- 2025 -

Informe 2024
Casos y modalidades reportadas a UFECI

—

UFECI | Unidad Fiscal Especializada en Ciberdelincuencia

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

- 2025 -

Informe 2024
Casos y modalidades reportadas a UFECI

—

UFECI | Unidad Fiscal Especializada
en Ciberdelincuencia

Informe 2024 - Casos y modalidades reportadas a UFECI

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

Edición: junio 2025

Índice

1. Introducción. 7

2. Objetivos. 8

3. Metodología. 8

4. Análisis de reportes 8

4.1. Comparación interanual 8

4.2. Reportes año 2024 10

4.3. Análisis de las modalidades y tendencias identificadas a partir de los reportes. 12

4.3.1. Los fraudes en línea 13

4.3.2. Accesos ilegítimos a plataformas 19

4.3.2.1. Usurpación de identidad + fraude 22

4.3.3. Phishing 24

4.3.4. Extorsión 25

4.3.5. Acoso y difusión no autorizada de imágenes íntimas como modalidad específica de violencia contra las mujeres. 26

4.3.6. Ransomware 27

5. Conclusiones 29

1. 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 fenómeno del cibercrimen, intensificar las tareas para su abordaje de modo articulado y atender a sus especificidades.

Hemos iniciado investigaciones preliminares y asistido a los magistrados en sus casos en más de 7.500 oportunidades -en el marco de aproximadamente 5.900 casos distintos- y **recibimos hasta el mes de diciembre de 2024 un total de 120.264 consultas y reportes de particulares** en nuestras casillas de correo electrónico por temas relacionados con nuestra especialidad.

La información provista en el marco de estos reportes 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, así como también elaborar diversas líneas de acción e intervención de la Unidad.

Dicho correo institucional, además funciona como un canal de orientación y derivación para la ciudadanía.

La pandemia del COVID-19 y las diversas medidas de aislamiento y distanciamiento social, han acelerado y consolidado la virtualización de muchos aspectos de la vida cotidiana; el trabajo, el comercio, el ocio, la realización de trámites diversos, las operaciones financieras, las transacciones económicas y también el modo de relacionarnos entre las personas.

En consecuencia, las conductas delictivas han seguido el mismo patrón, se han virtualizado ciertas maniobras tradicionales, así como también se han creado nuevas modalidades.

En adición, 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.

1.https://www.mpf.gov.ar/resoluciones/pgn/2015/PGN-3743-2015-001.pdf

2. OBJETIVOS.

El objetivo general del presente informe es identificar, tipificar y dimensionar los reportes recibidos en las casillas institucionales de la UFECI destinadas a tal efecto durante el año 2024.

En cuanto a los objetivos específicos, se buscará catalogar los reportes según su modalidad y clasificarlos según la herramienta o canal utilizado para la maniobra delictiva, así como también establecer características particulares de alguna de ellas, ya sea por su notable ocurrencia y/o por la especificidad y/o complejidad de la maniobra.

En definitiva, **a partir de las estadísticas recogidas desde enero a diciembre de 2024, el informe presenta la evolución de las modalidades de cibercrimen reportadas a la UFECI por la ciudadanía.**

3. METODOLOGÍA.

Como mencionamos anteriormente, para realizar el presente informe se utiliza el registro de los reportes recibidos principalmente en la casilla institucional **denunciasufeci@mpf.gov.ar.**

Cada reporte es etiquetado 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*.

Los mensajes que conformaron las respectivas conversaciones -es decir, los correos electrónicos intercambiados con cada persona- fueron agrupados luego en carpetas e identificadas con el nombre o la dirección de correo electrónico del interlocutor y las etiquetas asignadas. Esos correos son luego utilizados, si es posible, como insumo para iniciar investigaciones preliminares o nutrir casos en trámite.

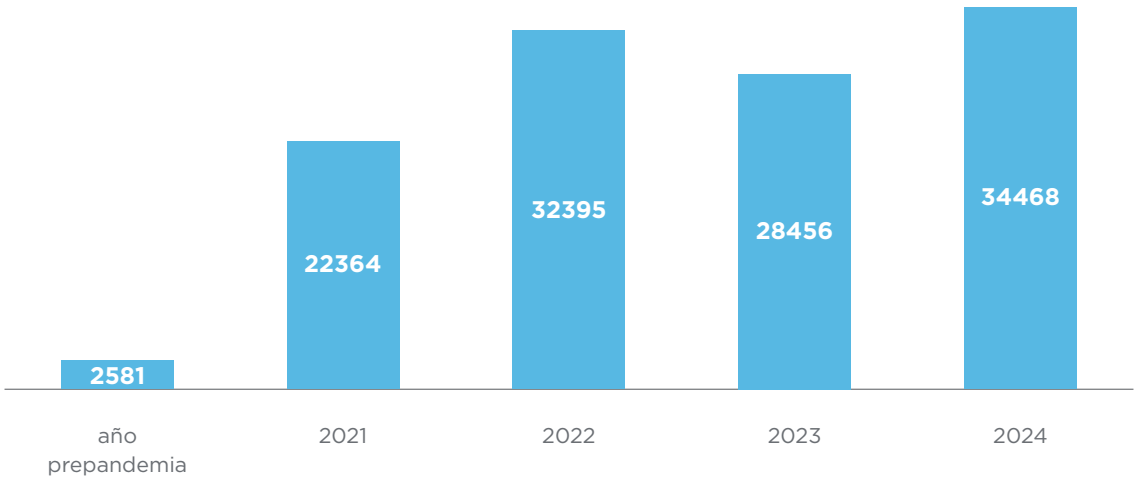
4. ANÁLISIS DE REPORTES

4.1. Comparación interanual

Como se mencionó en informes anteriores, la pandemia COVID-19 marcó un quiebre en la evolución de los reportes recibidos, debido a la adopción de nuevas tecnologías. 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), tendencia que se mantuvo en los años subsiguientes, y si bien se reflejan variaciones interanuales, **se ha establecido un nuevo "piso" de reportes muy superior al registrado previo a la pandemia.**

Comparación interanual - N° reportes



De enero a diciembre de 2021, se recibieron 22.364 reportes, en el año 2022 se registraron 32.395, 28.456 reportes fueron recibidos en 2023 y **en 2024 se alcanzó la cifra más alta registrada anualmente con 34.468 reportes.**

Diversas empresas, profesionales y organismos públicos 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. En línea con ello, la ciudadanía en general ha incorporado este salto tecnológico a su vida cotidiana.

En ese sentido, **consideramos que el grado de adopción de las nuevas tecnologías por parte de los ciudadanos para realizar sus diferentes actividades en la vida diaria, no retornará a los niveles anteriores a la pandemia, por lo tanto, es de esperar que el nivel de maniobras delictivas reportadas tampoco, en una suerte de relación directa con el proceso de tecnologización de la sociedad.**

Entre los factores generales que podrían explicar los números precedentes -con aumentos en los años 2022 y 2024-, se puede mencionar el esperable proceso que se da entre la aparición de la plataforma

y/o herramienta informática, el surgimiento de la maniobra delictiva que hace uso de aquellas, y la adopción de comportamientos precautorios por parte de la ciudadanía.

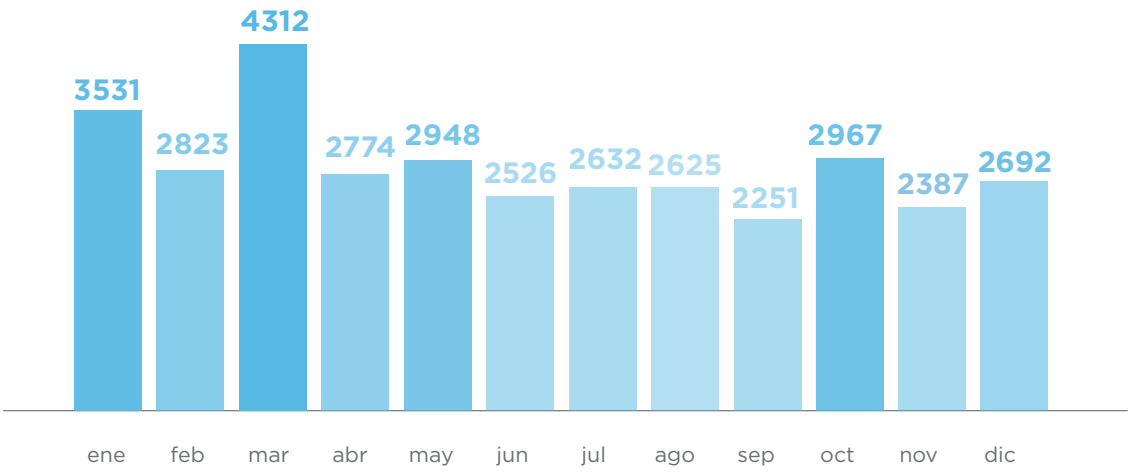
Siguiendo esa línea de razonamiento, frente a la novedad de la tecnología, se da usualmente un proceso de aprendizaje y adaptación que requiere el operar nuevas herramientas informáticas para las actividades cotidianas, el cual incluye por supuesto, la adopción de comportamientos precautorios y un mayor grado de conocimiento en la utilización de esa tecnología o plataforma (ej. uso seguro del *homebanking* y billeteras virtuales) por parte de las personas. Sin embargo, el surgimiento de nuevas tecnologías no se detiene, así como tampoco la aparición de nuevas modalidades delictivas asociadas a ellas. Esta dinámica entre la novedad y la apropiación o uso seguro, podría explicar en gran medida los números enunciados.

Las campañas de concientización y capacitación, tanto públicas (destinadas a ciudadanos y consumidores) como privadas (destinadas a usuarios y clientes), así como también la ineludible experiencia personal, contribuyen sin duda a construir este panorama y son una necesidad de primer orden para lograr una internet y una interacción con las nuevas tecnologías en general, en forma libre, accesible y segura.

4.2. Reportes año 2024

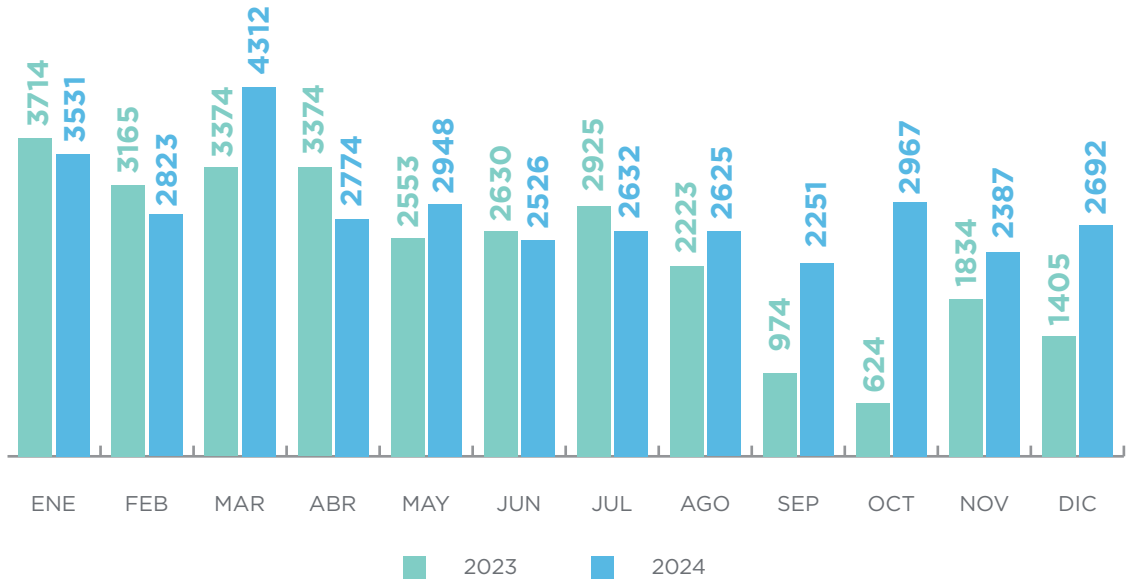
Como se adelantó durante 2024 registramos **34.468 reportes.** En la comparación intermensual, marzo es el mes con mayor cantidad de reportes (4.312), para luego registrarse una disminución del orden del 35% en los meses subsiguientes, registrando cifras similares que oscilan entre los 2.250 y 3.000 reportes mensuales.

Comparación mensual reportes 2024



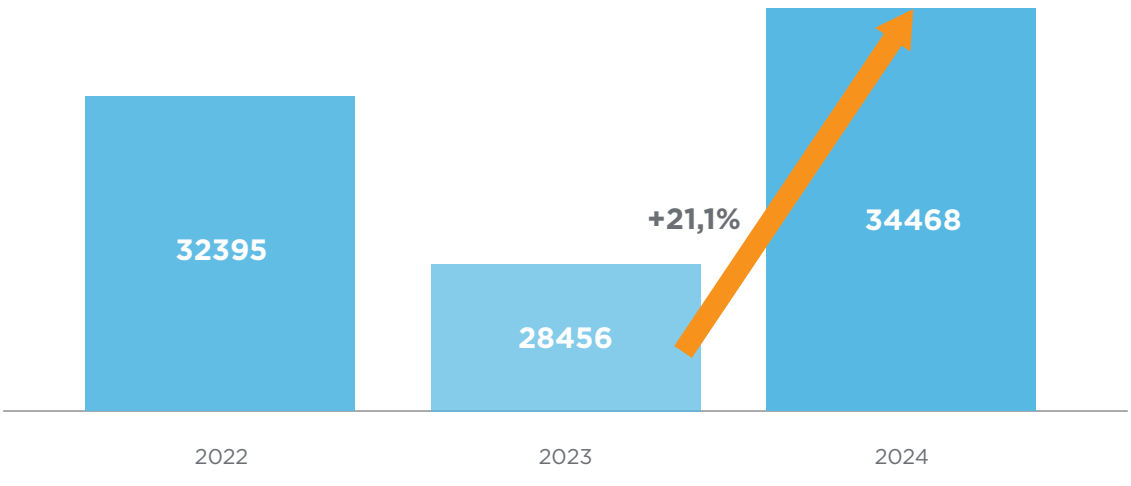
Si realizamos la comparación interanual con 2023, observamos un patrón similar en cantidad de reportes por mes, con excepción del mes de marzo (28% más), septiembre (131% más), octubre (375% más) y diciembre (92% más) de 2024 respecto a esos mismos meses del año anterior.

Comparación total reportes 2023-2024



Podemos concluir que, durante 2024 se han recibido un 21,1% más de reportes en la casilla de correo electrónico de la Unidad que en 2023.

Comparativo interanual 2022-2023-2024

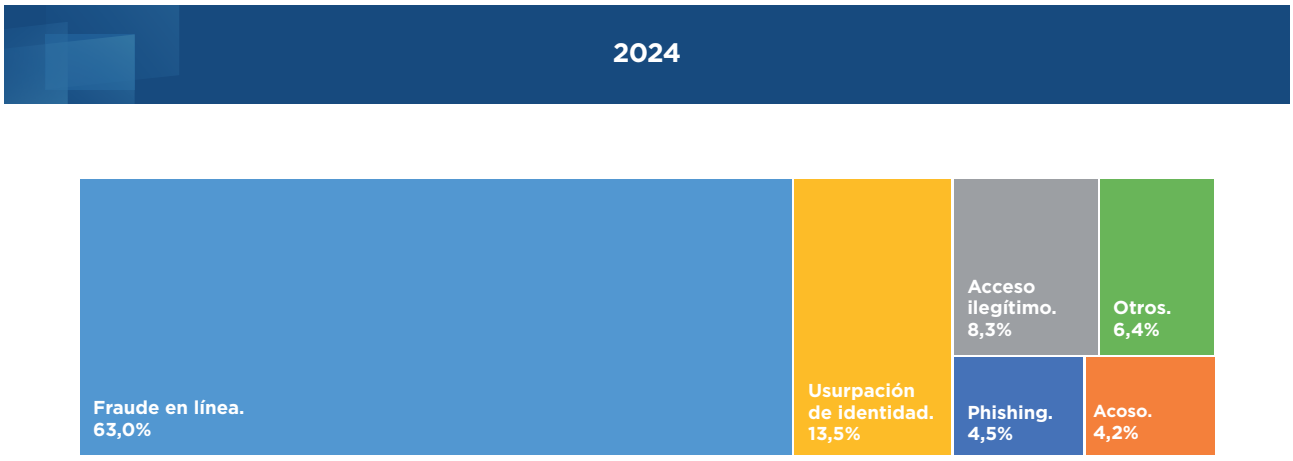


4.3. Análisis de las modalidades y tendencias identificadas a partir de los reportes.

A continuación, nos adentraremos en el análisis de los reportes en particular, clasificando las modalidades e identificando las principales tendencias, maniobras y métodos del cibercrimen durante 2024.

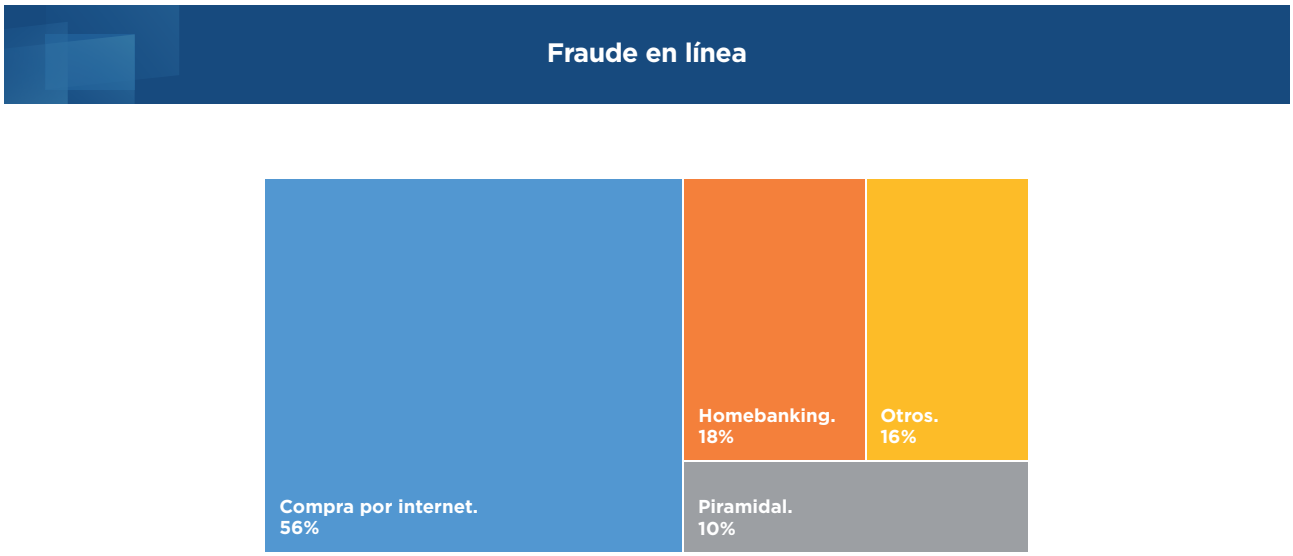
MANIOBRA	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Fraude en línea	2341	1809	2315	1931	1946	1627	1638	1615	1328	1893	1348	1938	**21729**
Usurpación de identidad	410	322	720	282	387	305	389	395	371	464	439	153	**4637**
Acceso ilegítimo	309	197	442	168	234	208	199	242	192	230	266	190	**2877**
Phishing	144	200	283	125	101	136	100	102	88	97	32	155	**1563**
Acoso	136	136	225	110	109	86	160	110	109	97	97	83	**1458**
Otros	191	159	327	158	171	164	146	161	163	186	205	173	**2204**
Total	**3531**	**2823**	**4312**	**2774**	**2948**	**2526**	**2632**	**2625**	**2251**	**2967**	**2387**	**2692**	**34468**

Como hemos comunicado en informes anteriores, la modalidad de "fraude en línea" sigue siendo la maniobra más reportada en 21.729 oportunidades, seguida de "usurpación de identidad seguida de fraude" en 4.637 ocasiones, "acceso ilegítimo" 2.877, maniobras de "*phishing*" en 1.563, y "acoso" en 1.458 reportes. Luego tenemos la categoría "otros" donde se incluyen diversas modalidades que no llegan a ser representativas. A continuación, se representa su incidencia respecto del total anual (en porcentaje).



4.3.1. Los fraudes en línea

Dentro de la modalidad **"Fraude en línea",** un 56% corresponde a operaciones de fraude en compra-venta por Internet (de bienes, o de servicios), un 18% representan fraudes a través del uso del *homebanking* y un 10% corresponde a los esquemas piramidales.



Las operaciones de **compra en internet** siguen representando un gran porcentaje de los reportes recibidos mensualmente en UFECI y son un insumo importantísimo para la generación de investigaciones preliminares. El total de 12.004 casos de 2024 engloba, en su inmensa mayoría, casos de personas que pagaron por un producto o servicio que vieron ofrecido en redes sociales o plataformas de mensajería que terminaron no recibiendo, pero también casos en los que se pagó por un servicio no prestado y, en menor medida, quienes dijeron ser estafados sin dar mayores precisiones.

Una maniobra que ha surgido notoriamente este año, son los **fraudes asociados a plataformas de inversión y ofertas de trabajo, también conocidas como "estafas piramidales".** Las víctimas con el afán de ganar dinero o preservar sus ahorros, buscan invertir en alguna solución financiera. A través de grupos de redes sociales, usualmente WhatsApp o Telegram, reciben ofertas muy tentadoras para invertir en plataformas de inversión -que se presentan como prestigiosas-, con beneficios o rendimientos muy superiores a las tasas de mercado. Luego mientras las víctimas van transfiriendo dinero a billeteras virtuales, en adición se les solicita invitar amigos o conocidos para sumar clientes. Algunas veces, unos pocos usuarios logran retirar o cobrar algún dividendo, para reforzar la confianza en la plataforma. Sin embargo, al final del proceso el dinero no se puede recuperar y se consuma el fraude.

Utilizando la misma maniobra, en otros casos se ofrecen trabajos remotos para empresas de primera línea, los cuales constan de realizar reseñas positivas, dar "*likes*" o "me gusta" *online* a publicaciones

y ofertas de productos. El fraude consiste en lograr que la víctima transfiera dinero a los responsables en concepto de impuestos o comisiones para retirar o liberar el pago de los supuestos dividendos.

Los fraudes a través de falsas ofertas de trabajo y los esquemas de inversión en criptoactivos son modalidades que, si bien se originaron en otras partes del mundo, están creciendo en la región (incluso notablemente en nuestro propio país) a partir del uso cada vez más cotidiano de las criptomonedas y el auge de las billeteras interoperables que han tenido por objeto incluir financieramente a todos los ciudadanos al poder contar con una herramienta de pago, sin necesidad de tener una cuenta bancaria.

La falta de recaudos en el uso de estas nuevas tecnologías de pago, sumado a posibles necesidades económicas de las víctimas (aunque no necesariamente, ya que pueden existir otros factores preponderantes, dependiendo el perfil de la víctima) ha hecho que los cibercriminales redireccionen estos ataques hacia nuestra región.

En estas maniobras suelen estar involucradas organizaciones criminales que operan, según la información relevada, en el continente asiático y, en general, están ligadas a redes de trata que captan víctimas mediante falsas ofertas de trabajo y luego las obligan a trabajar en centro de estafas en línea donde se comete todo tipo de delincuencia financiera. Entre ella, los esquemas de inversión cuyas modalidades si bien van mutando, se centran en una misma dinámica o estructura delictiva.

En ese sentido, cabe destacar que, en junio del 2023, Interpol emitió una alerta naranja a todos sus miembros ya que esta dinámica que afectó a miles de personas del sudeste asiático, se estaría expandiendo a nivel mundial.

Fuente: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/INTERPOL-publica-una-alerta-mundial-sobre-estafas-cometidas-por-victimas-de-la-trata-de-personas

Desde la UFECI, no descartamos que estas organizaciones criminales se encuentren operando en el país con la colaboración de sujetos locales. La evidencia que hemos colectado en nuestros casos respalda esta tesis, ya que, en general, hemos verificado que muchos de los dominios donde se montan estas plataformas fraudulentas son registrados en empresas radicadas en Asia (principalmente en Singapur), siendo las propias víctimas argentinas contactadas desde números telefónicos del exterior (como Reino Unido, Afganistán, China y otros países asiáticos y del medio oriente).

La otra dinámica que ha venido creciendo -a la par de los fraudes mediante falsas ofertas de trabajo- son los esquemas de inversión en criptoactivos. En la mayoría de los casos, las víctimas son contactadas por redes sociales y por otras tantas víctimas ya inmersas en el esquema para que inviertan en plataformas que prometen altas ganancias en criptoactivos (usualmente en USDT[2]) con la promesa de tener muy buenos rendimientos. Las víctimas envían sus fondos a direcciones de criptomonedas que son controladas por los estafadores. Los fondos, en un lapso corto de tiempo, se "acreditan" en esa plataforma y las víctimas invierten en los criptoactivos que los representantes de las plataformas les indican generalmente en grupos de Telegram hasta que, en un momento dado, ya no pueden retirar sus activos (usualmente bajo una serie de excusas) y la plataforma cae o deja de estar en línea, viéndose todos los inversores perjudicados por esta maniobra.

Este tipo de estafa se conoce como "carnicería de cerdos" (o *Pig Butchering* en inglés) porque los estafadores "engordan" a las víctimas con promesas de grandes ganancias antes de "sacrificarlas" para sustraerle todos sus fondos. El esquema comenzó en China en el año 2019, pero ha venido creciendo a nivel mundial con fuerte impacto en los Estados Unidos de América. El incremento paulatino en el uso de criptomonedas en la región ha hecho que, de algún modo, este tipo de maniobras se extienda a nivel local siendo ya una problemática mundial.

Sin ir más lejos, el Federal Bureau of Investigations (FBI) ha advertido un importante crecimiento de este tipo de casos desde el año 2023. En ese sentido, ha recopilado estadísticas a través de su Centro de Quejas de Crímenes de Internet (IC3) reportando que las pérdidas por fraude de inversión aumentaron de $3.31 mil millones en 2022 a $4.57 mil millones en 2023, un incremento del 38%. Dentro de estas cifras, el fraude de inversión relacionado con criptomonedas aumentó de $2.57 mil millones en 2022 a $3.96 mil millones en 2023, es decir, un aumento del 53% (https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf).

Ejemplo de ello, es que la Fiscalía de los Estados Unidos para el Distrito de Columbia presentó el pasado 16 de julio una acción de decomiso civil para recuperar las criptomonedas confiscadas por el FBI a perpetradores en el extranjero (ubicados en Tailandia) justamente por casos vinculados con

2.En términos sencillos, el USDT (Tether) es un tipo de stablecoin, que es una criptomoneda diseñada para mantener un valor estable en relación con una moneda fiduciaria, en este caso, el dólar estadounidense. A diferencia de otras criptomonedas que pueden experimentar alta volatilidad, el USDT está respaldado por reservas de dólares o activos equivalentes para mantener su paridad de 1:1 con el dólar, proporcionando así estabilidad y reduciendo el riesgo en transacciones y operaciones en el mercado de criptomonedas

estafas *Pig Butchering* y por un monto que llegaría a los USDT 2.546.415,01 (https://www.justice.gov/usao-dc/pr/us-files-civil-forfeiture-action-recover-cryptocurrency-worth-25-million-victims-pig).

En nuestro país, en el transcurso del año 2024 se han reportado 2.204 maniobras de este tipo y la UFECI ha generado alrededor de dos decenas de investigaciones preliminares, además de asistir a diversos fiscales del país en este tipo de casos, especialmente durante el último trimestre de 2024.

Esta modalidad de fraude había sido relevada por la UFECI en años anteriores y había sido objeto de alertas en agosto de 2023 y julio de 2024[3].

Dentro de los fraudes en línea englobamos también el **acceso indebido y posterior vaciamiento de cuentas bancarias**, modalidad que fue variando a lo largo de los años. Como adelantamos, durante 2024 recibimos un total de 3.806 reportes de esta modalidad específica (18% del total de fraude en línea).

De un número modesto de reportes en 2019, los casos se incrementaron a partir del aislamiento impuesto con la pandemia del COVID-19, que generó una mayor adopción por parte de los usuarios de la banca en línea. Durante esos primeros años los casos crecieron de la mano de campañas de

3.https://www.fiscales.gob.ar/ciberdelincuencia/alertan-sobre-una-maniobra-de-fraude-a-traves-de-plataformas-que-ofrecen-supuestas-oportunidades-laborales/
https://www.fiscales.gob.ar/ciberdelincuencia/alertan-sobre-maniobras-de-fraude-en-linea-a-traves-de-nuevas-plataformas-que-ofrecen-supuestas-oportunidades-laborales-y-de-inversion/

phishing (nos referiremos a esa modalidad más adelante) que buscaban, directamente, ganar acceso a las cuentas.

Los casos disminuyeron a partir de mediados de 2021. En ese sentido, como se indicó en el Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022-2023[4], otra medida que podría explicar la pérdida de interés de las organizaciones criminales en acceder a billeteras digitales, es la imposibilidad para los autores de conseguir abultar las cuentas mediante la solicitud de préstamos preaprobados, ofrecidos por los bancos a través de las mismas plataformas, los cuales eran acreditados de manera inmediata.

Para evitar que los cibercriminales accedan, de manera inmediata a estos préstamos, se implementaron diversas resoluciones judiciales y administrativas en ese sentido. El BCRA publicó la comunicación "A" 7319[5] donde se establecieron nuevos requisitos para el otorgamiento de créditos a través de canales electrónicos.

La Secretaría de Comercio Interior de la Nación aplicó multas[6] a dos entidades financieras por haber incumplido su obligación de garantizar la protección de datos personales, cuentas e intereses económicos de sus clientes, y por no asumir la responsabilidad ante aquéllos.

Finalmente, en el mes de mayo de 2021 desde el portal institucional de este Ministerio Público Fiscal se comunicó la opinión formulada por el 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. La decisión judicial logró suspender el cobro de un crédito generado mediante una ciberestafa. En adición, se brindaron una serie de recomendaciones para evitar ser víctima de este tipo de hechos[7].

Esta disminución del acceso directo a cuentas de banco vino de la mano del aumento paulatino de otras modalidades: la transferencia voluntaria a partir de un mensaje de WhatsApp supuestamente de un conocido (la "usurpación de identidad seguida de fraude" que mencionamos más arriba y sobre la que volveremos más adelante), el acceso a las aplicaciones luego de la sustracción del teléfono y el ingreso al teléfono (y a las aplicaciones) luego de la instalación de un *software* de acceso remoto.

En el caso de la sustracción del celular, si el equipo se encuentra desbloqueado o no cuenta con esa medida de seguridad, quienes lo sustraen pueden acceder a las cuentas de redes sociales, plataformas

4.https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023/

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

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

7.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/

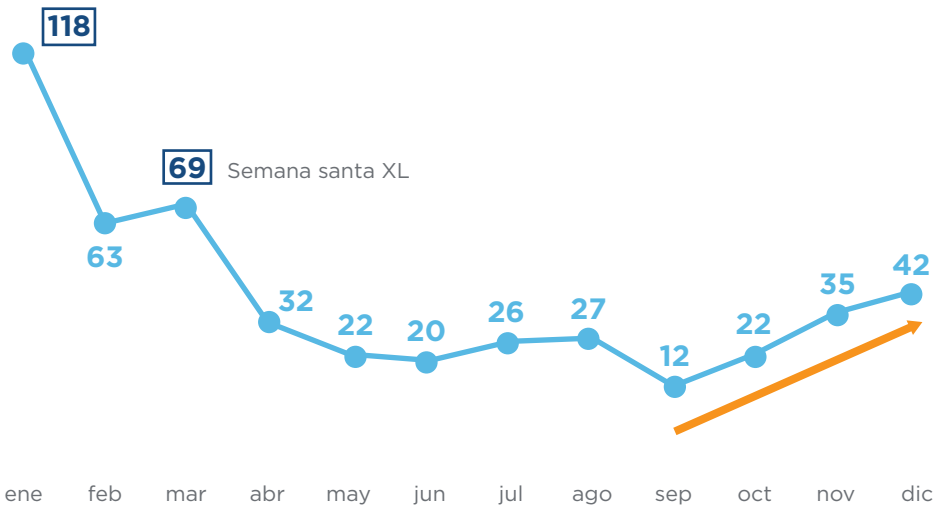
de mensajería, billeteras digitales y/o cuentas de banco. Una vez garantizado el acceso pueden realizar estafas usurpando la identidad de la víctima, solicitando dinero a los contactos, transfiriéndose dinero de las cuentas bancarias o solicitando préstamos a nombre de la víctima.

En el otro supuesto las víctimas reciben llamados de supuestos representantes de bancos, billeteras digitales, administradoras de tarjetas de crédito o empresas de servicios, usualmente con la excusa de autorizar una compra o realizar una verificación de seguridad. Luego, aprovechándose de usuarios poco informados, envían links a las víctimas, logrando instalar algún *software* de acceso remoto. Una vez que logran tomar control del dispositivo, ingresan a cuentas bancarias, billeteras virtuales o sacan préstamos a nombre de las víctimas. Una modalidad dirigida particularmente a adultos mayores, es el llamado engañoso simulando ser de una plataforma de *streaming* ofreciendo descuentos especiales para jubilados. Una variante de esta modalidad, detectada en los últimos meses del año, consiste en hacerse pasar por proveedores de servicios de internet o de telefonía celular, ofreciendo ese mismo tipo de descuentos para jubilados.

Los ataques en la actualidad incluyen no sólo las cuentas de banco sino también las billeteras digitales, cuya adopción en la sociedad ha ido en aumento a lo largo de los años. En el caso de cuentas de Mercado Pago, por ejemplo, se registraron un total de 740 casos a lo largo del año 2024. Una variante de ataque a esta billetera en particular se basa en un llamado que recibe la víctima, durante el cual su interlocutor se hace pasar por un representante de esa plataforma que necesita autorizar una compra que supuestamente intenta hacerse; en el marco de la conversación consigue hacerse de las credenciales de acceso a la cuenta, a partir de la cual la vacía, o logra que la víctima transfiera dinero a otra cuenta controlada por el atacante.

Otra de las modalidades que hemos observado durante el 2024, fueron los **fraudes en línea con ofertas de alquileres temporarios de inmuebles o reservas de establecimientos turísticos**. Se han reportado 488 casos, de los cuales el 51% han sido en los primeros tres meses del año, representando un claro sesgo estacional coincidente con el periodo vacacional estival (enero, febrero y marzo-incluyó un fin de semana extra largo del 24 al 30/3-). En esa línea, se avizoró un marcado crecimiento de los reportes a medida que se aproximaba la temporada estival 2025.

Fraude en línea - alquileres temporarios



La UFECI ya había advertido de esta maniobra en diciembre de 2021[8], en la cual el fraude se perfecciona con publicaciones de personas que no son los dueños reales o directamente no existe el inmueble.

4.3.2. Accesos ilegítimos a plataformas

Respecto a la modalidad **"Acceso ilegítimo"**, en los 2.877 reportes recibidos se destacan las maniobras de ingreso no autorizado a cuentas de WhatsApp (30%), billeteras de Mercado Pago (26%) y perfiles Facebook (15%) en primer lugar. Luego en forma más reducida, se reportaron accesos ilegítimos a cuentas de correo electrónico (Gmail y Hotmail) y perfiles de Instagram. También, dependiendo de los meses, se han reportado casos de acceso ilegítimo a otras billeteras digitales que operan en el mercado, pero los casos fueron ingresados en la modalidad de "fraude bancario", a la que nos hemos referido previamente.

Acceso ilegítimo

8.https://www.fiscales.gob.ar/ciberdelincuencia/advierten-sobre-el-aumento-de-estafas-con-falsas-ofertas-de-alquileres-temporarios-para-el-verano/

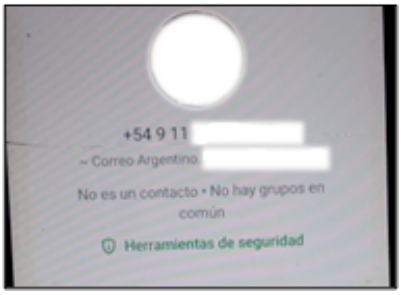
En los informes previos de la UFECI en 2022 y 2023, el acceso ilegítimo a billeteras de Mercado Pago ocupaba cómodamente el primer lugar de la modalidad, disminuyendo su incidencia en 2024 (740 reportes) para ocupar ahora el segundo lugar, detrás de las maniobras de ingreso no autorizado a cuentas de WhatsApp (872 ocasiones).

Respecto a la modalidad de acceso ilegítimo a cuentas de WhatsApp, se presenta generalmente de la siguiente manera: las víctimas reciben llamados con diversas excusas (turnos por campañas de vacunación, beneficios de algún organismo oficial, premios o descuentos de una empresa privada y del supuesto servicio técnico de la misma aplicación de WhatsApp, etc.). Luego le solicitan a la víctima que remita un código desde su teléfono, aludiendo ser un mecanismo de verificación del turno o beneficio, pero en realidad lo que se proporciona es el código que permite activar la cuenta de WhatsApp de la víctima en otro dispositivo. Una vez enviado este código (y colocado en el nuevo dispositivo) la víctima pierde el control de su cuenta.

Finalmente, haciéndose pasar por la víctima, los delincuentes contactan a los conocidos y mediante diferentes ardides les solicitan que les transfieran dinero. En muchas ocasiones los conocidos de la víctima llegan a transferir dinero antes de ser alertados de lo sucedido. También, se registran casos donde cuentas de otras redes sociales como Facebook (440 casos) y en menor medida Instagram (92 casos), son utilizadas para la misma maniobra (es posible que los casos de "acceso ilegítimo" de estas plataformas relevados sean el paso previo a este tipo de maniobras).

Llamados apócrifos con diversas excusas

¡Supuesto servicio técnico de Whatsapp!



Código de WhatsApp que no se debe compartir

< # > Codigo de WhatsApp:

O sigue este enlace para verificar tu numero: v.whatsapp.com/

No compartas este codigo con nadie.

Conversaciones apócrifas

4.3.2.1. Usurpación de identidad + fraude

Metodológicamente hemos clasificado los reportes que mencionan exclusivamente los accesos indebidos a cuentas de WhatsApp y los reportes que indican que, luego de ese acceso, se ha solicitado dinero a contactos. Los primeros, rotulados como accesos ilegítimos, representan un total de 872 casos como se mencionó anteriormente, mientras que los segundos, rotulados como **usurpación de identidad y fraude**, representan un total de 4.637 casos. La sumatoria de ambos (5.509 reportes) representa el creciente fenómeno de ataques contra cuentas de WhatsApp, ya sea como acceso ilegítimo únicamente o como medio comisivo del fraude.

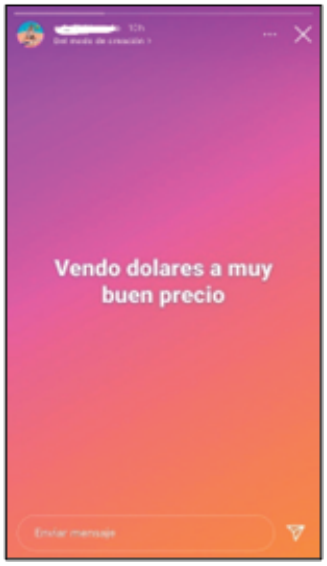
Si bien como enunciamos precedentemente, el acceso ilegítimo a cuentas de Instagram es menor cuantitativamente respecto a los reportes de WhatsApp, la red social Instagram es seguramente una de las redes más usadas en el país. Hoy es una plataforma más de comunicación, exposición y, en algunos casos, de monetización. Muchos emprendedores, comerciantes y empresas, publicitan y ofrecen sus productos a través de Instagram, convirtiendo a esta red social en un canal relevante de llegada a los clientes y consumidores. Perder el control de la cuenta, puede traer muchos perjuicios económicos y de reputación, ya sea porque los atacantes se hacen pasar por los propietarios legítimos organizando falsos envíos o sorteos[9], o porque se pide "rescate" para retomar el control de la cuenta.

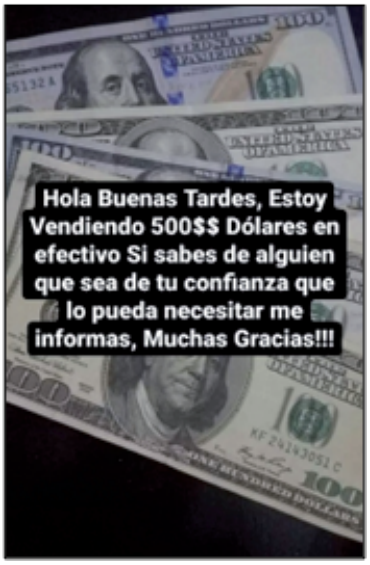
Desde la UFECI se advirtió sobre esto ya en 2019[10]. En el caso de Instagram, no existe el código de activación (como en WhatsApp) sino que los atacantes buscan que la víctima entregue su contraseña

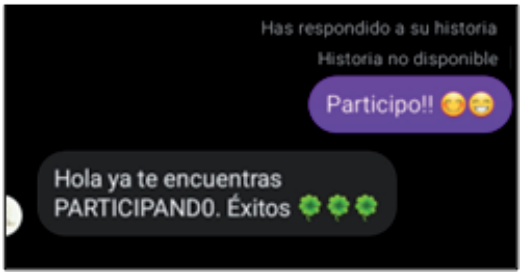
9.https://www.fiscales.gob.ar/ciberdelincuencia/la-ufeci-alerta-sobre-maniobras-de-fraude-relacionadas-con-falsos-sorteos-y-ventas-a-traves-de-instagram/

10.https://www.fiscales.gob.ar/ciberdelincuencia/consejos-de-la-unidad-fiscal-especializada-en-ciberdelincuencia-para-prevenir-ataques-a-cuentas-de-redes-sociales/

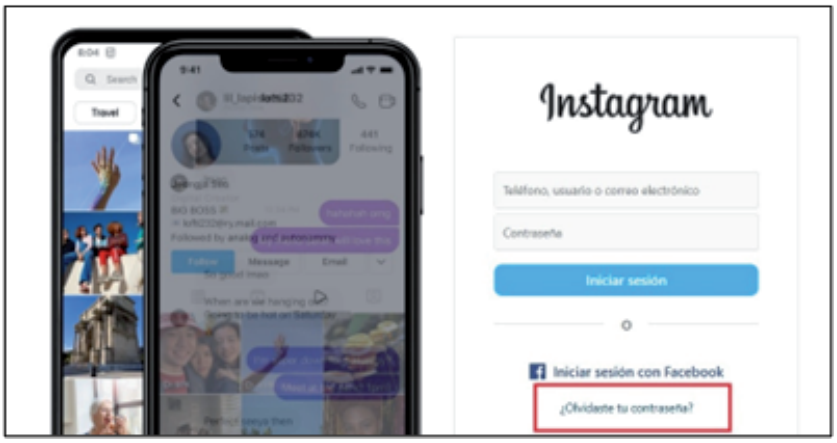
(generalmente a través de técnicas de *phishing* -captación engañosa de datos personales-) o que ellos puedan recuperarla de alguna manera.







Los atacantes solicitan recuperar la contraseña luego de hacer un SIM swapping



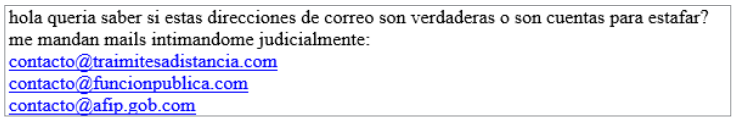
4.3.3. Phishing

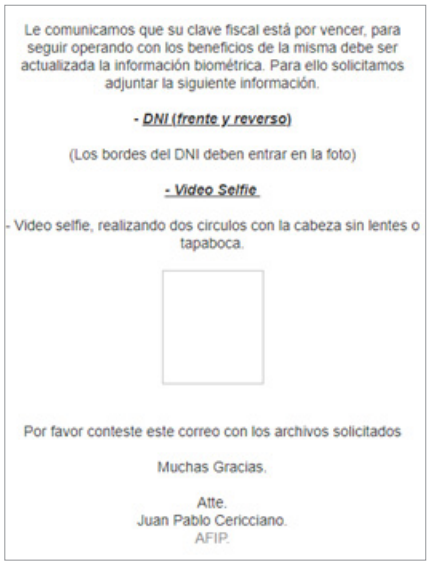
Analizando la modalidad **"*phishing*"**, podemos diferenciar los supuestos que utilizan un correo electrónico (35%) de aquellas maniobras que implican otros medios de contacto como redes sociales o llamados telefónicos (65%). Se destaca la baja de campañas específicas relacionadas a bancos y el cambio a casos relacionados con el Estado y organismos públicos en general, por ejemplo multas o citaciones judiciales.

Durante 2024, hemos recibido 545 reportes de campañas de *phishing* a través de correos electrónicos que simulan ser enviados para la realización de diversos trámites, o estudios jurídicos que se dedican a cobranzas de multas con organismos públicos o entes estatales.

Ejemplos: pago por grabado de autopartes para la verificación técnica vehicular (VTV), actualización de datos biométricos supuestamente pedidos por la entonces Administración Federal de Ingresos Públicos (AFIP)[11], pago de multa reclamado por la Policía Federal Argentina (PFA), entre otros.

Como indicamos anteriormente, en años anteriores predominaban en esta modalidad los correos electrónicos simulando ser enviados por bancos (públicos y privados), mientras que en este 2024 los reportes relacionados con organismos públicos o entes estatales ganaron incidencia llegando a niveles similares que aquellos correos electrónicos apócrifos de entidades bancarias.

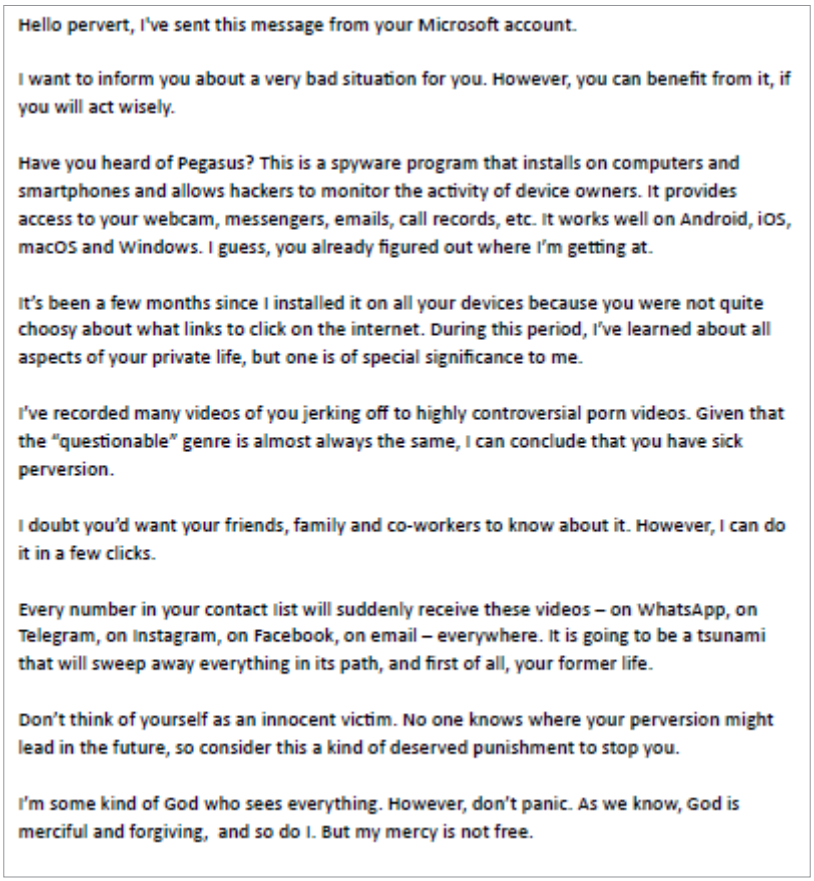




11.El Decreto 953/2024 del 24/10/2024 disolvió la AFIP siendo reemplazada por la AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO (ARCA).

4.3.4. Extorsión

Una modalidad que ha resurgido en los últimos meses, refiere a la modalidad de extorsión, ya que hemos recibido 774 reportes en el transcurso del año. En particular, se destaca la **extorsión a través de un correo electrónico** (109 casos). La maniobra consiste en hacerle saber a la víctima -a veces desde su propia casilla de correo- que a través de un *software* espía (*spyware*) se tuvo acceso a su computadora y sus dispositivos electrónicos, monitoreando el historial de navegación en Internet y la supuesta actividad del usuario, el cual habría sido registrado visualizando páginas de contenido pornográfico. Para no divulgar la información entre sus contactos, generalmente se le exige a la víctima un pago en criptoactivos.



Hello pervert, I've sent this message from your Microsoft account.

I want to inform you about a very bad situation for you. However, you can benefit from it, if you will act wisely.

Have you heard of Pegasus? This is a spyware program that installs on computers and smartphones and allows hackers to monitor the activity of device owners. It provides access to your webcam, messengers, emails, call records, etc. It works well on Android, iOS, macOS and Windows. I guess, you already figured out where I'm getting at.

It's been a few months since I installed it on all your devices because you were not quite choosy about what links to click on the internet. During this period, I've learned about all aspects of your private life, but one is of special significance to me.

I've recorded many videos of you jerking off to highly controversial porn videos. Given that the "questionable" genre is almost always the same, I can conclude that you have sick perversion.

I doubt you'd want your friends, family and co-workers to know about it. However, I can do it in a few clicks.

Every number in your contact list will suddenly receive these videos – on WhatsApp, on Telegram, on Instagram, on Facebook, on email – everywhere. It is going to be a tsunami that will sweep away everything in its path, and first of all, your former life.

Don't think of yourself as an innocent victim. No one knows where your perversion might lead in the future, so consider this a kind of deserved punishment to stop you.

I'm some kind of God who sees everything. However, don't panic. As we know, God is merciful and forgiving, and so do I. But my mercy is not free.

La UFECI ya había advertido en abril de 2020[12] y en agosto y septiembre de 2022[13], por esta modalidad.

12.https://www.fiscales.gob.ar/ciberdelincuencia/coronavirus-recomendaciones-de-la-ufeci-ante-nuevas-maniobras-de-ciberdelito/

13.https://www.fiscales.gob.ar/ciberdelincuencia/reiteran-la-alerta-sobre-una-maniobra-de-fraude-y-extorsion-a-cambio-de-no-revelar-datos-de-navegacion-en-sitios-de-contenido-pornografico/
https://www.fiscales.gob.ar/ciberdelincuencia/alertan-sobre-una-maniobra-de-fraude-y-extorsion-por-correo-electronico-a-cambio-de-no-revelar-datos-de-navegacion-en-sitios-de-contenido-pornografico/

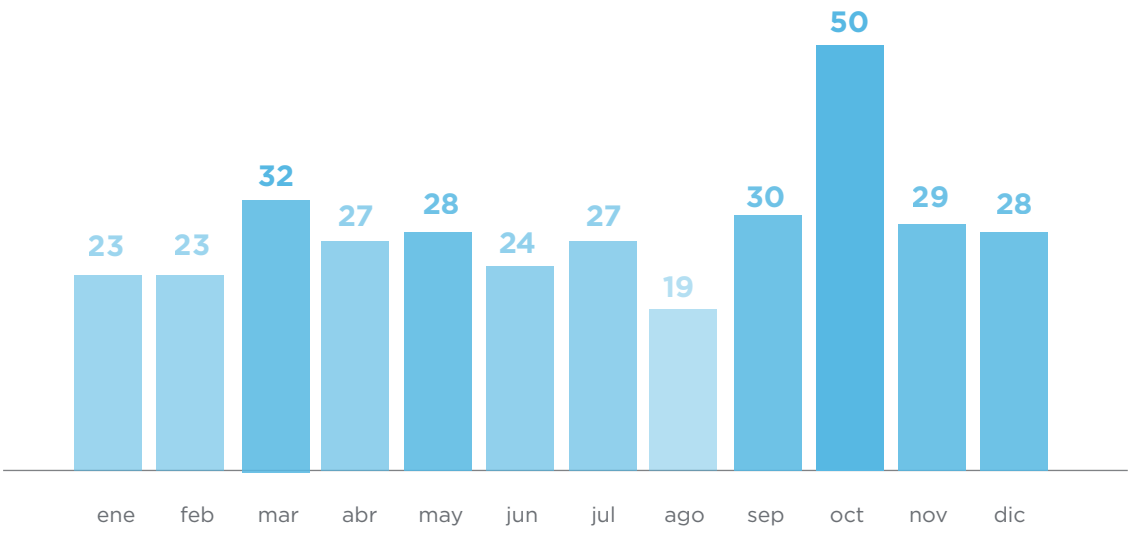
4.3.5. Acoso y difusión no autorizada de imágenes íntimas como modalidad específica de violencia contra las mujeres.

La UFECI ha recibido 1.458 reportes de acoso a través de medios telemáticos durante el año 2024. En algunos casos, esos reportes describen casos de violencia contra las mujeres.

A la luz de la sanción de la denominada "Ley Olimpia"[14] en octubre de 2023, la cual incorporó la violencia contra mujeres en entornos digitales a la Ley 26.485 (de protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres -sancionada en 2009-), durante 2024 la UFECI clasificó específicamente dentro de la modalidad de "acoso", los reportes recibidos cuyas víctimas alegaron la difusión no autorizada de imágenes íntimas, ya sea con o sin exigencias para retirar o no divulgar material, e independientemente del contexto en el que las imágenes fueron tomadas/entregadas y la forma en la que pretenden ser compartidas/divulgadas.

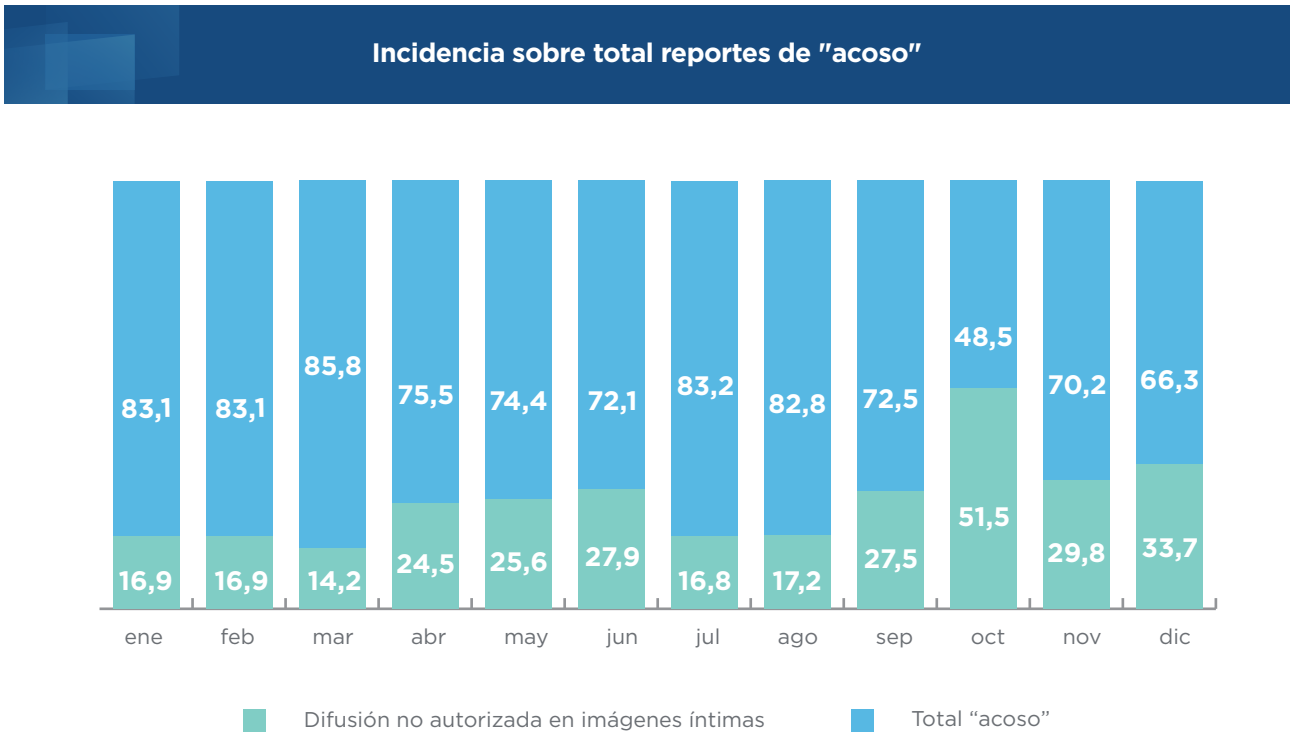
Dentro del universo de reportes de acoso, 340 se corresponden a este tipo, según la siguiente distribución mensual.

Difusión no autorizada de imágenes íntimas



Con un promedio de más de 28 casos por mes, se visualiza un aumento a partir del mes de septiembre. A continuación, se representa su incidencia en forma mensual respecto del total (en porcentaje).

14.https://www.argentina.gob.ar/noticias/ley-olimpia-el-gobierno-promulgo-la-legislacion-que-incorpora-la-violencia-digital-como-una



La difusión no autorizada de imágenes íntimas, representa el 23,3% del total de los reportes anuales por acoso, evidenciando la relevancia de la incorporación de la violencia digital entre las modalidades de violencia contra las mujeres, incorporando como objeto de la misma el respeto de la "dignidad, reputación e identidad, incluso en los espacios digitales"[15].

4.3.6. Ransomware

Otra modalidad que ha venido creciendo son los casos de *ransomware* que, si bien por su naturaleza, implican un acceso indebido a un sistema informático, lo cierto es que tienen características propias (como el pago de un rescate) que obligan a abordar la cuestión como un delito autónomo, pese a la concurrencia que se presentan en los casos con otros delitos conexos (como el daño informático).

El *ransomware* se caracteriza por la introducción en un sistema informático de un programa (*software*) malicioso (conocido como *malware*) que cifra el contenido del equipo atacado, a partir de lo cual los responsables del hecho piden una entrega de dinero -usualmente criptoactivos- para rescatar *(ransom)* los archivos, para lo cual se proporcionaría la clave para descifrarlos.

En algunos casos, además, se intimida a las víctimas con la divulgación pública de información

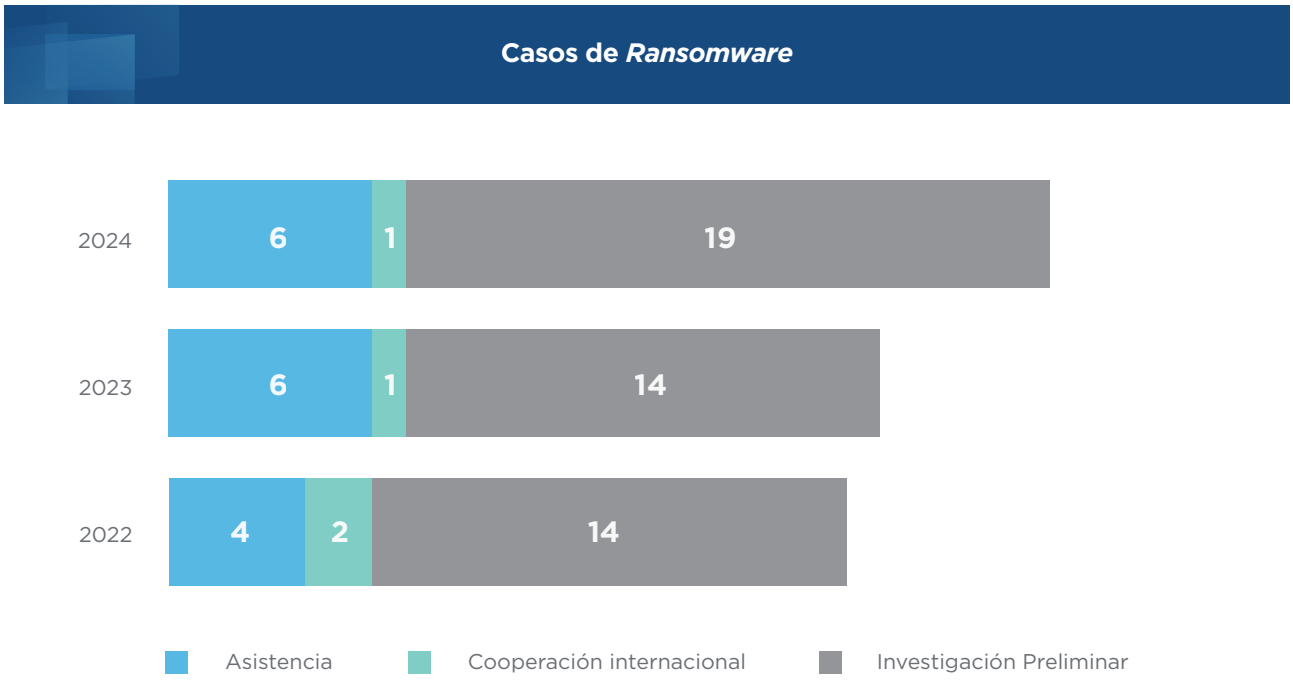
15.Ley 26.485, art. 3°, inc. d.

sensible, táctica conocida como de la “doble extorsión”.

En general, las organizaciones criminales que se encuentran detrás de estos ataques, suelen apuntar a objetivos más dirigidos que, o bien pueden ser empresas reconocidas con una actividad comercial de envergadura (como farmacéuticas, laboratorios, obras sociales o conglomerados económicos) o bien organismos públicos estatales o entidades financieras que cuentan con recursos económicos significativos. De este modo, los criminales pretenden obtener réditos económicos más importantes en la creencia de que la víctima pagará un rescate (usualmente en bitcoins) para liberar los archivos que fueron encriptados de manera maliciosa.

En la UFECI, desde el año 2022 a la fecha, hemos iniciado investigaciones preliminares y asistido a juzgados y fiscalías en esta temática en un total de 67 casos, algunos de los cuales se iniciaron a partir de información que nos han compartido autoridades extranjeras (usualmente Interpol).

Estos ataques se fueron incrementando en el tiempo pues, **mientras que en el 2022 y 2023 se registraron 20 y 21 casos respectivamente, en 2024 se ha dado un aumento del orden del 20%, contabilizando 26 casos a lo largo del año.**



En ese sentido, desde la UFECI podemos indicar (de modo inicial y sólo a los fines de dilucidar un patrón para este informe, sin considerar la posterior calificación legal que hayan realizado los magistrados de aquellas investigaciones preliminares que hemos judicializado), que en el **57%** de los casos las víctimas

se corresponden a los ecosistemas de organismos o servicios públicos, servicios de salud, energía y comunicaciones, demostrando el alto impacto social y económico que tienen estas maniobras.

Estas cifras no hacen más que resaltar la importancia de diseñar y ejecutar estrategias de seguridad informática, en especial en aquellos sectores mencionados.

5. CONCLUSIONES

El repaso de las estadísticas elaboradas y plasmadas en el presente informe refleja algunas cuestiones ciertamente preocupantes. Tal como se adelantó al comienzo, **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 en 2020, 2021 y parte de 2022, pareció haber agudizado temporalmente esta tendencia, el tiempo transcurrido luego de la vuelta a la actividad previa a marzo de 2020 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 de conductas delictivas reportadas. En adición, el desarrollo de nuevas soluciones tecnológicas que tuvo lugar durante ese periodo y la creciente adopción de herramientas digitales por parte de la ciudadanía como alternativa para realizar diversas actividades cotidianas, amplió enormemente el número de situaciones y personas potencialmente alcanzadas por la ciberdelincuencia.

En consecuencia, se agudizó la complejidad del fenómeno. Un ejemplo de ello, es el crecimiento durante 2024 de fraudes en línea del tipo esquema ponzi o estafa piramidal.

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 y las agentes que conforman el Ministerio Público Fiscal y las diferentes áreas del sistema judicial.

Finalmente, las campañas de concientización que generen en la ciudadanía en general y los usuarios en particular, un uso responsable y seguro de la tecnología, es fundamental para prevenir y morigerar el aumento de la ciberdelincuencia.

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