2021

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

UNIDAD FISCAL
ESPECIALIZADA
EN CIBERCRIMEN

2021

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia

Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020

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

Edición: septiembre 2021

Índice

I. Introducción. 7

II. Informe sobre la situación generada por la pandemia del COVID-19. 9

III. Conclusiones. 23

I. INTRODUCCIÓN.

Internet permitió la interconexión de miles de millones de personas, el acceso rápido y efectivo a una gran cantidad de información de múltiples orígenes, y el incremento exponencial del intercambio de bienes y servicios. Sin embargo, al mismo tiempo, las organizaciones criminales aprovechan la estructura de la red de alcance mundial para cometer nuevos tipos de delitos o para crear nuevas modalidades de delitos tradicionales.

La ciberdelincuencia es un fenómeno criminal que abarca tanto los ataques a los sistemas informáticos -por ejemplo, casos de accesos ilegítimos o de destrucción de información- como aquellos supuestos en los que se utilizan esos sistemas como medio para cometer otros delitos -como los fraudes a través de internet-.

En noviembre de 2015 se creó en el ámbito de nuestra institución la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) 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 (res P.G.N. n° 3743/2015[1])

Desde la creación de la Unidad, nuestras casillas de correo electrónico fueron difundidas en diversos sitios oficiales[2] con la finalidad de proveerle, a la ciudadanía, un canal de atención en el que pudieran realizar consultas y poner en conocimiento maniobras delictivas relacionadas con nuestra materia.

La criminalidad asociada al uso o a la afectación de sistemas y datos informáticos se caracteriza, entre otras cosas, por su dinamismo, por lo que la recepción, la sistematización y el posterior análisis de los mensajes se ha convertido, con el correr del tiempo, en un recurso invaluable -juntamente con la información que nos transmiten los y las fiscales cuando nos otorgan intervención en sus casos- no solo para comprender más acabadamente el fenómeno de la criminalidad informática en general y su evolución, sino también para detectar tempranamente el surgimiento de nuevas modalidades delictivas y generar estrategias de abordaje que permitan incrementar los niveles de respuesta de la institución.

Tal es así que, en función de los reportes recibidos, hemos iniciado múltiples investigaciones, desarrollamos documentos explicativos de circulación interna[3], actualizamos el contenido de las capacitaciones brindadas por nuestro equipo de trabajo y sugerimos a la ciudadanía, a través de los canales oficiales, la adopción de medidas de prevención para evitar ser víctimas de aquellas maniobras[4].

---

1. https://www.mpf.gov.ar/resoluciones/pgn/2015/PGN-3743-2015-001.pdf
2. https://www.argentina.gob.ar/justicia/convosenlaweb/denuncia
https://www.argentinacibersegura.org/pdf/denuncia-delito-informatico.pdf
https://bacsirt.buenosaires.gob.ar/index.php?u=como-denunciar#
3. https://intranet.mpf.gov.ar/ciberdelincuencia/ y https://www.mpf.gob.ar/ufeci/recursos/
4. https://www.fiscales.gob.ar/ciberdelincuencia/consejos-de-la-ufeci-para-evitar-maniobras-que-toman-el-control-de-las-cuentas-de-whatsapp/

Paralelamente, los mensajes recibidos fueron evaluados individualmente y respondidos a la brevedad, atendiendo las particularidades de cada caso, especialmente la información suministrada, el tipo de caso y la jurisdicción competente.

A continuación, presentamos un informe elaborado a partir de los datos recabados en el marco de nuestras funciones, fundamentalmente, en el transcurso de la pandemia, que consideramos podría resultar de interés.

---

https://www.fiscales.gob.ar/ciberdelincuencia/coronavirus-recomendaciones-de-la-ufeci-para-evitar-el-robo-de-datos-personales-cuentas-y-claves-bancarias-durante-el-aislamiento/
https://www.fiscales.gob.ar/ciberdelincuencia/grooming-recomendaciones-de-la-ufeci-en-el-marco-de-la-campana-de-prevencion-contra-el-acoso-sexual-cibernetico-de-adultos-a-ninos/
https://chequeado.com/el-explicador/consejos-para-no-caer-en-estafas-bancarias-y-que-hacer-si-ya-fuiste-victima-de-una/

II. INFORME SOBRE LA SITUACIÓN GENERADA POR LA PANDEMIA DEL COVID-19.

Transcurrido ya más de un año desde que comenzaron a dictarse diferentes medidas de aislamiento y distanciamiento preventivo con motivo de la pandemia, y tras haber relevado los numerosos reportes (mails) recibidos en la Unidad, nos encontramos en condiciones de plasmar y transmitir algunas conclusiones que, a nuestro modo de ver, podrían guardar cierta relación con el referido contexto.

II.1. Aumento en los casos asociados a la cibercriminalidad

Si bien el flujo de reportes ha variado considerablemente a lo largo de los años, se percibió un crecimiento exponencial en el último tiempo.

En ese sentido, nótese que en el transcurso del año 2019 se recibieron un total de 2.369, lo que equivale a aproximadamente 6,5 reportes diarios -sin distinción de días hábiles y no hábiles-, mientras que, para el año 2020, el número ascendió a 11.396, un 381% más, lo que equivale a alrededor de 31 reportes por día.

Los números expuestos reflejan la cantidad de ocasiones en las que hemos sido contactados, sin embargo, para una correcta ponderación de la labor que se lleva adelante, corresponde mencionar que en ocasiones, el intercambio de mensajes con quienes nos escriben se extiende más allá de nuestra respuesta inicial, por lo que el número total de correos electrónicos enviados y recibidos con motivo de los reportes es definitivamente superior.

Se trata de un aumento significativo que, de acuerdo a nuestra experiencia y conocimiento, podría tener una doble explicación.

Como punto de partida, comprendemos que el numero de reportes es directamente proporcional al volumen de maniobras ligadas a la informática que tienen lugar y afectan a la ciudadanía. Hemos podido comprobar que, a la vez que se percibe un crecimiento sostenido en el número de maniobras a nivel global[5], la cantidad de reportes que recibimos se incrementa también año tras año, y lo mismo ocurre con el surgimiento de nuevas modalidades delictivas o frente al aumento o disminución de determinado tipo de casos, en tanto también observamos un correlato de ello en los reportes.

Es así que los mismos motivos detrás de la tendencia al alza en los casos de criminalidad informática explicarían, parcialmente, el elevado número de reportes recibidos durante el año 2020.

---

5. A modo de ejemplo, las estadísticas del Internet Crime Complaint Center del Federal Bureau of Investigation (FBI) de los Estados Unidos exhiben que el número de casos presentados en esa oficina durante el año 2016 ascendió a 298.728, en el año 2017 a 301.580, en el año 2018 a 351.937, en el año 2019 a 467.361 y, ya para el año 2020, los casos ascendieron a 791.790 (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

Sin dudas, una de las fuentes principales de dicha tendencia es el propio desarrollo de las tecnologías de la información y la comunicación (TIC) y su nivel de penetración en la sociedad. Hoy en día, las TIC forman parte de la vida cotidiana de una gran parte de la población, por lo que no sorprende el ritmo con el que actividades de diferente naturaleza se adaptan o migran para aprovechar las diferentes bondades que ofrecen las nuevas tecnologías, y la actividad delictiva no es ajena a este proceso.

De acuerdo con el INDEC[6], para el último trimestre del año 2020, el 86% de los habitantes de nuestro país utilizaba internet, lo que representa un aumento de 5,6 puntos porcentuales con respecto al año anterior. Si bien se trata de un dato que no contempla pormenores como la calidad del servicio de internet, la velocidad y estabilidad, o el acceso a dispositivos informáticos[7], logra retratar un piso elevado y una clara tendencia al alza en lo que refiere a la posibilidad de acceder a internet y, por ende, a los servicios provistos por esa vía.

Pero más allá de este aumento observado año tras año, la actividad de la UFECI se incrementó aún más a partir del mes de marzo de 2020, cuando la situación generada por la pandemia del COVID-19 parecería haber potenciado los niveles de conexión por medio de las TIC de la población en general, tal como lo revelan múltiples indicadores.

En efecto, la empresa Mercado Libre[8] retrató que, al 3 de mayo de 2020, la cantidad de usuarios nuevos registrados en su plataforma de comercio electrónico se había incrementado, en nuestro país, en un 40% con relación al mismo periodo del año anterior, mientras que su plataforma de pagos electrónicos, Mercado Pago, registró un crecimiento de un 71%, en lo que refiere a pagos de servicios, y de un 66% en transferencias.

A su vez, un estudio elaborado por la plataforma Google[9] en el mes de octubre de 2020, reveló que casi un tercio de los argentinos encuestados, que habían realizado compras en línea en el último año, concretaron su primera operación durante el periodo de pandemia, y que la mitad de los compradores se habían inclinado por la modalidad *online* para minimizar así las salidas en el referido contexto.

Por otra parte, de acuerdo al Banco Central de la República Argentina[10], durante el año 2020 se registró un 19% más de operaciones por medios electrónicos que en el 2019, mientras que las transferencias electrónicas se acrecentaron en un 90%, producto de un aumento en las operaciones por medio de *homebanking* (86%) y *mobilebanking* (167%). A su vez, los pagos remotos con tarjeta de débito crecieron en un 227%.

---

6. https://www.indec.gob.ar/uploads/informesdeprensa/mautic_05_213B13B3593A.pdf
7. En ese sentido, informes preliminares de la Evaluación Nacional del Proceso de Continuidad Pedagógica, realizada en el mes de junio de 2020 sobre grupos de hogares de diferentes regiones educativas con niñas, niños y adolescentes en nivel inicial, nivel primario y nivel secundario, reflejaron que, aún cuando menos de la mitad de los hogares relevados contaba con acceso fijo a internet de buena calidad e, incluso, que un %27 accedía únicamente a través del servicio de telefonía (https://www.argentina.gob.ar/sites/default/files/resumen_de_datos_informes_preliminares_directivos_y_hogares_0.pdf).
8. https://ideas.mercadolibre.com/ar/noticias/efecto-cuarentena-mercado-libre/
9. https://www.thinkwithgoogle.com/_qs/documents/10736/Gu%C3%ADa_Argentina_consumidores_online_durante_la_pandemia.pdf
10. http://www.bcra.gov.ar/PublicacionesEstadisticas/informe-inclusion-financiera-022020.asp

El incremento aludido se vió reflejado también en el Estudio Anual 2020 de la Cámara Argentina de Comercio Electrónico[11], en el que se concluyó que el aumento interanual del rubro fue de un 124%, en términos de facturación, y de un 84% en lo que respecta a la cantidad de órdenes de compra formuladas.

Por fuera del plano comercial y financiero, nos encontramos también con que un gran número de organismos y empresas propiciaron, durante los periodos de aislamiento y distanciamiento social y obligatorio, la realización de trámites y operaciones de diferente índole por medios electrónicos. A modo de ejemplo, tan solo la plataforma de Trámites a Distancia (TAD) habría presentado un incremento de un 130% el número de usuarios registrados durante la pandemia, un 41% en los trámites generados en línea y un 22% en los documentos producidos digitalmente en la plataforma, en comparación con los años previos[12].

A su vez, el trabajo a distancia o teletrabajo, ligado desde su concepción a las TIC, se consolidó como en una gran cantidad de ámbitos laborales como una modalidad alternativa de trabajo, estimándose que el número de personas ocupadas trabajando desde sus viviendas habría alcanzado un valor de 1.364.066 para el tercer trimestre del año 2020, superando con creces los 212.380 que se estimaron para el primer trimestre de aquel año[13].

Las nuevas tecnologías permiten que cada vez más actividades puedan llevarse a cabo sin salir del hogar, por lo que encuentra sentido que su uso y, en función de ello, el número de interacciones y transacciones que podrían verse atravesadas por maniobras informáticas, se hayan acrecentado en tiempos de confinamiento. Organismos internacionales como Interpol, Europol, la Organización de los Estados Americanos y la Comisión Económica para América Latina y el Caribe de la Organización de las Naciones Unidas -entre otros- han observado también una relación entre los nuevos hábitos inherentes a la pandemia y el aumento en este tipo de delictividad a nivel mundial[14], y tal como veremos a continuación, el cotejo del caudal de reportes recibidos en la UFECI nos lleva a una conclusión similar.

Tomando como punto de partida el primer trimestre de los años 2019, 2020 y 2021, nos encontramos con que, en el primero de ellos, recibimos un total de 581 reportes, mientras que en el primer trimestre del año 2020 recibimos 790. Aquel aumento, de alrededor de un 36%, se presenta en dos trimestres anteriores a la adopción en nuestro país de medidas asociadas a la pandemia del COVID-19[15]. Se trata de una diferencia por demás importante que, si bien podría encontrar razón

---

11. https://www.cace.org.ar/noticias-el-comercio-electronico-crecio-un-124-y-supero-los-novecientos-mil-millones-de-pesos-en-ventas

12. https://publications.iadb.org/publications/spanish/document/Servicios-publicos-y-gobierno-digital-durante-la-pandemia-Perspectivas-de-los-ciudadanos-los-funcionarios-y-las-instituciones-publicas.pdf

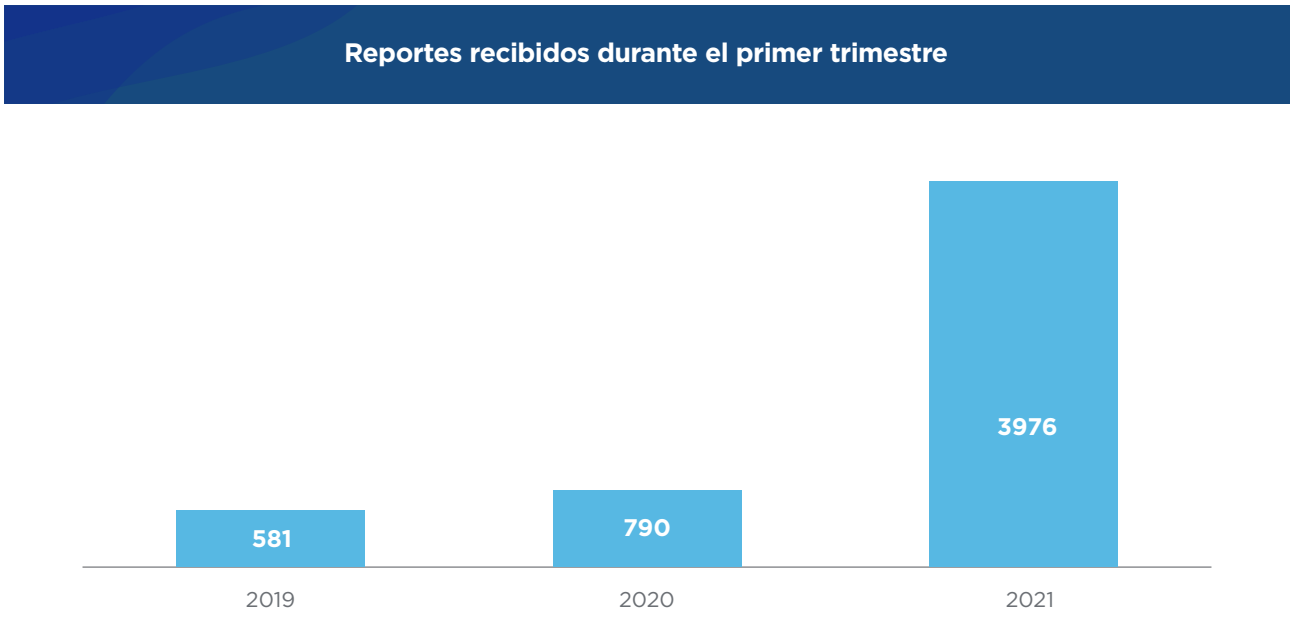
13. https://www.argentina.gob.ar/sites/default/files/2021/05/dt_5_-_evolucion_del_trabajo_remoto_en_argentina_desde_la_pandemia_1.pdf

14. De acuerdo a los informes publicados en https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf; https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf; https://www.oas.org/es/sms/cicte/docs/Ciberseguridad-de-las-mujeres-durante-COVID-19.pdf y https://repositorio.cepal.org/bitstream/handle/11362/46511/1/S2000678_en.pdf, respectivamente

15. Nos tomamos esa licencia, sin perjuicio de recordar que las primeras medidas oficiales en nuestro país se tomaron a mediados de marzo de 2020 y que

en diferentes variables, iría en consonancia con lo que se venía observando en torno al incremento sostenido de casos vinculados a la cibercriminalidad.

Sin embargo, en el primer trimestre del año 2021, atravesado ya por la pandemia y las diferentes medidas de prevención adoptadas, se detectó un aumento mayor. Se recibieron un total de 3.976 reportes, lo que se traduce en un aumento del 403% con relación al mismo periodo del año 2020.



La tendencia constatada a lo largo de los años podría explicar, parcialmente, el aumento en los reportes. Sin embargo, no puede dejar de verse que nos hallamos ante una divergencia considerablemente mayor. Teniendo en cuenta que el número de reportes parece variar en el tiempo en consonancia con el aumento en la delictividad informática, y ésta, a su vez, con el mayor desarrollo y adopción de las TIC, encuentra sentido que este incremento obedezca a un factor concomitante que cuente con un gran potencial disruptivo en lo que respecta a estas circunstancias, como podrían serlo las medidas de aislamiento adoptadas y los nuevos hábitos sociales derivados de la pandemia.

Corresponde aclarar, no obstante, que un porcentaje del aumento en las consultas realizadas por medios electrónicos o no presenciales podría responder también a variables ajenas al crecimiento de la criminalidad informática. Sin ir más lejos, al hecho de que más personas estén optando por evacuar consultas vía correo electrónico en supuestos en los que, en un contexto diferente, hubieran resuelto de manera presencial o telefónica, por lo que debe tenerse en consideración un posible sesgo en nuestras estadísticas que responda a dicha circunstancia.

---

los casos a nivel mundial de COVID-19 se venían reportando desde enero de ese año.

II.2. Análisis de las modalidades delictivas relevadas durante la pandemia.

Aclarado ello, nos avocaremos a continuación a analizar la información correspondiente a dos periodos consecutivos que consideramos propicios para evaluar, con una mayor extensión y profundidad, la posible incidencia del contexto descripto en lo que respecta a las modalidades delictivas relevadas. En este sentido, tomaremos como base los periodos comprendidos, en primer lugar, entre los meses de abril de 2019 y marzo de 2020 y, en segundo lugar, entre los meses de abril de 2020 y marzo de 2021.

En cuanto a los aspectos metodológicos, cabe mencionar que la clasificación de los reportes fue llevada a cabo mediante la lectura y el etiquetado de cada reporte en función de uno o más aspectos característicos de las maniobras puestas en conocimiento en cada caso. 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 se han utilizado o 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 los que denominaremos "modalidades secundarias" (fraudes en compras, fraudes bancarios, etc.).

Para mayor claridad, presentamos a continuación los lineamientos generales en los que nos basamos para adjudicarle a los reportes relevados aquéllas etiquetas que serán mencionadas en los próximos párrafos del documento, junto con algunas observaciones que podrían resultar de interés para una mejor comprensión del análisis llevado a cabo:

Fraude: 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[16].

Fraude relacionado con compraventas: maniobras fraudulentas -en los términos definidos precedentemente- que involucran 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.

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

Fraude bancario o relacionado con plataformas de homebanking: maniobras fraudulentas -en los términos definidos anteriormente- que involucran el 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.

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, de redes sociales y de cualquier otra plataformas.

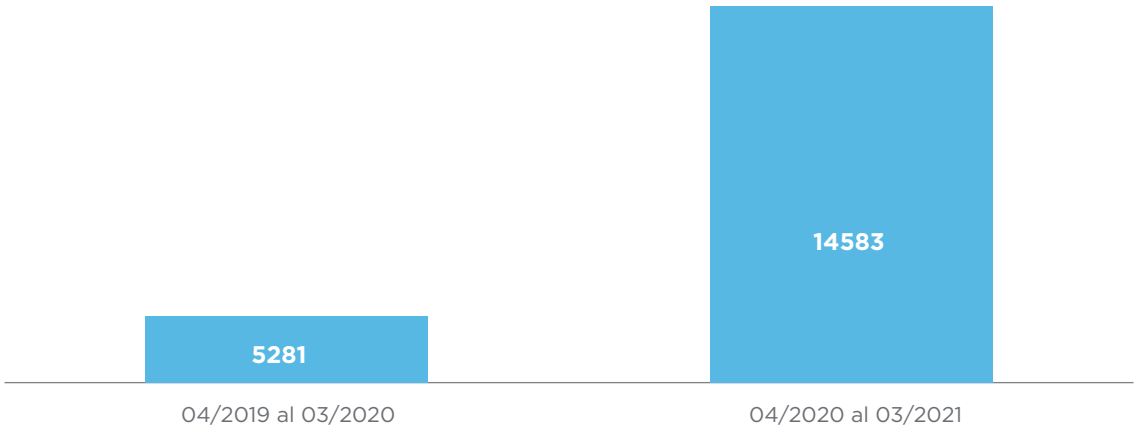
Usurpación de identidad: maniobras por medio de las cuales los autores se hacen pasar por un tercero, usualmente mediante la creación de direcciones de correo electrónico, sitios web o perfiles en redes sociales que aparentan pertenecer a las víctimas. Este tipo de maniobras pueden estar relacionadas 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 envio 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.

Adentrándonos ya en el análisis en cuestión, lo primero que puede observarse es que el aumento en la cantidad de reportes recibidos al comparar ambos periodos resulta abrumador. De 2.581 reportes recibidos en los doce meses anteriores a la pandemia, se pasó a recibir un total de 14.583. El aumento, en términos porcentuales, corresponde a un 465% aproximadamente.

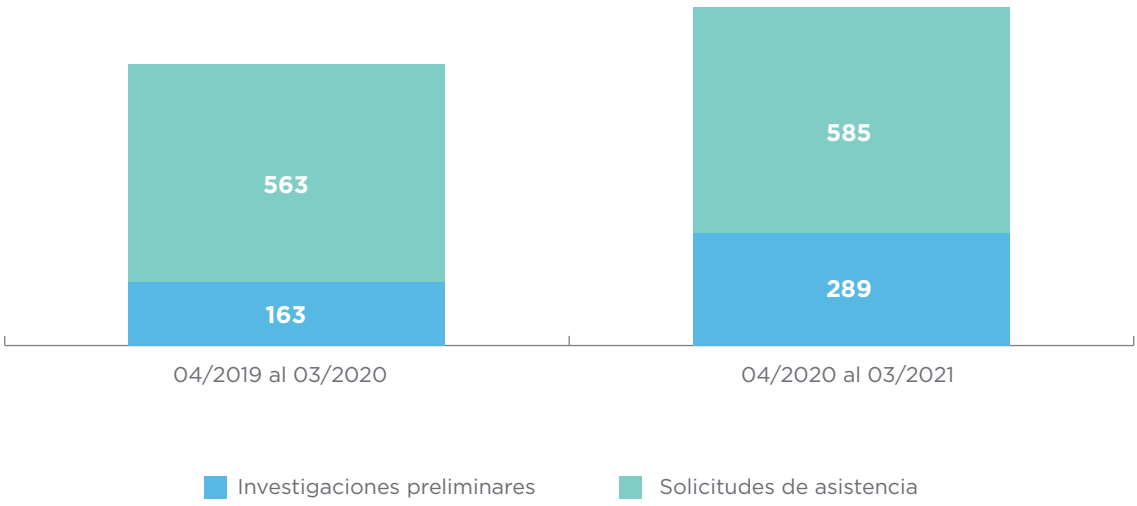
Reportes recibidos por periodo analizado



Ello, cabe destacar, impacta de lleno en otra de las labores que se llevan a cabo en la unidad, y que ocupan un lugar central en lo que hace a las funciones que nos han sido específicamente asignadas. En concreto, a partir de aquéllos, hemos iniciado, entre los meses de abril de 2019 y marzo de 2020, un total de 163 investigaciones preliminares, mientras que, entre los meses de abril de 2020 y marzo de 2021, el número se acrecentó a un total de 289. En este caso, el incremento fue de un 77,3%.

Dicho aumento en el caudal de trabajo debe valorarse sin dejar de lado otra de las áreas de actuación de la unidad, en la que también se evidenció un aumento. Ocurre que durante los doce meses previos a la pandemia, hemos atendido y dado respuesta a un total de 563 solicitudes de asistencia que nos cursaron fiscales/as y jueces/as de todo el país, mientras que en los doce meses posteriores, el número ascendió a 585, aunque debe tenerse en cuenta que durante muchos de esos meses hubo un período de feria judicial excepcional motivado por el inicio de la pandemia.

Casos tramitados por tipo de actuación



Regresando al análisis de los reportes, notamos que, en lo que respecta a las modalidades principales detectadas, los fraudes en línea se destacan significativamente por sobre las demás. En el periodo previo a la pandemia, los casos de fraude ascendieron a un total de 1.305, es decir que alrededor de la mitad de los reportes recibidos en todo ese tiempo consistieron en algún tipo de maniobra de índole defraudatoria.

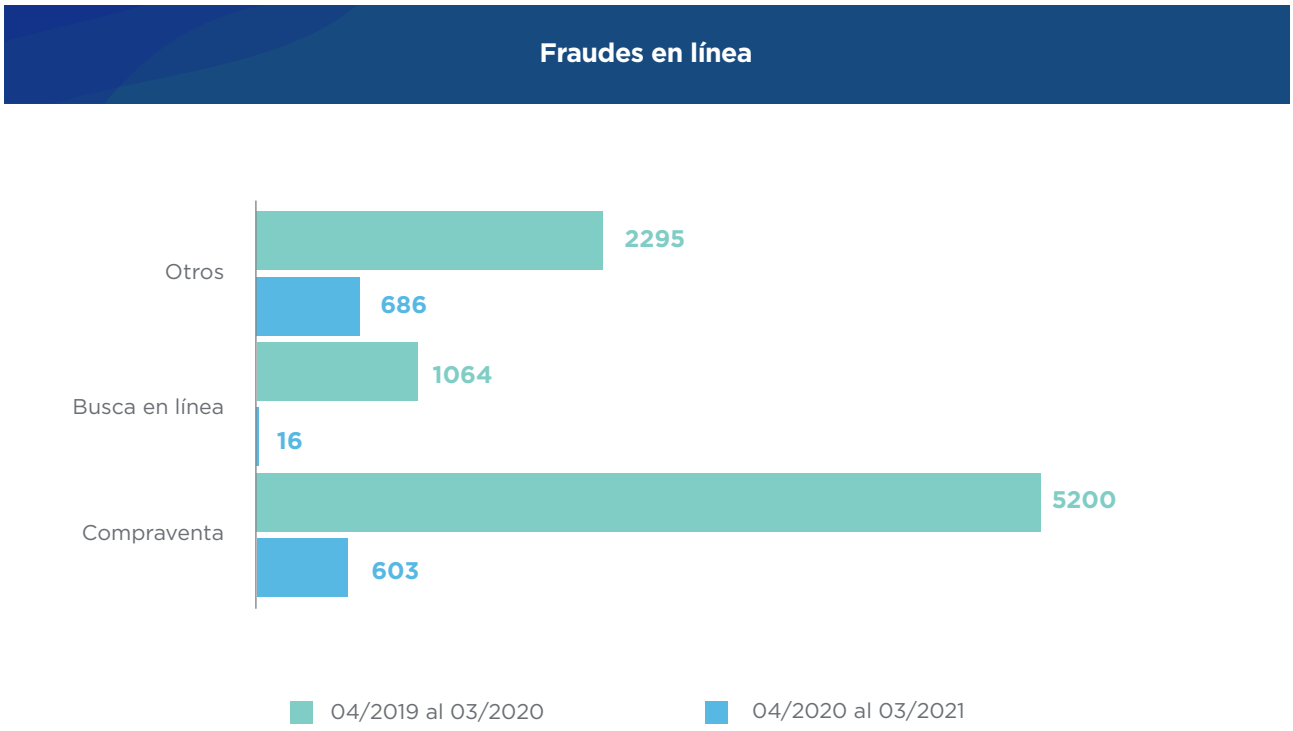
De aquéllos, 603 involucraban modalidades secundarias ligadas a operaciones o al ofrecimiento de productos para la compraventa y, 16, a maniobras que guardaban relación con el acceso indebido a cuentas bancarias luego de la captación bajo engaño de las credenciales de acceso a la plataforma de banca en línea o *homebanking*, es decir, un 46,2% versus un 1,2% de los fraudes, respectivamente.

En comparación, en los doce primeros meses de pandemia los fraudes detectados fueron 8.559, lo que representa un 58,7% aproximadamente del total de los casos. Se constató que el número de modalidades secundarias asociadas a compraventas alcanzó, durante el periodo, los 5.200 casos, mientras que aquéllas relacionadas con el *homebanking* ascendieron a 1.064. Comparando éste último valor con los números del periodo anterior, el incremento fue de un 6.550%[17].

Puede advertirse que la proporción de maniobras vinculadas a las compraventas aumentó, alcanzando

17. Un relevamiento realizado con anterioridad, en el que comparamos el número de maniobras asociadas al homebanking reportadas durante los años 2019 y 2020, ya daba cuenta de un crecimiento significativo -de un 3.652,9%-. Se observa, no obstante, que los casos continuaron aumentando a un ritmo vertginoso.

un 60,7% del total de los reportes de fraudes relevados, aunque la variación de los hechos asociados a la banca en línea resultó más significativa, alcanzando el 12,4% del total de los fraudes.



Las maniobras asociadas a las plataformas bancarias giraron fundamentalmente en torno a la obtención, por parte de los atacantes, de las credenciales para acceder a las cuentas de sus víctimas y el acceso a las mismas, para luego realizar transferencias y otro tipo de operatorias perjudiciales para sus titulares, como toma de préstamos preaprobados. En el caso de las maniobras de compraventa, el panorama resulta más diverso, sobre todo en lo que hace a las plataformas utilizadas por los autores para perpetrar las maniobras, aunque la mayoría son supuestos de captación de pagos en los que los autores crean cuentas en redes sociales o sitios web, que aparentan ser empresas o emprendimientos legítimos, y ofrecen desde allí productos o servicios de diferente naturaleza que, finalmente, no son suministrados a los compradores.

Durante la pandemia se advirtieron ciertas tendencias delictivas peculiares, constatadas a partir de los reportes, que amerita mencionar. Para empezar, en lo que respecta a las compraventas, comenzaron a detectarse casos en los que los servicios o productos se encontraban relacionados a la prevención del COVID-19. Sin embargo, adquiere especial relevancia el surgimiento de maniobras que, podría decirse, fueron diseñadas en función de las particularidades del contexto que atravesamos.

En ese sentido, detectamos que, frente a la instauración de programas gubernamentales asociados a la pandemia, comenzaron a desplegarse maniobras cuyo ardid o engaño giraba en torno a la tramitación de aquellos beneficios. Falsos formularios en línea para inscribirse, a través de los cuáles los autores captaban los datos personales de las víctimas que luego podían ser utilizados para cometer otro tipo de maniobras; accesos ilegítimos a cuentas bancarias y a cuentas de ANSES, por medio de los cuales se lograban realizar desplazamientos patrimoniales perjudiciales para sus titulares; y otro tipo de engaños desplegados para que, sencillamente, las víctimas realizaran pagos y transferencias a favor de los autores.

En el periodo comprendido entre los meses de abril de 2020 y marzo de 2021 detectamos un total de 663 casos con modalidades principales o secundarias atravesadas por estas circunstancias, lo que equivale a un 4,5% de la totalidad de los reportes recibidos en ese tiempo, de los cuales más de la mitad -365 casos- giraban en torno a los programas de asistencia económica.

A lo largo del tiempo, una de las maniobras esencialmente informáticas que ha mostrado cierta preponderancia es el *phishing*. En los doce meses anteriores a la pandemia, los reportes en los que las modalidades principales o secundarias involucraron casos de este tipo alcanzaron un total de 244, mientras que en el periodo posterior el número ascendió a 1079, un 9,4% y un 7,4% del total de reportes de cada uno de los periodos, respectivamente. La disminución en términos porcentuales respondería solo a una reducción en la dominancia, lo que lejos de reflejar una reducción en los casos -que, en rigor, aumentaron un 342.2%-, da cuenta del surgimiento de nuevas modalidades delictivas que atomizaron el catálogo de supuestos, reduciendo el impacto de las maniobras de *phishing* sobre el total.

De estos casos, nos encontramos con que la mayoría fueron llevados a cabo mediante el envío de correos electrónicos suplantando la identidad de alguna entidad financiera o plataforma digital; a su vez, se detectó un gran número de casos en los que el engaño fue desplegado telefónicamente. En este sentido, en el periodo anterior a la pandemia, 219 de los casos de *phishing* se llevaron a cabo por correo electrónico -un 89,7%-, mientras que, en el periodo de doce meses posteriores, 598 fueron bajo esa modalidad -un 55,4%-. Por otra parte, en este último periodo, se relevaron 275 casos en los que la maniobra fue llevada a cabo mediante llamadas telefónicas, un 25,5% del total de los casos de *phishing* (la modalidad específica cuando se hace por teléfono es conocida como *vishing* por *voice*).

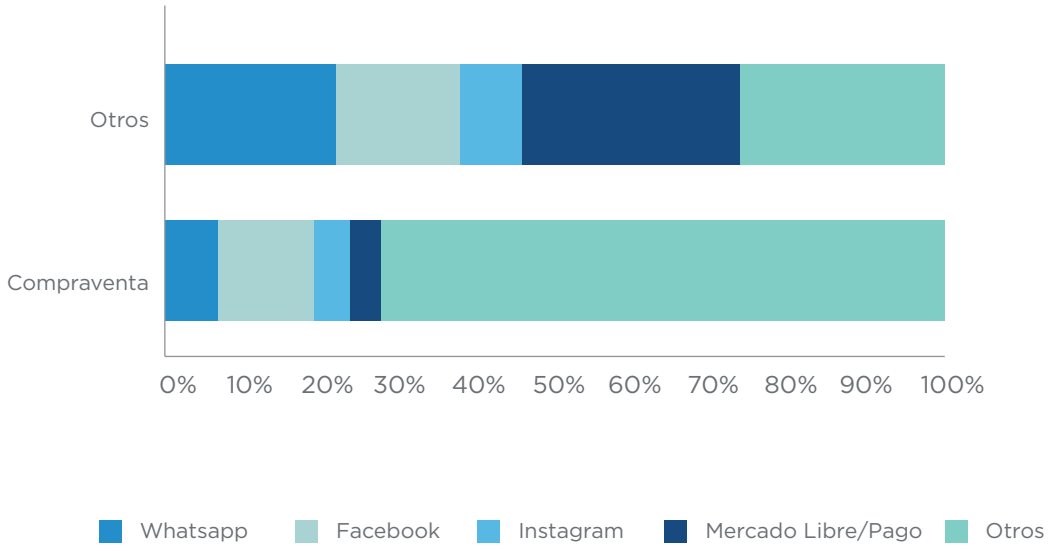
Otra de las principales modalidades identificadas en los reportes y, quizás, una de las que más se identifican como propias de nuestra materia, fue el acceso ilegítimo a sistemas o datos informáticos. En el periodo previo a la pandemia, los casos detectados ascendían a un total de 229, lo que representaba un 8,8% del total de reportes, mientras que en los doce meses posteriores se relevaron 1.220 maniobras, un porcentaje similar al anterior con relación al total -8.3%-, más allá de que, en términos netos, la cantidad de casos se quintuplicó.

A los efectos de caracterizar mejor esta modalidad, cabe mencionar que se detectó que las cuentas afectadas fueron, principalmente, de las plataformas Facebook, WhatsApp e Instagram. En los meses anteriores a la pandemia, se verificaron 30 maniobras asociadas a la primera, 17 a la siguiente, y 11 de la restante. Ahora bien, durante los doce meses de pandemia relevados, un nuevo actor se constituyó como la principal plataforma afectada: las cuentas de Mercado Libre/Mercado Pago[18].

Conjugando los casos asociados a las plataformas Mercado Libre y Mercado Pago -ambas pertenecientes a la misma compañía-, durante el primer periodo logramos identificar solamente 10 casos, sin embargo, para el año siguiente, el número ascendió a un total de 304, superando a WhatsApp -239 casos-, Facebook -171 casos- e Instagram -81 casos-.

Encuentra sentido que los autores de este tipo de delitos hayan encontrado un interés particular en explotar este tipo de cuentas, correspondientes a plataformas electrónicas de pago y compraventa, en un periodo en el que el comercio se volcó abruptamente hacia modalidades virtuales que permitieran operar a distancia.

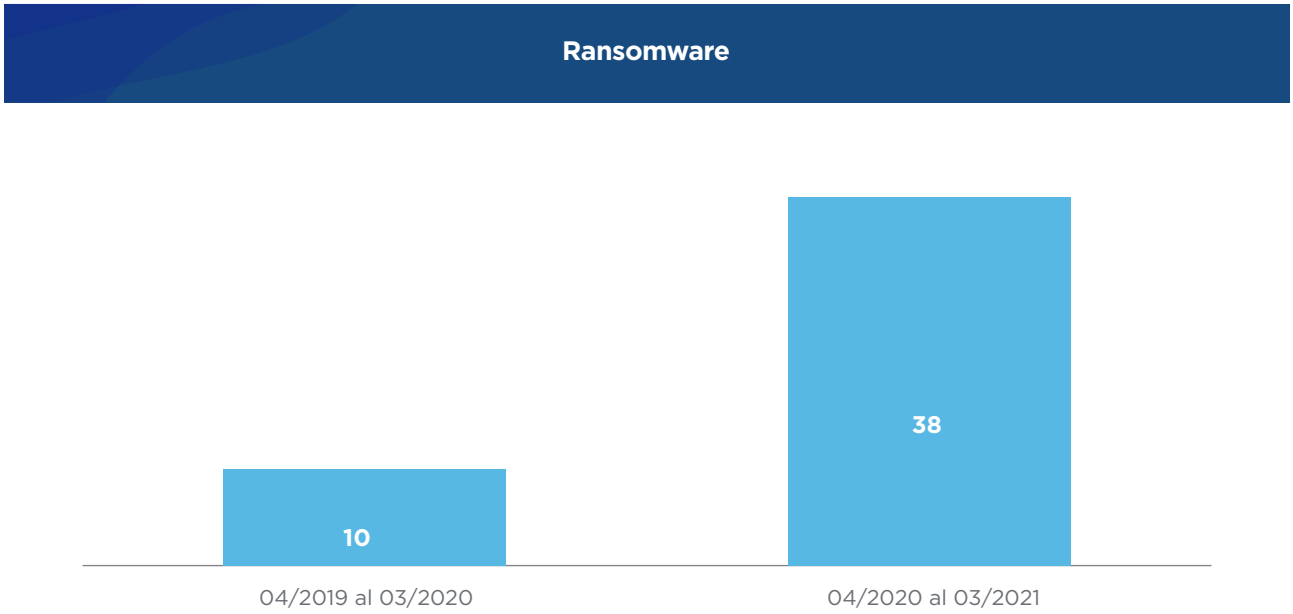
Distribución de fraudes en línea por plataforma



18. En menor cantidad, se detectaron accesos a otras billeteras digitales como PayPal, a cuentas de exchanges de criptoactivos como Ripio o Buenbit y a plataformas como Playstation que tienen asociada una tarjeta de crédito.

Durante el periodo de pandemia pudimos advertir un aumento en la cantidad de maniobras de *ransomware* reportadas. Si bien el número de casos se percibe como bajo en comparación con otras modalidades, debe tenerse en cuenta a la hora de valorar esta información que este tipo de ataques puede generar un impacto considerable en la sociedad, en tanto suele dirigirse a empresas o entidades cuyos servicios son utilizados por múltiples usuarios, los cuales pueden verse afectados también, directa o indirectamente, por la maniobra.

Dicho esto, durante los doce meses previos a la pandemia, los casos reportados fueron 10, mientras que, para el año siguiente, el número ascendió a 38, lo que significa que el aumento fue de aproximadamente 280%.

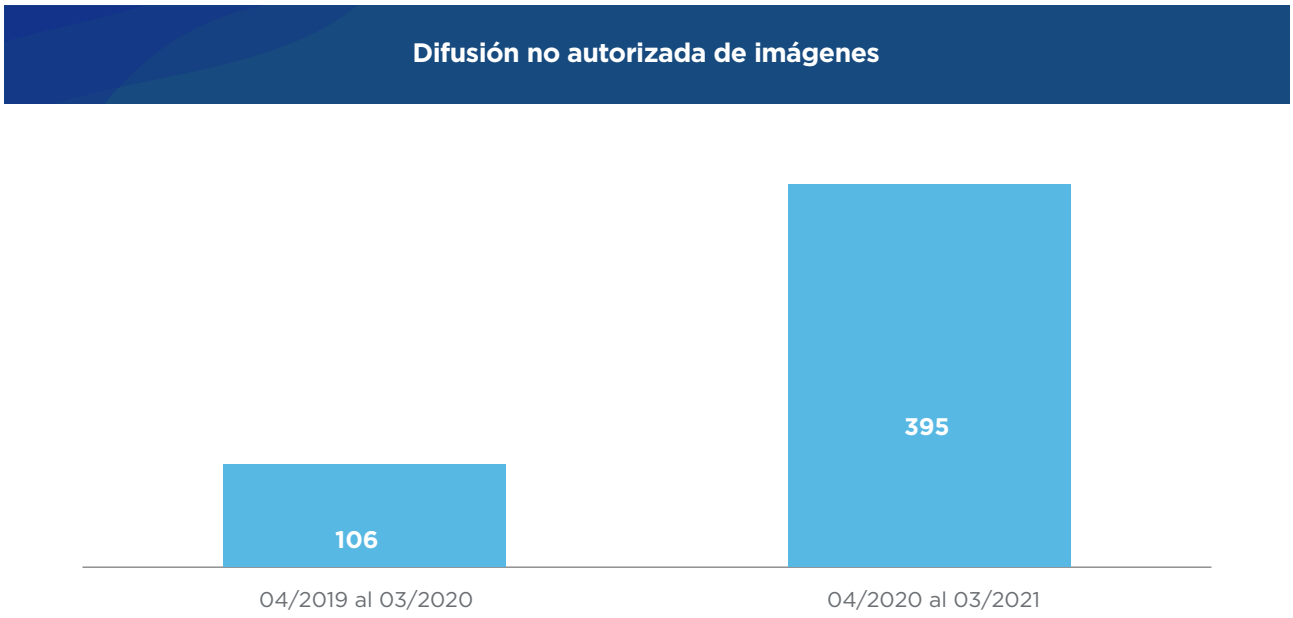


En los tiempos que corren, y a la luz de los proyectos de ley presentados y que están siendo analizados en la actualidad en los que se evalúa la incorporación de nuevas figuras penales, resulta de interés introducirse en los casos de difusión no autorizada de imágenes íntimas.

Corresponde indicar que esta conducta no está expresamente prevista en nuestro Código Penal, aunque dentro de la jurisdicción de la Ciudad Autónoma de Buenos Aires está mencionda en el Código Contravencional[19]. Es por ello que los datos relevados en nuestros reportes revelarán un sesgo, en tanto las consultas y las denuncias de un gran número de casos de esta naturaleza son canalizados directamente a través del sistema de justicia de la CABA.

19. Artículo 68 bis del Código Contravencional de la Ciudad Autónoma de Buenos Aires.

Aclarado ello, resta mencionar que de todos modos hemos recibido 106 reportes en el primero de los periodos analizados que involucraron este tipo de difusiones, mientras que en el periodo más reciente se reportaron 395 casos. El aumento de casos informados fue de un 272,6%.



Algo similar ocurre con los supuestos de usurpación de identidad, conducta que, por un lado, ha sido incorporada recientemente al Código Contravencional de la Ciudad Autónoma de Buenos Aires[20], y, a su vez, se encuentra contemplada en proyectos de reforma del Código Penal. Si bien los casos de *phishing* involucran algún tipo de suplantación de identidad, nos referiremos ahora en particular a supuestos en los que advertimos que el objeto de la conducta giraba en torno a ello y no, como ocurre con las maniobras de *phishing*, a la producción de un engaño idóneo para obtener un rédito económico.

Relevamos 81 casos en el primer periodo y, durante la pandemia, un total de 471, lo que significa que los casos aumentaron en un 481,4%, aunque manteniéndose en valores proporcionales similares con relación al total de reportes recibidos.

Nos encontramos a su vez en nuestro análisis con reportes de modalidades principales y secundarias de acoso, de naturaleza variada. Es decir, casos en los que las víctimas se ven afectadas por algún tipo de hostigamiento, perpetrado por medios digitales[21]. Claro está que algunos de estos supuestos se llevan a cabo mediante las modalidades descriptas precedentemente, por lo que aquellos valores

20. Artículo 68 quinquies del Código Contravencional de la Ciudad Autónoma de Buenos Aires.
21. Previsto también en el Código Contravencional de la Ciudad Autónoma de Buenos Aires, artículo 68 ter.

se verán parcialmente repetidos en el relevamiento realizado en relación a los acosos.

Dicho esto, en el periodo anual inmediatamente anterior a la pandemia, detectamos un total de 475 casos de acoso. Ya de por sí, dicho valor se presenta como significativo, teniendo en cuenta que se traduce en un 18,4% de los casos reportados durante ese plazo. Ahora bien, para el año siguiente, los casos aumentaron a 1.980, número que representa un 13,5% del total de ese periodo. Cabe remitirse a las apreciaciones formuladas en torno a la variación de los porcentajes de casos de *phishing*, en tanto, nuevamente, el número de casos aumentó significativamente -un 316.8%-, aunque el porcentaje con respecto al total de reportes de cada año se redujo, lo que en modo alguno puede interpretarse como una tendencia favorable.

Relevamos situaciones íntimamente relacionadas también con las anteriores, que clasificamos como difamaciones. Sobre estas, cabe mencionar que los valores pasaron de 301 casos a 1.323, un incremento del 339,5%. Al igual que en el análisis precedente, la relación con respecto a los totales descendió, en estos casos, del 11,6% al 9,07%.

Las modalidades descriptas precedentemente, en concreto, la difusión de imágenes, la usurpación de identidad, el acoso y las difamaciones, adquieren particular relevancia teniendo en cuenta que se trata de maniobras que suelen enmarcarse en situaciones de violencia de género. Es habitual encontrarnos con casos en los que los autores se valen de este tipo de recursos para producir un menoscabo en ciertos aspectos de la vida de las mujeres y, en definitiva, en su integridad psíquica, ello como un fin en sí mismo o, en otros casos, para amedrentarlas y compelerlas a actuar o dejar de actuar de una manera determinada.

III. CONCLUSIONES.

A modo de conclusión, mediante el análisis del material recopilado en el marco de nuestras funciones hemos podido constatar que, en lo que refiere a las maniobras informáticas, la tendencia tiene una dirección clara al alza. No solo en lo que respecta al número de casos, sino también, al surgimiento de nuevas modalidades delictivas. Se deduce también que situaciones como la que nos encontramos transitando actualmente, que fuerzan a una migración de múltiples actividades hacia la virtualidad, agudizan dicho incremento.

Esta situación resulta doblemente preocupante, por un lado, por el hecho de que la pandemia no ha finalizado aún, por lo que el flujo de casos de esta naturaleza debería continuar incrementándose en la medida que más personas se ven forzadas a migrar a las nuevas tecnologías para llevar a cabo sus diversas actividades cotidianas, pero además, si bien se podría presumir un posible efecto rebote en dicho proceso una vez que las medidas puedan ir flexibilizándose, lo cierto es que muchos de los avances y de los nuevos hábitos adquiridos parecerían haber llegado para quedarse.

Así, aun cuando el coeficiente de aumento detectado en los periodos comparados pueda llegar a reducirse, no caben dudas que, la situación retratada en los párrafos precedentes con relación a los doce meses de pandemia, será solo el punto de partida de lo que vendrá.

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