CIBERDELITOS DURANTE LA PANDEMIA DEL COVID-19 EN ARGENTINA: INFORME DE DENUNCIAS JUDICIALES Y MODALIDADES FRECUENTES 2020-2021

Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal

Autores:
Cintia Carnaghi
Kevin Wierzbinsky
Gustavo Sain

Ministerio de Justicia y Derechos Humanos
Argentina

Presidente de la Nación
Dr. Alberto Fernández

Ministro de Justicia y
Derechos Humanos de la Nación
Dr. Martín Soria

Secretario de Justicia
Dr. Juan Martín Mena

Subsecretario de Política
Criminal
Dr. Pablo Barbuto

Director Nacional de Política
Criminal en materia de Justicia
y Legislación Penal
Dr. Hernán Olaeta

Director de la Colección de
Estudios Estadísticos sobre cibercrimen
Mg. Gustavo Sain

ÍNDICE

5. OBSERVACIONES GENERALES

ANEXOS

1. Presentación

1.1. Introducción

Los *ciberdelitos* o delitos informáticos pueden ser entendidos como todas aquellas conductas ilícitas o antijurídicas que vulneran derechos o libertades de las personas y utilizan un dispositivo informático como *medio* para la comisión del mismo o como *fin* del delito mismo. Un dispositivo informático es toda aquella tecnología que procesa automáticamente datos e información con un fin determinado, como una computadora, una notebook, un celular inteligente, un Smart TV, una consola de videojuegos o cualquier equipo que tenga conexión a Internet, entre otros. La definición de ciberdelito o delito informático no está dada por la naturaleza criminal del acto, sino por el lugar que ocupa la tecnología en la comisión del hecho ilícito. Por ejemplo, si una persona intimida o amenaza a alguien lo puede hacer de diferentes maneras, por ejemplo, cara a cara en el mundo físico, vía telefónica o escrita. Ahora bien, cuando lo realiza a través de una computadora, celular o tablet, por ejemplo, estamos en presencia de un ciberdelito ya que el *medio* utilizado es un dispositivo informático. Cuando la tecnología es el *fin* del delito, el blanco del hecho ilícito es el propio dispositivo, donde por ejemplo un malware –software malicioso- como un virus, afecta el funcionamiento del sistema informático o los datos e información que almacena, procesa o trasmite también es un delito informático[1].

Un ciberdelito, en tanto hecho antijurídico, afecta a las personas en tanto sujetos de derechos. Cabe señalar una distinción con lo que se denomina "incidente de seguridad informático", siendo este cualquier evento que afecte el normal funcionamiento de la tecnología y el tratamiento de los datos y la información que almacena, procesa y transmite. Un incidente de seguridad puede constituir un delito informático o no, mientras que un ciberdelito puede cometerse sin necesidad de que constituya un incidente. Un incidente de seguridad informático, por ejemplo, es una falla de programación en un sistema, lo que no constituye, por ejemplo, un ciberataque, sino un error humano que altero el normal funcionamiento de la tecnología. Otro ejemplo es el grooming, el acoso sexual por parte de una persona adulta a un niño, niña o adolescente a través de servicios y aplicaciones de Internet. Ahí estamos en presencia de un ciberdelito que no produce ninguna alteración de funcionamiento de la tecnología informática. Un incidente de seguridad informática es un concepto clave del campo de la seguridad informática, el área de la informática orientada a impedir cualquier acción

[1] Sain, Gustavo.: "¿QUÉ SON LOS DELITOS INFORMÁTICOS?" En ***Rubinzal Culzoni online*** http://www.rubinzalonline.com.ar/. Buenos Aires, Rubinzal Culzoni Editores, agosto de 2015.

que afecte la ejecución de operaciones no autorizadas sobre un sistema informático. Los ciberdelitos, en cambio, son parte de la cibercriminalidad y representa aquellas conductas ilícitas donde la tecnología ocupa un rol condicionante para su comisión.

Al igual que los conceptos de ciberdelito e incidente de seguridad informático, el de ciberseguridad es un término que presenta diferencias con el de seguridad informática, aunque a veces tienden a presentarse como análogos. La ciberseguridad es un concepto amplio que va más allá de la seguridad de los dispositivos y la información almacenada, procesada y trasmitida en los dispositivos y sistemas. El mismo centra su eje en la *seguridad de las personas* y en tratar de prevenir actos disvaliosos que afecten sus derechos y garantías que puedan atentar contra su libertad, e integridad física y propiedad más que en la tecnología. Así, la ciberseguridad -si bien incluye a la seguridad informática como campo- no representa un problema meramente técnico, sino, básicamente *criminológico***.** Por ende la ciberseguridad debe ser parte de una *política de seguridad pública*[2]*.*

Según la Guía de evaluación del estado de la seguridad ciudadana en América Latina de la Organización de las Naciones Unidas (ONU)[3], una política de seguridad pública supone el desarrollo de tres acciones fundamentales, a saber; 1) la elaboración de un cuadro de situación de la violencia y el delito, 2) el desenvolvimiento de una estrategia institucional, y 3) desarrollo de una estrategia de control de la violencia y el delito. En cuanto a la primera dimensión, el *cuadro de situación de la violencia y el delito* es el proceso permanente de recopilación y sistematización de información y análisis de la misma que da cuenta de la situación del delito y la violencia existente en un tiempo y espacio determinado, su evolución, modalidades de manifestación, despliegue territorial e impacto social e institucional. Sin un diagnóstico de este tipo es imposible focalizar estrategias eficientes de prevención[4] y planificar acciones e intervenciones gubernamentales. Un cuadro de situación del delito consta de dos dimensiones, una

[2] Sain, Gustavo: Hacia un concepto amplio de ciberseguridad. En *Suplemento Innovación & Derecho*, Editorial La Ley-Thomson Reuters. Recuperado de http://www.laley.thomsonreuters.com/, agosto de 2022

[3] PNUD LAC SURF: ***Guía de evaluación el estado de la seguridad ciudadana en América Latina y el Caribe.*** Publicación de la Organización de las Naciones Unidas, 2007.

[4] La prevención abarca las acciones tendientes a impedir, evitar obstaculizar o limitar aquellos hechos que, dadas las circunstancias y elementos objetivos y concurrentes, pudieran resultar hechos delictivos u otro tipo de actos atentatorios de la seguridad pública.

objetiva y una subjetiva. La *dimensión objetiva* consta de hechos de violencia y los eventos delictivos cometidos en una jurisdicción y que hayan sido registrados por alguna agencia estatal u organización social, por un lado; y las condiciones sociales e institucionales de la violencia y el delito; los conflictos el orden público; las modalidades de criminalidad compleja; el delito violento; la violencia intrafamiliar y contra las mujeres, entre otros. La *dimensión subjetiva*, en cambio, refiere al conjunto de sensaciones, percepciones, valoraciones e interpretaciones sociales acerca del problema de la criminalidad y de las respuestas que el sistema de seguridad ciudadana[5].

Si se establece una analogía con el estado de ciberseguridad en Argentina en tanto una dimensión de la seguridad ciudadana, no existen estudios estadísticos que registren la cantidad de ciberdelitos ni incidentes de seguridad informática a nivel país, clasificaciones por tipo, modalidades de comisión, espacio geográfico y franjas horarias, perfiles etarios de las personas acusadas y tipo de víctimas, entre otros factores. En relación a la dimensión objetiva de los delitos informáticos, la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal del Ministerio de Justicia y Derechos Humanos de la Nación inició hace 10 años una serie de estudios estadísticos sobre delitos informáticos de la República Argentina, donde a partir de muestreos de las principales provincias del país, se relevaron las denuncias judiciales por infracciones a la Ley N° 26.388 de delitos informáticos y al Artículo 131 del Código Penal de la Nación, siendo la única estadística oficial a nivel nacional sobre ciberdelitos en el país[6]. En cuanto a la dimensión subjetiva, tanto a nivel de ciberdelitos como de incidentes de seguridad informáticos -salvo excepciones- hay una ausencia de encuestas de victimización y estudios certeros de evaluación a nivel nacional sobre las percepciones que posee la ciudadanía en materia de ciberseguridad. Existen artículos

[5] El abordaje de la dimensión subjetiva de la seguridad ciudadana se basa en datos provenientes de encuestas de victimización, estudios de evaluación ciudadana de los organismos del sistema de seguridad y sondeos de opinión pública. También puede fundarse en otro tipo de información procedente de notas de prensa o cualquier otra forma de manifestación de opiniones, percepciones y evaluaciones.

[6] A nivel de incidentes de seguridad informáticos, la Dirección Nacional de Ciberseguridad, dependiente de la Jefatura de Gabinete de Ministros de la Nación inició en el año 2020 la elaboración de reportes anuales de incidentes de seguridad informáticos del Centro de Emergencias Informáticas nacional (CERT.ar), aunque los mismos no representan una muestra representativa a nivel país ya que la mayoría de los mismos corresponden a los organismos de la Administración Publica Nacional. Por último, existen informes elaborados por empresas de seguridad informática al respecto -con fuentes de datos no especificadas- en términos de incidentes de seguridad informáticos o estadísticas judiciales realizadas por fiscalías en delitos informáticos por algunas jurisdicciones que no resultan representativas.

periodísticos que describen ciertos casos resonantes en cuanto a sus modus operandi de ciberdelitos, tanto así como algunos informes elaborados por empresas de seguridad informática en materia de incidentes de seguridad informáticos, sin rigurosidad en cuanto a la representatividad de las muestras, en tanto que no existen criterios de selección científicos para la pre selección del universo de personas entrevistadas.

El uso de tecnologías de la información y comunicación digitales –TICDs- se incrementó exponencialmente a nivel global durante los últimos años. El desarrollo de tecnologías de procesamiento masivo de datos (*big data*), la computación en la nube (*cloud computing*) y la llamada Internet de las cosas (Internet of things *IoT*), sumado a la utilización de redes sociales y sistemas de mensajería como herramientas cotidianas de comunicación, plantea la necesidad gubernamental de los Estados a proteger sus infraestructuras tecnológicas y los datos personales de la ciudadanía. Desde que la Organización Mundial de la Salud (OMS) decretó como pandémica la expansión del virus SARS-CoV2 que produce el COVID-19 a comienzos de 2020[7], muchos gobiernos de todo el mundo establecieron medidas de prevención a la ciudadanía basadas en el aislamiento social y reclusión domiciliaria, lo que produjo una notable aceleración de actividades remotas desde el hogar. De esta manera, el desarrollo del *teletrabajo*, la *educación a distancia* y el *incremento del comercio electrónico* a través de servicios y aplicaciones de Internet, pasaron a ser parte de las actividades cotidianas de grandes sectores de la población, lo que trajo aparejado, a su vez, un incremento de riesgos y amenazas en línea, tanto, así como el desarrollo de nuevas *modalidades de ciberdelito*, muchas de ellas, *más complejas y organizadas*. El desarrollo de este tipo de estudios pretende ser un insumo fundamental para el diseño de políticas públicas preventivas en materia de ciberseguridad.

1.2. Alcances del estudio

En el marco de las competencias asignadas a la Dirección Nacional de Política Criminal en Materia de Justicia y Legislación Penal de elaborar la estadística oficial en materia delictiva y el funcionamiento del sistema penal de la República Argentina (Resolución 1838/2021 del Ministerio de Justicia y Derechos Humanos de la Nación)**,** este estudio toma como referencia las denuncias ingresadas en los diferentes sistemas de justicia provinciales de la República Argentina en relación con las figuras penales contempladas en la Ley Nº 26.388 del año 2008 –conocida como "Ley de Delitos informáticos de la

[7] "LA OMS CARACTERIZA A COVID-19 COMO PANDEMIA". Publicación de la Organización Panamericana de la Salud (OPS), 11 de marzo de 2020. Disponible en https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia

República Argentina"- y sus modificatorias y la Ley Nº 26.904 del año 2013 sobre -o "Ley de Grooming"-. A partir de los señalado anteriormente, este estudio no pretende arrojar una muestra representativa del estado de la cibercriminalidad en el país ya que, si bien existen una serie de figuras penales incorporadas a partir de esta normativa, por definición, varios delitos convencionales que figuran en nuestro código pueden constituir delitos de tipo informático si median las tecnologías de la información y la comunicación digitales paraos su comisión, como se señaló anteriormente.

Asimismo, cabe señalar que una de las características que poseen los ciberdelitos es su *amplia cifra oculta,* es decir, el *bajo índice de denuncia judicial* que poseen esas conductas ilícitas, no solo en Argentina sino también a nivel global, fundamentalmente por varios factores, entre los que podemos señalar como más importantes;

- El desconocimiento de algunos usuarios de TICDs de que están siendo víctimas de un delito informático. Por citar un ejemplo, por un lado una persona puede descargar a su computadora, sin saberlo, un software espía –spyware- que registra todo lo que teclea un usuario/a sin percibir la existencia del mismo. Estos programas se denominan keylogger -logueo de claves- y los ciberdelicuentes lo utilizan, por ejemplo, para obtener sus credenciales de acceso a los sistemas, por ejemplo, nombre de usuario y contraseña de un sistema de homebanking para vaciar la cuenta bancaria de la potencial víctima.

- El temor de las empresas a denunciar ante la justicia un incidente de seguridad informático -como, por ejemplo, un ciberataque a sus sistemas- para no ver afectada su imagen y reputación organizacional, evitar sanciones y multas por parte de organismos gubernamentales, o simplemente evitar demandas colectivas por parte de clientes, entre otros motivos. En estos casos la mayoría de las veces la organización trata de solucionar este hecho ilícito en forma técnica a través de las áreas de TI -Tecnología Informática- o Sistemas, si no es que tienen un equipo de respuesta a emergencias informáticas (CERT, por sus siglas en inglés) o un área de ciberseguridad o seguridad de la información corporativa, sin realizar la correspondiente denuncia judicial.

- La ausencia de legislación que establezca una pena este tipo de conductas ilícitas en determinados países, -en materia penal, civil o comercial, entre otras, como así también en materia procesal penal, es decir, lo que marca una ausencia de herramientas legales que permitan obtener de manera adecuada rastros e indicios que posteriormente puedan ser aceptados por la justicia en términos de evidencia digital en el marco de una investigación criminal de este tipo de delitos.

- La falta de formación y capacitación de juece/as, fiscales, perito/as o miembros de las fuerzas de seguridad en función judicial para llevar adelante una correcta investigación criminal, tanto así como la ausencia de laboratorios forenses informáticos óptimos con la infraestructura tecnológica suficiente para desarrollar el procesamiento y análisis de la evidencia digital en el marco de las causas que involucran dispositivos informáticos.

- El imaginario social presente en un sector de la población de que la justicia no va a poder resolver esos casos en tanto que sus autore/as son personas con altos conocimientos en programación y sistemas informáticos –identificados como "hackers"- capaces de sortear la ley y ocultar su identidad ante una investigación criminal.

Pero básicamente los dos factores más importantes que explican la amplia cifra oculta de los delitos informáticos son las *resoluciones tecnológicas y administrativas* de este tipo de conductas, a saber;

- *Resoluciones tecnológicas:* Un ejemplo sucede cuando un virus informático intenta ingresar a una computadora y un programa antivirus lo detecta y lo elimina del sistema informático[8]. A partir de este ejemplo podemos identificar varios delitos; por un lado, alguien diseñó el programa malicioso con un fin ilícito. Asimismo, esa misma persona u otra/s lo distribuyó o intentó ingresar en forma indebida y no autorizada a un dispositivo de un tercero para instalado. En la mayoría de estos casos los usuario/as no realizan la denuncia judicial, ya que obtuvo una resolución técnica que impidió afectar la normal operatividad del dispositivo, tanto asi como su contenido, es decir, los datos y la información que almacena.

- *Resoluciones administrativas:* Un ejemplo lo es el sabotaje a una cuenta bancaria a partir del robo de credenciales de acceso a los sistemas de homebanking con el objetivo de "vaciarla", transfiriendo los fondos de la víctima a otra cuenta controlada por el/la ciberdelincuente. En estos casos de "hackeo", la principal preocupación del/ de la titular es recuperar el dinero perdido. En la mayoría de los casos, la víctima se comunica en primera instancia con la institución bancaria y notifica del acceso indebido. El caso puede pasar al área de fraude de la

[8] Un virus es un programa malicioso que tiene como objetivo causar daños al funcionamiento del sistema o afectar la disponibilidad de los datos e información almacenados o procesados por el mismo.

organización para ser analizado para la devolución del dinero. En este caso, si el banco le reintegra los fondos, hubo una resolución administrativa del hecho ilícito, para lo cual la persona habitualmente no realiza la denuncia penal correspondiente para la persecución penal del o los responsables del mismo[9].

Estos factores que explican el bajo índice de denuncia judicial que poseen este tipo de conductas permite entender, quizá, porque no existe la factibilidad de poder obtener, como suceden con otras figuras delictivas, *la tasa de ciberdelito por habitante de un país*, como sucede a nivel global con los homicidios o femicidios, por ejemplo. En la actualidad no existe país que puede afirmar cuál es esta cifra en forma certera.

ADVERTENCIA:

Los datos estadísticos presentados en el informe no pretenden ser representativos en términos absolutos acerca de la cantidad total de denuncias realizadas en base a las leyes de delitos informáticos y grooming de la República Argentina. Muchas oficinas judiciales de estadísticas abocadas al acopio de este tipo de información vieron limitada su funcionalidad durante los años 2020 y 2121 al igual que otras organizaciones en el marco del ASPO. Esto hizo que en algunas jurisdicciones los datos no reflejen los totales de ingresos, motivo por el cual la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal intentó obtener datos de otras fuentes ajenas a los Ministerios Públicos Fiscales que permitan dar una aproximación acerca de las figuras penales más denunciadas durante el período analizado por jurisdicción.

Es así como el presente estudio pretende dar una aproximación a las figuras más denunciadas por distrito, tanto así como las posibles variaciones en cantidades de las mismas, sin posibilidad de establecer comparativas entre provincias por lo dicho en el párrafo anterior. A partir de esta limitación, el objetivo principal del estudio es el de poder arrojar algunas conclusiones generales al fenómeno del ciberdelito durante la Pandemia del COVID-19 en la República Argentina.

[9] Sain, Gustavo: "CIBERCRIMEN: EL DELITO EN LA SOCIEDAD DE LA INFORMACIÓN". En Eissa, Sergio (Coord.): ***Políticas públicas y seguridad ciudadana***. Buenos Aires, Eudeba, 2015.

1.3. Figuras penales contempladas en la Ley Nº 26.388 o "Ley de delitos informáticos"

Artículo	Texto del Código Penal de la Nación	Descripción
Art. 2: Ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil y tenencia con fines de distribución	Art. 128 CP: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años. Todas las escalas penales previstas en este artículo se elevarán 1/3 en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años. *Nota: artículo modificado mediante la Ley Nº 27.436 en 2018*	Incluye la creación y elaboración de imágenes, fotografías o representaciones de personas menores de edad, tanto así como el lucro de la misma y la facilitación de recursos materiales y humanos para la organización de un negocio relacionado con este material. También la oferta, venta, alquiler, distribución gratuita mediante soportes físicos (papel, CDs, DVDs), tanto así como la transmisión por Internet (correo electrónico, sistema de mensajería, programas de intercambio de archivos o sitios web, entre otros). La tenencia personal a los fines de consumo también se encuentra penada bajo esta figura, tanto así como la transmisión o cesión a otra persona. Los contenidos no necesariamente deben ser reales sino representaciones de partes genitales con fines predominantemente sexuales. En este caso se excluye la finalidad educativa o de investigación.

Art. 4: Violación de correspondencia electrónica	Art. 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.	Refiere al acceso indebido a comunicaciones de carácter privado, es decir, de acceso restringido (por ejemplo, mediante nombre de usuario y contraseña) como sucede con el correo electrónico, un mensaje privado de una red social, chats personalizados, mensajes de texto (SMS) o de servicios de mensajería (WhatsApp, entre otros). Cuando se habla de comunicaciones electrónicas, las mismas no incluyen solamente texto, sino también elementos multimedia como audio y video, como sucede en conversaciones a través audios o videoconferencias. La apertura y acceso refriere específicamente a los mensajes y no a los sistemas de uso como por ejemplo a una casilla de mail. Cuando se hace alusión al apoderamiento puede ser mediante una impresión, tanto así como una fotografía de los mismos tomados por un celular. El desvío o supresión impide que el mensaje llegue a destino, eliminándolo o modificando el destinatario, por ejemplo.
Art. 5: Acceso ilegítimo a un sistema o dato informático	Art. 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.	A diferencia del artículo anterior que alude a las comunicaciones electrónicas, éste pena el acceso indebido y no autorizado a un sistema de carácter privado o restringido como lo puede ser una casilla de correo electrónico, el perfil de una red social, una cuenta de chat, o cualquier archivo o documento que sea de carácter restringido y no público. El uso de programas espías (Spyware) para recopilación de datos personales sin el consentimiento del usuario ingresa en

		esta figura, tanto así como el acceso a un dispositivo que no sea público sino que insuma un uso personal y específico de un usuario.
Art. 6: Publicación indebida de comunicaciones electrónicas	Art. 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.	El artículo refiere directamente a la publicidad del contenido de una comunicación electrónica de carácter privado y restringido sin autorización de su titular o legítimo usuario, como lo puede ser un correo electrónico, un mensaje privado de una red social, una comunicación de chat o servicio de mensajería, tanto así como una conversación de audio o de video de computadora o telefonía móvil. El artículo refiere como "conducta" publicar por sí o hacer publicar por un tercero, total o parcialmente, por cualquier medio y en forma indebida, una comunicación no destinada a publicidad, poniéndola en conocimiento de un grupo indeterminado de personas. Para que exista perjuicio debe causar o poder causar perjuicio a terceros (moral, patrimonial, material, etc.). El perjuicio debe derivar del contenido que se hace público indebidamente. El/la autor/a del contenido publicado indebidamente debe ser determinado o determinable (víctima del perjuicio). La exención de responsabilidad sucede cuando el/la agente hubiere obrado con el propósito inequívoco de proteger un interés público (protección de la seguridad, el orden público, instituciones democráticas, economía, interés público, aspectos vinculados con la conducta de funcionario/as público/as,).

Art. 7: Revelación de secretos	Art. 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.	Pena la publicación o comunicación de datos personales de tipo confidenciales a un tercero por parte de un funcionario público, como puede ser una disposición secreta, un decreto reservado, información clasificada que hace a la seguridad de la Nación, datos estadísticos no públicos, etc. En este caso no hay intrusión, se accede legítimamente a la información, pero ésta debe permanecer dentro de la administración pública ya que existe una prohibición legal de divulgación. El acto se consuma con la divulgación a quien no debe conocer la información. Por último, se exclusión de responsabilidad penal cuando dicha información se da a conocer a sujetos que se encuentran incluidos entre aquellos que sí pueden conocer esa información, como por ejemplo, un superior jerárquico.
Art. 8: Delitos relacionados con la protección de datos personales	Art. 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.	Al igual que el art. 153 bis del Código Penal, se pena el acceso a un sistema informático de acceso restringido en forma no autorizada, pero en esta figura se hace alusión a una base de datos personales más que el sistema en sí, con información personal de terceras personas que pueden afectar sus derechos o perjudicarles económicamente (lesión al honor, al patrimonio, a la vida, la salud, entre otros). Se sanciona a quien accede ilegítimamente, a sabiendas de la ilegitimidad, o violando sistemas de confidencialidad y seguridad de datos a una base de información personal.

	3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.	Asimismo, también pena la revelación de estos datos a terceras personas y la alteración de esta información. Se sanciona también a quien inserta ilegítimamente o hace insertar por otro, datos en una base de datos personales (alteración de la información, no importa si los datos que se insertan son verdaderos o falsos).
Art. 9: Estafa informática	Art. 173: (…) se considerarán casos especiales de defraudación y sufrirán la pena que él establece: (…) Inc. 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.	Requiere la existencia de defraudación (ardid o engaño) con causación de perjuicio patrimonial (desplazamiento de bienes o servicios en favor del/de la autor/a). Se incriminan las defraudaciones cometidas mediante cualquier modificación del resultado de un proceso automatizado de datos, sea que se produzca a través de la introducción de nuevos datos o de la alteración de los existentes, en cualquiera de las fases de tratamiento o procesamiento informático. Debe haber una alteración del normal funcionamiento del sistema informático o de la transmisión de datos. Cuando se refiere a manipulación informática alude a la alteración del normal funcionamiento de manera clandestina, es decir, sin autorización para dicha tarea. Puede incluir la alteración de registros para obtener beneficios de pagos mediante el acceso a una cuenta bancaria, y la realización de transferencias de dinero no autorizadas, entre otras.

		Incluye también la manipulación informática cuando se altera la transmisión de los datos con los que opera el sistema, aun cuando no se modifiquen los asientos, entradas o registros, mediante la interferencia de los datos que intercambia el sistema con los usuarios, para modificarlos y producir el desplazamiento patrimonial. También se incluye el robo de servicios de telecomunicaciones, como el servicio telefónico o de videocable, o los casos de "phishing" -en tanto técnica utilizada para el robo de identidad de las personas para cometer un delito posteriormente-.
Art. 10: Daño a bienes intangibles y distribución de virus informáticos	Art. 183: Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.	Esta figura pena la alteración, destrucción e inutilización de hardware (computadoras, celulares, CD, DVDS, pendrives, cámaras fotográficas, escáneres, o cualquier otro dispositivo), tanto así el daño a datos e información y programas mediante virus, gusanos y troyanos u otro malware que los pueda destruir, inutilizar, hacer desaparecer. Incluye la elaboración, distribución y venta de programas maliciosos diseñados con el fin de dañar un dispositivo informático o la información en él contenida, sea a título gratuito u oneroso.
Art. 11: Daño a bienes intangibles y distribución de virus informáticos (agravado)	Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: (…) 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros	En relación a la figura anterior, el daño resulta agravado si el objeto del crimen son los dispositivos, programas o información contenida en los sistemas informáticos del sector público, tanto así como aquellos destinados a la atención de salud, sistemas de comunicaciones , medios de trasporte o

	u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.	servicios de energía, lo que se denominan "infraestructuras críticas de información"
Art. 12: Interrupción o entorpecimiento de comunicaciones electrónicas	Artículo 197 - Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.	En materia de comunicaciones electrónicas, se incluyen los denominados ataques de denegación de servicio, es decir, el ataque por de varias computadoras hacia un dispositivo/s concreto/con la finalidad de entorpecer o interrumpir las comunicaciones, ralentizando u obstruyendo las comunicaciones. Incluye cualquier ataque que afecte el software y hardware de un dispositivo utilizado para establecer comunicaciones, como un celular o cualquier factor que altere o impida la comunicación entre personas a través de correo electrónico, comunicaciones de audio por internet, videoconferencias y sistemas de mensajería por celular, entre otros. Se sanciona también a aquel que, una vez interrumpida o entorpecida la comunicación, se resistiere violentamente al restablecimiento de la comunicación interrumpida.
Art. 13: Alteración de evidencia informática	Artículo 255. - Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la	Se criminaliza la sustracción, alteración, ocultamiento, destrucción o inutilización total o parcial, de objetos (hardware y software) destinados a servir como elementos de prueba ante la autoridad competente (administrativa o judicial).

custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).	Incluye la sustracción, alteración, ocultamiento, destrucción o inutilización total o parcial de registros o documentos que se encuentren bajo custodia de un funcionario público o de otra persona que oficia en interés de un servicio público. En caso de imprudencia o negligencia del depositario, la pena es de multa.

Figuras penales contempladas en la Ley Nº 26.904 o "Ley de grooming"

Artículo de la Ley	Texto del Código Penal de la Nación	Descripción
Art. 1: Grooming	'Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.'	Se reprime a la persona adulta que contacta a un menor de edad, valiéndose de herramientas informáticas, con la finalidad de cometer cualquier delito contra la integridad sexual. Según el artículo 25 del Código Civil y Comercial de la Nación, una persona menor de edad es aquella que no ha cumplido la edad de 18 años. El contacto puede darse en plataformas de intercambio de mensajes, redes sociales, mails, plataformas de videojuegos, foros, u otros espacios donde participan los niños, niñas y adolescentes.

2. Denuncias judiciales de delitos informáticos – Total País

2. Denuncias judiciales de delitos informáticos – Total país

Año 2020:

Referencias	Delitos investigados
Figuras penales contempladas en la Leyes N° 26.388 y 26.904	9.604

Año 2021:

Referencias	Delitos investigados
Figuras penales contempladas en la Leyes N° 26.388 y 26.904	11.593

2.1. Distribución por distrito

Año 2020:

Del total de delitos ingresados, la distribución por distrito es:

Distrito	Delitos investigados
Provincia de Buenos Aires	5.540
Tierra del Fuego	1.449
Santa Fe	640
Mendoza	407
Río Negro	356
Justicia Federal/Nacional	308
Córdoba	258
CABA	153
Chubut	72
Santa Cruz	66
Neuquén	64
Misiones	58
Tucumán	47
Formosa	44
La Pampa	43
Catamarca	27
San Luis	24
Entre Ríos	20

Corrientes	13
Salta	6
La Rioja	5
Santiago del Estero	4
Jujuy	-
Chaco	-
San Juan	-
TOTAL	**9.604**

Fuente: Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal – Ministerio de Justicia y Derechos Humanos de la Nación.

Año 2021:

Del total de delitos ingresados, la distribución por distrito es:

Distrito	Delitos investigados
Provincia de Buenos Aires	6.700
Tierra del Fuego	1.930
Mendoza	1.144
Santa Fe	803
Río Negro	427
Justicia Federal/Nacional	411
Córdoba	305
CABA	157
Neuquén	151
Santa Cruz	94
Misiones	85
Chubut	78
Tucumán	63
Catamarca	51
La Pampa	45
Formosa	36
Entre Ríos	33
San Luis	20
Salta	20
La Rioja	16
Corrientes	13
Santiago del Estero	11
Jujuy	-
Chaco	-
San Juan	-
TOTAL	**12.593**

Fuente: Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal – Ministerio de Justicia y Derechos Humanos de la Nación.

2.1. Distribución por figura penal

Del total de delitos ingresados, la distribución por figura penal es:

Año 2020:

Figura penal	Delitos investigados
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	4.446
Art. 131 CP: Grooming	1.751
Art 173 inc. 16 del CP: Estafa informática	1.593
Art. 183 CP: Daño a bienes intangibles y distribución de virus	1.086
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	257
Art. 153 CP: Violación de correspondencia electrónica	121
Art. 255 CP: Alteración de evidencia informática	124
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	95
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	49
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	49
Art. 157 CP: Revelación de secretos	19
Art. 155 CP: Publicación indebida de comunicaciones	14
TOTAL	**9.604**

Fuente: Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal – Ministerio de Justicia y Derechos Humanos de la Nación.

Año 2021:

Figura penal	Delitos investigados
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	4.526
Art 173 inc. 16 del CP: Estafa informática	3.766
Art. 131 CP: Grooming	1.878
Art. 183 CP: Daño a bienes intangibles y distribución de virus	1.295
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	482
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	164
Art. 153 CP: Violación de correspondencia electrónica	151
Art. 255 CP: Alteración de evidencia informática	106
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	102
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	78
Art. 157 CP: Revelación de secretos	24
Art. 155 CP: Publicación indebida de comunicaciones	21
TOTAL	**12.593**

Fuente: Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal – Ministerio de Justicia y Derechos Humanos de la Nación.

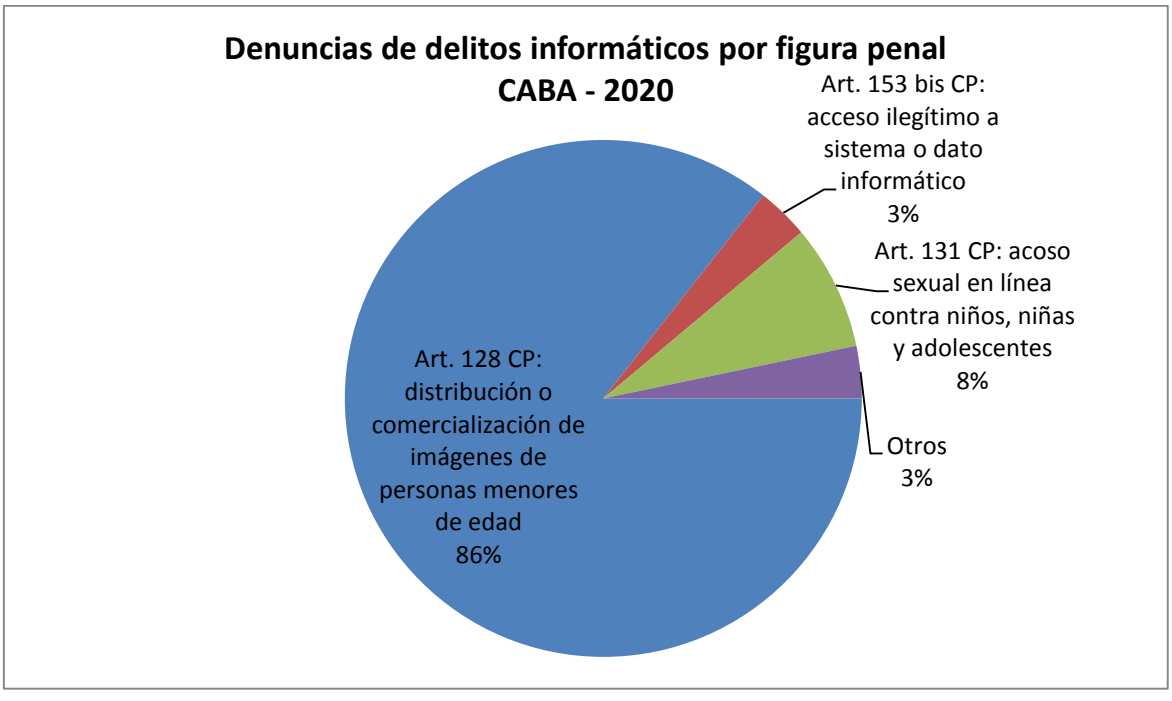
3. Denuncias judiciales de delitos informáticos – Por provincia

3.1. Ciudad Autónoma de Buenos Aires

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	131
Art. 131 CP: Grooming	12
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	5
Art 173 inc. 16 CPN: Estafa informática	2
Art. 183 CP: Daño a bienes intangibles y distribución de virus	2
Art. 153 CP: Violación de correspondencia electrónica	1
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**153**

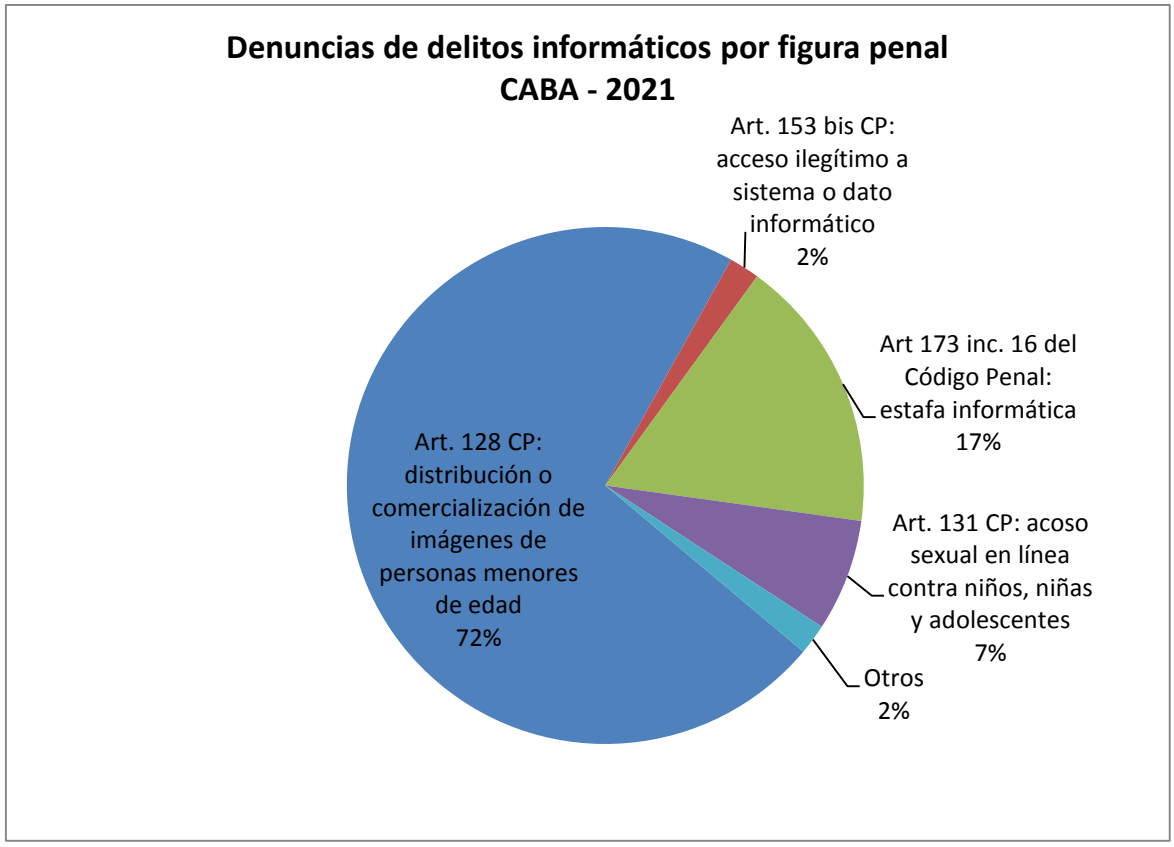
Fuente: Secretaría de Innovación del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	113
Art 173 inc. 16 CP: Estafa informática	27
Art. 131 del CP: Grooming	11
Art. 153 bis del CP: Acceso ilegítimo a sistema o dato informático	3
Art. 183 del CP: Daño a bienes intangibles y distribución de virus	2
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	1
Art. 153 del CP: Violación de correspondencia electrónica	-
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**157**

Fuente: Secretaría de Innovación del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

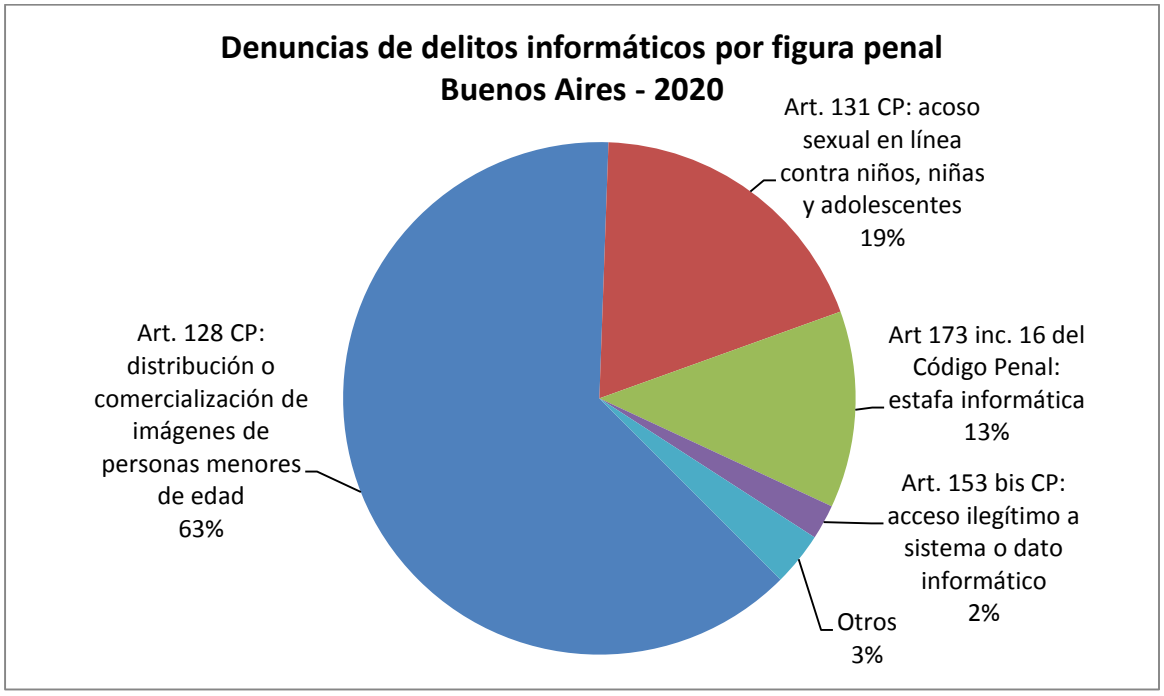


3.2. Buenos Aires

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	3.494
Art. 131 CP: Grooming	1.049
Art 173 inc. 16 CPN: Estafa informática	688
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	122
Art. 255 CP: Alteración de evidencia informática	58
Art. 183 CP: Daño a bienes intangibles y distribución de virus	47
Art. 153 CP: Violación de correspondencia electrónica	37
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	18
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	13
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	6
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	6
Art. 157 CP: Revelación de secretos	2
TOTAL	**5.540**

Fuente: Ministerio Público de la Provincia de Buenos Aires / Secretaría de Planificación de la Suprema Corte de Justicia de la Provincia de Buenos Aires.

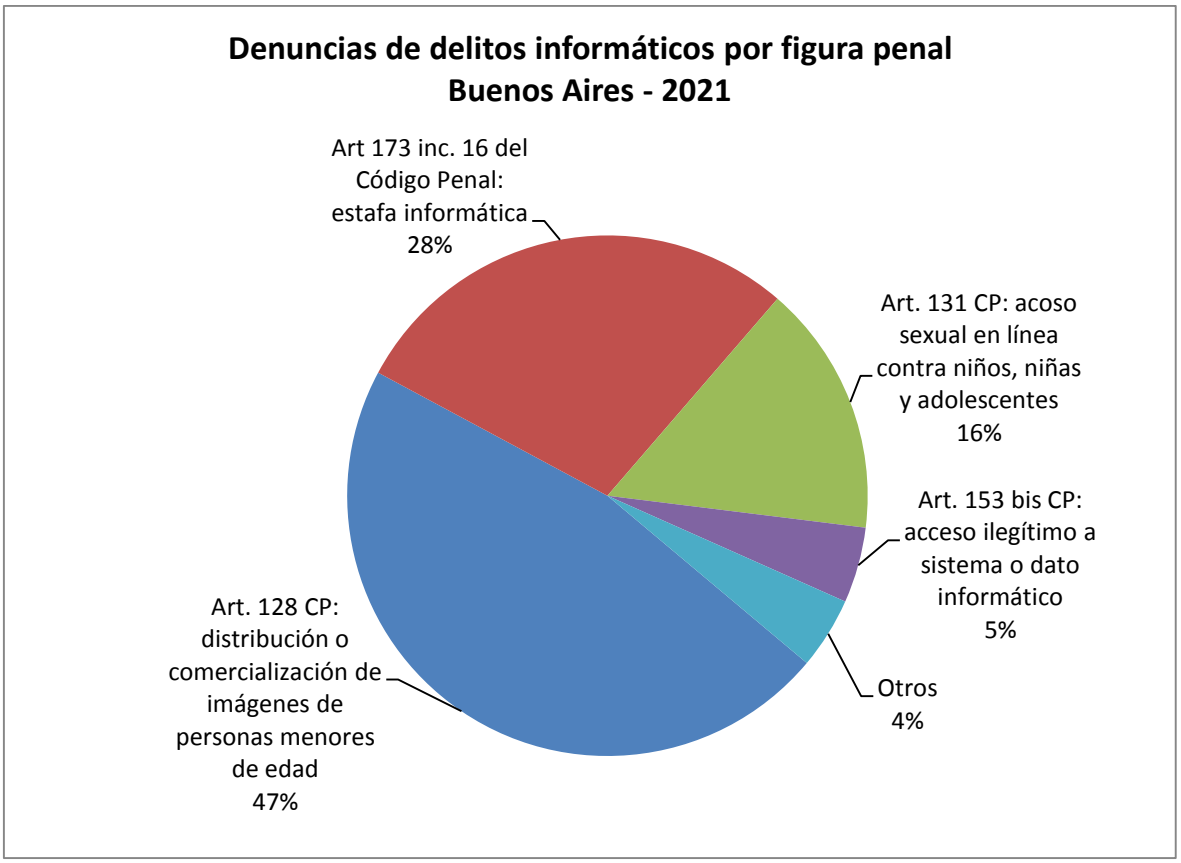


Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	3131

Art 173 inc. 16 CP: Estafa informática	1909
Art. 131 CP: Grooming	1047
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	315
Art. 183 CP: Daño a bienes intangibles y distribución de virus	91
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	60
Art. 255 CP: Alteración de evidencia informática	54
Art. 153 CP: Violación de correspondencia electrónica	52
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	26
Art. 184 CP: daño a bienes intangibles y distribución de virus agravado	8
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	6
Art. 157 CP: Revelación de secretos	1
TOTAL	**6700**

Fuente: Ministerio Público de la Provincia de Buenos Aires / Secretaría de Planificación de la Suprema Corte de Justicia de la Provincia de Buenos Aires.

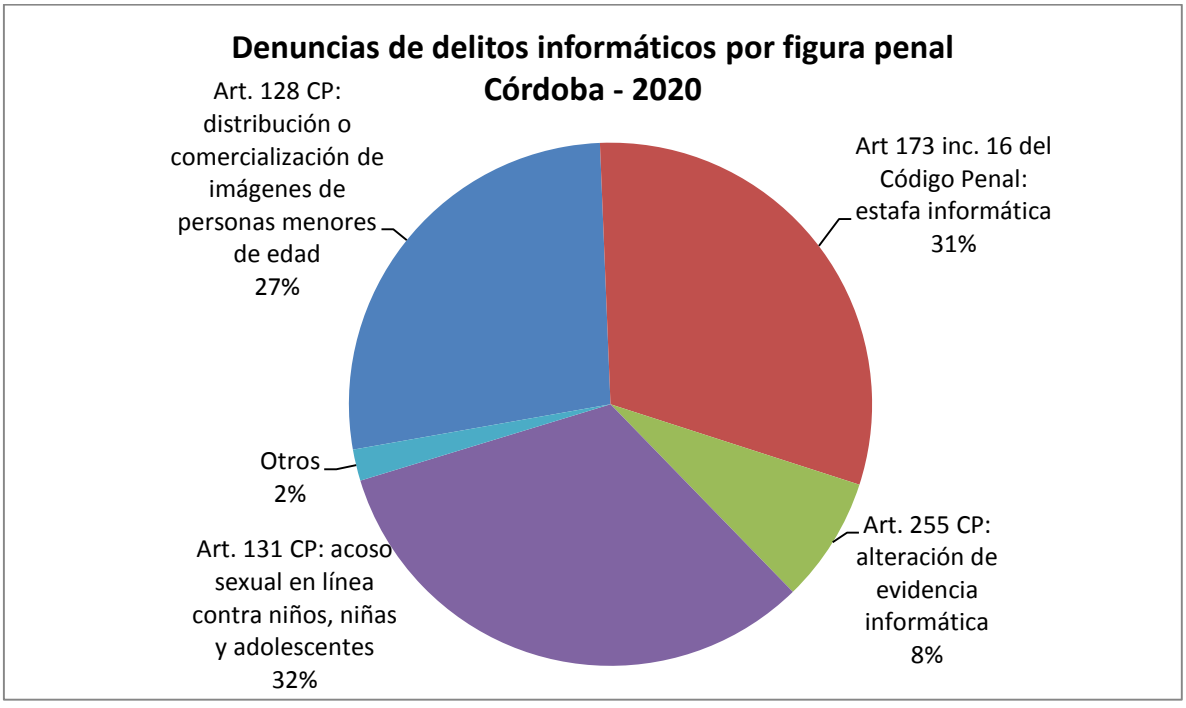


3.3. Córdoba

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	84
Art 173 inc. 16 CP: Estafa informática	79
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	70
Art. 255 CP: Alteración de evidencia informática	20
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	3
Art. 153 CP: Violación de correspondencia electrónica	2
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**258**

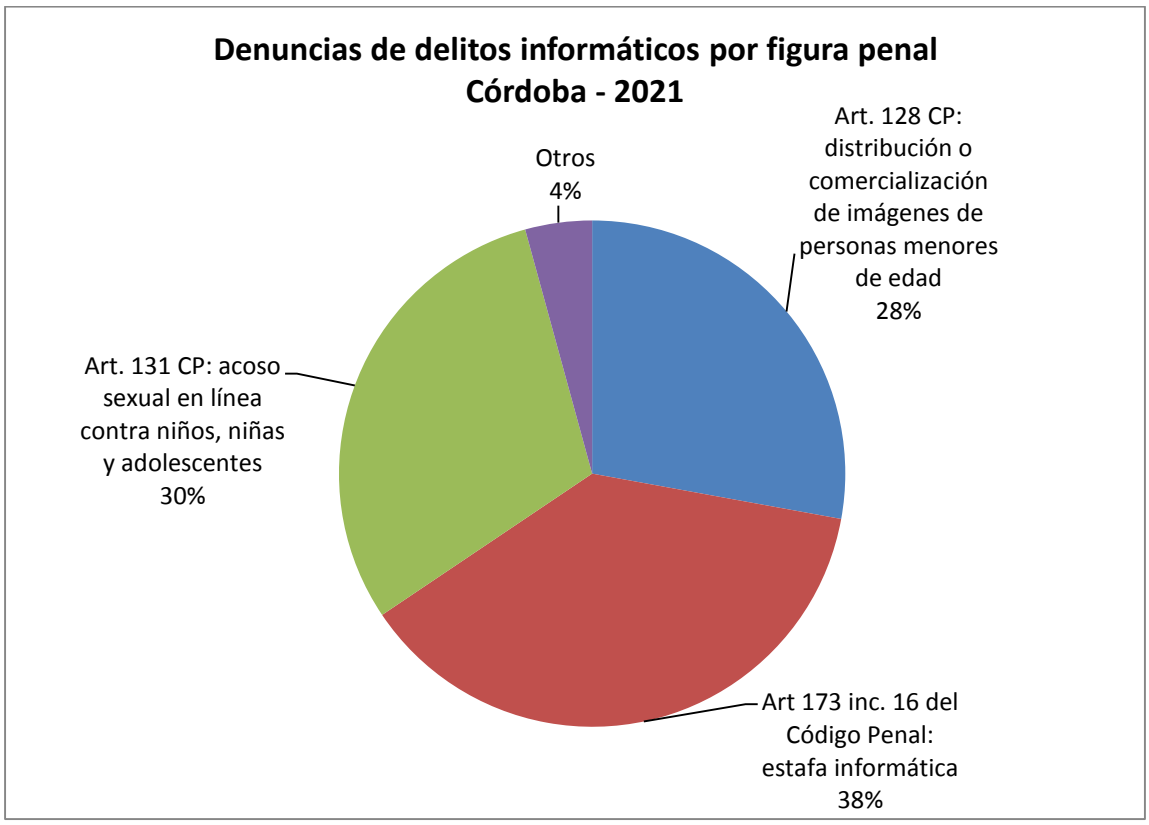
Fuente: Tribunal Superior de Justicia del Poder Judicial de la Provincia de Córdoba



Año 2021:

Figura penal	Denuncias
Art 173 inc. 16 CP: Estafa informática	115
Art. 131 CP: Grooming	92
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	85
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	5
Art. 255 CP: Alteración de evidencia informática	5
Art. 153 CP: Violación de correspondencia electrónica	3
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CPN: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**305**

Fuente: Tribunal Superior de Justicia del Poder Judicial de la Provincia de Córdoba

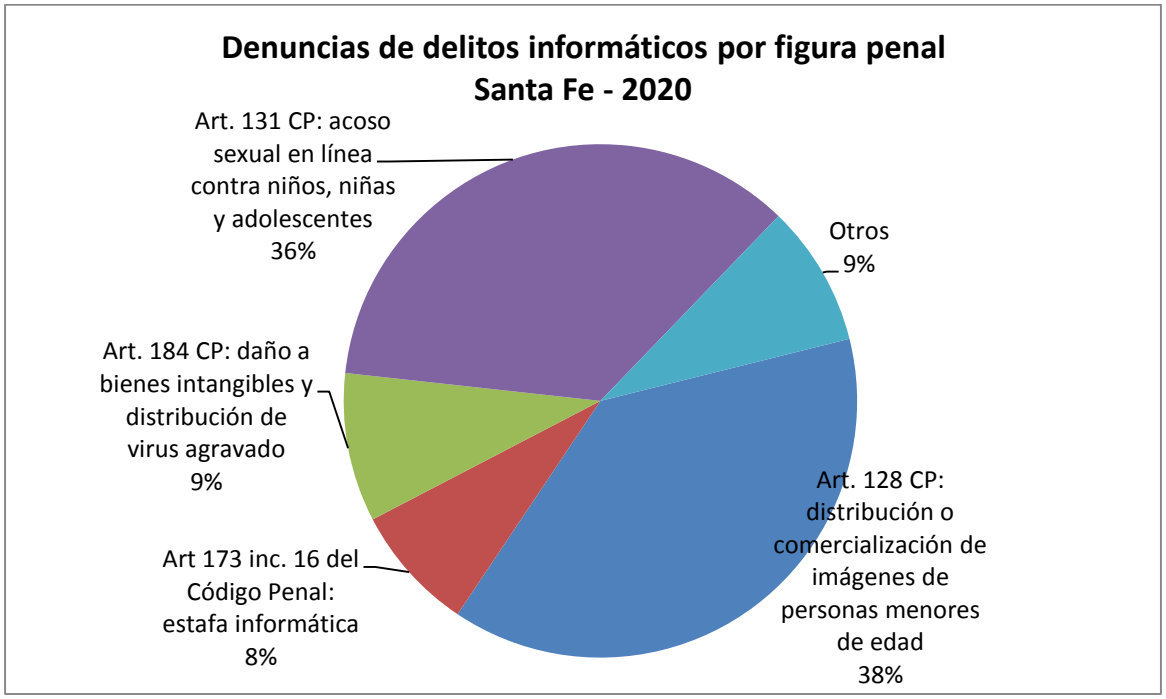


3.4. Santa Fe

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	245
Art. 131 CP: Grooming	227
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	60
Art 173 inc. 16 CP: Estafa informática	51
Art. 153 CP: Violación de correspondencia electrónica	18
Art. 183 CP: Daño a bienes intangibles y distribución de virus	15
Art. 157 CP: Revelación de secretos	7
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	5
Art. 255 CP: Alteración de evidencia informática	4
Art. 157 bis CPN: Delitos vinculados con la protección de datos personales	3
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	3
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	2
TOTAL	**640**

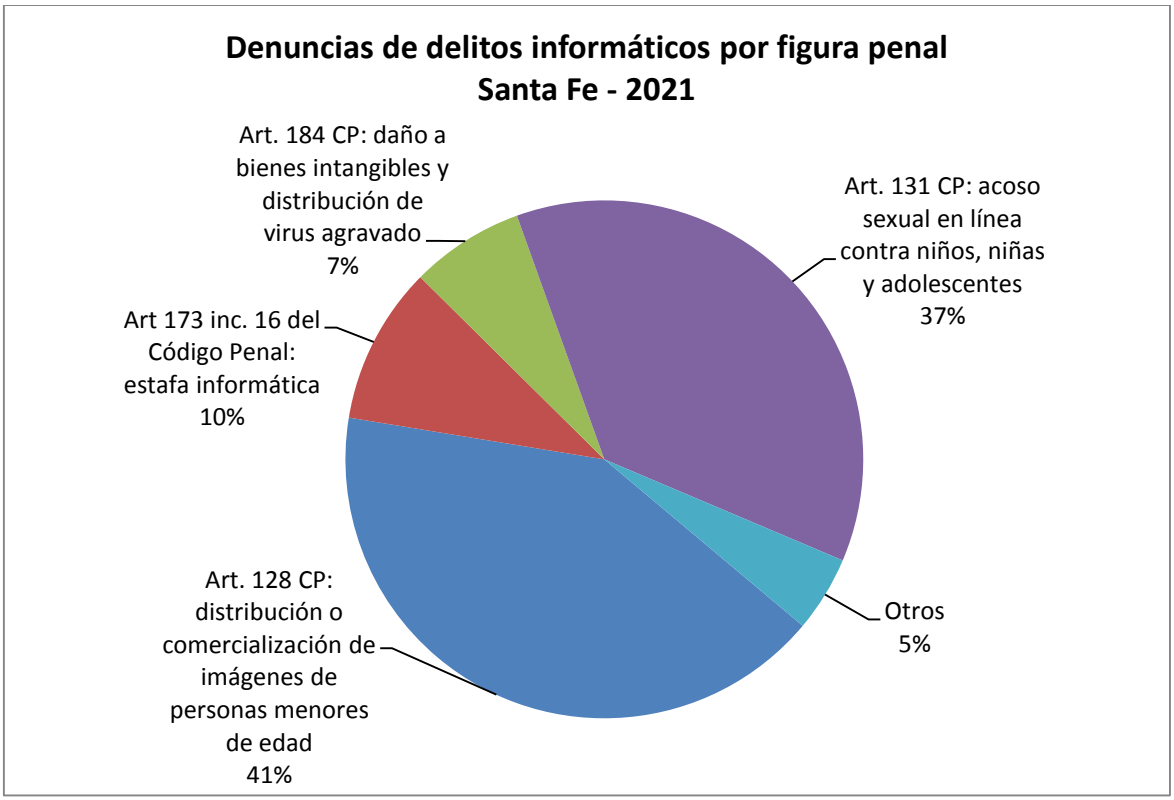
Fuente: Ministerio Público de la Acusación de la Provincia de Santa Fe



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	333
Art. 131 CP: Grooming	296
Art 173 inc. 16 CP: Estafa informática	79
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	57
Art. 153 CP: Violación de correspondencia electrónica	12
Art. 183 CP: Daño a bienes intangibles y distribución de virus	9
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	4
Art. 255 CP: Alteración de evidencia informática	4
Art. 157 CP: Revelación de secretos	3
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	2
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	2
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	2
TOTAL	**803**

Fuente: Ministerio Público de la Acusación de la Provincia de Santa Fe

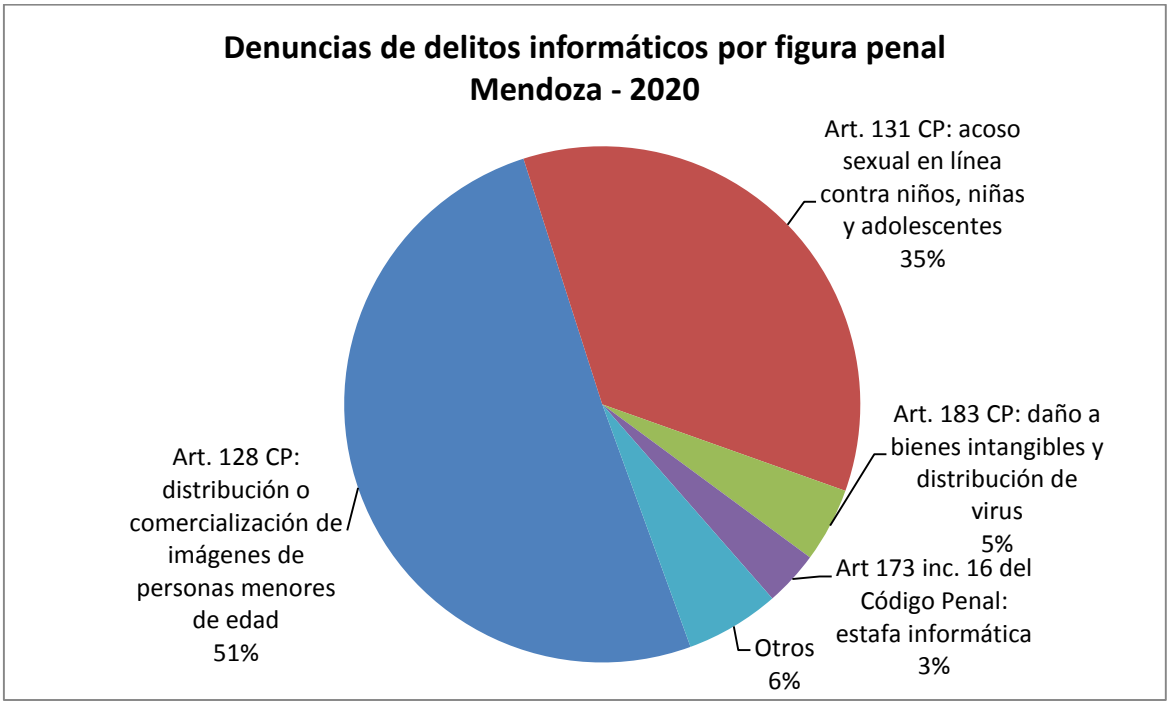


3.5. Mendoza

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	206
Art. 131 CP: Grooming	144
Art. 183 CP: Daño a bienes intangibles y distribución de virus	19
Art 173 inc. 16 CP: Estafa informática	14
Art. 255 CP: Alteración de evidencia informática	8
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	7
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	6
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	2
Art. 157 CP: Revelación de secretos	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
TOTAL	**407**

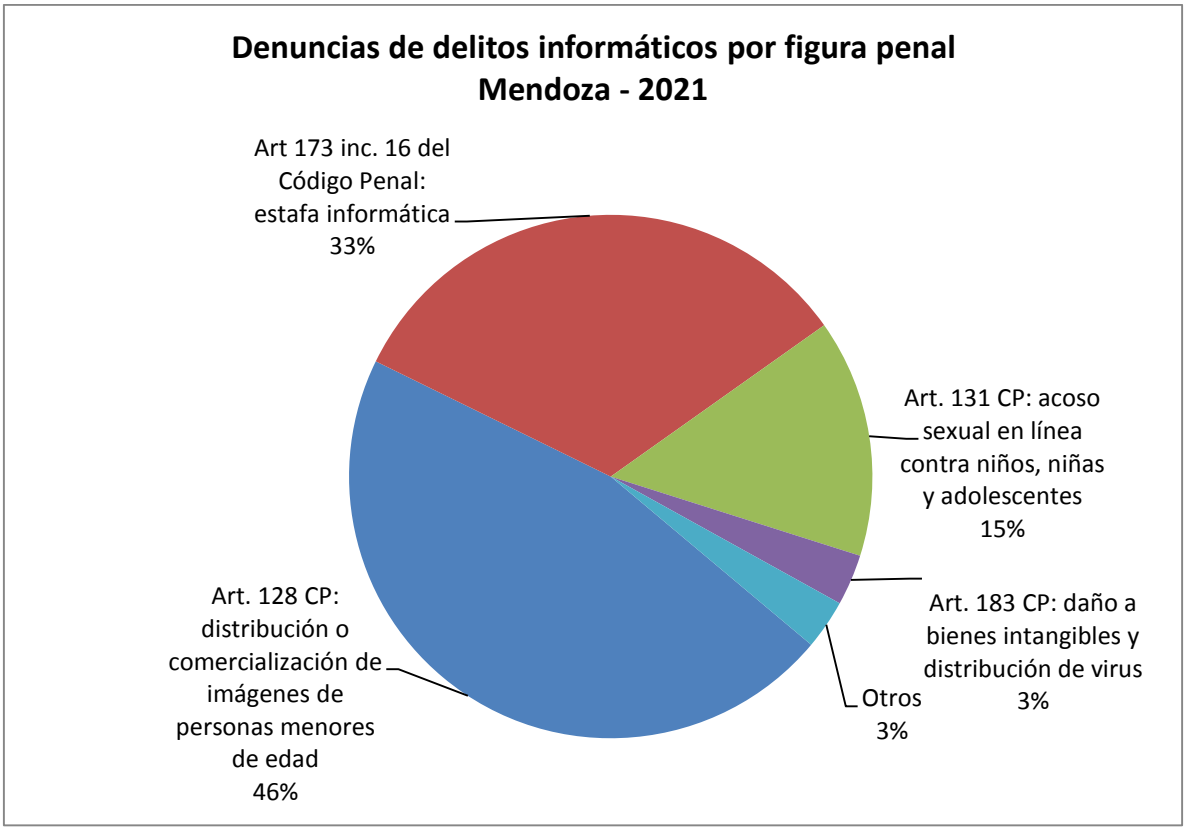
Fuente: Ministerio Público Fiscal de la Provincia de Mendoza



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	527
Art 173 inc. 16 CP: Estafa informática	376
Art. 131 CP: Grooming	168
Art. 183 CP: Daño a bienes intangibles y distribución de virus	36
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	10
Art. 157 CP: Revelación de secretos	9
Art. 255 CP: Alteración de evidencia informática	9
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	8
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
TOTAL	**1144**

Fuente: Ministerio Público Fiscal de la Provincia de Mendoza



3.6. Jujuy

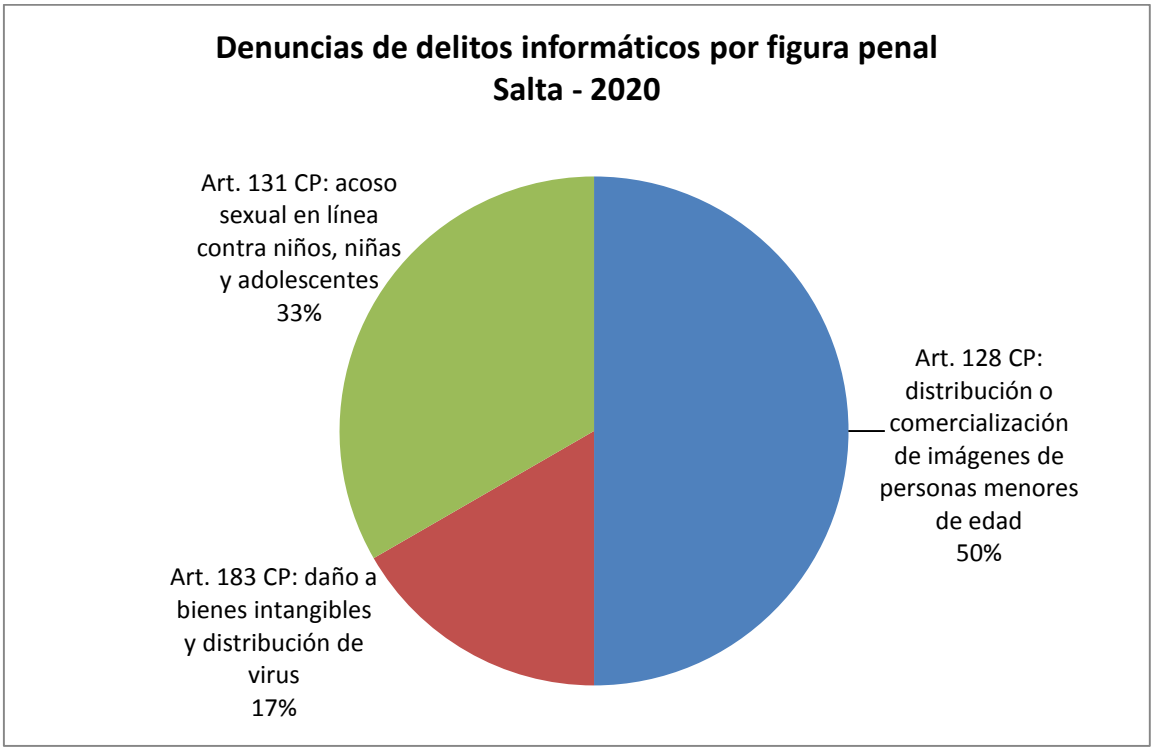
No informado

3.7. Salta

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	3
Art. 131 CP: Grooming	2
Art. 183 CP: Daño a bienes intangibles y distribución de virus	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: alteración de evidencia informática	-
TOTAL	**6**

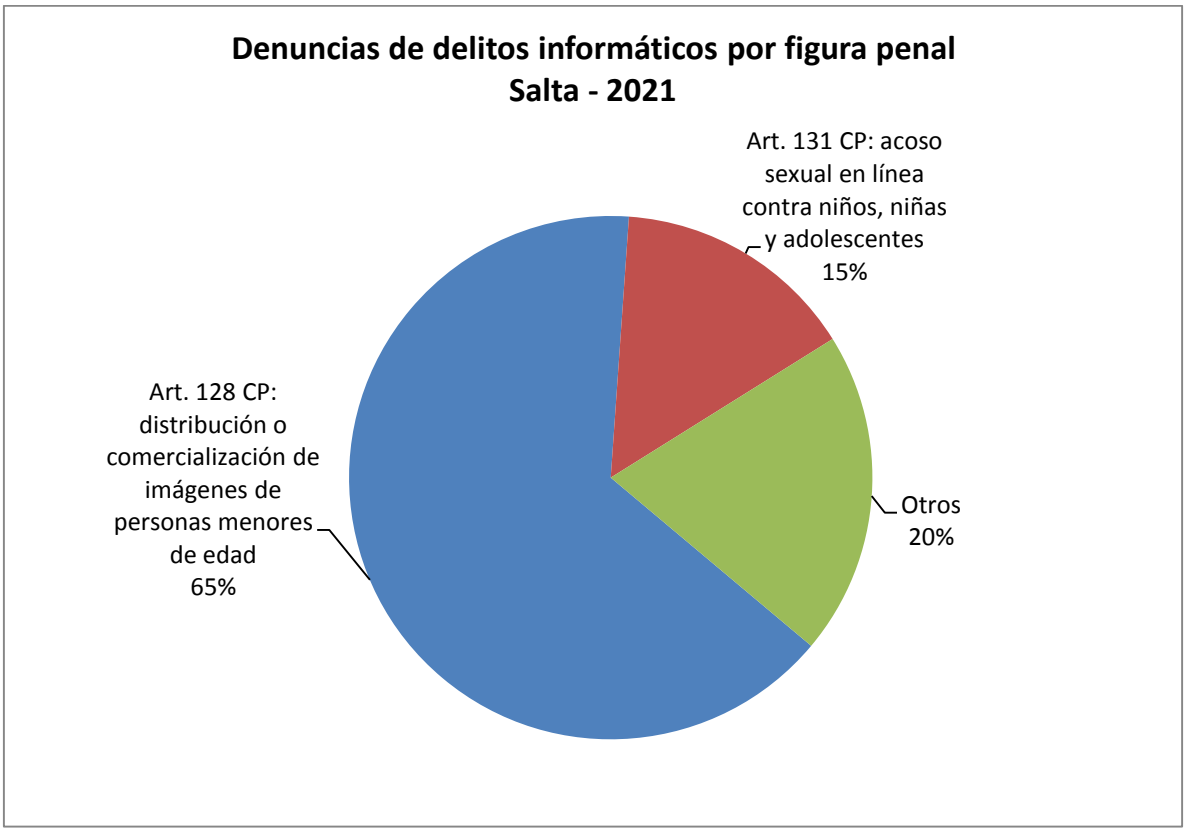
Fuente: Poder Judicial de la Provincia de la Provincia de Salta.



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	13
Art. 131 CP: Grooming	3
Art. 153 CP: Violación de correspondencia electrónica	1
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	1
Art 173 inc. 16 CP: Estafa informática	1
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	1
Art. 155 CP: Publicación indebida de comunicaciones electrónicas	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**20**

Fuente: Poder Judicial de la Provincia de la Provincia de Salta.

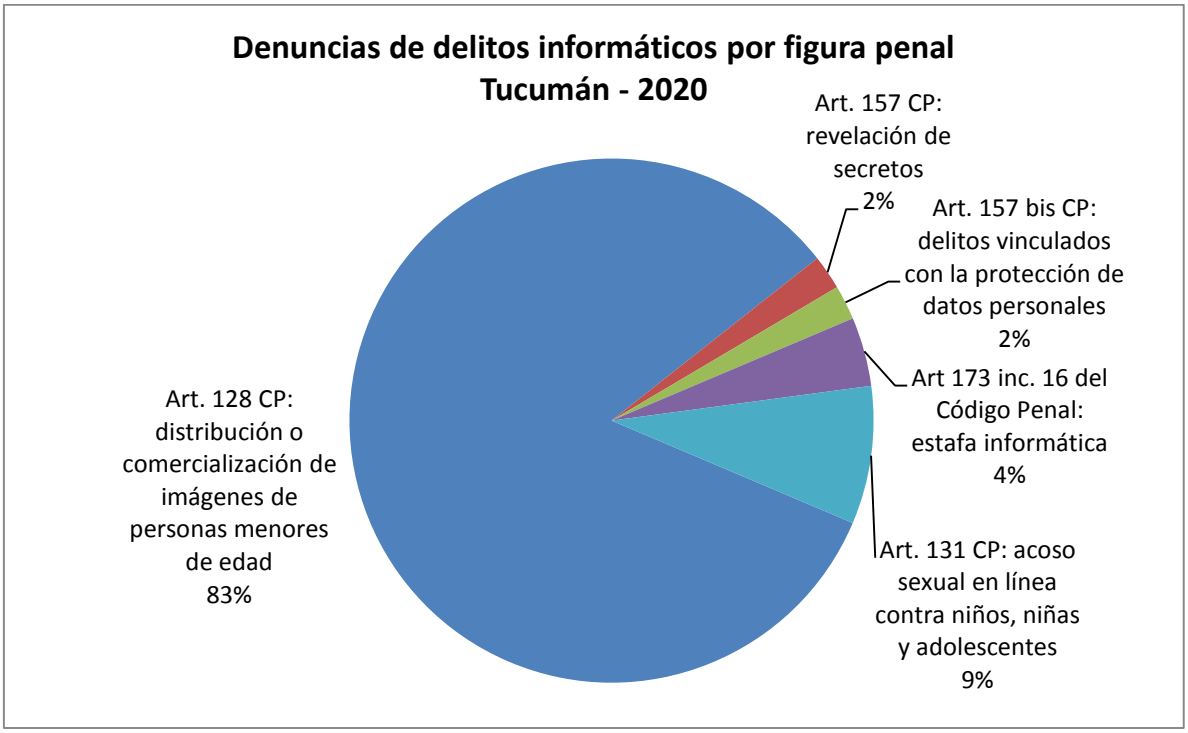


3.8. Tucumán

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	39
Art. 131 CP: Grooming	4
Art 173 inc. 16 del Código Penal: estafa informática	2
Art. 157 CP: Revelación de secretos	1
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**47**

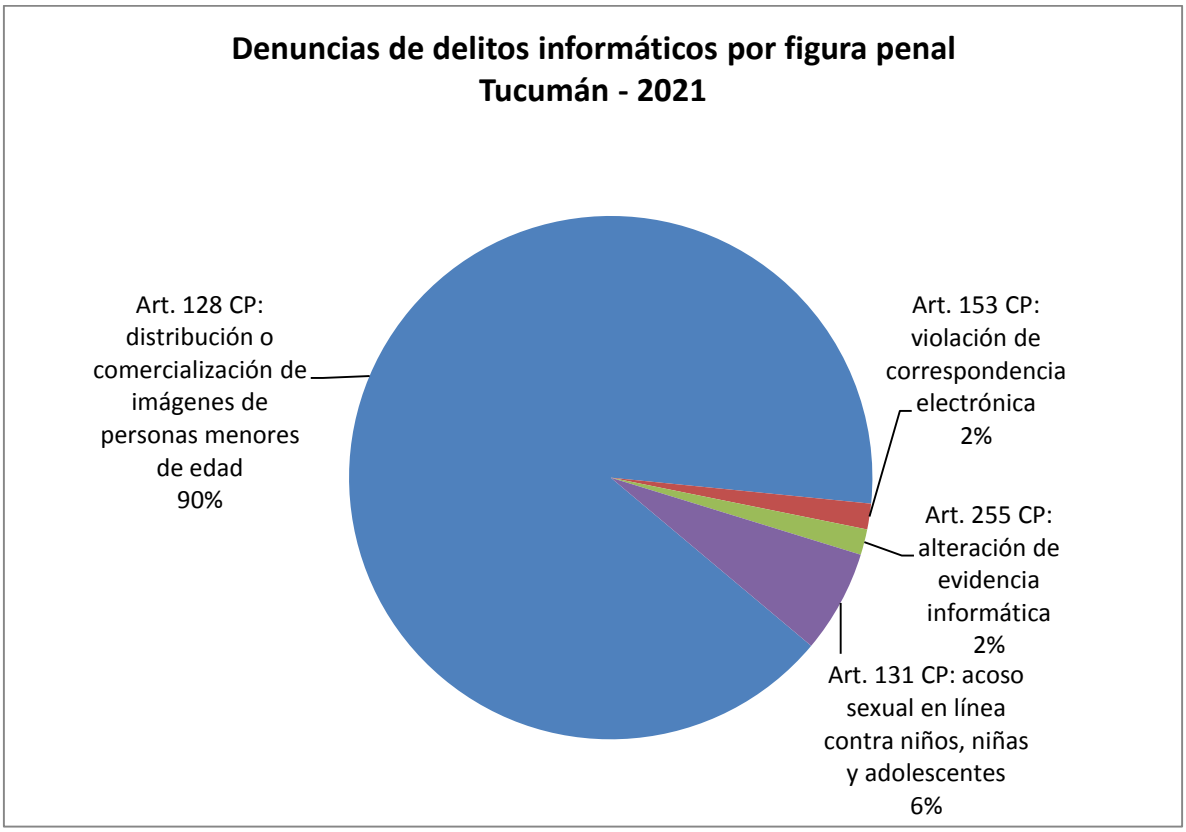
Fuente: Corte Suprema de Justicia de la Provincia de la Provincia de Tucumán



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	57
Art. 131 CP: Grooming	4
Art. 153 CP: violación de correspondencia electrónica	1
Art. 255 CP: Alteración de evidencia informática	1
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**63**

Fuente: Corte Suprema de Justicia de la Provincia de la Provincia de Tucumán

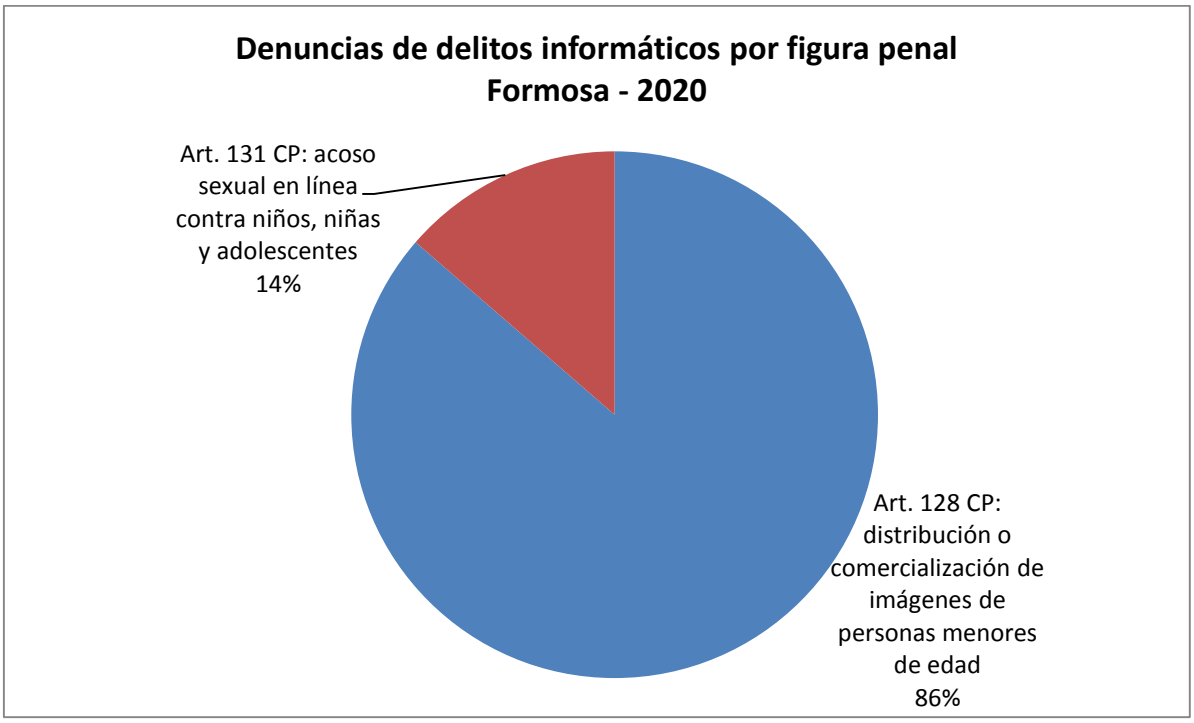


3.9. Formosa

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	38
Art. 131 CP: Grooming	6
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: alteración de evidencia informática	-
TOTAL	**44**

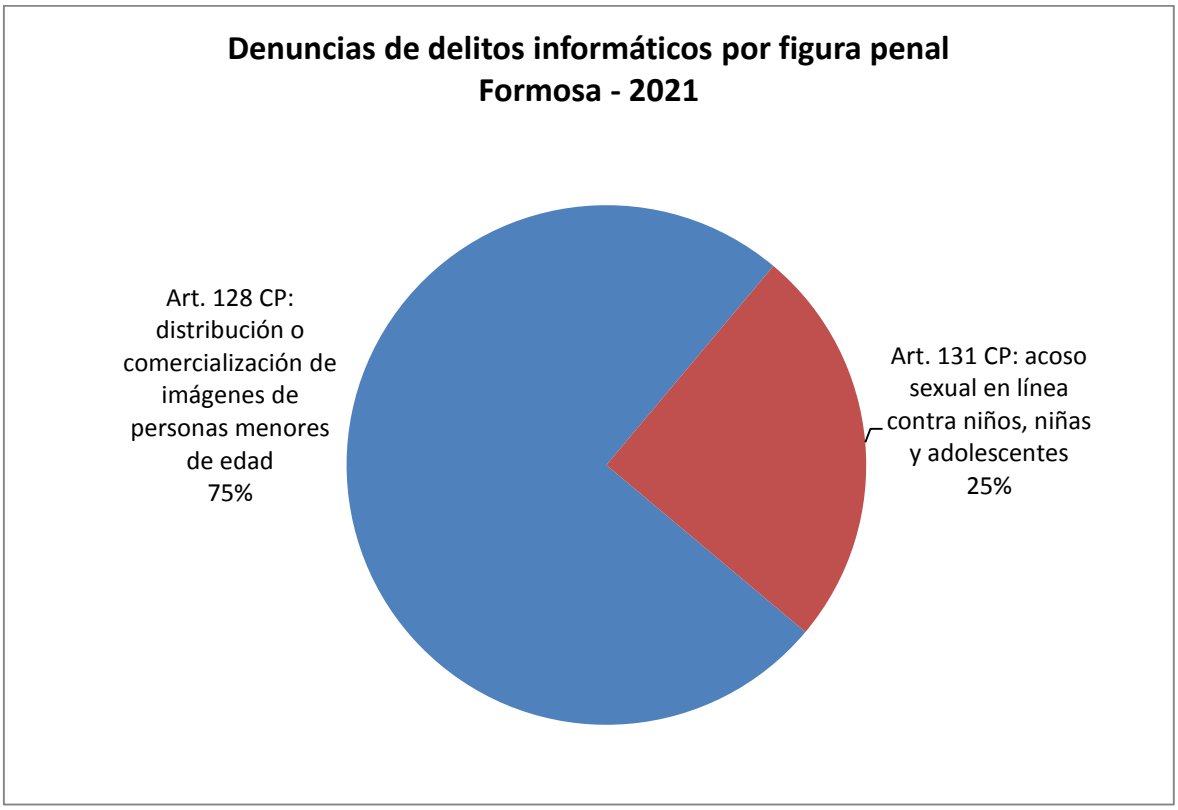
Fuente: Poder Judicial de la Provincia de Formosa



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	27
Art. 131 CP: Grooming	9
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**36**

Fuente: Poder Judicial de la Provincia de Formosa



3.10. Chaco

No informado

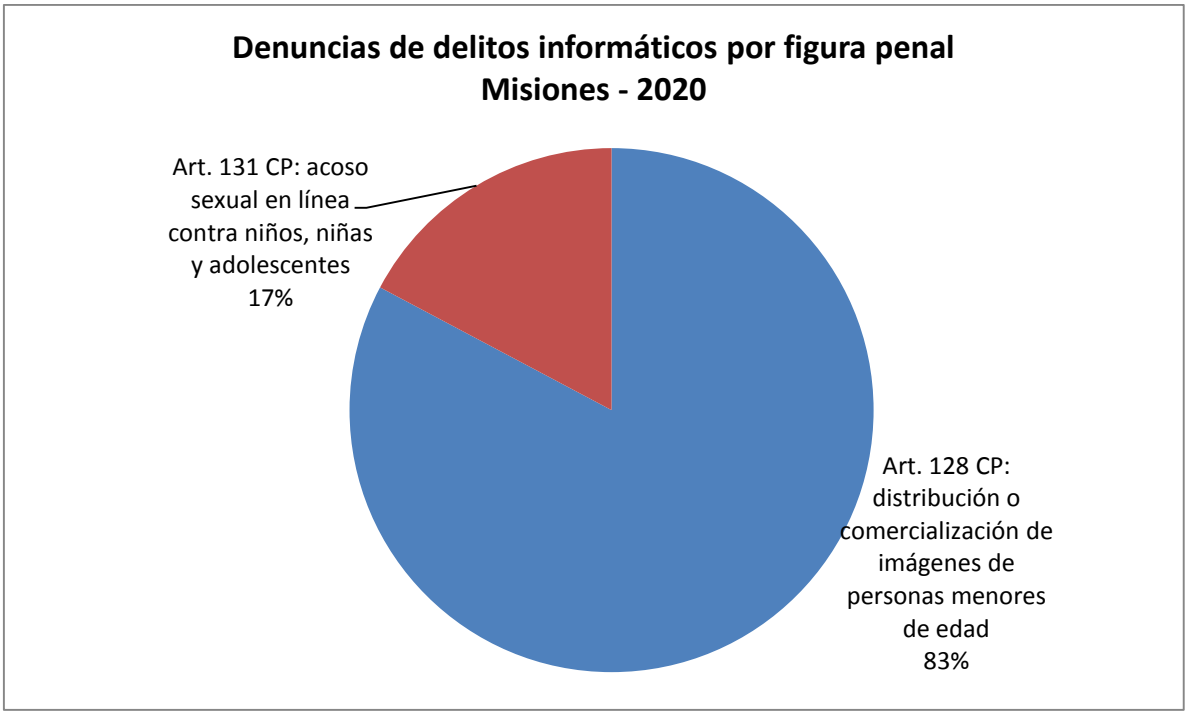
3.11. Misiones

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	48
Art. 131 CP: Grooming	10
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-

TOTAL	**58**

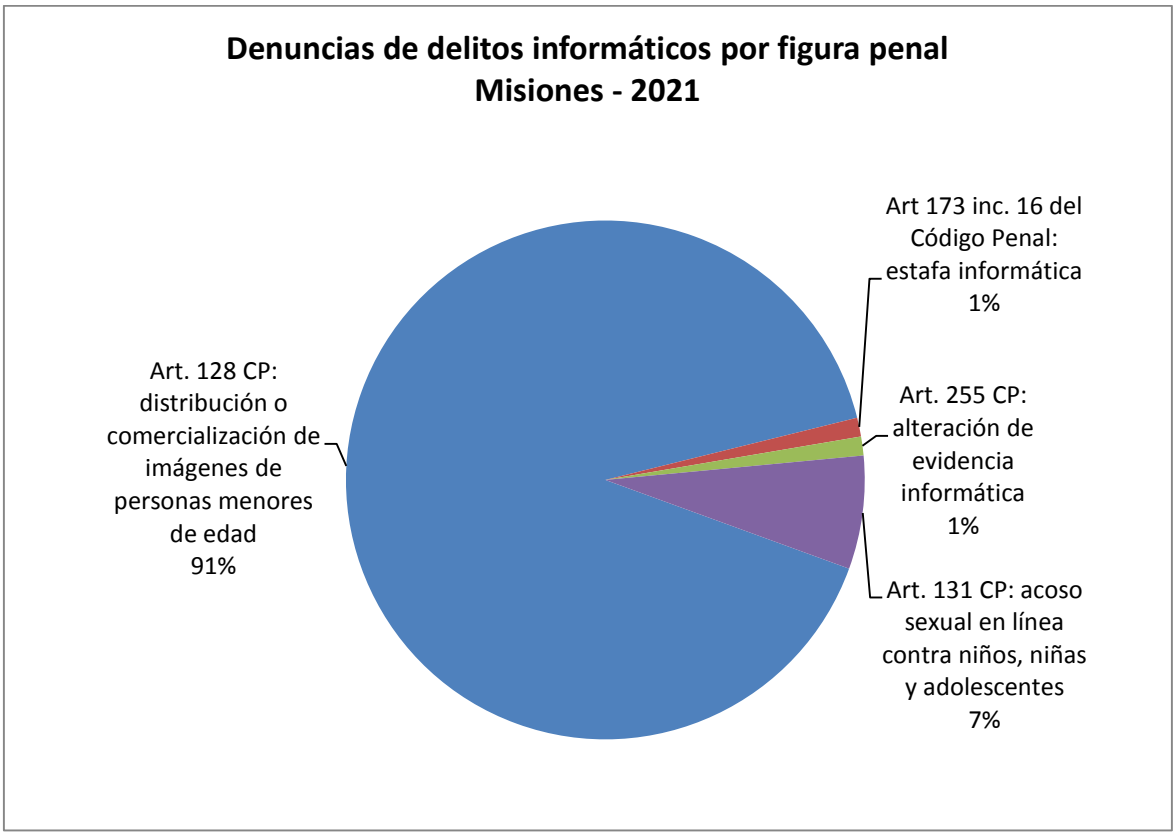
Fuente: Poder Judicial de la Provincia de la Provincia de Misiones



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	77
Art. 131 CP: Grooming	6
Art 173 inc. 16 del CP: estafa informática	1
Art. 255 CP: Alteración de evidencia informática	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**85**

Fuente: Poder Judicial de la Provincia de la Provincia de Misiones

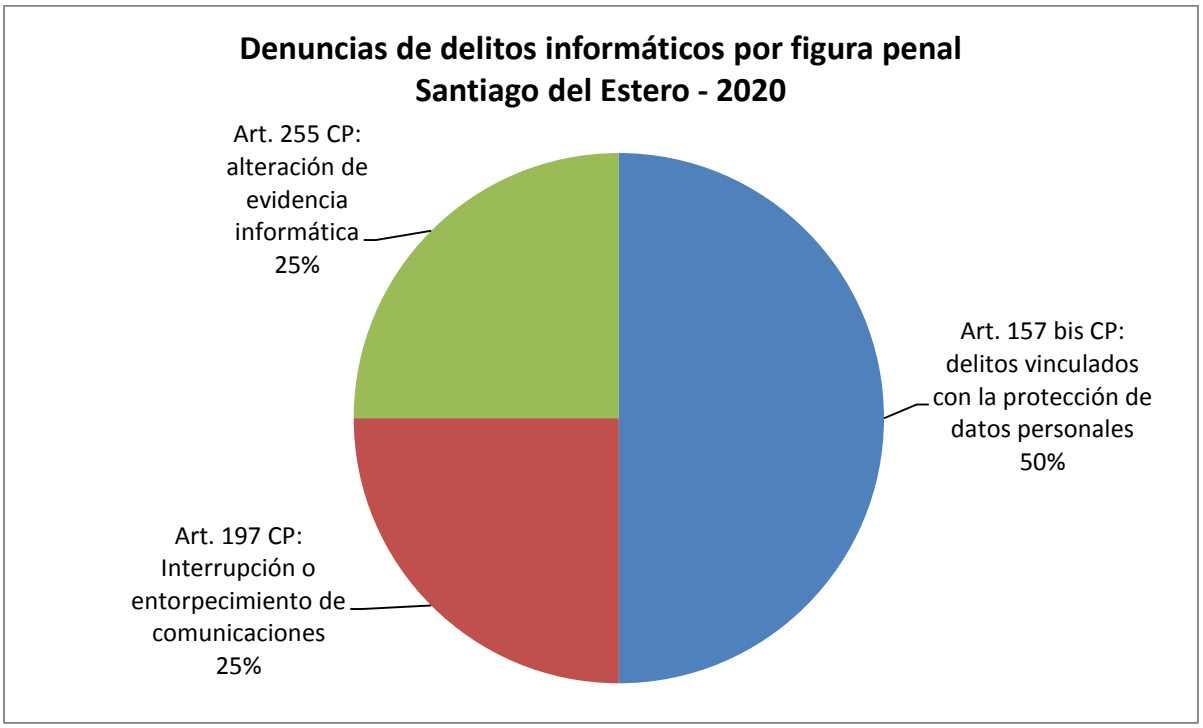


3.12. Santiago del Estero

Año 2020:

Figura penal	Denuncias
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	2
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	1
Art. 255 CP: Alteración de evidencia informática	1
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	-
Art. 131 CP: Grooming	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**4**

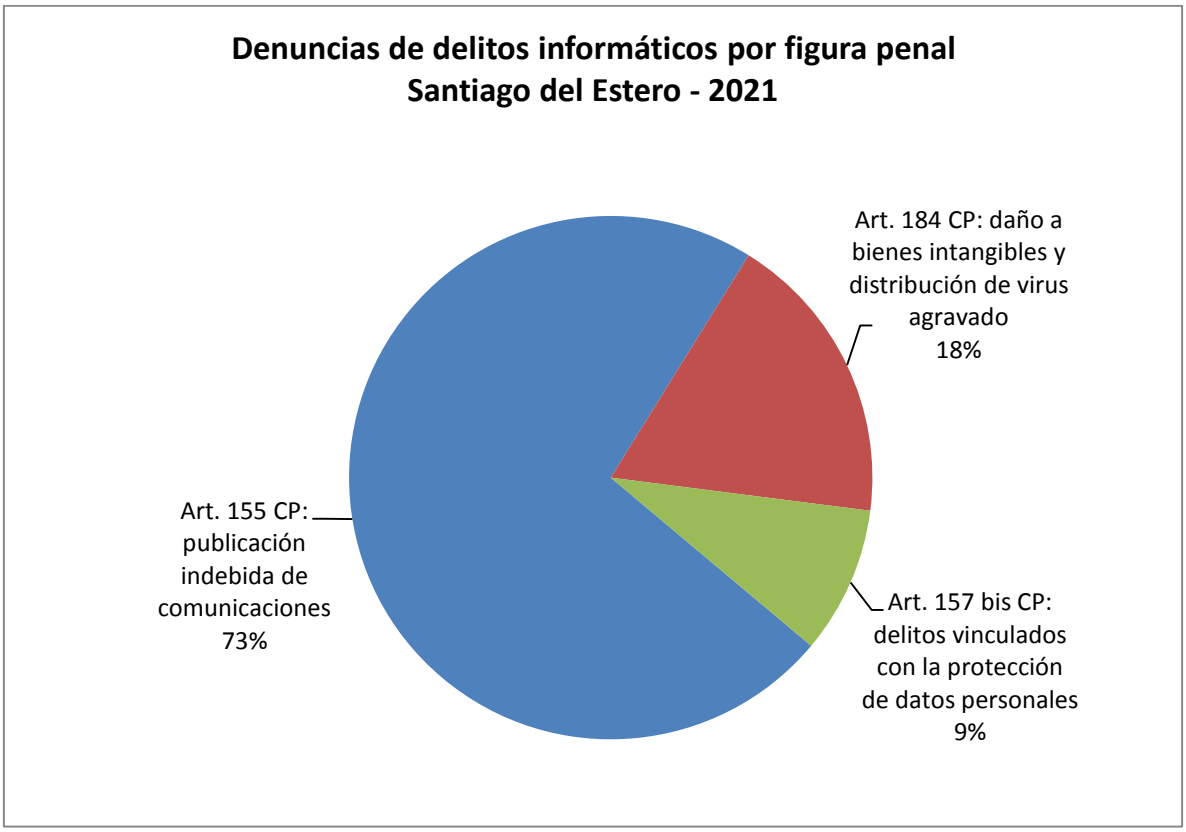
Fuente: Poder Judicial de la Provincia de Santiago del Estero



Año 2021:

Figura penal	Denuncias
Art. 155 CP: Publicación indebida de comunicaciones	8
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	2
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	1
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	-
Art. 131 CP: Grooming	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 255 CP: Alteración de evidencia informática	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 157 CP: Revelación de secretos	-
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
TOTAL	**11**

Fuente: Poder Judicial de la Provincia de la Provincia de Santiago del Estero

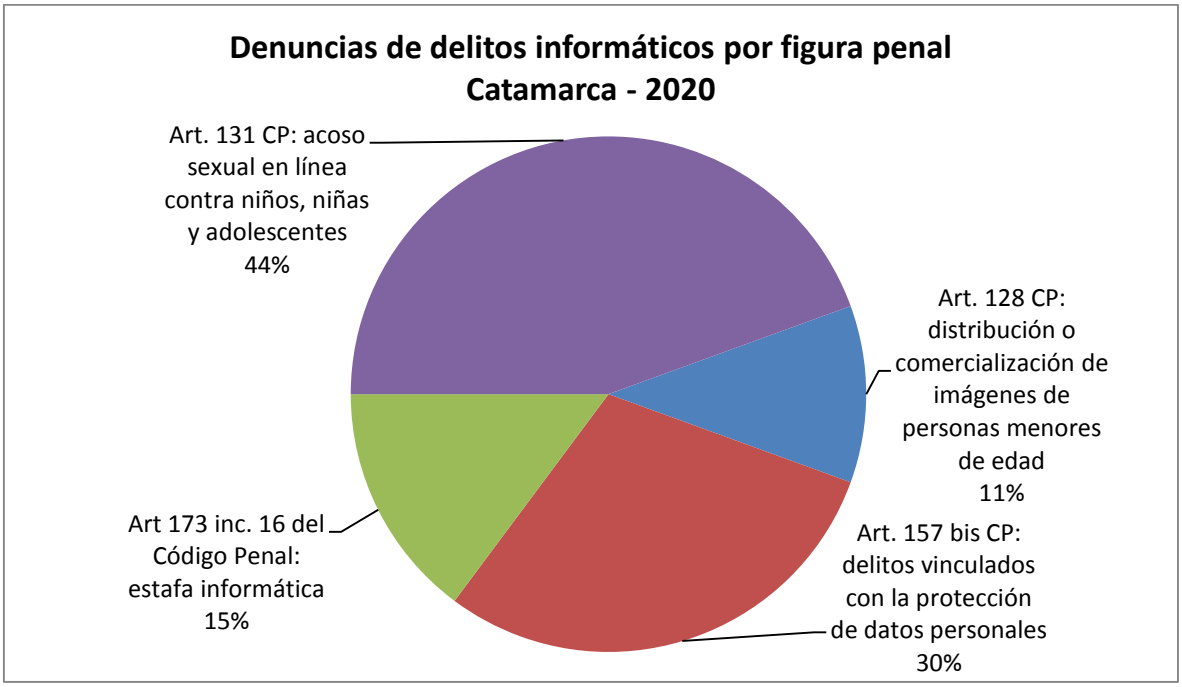


3.13. Catamarca

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	12
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	8
Art 173 inc. 16 del CP: Estafa informática	4
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	3
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**27**

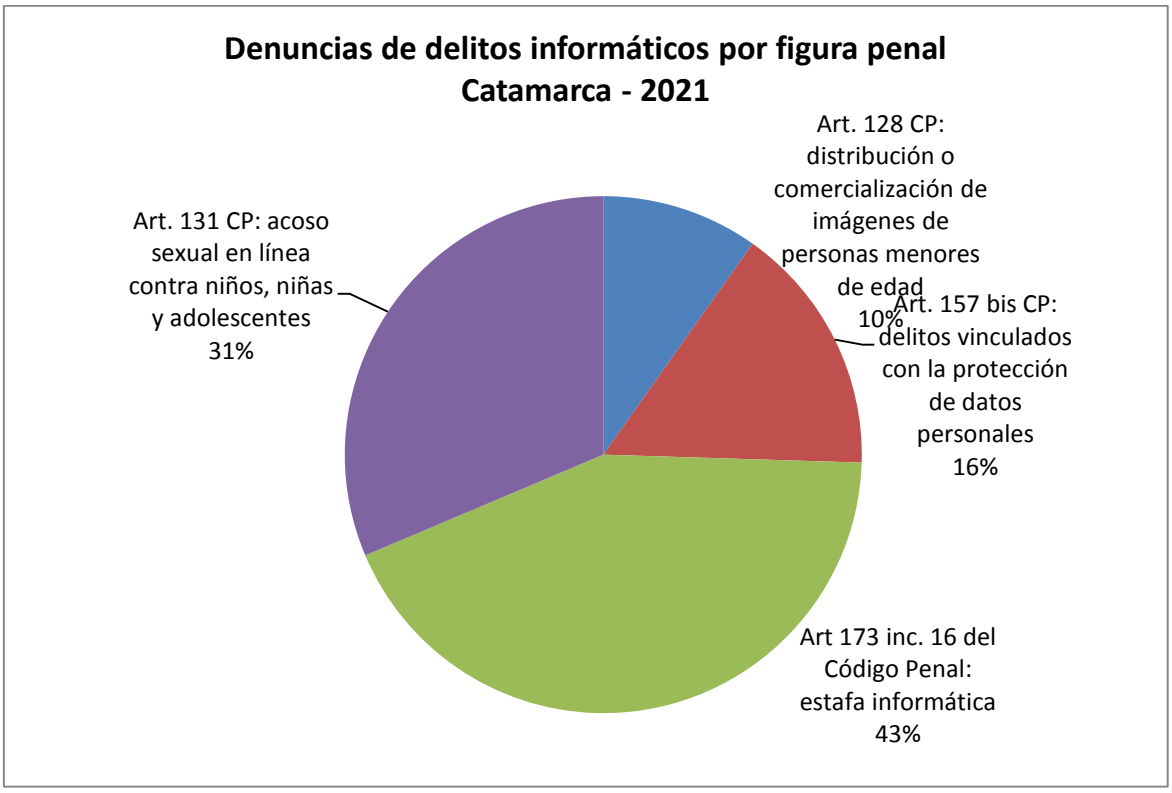
Fuente: Ministerio Público del Poder Judicial de la Provincia de Catamarca



Año 2021:

Figura penal	Denuncias
Art 173 inc. 16 del CP: Estafa informática	22
Art. 131 CP: Grooming	16
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	8
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	5
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**51**

Fuente: Ministerio Público del Poder Judicial de la Provincia de Catamarca

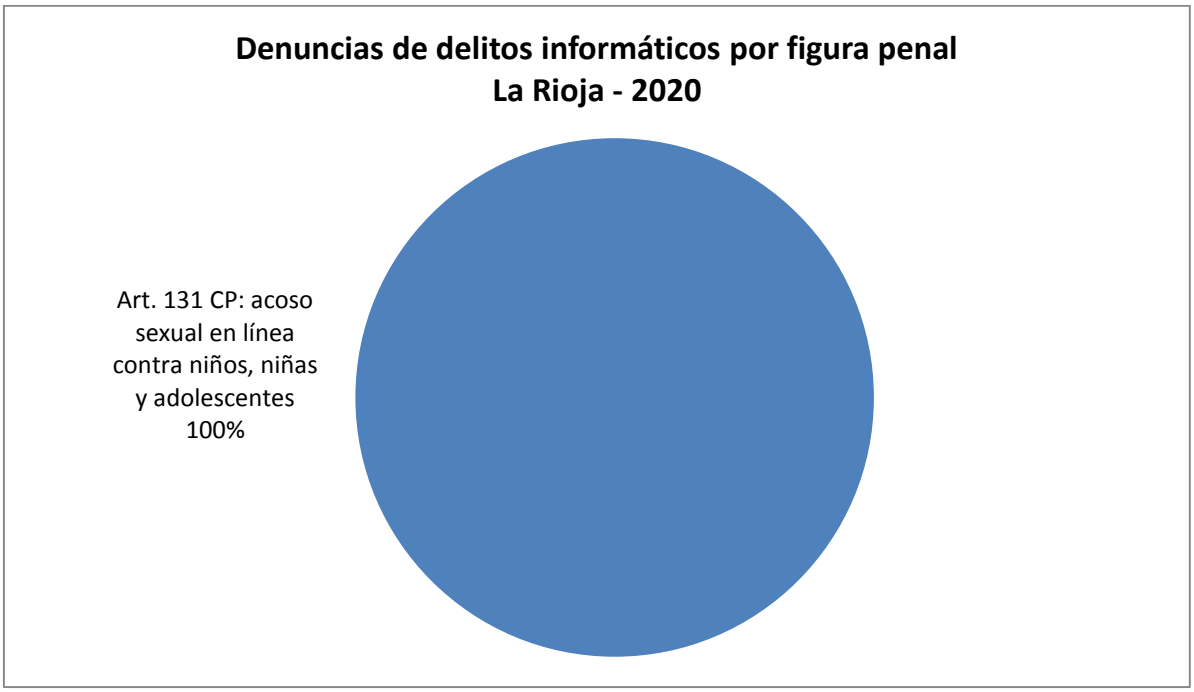


3.14. La Rioja

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	5
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**5**

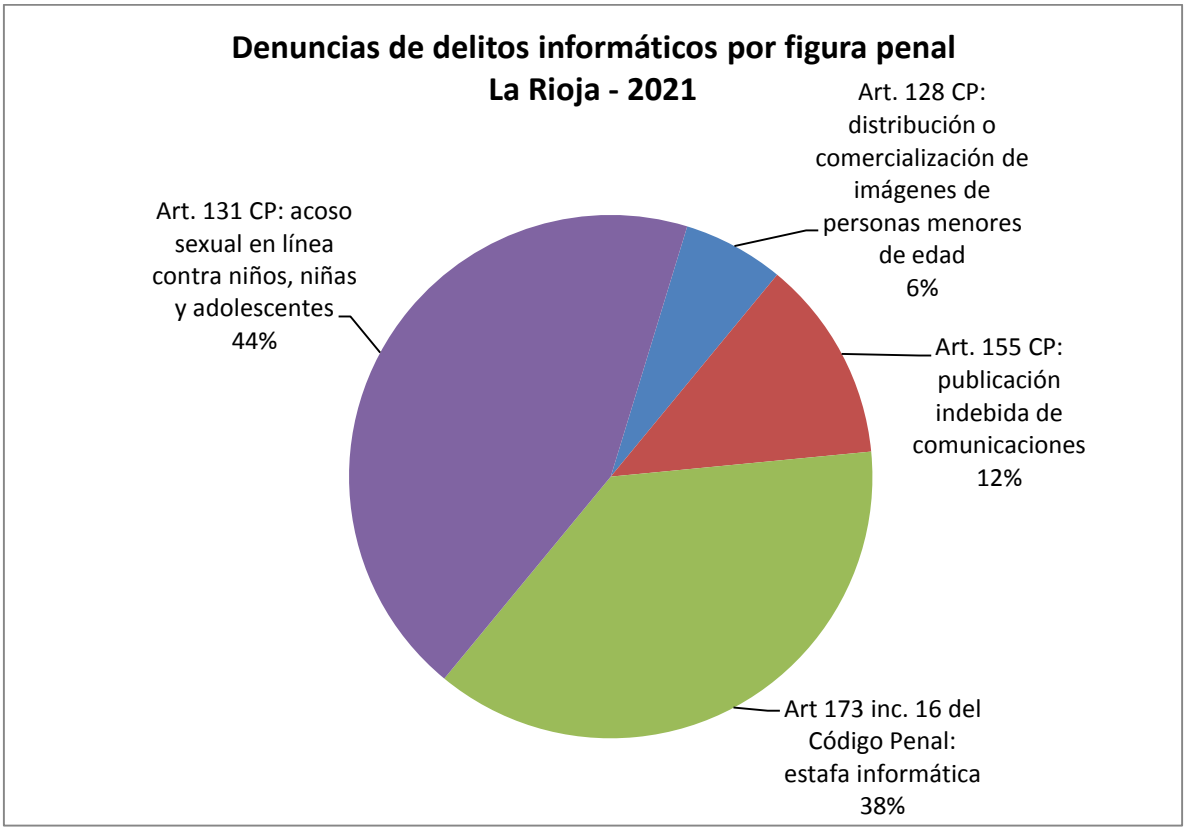
Fuente: Poder Judicial de la Provincia de la Provincia de La Rioja



Año 2021:

Figura penal	Denuncias
Art. 131 CP: Grooming	7
Art 173 inc. 16 del CP: Estafa informática	6
Art. 155 CP: Publicación indebida de comunicaciones	2
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**16**

Fuente: Poder Judicial de la Provincia de La Rioja



3.15. San Juan

No informado

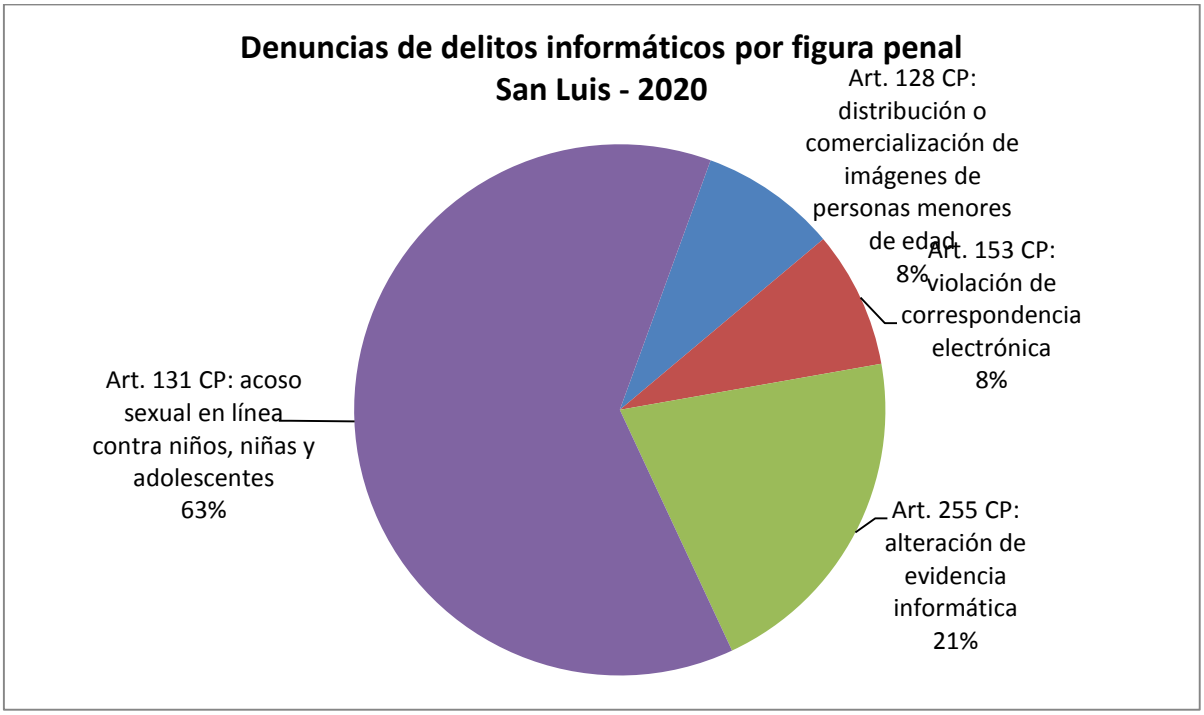
3.16. San Luis

<u>Año 2020:</u>

Figura penal	Denuncias
Art. 131 CP: Grooming	15
Art. 255 CP: Alteración de evidencia informática	5
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	2
Art. 153 CP: Violación de correspondencia electrónica	2
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-

Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**24**

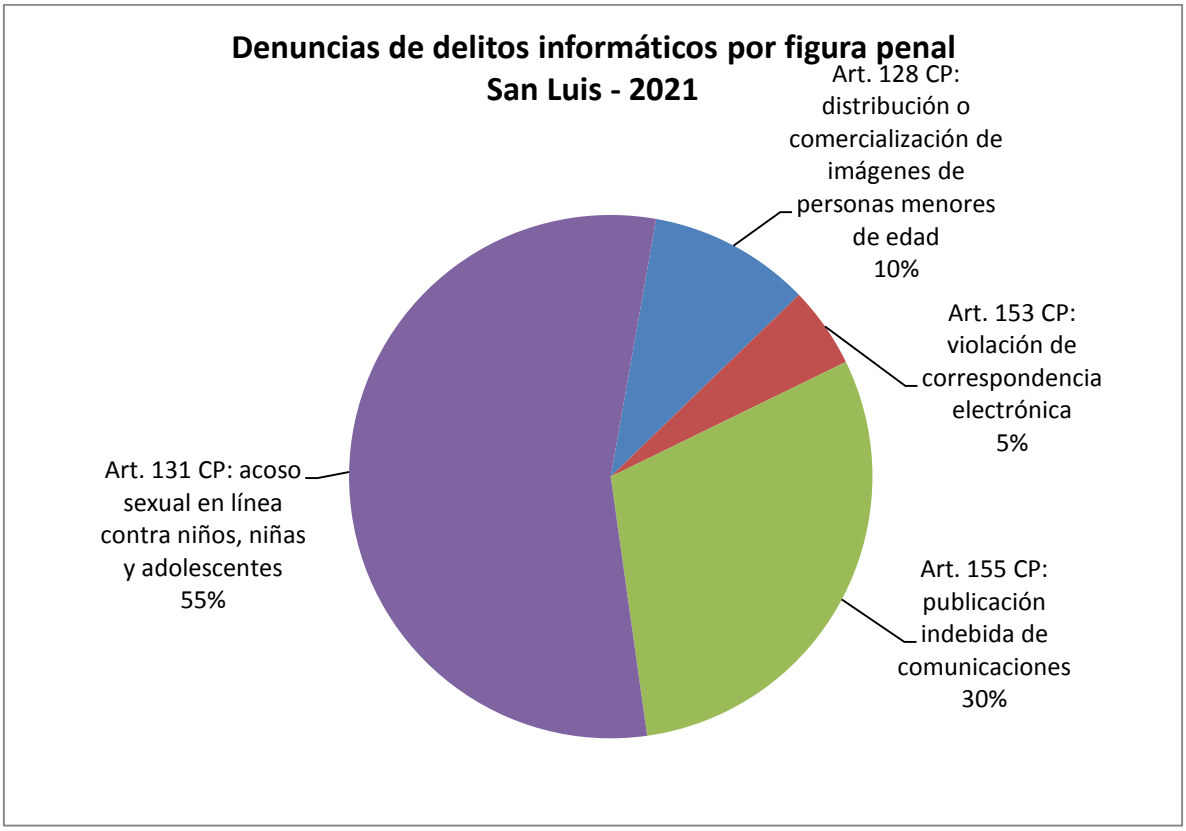
Fuente: Poder Judicial de la Provincia de San Luis



Año 2021:

Figura penal	Denuncias
Art. 131 CP: Grooming	11
Art. 155 CP: Publicación indebida de comunicaciones	6
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	2
Art. 153 CP: Violación de correspondencia electrónica	1
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
Art. 157 CP: Revelación de secretos	-
TOTAL	**20**

Fuente: Poder Judicial de la Provincia de San Luis

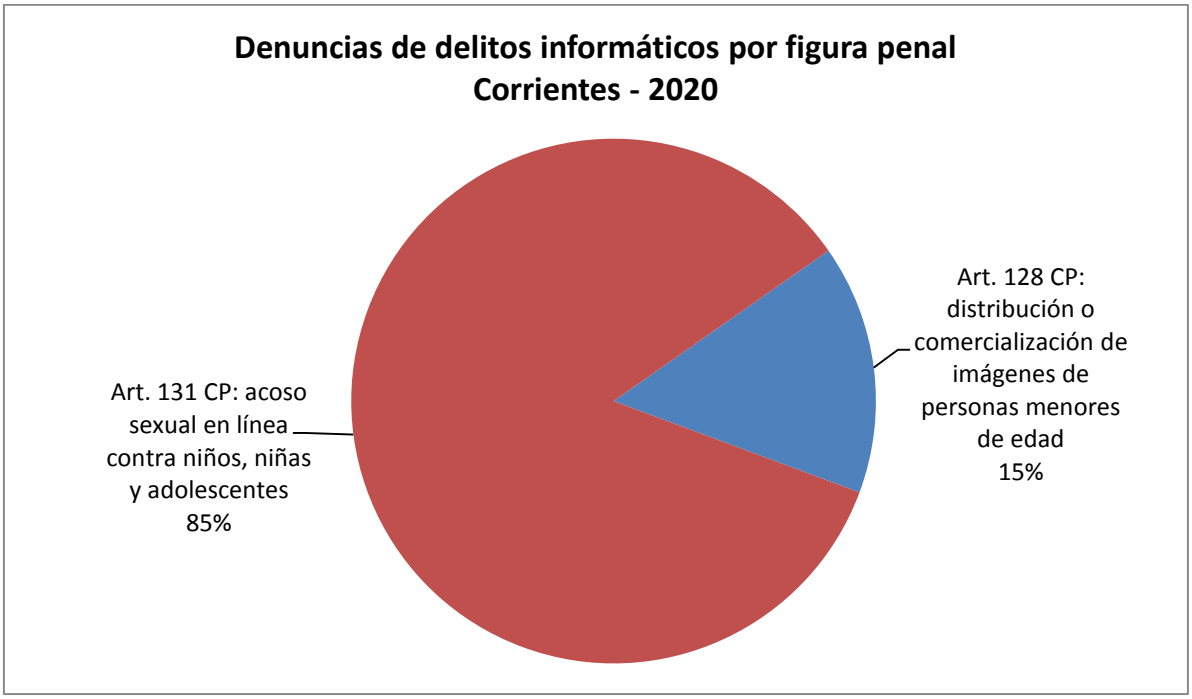


3.17. Corrientes

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	11
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	2
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**13**

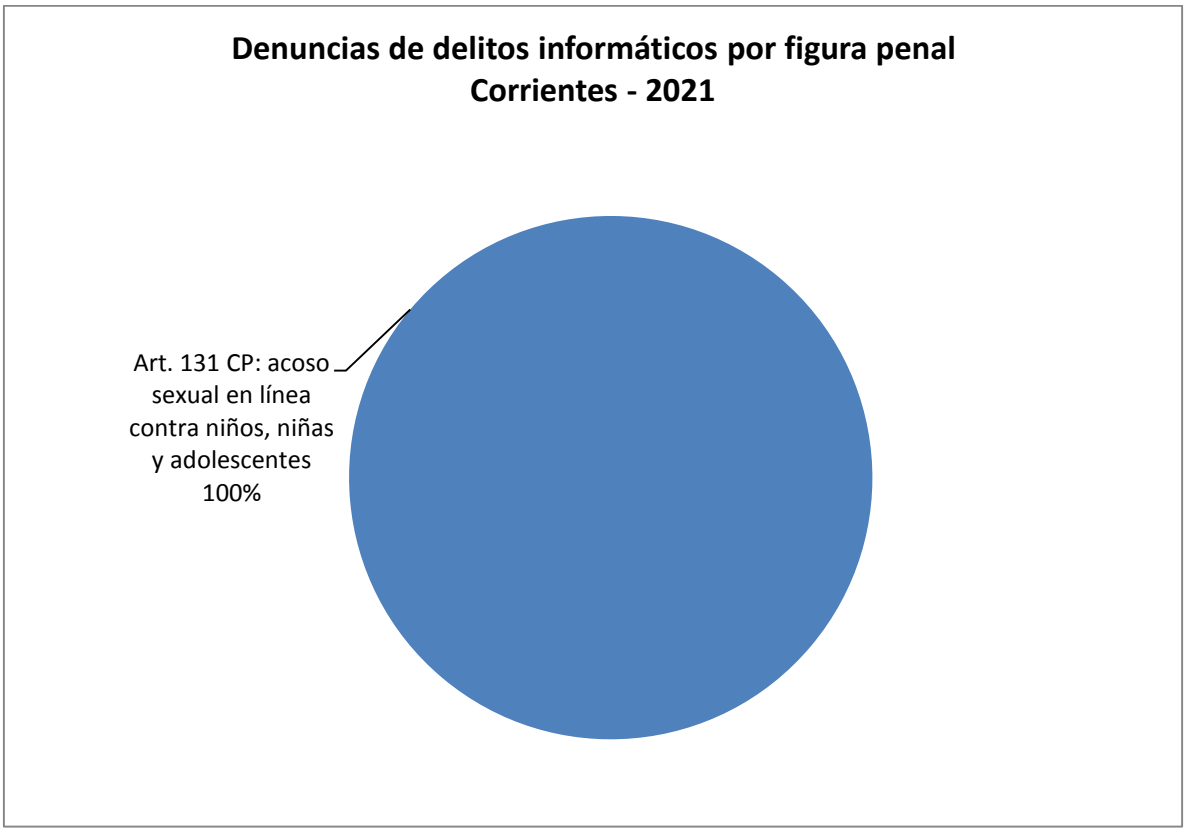
Fuente: Poder Judicial de la Provincia de Corrientes



Año 2021:

Figura penal	Denuncias
Art. 131 CP: Grooming	13
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**13**

Fuente: Poder Judicial de la Provincia de Corrientes

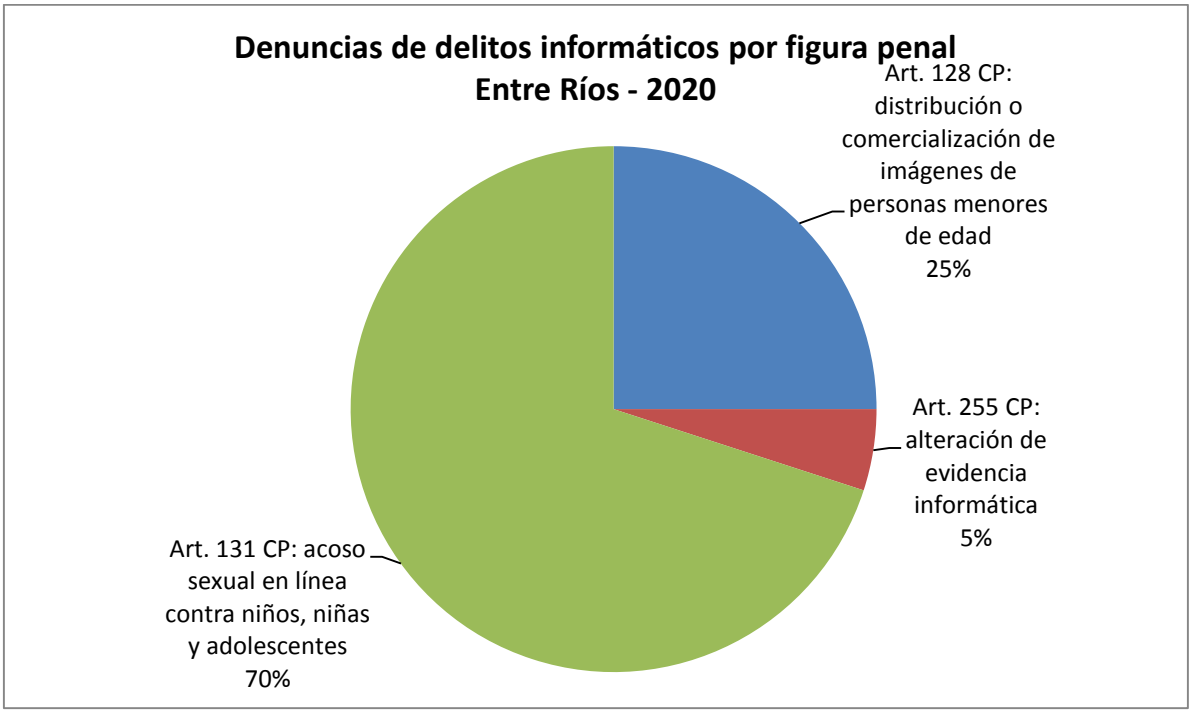


3.18. Entre Ríos

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	14
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	5
Art. 255 CP: Alteración de evidencia informática	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**20**

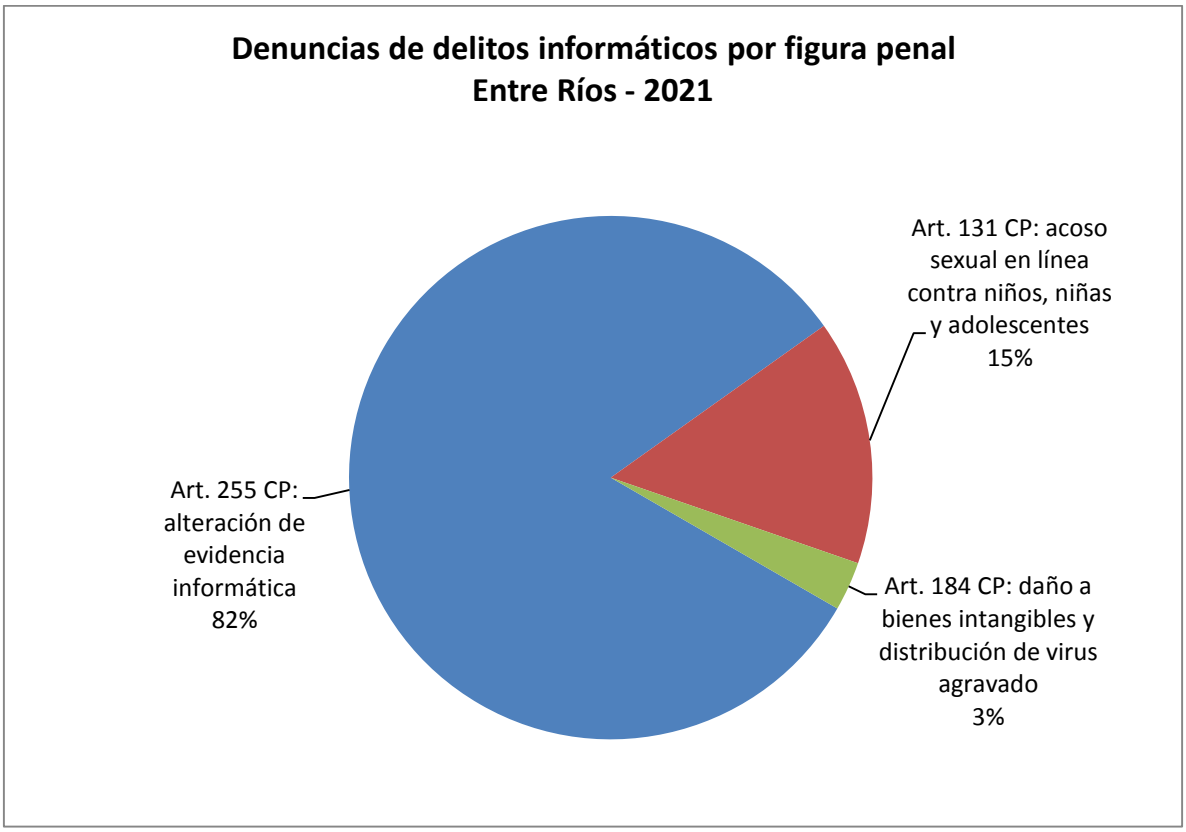
Fuente: Superior Tribunal de Justicia de la Provincia de Entre Ríos



Año 2021:

Figura penal	Denuncias
Art. 255 CP: Alteración de evidencia informática	27
Art. 131 CP: Grooming	5
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	1
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
TOTAL	**33**

Fuente: Superior Tribunal de Justicia de la Provincia de Entre Ríos

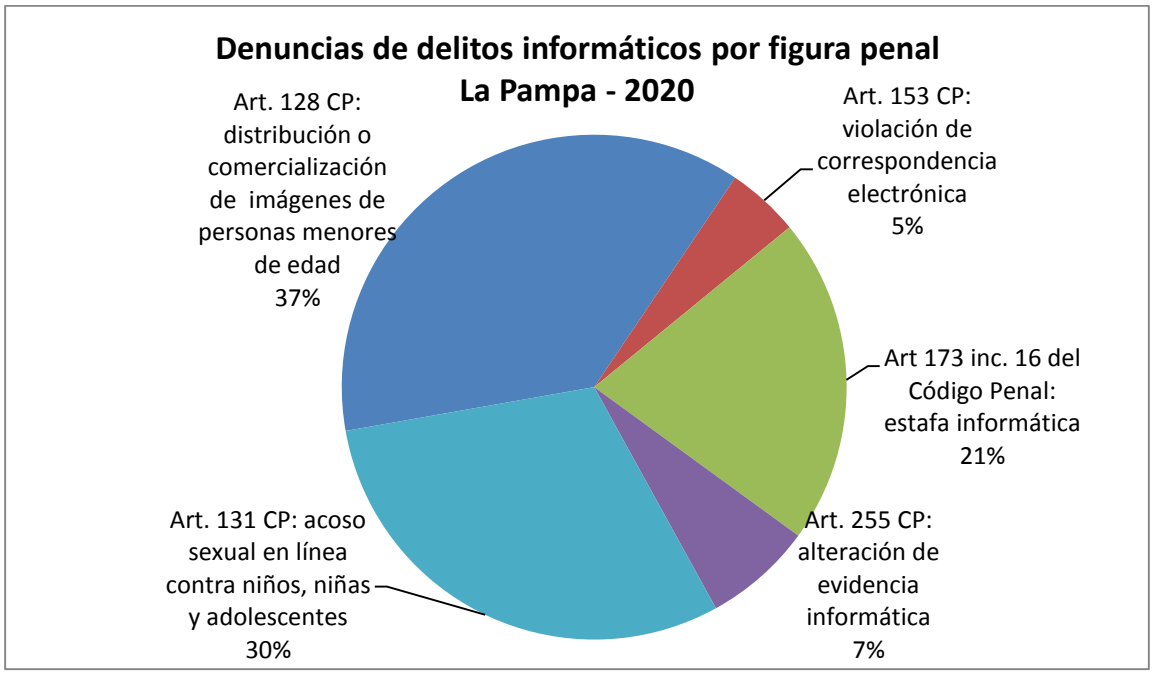


3.19. La Pampa

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	16
Art. 131 CP: Grooming	13
Art 173 inc. 16 del CP: estafa informática	9
Art. 255 CP: Alteración de evidencia informática	3
Art. 153 CP: Violación de correspondencia electrónica	2
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**43**

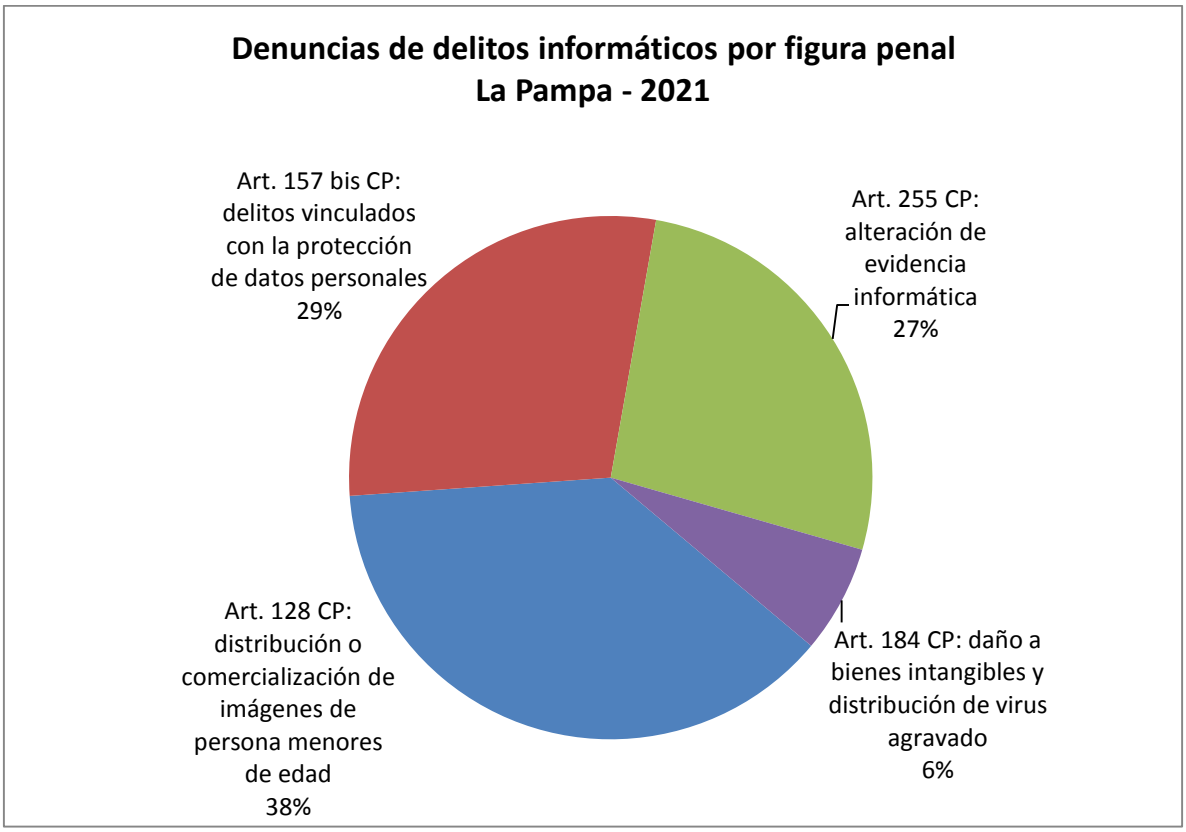
Fuente: Poder Judicial de la Provincia de La Pampa



Año 2021:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	17
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	13
Art. 255 CP: Alteración de evidencia informática	12
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	3
Art. 131 CP: Grooming	-
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art 173 inc. 16 del CP: Estafa informática	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
TOTAL	**45**

Fuente: Poder Judicial de la Provincia de La Pampa

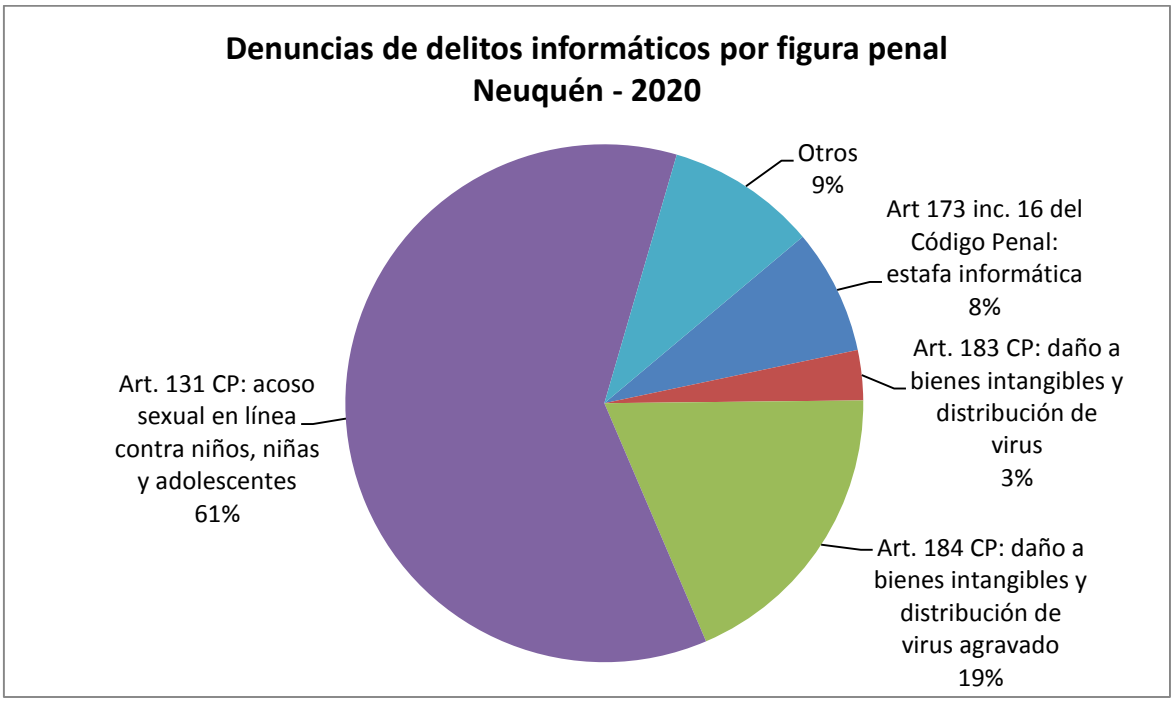


3.20. Neuquén

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	39
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	12
Art 173 inc. 16 del CP: Estafa informática	5
Art. 155 CP: Publicación indebida de comunicaciones	2
Art. 183 CP: Daño a bienes intangibles y distribución de virus	2
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	1
Art. 153 CP: Violación de correspondencia electrónica	1
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	1
Art. 157 CP: Revelación de secretos	1
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**64**

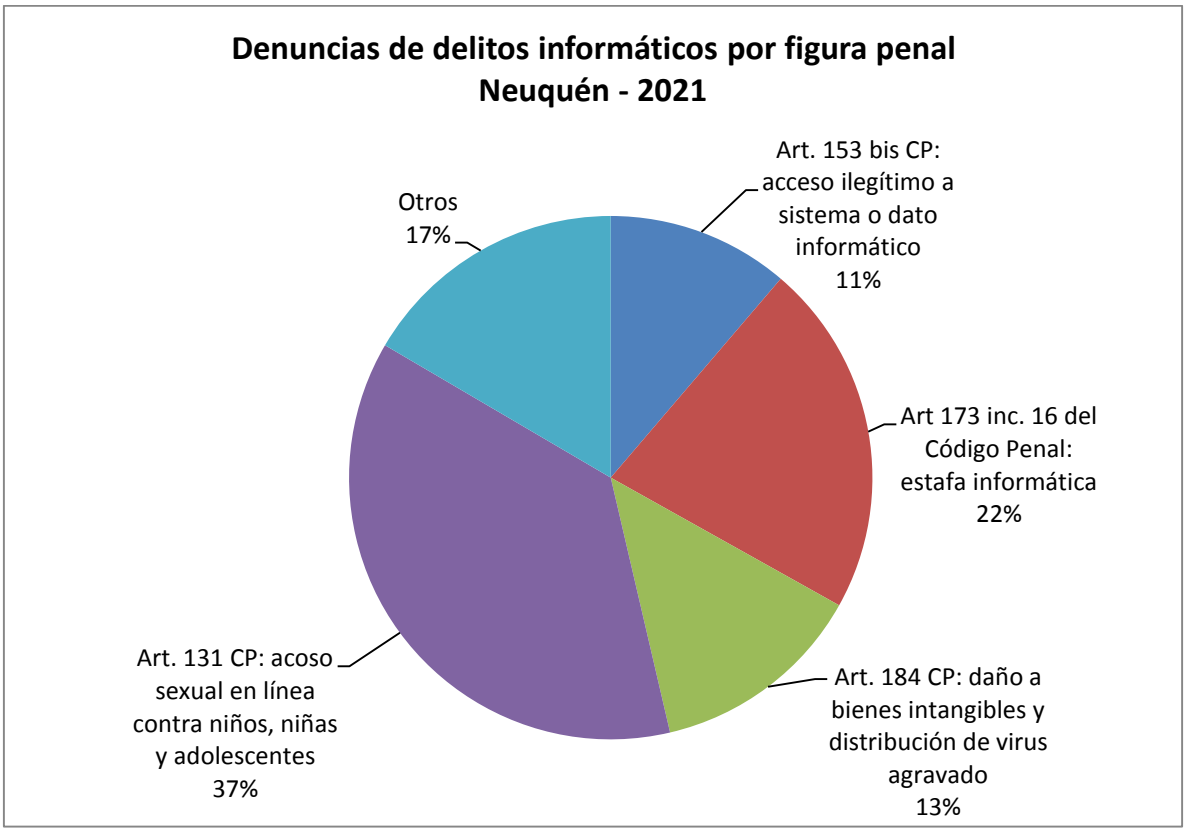
Fuente: Poder Judicial de la Provincia de Neuquén



Año 2021:

Figura penal	Denuncias
Art. 131 CP: Grooming	56
Art 173 inc. 16 del CP: Estafa informática	33
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	20
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	17
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	7
Art. 183 CP: Daño a bienes intangibles y distribución de virus	6
Art. 153 CP: Violación de correspondencia electrónica	4
Art. 155 CP: Publicación indebida de comunicaciones	4
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	4
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**151**

Fuente: Poder Judicial de la Provincia de Neuquén

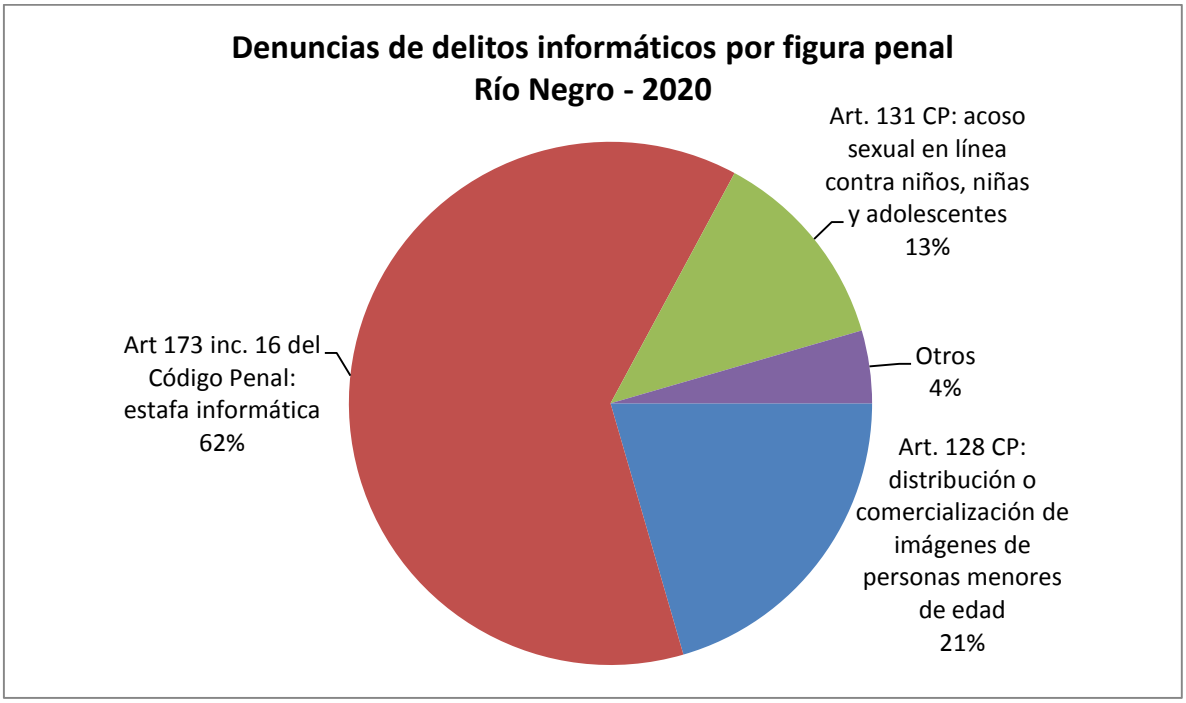


3.21. Río Negro

Año 2020:

Figura penal	Denuncias
Art 173 inc. 16 del CP: Estafa informática	222
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	73
Art. 131 CP: Grooming	45
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	6
Art. 255 CP: Alteración de evidencia informática	5
Art. 153 CP: Violación de correspondencia electrónica	4
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	1
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**356**

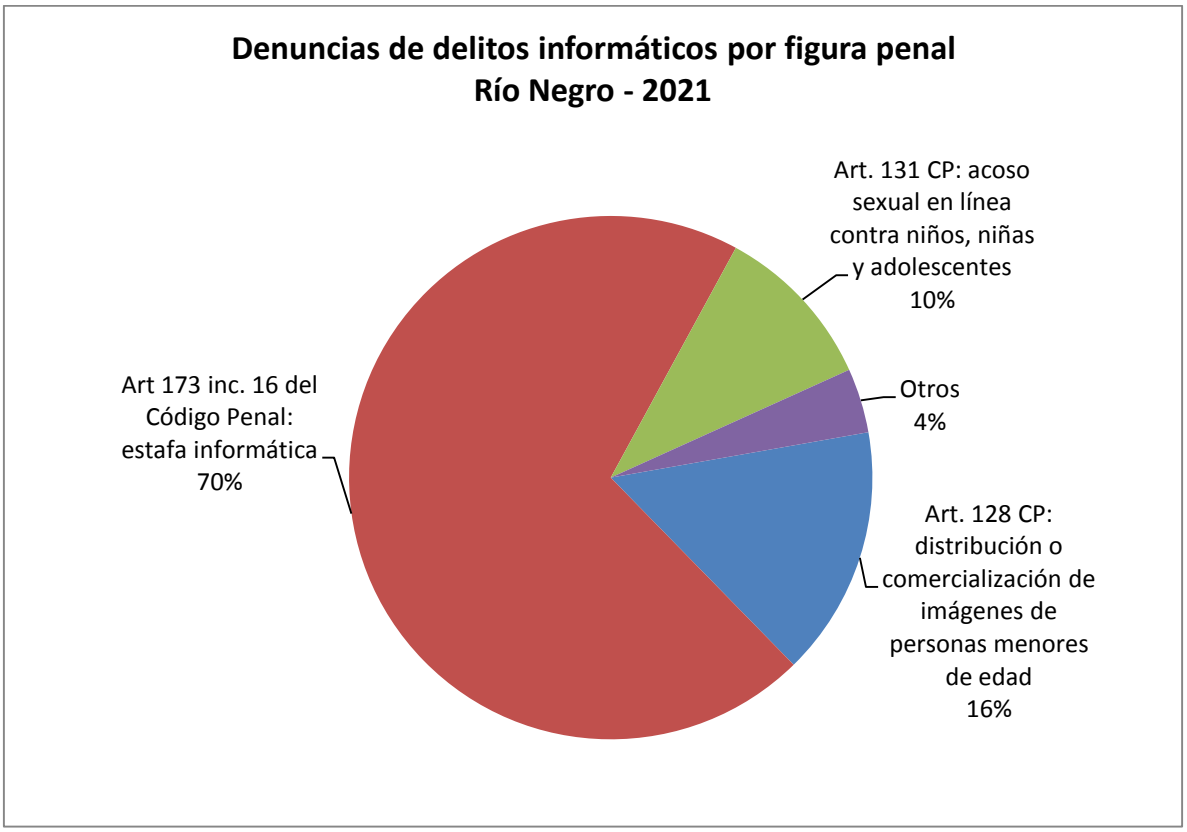
Fuente: Poder Judicial de la Provincia de Río Negro



Año 2021:

Figura penal	Denuncias
Art 173 inc. 16 del CP: Estafa informática	300
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	66
Art. 131 CP: Grooming	44
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	9
Art. 153 CP: Violación de correspondencia electrónica	7
Art. 255 CP: Alteración de evidencia informática	1
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 183 CP: Daño a bienes intangibles y distribución de virus	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
TOTAL	**427**

Fuente: Poder Judicial de la Provincia de Río Negro

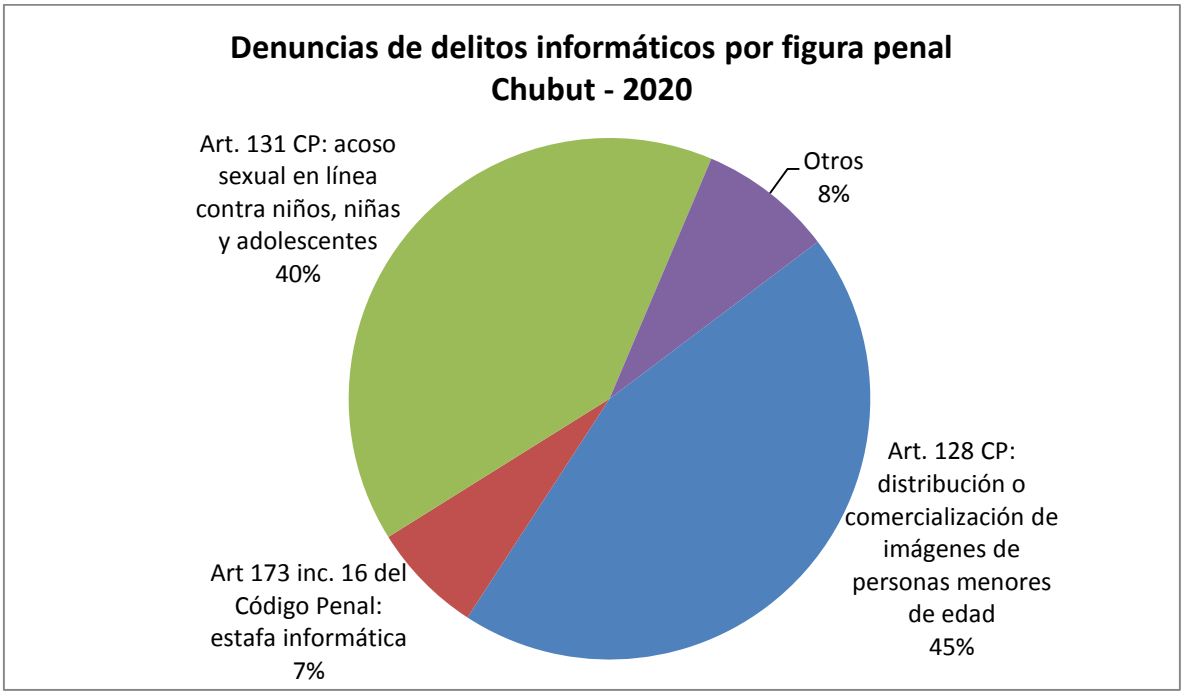


3.22. Chubut

Año 2020:

Figura penal	Denuncias
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	32
Art. 131 CP: Grooming	29
Art 173 inc. 16 del CP: Estafa informática	5
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	2
Art. 183 CP: Daño a bienes intangibles y distribución de virus	2
Art. 157 CP: Revelación de secretos	1
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**72**

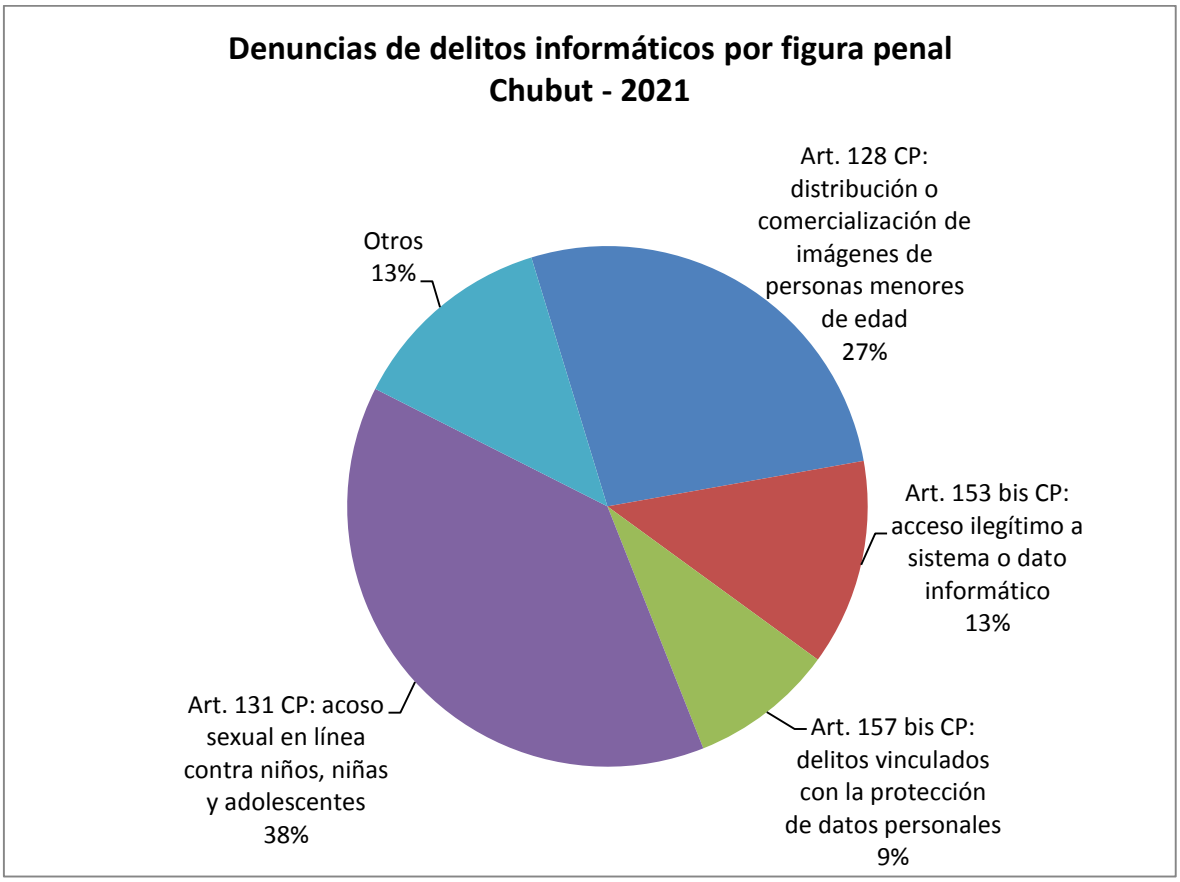
Fuente: Superior Tribunal de Justicia de la Provincia de Chubut



Año 2021:

Figura penal	Denuncias
Art. 131 CP: Grooming	30
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	21
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	10
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	7
Art. 153 CP: Violación de correspondencia electrónica	3
Art 173 inc. 16 del CP: estafa informática	3
Art. 183 CP: Daño a bienes intangibles y distribución de virus	3
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	1
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**78**

Fuente: Superior Tribunal de Justicia de la Provincia de Chubut

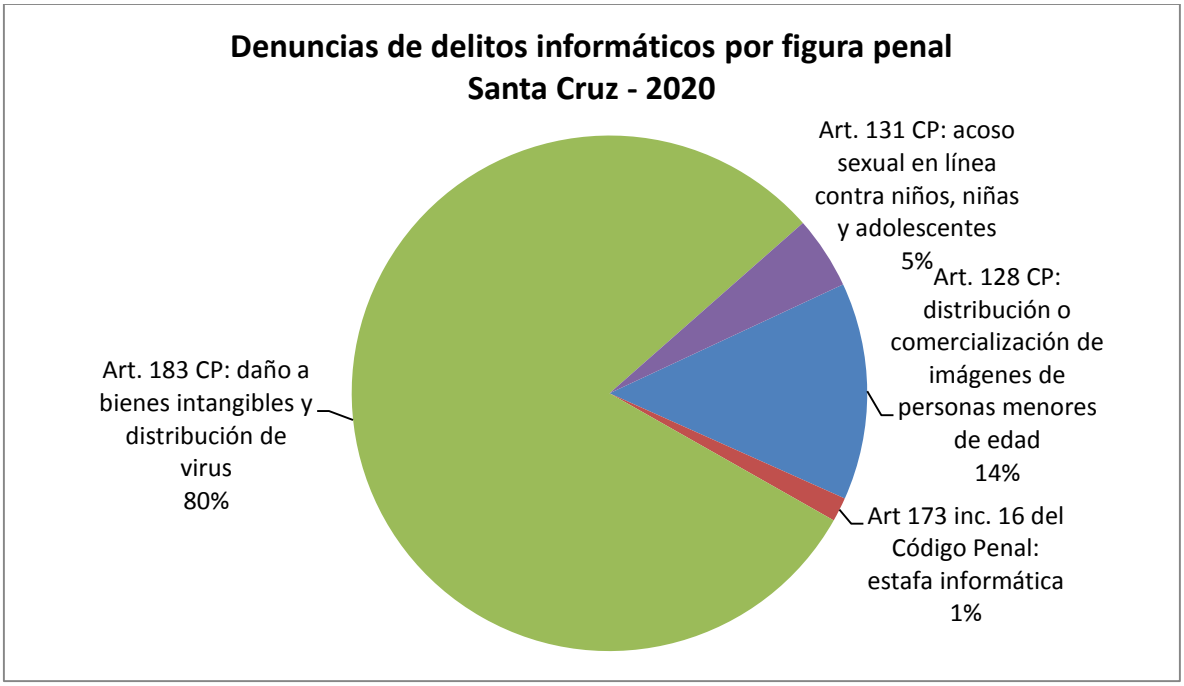


3.23. Santa Cruz

Año 2020:

Figura penal	Denuncias
Art. 183 CP: Daño a bienes intangibles y distribución de virus	53
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	9
Art. 131 CP: Grooming	3
Art 173 inc. 16 del CP: Estafa informática	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 CP: Revelación de secretos	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**66**

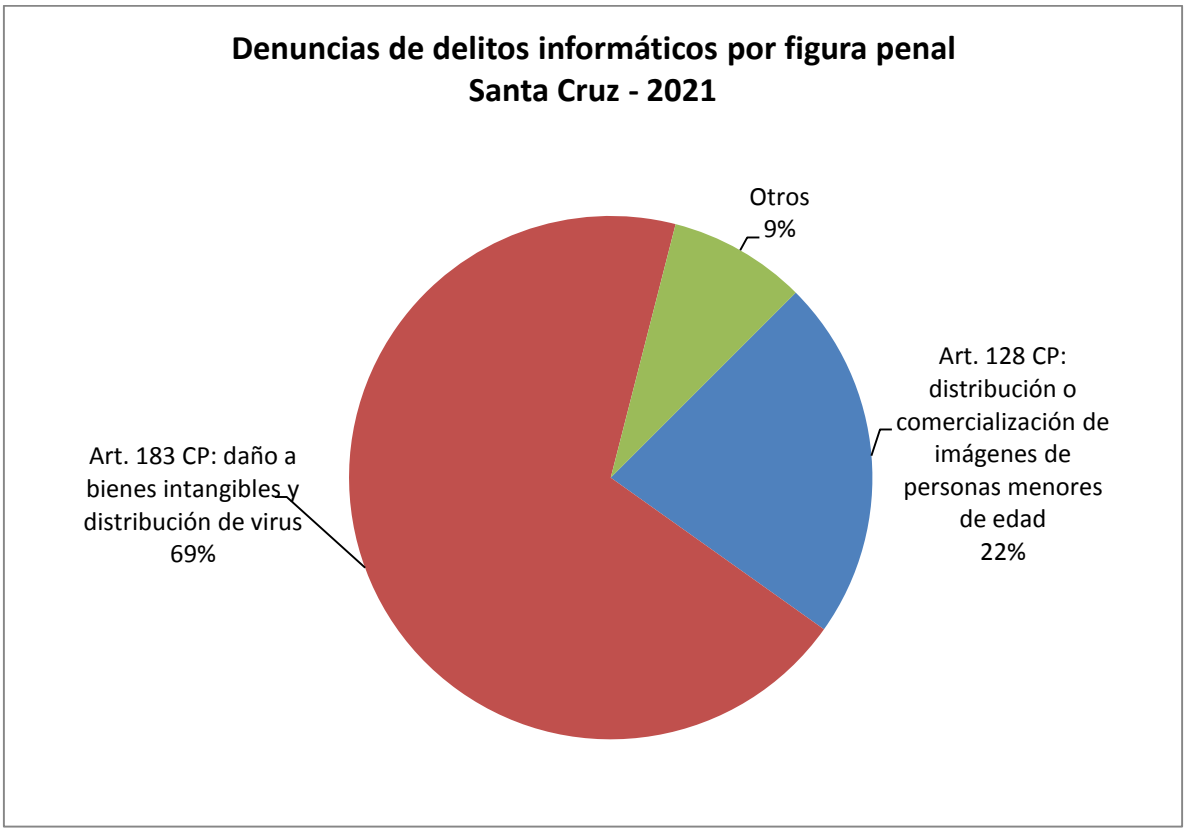
Fuente: Superior Tribunal de Justicia de la Provincia de Santa Cruz



Año 2021:

Figura penal	Denuncias
Art. 183 CP: Daño a bienes intangibles y distribución de virus	65
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	21
Art 173 inc. 16 del CP: Estafa informática	3
Art. 131 CP: Grooming	3
Art. 157 CP: Revelación de secretos	1
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**94**

Fuente: Superior Tribunal de Justicia de la Provincia de Santa Cruz

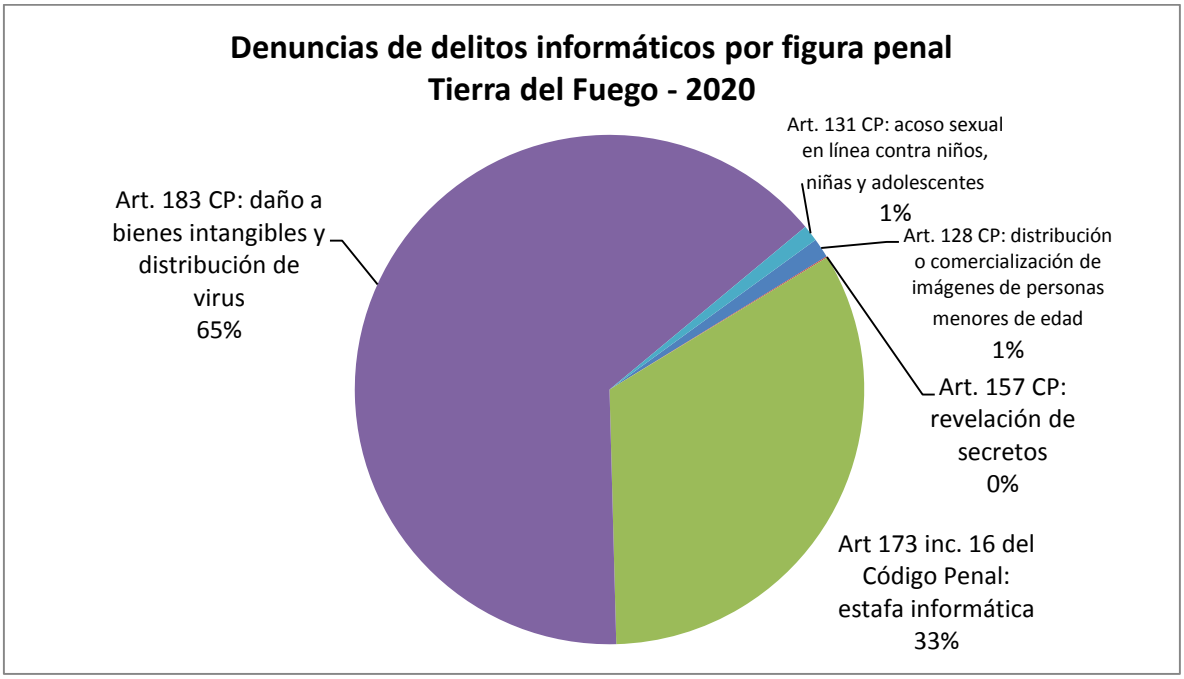


3.24. Tierra del Fuego

Año 2020:

Figura penal	Denuncias
Art. 183 CP: Daño a bienes intangibles y distribución de virus	933
Art 173 inc. 16 del CP: Estafa informática	482
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	18
Art. 131 CP: Grooming	15
Art. 157 CP: Revelación de secretos	1
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**1.449**

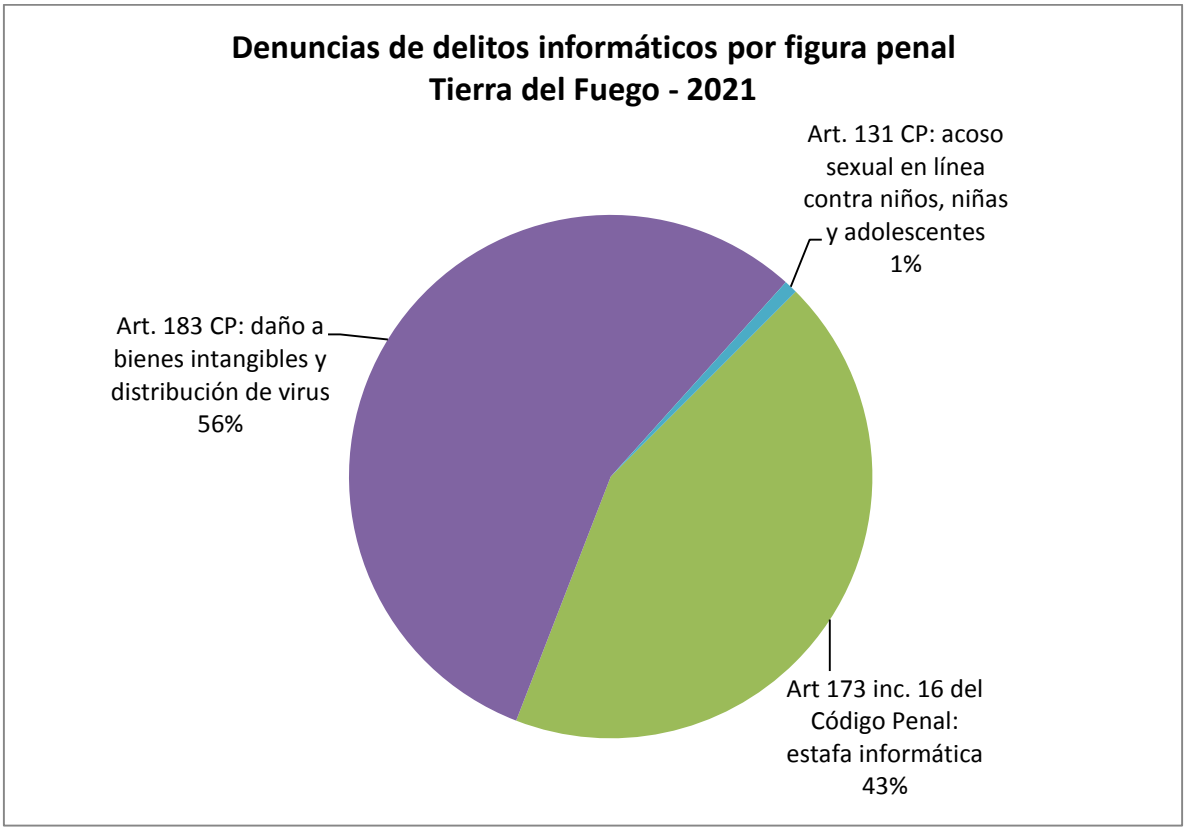
Fuente: Superior Tribunal de Justicia de la Provincia de Tierra del Fuego



Año 2021:

Figura penal	Denuncias
Art. 183 CP: Daño a bienes intangibles y distribución de virus	1.071
Art 173 inc. 16 del CP: Estafa informática	833
Art. 131 CP: Grooming	16
Art. 128 CP: Tenencia, distribución, comercialización de imágenes de abuso sexual de NNyA	7
Art. 157 CP: Revelación de secretos	3
Art. 153 CP: Violación de correspondencia electrónica	-
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	-
Art. 155 CP: Publicación indebida de comunicaciones	-
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	-
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	-
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	-
Art. 255 CP: Alteración de evidencia informática	-
TOTAL	**1.930**

Fuente: Superior Tribunal de Justicia de la Provincia de Tierra del Fuego

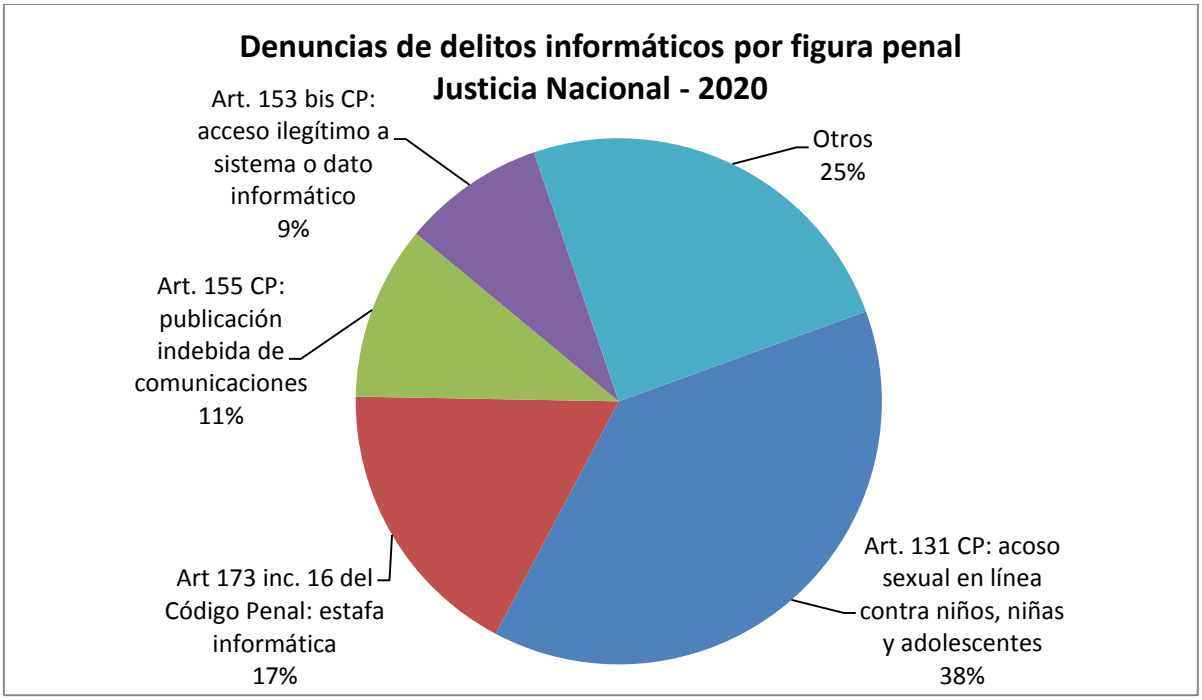


3.25. Justicia Nacional

Año 2020:

Figura penal	Denuncias
Art. 131 CP: Grooming	118
Art 173 inc. 16 del CP: Estafa informática	54
Art. 155 CP: Publicación indebida de comunicaciones	33
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	27
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	20
Art. 153 CP: Violación de correspondencia electrónica	13
Art. 255 CP: Alteración de evidencia informática	11
Art. 183 CP: Daño a bienes intangibles y distribución de virus	11
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	11
Art. 157 CP: Revelación de secretos	5
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	3
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	2
TOTAL	**308**

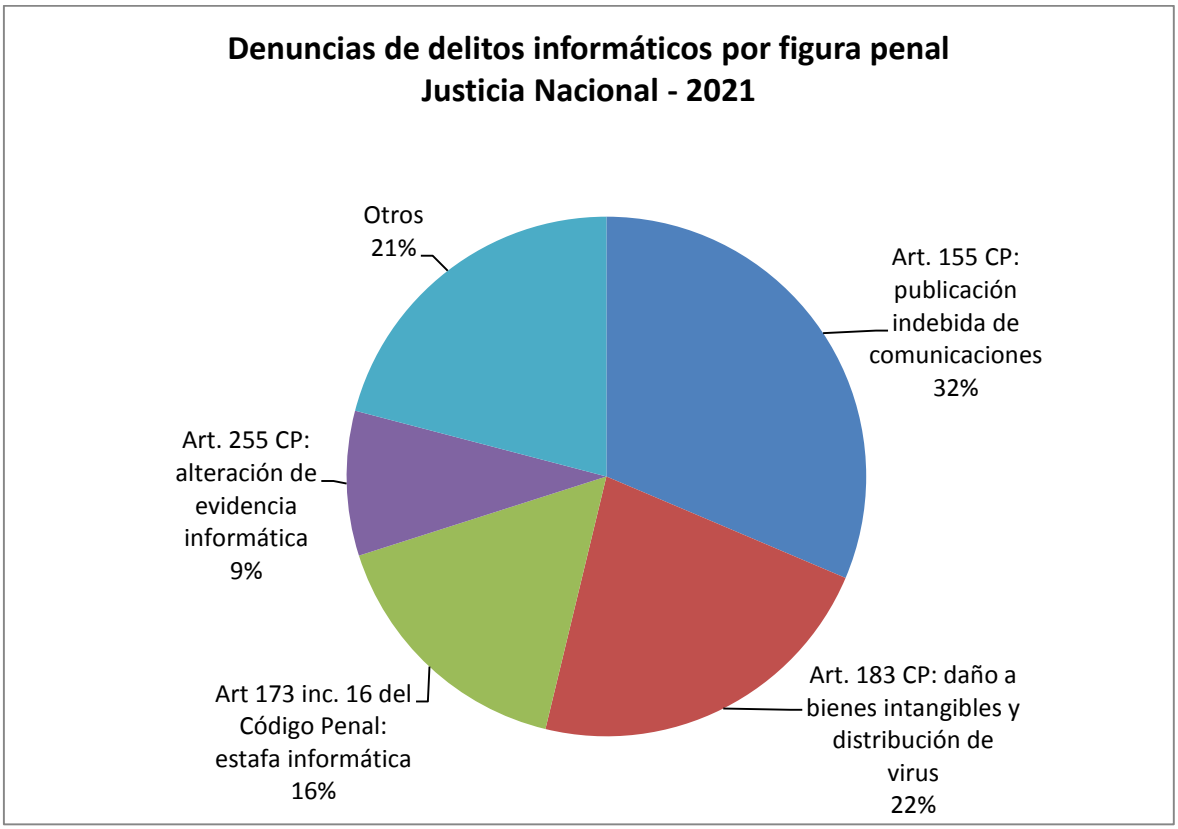
Fuente: Secretaría de Coordinación Institucional del Ministerio Público Fiscal de la Ciudad de Buenos Aires



Año 2021:

Figura penal	Denuncias
Art. 155 CP: Publicación indebida de comunicaciones	129
Art. 183 CP: Daño a bienes intangibles y distribución de virus	92
Art 173 inc. 16 del CP: Estafa informática	67
Art. 255 CP: Alteración de evidencia informática	37
Art. 128 CP: Tenencia, distribución o publicación de imágenes de abuso sexual de NNyA	27
Art. 153 CP: Violación de correspondencia electrónica	18
Art. 131 CP: Grooming	11
Art. 157 bis CP: Delitos vinculados con la protección de datos personales	11
Art. 184 CP: Daño a bienes intangibles y distribución de virus agravado	7
Art. 157 CP: Revelación de secretos	6
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	5
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	1
TOTAL	**411**

Fuente: Secretaría de Coordinación Institucional del Ministerio Público Fiscal de la Ciudad de Buenos Aires


Denuncias de delitos informáticos por figura penal
Justicia Nacional - 2021
Otros 21%
Art. 155 CP: publicación indebida de comunicaciones 32%
Art. 255 CP: alteración de evidencia informática 9%
Art 173 inc. 16 del Código Penal: estafa informática 16%
Art. 183 CP: daño a bienes intangibles y distribución de virus 22%

4. DOSSIER:

Modalidades cibercriminales detectadas a partir de la Pandemia del COVID-19 en Argentina

4.1. Introducción

En términos criminológicos, el criterio que mejor explica al delito informático es el *criterio de oportunidad.* Si bien es una correinte criminológica que no aplica en el mundo físico, en los entornos digitales algunos individuos toman decisiones acerca de cometer un delito basándose en una serie de inputs entre los que figuran; el esfuerzo que implica, los beneficios potenciales, el apoyo con el que cuenta, el esfuerzo que implica, el riesgo de ser detenido y las necesidades particulares de la propia persona. En este sentido, desde que Internet pasó a ser una parte de la vida cotidiana de las personas a mediados de la década de 1990[10], lo/as ciberdelincuentes cuentan con una red de alcance global para establecer comunicaciones con posibilidades de alcanzar a una gran cantidad de personas en cuestión de segundos, con el uso de tecnologías de fácil manejo y de manera anónima, esta última característica a partir de la posibilidad de construcción de identidades ficticias para el uso de servicios y aplicaciones que permite la mayoría de las empresas proveedoras de Internet.

A partir de la pandemia del COVID-19 a nivel global, gran parte de la ciudadanía ha tenido mayores posibilidades de aprehensión de uso de TICDs a partir del desarrollo del trabajo desde el hogar, e-learning y la realización de trámites en línea, tales como servicios de mensajería, uso de redes sociales, aplicaciones de videollamadas y sistemas de pago electrónico, entre otros. En este sentido, lo/as ciberdelincuentes han aprovechado el incremento de uso de servicios y aplicaciones en línea y para de *sofisticar sus técnicas de comisión de ciberdelitos y establecer nuevas modalidades de ilícitas* ya existentes en el período pre-pandemia en Argentina. Este fenómeno está acompañado con una particularidad que se vio con la llegada del Aislamiento Social Preventivo y Obligatorio (ASPO) decretado por el gobierno nacional en marzo de 2020,

[10] Internet surgió siendo una red de computadoras militares en los Estados Unidos en 1969, creada por el Departamento de Defensa de ese país con el objetivo de crear un medio de comunicacion alternativo a los convencionales. Su fin era puramente militar, ya que la idea original era diseñar una tecnología que no impidiera la "incomunicacion" en ese territorio en caso que colapsaran los sistemas tradiciones de telecomunicaciones por un ataque nuclear soviético. Una vez finalizada la Guerra Fría, el gobierno de ese pais decidió expander globalmente esta tecnología a mediados de la década de 1990 para el uso civil mediante el desarrollo del comercio electrónico, presentada como "la" modalidad de negocios del siglo 21.

que es la aparición de *asociaciones ilícitas y bandas con cierto grado de organización* que toman al cibercrimen como emprendimiento delictivo a nivel local, muchas de ellas operativas desde instituciones penitenciarias[11].

4.2. Modalidades de ciberdelito a nivel de usuario/as particulares

Fraudes y estafas en línea

Para la Organización para la Cooperación del desarrollo Económico (OCDE), un fraude es la adquisición indebida de bienes ajenos por medio del engaño. Si bien la estafa suele ser utilizada como sinónimo, la misma constituye un tipo de fraude que persigue una finalidad económica. Básicamente, un fraude es una acción que se comete con el objetivo de producir un perjuicio a una persona, organización o al Estado en beneficio de quien lo lleva adelante. El engaño puede realizarse a través de una ocultación, falsificación o artificio, entre otros. El fraude económico suele ser entendido como estafa, donde el objetivo del engaño es producir un perjuicio de tipo patrimonial a la víctima –financiero o material– con un fin puramente de lucrativo en beneficio del autor. En cuento a la aparición de Internet como medio de comunicación cotidiano durante el siglo 21, podría definirse a los fraudes que se cometen a través de esta plataforma tecnológica como *''cualquier tipo de esquema de fraude que utiliza uno o más componentes de Internet*, *como salas de chat*, *correo electrónico*, *tableros de mensajes o sitios web*, *para presentar solicitudes fraudulentas a posibles víctimas*, *a realizar transacciones fraudulentas o transmitir el producto del fraude a instituciones financieras u otras personas relacionadas''*[12].

---

[11] Para mayor información, véase:
"ESTAFAS VIRTUALES EN ROSARIO: DETIENEN A BANDA DE CORDOBESES". Sitio web de Radio Cadena 3 (santa Fe), 7 de abril de 2022. Disponible en https://www.clarin.com/policiales/desbaratan-banda-estafas-virtuales-funcionaba-carcel-batan_0_0lTlTnawzY.html#:~:text=La%20Polic%C3%ADa%20de%20la%20Ciudad,ciudad%20de%20Mar%20del%20Plata.
"DESBARATAN UNA BANDA DE ESTAFAS VIRTUALES QUE FUNCIONABA DESDE LA CÁRCEL DE BATÁN". Diario Clarín, 23 de mayo de 2022. Disponible en https://www.clarin.com/policiales/desbaratan-banda-estafas-virtuales-funcionaba-carcel-batan_0_0lTlTnawzY.html#:~:text=La%20Polic%C3%ADa%20de%20la%20Ciudad,ciudad%20de%20Mar%20del%20Plata.
"DESBARATAN UNA BANDA DE ESTAFADORES QUE VIRTUALES QUE FUNCIONABA DESDE LA CÁRCEL DE URDAMPILLETA". Diario "La Mañana" de Bolívar, 2 de diciembre de 2022. Disponible en https://www.diariolamanana.com.ar/noticia/desbarataron-una-banda-de-estafas-virtuales-que-funcionaba-desde-la-carcel-de-urdampilleta/#:~:text=La%20Polic%C3%ADa%20de%20la%20Sub,y%20que%20resid%C3%ADan%20en%20Bol%C3%ADvar.

[12] United States Department uf Justice: ¿WHAT IS INTERNET FRAUD? Disponible en www.justice.gov [consultado 10-12-2007]

La mayoría de los fraudes y estafas cometidos en este período en el país, estuvieron basados en campañas de **phishing**. La palabra phishing es una contracción de las palabras en inglés *password harvesting fishing* –algo así como "cosecha y pesca de contraseñas". Criminológicamente es un fraude orientado a obtener datos personales de una víctima en forma ilícita, una técnica utilizada por lo/as ciberdelincuentes para obtener información de una persona u organización para cometer un ilícito posterior en nombre de las mismas, es decir, usurpando su identidad. Como fraude, podríamos decir que representa es un fraude de "robo de identidad" que utiliza herramientas de *ingeniería social*. La ingeniería social es una rama de la informática que hace alusión al proceso por el cual se intenta obtener información de un usuario mediante métodos y herramientas no técnicas, como por ejemplo, el proceso comunicacional. Es utilizada por los "phishers" para ganarse la confianza de la víctima y así obtener sus datos para la comisión de un delito posterior, generalmente una estafa.

En los casos de phishing, el/la ciberdelicuente a su vez suplanta la identidad de un tercero, es decir, se hace pasar, por ejemplo, por un banco, un organismo público, una tarjeta de crédito o una ONG, entre otras organizaciones, enviando comunicaciones fraudulentas por Internet (a través de correos electrónicos, mensajes de texto de telefonía móvil –SMS-, mensajes privados en redes sociales, mensajes de WhastApp o de chats, o publicaciones en grupos de discusión o foros de sitios web, entre otros). Los motivos de la comunicación son, habitualmente, un supuesto problema de seguridad, la actualización de datos, aprovechamiento de una oferta o promoción, la caducidad de un servicio o producto o la urgencia por una necesidad de la potencial víctima. Los datos solicitados más frecuentes son nombre y apellido, DNI, número de tarjeta de crédito, credenciales de acceso a servicios y aplicaciones (nombre de usuario y contraseña) o número de cuenta bancaria, entre otros.

Phishing bancario

Como modalidad delictiva, el fraude más común para el robo de identidad mediante esta técnica es la del *phishing bancario*. Antes de la pandemia, la vía de contacto más frecuente era el correo electrónico, donde a través de un mensaje, la supuesta institución bancaria le solicita en tanto cliente valide su usuario y contraseña de acceso a homebanking o banca electrónica. El cuerpo del mensaje contiene un enlace que deriva a un sitio web falso creado por el estafador para que la víctima vuelque sus "credenciales de acceso" o claves de usuario a homebanking. El "phisher" intentara

utilizar esos datos para hacer transferencias bancarias a una cuenta manejada por el mismo.

Correo electrónico fraudulento mediante la técnica de phishing bancario

Sitio web falso montado por un phisher para la obtención de credenciales de acceso bancarias

En la mayoría de los casos, dichos mensajes provenían del exterior de la República Argentina –a veces traducidos al idioma español mediante traductores - y eran enviados en forma masiva a una lista de direcciones de correo electrónico a modo de SPAM o correo no solicitado conformadas mediante la recopilación de direcciones publicadas en la web o compradas en determinados foros de Internet. Estos envíos "al voleo" parten del desconocimiento de datos previos de la víctima, motivo por el cual el destinatario del mensaje podía no tener una cuenta en el banco desde donde supuestamente provenía la comunicación fraudulenta.

A partir del Aislamiento Social Preventivo y Obligatorio (ASPO) decretado por el Gobierno Nacional a partir de marzo de 2020[13], las solicitudes fraudulentas de phishing comenzaron a ser dirigidas, personalizadas. Esta modalidad se denomina *spearphishing*, donde el "phisher" cuenta con información personal de la víctima en forma previa al establecimiento de la comunicación, tales como numero de celular, nombre, apellido, número de DNI y foto, entre otros.

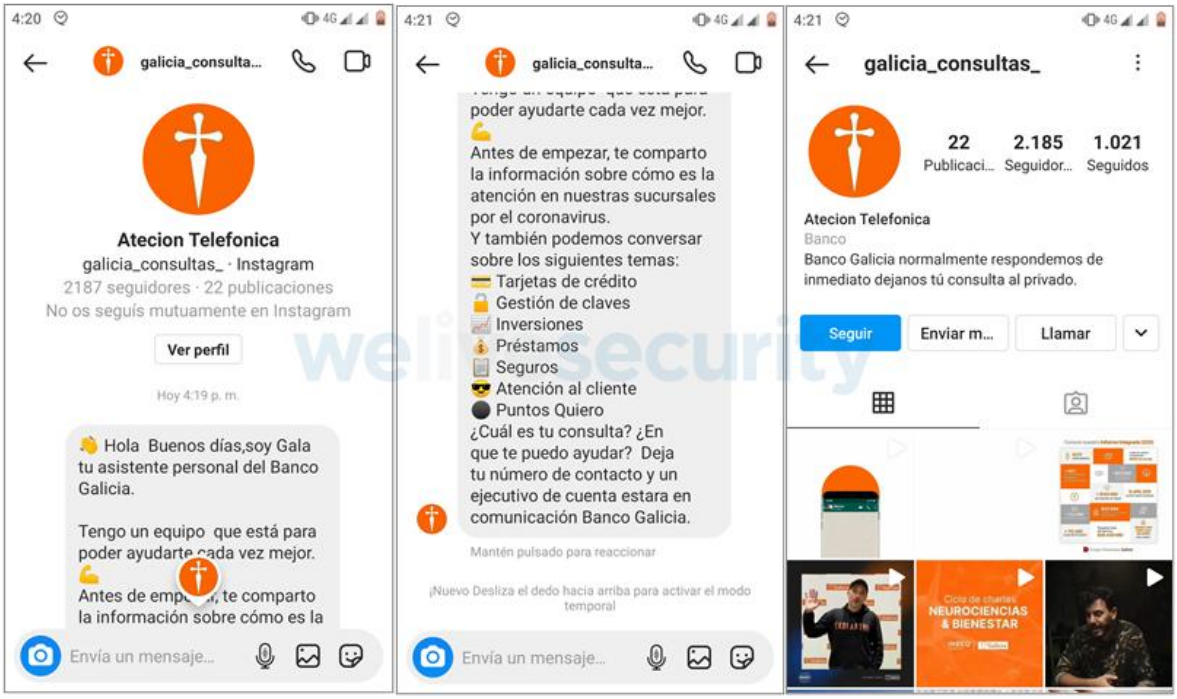
Bajo esta modalidad, se ha notado un incremento de casos de phishing bancario a través de cuentas falsas de bancos creadas en redes sociales. La ampliación de vías de contacto en la Web inauguradas por las instituciones bancarias a partir del trabajo remoto de muchos de sus clientes y el aforo temporal en la atención personalizada de las sucursales, se presentaron como sustituto de la atención personalizada en sucursales.

[13] Decreto 297/2020 del Poder Ejecutivo Nacional

Noticia sobre phishing bancario en redes sociales

En este sentido, cuentas no verificadas en Instagram -y en menor medida de Facebook- simulaban ser las oficiales del banco. Las cuentas validadas o certificadas en redes sociales y sistema de mensajería privada es un mecanismo que utilizan las empresas proveedoras de servicio de Internet para autenticar las cuentas como comprobación verdadera de legitimo usuario. Mediante una tilde, la empresa en cuestión "valida" la identidad de la persona u organización que se encuentra detrás de esa cuenta.

A diferencia del phishing tradicional, en el que se envían comunicaciones "al voleo", la mayoría de los usuarios que seguían estas cuentas falsas eran clientes reales de la institución bancaria suplantada. Tal situación le permite al atacante hacer más selectivo el fraude en cuanto al universo de potenciales víctimas. Una vez que un usuario comenzaba a seguir dichos perfiles de redes sociales fraudulentos, los phishers establecían la comunicación a través de mensajes directos dentro de la plataforma con la misma lógica del phishing tradicional para tratar de obtener datos personales de la víctima.



Mensajes fraudulentos de phishing bancario a través de mensajes directos en redes sociales

Instagram y Facebook -al igual que la mayoría de los servicios y aplicaciones de Internet- permiten la construcción de identidades ficticias para la apertura de cuentas o perfiles de redes sociales, lo que es aprovechado por lo/las ciberdelincuentes para suplantar la identidad de bancos, en la mayoría de los casos, sin supervisión o control por parte de la empresa proveedora en los casos que se usurpa la identidad de organizaciones.

Fraude de compraventa en redes sociales

Tras el cierre temporal de tiendas físicas y la disminución del trabajo presencial en el ASPO, se produjo un lógico incremento de operaciones de compraventa en línea, fundamentalmente en redes sociales. A partir de este fenómeno La empresa META, por ejemplo, creó Facebook Marketplace, un espacio dentro de la red social para que lo/as usuario/as puedan comprar y vender productos entre sí. En este caso, la empresa solo brinda el lugar para realizar la actividad, sin intereses económicos ni cobro de comisiones. A diferencia de las tiendas en línea, la plataforma solo oficia como intermediaria, sin términos y condiciones de uso comerciales para la realización de las transacciones, ni tampoco políticas de políticas de devolución ni garantías de productos, como tampoco sistemas de pago electrónico asociadas a cuentas bancarias o tarjetas de crédito para que los usuarios realicen las transacciones en línea. En estos

casos, las operaciones corren por cuenta de los acuerdos establecidos por lo/as usuario/as, generalmente estableciendo las condiciones de pago y entrega mediante utilizando el servicio de mensajería directa que brindan estas plataformas.

Ante el notable incremento del número de operaciones de compraventa en los entornos digitales, los estafadores aprovecharon la necesidad de muchos usuarios para elaborar tiendas falsas en redes sociales, como por ejemplo en Instagram, también propiedad de la empresa META. Para atraer a las víctimas, lo/as estafadore/as venden productos a bajo precio del promedio de mercado y libres de impuestos en aquellos importados, por tratarse de "zona franca" de compraventa. Asimismo, ofrecen garantías y muestran imágenes ficticias de clientes satisfechos, que están acompañados de comentarios positivos por las transacciones realizadas, todas tomadas de forma pública de la web. Los pagos deben ser siempre en efectivo o con depósito bancario. La estafa consiste en comprar un producto, realizar el pago para después no recibirlo.

Tienda falsa de compraventa de productos en redes sociales

Al igual que las cuentas falsas de bancos en redes sociales, tanto en Instagram o Facebook, las cuentas que aparecen con una tilde azul son cuentas verificadas o certificadas por la empresa META. Las mismas acreditan la identidad de la persona o la organización que se encuentra detrás de la cuenta. No todos los usuarios conocen esta medida de validación. Asimismo, no existe el impedimento técnico de creación de cuentas duplicadas, ya que no existe un límite para la apertura de nuevas cuentas. Estos

dos factores lo que facilita la comisión de este fraude por parte de lo/as ciberdelincuentes.

Ejemplo de cuentas validadas o certificadas en redes sociales

Fraude de turno de vacunación

Durante el ASPO, se produjeron diversos fraudes de robo de identidad a usuarios basados en la sustracción de cuentas de usuario para diversos fines, principalmente, económicos. Las técnicas utilizadas por los phishers estaban basadas en la obtención de alguna información solicitada por las empresas proveedoras de servicio de Internet a los usuario/as para verificar su identidad, tanto sea para iniciar la sesión en un nuevo dispositivo como para la apertura de una cuenta nueva.

En este sentido, la mayoría de las empresas denominadas "gigantes de Internet" utilizan algo que se llama *factor de doble autenticación o verificación*, una medida de seguridad adicional al nombre de usuario y contraseña que habitualmente debe ingresar el titular de una cuenta. Funciona mediante la solicitud de un dato anexo que se utiliza para intentar corroborar que efectivamente la persona detrás de la pantalla que intenta iniciar una sesión es el titular o legítimo usuario del servicio o aplicación en cuestión.

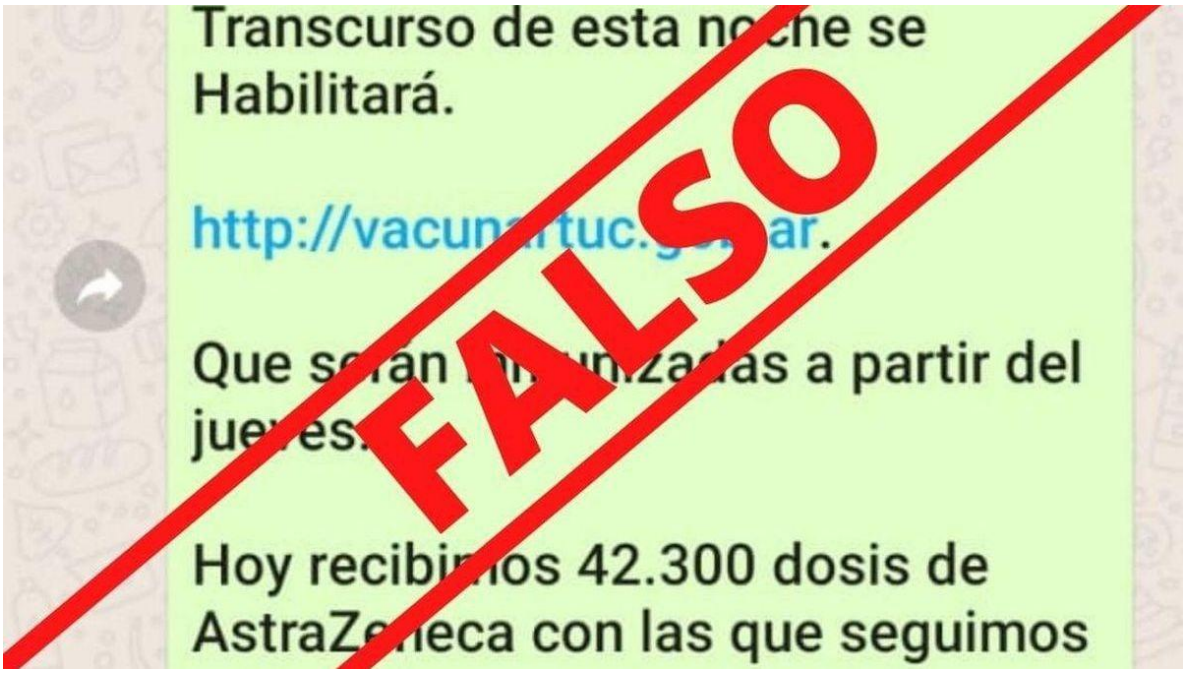
El servicio de mensajería WhatsApp, envía mediante un mensaje de texto -SMS- un código numérico de seis dígitos al número de teléfono registrado por el titular de la cuenta. Al igual que las cuentas certificadas y verificadas por la empresa Google -dueña del servicio- muchos usuarios desconocen esta funcionalidad. Lo que fue aprovechada por lo/las ciberdelincuentes para establecer un nuevo fraude de robo de identidad.

Codigo de seguridad enviado por la empresa META para un nuevo inicio de sesión en WhatsApp

A diferencia de otras jurisdicciones que gestionaban los turnos para la provisión de dosis de la vacuna contra el COVID-19 en Argentina mediante una aplicación oficial, el Gobierno de la Ciudad Autónoma de Buenos Aires notificaba a sus ciudadanos registrados los turnos correspondientes a través del servicio WhatsApp. Para esta modalidad, el phisher contaba con el número de celular, el documento, el nombre y el apellido de la potencial víctima –spearphishing-. Luego establecía una comunicación engañosa haciéndose pasar por un representante del Ministerio de Salud de la jurisdicción, encargado de informarle fecha, hora y lugar donde debía asistir para la aplicación de la segunda dosis de vacunación.

El fraude consistía en que la víctima confirme el supuesto turno mediante el envío del código numérico de seis dígitos que le había llegado a su celular via mensaje de texto -SMS-. Una vez informado el número, el phisher lo utilizaba para iniciar la sesión de WhatsApp con el número de celular de la víctima en otro dispositivo, es decir, que utilizaba y el doble factor de autenticación. Una vez que se hizo de la cuenta del usuario, emprendía una estafa usurpando la identidad de la víctima que consistía en enviar mensajes a sus contactos solicitándoles dinero por un problema personal, inconvenientes con la tarjeta de débito; o el ofrecimiento de la venta de dólares a bajo

precio de acuerdo a los valores de mercado vigentes. Si bien este fraude se inicia con la aplicación de la segunda dosis de vacunas en CABA, el mismo se replicó en varias jurisdicciones del país.



Ejemplo de mensaje engañoso del fraude de vacunación

Fraude del intento de hackeo a cuenta de servicio de Internet

Algunos fraudes y estafas en línea adoptaron modalidades basadas en técnicas de comisión similares a las utilizadas en el mundo físico. En este tipo de fraude, se utilizó el mismo modus operandi utilizados por los "secuestros virtuales". Este tipo de secuestros –que adoptan esa denominación a partir de que no son reales, no porque fuesen cometidos en "entornos virtuales de Internet"- se inician con un llamado telefónico -la mayoría de las veces mediante telefonía fija, no celular- donde un supuesto secuestrador tiene cautivo/a a un familar de la potencial víctima y exige a cambio de su liberación, el pago de una suma importante de dinero en forma inmediata a modo de rescate, bajo amenaza de dañar o asesinar a la persona secuestrada si no cumple con ese pedido. Generalmente, acuerdan la operación en un lugar cercano al domicilio de la víctima del llamado y en altas horas de la noche o la madrugada, en tanto que de esa forma el engaño puede resultar más eficaz si la persona se encuentra cansada o dormida.

Partiendo de esta modalidad, lo/as ciberdelincuentes hicieron uso de esta técnica horaria para simular un intento de sabotaje a una cuenta de servicio o aplicación o perfil

de una red social. Un ejemplo sucede cuando la víctima recibe un mensaje de WhatsApp en horas de la madrugada, por parte de un supuesto empleado del área de seguridad de una empresa proveedora y le informa que existen intentos de acceso así cuenta por parte de un/a tercero/a o que la misma fue vulnerada (hackeada). Para recuperarla, intenta iniciar un proceso de acreditación de identidad con el claro fin de obtener datos personales del usuario. Al igual que otros fraudes de tipo spearphishing, el/la estafador/a le envía a la víctima una imagen con datos personales de ella, como, por ejemplo, su foto o el número de pasaporte. El phisher puede también intentar establecer una comunicación telefónica a través de videollamadas producidas dentro de la aplicación, inclusive por vía telefónica a su línea móvil, es decir, fuera de la aplicación WhatsApp.

Ejemplo de fraude del intento de hackeo a cuenta de Twitter

Fraude de soborno extorsivo

El fraude se inicia a partir de un intercambio de mensajes por parte de un usuario –generalmente de sexo masculino- que establece comunicación con una supuesta mujer a través de los servicios de mensajería de una aplicación de encuentros o sitios web de citas. En el intercambio, la mujer obtiene datos personales del usuario tales como nombre, edad, ciudad de residencia y número de teléfono celular.

En el intercambio, la mujer convence a la víctima de practicar sexting, dentro de la aplicación o el sitio o por sistema de mensajería, fuera de aquel. El sexting es el intercambio de imágenes y videos eróticas y/o pornográficos con escenas de desnudez, semidesnudez o representaciones genitales que sirve como especie de sexo digital o cibersexo o intercambio previo para un posible encuentro personal posterior.

Una vez finalizado el intercambio, momentos después llega una comunicación por WhatsApp al hombre por parte de un supuesto policía o empleado de una fiscalía aduciendo que dicha persona se había comunicado con una menor de edad víctima de una red de trata que estaba siendo investigada por la justicia, o en su defecto, que la madre o el padre de la persona menor de edad se presentó en la comisaría para realizar la denuncia al descubrir los mensajes en el celular de su hija.

Una vez notificada la situación, el agente de la ley le ofrece solucionar el problema legal a cambio de una suma de dinero para evitar presentar la denuncia formalmente. Para que el engaño sea más creíble, el mensaje puede estar acompañado por el envío de una copia de la denuncia en curso donde figura el nombre de la víctima y los cargos que se le imputa, como también así la muestra de las "pruebas", las imágenes eróticas intercambiadas por el hombre dentro de la red social

Ejemplo de mensaje extorsivo a una víctima del fraude de soborno

El fraude extorsivo se complementa con amenazas de que si el pago no se realiza rápidamente su domicilio puede ser allanado, o en su defecto, los padres de la menor van a hacer pública esa información en las redes sociales "escrachando", en oportunidades, en medios de comunicación. La mayoría de las veces, lo/as ciberdelincuentes se aprovechan del desconocimiento que las aplicaciones de citas o sitios de encuentros exigen en sus términos y condiciones de uso del servicio los usuarios sean mayores de edad. Esto, sumado a que los mecanismos de acreditación de identidad de las propios empresas proveedores a veces resultan endebles brinda el marco de oportunidad ideal para la comisión de esta estafa.

Fraude de retiro de encomienda postal

El fraude se inicia con un mensaje recibido a la potencial víctima vía correo electrónico o mensaje de texto (SMS) donde se le notifica sobre un paquete de encomienda pendiente de retiro a su nombre. El contenido de la comunicación puede poseer un enlace que deriva a un sitio web falso de la supuesta empresa postal en cuestión donde el cliente puede chequear el estado del envío, como técnica utilizada por el phisher para hacer más creíble el engaño. El fraude tiene como finalidad obtener datos del usuario para robar su identidad, tanto, así como producir una estafa mediante el pago de cierta cantidad de dinero en conceptos de cargos aduaneros. Aquí lo/as ciberdelincuentes juegan con el factor curiosidad de las víctimas a partir de la posibilidad de pérdida de un envío postal donde la persona desconoce el contenido del mismo.


Correo Argentino

¡Llegó tu encomienda!

Le informamos que su encomienda procedente del exterior se encuentra disponible en nuestro centro de distribución logístico para su entrega. Para proceder a la entrega de la misma debe abonar los aranceles que Aduana nos exige, según sus tasas arancelarias este es de $10.040,12 en dicho envío.

Esta diferencia debe ser abonada para entregar el producto en su domicilio o retirarlo en alguna de nuestras sucursales, de no ser así, su envío volverá al País de origen después del lapso de espera de 72 hs.

Para proceder a la liberación debe cancelar esta diferencia arancelaria dentro del plazo estipulado. Para solicitar los detalles del pago necesitamos, adjunte una captura de su DNI de frente, reverso y una selfie sosteniendo el mismo con una mano, ya que de otra forma no podremos gestionar dicho trámite por usted y necesitara un Despachante de Aduana.

Recuerde que nuestra área de trabajo solo abarca las gestiones de liberación y pagos por lo cual cualquier respuesta que no contenga las tres imágenes requeridas para iniciar el trámite de despacho será ignorada.

Si usted no desea retirar su encomienda, por favor no conteste este correo.

Paula D. Bonamassa.
Saludos Cordiales.
Correo Argentino.

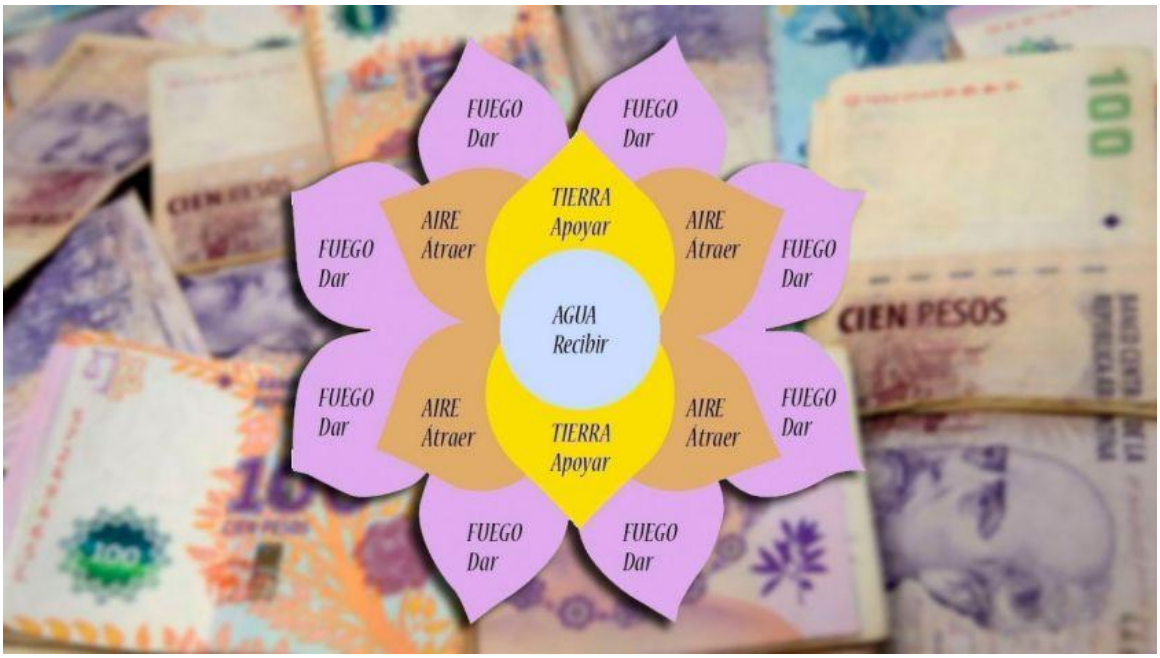
Ejemplo de mensaje fraudulento del fraude de retiro de encomienda

Fraudes basados en esquemas piramidales

La estafa comienza con la oferta realizada por una supuesta persona física o jurídica que promete altas rentabilidades por ingresar dinero a un esquema piramidal de inversión. La misma busca atraer dinero prometiendo ganancias basadas en intereses elevados a medida que ingresan más "inversionistas" al sistema. En un momento, la cadena se corta ya que es un esquema altamente especulativo basado en los aportes que realizan los eslabones inferiores. Un negocio de este tipo basado en la inversión de dinero de terceros posee una cadena de pagos finita, por dos simples motivos; 1) porque se acaba el dinero circulante o 2) no ingresan más personas al esquema. Las ganancias siempre son un porcentaje de lo invertido por los escalones menores de la pirámide. Cuando la cadena se corta; los fundadores se quedan con la mayor parte de los ingresos, y los últimos en llegar nunca recuperan lo invertido.

Ya desde antes de la pandemia se vieron estafas bajo nombres como la *"Flor de la Abundancia", "Mandala de la Prosperidad", "Telar de los Sueños", "Ruedas de amistad"* entre otros, que prometen ingresos rápidos y elevados a cambio de un aporte inicial. Muchos de ellos buscan captar mujeres con mensajes feministas, basados en un discurso que genera una mística de empoderamiento apoyados en testimonios de violencia doméstica e intercambio de mantras. Otros, motivado por una merma o lógica disminución de las actividades laborales durante el ASPO ofrecían invertir en criptomonedas prometiendo altas rentabilidades. Lo que transforma a este esquema de inversión es una estafa, la persona u organización con la cual se firma el acuerdo, en algún momento, no cumple con lo pactado, por ende, es un engaño. A diferencia de un casino de juegos, donde un jugador sabe que puede perder dinero si no gana en función del azar, aca no se advierte de las posibles pérdidas económicas que puedan sufrir aquellas personas que ingresan a la "inversión", sino muy por el contrario se las motiva con promesas de ganar cada vez más dinero sin esfuerzo alguno.

La *"Flor de la abundancia",* por ejemplo, es una estafa que se compone de 15 "pétalos" y un "centro"; lo que representa 15 personas en total, divididas en cuatro niveles. En el nivel 4, el cual lleva el nombre del elemento del *Fuego*, se ubican ocho personas que pretenden ingresar en la flor. Para hacerlo, deben depositar en la cuenta de alguien —conocido o no— una determinada cantidad de dinero. En el tercer nivel, llamado *Aire*, hay cuatro personas que ya depositaron la suma inicial y ahora deben atraer dos nuevos interesados para escalar al siguiente nivel. En el nivel 2 -Tierra- se sitúan dos personas que están a la espera de que el individuo del escalafón superior cobre para ocupar su lugar. Por último, en el nivel -Agua- se centra la persona que recibe el dinero de los primeros ocho interesados. De este modo, cobra el 800% de su inversión inicial. Es decir que si su depósito fue de 2 mil pesos, se lleva 16 mil. La estafa consiste en que se promete ganancias en base a un capital invertido. Sin embargo, como se señaló anteriormente, las ganancias del capital se obtienen por la plata que otras personas invirtieron. Así se genera una estructura que se agranda hasta el punto que colapsa y deja a varios inversore/as con pérdidas totales. En definitiva, una persona debe llevar a cabo una estafa para no perder dinero.

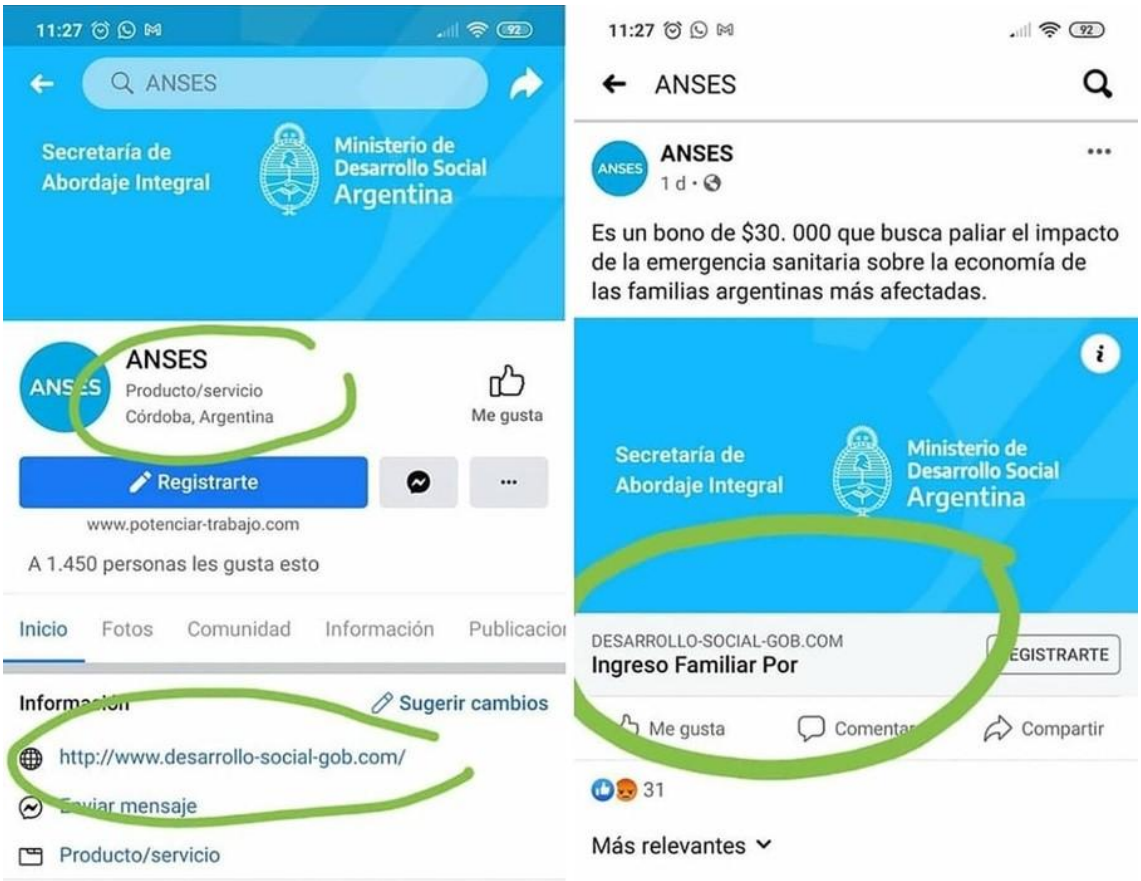


Fraude de inversión de la "flor de la abundancia"

Fraudes relacionados con programas o beneficios gubernamentales

A través de anuncios en sitios web, mensajes de texto móviles (SMS) o WhatsApp se informa de un supuesto beneficio a la víctima relacionado con un bono o beneficio excepcional, como por ejemplo, el Ingreso Familiar de Emergencia (IFE) lanzado por el gobierno para asistencia familiar[14]. Los estafadores crean sitios web o perfiles de redes sociales falsos simulando ser la autoridad gubernamental competente. En oportunidades falsos gestores de la Administración Nacional de la Seguridad Social (ANSES) contactaron a los supuestos beneficiarios por teléfono, pidiéndoles sus nombres, fechas de nacimiento y otras informaciones para otorgarles el subsidio, e incluso haciéndolos ir hasta un cajero para que tramitaran una clave de seguridad, con la que luego podían acceder a la cuenta de la víctima.

[14] COVID-19: "EL GOBIERNO IMPLEMENTARÁ EL INGRESO FAMILIAR DE EMERGENCIA (IFE) PARA ALIVIAR LA SITUACIÓN DE LOS TRABAJADORES MÁS AFECTADOS POR LA EMERGENCIA". Presidencia de la Nación, 23 de marzo de 2020. Disponible en https://www.argentina.gob.ar/noticias/covid-19-el-gobierno-implementara-el-ingreso-familiar-de-emergencia-ife-para-aliviar-la



Cuenta falsa de Instagram de la Administración Nacional de Seguridad Social (ANSES)

Como se señaló anteriormente, las redes sociales -al igual que la mayoría de los servicios y aplicaciones de Internet- permiten la construcción de identidades ficticias –inclusive de organismos de gobierno- y salvo denuncia de las organizaciones a las cuales suplantan identidad, en la mayoría de los casos las empresas no poseen sistemas de alerta ante estos casos ni mecanismos de supervisión y control por parte de los administradores del sitio en este sentido. Acá lo/as estafadores se valen del factor necesidad, a partir de posibles pérdidas laborales o disminución de ingresos durante el Aislamiento Social Preventivo y Obligatorio en Pandemia.

Fraude de DEBIN

Otro fraude relacionado con fondos bancarios es el *Fraude de DEBIN*. El débito inmediato es un sistema de pago electrónico autorizada por el Banco Central de la República Argentina en 2017 donde el/la vendedor/a de un producto o servicio o una persona física, en acuerdo con otra, envía una solicitud de débito automático de fondos

de una cuenta bancaria al titular de la misma[15]. Con el objetivo de agilizar el intercambio de activos financieros, la banca electrónica o homebanking cuenta con esta modalidad en el país. Durante la pandemia circularon engaños mediante el uso de esta modalidad, donde lo/as estafadore/as enviaban a la víctima mensajes fraudulentos donde se solicitaba autorizar una transferencia de fondos en calidad de pago cuando en realidad quien desconocía esta modalidad, al autorizar la operación lo que realmente estaba haciendo el titular es dar el visto bueno a la sustracción de dinero de su cuenta bancaria, previa solicitud de número de cuenta, alias o CBU.

Cómo funciona el Debito Inmediato (DEBIN)

Fraudes de inmunización del COVID-19

Durante los primeros meses de la pandemia, en diferentes sitios web empezó a circular la venta de productos que ofrecen remedios o curas falsas contra esta forma de Coronavirus, tales como tés, aceites esenciales y terapias intravenosas con vitamina C son solo algunos de los supuestos tratamientos antivirales que se vendían por la red. También ha habido venta online de supuestos remanentes de vacunas como Sputnik V y Astrazeneca, entre otras. En Argentina se ofrecían productos como suero equino para

[15] "DEBIN: DÉBITO INMEDIATO". Sitio Web del Banco Central de la República Argentina (BCRA). Disponible en https://www.bcra.gob.ar/Micrositios/Micrositio_debin.asp

aliviar la enfermedad de aquellos que se contagiaron el virus, sin autorización de las autoridades sanitarias. El fraude consistía en la venta de productos no avalados por la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT) del Ministerio de Salud de la Nación, como por ejemplo, dióxido de cloro.

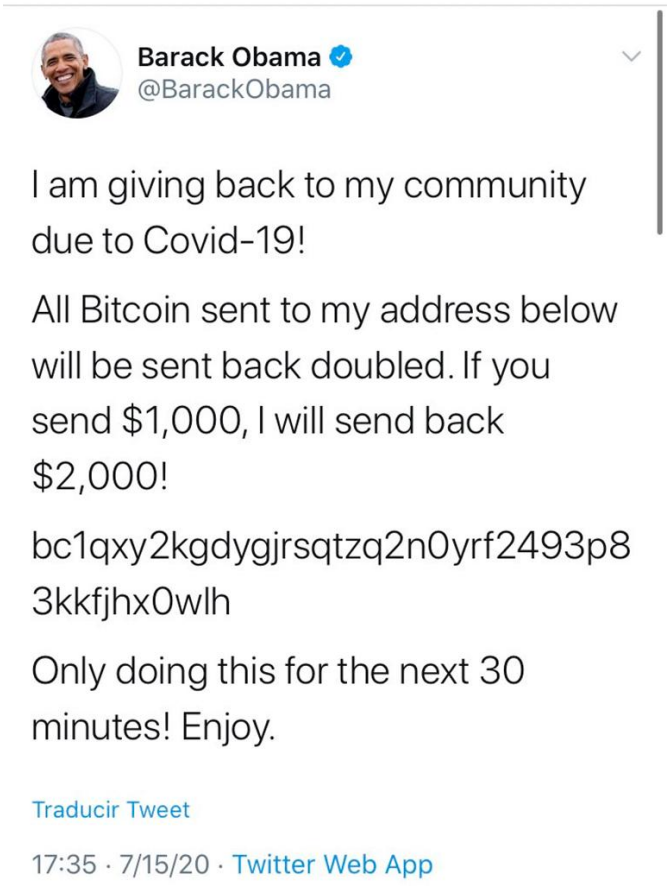
Advertencia de la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT) sobre la venta de Dióxido de Cloro en línea

Fraude de obsequio de criptomonedas

A mediados de 2021 se inició un fraude vinculado al uso de criptomonedas, fundamentalmente en la red social Twitter. Las monedas digitales basadas en sistemas criptográficos son sistemas de pago electrónicos que no dependen de la economía de un país ni de las fluctuaciones económicas de un banco central. Las "cripto" operan fuera del circuito financiero tradicional y no se encuentran asociadas a cuentas bancarias ni tarjetas de crédito de lo/as usuario/as. Funcionan en el ciberespacio y se basan en un esquema de confianza dentro de la comunidad de usuarios, quienes realizan las transacciones entre sí sin ningún tipo de intermediarios. Si bien la cotización de cada una de ellas no depende de la economía de los países ni de ninguna política económica, las mismas poseen una cotización en alguna moneda convencional, -dólares, euros o alguna moneda local-. Las operaciones son de tipo anónimas, lo que también representa un medio que permite blanquear ilícitamente fondos provenientes de actividades delictivas.

A diferencia de los fraudes descriptos anteriormente, este engaño no estuvo basado en campañas de phishing orientadas a usuario/as, sino que se valieron de determinadas vulnerabilidades o fallas de seguridad de los servidores de la empresa Twitter para

"hackear" cuentas certificadas de personalidades famosas. Esta violación de seguridad a la empresa fue realizada con el fin de ofrecer el doble de dinero transferido a una billetera digital, por ejemplo, por cuestiones caritativas. Usuarios como Elon Musk, Bill Gates, Barack Obama o Jeff Bezos fueron víctimas de suplantación de identidad para la comisión de este fraude. El tuit del CEO de Amazon, Jeff Bezos señalaba, por ejemplo**,** en un tuit publicado en su cuenta vulnerada, lo siguiente; ***"He decidido devolver a mi comunidad. Todo el dinero que se envíe a mi dirección será devuelto al doble. Sólo estoy haciendo un máximo de USD 50.000.000".*** El mensaje incluía un código para hacer la transferencia. En Argentina una de las cuentas comprometidas fue la cuenta del por aquel entonces Senador de la Nación, Jorge Taiana. El engaño trató de hacerse más creíble cuando por ejemplo se lanzaron estos mensajes engañosos de obsequios de dinero cripto después de la participación del CEO de Tesla, Elon Musk el 21 de mayo de ese año en el famoso programa *Saturday Night Live* en Estados Unidos, donde es bien sabido su agrado a este tipo de sistemas de pago electrónico.



Mensaje fraudulento publicado desde la cuenta del ex presidente de los Estados Unidos, Barack Obama

Si bien la empresa Twitter reconoció el incidente, al día de hoy no se sabe el verdadero motivo de compromiso de miles de cuentas verificadas para la comisión de esta estafa. Al respecto, en su momento y bajo la cuenta @TwitterSupport, la firma emitió el siguiente mensaje: *"Somos conscientes de un incidente de seguridad que afecta a las cuentas de Twitter. Estamos investigando y tomando medidas para solucionarlo. Informaremos a todos en breve. Es posible que no pueda tuitear o restablecer su contraseña mientras revisamos y tratamos este incidente".*

Fraudes cometidos a partir de la técnica de SIM Swapping

Mal llamada clonación de SIM o duplicación de línea de teléfono celular, el SIM Swapping o "fraude de intercambio de la tarjeta SIM" se inicia una vez que un/a ciberdelincuente cuenta con ciertos datos personales de la víctima para suplantar su identidad frente a la empresa proveedora de servicios de telefonía. Con información como *número de teléfono, nombre y apellido, DNI, domicilio*, el perpetrador se comunica al servicio de atención al cliente de la empresa haciéndose pasar por el titular de la línea y solicita suspender la misma por robo o extravío.

Una vez dada de baja, a las horas solicita el alta nuevamente con otra tarjeta SIM instalada en otro equipo. Activada la línea en otro móvil, el celular de la víctima deja de tener cobertura y se queda sin servicio. En cuanto al proceso de alta, si bien algunas operadoras permiten sustituir la tarjeta SIM por una nueva solicitándola por vía telefónica o a través de Internet –opción que se habilitó en pandemia- en algunos casos es necesario dirigirse a una tienda física. En oportunidades, lo/as ciberdelincuentes hacen uso de fotocopias del DNI e intentan aparentarse físicamente a la foto de la persona que aparece en el documento, para así engañar a lo/as empleado/as. Asimismo, hay casos de empleados infieles de las empresas de telefonía celular quienes realizan la operatoria a cambio de dinero por parte de los perpetradores.

Los objetivos de lo/as ciberdelincuentes una vez que se hacen con la línea de telefonía móvil de la víctima son varios, pero el fin es tener acceso a servicios y aplicaciones del titular de la línea como a su cuenta bancaria, cuentas de servicios de pago electrónico o perfiles de redes sociales, entre otros. La ventaja de SIM Swapping es que muchos de dichos servicios se encuentran sincronizados con otras cuentas, como por ejemplo las cuentas de Google si es un celular con sistema Operativo Android. Asimismo, muchos usuarios activan el factor de doble autenticación, donde el mismo se establece a través de SMS, en poder del/de la ciberdelincuente, como es el caso de WhatsApp.

A raíz del incremento de los casos de SIM Swapping a partir del ASPO en Argentina, la justicia federal ordenó al Ente Nacional de Comunicaciones (ENACOM) obligue a las empresas prestadoras del servicio de telefonía celular a establecer implementar mecanismos de verificación de identidad más exhaustivos a la hora de dar de alta líneas de telefonía en dispositivos nuevos[16]. En función de este pedido, el organismo rector solicitó a las mismas informe cuales son los procedimientos utilizados para verificar la titularidad de un cliente en la activación de líneas y obligó a las empresas a establecer un nuevo mecanismo en un plazo no mayor a 60 días[17].

4.3. Modalidades de ciberdelito a nivel de organizaciones

Ataques de ransomware a organizaciones

El **ransomware** -conjunción de las palabras en inglés "*ransom*" -rescate- y software- es un programa malicioso –malware- que encripta determinados archivos de un dispositivo o sistema o el acceso a los mismos. El "secuestrador" de los datos solicita un "rescate" de la base de datos mediante el pago de una suma de dinero mediante criptomonedas, generalmente, para liberar la información. Los primeros tipos de ransomware bloqueaban el acceso al equipo de un usuario haciéndoles llegar un supuesto mensaje de agencias de seguridad acusándolos de infligir la ley. Estos se denominaban "ransomware de inicio de sesión" y solo afectaba los archivos de inicio del sistema operativo de las computadoras para impedir su normal funcionamiento. Los argumentos eran el de visitar sitios web de pornografía y descarga de archivos protegidos por los derechos de autor (música, películas, etc.) en este caso información almacenada en los dispositivos no se cifraban mediante técnicas criptográficas, entre otros.

[16] "LA JUSTICIA INTIMÓ AL ENACOM A QUE TOME MEDIDAS PARA EVITAR NUEVOS HACKEOS". Diario "La Nación", 10 de enero de 2023. Disponible en https://www.lanacion.com.ar/politica/la-justicia-intimo-al-enacom-a-que-tome-medidas-para-evitar-nuevos-hackeos-nid10012023/

[17] "PARA FRENAR EL SIM SWAPPING, EL ENACOM LE EXIGE A LAS OPERADORAS IMPLEMENTAR EN 60 DÍAS NUEVOS SISTEMAS DE VALIDACIÓN DE LA IDENTIDAD DE SUS CLIENTES". Diario "La Nación", 16 de marzo de 2023. Disponible en https://www.lanacion.com.ar/tecnologia/para-frenar-el-sim-swapping-el-enacom-le-exige-a-las-operadoras-implementar-en-60-dias-nuevos-nid16032023/

Mensaje extorsivo de ransomware de inicio

Al igual que los ataques de phishing, en un principio las solicitudes eran generales y se utilizaban direcciones de mail que aparecían públicamente en sitios de Internet y se enviaban como SPAM o correo no deseado. En los últimos años se ha segmentado el público y se han ampliado los objetivos de usuarios particulares, empresas y organismos gubernamentales con ataques dirigidos mediante la explotación de vulnerabilidades de los sistemas o campañas de phishing, ya mediante el uso de sistemas de cifrado de datos.

El caso más conocido sobre este tipo de malware es el del emblemático caso del ransomware Wannacry de 2017 por afectar a más de 150 países en todo el mundo. Dicho malware no justamente fue noticia por la filtración de datos privados de las organizaciones afectadas sino por la sensibilidad que generó en un comienzo al afectar la información de un hospital de Gran Bretaña, una semana después del ataque al puente de Westminster a metros del Parlamento Británico[18].

[18] "CÓMO SURGIÓ Y SE PROPAGÓ WANNACRY, UNO DE LOS CIBERATAQUES MÁS GRANDES DE LA HISTORIA". Diario Infobae, 12 de mayo de 2018. Disponible en https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/

Ventana emergencia en computadoras con Windows XP del ransomware WannaCry

Meses antes de que la Organización Mundial de la Salud decretara la Pandemia del COVID-19, los atacantes comenzaron a realizar copias de información en forma remota antes de encriptar la información para luego amenazar a la organización víctima con hacerla pública en Internet en caso de no pagar el rescate, lo que constituye una doble extorsión. Asimismo, aumentaron los ataques mediante la explotación de vulnerabilidades de los sistemas[19] y a los empleados de las organizaciones que se conectaban a las redes corporativas a partir de la expansión del trabajo remoto para tratar de obtener las credenciales de acceso de las organizaciones mediante ataques de fuerza bruta. Se denomina ataque de fuerza bruta a los intentos establecidos por una persona no autorizada de probar diferentes combinaciones de claves en para ingresar a un sistema informáticos. La misma puede realizarse en forma manual o a través de programas informáticos.

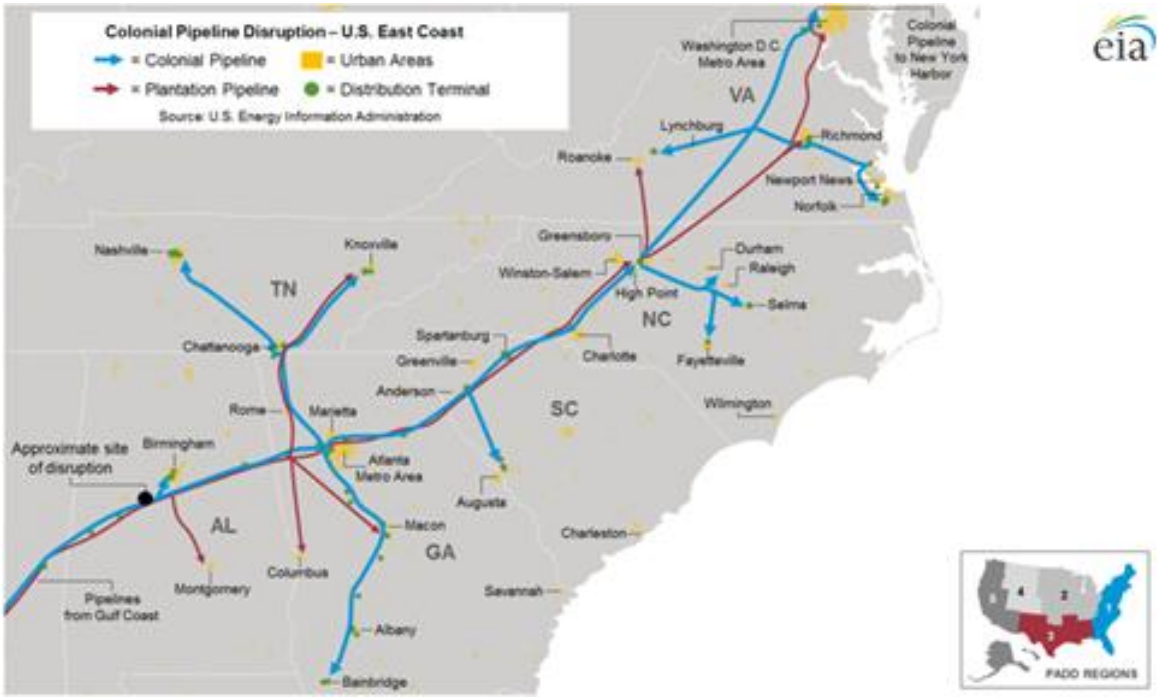
[19] Una vulneración de seguridad es cualquier incidente que da lugar al acceso no autorizado a datos, aplicaciones, redes o dispositivos informáticos. Es una debilidad que presenta un sistema y permite al acceso no autorizado a la información. Por lo general, ocurre cuando un intruso logra burlar los mecanismos de seguridad.

Por otro lado, se incrementó la cantidad de sitios donde se ofrece del ransomware como servicio por parte de hackers maliciosos en la Internet oscura o Dark Web[20]. El modelo de negocios de ransomware como servicio (RaaS, por sus siglas en inglés) incluye la descarga del software malicioso, soporte, la venta de vulnerabilidades Zero Day y la venta de credenciales robadas en mercados negros en línea. Es así como durante el transcurso de la pandemia se produjo un notable incremento de estos ataques a nivel de organizaciones que tuvieron como objetivo fundamentalmente al sector privado, donde los blancos principales fueron grandes empresas, fundamentalmente por la capacidad adquisitiva para pagar las millonarias sumas demandadas.

Otra característica que se dio durante la pandemia a nivel global fue el incremento de ataques de ransomware a infraestructuras críticas de información[21]. Un ataque de ransomware afectó a la empresa de transporte de petróleo y gas de los Estados Unidos "Colonial Pipeline", produciendo demoras en los servicios a toda la Costa Este de ese país durante casi una semana. De manera preventiva, la firma decidió suspender la provisión de ambos insumos desde la ciudad de Houston hasta New York que ante la posibilidad de que los ciberdelincuentes dañaran físicamente el oleducto.

[20] La Dark Web consta de una serie de sitios web no públicos, -no localizados por los motores de búsqueda- para mantenerlos inaccesibles, para su uso se requiere de un navegador específico (Navegador TOR, The Onion Router) y el uso de redes distribuidas descentralizadas (Cadena de Bloques o Blockchain). El objetivo de mantener la privacidad de las comunicaciones y el anonimato de sus usuarios.

[21] Las infraestructuras críticas de información son sistemas y redes informáticas que hacen a la operatividad y suministro de servicios esenciales para las personas, por ejemplo, el sector bancario, el energético, la provisión de combustible, los medios de trasporte, el gas, etc.



Mapa de zonas geográficas donde se vio afectada la provisión de combustible mediante el ataque a la empresa Colonial Pipeline de Estados Unidos.

Si bien el ataque solo comprometió información corporativa sensible, la empresa pagó 5 millones de dólares para la liberación -o no publicación- de la información cifrada. Para la Agencia Federal de Investigación de los Estados Unidos (FBI) se trató de un grupo organizado que produjo el ataque a partir de una vulnerabilidad del sistema de energía. La empresa reconoció haber pagado el rescate de los archivos por motivos aun no esclarecidos, pese a las recomendaciones habituales de no efectivizar el pago por parte de los especialistas[22].

4.4. Blanqueo ilícito de capitales por Internet

El blanqueo ilícito de capitales consiste en legitimar fondos provenientes de actividades ilegales, comúnmente conocido "lavado de dinero". Es un delito difícil de descubrir a partir del uso de testaferros o "prestanombres" y la realización de operaciones por debajo del umbral permitido por las autoridades de control financiero establecida por

[22] "COLONIAL PIPELINE: EN ESTADOS UNIDOS PAGAN US$ 5 MILLONES A HACKERS PARA VOLVER A TENER COMBUSTIBLE". Diario Clarín, 13 de mayo de 2021. Disponible en https://www.clarin.com/mundo/colonial-pipeline-unidos-pagan-us-5-millones-hackers-volver-tener-combustible_0_9T02sX1zs.html

el Grupo de Acción Financiera Internacional (GAFI)[23], esta última conocida como "técnica de smurfing.

A partir del surgimiento de la Internet comercial a mediados de la década de 1990, *la nueva economía digital* ofrece una serie de servicios económico-financieros mediados por tecnologías de la información y la comunicación en Internet tales como la compraventa de bienes y servicios, el desarrollo de servicios de pago electrónico, las transferencias de fondos en línea y el uso de servicios bancarios en forma electrónica, entre otros. En los últimos años se produjo el surgimiento de bancos digitales en Argentina, de existencia únicamente en ciberespacio, sin sedes físicas. A diferencia de los bancos tradicionales donde la apertura de una cuenta bancaria es de forma personalizada, las mismas permiten comenzar a operar mediante métodos digitales de acreditación de identidad en forma remota[24].

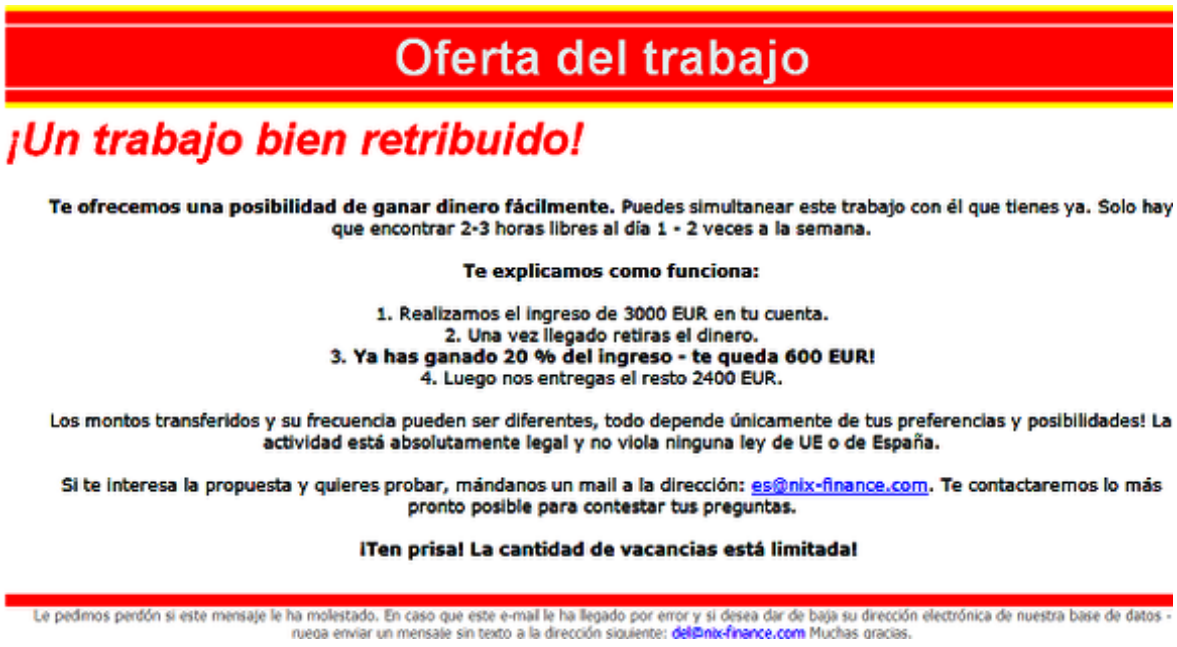
Durante la pandemia se han incrementado los intentos de apertura de cuentas bancarias en bancos digitales mediante la sustitución de identidad, tanto así como la apertura de varias cuentas por cliente utilizadas para legitimar fondos ilícitos provenientes de los fraudes y estafas en línea. Para los casos de ransomware, los atacantes utilizan como método de pago de rescate las criptomonedas, que operan por fuera del sistema financiero tradicional, pero para los casos de transferencia de fondos de un sistema de homebanking por parte de un phishers se necesitan cuentas bancarias convencionales.

Una de las formas de obtener estas cuentas es mediante *fraudes de empleo por Internet***.** En este caso, tras el ofrecimiento formal de formar parte de una empresa, se solicita a la víctima autorización para ingresar fondos a su cuenta bancaria como parte de los movimientos financieros de la firma. Una vez realizado el depósito, se le solicita al "empleado" entregarla a un "corresponsal" de la firma. Así, en la operatoria ilícita, el único registro final electrónico es la cuenta bancaria de la víctima, lo que en este caso está oficiando como se conoce en la jerga como "mula".

---

[23] El Grupo de Acción Financiera Internacional (GAFI o FATF, por su sigla en inglés) es una organización intergubernamental creada en 1989 por los países integrantes del G-7, que fija los estándares internacionales y promueve la efectiva implementación de políticas, medidas legales, regulatorias y operativas para prevenir y combatir el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva, así como también otras amenazas relacionadas con la integridad del sistema financiero internacional, la seguridad y la paz mundiales.

[24] "BILLETERA DIGITAL: USUARIOS PODRÁN HACER PAGOS Y TRANSFERENCIAS DESDE CUENTAS BANCARIAS". Sección "Actualidad" del sitio Web de la Editorial ERREIUS, 20 de mayo de 2022. Disponible en https://www.erreius.com/actualidad/10/comercial-empresarial-y-del-consumidor/Nota/1617/billetera-digital-usuarios-podran-hacer-pagos-y-transferencias-desde-cuentas-bancarias



Oferta del trabajo

¡Un trabajo bien retribuido!

Te ofrecemos una posibilidad de ganar dinero fácilmente. Puedes simultanear este trabajo con él que tienes ya. Solo hay que encontrar 2-3 horas libres al día 1 - 2 veces a la semana.

Te explicamos como funciona:

1. Realizamos el ingreso de 3000 EUR en tu cuenta.
2. Una vez llegado retiras el dinero.
3. **Ya has ganado 20 % del ingreso - te queda 600 EUR!**
4. Luego nos entregas el resto 2400 EUR.

Los montos transferidos y su frecuencia pueden ser diferentes, todo depende únicamente de tus preferencias y posibilidades! La actividad está absolutamente legal y no viola ninguna ley de UE o de España.

Si te interesa la propuesta y quieres probar, mándanos un mail a la dirección: es@nix-finance.com. Te contactaremos lo más pronto posible para contestar tus preguntas.

¡Ten prisa! La cantidad de vacancias está limitada!

Le pedimos perdón si este mensaje le ha molestado. En caso que este e-mail le ha llegado por error y si desea dar de baja su dirección electrónica de nuestra base de datos - ruega enviar un mensaje sin texto a la dirección siguiente: del@nix-finance.com Muchas gracias.

4.5. Otras modalidades:

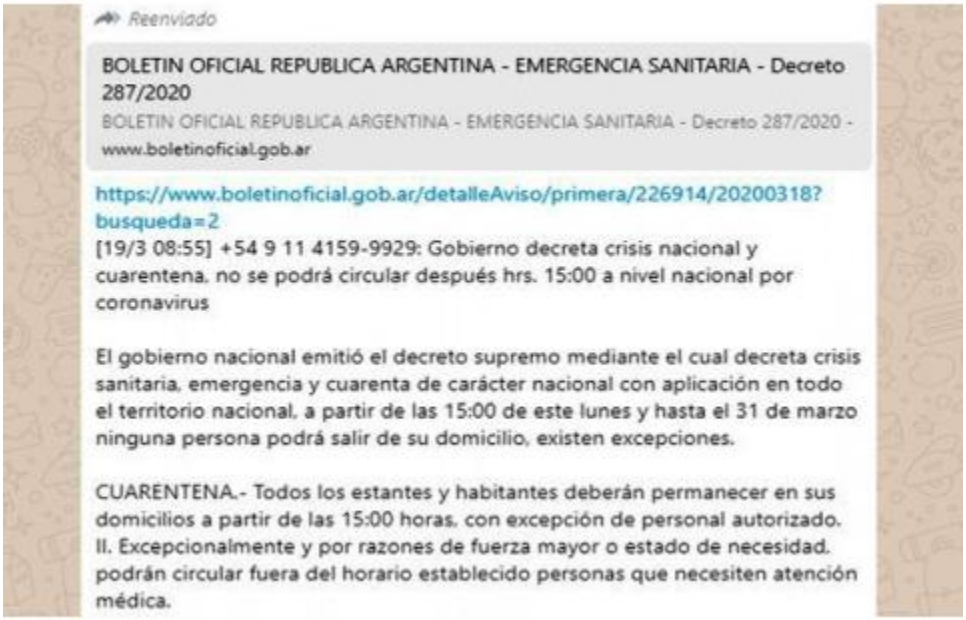
Ataque de denegación de servicio indirecto

Durante la pandemia se produjo también un notable incremento de distribución de noticias falsas, un tema de debate en los últimos años a partir de caso Cambridge Analytica y la supuesta distribución durante la campaña electoral para la presidencia de los Estados Unidos de 2016[25]. Si bien las mismas no representa un delito, en Argentina, días previos al ASPO decretado por el gobierno, se montó una campaña de desinformación a través de mensajes de WhatsApp donde su finalidad no era establecer confundir a la opinión pública sino atacar un servicio público brindado por el gobierno nacional; el Boletín Oficial de la República Argentina (BO).

El contenido de dichas noticias -que se viralizaron por redes sociales, sistemas de mensajería instantánea y sitios web- remitían a supuestas comunicaciones oficiales relacionadas con el virus COVID-19; personas "beneficiadas" para realizar teletrabajo, otorgamiento de subsidios varios, excepciones impositivas para sectores productivos y un supuesto colapso de Internet a nivel nacional, entre otros motivos. Los mensajes

[25] "5 CLAVES PARA ENTENDER EL ESCÁNDALO DE CAMBRIGDE ANALYTICA QUE HIZO QUE FACEBOOK PERDIERA US37.000 MILLONES EN UN DÍA". Sitio Web de la BBC de Londres, 20 de marzo de 2018. Disponible en https://www.bbc.com/mundo/noticias-43472797

contenían el enlace web verdadero al sitio del Boletín Oficial. Obviamente tal normativa no existía y el objetivo era saturar o hacer caer el servidor del sitio oficial de los actos de gobierno a modo de ataque de denegación de servicio indirecto. Un ataque de denegación de servicio se realiza habitualmente a través de botnets, redes de dispositivos que realizan tareas programadas como por ejemplo, dirigir solicitudes de acceso al mismo tiempo a un servidor que aloja un sitio web, con el fin de saturarlo, ralentizar su funcionamiento o producir la caída del servicio.



Noticia falsa enviada por WhatsApp sobre un supuesto decreto presidencial sobre la emergencia sanitaria por la pandemia del COVID-19

Observaciones generales

En términos estadísticos, existe un incremento del 20% entre el total de denuncias ingresadas en 2020 y 2021 a nivel país (de 9.604 a 11.593 en el trascurso de 12 meses). Es un aumento significativo pese a la amplia cifra oculta que poseen este tipo de conductas. Más de la mitad de las causas iniciadas tienen como epicentro a la provincia de Buenos Aires, donde en 2020 representa poco más de la mitad de ingresos a nivel nacional (57%), 5.540 denuncias por sobre 9.604- y en 2021 también traspasa ese umbral (53%), 6.700 ingresos por sobre un total de 12.593-. Resulta significativa la cantidad de denuncias sobre delitos informáticos que recibe un distrito como la Provincia de Tierra del Fuego[26], ocupando el segundo lugar tanto en el año 2020 con 1.449 denuncias como en el 2021, con 1.900 causas iniciadas. Si bien la estadística es un dato frio, esto puede deberse a los mecanismos de registro de las oficinas encargadas de recepcionar la cantidad de denuncias de este tipo de ilícitos o, lisa y llanamente a un incremento exponencial de ingresos durante pandemia que supera la media de cualquier provincia en cuanto a cantidad de habitantes. Amerita ampliar esta cuestión en futuros estudios estadísticos de este tipo. En cuanto al tercer y cuarto puesto, las provincias de Santa Fe y Mendoza alternan en ambos años en esas posiciones con porcentajes mucho menores que las provincias de Buenos y Tierra del Fuego, con 640 denuncias en 2020 para la provincia del centro (7% del total) y 803 en 2021 (6%), mientras que el distrito cuyano registró 407 ingresos en 2020 (4% del total) y 1.194 en 2021 (9%). Resulta llamativo que la Provincia de Córdoba registre un porcentaje bajo de denuncias en comparación del resto de jurisdicciones, siendo el segundo distrito con mayor cantidad de habitantes del país detrás de la Provincia de Buenos Aires[27]. En el año 2020 registró únicamente 258 denuncias y en 2021 305.

En términos de figuras delictivas, al igual que los resultados de los primeros muestreos anuales realizados por la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal entre los años 2013 y 2017, las figuras más denunciadas están relacionadas con los delitos contra la integridad sexual de niños, niñas y adolescentes. Las figuras con más índice de ingresos penales refieren al art. 128 del Código Penal de la Nación, la Tenencia, distribución y publicación de imágenes de abuso sexual de niños, niñas y adolescentes y el art. 131 de Grooming, respectivamente concentrando el 65% del total de denuncias durante 2020 en todo el país ambos delitos y casi el mismo

[26] Según datos del Censo 2022 del Instituto Nacional de Estadísticas y Censos (INDEC) la Provincia de Tierra del Fuego registra 190.641 habitantes.

[27] Según datos del Censo 2022 del Instituto Nacional de Estadísticas y Censos (INDEC) la Provincia de Córdoba registra 3.978.904 habitantes, siendo el segundo distrito más importante de la República Argentina, detrás de la Provincia de Buenos Aires, que posee 17.569.053 habitantes.

porcentaje al año siguiente, 66% en 2021. Entre ambas, el ciberdelito que registra mayor cantidad de ingresos es el art. 128, representando el 46% del total país en 2020 (4.446 registros por sobre 9.604) y un 36% al año siguiente (4.526 denuncias por sobre 1.293 en 2021). Ambas figuras -a diferencia del resto de las contempladas en la Ley N° 26.388 de delitos informáticos y la Ley N° 26.904 de Grooming afectan directamente a la seguridad de las personas, específicamente a una parte de la población en situación de vulnerabilidad como lo son los niños, niñas y adolescentes, en términos de su integridad física y psicológica en tanto se trata de delitos contra la integridad sexual. El resto de los ciberdelitos incorporados a nuestro código por estas normativas protegen a los dispositivos, redes y sistemas informáticos y a los datos e información que almacenan, trasmiten o procesa como bienes jurídicos.

En términos de distritos, la mayoría de las provincias mantienen esta proporción, con excepciones destacables. Tanto en la Provincia de Buenos Aires como la Ciudad Autónoma de Buenos Aires durante 2020 los delitos más denunciados mantienen correlación con la tendencia nacional, a saber, en primer lugar, la Tenencia, distribución y publicación de imágenes de abuso sexual de niños, niñas y adolescentes y en segundo lugar la figura de Grooming. Pero en ambos distritos, al año siguiente; las estafas informáticas pasaron al segundo lugar en orden de importancia, registrando más casos que el Grooming. En CABA, la cantidad de denuncias por esta figura representó el 17% del total (27 casos por sobre 157 totales), mientras que en PBA el porcentaje es mayor, más de un cuarto del total de ingresos (28%), 1.909 ingresos por sobre un total de 6.700- durante ese año. Esto puede ser producto de la aparición de bandas abocadas a los fraudes y estafas en línea en los últimos años del país, pero también por un requisito que comenzaron a implementar diferentes organizaciones en pandemia –como por ejemplo los bancos- de solicitar la denuncia judicial antes de comenzar el reclamo administrativo. Previo a pandemia, este requisito no era común, ya que los casos de phishing bancario no representaban una cantidad significativa para la economía de estas instituciones, para lo cual la mayoría de las resoluciones eran de tipo administrativas, fundamentalmente mediante el resarcimiento del dinero a la víctima de la estafa, considerada como “fuga de negocios” por las instituciones.

En este sentido, la Provincia de Córdoba demuestra el ejemplo inverso, siendo en el año 2021 la figura de Estafa informática la que registra mayor cantidad de ingresos, dejando en segundo lugar al Grooming y la Tenencia, distribución y publicación de imágenes de abuso sexual de niños, niñas y adolescentes, respectivamente. Durante ese año, 1 de cada 3 ingresos corresponden al artículo 173 inc. 16 del Código Penal de la Nación. La Provincia de Catamarca, al igual que Córdoba, también registra la mayor cantidad de ingresos por Estafas informáticas durante ese mismo año, con el 43% del total de denuncias (22 casos por sobre 55 ingresos). El único distrito que abrió mayor cantidad

de causas relacionadas con esta figura durante ambos años es la Provincia de Río Negro, con un porcentaje del 62% del total en 2020 y el 70% en 2021. Durante el primer año 222 casos por sobre un total de 356 estuvieron relacionados con este ciberdelito, mientras que al año siguiente esta cifra subió a 300, por sobre un total de 427 causas. En retrospectiva, si se analizan los datos volcados en los muestreos sobre denuncias judiciales de delitos informáticos realizados durante los años 2013 y 2017 por la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, las denuncias por Estafas informáticas no representaban un número significativo en cantidad de ingresos en relación a otras figuras de las leyes N° 26.388 y 26.904[28].

Otra figura que ha recibido un incremento significativo de denuncias en los años en cuestión fue el artículo 183 del Código Penal de la Nación: Daño a bienes intangibles y distribución de virus. A nivel país, ocupa el cuarto lugar de relevancia detrás de los delitos contra la integridad sexual de niños, niñas y adolescentes (arts. 128 y 131 del CPN) y la Estafa Informática. En el año 2020 registró 1.806 ingresos por sobre 9.604, lo que representa el 11% del total, mientras que en 2021 aumenta a 1.295 casos, con un porcentaje similar al año anterior en relación al resto de figuras, un 10%, por sobre un total de 12.593 registros. Podemos suponer que esto puede deberse a denuncias realizadas por organizaciones más que usuarios particulares en función de la aparición de bandas organizadas en los últimos años que realizan principalmente ataques de ransomware, aunque se necesita un análisis más específico para realizar una afirmación de este tipo. Si bien como se señaló a lo largo del informe, las organizaciones intentan resolver estos ciberdelitos en términos de incidentes de seguridad informáticos como un problema interno, el incremento de ciberataques y la amenaza de hacer pública esta información institucional por parte de lo/as ciberdelincuentes mediante extorsión, ha cambiado la lógica en este sentido, apelando a la denuncia judicial.

A nivel distrital, el Daño a bienes intangibles y distribución de virus varía en cuanto a la cantidad de denuncias, a diferencia de lo que sucede con los Artículos 128 y 131 de nuestro Código, que mantiene una tendencia similar a nivel nacional. Cabe destacar los dos casos más paradigmáticos en relación a esta figura, representado por las dos provincias más australes del país, a saber, Santa Cruz y Tierra del Fuego. La particularidad que presentan a diferencia del resto del país es que el Artículo 183 fue el que más denuncias recibió durante los años 2020 y 2021 en ambos distritos. En la provincia de Santa Cruz, 53 de 66 denuncias refieren a esta figura durante el 2020 –el 80% del total- mientas que, en 2021, ascendió a 65, representado un 69% de ingresos en ese período. En cuanto a la Provincia de Tierra del Fuego durante el 2020, el 65% de

[28] Ver informes anteriores de la **"Colección de Estudios Estadísticos sobre Cibercrimen"** en el Sistema Argentino de Informática Jurídica en http://www.bibliotecadigital.gob.ar/

los ingresos corresponden a este delito, con 933 causas de un total de 1.449, mientras que, en 2021, el 56% de denuncias estuvieron relacionadas con esta figura con 1.071 casos sobre 1.930.

Por último, cabe destacar la estadística que presenta durante el año 2021 la Provincia de Entre Ríos, donde la mayoría de denuncias recibidas durante ese período (82%) refieren al artículo 255 del Código Penal de la Nación, a saber: Alteración de evidencia informática. Si bien, en comparación de otras jurisdicciones la cantidad de denuncias totales durante ese año fueron pocas (33 causas tramitadas), 27 casos estuvieron relacionadas con este ciberdelito que explica la pérdida, contaminación o alteración dolosa de pruebas informáticas en el marco de una causa judicial o una caratulación errónea de un hecho bajo esta figura, en este caso cuando se pierden elementos probatorios varios en el curso de una investigación .

ANEXO I

Fuentes de Información estadística

- Secretaría de Innovación del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.
- Ministerio Público de la Provincia de Buenos Aires
- Secretaría de Planificación de la Suprema Corte de Justicia de la Provincia de Buenos Aires.
- Tribunal Superior de Justicia del Poder Judicial de la Provincia de Córdoba
- Ministerio Público de la Acusación de la Provincia de Santa Fe
- Ministerio Público Fiscal de la Provincia de Mendoza
- Poder Judicial de la Provincia de Salta.
- Corte Suprema de Justicia de la Provincia de Tucumán
- Poder Judicial de la Provincia de Formosa
- Poder Judicial de la Provincia de Misiones
- Poder Judicial de la Provincia de Santiago del Estero
- Ministerio Público del Poder Judicial de la Provincia de Catamarca
- Poder Judicial de la Provincia de La Rioja
- Poder Judicial de la Provincia de San Luis
- Poder Judicial de la Provincia de Corrientes
- Superior Tribunal de Justicia de la Provincia de Entre Ríos

- Poder Judicial de la Provincia de La Pampa
- Poder Judicial de la Provincia de Neuquén
- Poder Judicial de la Provincia de Río Negro
- Superior Tribunal de Justicia de la Provincia de Chubut
- Superior Tribunal de Justicia de la Provincia de Santa Cruz
- Superior Tribunal de Justicia de la Provincia de Tierra del Fuego
- Secretaría de Coordinación Institucional del Ministerio Público Fiscal de la Ciudad de Buenos Aires

ANEXO II

Fuentes de Información del Dossier

Observatorio de prensa sobre ciberdelito de la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal del Ministerio de Justicia y Derechos Humanos de la Nación.

Sain, Gustavo: "NUEVAS MODALIDADES DE DELICTIVAS EN MATERIA DE CIBERCRIMEN DURANTE LA PANDEMIA DEL COVID-19". En ***Revista Temas de Derecho Penal y Procesal Penal***. Buenos Aires, ERREIUS, Vol. 12, Diciembre de 2021.

Dirección Nacional de Ciberseguridad de Jefatura de Gabinete de Ministros de la Nación: ***Delitos informáticos en Argentina: Modalidades detectadas durante la Pandemia del COVID-19: Recomendaciones preventivas para los ciudadanos.*** Publicado en Junio de 2022.

Agradecimientos

- ✓ Al Dr. Mario Adaro, Ministro de la Corte de Justicia del Poder Judicial de la Provincia de Mendoza.

- ✓ Al Dr. Alejandro Gullé, Procurador de la Suprema Corte de Justicia del Poder Judicial de la Provincia de Mendoza.

- ✓ A la Dra. Brenda Eldrid, Especialista en Derecho Informático.