Central de la República Argentina: http://www.bcra.gob.ar/SistemasFinancierosYdePagos/Entidades_financieras_informacion_estructura.asp?bco=AAA00&tipo=1&Tit=1

BCRA. (s.f.). *Carta Orgánica.* Obtenido de Banco Central de la República Argentina: http://www.bcra.gob.ar/Institucional/Carta_Organica.asp

BCRA. (s.f.). *Home Banking.* Obtenido de Banco Central de la República Argentina: http://www.bcra.gov.ar/BCRAyVos/Preg-Frec-Qu%C3%A9-es-Home-Banking.asp

Fernández, Victor, Lauxmann, Carolina & Tealdo, Julio. (2012). Sisema bancario y de producción en Argentina. *Problemas del desarrollo, 43*(170), 69-99.

Fine, C. (2019). Digitalización financiera: el community banking en la era de la disrupción digital. *PROQUEST, 2*(29), 2-10.

Humanos, M. d. (2021). *¿Qué es un keylogge?* Obtenido de Argentina.gob.ar: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-keylogger

Martínez, J. (2021). *Sistema Bancario.* Obtenido de Diccionario Judicial y Social: https://diccionario.leyderecho.org/sistema-bancario/

Mazzinghi, M. (2015). *Los contratos bancarios en el nuevo Código.* Obtenido de Estudio Mazzinghi Abogados: https://estudiomazzinghi.com.ar/publicaciones/los-contratos-bancarios-en-el-nuevo-codigo/

Mombrú Ruggiero, A.y Margetic, A. (2013). *El hacedor de Tesis.* L.J.C. Ediciones: Buenos Aires.

Nación, B. (2021). *Home Banking Primer Ingreso.* Obtenido de https://www.bna.com.ar/Personas/HomeBanking/PrimerIngreso

Poleri, S. (8 de Febrero de 2021). Ciberdelitos: durante la pandemia hubo más del doble de denuncias que en los tres años previos. *La Nación*.

Productivo, M. d. (29 de junio de 2021). *Comercio Interior multó a entidades bancarias por su responsabilidad frente a las estafas que sufrieron sus clientes.* Obtenido de https://www.argentina.gob.ar/noticias/comercio-interior-multo-entidades-bancarias-por-su-responsabilidad-frente-las-estafas-que

Productivo, M. d. (Agosto de 2021). *Informe de denuncias. Defensa al consumidor.* Obtenido de https://www.argentina.gob.ar/sites/default/files/informe_de_reclamos_2021.pdf

Rojas Poblete, C. (2016). Evaluación de la seguridad de aplicaciones móviles bancarias. *Tesis de Maestría en Ciencias. Mención en computación*. Santiago de Chile: Universidad de Chile. Facultad de Ciencias Físicas y Matemáticas. Departamento de Ciencias de la Computación.

Techlandia. (s.f.). *Diez delitos cometidos por medio de redes sociales.* Obtenido de https://techlandia.com/10-delitos-cometidos-medio-redes-sociales-galeria_378067/

UFECI. (Septiembre de 2021). Unidad Fiscal Especializada en Ciberdelincuencia. *Ministerio Público Fiscal*. Ministerio Público Fiscal. Obtenido de Ministerio Público Fiscal.

Valleboni, C. (13 de Marzo de 2021). *¿Y después qué? El desafío de los bancos tras la digitalización de sus clientes.* Obtenido de https://www.forbesargentina.com/negocios/y-despues-que-desafio-bancos-tras-digitalizacion-sus-clientes-n5302

Vernengo, I. (2020). Adecuación de la seguridad bancaria a raíz de la pandemia. *Innovación. Seguridad. Análisis y Tendencias*.

Vives, X. (2019). La banca frente a la disrupción digital. *PROQUEST, 1*(14), 20-46.

Westreicher, G. (25 de Julio de 2020). *Sistema Bancario.* Obtenido de https://economipedia.com/definiciones/sistema-bancario.html

Zarich, M. (2021). *La pandemia obligó al sistema bancario a acelerar procesos de digitalización.* Obtenido de Bancos y Seguros: https://www.nbsbancosyseguros.com/la-pandemia-obligo-al-sistema-bancario-a-acelerar-procesos-de-digitalizacion-martin-zarich/

Índice

ÍNDICE DE GRÁFICOS, IMÁGENES Y TABLAS