- 2023 -

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023

—

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

- 2023 -

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023

—

UFECI | Unidad Fiscal Especializada
en Ciberdelincuencia

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023

Diseño: Dirección de Comunicación Institucional
Edición: Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

Edición: diciembre 2023

Índice

INTRODUCCIÓN

La Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) fue creada en noviembre del año 2015[1], con el objetivo de fortalecer la política criminal contra el cibercrimen, intensificar las tareas para su abordaje de modo articulado y atender a sus especificidades.

Desde aquel entonces, hemos iniciado investigaciones preliminares y asistido a los magistrados en sus casos en más de cuatro mil quinientas oportunidades -en el marco de alrededor de tres mil casos distintos- y recibimos más de cuarenta y cinco mil consultas de particulares en nuestras casillas de correo electrónico por temas relacionados con nuestra especialidad.

La información provista en el marco de aquellas consultas y casos se consolidó como un insumo fundamental para la observación y el análisis de la particular evolución de la criminalidad informática. Ello nos ha ayudado, a lo largo de los años, a perfeccionar nuestra actuación bajo un paradigma de persecución penal estratégica, comprensivo de las tendencias criminales, sus alcances y su impacto en la sociedad, permitiéndonos de ese modo afianzar nuestra actividad vinculada a la elaboración y la tramitación de investigaciones preliminares.

El análisis de la información ha sido sumamente valioso también a la hora de diagramar las diferentes capacitaciones brindadas por la Unidad, impulsar campañas de prevención para la ciudadanía y generar documentos técnicos, de difusión interna, para una mejor comprensión del fenómeno que nos ocupa.

En este sentido, en el mes de septiembre de 2021 publicamos un informe elaborado a partir de las consultas y situaciones reportadas por particulares durante el primer año de la pandemia del COVID-19[2]. El estudio puso en evidencia que dicho contexto, atravesado por diferentes medidas de aislamiento y distanciamiento social, trajo consigo una disrupción en la actividad ligada a la cibercriminalidad: aun cuando el número de casos y reportes exhibía año tras año un crecimiento significativo, entre los meses de abril de 2020 y marzo de 2021, la cantidad de consultas se quintuplicó.

Tras haber procesado la información recolectada hasta el mes de marzo de 2023, nos encontramos ahora en condiciones de elaborar un nuevo documento, respetando la metodología aplicada en aquella ocasión, con el que pretendemos graficar el panorama general de las tipologías detectadas y sus variaciones, como así también, darle seguimiento a las distintas apreciaciones e hipótesis presentadas en aquel estudio primigenio.

1. https://www.mpf.gov.ar/resoluciones/pgn/2015/PGN-3743-2015-001.pdf
2. https://www.mpf.gob.ar/ufeci/files/2021/09/UFECI_informe-pandemia.pdf

I. EVOLUCIÓN DEL FENÓMENO DEL CIBERCRIMEN A LA LUZ DE LOS REPORTES RELEVADOS

Al analizar el volumen total de reportes recibidos, pudimos confirmar que la tendencia al alza relevada en periodos previos se mantuvo. Como se mencionó en el informe previo, en los doce meses anteriores a la pandemia, es decir, entre abril de 2019 y marzo de 2020, la Unidad fue contactada por particulares a través de nuestras casillas de correo electrónico en 2.581 ocasiones, mientras que, en el periodo comprendido entre los meses de abril de 2020 y marzo de 2021, el número ascendió a 14.583 (un 465% de aumento).

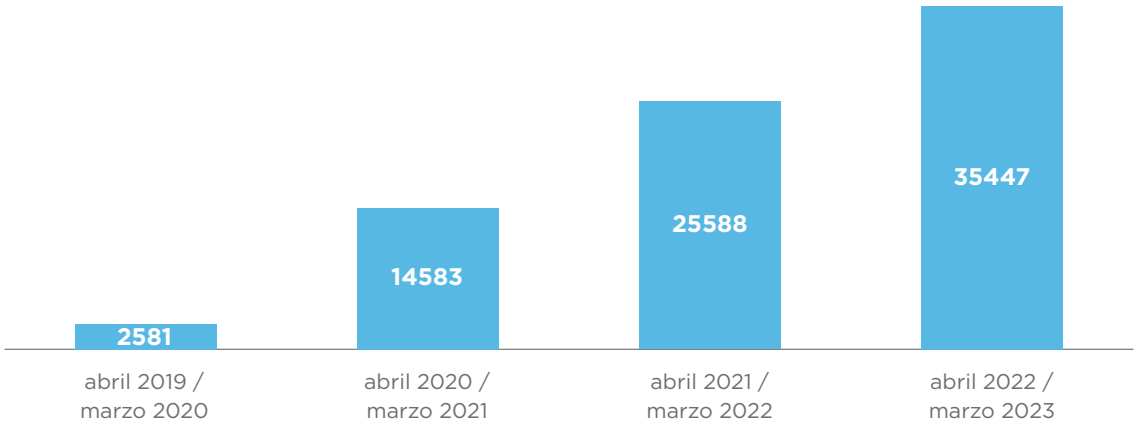
Producto de la evolución de la situación epidemiológica, las diferentes medidas de aislamiento y distanciamiento fueron variando. Más allá de algunos periodos puntuales en los que las medidas se reforzaron, un repaso a la distancia nos permite constatar que en los últimos meses del año 2021 comenzó un proceso paulatino de flexibilización que trajo aparejado que el año 2022 transcurriera con escasas restricciones de ese tenor.

En el informe precedente concluimos que parte del aumento de reportes detectado podía responder a las diferentes alteraciones que las medidas de aislamiento produjeron en los hábitos de las personas, mientras que otra porción era producto del crecimiento que se viene observando año tras año, a nivel global, con relación a los crímenes cometidos mediante el uso de dispositivos informáticos. Nos parecía poco probable, no obstante, que el grado de adopción de las nuevas tecnologías por parte de los ciudadanos para realizar diferentes actividades cotidianas pudiera retornar a los niveles anteriores a la pandemia.

En efecto, las nuevas tecnologías suelen proponer una mejora en la experiencia de los usuarios para realizar actividades de distinta naturaleza, sin embargo, su uso suele requerir de un proceso previo de aprendizaje y adaptación que puede operar como una barrera en su adopción. Sorteado dicho proceso, se reducen las razones para no optar por su uso. Pero, además, durante los últimos años, diversas empresas, profesionales y organismos implementaron nuevos canales de atención y provisión de servicios a través de desarrollos tecnológicos, incrementando así el catálogo de actividades que los ciudadanos pueden llevar a cabo por ese tipo de plataformas.

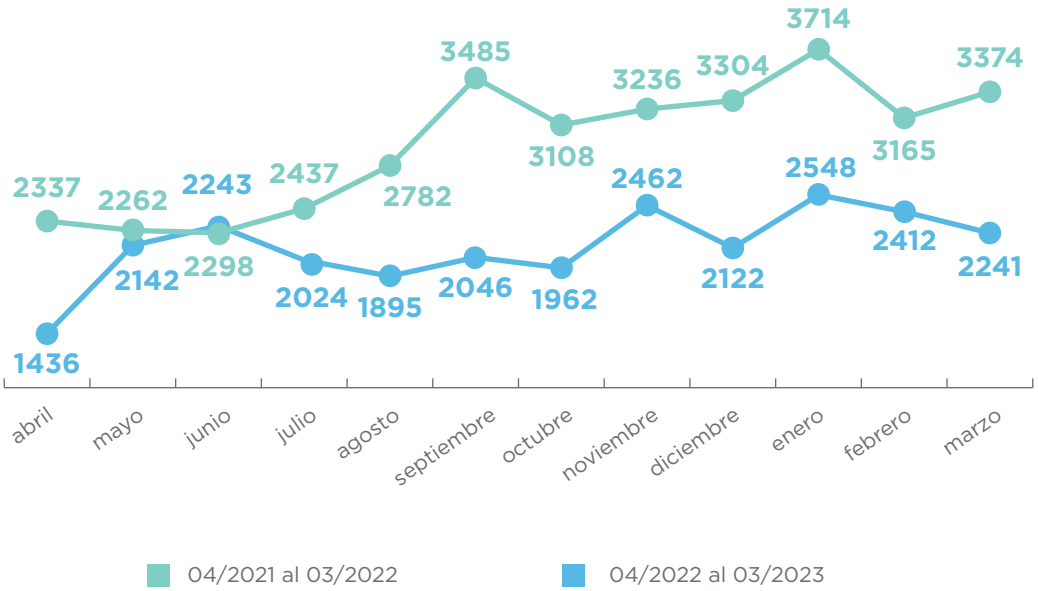
Los números reflejan que, lejos de reducirse, los reportes aumentaron significativamente. Entre los meses de abril de 2021 y marzo de 2022, se recibieron un total de 25.588, es decir, un 75,5% más que en el periodo previamente analizado, mientras que, entre los meses de abril de 2022 y marzo de 2023, se recibieron 35.447 reportes, lo que constituye un aumento del 38,5% con respecto al anterior.

Reportes recibidos por período de doce meses



Es posible, no obstante, advertir cierta incidencia del grado de aislamiento de la sociedad en el número de reportes recibidos. En efecto, aún verificándose un aumento año tras año, el porcentaje de crecimiento tendió a la baja luego del abrupto ascenso detectado en los primeros doce meses de la pandemia. A su vez, al observar la evolución mensual, pudimos verificar una variación significativa en el mes de mayo de 2021, que se tradujo en un aumento del 49% en el número de consultas recibidas con respecto al mes previo. Se descarta que se trate de un aumento por motivos estacionales, en tanto no se detectó un correlato de dicha variación en el periodo siguiente.

Reportes recibidos por mes



Al evaluar las particularidades del contexto que se atravesaba en el país para ese entonces, nos encontramos con que el 8, el 16 y el 30 de abril de 2021, se dictaron los Decretos 235/2021, 241/2021 y 287/2021, a través de los cuáles se dispusieron diferentes medidas tendientes a disminuir los niveles de circulación de la ciudadanía y evitar aglomeraciones, para de ese modo hacer frente a lo que se identificó como una segunda ola de contagios de COVID-19. Poco después, el 22 de mayo de 2021, se dictó el Decreto 334/2021, por medio del cual se agravaron las restricciones en ciertos puntos del territorio nacional considerados de "alto riesgo" hasta el 30 de mayo de ese año. Tras ello, se prorrogaron las disposiciones contempladas en los primeros tres decretos hasta el 6 de agosto de 2021.

Más allá de esta hipotética relación entre el grado de aislamiento y cantidad de reportes recibidos, lo cierto es que, tal como se aclaró en el informe precedente, ello podría responder también en parte a que las dificultades para realizar consultas de manera presencial constriñen a la ciudadanía a utilizar en reemplazo medios electrónicos de contacto, y así, en vez de acercarse a una sede policial, fiscal o judicial para realizar sus consultas con relación a posibles maniobras delictivas podrían haber optado en mayor medida por enviar un correo electrónico a nuestra Unidad.

Consideramos, no obstante, que las medidas de aislamiento y distanciamiento dispuestas con motivo de la pandemia generaron cambios más profundos en los hábitos de la sociedad. Particularmente, se aceleró la adopción de las nuevas tecnologías y, de la mano de ello, el uso de plataformas virtuales para la contratación y el pago de servicios; para la adquisición de bienes y para la realización de trámites de diferente naturaleza. Y así como el número de casos asociados a la criminalidad informática aumentó con el paso de los años, en una suerte de relación directa con el proceso de tecnologización de la sociedad, es de esperar que, frente a una agudización de este proceso, el crecimiento de la criminalidad asociada a aquél se agudice también.

Encuentra sentido entonces que los casos atravesados por aspectos informáticos hayan aumentado significativamente desde el inicio de la pandemia, y así, que el considerable aumento observado en el número de consultas recibidas en la Unidad responda también, aunque más no sea parcialmente, a dicho factor.

II. INVESTIGACIONES PRELIMINARES Y SOLICITUDES DE ASISTENCIA

El aumento en el número de reportes impactó también en nuestra labor asociada al inicio y la tramitación de investigaciones preliminares. En términos netos, el número de investigaciones iniciadas entre los meses de abril de 2021 y marzo de 2022 no varió sustancialmente en comparación con el periodo anterior. En aquella ocasión el número de investigaciones preliminares ya había aumentado considerablemente -un 77,3% en comparación con los doce meses previos-, alcanzando los 289 casos, mientras que, en el periodo mencionado ese número se redujo a 287. Sin embargo, entre los meses de abril de 2022 y marzo de 2023 el número de investigaciones preliminares iniciadas aumento hasta alcanzar un total de 353, lo que equivale a un 23% más que en el periodo previo.

Ahora bien, en el último tiempo, el procesamiento y análisis de los reportes nos permitió identificar un gran número de conductas que derivaron en afectaciones masivas, con decenas o incluso centenas de víctimas. Aquellos casos requirieron de un abordaje estratégico que involucró, entre otras medidas, la identificación de reportes relacionados para poder así reunirlos en un único caso, sistematizar la información provista y someterla a procesos de análisis y entrecruzamiento que nos permitieran extraer nuevos datos y conclusiones que colaboren en el esclarecimiento de los casos y la identificación de sus autores.

A modo de ejemplo, detectamos una serie de reportes que daban cuenta de una maniobra vinculada a los servicios de mensajería "puerta a puerta", en los que se les solicitaba a las víctimas, por medio de un correo electrónico que impostaba a la empresa "Correo Argentino", el depósito de sumas de dinero para liberar supuestas entregas, por lo que se invitó a la ciudadanía a través del portal institucional a

comunicarse con la Unidad en caso de haber sido víctima de dicho accionar[3]. Al momento de formular la denuncia contabilizamos un total de 153 damnificados.

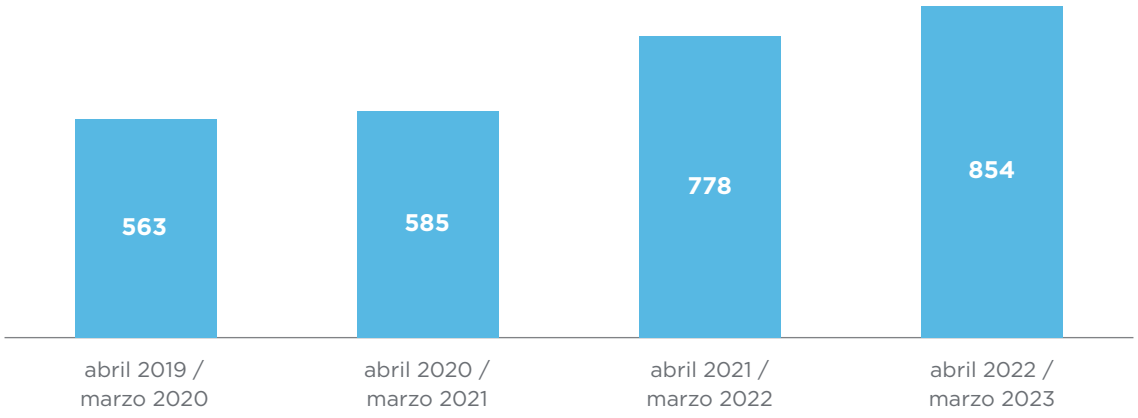
En otros casos, la vinculación entre las maniobras no fue tan evidente desde el comienzo, sin embargo, la identificación de ciertos puntos en común entre algunos de los reportes y la sistematización de la información provista nos permitió confirmar la relación e identificar un número mayor de damnificados que, en definitiva, habrían sido víctimas de maniobras llevadas a cabo por un mismo grupo de personas.

Por mencionar uno de estos supuestos, entre comienzos y mediados del año 2021 comenzamos a relevar un gran número de casos de fraudes caracterizados por un *modus operandi* similar, en los cuales los autores montaban perfiles en la red social Instagram y páginas web de *e-commerce* para captar víctimas, a las que se invitaba a realizar transferencias de dinero para el pago de supuestos productos que se ofrecían a la venta, los cuáles finalmente no eran entregados. Entre los meses de abril de 2021 y marzo de 2022, iniciamos 14 investigaciones preliminares por esta clase de hechos, en el marco de los cuales identificamos, entre los reportes recibidos, un total de 576 víctimas.

En lo que respecta a las solicitudes de asistencia cursadas a la Unidad por Fiscalías y Juzgados Federales de todo el país, por Fiscalías y Juzgados Nacionales con jurisdicción en la Ciudad Autónoma de Buenos Aires y por las Procuradurías, Unidades Fiscales y demás áreas de la Procuración General de la Nación, se pudo observar un crecimiento. Entre los meses de abril de 2021 y marzo de 2022 contabilizamos 778 intervenciones de este tipo, es decir, un aumento del 33% mientras que, entre los meses de abril de 2022 y marzo de 2023 se nos solicitó asistencia en 854 oportunidades, lo que se traduce en un aumento del 9,8% con respecto a los doce meses anteriores.

3. https://www.fiscales.gob.ar/ciberdelincuencia/advierten-sobre-maniobras-de-fraude-electronico-por-suplantacion-de-identidad-vinculadas-a-los-servicios-puerta-a-puerta-del-correo-argentino/

Asistencias



Lo expuesto no hace más que reafirmar que la criminalidad se encuentra atravesada cada día más por el desarrollo tecnológico, en tanto las diferentes dependencias fiscales y judiciales encuentran cada vez más necesaria la intervención de la Unidad para el abordaje de aspectos de la investigación ligados a nuestra *expertise*.

III. ANÁLISIS DE LAS MODALIDADES Y TENDENCIAS IDENTIFICADAS A PARTIR DE LOS REPORTES

Nos adentraremos a continuación en el análisis de los reportes en particular. Cabe destacar que, a la hora de procesar los mensajes recibidos, se respetó la metodología descripta en el informe primigenio. Cada conversación fue leída y etiquetada en función de uno o más aspectos característicos de las maniobras puestas en conocimiento en cada ocasión. Estas etiquetas fueron ideadas partiendo de diferentes aspectos que consideramos relevantes, de acuerdo a la materia que nos ocupa. Las denominaciones guardan una relación directa con aspectos jurídico-penales, con las plataformas o empresas que han sido utilizadas o se han visto involucradas de algún modo en la maniobra, aunque también con otras particularidades como, por ejemplo, el *modus operandi*. A su vez, distinguimos aquella etiqueta que consideramos central según cada caso, a la que nos referiremos en adelante como "modalidad principal" (por ejemplo, "fraude en línea"), para distinguirla de las restantes, a las que denominaremos "modalidades secundarias" ("fraudes en compras", "fraudes bancarios", etc.).

Repasamos a continuación los lineamientos sobre los cuales se le asignaron a los reportes las etiquetas que se mencionarán a lo largo del documento:

Fraude en línea: maniobras en las que se ataca el patrimonio de las víctimas mediante el despliegue de un ardid o engaño, abusando de su confianza o a través de técnicas de manipulación informática que alteran el normal funcionamiento de un sistema informático o la transmisión de datos, es decir, posibles estafas o defraudaciones en los términos establecidos en nuestro ordenamiento penal[4].

Fraude relacionado con compraventas: maniobras fraudulentas -en los términos definidos precedentemente- que involucran, en particular, un falso ofrecimiento de productos y servicios para la venta o que son desplegadas a los efectos de hacer incurrir en error a alguna de las partes de una operación legítima, para captar así los pagos de las víctimas. En el entorno digital, suele llevarse a cabo mediante páginas o perfiles en redes sociales en los que se ofrecen los productos y servicios, pudiendo tratarse de falsos emprendimientos o de imitaciones de páginas y perfiles de compañías existentes, desde las cuáles engañan a las víctimas y les brindan las indicaciones para formular los pagos perjudiciales.

Fraude bancario o relacionado con plataformas de homebanking: maniobras fraudulentas -en los términos definidos anteriormente- que involucran, en particular, un acceso ilegítimo a las cuentas de las plataformas de banca online de las víctimas, previa obtención de las credenciales necesarias por medio de un ardid o engaño o mediante técnicas de manipulación informática, y la subsiguiente realización de transferencias y/u otro tipo de operaciones en perjuicio de sus titulares.

4. Libro Primero, Título VI, Capítulo IV del Código Penal de la Nación

Phishing: maniobras tendientes a la obtención de información confidencial de terceros, mediante técnicas de ingeniería social que involucran correos electrónicos, sitios web o perfiles en redes sociales engañosos, en los que los autores se hacen pasar por terceros.

Acceso ilegítimo: maniobras por medio de las cuales se accede por cualquier medio a un dato o un sistema informático de acceso restringido, sin la debida autorización o excediendo la que se posee, lo que incluye el ingreso a cuentas ajenas de correo electrónico, redes sociales o de otra naturaleza que cuenten con medidas de seguridad para poder ingresar.

Usurpación de identidad: maniobras por medio de las cuales los autores se hacen pasar por un tercero, usualmente mediante la creación de direcciones de correo electrónico, sitios web, perfiles en redes sociales y plataformas de mensajería que aparentan pertenecer a las víctimas. Este tipo de maniobras pueden estar relacionadas con algún supuesto de hostigamiento o acoso digital o como medio comisivo de un fraude.

Ransomware: maniobras llevadas a cabo mediante la ejecución de un programa informático malicioso en la/s terminal/es afectada/s, el cual encripta una variedad de archivos que se supone resultan de interés para la víctima, tras lo cual, se le exige a la víctima -por lo general, a través de un mensaje que se despliega en los propios dispositivos afectados- el pago de una suma de dinero, usualmente, en Bitcoin u otro criptoactivo, para recibir así la clave y las indicaciones para desencriptar los archivos.

Acoso: maniobras tendientes a hostigar o provocar algún tipo de malestar en un tercero. En el entorno digital, suele llevarse a cabo a través del envío reiterado de mensajes privados o públicos, por medio de publicaciones en múltiples plataformas y redes sociales y a través de cuentas falsas.

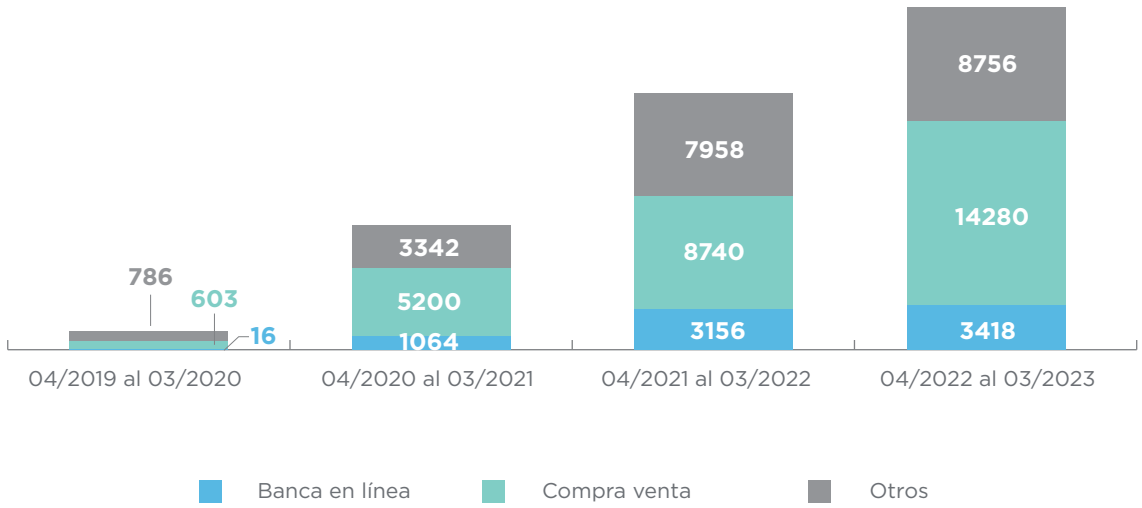
Difamaciones: maniobras tendientes a afectar el prestigio, la dignidad o la reputación de un tercero. En el entorno digital, suele llevarse a cabo mediante el envío de mensajes a múltiples destinatarios o a través de publicaciones en múltiples plataformas y redes sociales, o a través de cuentas falsas en las que se hacen pasar por la víctima, y en particular, mediante el envío o la publicación de imágenes íntimas de la víctima sin su consentimiento.

Aclarado ello, lo primero que se destaca es la dominancia de los casos de fraude. En los doce meses comprendidos entre abril de 2021 y marzo de 2022, el número de reportes que recibieron dicha etiqueta a título de modalidad principal o secundaria ascendió a 19.854, de los cuales 3.156 correspondían a casos ligados a plataformas de banca electrónica, mientras que otros 8.740 correspondían a fraudes relacionados con operatorias de compraventa. El aumento en los casos de fraude, en comparación con los doce meses previos, fue de un 106,7%.

El número se acrecentó en los meses siguientes, en tanto entre abril de 2022 y marzo de 2023 los reportes por fraudes ascendieron a 26.454, es decir, un 33,2% de aumento. Sobre estos reportes,

aquellos vinculados a compraventas totalizaron 14.280, mientras que los que se relacionaron con la banca electrónica alcanzaron un total de 3.418. Cabe destacar que los supuestos de fraude constituyeron, respectivamente, el 77,6% y el 74.6% del total de casos relevados a partir de los reportes recibidos en los dos últimos periodos bajo análisis, lo que denota una clara dominancia.

Fraude en línea



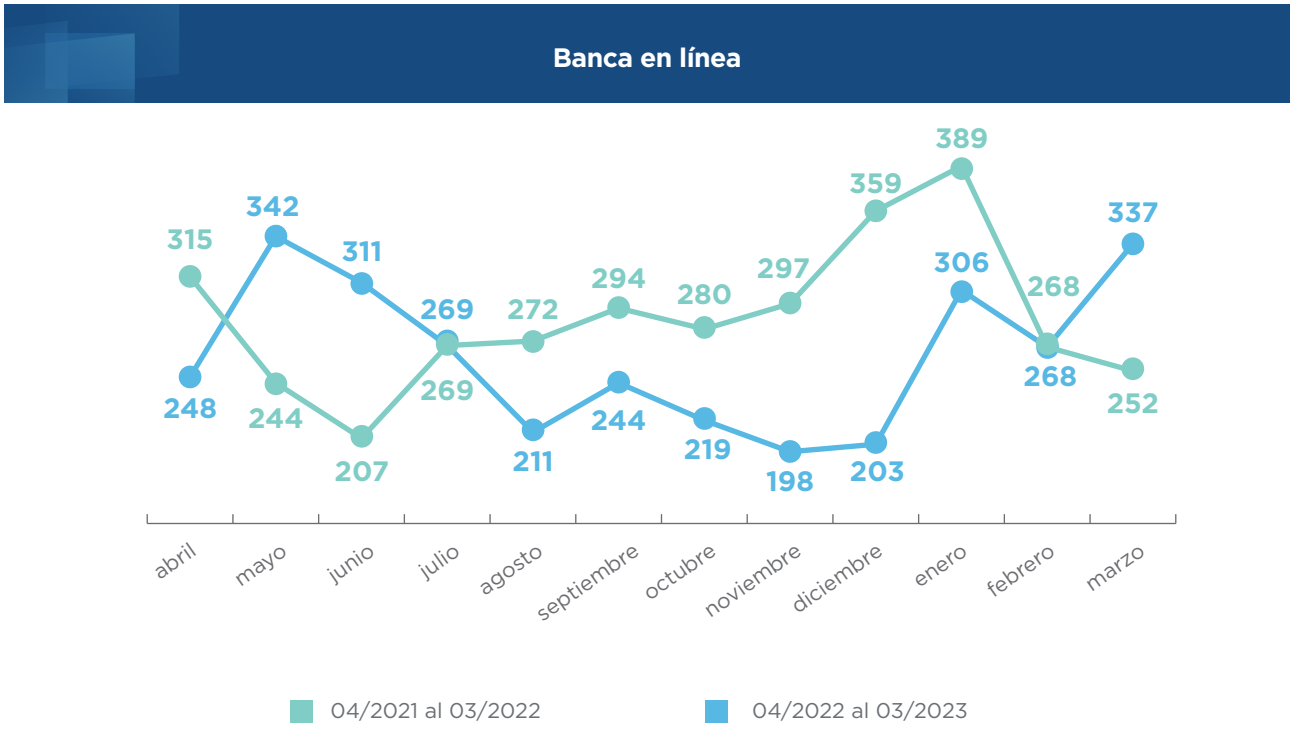
Las maniobras asociadas a compraventas continúan ocupando un espacio central entre los reportes. Al dar cuenta de algunas de las investigaciones preliminares iniciadas en la Unidad, en las que concentramos a un gran número de víctimas, retratamos el esquema con el que suelen llevarse a cabo, como así también, el modo diferencial en el que abordamos esta problemática, en función del volumen de casos y las relaciones que hemos podido detectar.

Por otra parte, los casos de fraude ligados a la banca en línea presentan fluctuaciones que vale la pena mencionar.

Es posible concluir que el periodo comprendido entre los meses de abril de 2021 y marzo de 2022 se constató un aumento considerable en el total al compararlo con el periodo previo, un 196,6% para ser precisos. Sin embargo, al comparar dicho periodo con aquél comprendido entre los meses de abril de 2022 y marzo de 2023, se advierte que la suba para este último fue marcadamente inferior (un 8,3%), menor incluso en comparación con el aumento en el número de reportes totales y específicamente de casos de fraude.

Se observa que luego de alcanzar un pico en el mes de mayo de 2021, los valores fueron disminuyendo

progresivamente hasta la llegada del mes de agosto de 2021, inclusive. Y lo cierto es que en los sucesivos meses los valores permanecieron por debajo de aquel alcanzado en mes de mayo, con los meses de diciembre de 2021 y enero de 2022 como únicas excepciones.



Si bien no se descarta la injerencia de otros factores, la merma parece coincidir con ciertos eventos que visibilizaron y abordaron una problemática relacionada con un *modus operandi* que, en función de nuestra clasificación, recae bajo dicha etiqueta.

En concreto, los autores lograban acceder a cuentas de *homebanking* de terceros, mediante credenciales obtenidas previamente a través del despliegue de técnicas de ingeniería social, y desapoderaban a sus titulares de los fondos realizando transferencias a otras cuentas. Se detectó que en múltiples ocasiones, antes de sustraer los fondos, los autores conseguían abultar las cuentas mediante la solicitud de préstamos preaprobados, ofrecidos por los bancos a través de la misma plataforma, que eran acreditados de manera inmediata.

Si bien la modalidad en cuestión fue ampliamente abordada por los medios de comunicación a lo largo de los meses, adquirió un mayor protagonismo frente al dictado de resoluciones judiciales y administrativas. En este sentido, en el mes de mayo de 2021, desde el portal institucional de este Ministerio Público Fiscal se comunicó la opinión formulada por titular de la Unidad en torno al recurso interpuesto por una entidad bancaria con motivo de una medida cautelar concedida a favor

de la víctima de una maniobra de esta naturaleza[5]. En la ocasión, se brindaron además una serie de recomendaciones para evitar ser víctima de este tipo de hechos.

El 24 de junio de 2021 salió a la luz la multa aplicada por la Subsecretaría de Acciones para la Defensa de las y los Consumidores, dependiente de la Secretaría de Comercio Interior de la Nación, a dos entidades financieras por haber incumplido su obligación de garantizar la seguridad en cuanto a la protección de datos personales, cuentas e intereses económicos de sus clientes, y por no asumir la responsabilidad ante aquéllos[6].

Poco después, el 1 de julio de 2021, el Banco Central de la República Argentina publicó la comunicación "A" 7319[7], en la que se establecieron nuevos requisitos para el otorgamiento de créditos a través de canales electrónicos. Las entidades financieras fueron conminadas a verificar fehacientemente la identidad de las personas que los solicitan, a monitorear y controlar los puntos de contacto indicados por el usuario y comprobar que no hayan sido modificados recientemente. Se indicó que la verificación debía efectuarse mediante técnicas de identificación positiva y que, cumplido ello, la entidad debía comunicarle al cliente que el crédito se encontraba aprobado y que, de no mediar objeciones, el monto será acreditado en su cuenta a partir de las 48 horas hábiles siguientes.

Más allá de lo señalado, en los sucesivos meses se detectaron una serie de campañas dirigidas a obtener mediante engaño las credenciales de usuarios de plataformas de banca electrónica. El análisis de los reportes fue de suma utilidad a los efectos de advertir y adoptar las medidas de prevención a nuestro alcance para intentar reducir el impacto y las potenciales víctimas de aquellas maniobras, concretamente, motivó el lanzamiento de sendas alertas por medio de las plataformas de comunicación del Ministerio Público Fiscal de la Nación[8].

El contacto constante con la ciudadanía a través de los reportes nos permitió advertir que, al tiempo que los casos mencionados disminuían, otras modalidades comenzaban a crecer. En particular, se constató un crecimiento considerable en los casos de fraude cometidos mediante usurpación de identidad. En el periodo comprendido entre los meses de mayo y julio de 2021 -el mismo periodo en el que se detectó una tendencia bajista en los casos que involucraban plataformas de banca electrónica-, se pasó de 84 reportes a 280, un aumento del 233,3%. El aumento se sostuvo durante el periodo abarcado por los meses de abril de 2022 y marzo de 2023, en tanto el periodo cerró con 491 reportes mensuales, habiendo alcanzado en el mes de noviembre de 2022 un pico de 522.

---

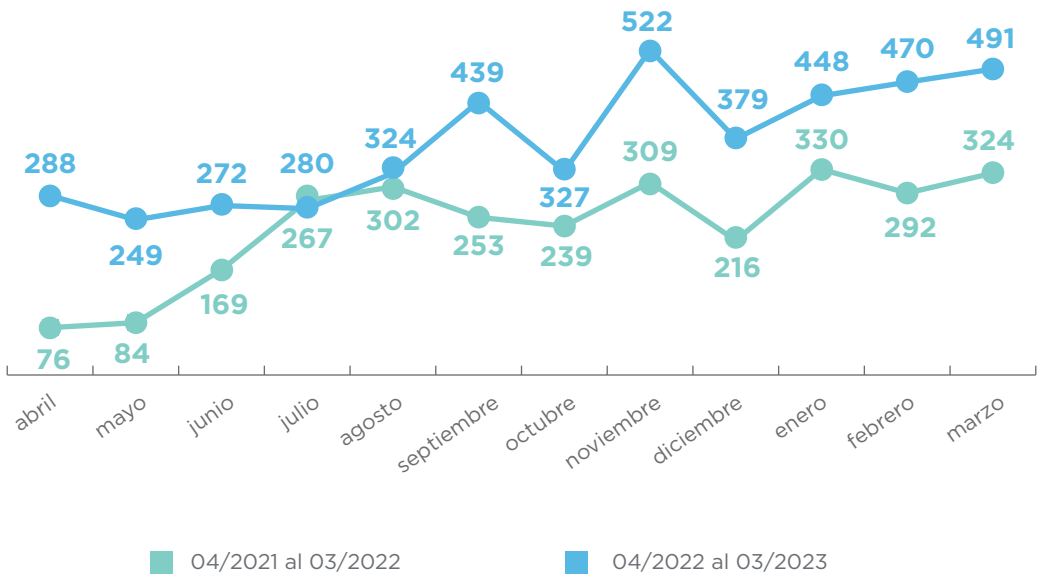
5. https://www.fiscales.gob.ar/ciberdelincuencia/piden-que-se-confirme-una-medida-cautelar-que-ordeno-al-banco-nacion-suspender-el-cobro-de-un-credito-generado-mediante-una-ciberestafa/

6. https://www.argentina.gob.ar/noticias/comercio-interior-multo-entidades-bancarias

7. http://www.bcra.gov.ar/pdfs/comytexord/A7319.pdf

8. https://www.fiscales.gob.ar/ciberdelincuencia/advierten-sobre-una-maniobra-para-apoderarse-de-cuentas-de-clientes-del-banco-de-galicia-mediante-mensajes-fraudulentos-por-correo-electronico/; https://www.fiscales.gob.ar/ciberdelincuencia/advierten-sobre-una-maniobra-fraudulenta-para-apoderarse-de-cuentas-de-clientes-del-banco-provincia/.

Usurpación de identidad



La mayoría de los casos observados giraban en torno a cuentas de plataformas de mensajería, en particular, de WhatsApp. Se constataron sin embargo dos variantes de esta clase de conductas: por un lado, los autores se hacían pasar por terceros utilizando cuentas asociadas a números telefónicos distintos a los de las personas cuya identidad suplantaban, aunque copiando su imagen de perfil. En otros casos, la maniobra gozaba de otro nivel de sofisticación, en tanto los autores lograban acceder en forma ilegítima a las cuentas cuya identidad suplantarían. Tras ello, interactuaban con sus contactos y solicitaban transferencias a cuentas bancarias o billeteras virtuales con diferentes excusas.

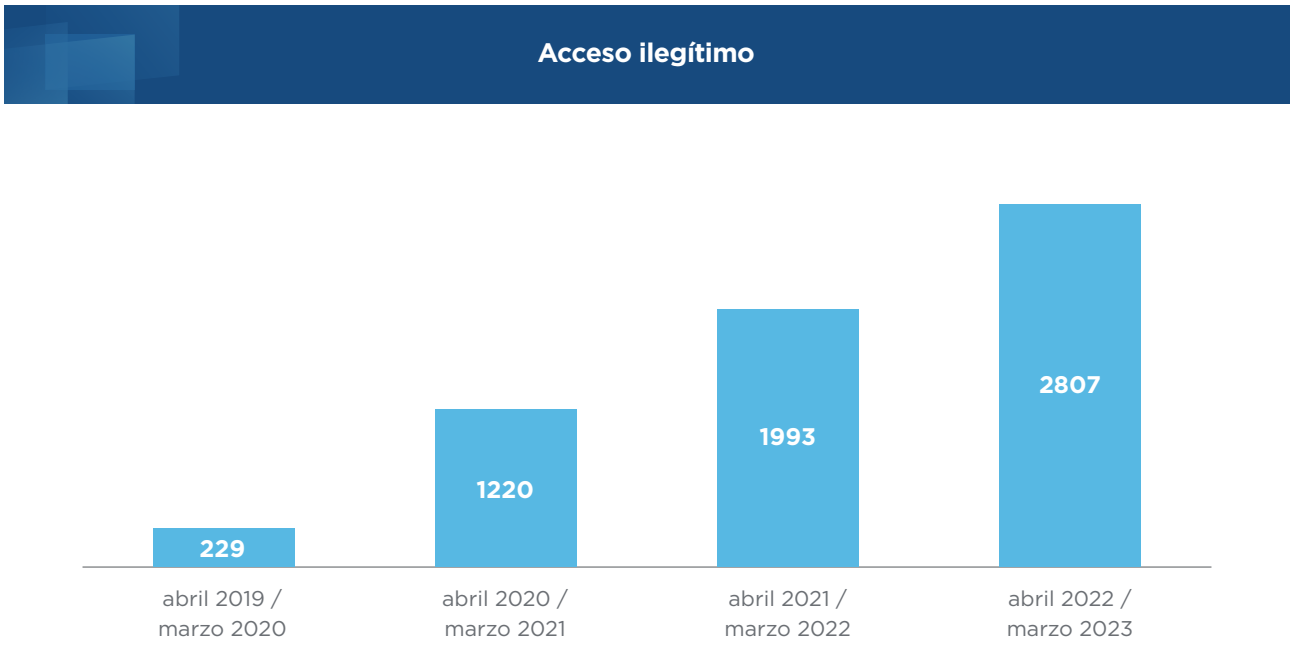
En virtud de ello, desde la unidad se realizaron diferentes campañas de concientización para la ciudadanía en general, incluyendo una serie de recomendaciones para evitar ser víctimas de este tipo de maniobras[9]. Paralelamente, se realizó una capacitación para los miembros de este Ministerio Público Fiscal a fin de dotarlos de información y las herramientas útiles para el abordaje de las correspondientes investigaciones[10].

Enfocándonos en los reportes que involucraron específicamente accesos ilegítimos a cuentas -como modalidad secundaria-, pueden formularse múltiples apreciaciones. Para empezar, el volumen de casos relevados confirmó una tendencia al alza que ya había sido anticipada en el informe primigenio. En efecto, en los doce meses previos al inicio de la pandemia se habían individualizado 229 reportes

9. https://www.fiscales.gob.ar/ciberdelincuencia/la-ufeci-advierte-sobre-nuevas-maniobras-fraudulentas-dirigidas-a-tomar-el-control-de-las-cuentas-de-whatsapp-con-falsos-turnos-de-vacunacion/

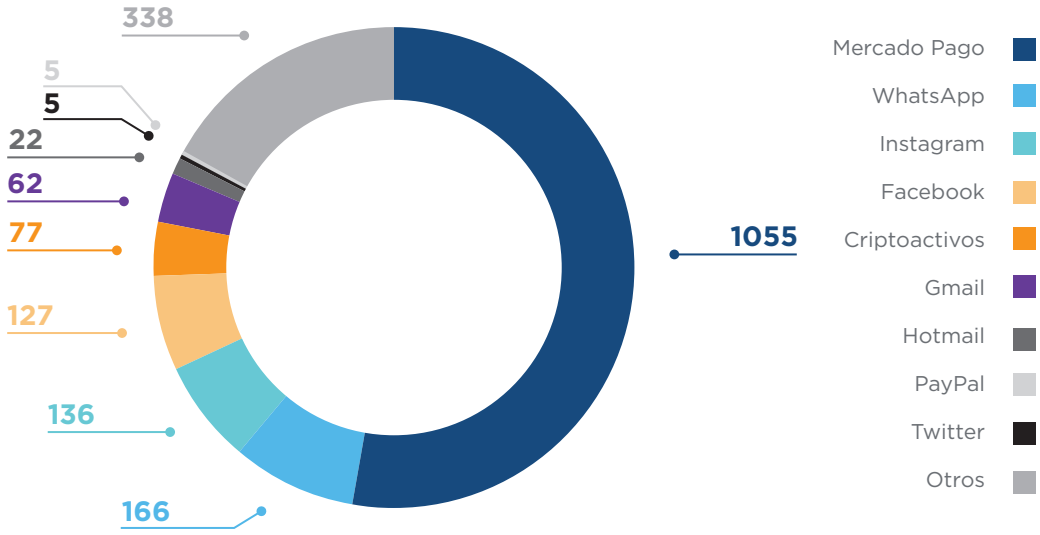
10. https://www.fiscales.gob.ar/ciberdelincuencia/la-ufeci-y-whatsapp-capacitaron-a-personal-judicial-y-del-mpf-frente-a-las-maniobras-fraudulentas-para-tomar-control-de-las-cuentas-de-mensajeria/

de esta naturaleza, mientras que en los doce meses que le siguieron el número aumentó a 1.220. En el periodo que va desde abril de 2021 hasta marzo de 2022 dicho número ascendió a un total de 1.993, una variación del 63.3%, mientras que, en los doce meses siguientes, se relevaron 2807 reportes, un aumento del 40,8%.



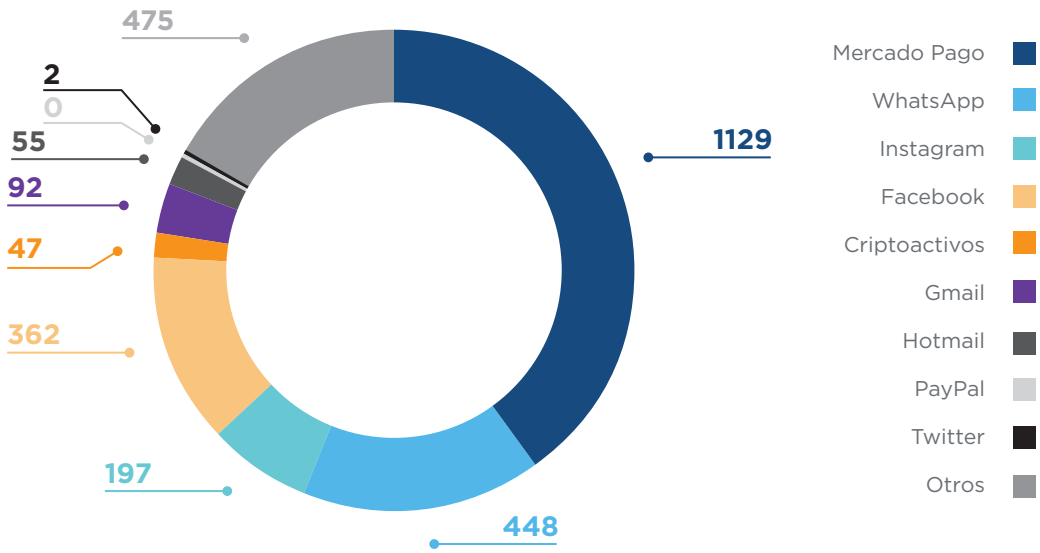
Al segregar la información relativa a este tipo de casos, pudimos determinar que, entre los meses de abril de 2021 y marzo de 2022, la mayoría de ellos -más de la mitad- guardaron relación con plataformas que brindan servicios de billetera virtual, concretamente, cuentas de Mercado Pago.

Abril de 2021 a Marzo de 2022



Y lo mismo pudo comprobarse al analizar el periodo siguiente, en tanto las cuentas de Mercado Pago habrían sido el servicio con mayores registros de accesos ilegítimos a partir de los reportes. Sin embargo, puede verse cómo los accesos a cuentas de WhatsApp se incrementaron significativamente, pasando de 166 casos a 448, un 169,9% más.

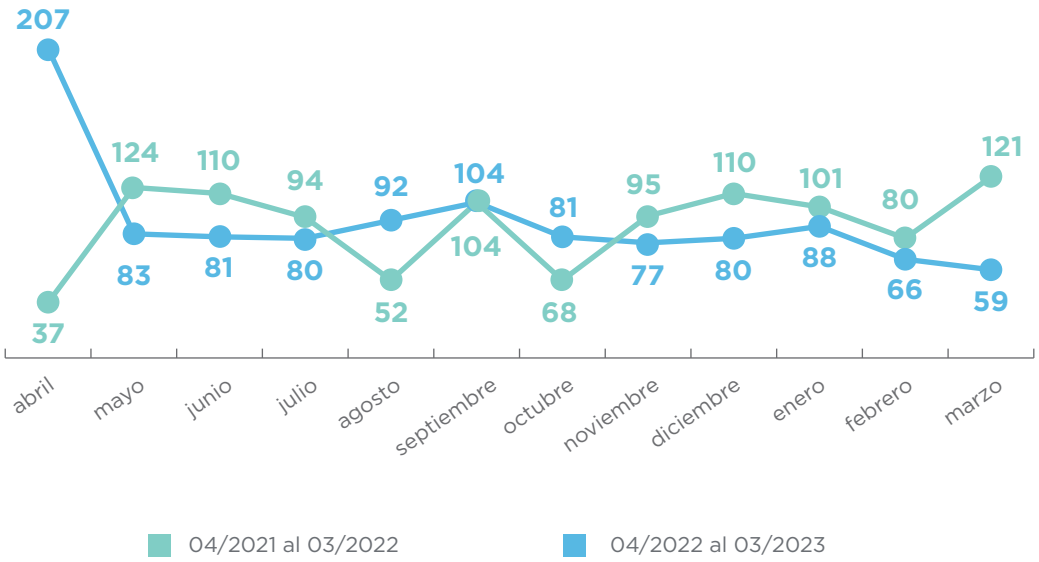
Abril de 2022 a Marzo de 2023



Cabe señalar que los accesos a esta clase de cuentas relevados a través del análisis de los reportes, como así también, a cuentas vinculadas al uso de criptoactivos, habrían involucrado además de la intromisión el despliegue de fraudes o intentos de desapoderar a las víctimas de sus fondos. El aumento en la penetración en el mercado de los nuevos sistemas de pago electrónico y la creciente adopción de los criptoactivos por parte de la sociedad generan un nuevo espacio en el que los atacantes pueden desplegar sus maniobras delictivas. Ello, sumado a las nuevas medidas de seguridad impuestas para los sistemas de banca electrónica del sistema financiero tradicional, revelan una posible transición de la criminalidad a este tipo de desarrollos.

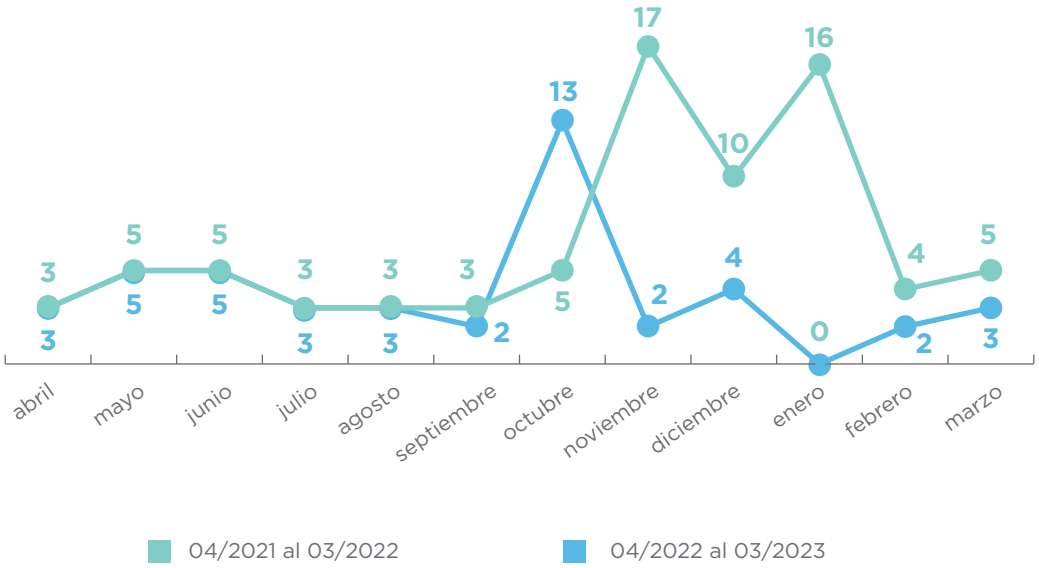
En el caso de Mercado Pago se advierte, más allá de las fluctuaciones, una tendencia al alza durante el primero de los periodos bajo estudio. Durante el primer mes relevado -abril de 2021- se contabilizaron 37 reportes mientras que, para el último mes de dicho periodo -marzo de 2022-, el número ascendía a 121, lo que equivale a un aumento del 227%. El periodo siguiente comenzó con 207 casos -abril de 2022-, sin embargo, a partir de allí los reportes comenzaron a disminuir para finalmente cerrar los doce meses con un total de 59 casos en marzo de 2023.

Mercado Pago



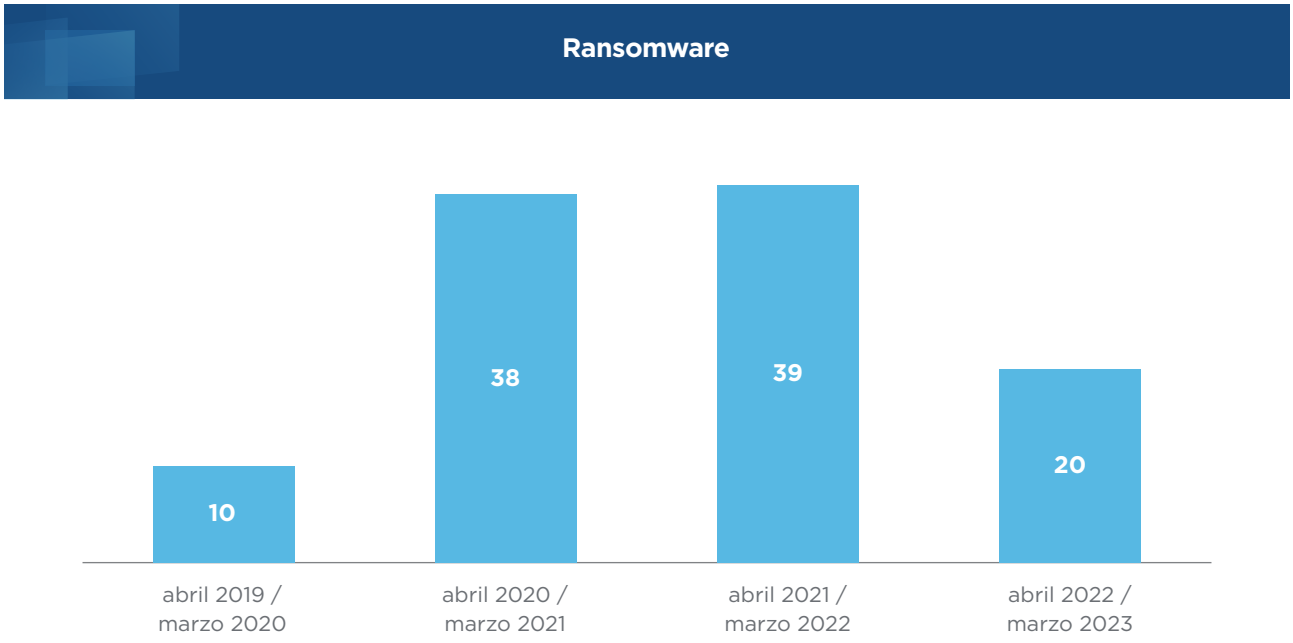
En lo que respecta a los criptoactivos, la tendencia no parece tan clara. Sin embargo, sí se puede constatar un aumento significativo en el número de reportes a partir del mes de noviembre de 2021. En efecto, de un promedio de 3,85 reportes que recibimos en los meses previos, para el mes de noviembre el número ascendió a 17, en diciembre de 2021 se detectaron otros 10 reportes, y en enero de 2022 un total de 16, para luego regresar a un nivel similar a los de los meses previos, sobre los cuales se mantuvieron entre abril de 2022 y marzo de 2023, con excepción de un aumento aislado relevado en el mes de octubre.

Criptoactivos



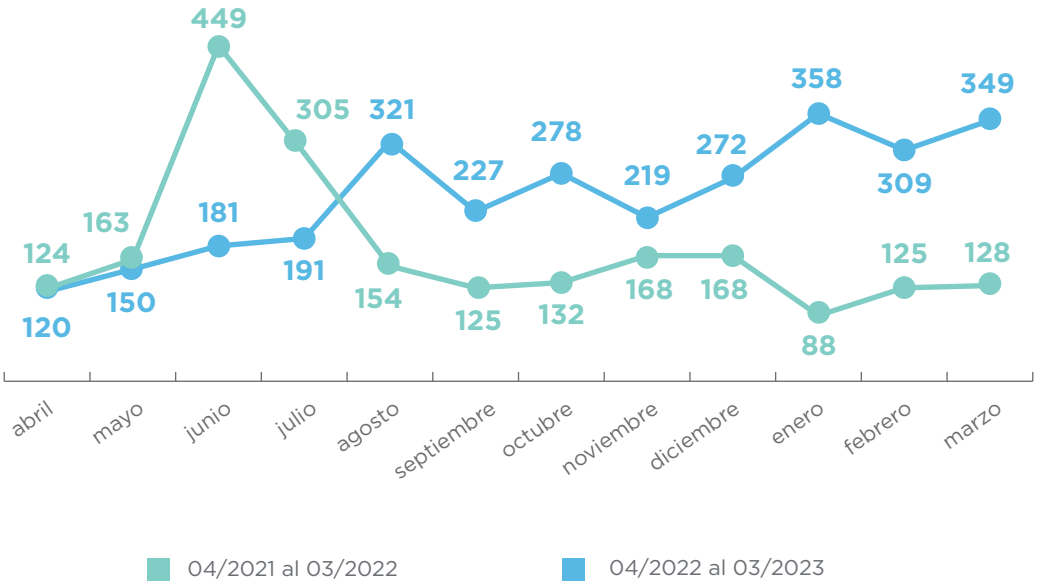
El pico identificado en el año 2021 coincide con el periodo en el que Bitcoin alcanzó su máximo valor histórico. Precisamente, el día 10 de noviembre de 2021, su precio alcanzó los U$D 69.045, lo que colocó a los criptoactivos en un lugar protagónico de la agenda mediática y despertó el interés de un gran número de personas. Es posible que ello, sumado al incipiente grado de familiarización con la tecnología de algunos de los nuevos usuarios que se introdujeron en el ecosistema de los criptoactivos para ese entonces, hayan generado un terreno fértil para que los atacantes pudieran desplegar esta clase de maniobras sobre los diferentes desarrollos ligados a su uso.

En lo que respecta a los reportes relacionados con posibles casos de *ransomware* -atravesados de manera transversal por los criptoactivos, en tanto los pagos exigidos por los autores suelen solicitarse en esa especie-, no se advirtió un incremento o variaciones que pudieran considerarse relevantes. Sin embargo, el numero de reportes identificados en el periodo anterior -que, de por sí, implicó un aumento de un 280% al compararlo con los doce meses previos- se mantuvo virtualmente estable para el periodo comprendido entre abril de 2021 y marzo de 2022, en tanto se constataron un total de 39 contactos vinculados con este tipo de maniobras contra los 38 del periodo previo. Para el periodo siguiente, no obstante, los reportes de este tipo de casos se redujeron.



Las técnicas de *phishing* son un elemento recurrente en un gran número de modalidades delictivas propias de nuestra materia. Aun frente al surgimiento de nuevas maniobras, los casos de phishing continúan ocupando un lugar preponderante dentro del ámbito de la cibercriminalidad. Entre los meses de abril de 2021 y marzo de 2022, se detectaron 2.129 reportes que aludían a sucesos que involucraron el despliegue de este tipo de técnicas, lo que constituye un 97,3% de aumento con respecto al periodo previo. Para el periodo siguiente los casos aumentaron a 2.975, lo que se traduce en un porcentaje de aumento marcadamente menor al anterior (39,7%), aunque denota una clara tendencia al alza.

Phishing



Al observar las variaciones de este tipo de casos a lo largo de los doce meses analizados, nos encontramos con una marcada divergencia durante el mes de junio de 2021, ocasión en la que se identificaron 449 reportes que aludían a maniobras de *phishing*.

Aunque existe un gran número de maniobras que involucran técnicas de *phishing*, algunas de las más características son aquéllas que contemplan el envío masivo de correos electrónicos a los efectos de engañar a las víctimas para que provean sus credenciales para acceder a una plataforma determinada. Pues bien, debido a su naturaleza masiva, cuando una actividad de esta naturaleza es desplegada es posible detectar fluctuaciones como la descripta. En concreto, durante el mes de junio pudimos detectar una campaña orientada a captar credenciales de usuarios relacionadas con plataformas bancarias y billeteras virtuales, llevada a cabo por medio de correos electrónicos y llamadas telefónicas que simulaban provenir de las entidades en cuestión. Es posible que la caída abrupta en estas maniobras guarde relación, al igual que en el caso de los fraudes relacionados con la banca electrónica, a las medidas adoptadas tendientes a obstaculizar la labor criminal.

Debido a la temática que atraviesa a la Unidad, es habitual encontrarnos con consultas en relación a conductas que, si bien no se encuentran contempladas expresamente en nuestro Código Penal, se encuentran atravesadas por aspectos informáticos. Sin ir más lejos, solemos recibir reportes relacionados con situaciones de acoso y de difamaciones -siendo la difusión de imágenes íntimas la modalidad detectada principalmente- que, en muchas ocasiones, se enmarcan dentro de un contexto de violencia de género. En concreto, durante el periodo comprendido entre los meses de abril de 2021 y marzo de 2022 se relevaron 1.488 reportes relacionados con situaciones de acoso y 171

casos de difusión de imágenes íntimas, mientras que, en el periodo siguiente, se relevaron 241 y 1.685 casos, respectivamente.

Teniendo en cuenta que la mayoría de estas conductas encuadran en figuras comprendidas en el Código Contravencional de la Ciudad Autónoma de Buenos Aires[11], encuentra sentido que las consultas de este tipo migren progresivamente a la justicia competente para investigarlas. Aun así, el número de reportes recibidos con relación a estos supuestos continúa siendo elevado y presenta una tendencia al alza.

11. Artículos 68 ter y 68 bis, respectivamente, del Código Contravencional de la Ciudad Autónoma de Buenos Aires.

IV. CONCLUSIONES

El repaso de las estadísticas elaboradas y plasmadas en el presente informe refleja algunas cuestiones ciertamente preocupantes. Tal como se adelantó al comienzo -y se advirtió en el documento en el que se analizó la situación relativa al periodo previo a los que hoy nos ocupan-, la tendencia al alza, en lo que respecta al número de conductas ligadas al cibercrimen, se consolida cada vez más.

Si bien el mayor nivel de aislamiento al que se vio forzada la sociedad como resultado de las medidas adoptadas para hacer frente a la propagación del COVID-19 pareció haber agudizado temporalmente esta tendencia, el paso del tiempo y el retorno progresivo a los niveles de movilidad previos a la pandemia no trajo consigo una disminución en los casos de criminalidad informática relevados.

Por el contrario, parecería ser que el aumento de casos observado para ese entonces se constituyó simplemente como un nuevo piso a partir del cual el número de conductas continuó creciendo a un ritmo similar al que se venía observando históricamente. Pero además, el desarrollo de nuevas soluciones tecnológicas que tuvo lugar durante ese periodo y la creciente adopción por parte de la ciudadanía de herramientas digitales como alternativa para realizar diversas actividades cotidianas, amplió enormemente el número de situaciones y personas potencialmente alcanzadas por la ciberdelincuencia, y en consecuencia, la complejidad del fenómeno.

Ahora bien, no puede dejar de señalarse que, así como la criminalidad evoluciona, las técnicas y las herramientas para poder investigar este tipo de hechos también lo hacen. Es así que, para poder continuar enfrentando este fenómeno en crecimiento, en sus diferentes matices, se torna imprescindible el sostenimiento de una estrategia de capacitación constante para todos los agentes que conforman el Ministerio Público Fiscal y las diferentes áreas del sistema judicial.

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO FISCAL | PROCURACIÓN GENERAL DE LA NACIÓN
Av. de Mayo 760 (C1084AAP) - Ciudad Autónoma de Buenos Aires - Argentina
(54-11) 4338-4300
www.mpf.gob.ar | www.fiscales.gob.ar