2.019

# LA IMPUNIDAD DE LOS DELITOS CIBERECONÓMICOS, ESTÁ ÍNTIMAMENTE RELACIONADA CON LA FALTA DE CAPACITACIÓN DE LOS OPERADORES INVESTIGATIVOS


ANDREA DANIELA ALE

Abril, 2.019

# LA IMPUNIDAD DE LOS DELITOS CIBERECONÓMICOS ESTÁ ÍNTIMAMENTE RELACIONADA CON LA FALTA DE CAPACITACIÓN DE LOS OPERADORES INVESTIGATIVOS"

**ANDREA DANIELA ALE**

**UNIVERSIDAD CATÓLICA DE SALTA**

**FACULTAD DE CIENCIAS JURÍDICAS**

**LICENCIATURA EN SEGURIDAD PÚBLICA**

**SALTA, 2.019**

## AUTORIDADES

**Gran Canciller**

S.E.R. Monseñor MARIO ANTONIO CARGNELLO Arzobispado de Salta

**Rector**

Ing. RODOLFO GALLO CORNEJO

**Vicerrectora Académica**

Mg. CONSTANZA DIEDRICH

**Vicerrector Administrativo**

Dr. DARIO EUGENIO ARIAS

**Vicerrector de Formación**

Pbro. Dr. CRISTIAN ARNALDO GALLARDO

**Vicerrector de Investigaciones y Desarrollo**

Dr. FEDERICO COLOMBO SPERONI

**Director General del Sistema de Educación a Distancia**

Ing. Lic. DANIEL TORREZ JIMENEZ

**Secretaria General**

Lic. SILVIA ALVAREZ

**Decano de la Facultad de Ciencias Jurídicas**

Dr. EDUARDO JESÚS ROMANI

**Secretario Académico de la Facultad de Ciencias Jurídicas**

Dra. MARÍA PÍA MORENO

**Jefe de Carrera de la Licenciatura en Seguridad**

Lic. HUMBERTO SALVADOR LESCANO

## DEDICATORIA:

El presente trabajo deseo dedicarlo principalmente a mi familia, integrada por mi marido MIGUEL y mis dos pequeños hijos, CANDELA y MÁXIMO de 8 y 6 años de edad, respectivamente; quienes son el motor de mi vida y quienes diariamente en forma paciente me han brindado su apoyo incondicional para poder concretar este gran logro y poder culminar mi carrera universitaria.

En cuanto a mi marido, con su ayuda he logrado sortear obstáculos y trabas propios del vivir cotidiano y laboral, que pudieran dificultar la continuidad de mis estudios, brindándome su apoyo y comprensión para poder aprobar cada materia; además de la realización e investigación de este trabajo integrador final.

A mis niños, que con su corta edad, supieron vislumbrar y sacrificar horas destinadas a compartir en familia y juegos; entendiendo únicamente con sus palabras que "… *mamá debía estudiar e ir a la escuela*…"; siendo esto suficiente para nutrirme de amor y alegría en tan sencillas y sabias palabras que llenaron mi corazón de ganas de seguir adelante hasta alcanzar mi mayor logro y poder recibirme.

A ellos tres… está dedicado mi presente trabajo.

## AGRADECIMIENTOS:

En primer lugar, mi más profundo, sincero y eterno agradecimiento es hacia mi familia, quienes son los que diariamente me han acompañado para concretar este anhelo, rescindiendo días de haber podido compartirlos en familia, con la finalidad de alcanzar este resultado favorable y esperado que me permitirá tener un mejor desempeño en mi vida personal y profesional.

Seguidamente, a los docentes en general pero especialmente a quienes por circunstancias laborales he tenido el honor de compartir en distintas ocasiones y de conocerlos no solo como capacitadores sino también como colegas y personas.

Por último, a la prestigiosa Institución a la cual pertenezco, Policía de la Provincia de Salta, que a través de quien dirige la misma me ha dado la oportunidad de poder crecer personal y profesionalmente, al darme la posibilidad de capacitarme y adquirir nuevos conocimientos que reflejaré durante el desempeño de mi carrera policial tendiente a brindar un servicio eficiente y de excelencia hacia la comunidad.

Correspondencia Gral. N° 706

**FACULTAD DE CIENCIAS JURÍDICAS**

**RESOLUCION Nº 002/17**
**CARRERA LICENCIATURA EN SEGURIDAD**
**MODALIDAD A DISTANCIA**

En Campo Castañares, sito en la Ciudad de Salta, Capital de la Provincia del mismo nombre, República Argentina, sede de la Universidad Católica de Salta, a los tres días del mes de febrero del año dos mil diecisiete.

**VISTO:**

La nota presentada por la alumna **ALE, ANDREA DANIELA**, DNI 28251251, de la U.G. 03 Salta, en la que solicita aprobación de Tema y Director de Trabajo Final Integrador; y

**CONSIDERANDO:**

Que, lo solicitado encuadra en los requisitos establecidos en el Reglamento de Trabajo Final Integrador de la carrera de Licenciatura en Seguridad, aprobado por Resoluciones Rectorales 797/2008 y 1029/2011.
Que, el tema objeto de Trabajo Final Integrador: **"La impunidad de los delitos cibereconómicos, está intimamente relacionado con la falta de capacitación de los operadores investigativos"** se fundamenta en que se está gestando una reforma en el Código Penal de la Nación para disminuir las penas en los delitos económicos y considerar únicamente como fraude informático cuando se procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro, aunque en la realidad siempre media un ardid o engaño que hace vulnerable a la víctima. Que tiene como objetivos generales determinar los hechos considerados fraudes cibereconómicos y la manera como afectarían a la víctima; establecer los procedimientos de investigación y evaluar la actuación de las fuerzas policiales en materia de prevención de estos delitos. Asimismo los objetivos específicos se ajustan a la temática propuesta.

Que, de conformidad al análisis realizado del tema y consideración del Currículum Vitae del Director presentado, Dr. **RICARDO RAFAEL TORANZOS**, DNI 16899382, docente de esta Casa de Altos Estudios, corresponde acceder a lo peticionado;

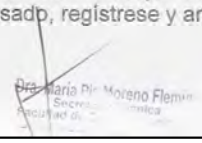
Por ello:

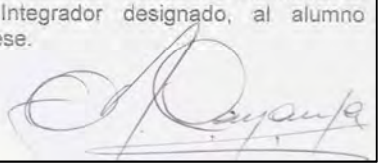
**EL SEÑOR DECANO DE LA FACULTAD DE CIENCIAS JURÍDICAS DE LA UNIVERSIDAD CATOLICA DE SALTA**

**R E S U E L V E**

**Artículo 1°:** Aprobar el Tema: **"La impunidad de los delitos cibereconómicos, está intimamente relacionado con la falta de capacitación de los operadores investigativos"** presentado por la alumna **ALE, ANDREA DANIELA**, DNI 28251251, de la U.G. 03 Salta, y la Dirección del Trabajo Final Integrador a cargo del Dr. **RICARDO RAFAEL TORANZOS**, DNI 16899382.

**Artículo 2°:** Comuníquese a Secretaría General, Dirección de Alumnos, al Director de Trabajo Final Integrador designado, al alumno interesado, registrese y archívese.





# ÍNDICE TABLA DE CONTENIDOS

## RESUMEN

Este trabajo fundamenta la necesidad existencial y empírica de capacitar y perfeccionar a los agentes encargados de investigar delitos de seguridad informática-económica. Los antecedentes determinan que quienes que se dedican a delinquir mediante elementos informáticos, tecnológicos y/o telemáticos, demuestran un amplio manejo de estas herramientas, sumado a los recursos logísticos que implementan. La hipótesis plantea que los operadores a cargo de la investigación no están en condiciones de brindar una respuesta eficiente y en corto plazo al ciudadano que ha sufrido un perjuicio de ésta índole; como consecuencia de la falta de instrucción que poseen, iniciada desde la recepción de denuncia hasta el desconocimiento de métodos en materia de delitos cibereconómicos que le permitan individualizar a los autores. Al respecto, se han realizado encuestas anónimas que evidencian el desconocimiento acerca de la existencia de un área dedica exclusivamente a éste tipo de investigación.

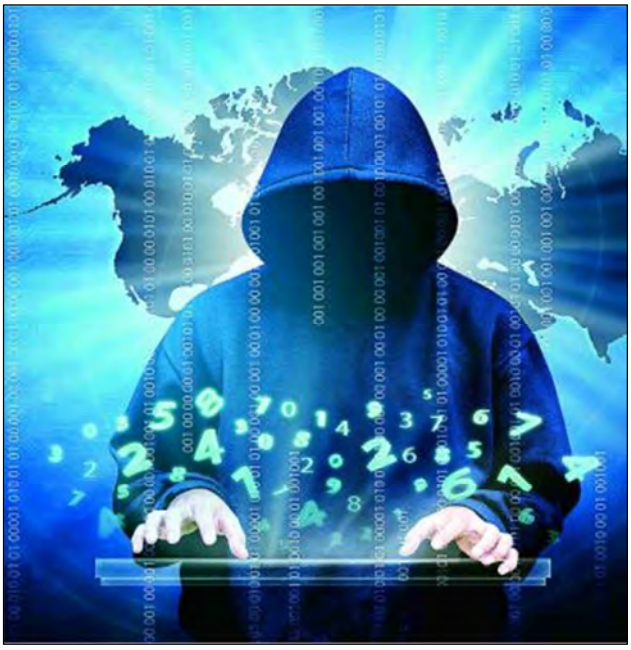
## PALABRAS CLAVES:

- Fraude.
- Cibereconómicos.
- Ciberdelitos.
- Phishing.
- Vishing
- Smishing.
- Pharming.
- Skimming.

# PRIMERA PARTE

## Parte General

## Introducción



En la actualidad, tanto la tecnología como la informática, han generado un proceso mundial de transformaciones sociales, comunicacionales, culturales y económicas entre distintos países del mundo y por ende en cada persona, independientemente del grado de instrucción o clase social a la cual pertenezca; por ello, no debe dejar de considerarse que existen agentes en distintos organismos que brindan un servicio a la comunidad y que no están vinculados al uso del internet, redes sociales y mucho menos, respecto a la existencia de los delitos informáticos y/o ciberdelitos. Por tal motivo, quienes están a cargo de las investigaciones de ésta clase, deben conocer las herramientas necesarias que les permitan esclarecer ilícitos y crear políticas de prevención dirigidas a la comunidad en general.

A dicha problemática e hipótesis presentada, considero particularmente, que el actor que delinque en esta modalidad, tiene además a favor, la existencia de vacíos legales y la inexistencia de antecedentes por sentencias condenatorias ejemplificativas; lo cual es socialmente necesario, ya que a veces las víctimas elegidas son muy vulnerables, como es el caso de los adultos mayores o personas con capacidades

diferentes o quienes carezcan de instrucción, y necesitan sentir la protección legal del sistema judicial, que garantice los derechos de los ciudadanos. No debe dejar de mencionarse que en estos casos puede ocurrir que la víctima no se percate nunca del fraude o lo haga luego de un prolongado tiempo, como consecuencia del anonimato que le otorgan este tipo de herramientas a los causantes, lo cual dificulta mayormente la investigación.

De la experiencia laboral propia y de la información recaba, considero que los ciberdelitos que están direccionados a vulnerar los datos personales de la víctima, para su comisión pueden configurarse con algunas de éstas dos conductas, la primera de ellas, es a través del acceso ilícito a un sistema informático o parte de él para disponer de la información que contiene; y en segundo lugar, el mantenimiento en el sistema con la misma finalidad de disponer de su contenido. En ambos casos, el causante no posee autorización para acceder a tal información, vulnerando las medidas de seguridad establecidas para impedirlo, sin necesidad de que éstas sean complejas o no.

Por ello, a través del presente trabajo de investigación, se propone investigar y validar la hipótesis presentada.

**Definición del tema de investigación:**

***"La impunidad de los delitos cibereconómicos relacionada a la falta de capacitación de los operadores investigativos"***

**Objetivos Generales:**

- Determinar los hechos considerados fraudes cibereconómicos y la manera cómo afectarían a la víctima.
- Establecer los procedimientos de investigación para hechos delictivos que por su modalidad y características, sean de específica competencia a este tipo de

fraudes económicos e informáticos.

- Evaluar la actuación de las fuerzas policiales en materia de prevención de fraudes cibereconómicos y delitos informáticos.

**Objetivos Específicos:**

- Realizar un análisis delictual de los tipos de fraudes cibereconómicos más frecuentes en la provincia.
- Instruir a la fuerza policial de la problemática existente en fraudes cibereconómicos y delitos informáticos, a fin de que se prevenga a la sociedad ante el accionar delictivo de este tipo de delitos.
- Aportar al personal investigativo, conocimientos íntegros sobre este tipo de hechos.
- Propiciar mecanismos de investigación tendientes a contrarrestar la comisión de este tipo de ilícitos; y en aquellos casos que hayan sido perpetrados, elaborar herramientas tendientes a su eficiente esclarecimiento.

**Hipótesis:**

La capacitación y actualización de conocimientos respecto a los ilícitos informáticos y económicos, a los operadores a cargo de la investigación, permitirá proyectar protocolos de intervención y procedimentales, tendientes a la recolección de pruebas y al esclarecimiento de los hechos delictivos de forma eficiente y plazos cortos a mediano.

Asimismo, permitirá dar respuestas satisfactorias a las víctimas de este tipo de delitos, procurando la identificación del causante con los medios de pruebas necesarios para ponerlo a disposición de la justicia.

Esto también permitirá que al tener conocimiento acerca de la temática planteada, cuáles son y cómo detectar las actividades ilícitas en materia de fraudes económicos, se podrán crear políticas de prevención y difundirlas a través de los medios masivos de comunicación para alertar y proteger a la sociedad de los delitos informáticos y tecnológicos que causen detrimento económico.

**Desarrollo:**

Considero que primeramente, para continuar con la exposición del presente trabajo, es necesario conocer que son los delitos, a los que podemos definir como a la acción típica, antijurídica, dolosa o culposa y punible.

En cuanto a los delitos informáticos o ciberdelitos, o delitos tecnológicos, debemos definirlos como aquellos que son cometidos a través del uso de elementos tecnológicos o “nuevas tecnologías”.

Estos tipos de delitos, prevé acciones que se cometen mediante un soporte informático o telemático, que atentan contra las libertades, bienes o derechos de las personas.

La variedad de ciberdelitos es extensa, no se trata exclusivamente de un ciberdelincuente que busca y accede a datos que le son ajenos con fines económicos; sino que existen otros que atentan contra la integridad física y/o sexual de la persona, siendo los más conocidos para mencionar al cyberbulling, grooming, phishing, pharming, terrorismo virtual, defraudación por estafas informáticas, etc.

A continuación, se anexa una definición de los DELITOS INFORMÁTICOS para mayor ilustración del desarrollo del presente trabajo.

**Delitos Informáticos**

El delito informático implica actividades criminales, que en un principio fueron consideradas como figuras típicas el “robo, hurto, fraudes, falsificaciones, estafas, etc”. Debemos dejar constancia que no hay una definición propia de lo que son los “DELITOS INFORMÁTICOS”, aunque hay varios autores que lo han definido desde un punto de vista amplio como “*cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya que como método, medio o fin y, en ese sentido estricto, el delito informático, es cualquiera acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin”.* (Tobares Catalá, G).

**Antecedentes:**


Al referirnos de una clasificación acerca de los delitos informáticos, podemos mencionar como antecedente al **Convenio sobre ciberdelincuencia**, conocido como "Convenio de Budapest sobre ciberdelincuencia". Es el primer tratado internacional acerca de las infracciones suscitadas por los **delitos informáticos y en internet**; mediante la armonización de leyes, mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Este convenio y su informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa el 08 de noviembre del año 2.001. El 23 de noviembre de 2.001 se abrió la firma de Budapest y entró en vigencia el 1 de julio de 2.004. A partir del 28 de Octubre de 2.010, fueron treinta los estados que firmaron, ratificaron y se adhirieron a la Convención, mientras que otros dieciseis firmaron la Convención, pero no la ratificaron. El 1 de Marzo de 2.006, el **Protocolo Adicional a la Convención sobre el delito cibernético**, entró en vigencia.

Este convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que particularmente trata de las infracciones de derechos de autor, fraude informático, pornografía infantil, delitos de odio y violaciones de seguridad de red; como también una serie de competencias y procedimientos como la búsqueda de las redes informáticas y la interceptación legal.

El principal objetivo de este convenio, es la aplicación de una política penal común tendiente a la protección de la sociedad en contra del cibercrimen, mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional en lo que se refiera a delitos informáticos; como así también de otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.

El convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua, con consentimiento o disponibles al público, y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las partes colaboradoras.

El Convenio se complementa con un Protocolo Adicional que realiza cualquier publicación de la propaganda racista y xenófoba a través de redes informáticas como una ofensa criminal. En la actualidad, el terrorismo cibernético también se estudia en el marco del Convenio.

Éste incluye una lista de delitos que cada estado firmante debe incluir en su legislación propia, tales como la piratería, que incluye la producción, venta o distribución de herramientas de hacking; los delitos relacionados con la pornografía infantil y se expande la responsabilidad penal por la violación de la propiedad intelectual. Por ello, exige a cada estado firmante la implementación de ciertos mecanismos procesales dentro de sus leyes; por ejemplo, que las autoridades

policiales deben tener competencia para obligar a un proveedor de servicios de internet a la monitorización de las actividades de una persona en línea en tiempo real.

Por último, el Convenio obliga a los estados partes a prestar cooperación internacional en la mayor medida posible para las investigaciones y procedimientos relativos a delitos penales vinculados a sistemas y datos informáticos o para la recolección de las pruebas electrónicas de un hecho penal. Las fuerzas de seguridad tendrán que asistir a la policía de otros países participantes para cooperar con sus solicitudes de asistencia mutua.

A pesar del marco jurídico común mencionado, la eliminación de obstáculos jurisdiccionales en materia de competencia de aplicación de la ley de delitos informáticos sin fronteras no puede ser posible, en virtud de las disposiciones sustanciales de los principios constitucionales de cada país parte. *(Por ejemplo, en Estados Unidos, no puede penalizarse todos los delitos relacionados con la pornografía infantil citados en el Convenio, en particular la prohibición de la pornografía infantil virtual, debido al principio de la Primera Enmienda de la libertad de expresión).*

Según el convenio, en lo que se refiere particularmente a la prohibición de la pornografía infantil virtual, incluye todas las imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito; pero en este caso la Corte Suprema de los EE.UU revocó por inconstitucional una disposición de la CPPA, que prohíbe “cualquier representación visual”, que “es, o parece ser, de un menor participando en sexo explícito”. En respuesta del rechazo, el Congreso de EE.UU., aprobó la LEY PROTECT, para modificar la disposición, lo que limita la prohibición a cualquier representación visual, es decir, es “indistinguible un menor participando en una conducta sexualmente explícita”.

En lo que se refiere al citado convenio y la Argentina, en el año 2.008 se sancionó la ley Nº 26.388 que modificó el Código Penal de la Nación y se incorporaron un conjunto de delitos vinculados a la problemática inherente a los delitos informáticos.

En el año 2.010, el Consejo de Europa invitó formalmente a Argentina a adherirse al Convenio de Budapest; lo que llevó a que fines del año pasado, que la cámara de Senadores diera media sanción para dicha adhesión de nuestro país para el Convenio sobre Ciberdelito, al que ya se sumaron más de 50 países. A través de éste tratado, se busca consensuar las investigaciones de los ilícitos informáticos e impulsar la cooperación internacional. Ahora falta, que la Cámara de Diputados refrenda el proyecto legislativo citado, con la finalidad de dar una herramienta a la Justicia para investigar delitos que se cometen a través de la web y mediante el uso de elementos informáticos, tales como son el fraude y estafas informáticas, la publicación y distribución de pornografía infantil, delitos vinculados con la propiedad intelectual, entre otros delitos previstos.

Al aprobarse dicha adhesión, la investigación de los delitos cometidos vía internet, proporcionará a los investigadores y a la justicia la posibilidad de asegurar los contenidos y datos digitales, con la cooperación de otros estados nacionales. Facilitará la obtención de la evidencia digital en las investigaciones de crímenes que requieran obtener prueba alojada en países extranjeros, una situación que es cada vez más común y frecuente en los casos de delincuencia transnacional y delitos complejos. También será útil para la adecuada protección de las garantías individuales de los ciudadanos sospechados en las investigaciones.

De ser viable la aprobación de la cámara baja, esto necesariamente implicará que se reformen los códigos de fondo y de forma, nacionales y provinciales, con la finalidad de regular los medios de pruebas para la obtención de la prueba digital.

Considerando personalmente que también deberán adecuarse de acuerdo a las distintas conductas previstas penales sus respectivos agravantes al cometerse hechos de ésta índole que le permite al causante de alguna forma tener un anonimato a través del uso de los elementos informáticos.

**Clasificación:**

Por el convenio de Budapest se ha definido una clasificación acerca de los delitos cibernéticos previstos en los artículos del 1º al 10º del citado convenio, a saber:

- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de datos.
- Ataques a la integridad del sistema.
- Abuso de los dispositivos.
- Falsificación informática.
- Fraude informático.
- Delitos relacionados con la pornografía infantil.
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Asimismo, se exponen cuestiones de derecho procesal, como la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido.

Por una cuestión de organización y con la finalidad de realizar una ilustración acerca de las figuras penales mayormente conocidas en la sociedad relacionada con

los ciberdelitos, haré una introducción sintética, respecto a los delitos de "CYBERBULLING", "GROOMING" y otros.

**Cyberbulling:**

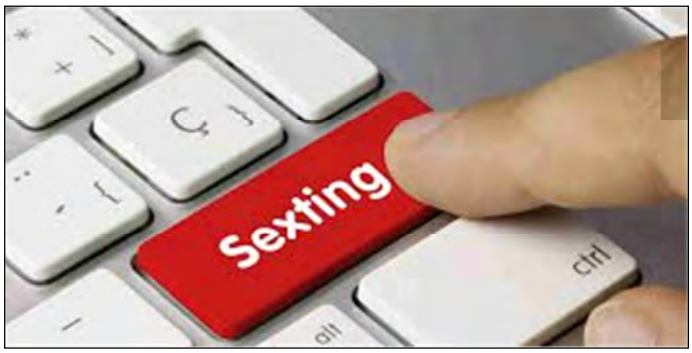
El **CYBERBULLING,** o conocido también como ciberacoso, es el uso de los medios telemáticos, para ejercer el acoso psicológico entre iguales; no limitándose únicamente al acoso de índole estrictamente sexual.

El caso de cyberbulling está previsto cuando un menor de edad atormenta, amenazas, hostiga, humilla o molesta a otro menor mediante internet, teléfono móvil, consolas de juegos u otras tecnologías telemáticas.

**Sexting o revenge porn**

Este delito está estrechamente ligado al ***SEXTING O REVENGE PORN*** (porno vengativo), consistente en el contenido sexual explícito que se publica en internet, sin el consentimiento del individuo que aparece representado. Mucho de este material es producido por la propia víctima y enviado al infractor a través de canales como lo es la aplicación de whatsapp, por ejemplo.

La pornografía vengativa, al someter a la víctima en una situación de exposición no consentida de su sexualidad, se considera como **violencia sexual**, aunque no sea física sino únicamente psicológica.



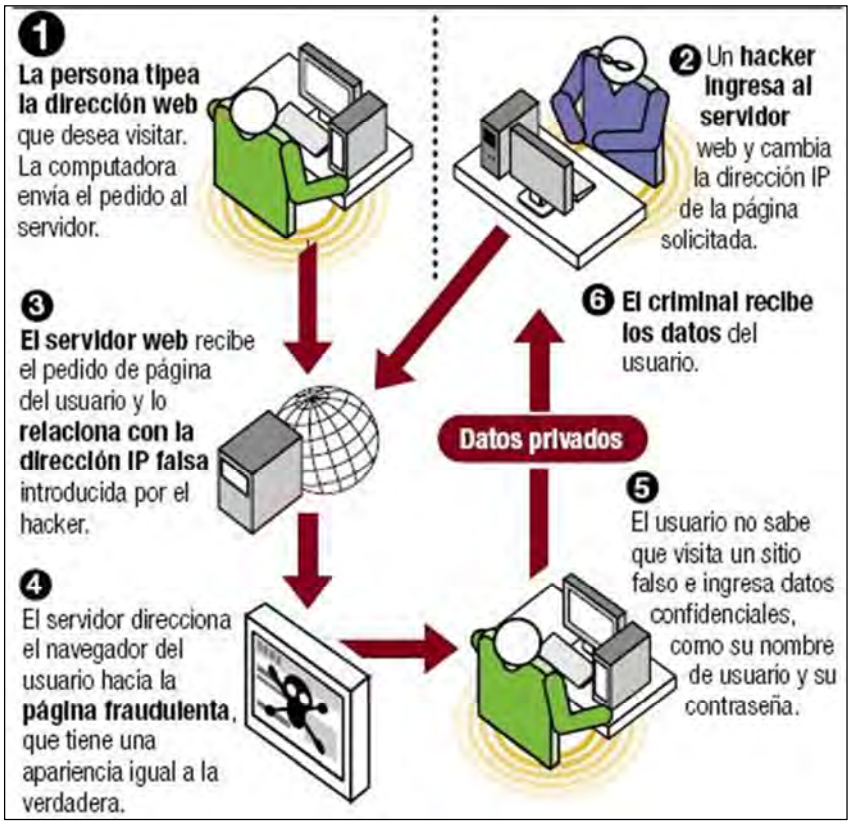

**Grooming:**

El **GROOMING**, se trata de una serie de conductas y acciones emprendidas por un adulto con el objeto de ganarse la confianza de un menor de edad, creando una conexión emocional con el fin de disminuir las inhibiciones del menor y poder abusar sexualmente de él.

En algunos casos el objetivo puede ser buscar la introducción del menor a la prostitución infantil, o a la producción de material pornográfico.


**Pharming*:***

El ***PHARMING*** es la explotación de una vulnerabilidad en el software de los servidores DNS (o en los equipos propios), que permite al atacante redirigir un nombre de dominio a otra computadora distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para el nombre de éste dominio.




**Phishing:**

La figura del ***PHISHING*** o también conocido como “suplantación de identidad”. Es el modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

El ciberdelincuente, conocido como ***phiser***, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.

## SEGUNDA PARTE

**Marco Legal**

## Legislación Argentina

Antes de comenzar a desarrollar puntualmente acerca del tema que nos compete, como es el caso de los “DELITOS CIBERECONÓMICOS”; quisiera hacer referencia a nuestra legislación argentina en lo que se refiere a los Delitos Informáticos, Ley Nº 26.388/08, publicada mediante Boletín Oficial el 25JUN´08.

Esta ley, a través de su artículo Nº 9 incorpora al Artículo Nº 173 el inciso 16 en el Código Penal de la Nación Argentina, figura que prevé la comisión de la estafa mediante el uso de elementos informáticos, estableciendo que: ***“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”.***

Es loable destacar que la Ley de Delitos Informáticos, tiene por objeto incorporar en nuestro Código Penal, normas referidas a las nuevas tecnologías en lo que respecta al manejo de información y de las comunicaciones, circunstancias sobre la cual el aspecto punitivo no podía estar ausente en detrimento de falencias y lagunas legales.

En virtud de ello, genéricamente se hará mención respecto de las modificaciones alcanzadas por la mencionada ley, en razón de la importancia que ha significado la incorporación de la misma y de la previsión en cuanto al uso de elementos informáticos y telemáticos para la comisión de distintas conductas delictivas.

Igualmente no podemos dejar de mencionar que esta ley, también ha realizado modificaciones en lo que se refiere a los delitos en contra de la “integridad sexual”, al haber previsto en el Artículo Nº 128 del Código Penal, la incorporación de fondo de tipos penales que hacen una reformulación de la pornografía infantil.

También lo ha hecho con la sustitución del capítulo III, Título V del Código de Fondo nacional, al prever en lo que se refiere al capítulo de "Violación de Secretos y de la Privacidad", modificación en los artículo Nº 153, 153 bis, 155, 157 y 157 bis.

De igual manera, en lo que se refiere al "Daño Informático", se ha previsto en el Artículo Nº 183, segundo párrafo del CP, que: ***"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".***

Continuando con el mismo título, en el Artículo Nº 184 del Código Penal se ha incorporado el inciso 6, que prevé para el daño cuando: ***"Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de previsión o transporte de energía, de medios de transporte u otro servicio público"****.*

En el capítulo II del Código Penal que prevé entre otros a la protección de las comunicaciones, esta ley ha previsto la modificación del artículo Nº 197, estableciendo que ***"Será reprimido con…el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida."***

El artículo Nº 255 del Código Penal, en lo que respecta al título de "Violación de sellos y documentos", ha previsto con la incorporación de la ley de Delitos Informáticos, que ***"Sera reprimido… 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 custodia de un funcionario público o de otra persona en el interés del servicio público….".***

***Delitos Cibereconómicos:***

A continuación, procederé a desarrollar puntualmente en lo que se refiere a los DELITOS CIBERECONÓMICOS, para lo cual debemos identificar que en este tipo de delitos, el bien jurídico protegido, el cual se trata del patrimonio como el verdaderamente afectado.

Desde el punto de vista objeto, la acción típica, propone que la figura penal se trata de "…. ***él que defraudare a otro***…"; teniendo en cuenta que la defraudación debe contener todas las exigencias propias de cualquier defraudación patrimonial, pero con la incorporación de que ésta se haya cometido mediante la utilización de un mecanismo de manipulación informática como elemento constitutivo del ardid y del consecuente error de la víctima, que será el requisito que la ley prevé al expresar que la conducta delictual será "…***mediante cualquier técnica de manipulación informática…".***

En cuanto al concepto de **"manipulación informática"**, este se corresponde con la conducta de **alterar, modificar u ocultar datos informáticos** de manera que, se realice operaciones de forma incorrecta o que no se lleven a cabo; también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener.

De esta manera, un sujeto pasivo (víctima), puede efectuar instrucciones incorrectas en un programa de manera tal que sin darse cuenta, efectúe transferencia desde la cuenta bancaria propia con todos los ingresos a otra determinada cuenta (del

causante), al haber caído en un ardid fraudulento, por ejemplo, en el conocido caso como “Reparación Histórica de Anses”.

Otro caso, es en cuanto a la manipulación en el ingreso de información a una computadora que se utiliza como base de datos, la cual será ingresada al servidor por medio de un programa adecuado, el cual procederá a ordenarla, clasificarla, realizar operaciones y/o archivarlas. En este caso no se produce un daño, sino que el autor altera la información que ingresa a fin de obtener un beneficio económico para sí o para un tercero. *Por ejemplo, en el caso de que una persona tuviera a cargo el pago de los sueldos de determinada repartición, enviará al banco información falsificada respecto al pago de haberes de ciertos empleados, lo cual no se condice con los recibos de sueldos impresos, direccionando dinero fraudulentamente en beneficio propio o de otro tercero.*

También podemos mencionar, como el caso descripto en el párrafo que antecede, que cuando el autor manipula los datos de la computadora, se puede hacer al menos de dos formas, pudiendo hacerlo al introducir información falsa al ordenador (como en el caso anterior) o, alterando los datos una vez que éstos han sido correctamente introducidos al sistema o bien eliminando información. En ninguno de estos supuestos, se puede hablar de daños ya que la hipótesis se asemeja más a la estafa, en concordancia con otro delito posiblemente, como puede ser la figura de administración infiel, como es el caso del ejemplo presentado.

Como ejemplo de los hechos citados, podemos mencionar un agente bancario que altera el programa de cálculo de intereses de las cuentas de ahorro de manera tal que sólo los dos primeros dígitos de los decimales se toman como intereses y los restantes se transfieren a una cuenta controlada por él. Puede aplicarse también a un programa de redondeo, pensiones, amortizaciones, etcétera.

Otro caso ejemplificativo de manipulación es el de los datos que salen de la computadora, conocido como “Caballo de Troya”. Este caso se da cuando los datos se transfieren a otra computadora, en los programas de impresión (output) o en programas de actualización, o sea, una vez que los datos son ingresados, ordenados y procesados de cálculos elaborados. La elaboración final por lo general, se imprime y almacena. Es posible manipular la información que se imprime y almacena de manera tal que la alteración no puede detectarse, durante el procesamiento de datos. Esta comisión de hechos es la más difícil de detectar, ya que generalmente se realiza en la etapa final del proceso.

Si bien se podría continuar citando otros ejemplos, ya que el abanico de alternativa de posibilidades en cuanto a la manipulación informática va de la mano de la imaginación del agente autor de estas maniobras y de las posibilidades superadoras de la técnica y no solo se reduce a la utilización del ordenador, sino que abarca otros aparatos o sistemas, tales como los cajeros automáticos, es por ello que se adopta los términos ***“mediante cualquier técnica de manipulación informática”***.

Es loable destacar, con respecto a la manipulación informática, que la misma en sí no es típica, sino que lo es aquella que además ha provocado una alteración en el sistema informático o transmisor de datos de la víctima o de un tercero.

Teniendo en cuenta este criterio, se considera que en la redacción del artículo 183 del Código Penal, 2º parte; al expresar ***“…la producción de un daño informático…”***, no sería necesario mencionarlo ya que está implícito al referir ***“…que altere el funcionamiento del sistema informático o de transmisión de datos…”***, que se vincula necesariamente con la misma manipulación y sólo excluye el manejo o la operación que se sirva del medio informático para obtener una ventaja patrimonial indebida, que no modifica su normal programación o funcionamiento.

Hubiera sido suficiente con consignar al respecto para este tipo de defraudación, la que **“fuera cometida mediante cualquier técnica de manipulación informática…”.** Esta situación es criticable puesto que ésta vaguedad e imprecisión de término, al aducir que la manipulación debe derivar en la anormalidad funcional como único supuesto para que opere la norma, genera que la laguna legal de atipicidad que pretendía subsanar seguirá intacta en los casos en que la manipulación consista en el usufructo de fallas o anomalías del sistema preexistente y no provocadas.

Al hacerse referencia a “mediante cualquier técnica de manipulación informática”, se está haciendo alusión en forma abierta a un abanico de posibilidades en lo que respecta a la delincuencia informática o estafa informática, ya que llegado el caso concreto de la defraudación, puede alcanzar a derivaciones y proyecciones inimaginables por parte de autores de éste tipo de delitos, lo que permitirá a la justicia hacer aplicable esta situación a los casos en que el bien jurídico afectado sea el patrimonio, toda vez que sea un hecho defraudatorio mediante el uso de una técnica informática que altere el funcionamiento de un sistema informático o de la transmisión de datos.

De igual manera, debe tenerse en cuenta que esta norma puede ser criticada y por ello tendrá que superar cuestionamientos, tales como lo puede ser desde el punto de vista de la defensa, con el Artículo 18 de la Constitución Nacional, ya que si bien la norma existe será difícil de defender, en virtud de que podrá decirse que si bien la definición citada se ajusta a una conducta defraudatoria; poco se diferencia conceptualmente del delito de hurto del cual pretendía diferenciarse. Esta norma elabora como verbo típico el acto de manipular lo que de por si nada explica, puesto que hace referirse a una actividad prolongada sobre un objeto para la obtención de algún provecho, haciendo mención así al concepto de perjuicio patrimonial derivado de

su calidad de defraudación especial y su ubicación sistemática en el código sustantivo en el capítulo de los delitos contra la propiedad.

Sin embargo, no se entiende porque el legislador insiste en concebir como defraudatorio el acto de apoderarse de manera no evidente de algo ajeno; de manera agazapada o expectante, o con la apariencia de realizar actividades inocuas alrededor de la propiedad ajena para hacerse de la misma ante alguna distracción de su titular.

Por ello, todos los casos que no se puedan comprender dentro de este supuesto de conducta defraudatoria, citada en el párrafo anterior, se encontrarán encuadradas en el supuesto del tipo penal que refiere al "uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática"; ya que la acción estará caracterizada por una manipulación informática fraudulenta como un medio para lograr la disposición patrimonial y dicha conducta tiene correlato con la modalidad de alterar, modificar u ocultar datos informáticos de la tarjeta y/o de los usuarios, de modo que se realicen operaciones en forma no adecuada o que no se lleven a cabo; y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma, un sujeto activo, puede introducir instrucciones incorrectas en el sistema, de manera que no se anote cargos en su cuenta, o la ejecución del pago, transferencia, transacción, etc.; por medio de aparatos electrónicos o computadoras.

**Privacidad de los E-MAILS:**

La ley Nº 26.388/08 de Delitos Informáticos, en su artículo 4º, prevé la sustitución del artículo Nº 153 del Código Penal en lo que respecta a la "***Privacidad de los e-mails***", previendo para ello que: *"Será reprimido…* ***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….”***.

A través de esta modificación se equipara el e-mail y al SMS a la correspondencia epistolar. Esta situación ya ha generado en las empresas un análisis de sus políticas puesto que hasta ahora cualquier empresa podía monitorizar los e-mail de las cuentas corporativas de sus empleados, pero con ésta nueva legislación no puede hacerlo; a menos que aplique una política general a todos los empleados y que mediare un acuerdo pre firmado con cada uno de ellos que autorice esta práctica indicando quien o quienes son los autorizados, forma que se realizara esta práctica y cualquier elemento complementario que asegure que esta tarea no será considerada una violación al artículo 153 del Código Penal.

Lo mismo ocurre en las compañías que prestan servicios de internet y telefonía móvil sobre la política con el personal que tienen acceso a las cuentas de e-mail y a los SMS, que si bien hoy confiamos en que no se leen, en el caso de los e-mails es práctica habitual cuándo el cliente tiene problemas con la cuenta el chequear los e-mail que recibió, en este caso solo salvable con políticas de servicio y confidencialidad muy claras.

**Hacking: acceso no autorizado**

Continuando con las modificaciones previstas por la ley Nº 26.388/08, el artículo 5º dispone la incorporación del Artículo 153 Bis al Código Penal, disponiendo lo siguiente: *"Será reprimido con prisión…, 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… 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.".* En este caso, tiene una pena que queda unida al delito mayor que con ella pueda producirse.

El abanico es muy amplio y el problema reside en como probar quién cometió el delito; además de existir un delito mayor cometido por ese "hackeo" al probar que fue producto del mismo. En resumen debemos decir que se avanzó legislativamente pero como el problema sigue siendo la autenticación de la identidad y la identidad sigue siendo muy fácil de violar, no se verán muchos resultados en este aspecto. También se ha legislado en lo que se refiere a la Protección de datos personales (HABEAS DATA).

**Protección de datos personales (habeas data)**

La Ley Nº 25.326 de protección de Datos Personales había incorporado este artículo cuando fue sancionada el 30 de octubre del año 2.000; el nuevo artículo incorpora a través del artículo Nº 8, previendo que se sustituya el artículo 157 bis del Código Penal estableciendo que "*Será reprimido… 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 otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar*** *por disposición de la ley.*

*3.* ***Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.***

*Cuando el autor sea funcionario público....*

La Ley de Habeas Data, no incluye solo a quién realice estas acciones en entornos informatizados sino también en aquellos casos que el soporte sea manual. El inciso 2 limita a la condición de forma ilegítima el proporcionar o revelar información personal. Es decir que debe probarse que quien lo hizo no estaba autorizado legalmente a hacerlo. Esto pone la carga de prueba en quien denuncia, antes el acusado debía probar que su accionar era legítimo. Por ejemplo, cuando se altere los cupones de una urna para un sorteo.

El inciso 3, se agrega teniendo en cuenta en forma taxativa la incorporación de datos no brindados por el titular de los datos y en forma ilegítima, es decir, que ninguna ley regule que pueda hacerlo. Por ejemplo si un empleado, estudiante o cliente; que no está obligado a dar datos personales que revelan su origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual (art. 2 Ley 25.326 Habeas Data); si alguien insertara en su legajo alguno de estos datos estaría incurriendo en el delito tipificado en este inciso.

Volviendo al tema de los delitos cibereconómicos, la nueva ley se ha extendido a la inclusión de la categoría de estafas o defraudaciones, de modo tal que este perjuicio patrimonial sea ocasionado por la manipulación de los sistemas informáticos o mediante la transmisión de datos cuando se altera su sistema operativo.

La manipulación de sistemas informáticos o de transmisión de datos que se vincula con tarjetas de crédito, débito o de compras, será una modalidad defraudatoria propia del inciso 15º, mientras que toda otra operación no vinculada con tales instrumentos encontrará su adecuación típica en el inciso 16º, ambos del Art. 173 del C.P., cuando se altere el normal funcionamiento del sistema o de la transmisión de sus datos". Aunque no quedan incluidos dentro de este supuesto los casos de ingeniería social, donde el autor con cierta habilidad se hace dar la clave de acceso a un sistema informático, ya sea telefónicamente o mediante phishing, pero este caso queda encuadrado en la figura genérica del artículo 172 del C.P., porque en este caso no hay una manipulación informática destinada a alterar el sistema, sino a un accionar sobre el punto más débil de cadena de seguridad informática, que es el factor humano.

Ya se adelantó que la acción típica se concreta cuando la manipulación informática debe "alterar" el normal funcionamiento de un sistema informático o la transmisión de datos. La manipulación debe alterar el funcionamiento del sistema informático o de telecomunicaciones. No es cualquier manipulación informática, sino sólo la que es apta para producir dicho efecto. Si por un error en la programación ello no sucede, estaremos ante un delito tentado o uno imposible si por la programación del sistema nunca hubiera sido posible realizar la alteración de la forma en que se lo intentaba.

Etimológicamente "alterar", del latín alterare, significa modificar, cambiar la esencia o forma de algo, trastornar, perturbar. Estos conceptos se adaptan perfectamente al término referido a la manipulación alterativa, pues aquélla consiste en justamente modificar o cambiar el funcionamiento normal de un sistema o la transmisión de datos, y el agente incurre en el tipo al llevar a cabo esa actividad.

El “sujeto activo” puede ser cualquier persona, el dato lo da el comienzo de la redacción de la norma "el que", es decir que no se requiere una calidad especial. Si

bien estos casos en términos latos, se podría decir que normalmente intervienen sujetos "especializados" en estos menesteres. No obstante, normalmente se menciona al hacker como aquél que capta o interfiere con información sensible y puede utilizarla en perjuicio del poseedor de la misma, en principio puede ser una mera intromisión en la intimidad de la persona, pero si se sirve de dicha información para defraudar, es obvio que se produce una situación progresiva, por ejemplo, ingresar en las cuentas corrientes, en operaciones bancarias, o base de datos de un banco y de esta manera establecer la frecuencia de los depósitos en cuenta corriente de una empresa; qué porcentaje es en efectivo y qué porcentaje es en otro valores; a qué hora realiza los depósitos y en qué agencia bancaria, pues de mero intruso pasa a ser ejecutor de un delito contra la propiedad.

Esta actividad puede ser realizada por una modalidad denominada **"*cracking*"**. El cracker con frecuencia, es un autodidacta informático que intenta emular al hacker, desarrollando pequeños programas que permitan saltear la rutina interna del programa al que se quiere acceder por la que se chequea si se está registrado mediante los medios de generación de claves denominados keygens o key generators. Desconoce los sistemas informáticos y usualmente su reto es la simple vulneración del software comercial, plasmando conductas de "piratería informática". Por esto suele definirse a esta conducta como la de quebrar, remover o eliminar la protección de un programa de forma tal que el mismo funcione, luego de "crackeado", como si hubiera sido adquirido en forma legal por un usuario registrado".

En este último supuesto, estos individuos a veces utilizan una modalidad vandálica que destruye todos los sistemas, pero esto será materia de abordaje en el tópico de los daños informáticos. Lo real y concreto, es que tanto los "hackers" como los "crackers"

en la medida en que manipulen fraudulentamente alterando el normal funcionamiento de un sistema informático o la transmisión de datos, incurren en el tipo en cuestión.

En cuanto al “sujeto pasivo”, puede ser también cualquiera persona quien resultó engañado y dispuso perjudicialmente del patrimonio. También como en el caso del inciso 15º se puede dar la estafa en triángulo.

Se ha cuestionado que en esta fórmula se prescinde de la intervención del sujeto activo con el sujeto pasivo aun cuando se expresa, el que "defraudare a otro…", sin contenido a la intervención de ese "otro". Dicha interacción resulta indispensable para cualquier supuesto de defraudación, en cambio en este supuesto los protagonistas vuelven a ser el sujeto activo y la máquina o sistema informático "manipulado" para beneficio del primero, sin entrar en la escena nunca la segunda voluntad humana defraudada en la relación contraída; de modo que el sistema o dato informático pasa a ser medio, objeto y sujeto de la presunta defraudación.

Esta unilateralidad en la realización del acto lesivo lo acerca más al apoderamiento como acto de sometimiento de uno a otro, prescindiendo de la voluntad de ese otro, ya sea para hacerse de la cosa bajo engaño, o relacionarse lícitamente en un primer tramo para en un segundo defraudar su buena fe.

La comisión de este tipo de delito es doloso, de dolor directo ya que el agente debe conocer y querer la realización de los elementos objetivos de tipo penal.

En cuanto a la consumación y la tentativa, como en todos los casos del tipo defraudatorio, la consumación se produce con el perjuicio patrimonial derivado del uso por parte del agente de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos del sujeto pasivo. La tentativa es admisible.

## TERCERA PARTE

### Delitos Económicos mediante el uso de elementos tecnológicos:

Los fraudes económicos pueden efectuarse con medios tecnológicos como informáticos. En la Policía de la Provincia de Salta, existe un área específica encargada de la investigación de este tipo de delitos, es la División Delitos Económicos, la cual depende orgánicamente del Departamento Investigaciones y de la Dirección General de Investigaciones pero funcionalmente de la Unidad de Delitos Económicos Complejos, dependiente del Ministerio Público Fiscal.

Esta División actualmente posee un total de catorce efectivos policiales, compuesta por la titular de la misma, una segunda Jefa de División, un oficial subalterno y once suboficiales, que desarrollan funciones de sumariante, servicio de calle y cuatro de ellos, además de lo citado, son choferes.

Si bien no poseen ámbito de jurisdicción dentro de la provincia, esta está limitada por la competencia de intervención de la Fiscalía interviniente, en virtud de que instruyen actuaciones que se inician por la recepción de denuncias propiamente en la División citada, como así también aquellas que son derivadas de otras dependencias policiales y/o fiscalías del área capital e interior de la provincia, sobretodo, en aquellos casos donde no existe una fiscalía especializada en materia de Delitos Económicos.

Regresando a la temática planteada, debemos mencionar que existen distintos tipos de delitos suscitados mediante la utilización de medios informáticos y/o tecnológicos, o ambos en algunos casos, desarrollando a continuación los mayormente ocurridos e investigados, desde la modalidad más simple a la más compleja.

Cabe mencionar que en cuenta nuestra legislación en materia penal, aún en la fecha, no se ha tenido en cuenta por parte de nuestros legisladores determinar un

agravante para los hechos delictivos que se comentan mediante el uso de elementos telemáticos y/o tecnológicos, como puede ser un teléfono celular, sino que únicamente se ha limitado a los elementos informáticos. Sin embargo, la experiencia nos llevar a demostrar que es necesario tener en cuenta éste supuesto, además de circunstancias agravantes que pueden estar dadas por ***1) la condición de la víctima*** *(por ejemplo, un adulto mayor, el grado de instrucción),* ***2) el perjuicio económico sufrido*** *(en algunos casos ahorros de toda la vida y/o cuantiosas sumas de dinero) y* ***3) el impacto social por el número de víctimas.***

Si bien ya hemos desarrollado los FRAUDES ECONÓMICOS utilizados a través de los medios informáticos, haremos mención a continuación de los cometidos a través de los ***MEDIOS TECNOLÓGICOS O TELEMÁTICOS***, que suelen ser los mayormente denunciados y en los cuáles la legislación únicamente los tipifica dentro de la figura penal de la ESTAFA y/o DEFRAUDACIONES, sin tener en cuenta, cómo se desarrolla la modalidad, las condiciones personales de las víctimas o el monto del perjuicio económicos sufrido.

**ESTAFA. Modalidad "Secuestro Virtual".**

En este tipo de modalidad, la víctima recibe un llamado telefónico al teléfono de línea fija, donde una persona desconocida, simulando ser autoridad pública del Samec, personal policial o agente de tránsito, le expresa que un familiar habría sufrido un accidente vial y habría aportado dicho número, consultando por quien o quienes estarían ausente en el lugar. Quien recibe este llamado, por la situación que se le relata puede sufrir un shock emocional o crisis, suministrando involuntaria e inconscientemente la información personal requerida, llegando el momento en que el victimario, como parte del ardid, le hace saber que en realidad no sería un "accidente

sino el secuestro", de quien estaría justamente ausente en el hogar. Acto seguido, le solicita que se deposite dinero a través de alguna remecedora tales como "pago fácil, rapipago, westerunion", a cambio de la supuesta liberación del familiar, indicándole que le aporte un número de celular para poder llamarla y mantener a la víctima en permanente comunicación y así evitar que ésta solicite ayuda o diera conocimiento a la policía.


**ESTAFA. Modalidad "Premio Virtual".**

Esta modalidad, tiene similitud con la anteriormente mencionada, por el medio utilizado y el ardid o engaño utilizado, conocido dentro de la jerga policial como *"PREMIO VIRTUAL"*, en cuyo caso, quien llama le expresa que, "de un supuesto sorteo, quien atendió y/o el titular de la línea ha resultado ganador de un importante premio…"; momento en que de manera inconsciente, la víctima comienza a

proporcionarle datos personales tales como nombres, apellidos, número de documento de identidad, domicilio, entre otros.


Durante la comunicación y el desarrollo del ardid utilizado por el delincuente, comienza a adquirir una serie de datos personales que posteriormente podrán ser utilizados para volcarlos, por ejemplo, en una falsa página o “spam” creada al solo fin de dar mayor sustento al engaño, donde se hace constar el nombre aportado por el damnificado como “ganador”, indicándole para ello un link al cual debe ingresar.

Seguidamente, se le informa a la víctima que es necesario un depósito de dinero a nombre de una determinada persona, generalmente de un supuesto escribano o contador, en concepto de “pago de impuestos por el premio adquirido”, que suelen ser vehículos 0 km. ó su equivalente en dinero en efectivo, además de estar acompañado de regalos de electrodomésticos tales como Smart tv o tablets; argumentando que estos serían impuestos de ADUANA o AFIP.

Una vez que el sujeto pasivo, con la finalidad de poder recibir el supuesto premio, efectúa el primer pago de dinero; el causante sigue con el ardid realizando distintas llamadas posteriores al primer cobro, expresándole que debe realizar otros pagos de impuestos o similares, sea por el traslado del supuesto automóvil o para el depósito en la cuenta de caja de ahorro que ya seguramente le fue aportado por la víctima, logrando de ésta manera una comunicación frecuente y un situación cíclica en la cual el

sujeto pasivo al no querer perder el premio ni el dinero que ya ha depositado, continua cumpliendo las exigencias de la persona que lo llama y le pide que efectúe las transferencias o depósitos de dinero en distintas remecedoras o entidad bancaria. Esta situación continua hasta que la víctima se da cuenta que ha resultado estafada y deja de realizar envío de dinero; cortando de esta forma la comunicación.

**ESTAFA. Modalidad "Cuento del tío". (Abuelitos)**

En este tipo de delitos, las víctimas elegidas por parte de los causantes son los adultos mayores, es decir, personas a partir de los 55 a 60 años en adelante; cuya modalidad es la conocida en la jerga policial como "Cuento del tío a abuelitos". En lo que se refiere al desarrollo de estos delitos, los mismos se inician a través de un ***elemento tecnológico o telemático***, como es un teléfono celular o fijo. El causante, se comunica al número telefónico de línea fija de la persona elegida, donde simulando ser hija/o, nieta/o y/o sobrina/o, le expresa que se encuentra en el banco donde se anotició que los billetes de pesos argentino, generalmente de la denominación de mayor circulación como es el de CIEN PESOS, estarían por caducar, al igual que los dólares; por lo que le indica que enviaría a un conocido de profesión "contador o escribano", supuestamente de algún banco, hasta el domicilio de la víctima a retirar el dinero. Asimismo, le expresa que no debe cortar la comunicación por cuanto la estaría llamando desde el banco. Seguidamente, un desconocido/a, se presenta a los pocos minutos en el inmueble del damnificado, quien confiando en que se trataría de una familiar la persona que se encuentra en comunicación telefónica, le hace entrega del dinero, generalmente, suelen ser ahorros de toda la vida. Acto seguido, el supuesto profesional del banco se retira y le expresa que regresaría con los nuevos billetes ya cambiados. Al corroborar la persona llamante que se hizo entrega del dinero y asegurar

que la víctima ya no contaría con más dinero para entregar, de acuerdo a las preguntas que le refiere, corta la comunicación.

Si bien, el medio utilizado para cometer este tipo de delitos es a través de un teléfono celular, el trabajo de inteligencia previo que realizan los causantes para identificar sus víctimas, es a través de medios informáticos, como son bases de datos de empresas telefónicas como TELECOM, CABLE VISIÓN, etc., que suelen estar en internet y son de acceso público, con la finalidad de determinar los datos personales como nombre, apellido, dirección y número de documento de identidad que identifique la edad del titular.

Asimismo, suelen munirse de tarjeta sim (chip) “alternativos”, cuya titularidad aportada a la empresa de telefonía celular suele ser de otra persona, puesto que lo adquieren de puestos de venta público o de la vía pública.

Sin embargo, esta simple utilidad que suelen dar los delincuentes al teléfono celular, lleva a que los investigadores, deban estar familiarizados con la tecnología y las herramientas necesarias para poder establecer quien efectuó la comunicación a la víctima, desde donde provino e identificación de quien retiró el dinero. De igual manera, deberá determinar los vínculos existentes entre éstas personas y todos los medios utilizados por parte de los causantes para asegurar su cometido; como también identificar todo otro elemento que se útil para el esclarecimiento del hecho investigado.

Por tal motivo, quienes se encuentran a cargo de esta investigación, como de los supuestos anteriormente citados, deberá tener conocimiento de cómo realizar los requerimientos judiciales a las empresas telefónicas pertinentes, realizar análisis de las comunicaciones existentes y determinar la ubicación del móvil en cuanto a su geolocalización, munirse de información a través de redes sociales de acceso público u

otros sitios que pudiera consultar tendiente a determinar la identificación de los causantes, entre otros.

Estas diligencias, no sólo competen a la fuerza de seguridad en su condición de "auxiliar de justicia" para realizar la investigación, sino también que quienes tienen a cargo dirigir la investigación, como es el caso del Ministerio Público Fiscal en Salta, deben tener ciertos conocimientos como los ya mencionados y sobretodo una menta abierta y proyectada a que a veces estas modalidades delictivas son abstractas por los medios utilizados y que requieren de una capacitación permanente que sea acorde a los avances tecnológicos que diariamente van mutando mundialmente.

**ESTAFA POR USO DE TARJETA DE DÉBITO O CRÉDITO. Modalidad "Transferencia bancaria".**

Actualmente, las modalidades citadas continúan en auge, pero así como la sociedad se ha ido concientizando de las medidas de prevención que las fuerzas de seguridad le inculcan y difunden a través de los medios de comunicación, han ocasionado que los delincuentes también muten en cuanto a su proceder delictivo, generando inclusive, cierta exposición de la identidad personal o de alguien de su entorno familiar, personal o de amistad.

Desde mediados del año pasado, se ha notado un incremento de denuncias donde la víctima ha realizado operaciones a través del uso de cajeros automáticos y por intermedio del uso de tarjeta de débito y en menor caso, de tarjetas de crédito.

El inicio de esta modalidad puede estar dado por una comunicación telefónica a la víctima, refiriéndole que ha ganado un premio o bien, que ha sido beneficiario de una

bonificación de suma de dinero, como por ejemplo, el ardid de “reparación histórica de anses o salario universal, pensión contributiva”, etc..

También, suele originarse cuando la víctima, observa en redes sociales tales como facebook, instagram, twitter, etc., pero mayormente en “Facebook”, el ofrecimiento de “préstamos de dinero”, con intereses mínimos; aportando a través del “Messenger”, datos personales para ser contactada y poniendo de manifiesto, como ser nombres, teléfono y/o correo electrónico y el interés en el ardid desplegado, del cual obviamente no tiene conocimiento.

Una vez que el causante ha entablado contacto con la víctima, sea a través de llamadas telefónicas o comunicaciones a través de la aplicación de “whassApp”, le solicita que se traslade a un cajero automático próximo con la tarjeta de débito, indicándole que no debe poseer ningún préstamo personal anterior y en caso de tenerlo, deberá solicitar a un familiar o persona de confianza, que le facilite una cuenta con dicho requisito. Seguidamente, luego de ciertas indicaciones que le refiere cuando el damnificado se encuentra en el interior de lobby del banco, hace que

involuntariamente genere un préstamo personal y/o que el dinero que posee acreditado, sea transferido de forma inmediata a otra cuenta bancaria.

En los casos planteados, podemos notar que no existen sofisticados recursos logísticos ni exposición directa por parte del causante, debido a que el medio utilizado es el uso del teléfono, tanto de línea fija como celular. Generalmente, en estos casos, el chip que se manipula puede ser un “activador” o “chip bomba”; en la cual la empresa prestataria desconoce titularidad o en su defecto, se han utilizado datos de otras personas ajenas totalmente al hecho.

A diferencia del último hecho citado respecto de los dos primeros, puede apreciarse que se utiliza además del teléfono, una tarjeta de débito, un cajero automático y existe exposición directa del causante o alguien del entorno de éste, en virtud de que se aporta datos personales del titular de una cuenta bancaria, la cual será la receptora del dinero que posteriormente podrá ser cobrado o transferido.

En este caso no solamente se observa el uso de elementos tecnológicos sino también informáticos, debido al que al realizar una transferencia directa de tipo bancaria a través de cajero automático, involuntariamente, con las indicaciones que le van proporcionando, la víctima, le proporcionada información personal bancaria, además de los datos personales que pudiera citado anteriormente; la cual puede ser utilizada fraudulentamente por el causante.

**Delitos Cibereconómicos: tipos**

**Casos de delitos cibereconómicos:**

A continuación, procederemos a desarrollar un poco más en profundidad y puntualmente los fraudes y defraudaciones informáticas, consideradas éstas como las

conductas producidas por las acciones delictivas derivadas de metodologías asociadas a los conceptos de PHISHING, VISHING, SMISHING, PHARMING, SKIMING/CLONING, etc.; como también de otra cualquier conducta orientada a modificar, alterar, ocultar y/o manipular datos, sistemas y programas informáticos con un fin ilícito.

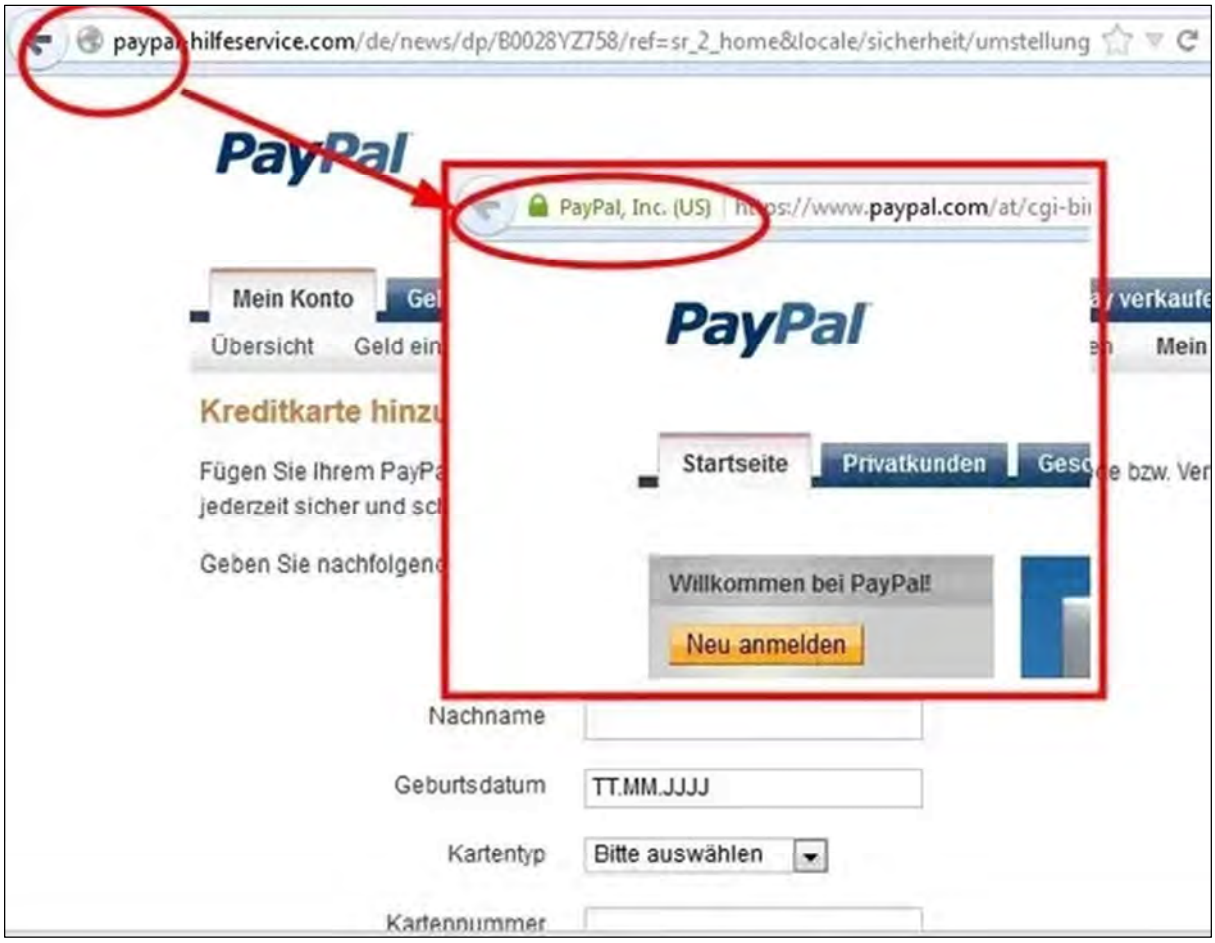
**Acciones delictivas derivadas:**

**PHISHING: (Password – Fishing)**

Es una forma de engaño que traducida al español hablaríamos de “pescar”. Esta maniobra delictiva refiere que es la acción mediante la cual los sujetos activos envían un mensaje de tipo “anzuelo” o “señuelo” a una o varias personas, intentando convencerlas para que revelen sus datos personales mediante la contestación de un correo electrónico o a través de un link en el mismo cuerpo del mensaje.

Usualmente, esta información es luego utilizada para realizar acciones fraudulentas tales como transferencias de fondos desde la cuenta bancaria de la víctima hacia la del causante; compras con tarjetas de débito, crédito u otras acciones delictivas que pueden efectuarse mediante la utilización de esos datos.

Como variantes de la modalidad de Phishing, podemos citar a las acciones delictivas conocidas como ***VISHING*** y ***SMISHING.***

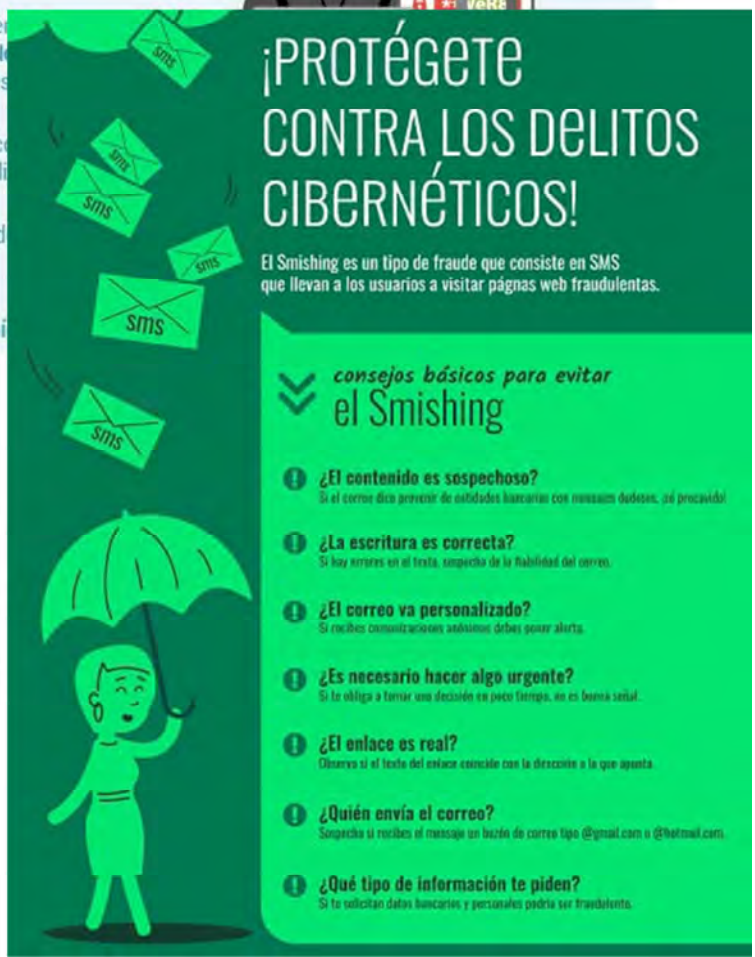

hilfeservice.com/de/news/dp/B0028YZ758/ref=sr_2_home&locale/sicherheit/umstellung
PayPal
PayPal, Inc. (US)
https://www.paypal.com/at/cgi-bi
PayPal
Mein Konto
Übersicht
Startseite
Privatkunden
Willkommen bei PayPal!
Neu anmelden
Kreditkarte hinzu
Nachname
Geburtsdatum
TT.MM.JJJJ
Kartentyp
Bitte auswählen
Kartennummer

**Vishing:**

El **VISHING**, es la acción mediante la cual no indican un link donde deba ingresar la víctima, sino que ofrece un número de teléfono donde comunicarse. Evidentemente, este número es falso y no corresponde a la entidad que se está simulando ser. Esta práctica fraudulenta, que consiste en el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o útil para el robo de identidad.

Por ejemplo: le llega a la persona un correo desde una empresa denominada “CRUCEROS CELEBRITY”, ofreciéndole un paquete turístico a un precio irrisorio al del mercado y de la competencia con propuestas interesantes, dejando como número de contacto para que el interesado se comunique a un número telefónico. Al contactarse el sujeto pasivo, obviamente será atendido por una persona que se identificará como perteneciente a dicha empresa y mediante dicho ardid le solicitará información personal y datos de sus tarjetas de crédito o débito, o le requerirá transferencia bancaria a una cuenta que luego de la acreditación del dinero dará de baja o a una billetera virtual para el correspondiente pago del supuesto paquete que adquirió.

Es importante, como medida de prevención, que se deba tener en cuenta que será un “sitio seguro” y no un spam, cuando puede observarse que la URL se encuentra en color “verde” y con un ícono de “candado”; como puede observarse en la imagen que a continuación se anexa, donde se observan ambos casos.


**Smishing:**

La figura del **SMISHING**, es la acción a través de la cual el medio de comunicación empleado por

parte del sujeto activo hacia la víctima es a través de la llegada de un mensaje de texto, es decir, que es una técnicas de ingeniera social con mensajes de texto dirigidos a los usuarios de telefonía móvil, donde generalmente indica un falso mensaje respecto de la acreditación de un premio o sorteo, bonificaciones por algún servicio público o privado, o por beneficios de alguna firma o empresa de tarjeta de crédito, e informa un número telefónico para comunicarse. En esta modalidad, es cuando directamente inicia la comunicación telefónica el sujeto desconocido hacia el número telefónico del sujeto pasivo, elegido al azar, identificándose como empleado de alguna empresa conocida, por ejemplo “Personal”, haciéndole conocer que en un sorteo que se realizó entre los socios de las líneas salió ganadora y acreedora de un supuesto premio.

Un claro ejemplo de éste tipo de casos es de los conocidos como “***PREMIOS VIRTUALES***”.

**Pharming:**

Esta es otra forma de fraude en línea similar al Phishing. Los Pharmers, es decir, quienes se dedican a cometer delitos a través de ésta modalidad, atacan la red y equipos de los usuarios modificando y redirigiendo el tráfico a otros sitios fraudulentos.

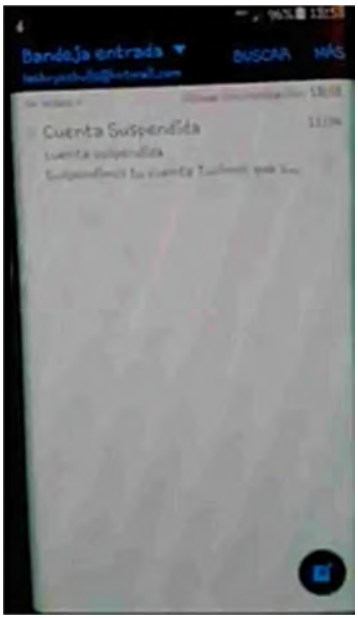
Con ello, utilizan los mismos sitios web falsos y el robo de información confidencial para perpetrar estafas en línea, pero en muchos sentidos, es más difícil de ser detectados ya que no necesitan que la víctima acepte el mensaje que le fue enviado de “señuelo”.

El Pharming redirige a sus víctimas al sitio web falso, inclusive si escriben correctamente la dirección web de su banco o de otro servicio en línea en el explorador de internet; por lo que no es requisito para esta modalidad que los usuarios hagan un

“clic” en los vínculos engañosos que se incluyen en mensajes de correo electrónico falsos.

Al respecto, como medida de prevención, debemos tener en cuenta si el mensaje recibido en su cuenta posee que la dirección de https se encuentre en color verde y posea el símbolo de un candado, para tener la seguridad de que es el sitio real del banco o página a la cual se ha ingresado.

Para mayor ilustración se anexa un video ilustrativo donde se simula una página del sitio de “Mercado Libre” y le solicita a la víctima que revalide sus datos personales y de cuenta para poder continuar haciendo uso del sitio comercial mencionado. (ANEXO I)




**KEYLOGGER:**

El keylogger es un programa (software) o hardware que registra y almacena todas las teclas presionadas o pulsadas en un teclado de un dispositivo electrónico (computadora, tablet, celular, smartv, etc.).

Su uso tiene por objetivo capturar datos privados de acceso a diversos sistemas y/o aplicativos, como ser usuario y contraseña de un home banking por ejemplo, los números de la tarjeta de crédito o débito, clave fiscal, de correo electrónico, entre otros.

Esta modalidad actualmente ha evolucionado y existen programas que permiten capturar también movimientos del mouse.

**SKIMMING / CLONNING:**

Este accionar consiste en la clonación de tarjetas de crédito y débito. El dispositivo "skimmer", permite leer y almacenar los datos de las tarjetas para su copia en otra tarjeta física o para operar con ella en lugares donde no se requiere la presentación del medio físico. Por ejemplo la compra online o telefónica.

El skimming es un método que utilizan los delincuentes para capturar los datos codificados que poseen en la banda magnética las tarjetas.

Se hace utilizando dispositivos físicos o equipos. El objetivo es capturar o "skim" la información codificada en la banda magnética para después producir tarjetas clonadas con el fin de utilizarlas en forma fraudulenta.

El skimming no se refiere a la creación de una tarjeta falsificada o clonada, sino al acto de robar la información o datos de las tarjetas. Al obtener dicha información, el sujeto activo puede vender la misma, realizar transacciones de extracción de dinero de cajeros automáticos, transferencias de dinero, compra de cripto monedas y enviarlas a una billetera o monedero virtual o compras online y telefónicas.

## SKIMMING EN LOS CAJEROS AUTOMÁTICOS:

El skimming en los cajeros automáticos es un método que usan los delincuentes para capturar los datos de la banda magnética mientras la tarjeta se está usando en el cajero automático.

Los delincuentes utilizan diversos métodos y dispositivos para robar los datos de la cuenta de la tarjeta y también el PIN o NIP del cliente. Una vez que ya se ha obtenido esta información, es decir, los datos completos de la pista de la banda magnética y los PINes, proceden a copiar ésta información en otras tarjetas que posean banda magnética creando de esta forma tarjetas clonadas con la finalidad de proceder a extraer dinero de las cuentas de las víctimas, realizar compra de criptomonedas y/o transferir las mismas a una billetera virtual, realizar compras online o distribuir en venta a corredores que son empleados por grupos organizados con el objetivo de sacar dinero de las cuentas vulneradas.

Para poder perpetrar el skimming exitosamente, se requieren un dispositivo llamado “skimmer” y un dispositivo para capturar el PIN.


***Diversos métodos de Skimming:***

Los “skimmers” son los dispositivos fabricados a la medida para almacenar datos, los cuales, se usan para robar los datos codificados en la pista de la banda magnética de las tarjetas genuinas.

Otros son diseñados para que puedan ser colocados sobre la abertura o “boca” del lector de tarjetas del cajero automático.

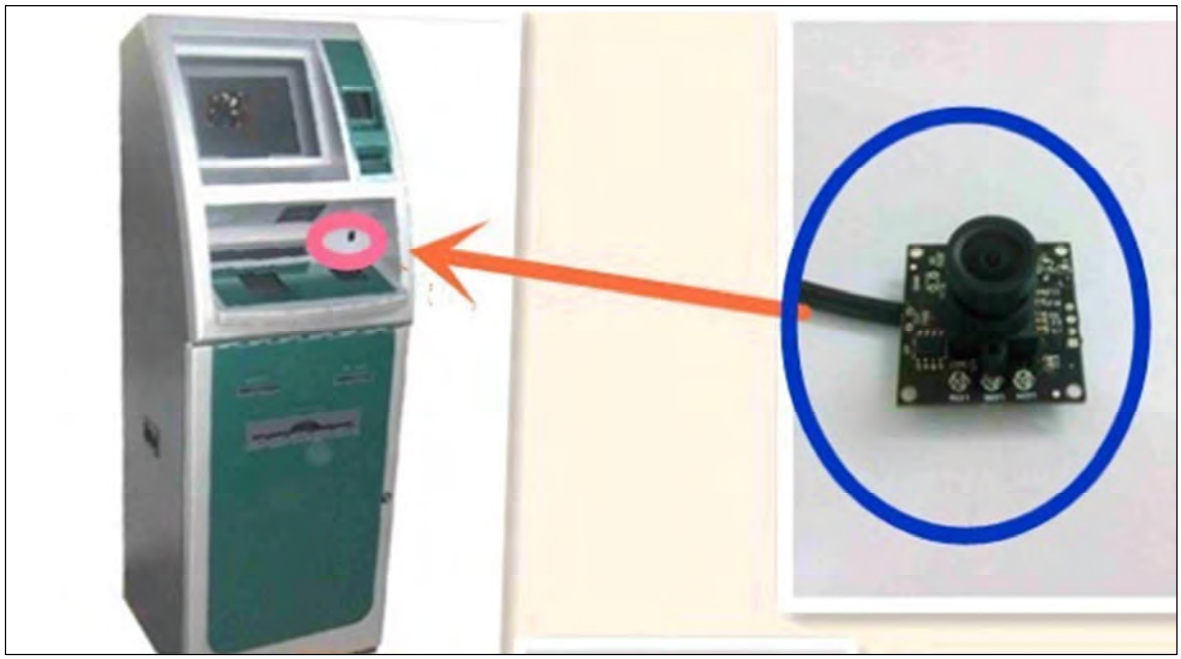
Se fabrican frentes o paneles falsos que cubren toda la superficie del frente del lector de tarjetas. Diseñados para que parezcan que son parte del cajero automático.


**Diversos métodos para capturar el PIN:**

***Cámara Estenopeica:***

Este es el método más sofisticado y el más ampliamente utilizado. Consiste en instalar una cámara estenopeica cerca del cajero automático, la cual graba en video al tarjetahabiente mientras ingresa su PIN.

La imagen de video se almacena o transmite a un dispositivo receptor situado a un máximo de cien metros.



***Teclado de PIN falso:***

Se coloca sobre el teclado de PIN legítimo. El perpetrador del fraude coloca sobre el teclado legítimo un falso teclado de manera superpuesta de forma tal que éste último capture los PINes que se ingresan los usuarios del cajero.

***Espiar al usuario por encima del hombro:***

Los PINes se obtienen espiando por encima del hombro a la víctima del fraude mientras está ingresando su PIN.

Es un método poco tecnológico que es sin embargo, muy efectivo. Años anteriores fue un método exitoso pero que fue quedando en desuso por la implementación de medios tecnológicos como la utilización del falso teclado y un dispositivo skimmer en el sector de lectura de tarjeta.

**OTROS MÉTODOS PARA ROBAR TARJETAS EN CAJEROS AUTOMÁTICOS:**

***Distraer al Usuario:***

El perpetrador del fraude, provoca algún tipo de situación que lleve a distraer o dispersar la atención del sujeto pasivo que está operando en el cajero automático

designado como objetivo. El skimming se realiza entonces utilizando un dispositivo de mano mientras la víctima se encuentra distraída.

***El conocido como "buen samaritano":***

Utilizando una banda o magna de metal o plástico, se bloquea la ranura que dispensa el efectivo en el cajero automático.

Cuando el cajero no dispensa el dinero, el sujeto conocido en la jerga policial como "buen samaritano", se acerca a la víctima con fines de brindarle ayuda y le sugiere que ingrese nuevamente el PIN, mientras éste lo observa.

La máquina retiene la tarjeta insertada y el delincuente la recupera una vez que el sujeto pasivo se retira del lobby del cajero, suponiendo que fue el banco que retuvo la misma y que luego ésta se la restituirá.

**DIVERSOS MÉTODOS DE SKIMMING:**

***Ataques de Malware:***

El malware es la nueva tendencia en los ataques para robar datos de tarjetas en cajeros automáticos.

En este caso, el atacante puede implantar el malware después de comprometer la seguridad del cajero automático físico o del software que hace funcionar la máquina.

Algunos tipos de malware que específicamente se usan en los cajeros automáticos no solamente son capaces de capturar los datos del usuario (tarjetahabiente), sino que también le dan al atacante la habilidad de dispensar efectivo y elegir la denominación de

billetes que desean dispensar sin límite de disponible, siempre y cuando el cajero cuente con dinero.

**Ejemplo en video de dispositivo de skimming en un cajero automático:** (ANEXO 2)

## ESTAFAS A TRAVÉS DE COMPRAS VÍA ONLINE:

En cuanto a esta modalidad, tipificada en nuestro Código Penal como el delito de ESTAFA; se suscita en circunstancias en que el sujeto pasivo, con la intensión de realizar la compra de algún objeto, tales como celulares, consolas de video juego, vehículos, entre otros; ingresa a sitios de venta y compra de tales artículos conocidos tales como “OLX”, “MERCADO LIBRE”, entre otros; y al observar una publicación de su interés sueles contactarse posteriormente con el “vendedor”.

Al iniciar la comunicación entre ambas partes, generalmente a través de una dirección de correo electrónico que el causante aporta como propia, logra que el damnificado deje de interactuar a través de la página oficina comercial y por ende que el contrato sea sin intermediario y únicamente entre los particulares.

Por ejemplo, ante el interés de comprar un vehículo marca VW modelo Fox, dominio JKZ-864, a un precio de $50.000 (CINCUENTA MIL PESOS); el sujeto pasivo se muestra interesado por cuanto es un precio inferior al actualizado en el mercado, argumentando el sujeto activo, como parte del ardid que por razones de “viaje urgente y mudanza debe vender el rodado al encontrarse en otra país en el cual no puede registrar el automóvil en venta.

Durante los mensajes sucesivos el causante le envía fotografías ilustrativas del rodado y documentación, a fin de dar mayor credibilidad a su maniobra fraudulenta; solicitándole que la víctima efectúe el pago a través de la página que supuestamente sería oficial del sitio, es decir, que para ello crea una “página falsa o spam” del sitio, por ejemplo de “Mercado Libre”, en la cual una supuesta asesora de dicha empresa, haciendo uso del logo, se contacta con el comprador haciéndole saber que tendría

conocimiento de la operación de compra y venta del rodado y sería la designada para “garantizar una compra segura”.

Teniendo en cuenta el ardid de que el automóvil se encontraría fuera del país y que sería enviado a este por medio de barco, por ejemplo, el causante le solicita al damnificado que efectúe el pago con criptomoneda, siendo la usualmente más conocida “bitcoins”, debiendo para tal operación gestionar el comprador una “billetera virtual de bitcoins”.

Una vez que la víctima deposita los bitcoins o efectivo en la billetera virtual del causante y aguarda que se le envíe el rodado comprado, el causante cesa con las comunicaciones a través del correo electrónico y suele bloquear o borrar la página de publicidad de venta del automóvil; dándose cuenta el sujeto pasivo que resultó víctima de éste tipo de engaño y fraude.

En este caso, el sujeto activo, mediante el uso de herramientas informáticas (computadora, celular, tablets, etc.), y un ardid se contacta con la víctima de quien logra la confianza y credibilidad. Una vez que éste último realizó la transferencia de dinero a través de billetera virtual, pierde todo contado con el causante.

Al respecto debemos mencionar que las billeteras virtuales son creadas digitalmente y es actualmente imposible establecer quién es el titular de la misma por cuanto no existe un régimen u organismo que las controle o reglamente.

Poseen una identificación alfanumérica de 64 bits, entre mayúsculas y minúsculas que en segundos van mutando de transferencias de dinero hacia otras cuentas.

Para mayor conocimiento al respecto de ésta modalidad, tampoco legislada en nuestro país, procederemos a desarrollar una breve reseña acerca de estas herramientas informáticas e innovadoras.

## BILLETERA VIRTUAL:

Una billetera virtual o wallet de monedas digitales es la herramienta informática que permite transacciones a través de bitcoins. Este software permite a los tenedores de bitcoins tener una dirección privada donde proteger y transaccionar sus bitcoins.

La función de la billetera de Bitcoins es poder acceder a la blockchain (una suerte de gran hoja de cálculo pública, distribuida y virtual donde están asentados todos los movimientos de las criptomonedas desde que se creó Bitcoin).

La wallet es la herramienta que permite interactuar con esos datos (lo que se compra o se “mine”) y guardarlos como ahorro, venderlos, regalarlos, gastarlos o usarlos en sitios de apuestas.

Existen una gran cantidad de billeteras para guardar Bitcoins, las más populares son XAPO, WIREX, COINBASE, MYCELIUM WALLET; entre otras. Hay monederos para el teléfono, computadora, “offline” en papel y en versión de web. La opción más recomendable es tener una billetera en la computadora de escritorio; se recomienda tener una cantidad relativamente grande de bitcoins y a partir de ahí una cantidad más pequeña en el Smartphone en el caso de que se hagan transacciones con la criptomoneda.

La **Hive** (OS X), **MultiBit** (Windows, OS X, Linux) y **DarkWallet** son algunas de las mejores opciones del mercado. La otra cara de la moneda son los monederos virtuales, que cumplen la misma función que tener uno instalado en la computadora. La diferencia es que estos monederos son controlados por terceros, lo que significa que

otra persona está cargo de controlar los fondos individuales en bitcoins de los usuarios. Los más populares son Coinbase, Circle, Blockchain y Xapo.

Las llamadas “paperwallet” son expresiones físicas de las llaves públicas y privadas que funciona virtualmente en las transacciones de bitcoin. Funciona utilizando la tecnología QR para escanear. La gran ventaja de esta modalidad es que la inversión está casi absolutamente a salvo de ataques informáticos. Cualquier usuario de bitcoins puede crear sus propios paperwallet.

**BITCOINS:**

Los bitcoin además de ser un tipo de criptomenda, debemos decir que previamente a ello hay que entender otros conceptos básicos. Primero es que se basa en una red de ordenadores descentralizada, lo que suponen nodos repartidos por todo el mundo con copias de todas las transacciones que se han realizado.

En segundo lugar, el concepto de los mineros, que son las personas que forman parte de los nodos y que tienen el incentivo de que cada vez que se generan Bitcoins nuevos se reparten entre quienes forman parte de los nodos.

Y el último, pero no por ello el menos importante, es el concepto de las exchanges, que son las que permiten cambiar monedas como los euros o los dólares por Bitcoins; y por este medio poder interactuar para guardarlos o intercambiarlos en el mundo digital del comercio mundial a través de las billeteras virtuales de bitcoins que se llaman “wallets” o carteras.

Cuanto más grande sea la red de Bitcoins más seguras serán las transacciones ya que una vez que la transacción se efectúa, esta es replicada en toda la red de ordenadores de manera que ya no la puedas modificar ni saber de dónde viene y quién

la ha realizado; ya que para poder hacerlo tendría que modificar la transacción en todos los ordenadores.

Además de ello, debemos mencionar que la cantidad de criptomonedas que se emiten cada año está configurada en su algoritmo; sumado a que cada cuatro años, se reduce por dos la cantidad que se producen y sólo se emitirán un total de 21 millones de Bitcoins. Esto es una diferencia fundamental con las monedas convencionales, puesto que los bancos modifican su valor a su libre albedrío.

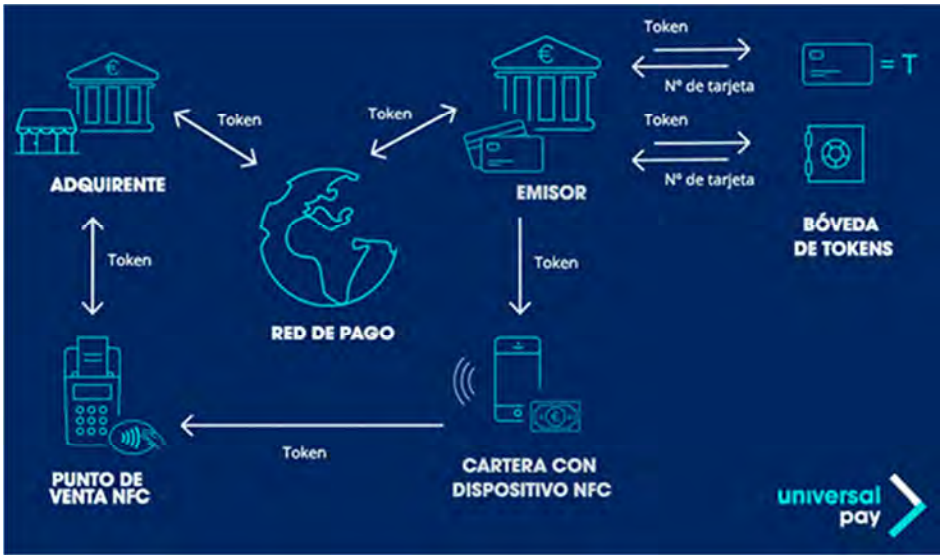
Esto le da más capacidad de generar valor frente a unas monedas que pueden devaluarse cuando los bancos digan. Las monedas deben cumplir tres funciones, la de permitir almacenar un valor, realizar intercambios y transacciones, y referenciar objetos. Referenciar, quiere decir que se puede utilizar de referencia de valor, como cuando dices el precio de tu teléfono para que el resto podamos hacernos una idea de su valor.

En virtud de esta definición no podemos decir que las criptomonedas sean monedas de verdad porque no cumplen estas tres propiedades; pero la que más se cumple es la de almacenamiento de valor, como si fuera oro virtual. Pero como medio de intercambio no se acepta en demasiados sitios, y como su valor está cambiando constantemente tampoco sirve como referencia. Las criptomonedas, no serán monedas de verdad hasta que no se cumplan estas tres propiedades.

## BLOCKCHAIN Y LA TOKENIZACIÓN:

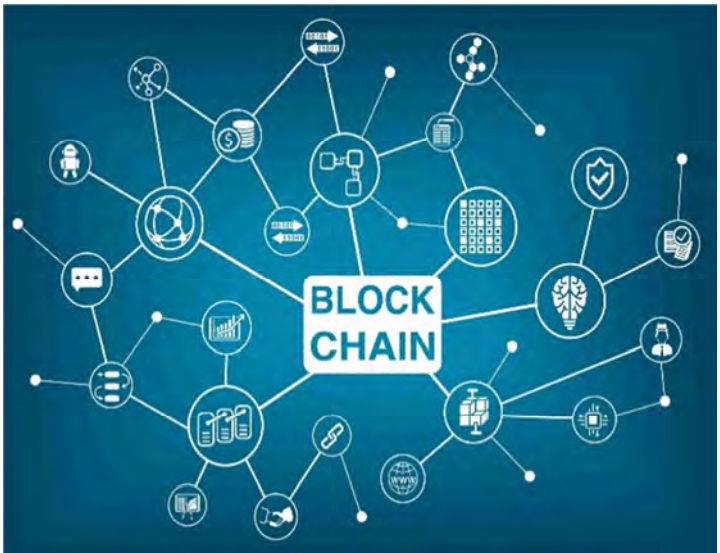
La Blockchain o cadena de bloques, es la tecnología que hay detrás del Bitcoin, y se puede separar de él para hacer otras cosas con ella. Por ejemplo sirve para crear otras criptomonedas que se basen en los mismos principios, pero que tengan otras propiedades al haber sido cambiados el algoritmo o la política monetaria. Esto es

precisamente lo que ha pasado por lo que han ido surgiendo muchas otras criptomonedas.




Otra moneda que ha surgido con esto llamada “Ethereum” y que probablemente sea lo más disruptivo que hay en el mercado a parte del Bitcoin. Su diferencia es que no se dedica únicamente a almacenar transacciones de monedas, sino a otras más genéricas como la ejecución de aplicaciones descentralizadas que no necesitan un servidor central.

El Blockchain también se puede utilizar para crear otros tipos de representación de valor. Es lo que se conocen como *Tokens*. Estos pueden ser criptomonedas, pero también lo que se conocen como tokens de utilidad, que son básicamente los que



puedes usar dentro de un ecosistema para participar en un servicio o utilidad. Un ejemplo son los casinos, donde compras sus propios tokens o fichas que luego puedes utilizar en sus máquinas y restaurantes.

Los “security tokens” son representaciones digitales de activos electrónicos, como las acciones, pero que se emiten de forma digital en vez de con un papel como suele hacerse convencionalmente. Esto se puede aplicar también a la hora de tokenizar edificios, arte y muchas otras cosas.

Los tokens son un producto insuperable porque se pueden revender cuando quieras para tener liquidez**,** lo que los convierte en activos más atractivos. Las criptomonedas, la cadena de bloques y los tokens son unas tecnologías disruptivas que van a cambiar muchas industrias en los próximos años.

**OTROS DELITOS INFORMÁTICOS AÚN NO TIPIFICADOS EN ARGENTINA:**

**Usurpación, robo y/o suplantación de identidad digital:**

Nuestra legislación no ha considerado aún como delito que una persona simule ser otra persona, es decir, que se haga pasar por otra persona en un blog, en una red social ni en cualquier otro medio electrónico.

**Acción coordinada de ciberejércitos de tendencia:**

No está previsto las acciones coordinadas y realizadas en redes sociales, blogs, sitios de opinión, comentarios en periódicos online y todo portal pasible de dejar un comentario u opinión; a fin de opinar, comentar, retrucar, difamar o glorificar una o grupo de personas determinadas que reciben lineamientos editoriales de quien los contrata. Entre sus objetivos principales están lo de desinformar o tergiversar la información online con el objeto de generar una tendencia de opinión. En algunas ocasiones son denominados ejército de Trolls.

**Violación a la intimidad:**

Si bien existen delitos penales relacionados con accesos indebidos de datos y hackeo; la acción de violación a la intimidad solo está contemplada en el artículo Nº 1770 del Código Civil y Comercial.

**Daño al honor en internet:**

Existen legislaciones en otros países que permiten un mecanismo fácil y rápido para poder quitar de los resultados de búsqueda, contenidos hechos con la intención de causar un perjuicio.

**Responsabilidad de las compañías tecnológicas:**

No está previsto en la legislación la responsabilidad de las empresas que proveen buscadores en internet o sitios que reproducen contenido respecto de la información que se publica por parte de los usuarios.

**Abuso de los dispositivos:**

La producción, venta, importación, difusión u otra forma de puesta a disposición del dispositivo, incluido un programa informático, dañado o adaptado principalmente para la comisión de delitos; no se encuentra prevista en nuestra legislación.

**Hurto informático:**

La tipificación de apoderamiento ilegítimo hace referencia solo a cosas muebles. En el caso del software, datos y bases de datos no personales son bienes intangibles.

**Captación o venta ilegítima de datos:**

Se refiere concretamente a las acciones relacionadas con obtener, captar, vender y enviar datos personales, financieros o confidenciales. Cabe aclarar que el código penal ha tipificado las acciones previstas a los keylogger y phishing con sus modalidades en los casos mediante los cuales se produzcan delitos relacionados con el fraude, hurto de cosa mueble, falsificación o alteración de moneda y apropiación de cosa perdida.

**Porno venganza / sexting:**

Es la publicación o difusión por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas.

Actualmente, se han conocidos varios casos de éste tipo de modalidad en nuestro país y provincia, de los cuales ya se han realizados comunicados a través de los medios de comunicación desde la División Prensa y Difusión de la Policía de Salta a fin de prevenir a la población para que no sea víctima de éste tipo de modalidad delictual.

Cabe mencionar que en estos casos los hechos fueron encuadrados dentro de la figura penal del delito de EXTORSIÓN; cuando en realidad, las acciones previstas por el sujeto activo encuadran con el delito conocido como SEXTING o PORNO VENGANZA.

Por ello es necesario que la legislación continúe evolucionando y adecúe su tipificación a los hechos que se suscitan en el vivir cotidiano de las personas, que buscan una solución a sus problemas de los cuales resultan víctimas a través del uso frecuente o no de los medios informáticos y tecnológicos y que nuestra legislación aún no ha previsto.

La globalización ha llevado a que las personas se encuentren constantemente interactuando a través de la tecnología, sea por razones personales, profesionales o simplemente de ocio; y a veces, al no existir un uso consciente de ello han llevado a vivenciar a las víctimas malas experiencias en situaciones que pueden tener consecuencias de índole personal como en un caso de grooming, por ejemplo; o de detrimento económico.

## MÉTODO CIENTIFICO DE INVESTIGACIÓN:

### Método hipotético – deductivo

El método hipotético – deductivo, es un modelo del método científico compuesto por los siguientes pasos:

**Observación del fenómeno a estudiar.**

*"Los operadores investigativos a cargo de la investigación de los delitos cibereconómicos".*

**Creación de una hipótesis para explicar dicho fenómeno.**

*"La capacitación y actualización de conocimientos respecto a los ilícitos informáticos y económicos, a los operadores a cargo de la investigación, permitirá proyectar protocolos de intervención y procedimentales, tendientes a la recolección de pruebas y al esclarecimiento, de los hechos delictivos de forma eficiente y plazos cortos a mediano".*

**Deducción de consecuencias o proposiciones más elementales de la propia hipótesis.**

*Se determina que los procedimientos de investigación y el accionar de éstos agentes no ha generado resultados favorables, contrariamente se incrementaron las denuncias.*

**Verificación o comprobación de la verdad de los enunciados deducidos, comparándolos, con la experiencia.**

*Se establece que con la capacitación de los recursos, se pueden crear políticas de prevención y protocolos de intervención en materia de seguridad informática y ciudadana.*

Por tal motivo, se procedió a combinar la formación de la hipótesis y la deducción, y teniendo en cuenta que la realidad existente ha determinado que se han incrementado las denuncias por los delitos cibereconómicos, lo cual se puede apreciar a través de los resultados estadísticos aportados. Es por ello, que como solución o ley probabilística para poder soslayar y disminuir en poco tiempo estos antecedentes, se hace necesario que los operadores a cargo de la investigación, sean instruídos con conocimientos y técnicas que les permitan un eficiente esclarecimiento.

Personalmente, considero que ésta solución es acorde a la hipótesis del problema planteado, por cuanto de nada nos sirve contar con recursos humanos y logísticos, si éstos no pueden generar políticas de prevención en seguridad informática tendientes a proteger a la sociedad; o bien, a la investigación para su pronto esclarecimiento cuando ya han sido cometidos.

**Método cuantitativo:**

En de que el método cuantitativo es aquel que nos permite, de manera objetiva, examinar datos en virtud forma numérica y es una herramienta de la rama de la estadística. Teniendo en cuenta que se procedió a realizar encuestas a personas que se desempeñan en diferentes organismos públicos y privados, de importante injerencia en el rol social, entre ellos a estudiantes del último año de la Escuela de formación para oficiales de policía, se logró determinar que las personas jóvenes, en el promedio de 18 a 24 años, tienen un conocimiento lato de la existencia de los delitos informáticos, pero no específicamente de los fraudes económicos; mientras que la edad intermedia de 25 a 45, solo la minoría los conoce, la edad superior a éstos, tiene conocimiento de este accionar delictivo en menor medida.

Por los resultados obtenidos, nos permite comprender explicativa y predicativamente la realidad de los conocimientos con los que cuentan los operadores a cargo de la investigación, como de los comunicadores sociales; con la finalidad de proyectar políticas de capacitación por los agentes investigativos y propiciar mecanismos tendientes a contrarrestar la comisión de estos tipos de delitos; mientras que a través de los comunicadores sociales, se pueden emitir mensajes precisos, sencillos y directos hacia la comunidad en general para prevenir estas conductas ilícitas.

## RESULTADOS:

Teniendo en cuenta que este trabajo integrador final se basa en la hipótesis de que la impunidad de los delitos cibereconómicos, se encuentra íntimamente relacionado con la falta de capacitación de los operadores investigativos; se procedió a tomar como “muestra de análisis” y realizar una encuesta anónima a 40 personas, de distintos sexos y edad, que se desempeñan dentro del ámbito de la seguridad pública, judicial, medios masivos de comunicación e instituto de formación para oficiales de la policía de la provincia; tendiente a establecer si existe un conocimiento social acerca de éste tipo de delitos, objeto del presente análisis y de la existencia de los organismos encargados de su prevención e investigación.

Los resultados obtenidos, han evidenciado cuantitativamente, que la población en general no posee un conocimiento acerca de la existencia de los delitos cibereconómicos ni de la existencia de un organismo encargado de su investigación por lo que es necesario que se difunda aún más este tipo de problemática perteneciente a la nueva revolución tecnológica en la que nos encontramos inmersos.

Independientemente de ello, es necesario que exista una capacitación constante para quienes se encuentran encargados de la investigación de éste tipo de delitos en virtud de que la tecnología evoluciona constantemente.

Cualitativamente, los resultados obtenidos han evidenciado que la tendencia está dada en que si bien existe un conocimiento generalizado o lato de los que son los delitos cibereconómicos, no existe una difusión masiva y constante a través de los medios de comunicación de las medidas de prevención que se puede tener para no incurrir y ser víctimas de este tipo de delincuentes.

Para mayor ilustración, a continuación, se presentan los resultados de las encuestas realizadas.

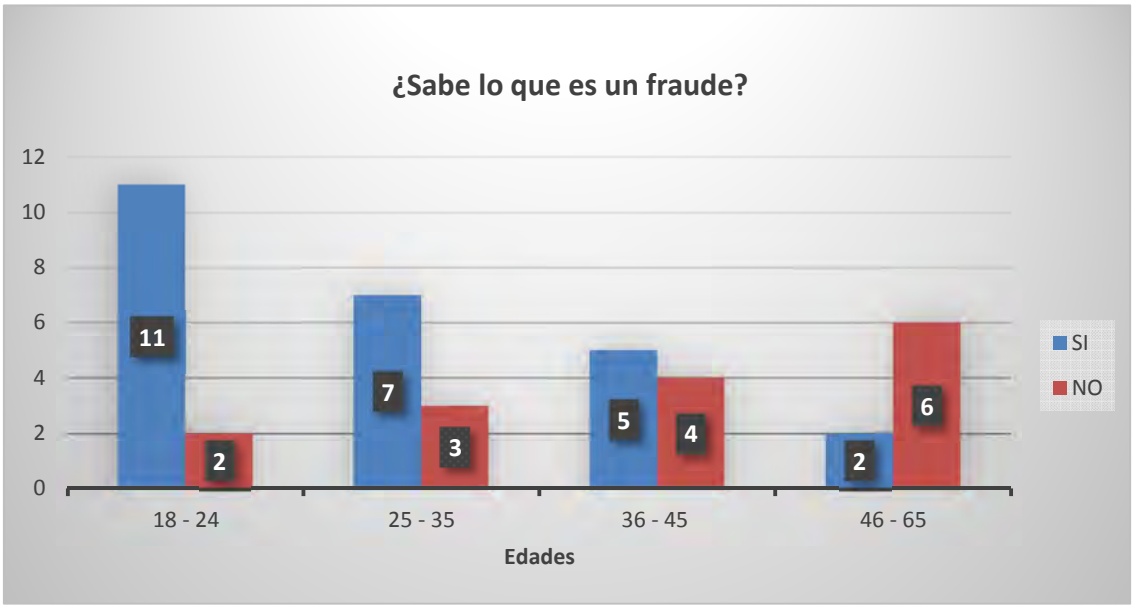
**FORMULARIO DE LA ENCUESTA REALIZADA:**

| Nº | Cuestionario | SI | NO |
|---|---|---|---|
| 1 | ¿Sabe lo que es un fraude? | | |
| 2 | ¿Sabe lo que es un delito cibereconómico? | | |
| 3 | ¿Alguna vez fue víctima de un delito cibereconómico?; ¿o alguien de su entorno familiar o personal lo fue? | | |
| 4 | ¿Denunció el hecho?. ¿Dónde? | | |
| 5 | La persona que lo atendió, ¿lo asesoró al respecto? | | |
| 6 | ¿Fue favorable la respuesta que recibió por parte de la persona que lo atendió? | | |
| 7 | ¿Se anotició a través de los medios de comunicación acerca de algún delito cibereconómico recientemente o durante los últimos dos años? | | |
| 8 | ¿Conoce si existe alguna área de la policía dedicada a investigar los delitos económicos y/o cibereconómicos? | | |
| 9 | A su entender, ¿la policía se encuentra capacitada para la investigación de estos tipo de delitos? | | |
| 10 | ¿Cree que se debe difundir medidas de prevención respecto de los delitos cibereconómicos o aún no lo considera necesario? | | |

## *Cuestionario:*

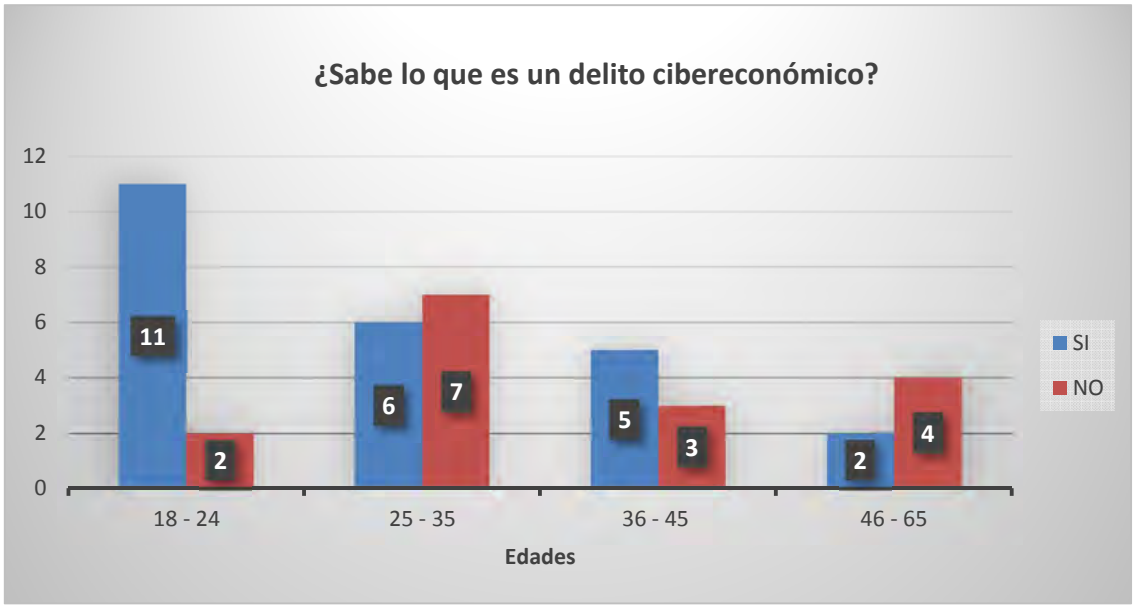
### *1.- ¿Sabe lo que es un fraude?*

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 – 60 |
| SI | 11 | 7 | 5 | 2 |
| NO | 2 | 3 | 4 | 3 |



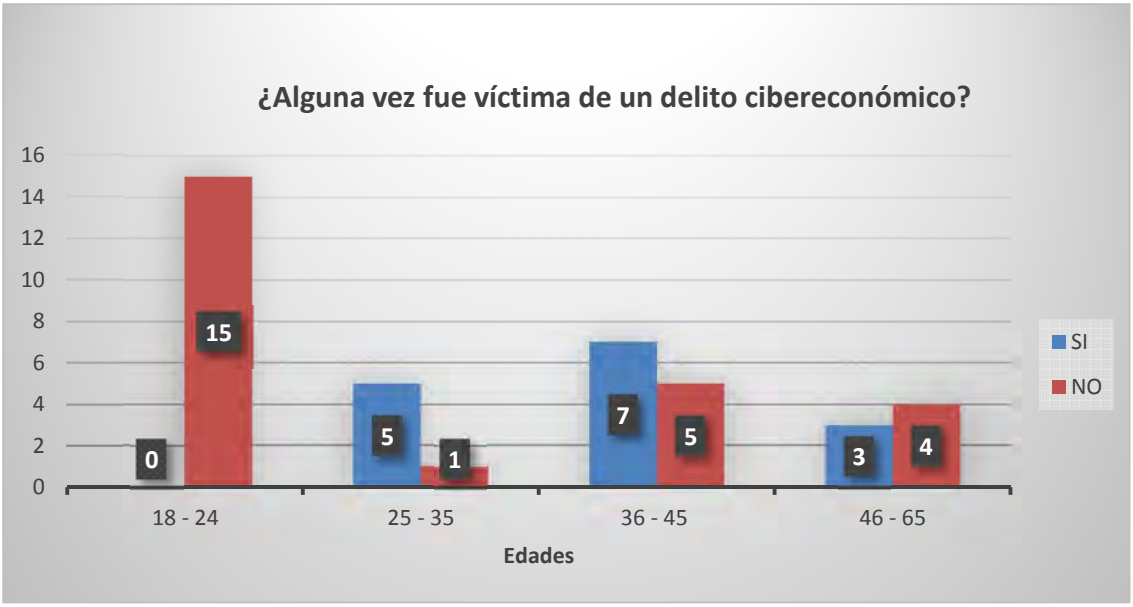

### *2.- ¿Sabe lo que es un delito cibereconómico?*

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 11 | 6 | 5 | 2 |
| NO | 2 | 7 | 3 | 4 |



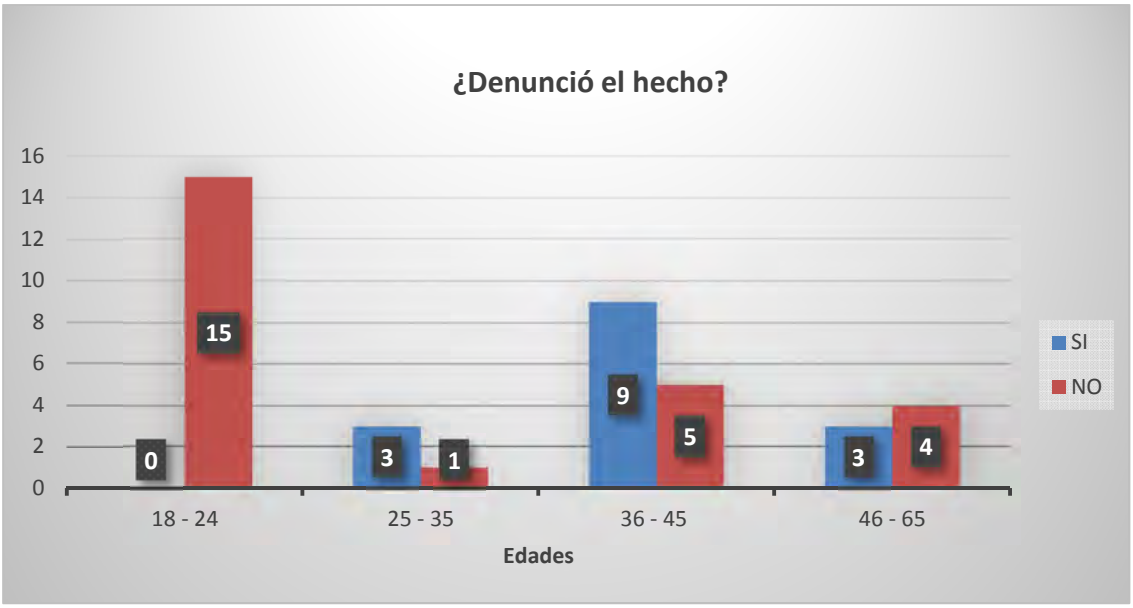

***3.- Alguna vez fue víctima de un delito cibereconómico?; ¿o alguien de su entorno familiar o personal lo fue?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 0 | 5 | 7 | 3 |
| NO | 15 | 1 | 5 | 4 |



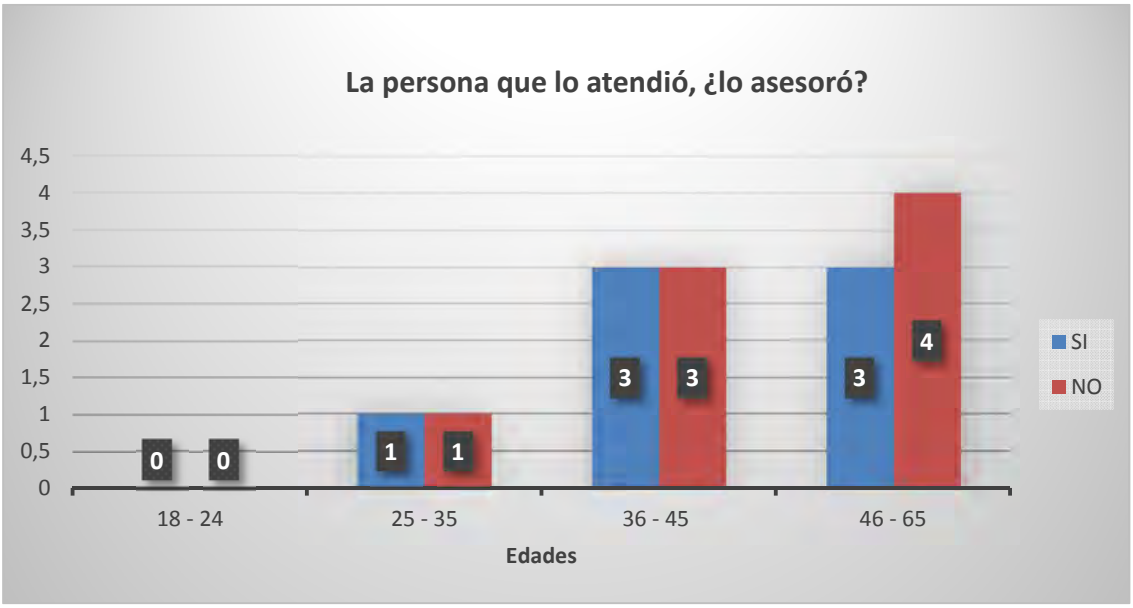

### *4.- ¿Denunció el hecho?. ¿Dónde?*

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 0 | 3 | 9 | 3 |
| NO | 15 | 1 | 5 | 4 |



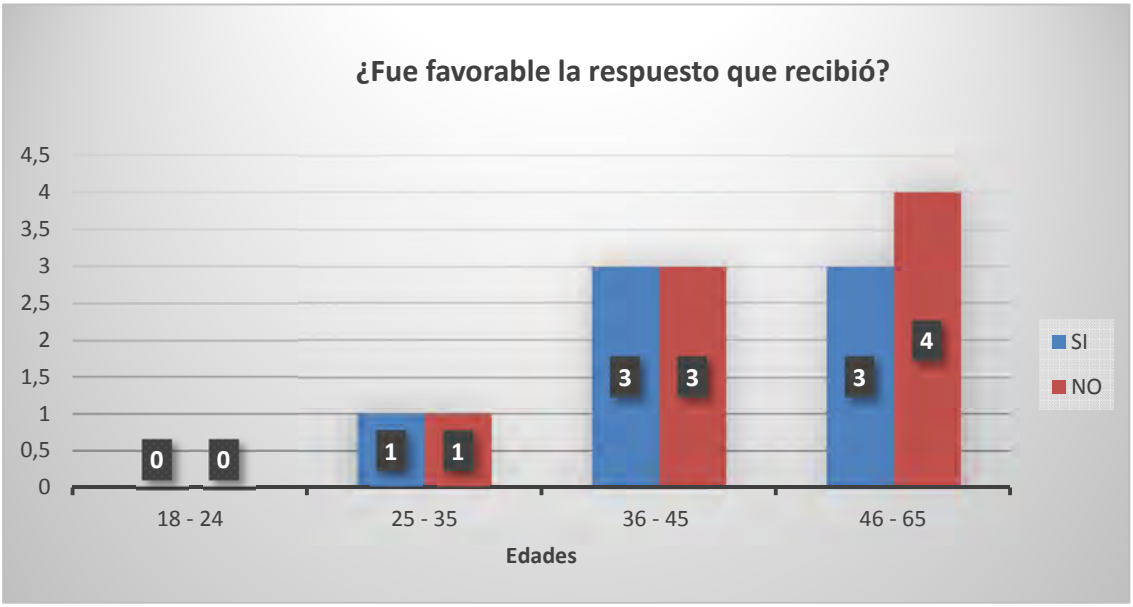
***5.- La persona que lo atendió, ¿lo asesoró al respecto?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 0 | 1 | 3 | 3 |
| NO | 0 | 1 | 3 | 4 |



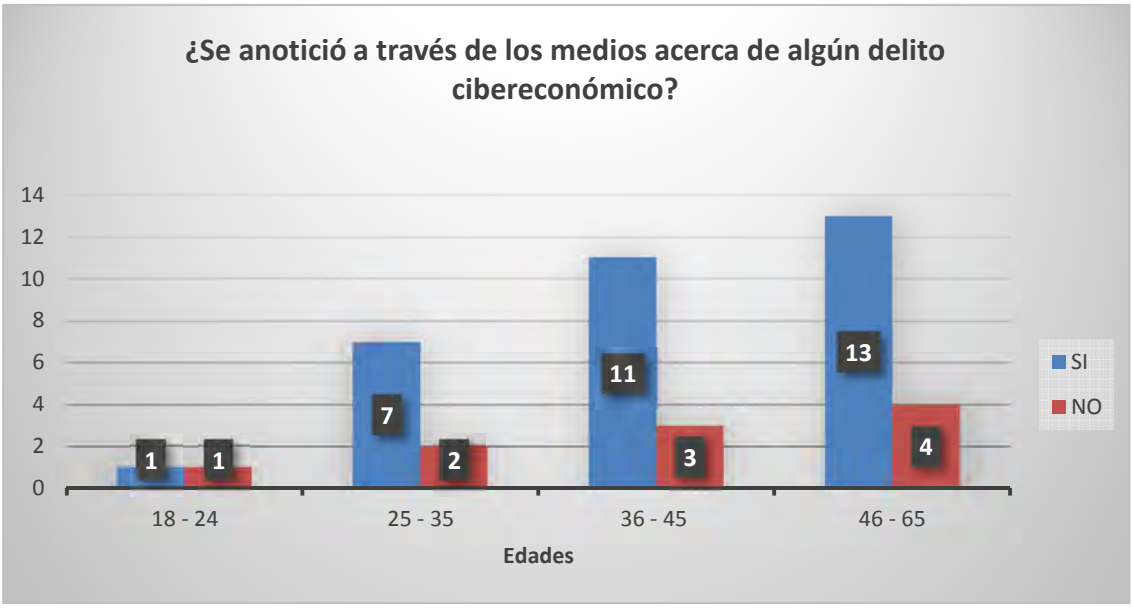

***6.- Fue favorable la respuesta que recibió por parte de la persona que lo atendió?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 0 | 1 | 3 | 3 |
| NO | 0 | 1 | 3 | 4 |



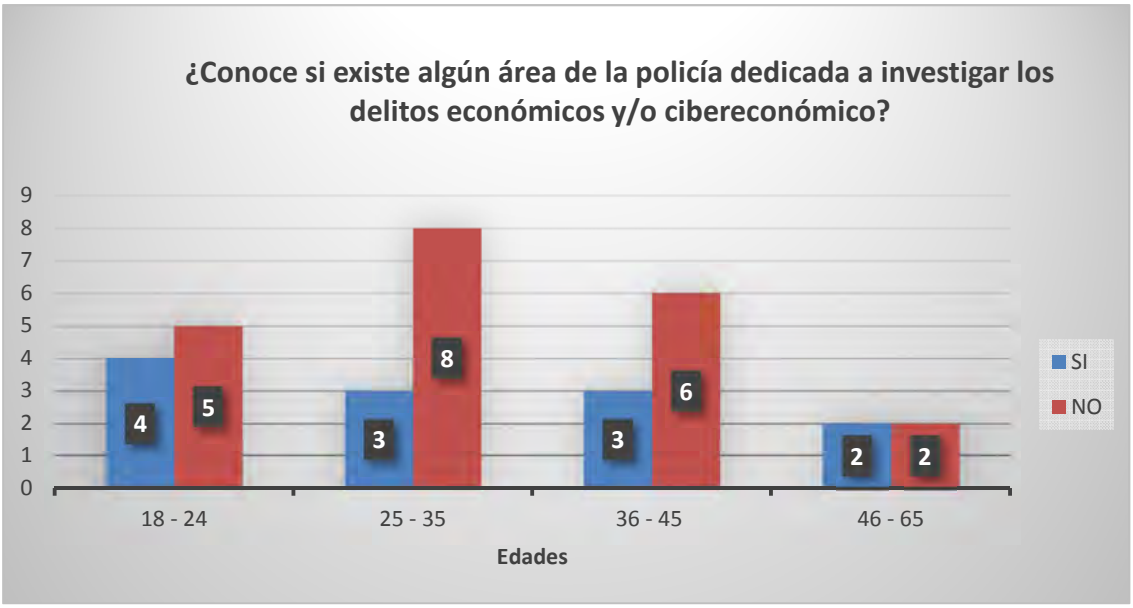

***7.- ¿Se anotició a través de los medios de comunicación acerca de algún delito cibereconómico recientemente o durante los últimos dos años?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 1 | 7 | 11 | 13 |
| NO | 1 | 2 | 3 | 2 |



***8.- ¿Conoce si existe algún área de la policía dedicada a investigar los delitos económicos y/o cibereconómicos?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 4 | 3 | 3 | 2 |
| NO | 5 | 8 | 6 | 9 |

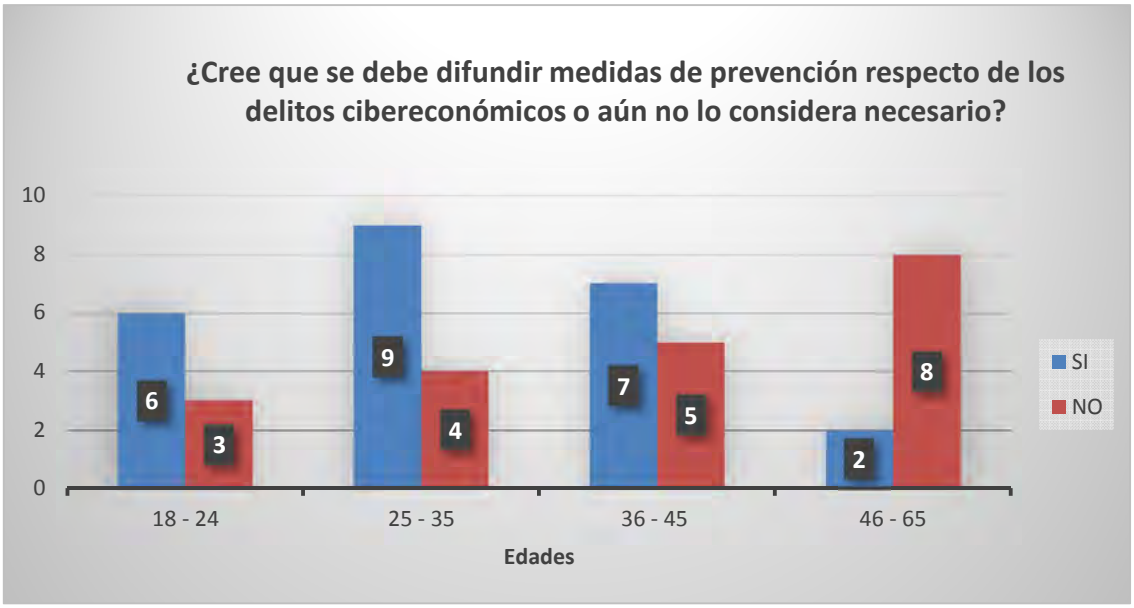



***9.- A su entender, ¿la policía se encuentra capacitada respecto a esta modalidad delictiva?***

| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 3 | 2 | 3 | 2 |
| NO | 7 | 6 | 9 | 8 |


***10.- ¿Cree que se debe difundir medidas de prevención respecto de los delitos cibereconómicos o aún no lo considera necesario?***

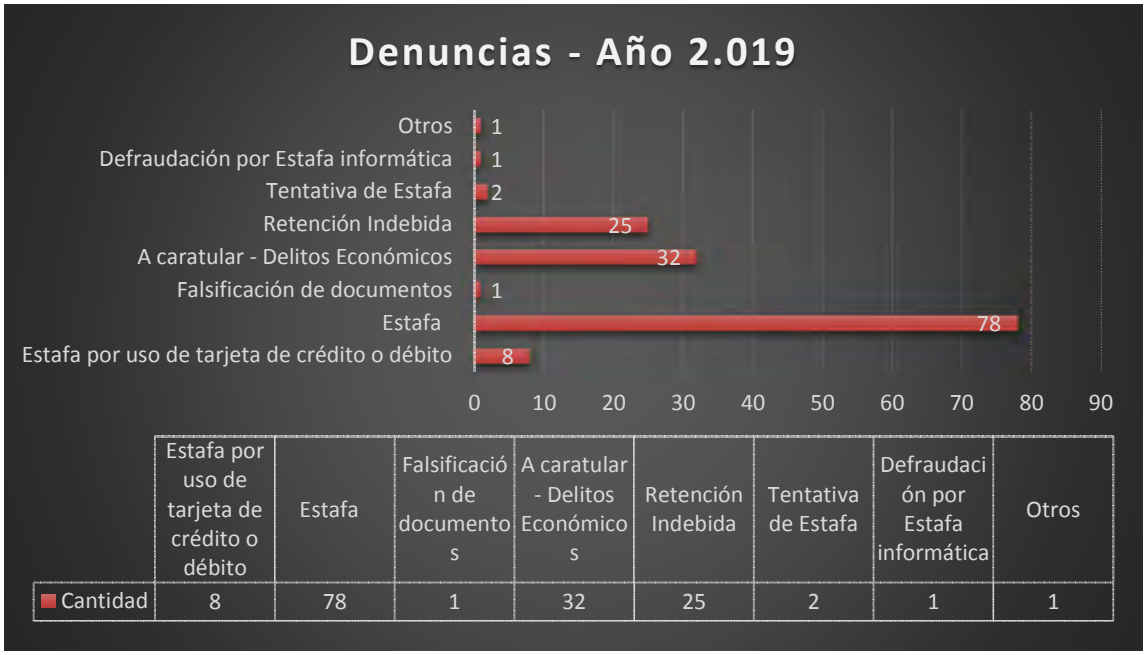
| Cuestionario | Edad | | | |
|---|---|---|---|---|
| | 18 - 24 | 25 - 35 | 36 - 45 | 46 - 60 |
| SI | 6 | 9 | 7 | 2 |
| NO | 3 | 4 | 5 | 4 |




## ESTADISTICAS DE LOS DELITOS ECONÓMICOS DENUNCIADOS EN LA DIVISIÓN DELITOS ECONÓMICOS

### HECHOS DENUNCIADOS EN EL AÑO 2.019 HASTA EL 29 DE ABRIL:

| Delito | Cantidad |
|---|---|
| Estafa por uso de tarjeta de crédito o débito | 8 |
| Estafa | 78 |
| Falsificación de documentos | 1 |
| A caratular - Delitos Económicos | 32 |
| Retención Indebida | 25 |
| Tentativa de Estafa | 2 |
| Defraudación por Estafa Informática | 1 |
| Otros (Circunvención de Incapaces/Amenazas) | 1 |
| Total de Delitos Denunciados | 148 |

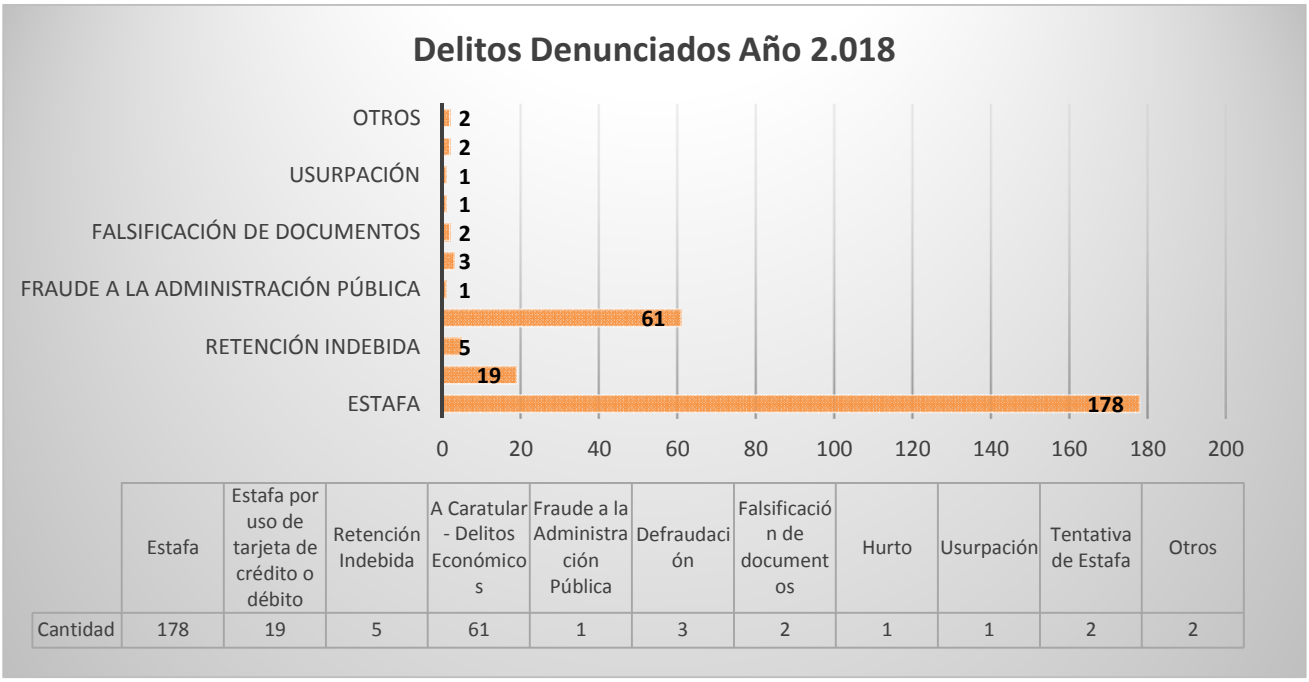



## ESTADISTICAS DE HECHOS DENUNCIADOS EN EL AÑO 2.018:

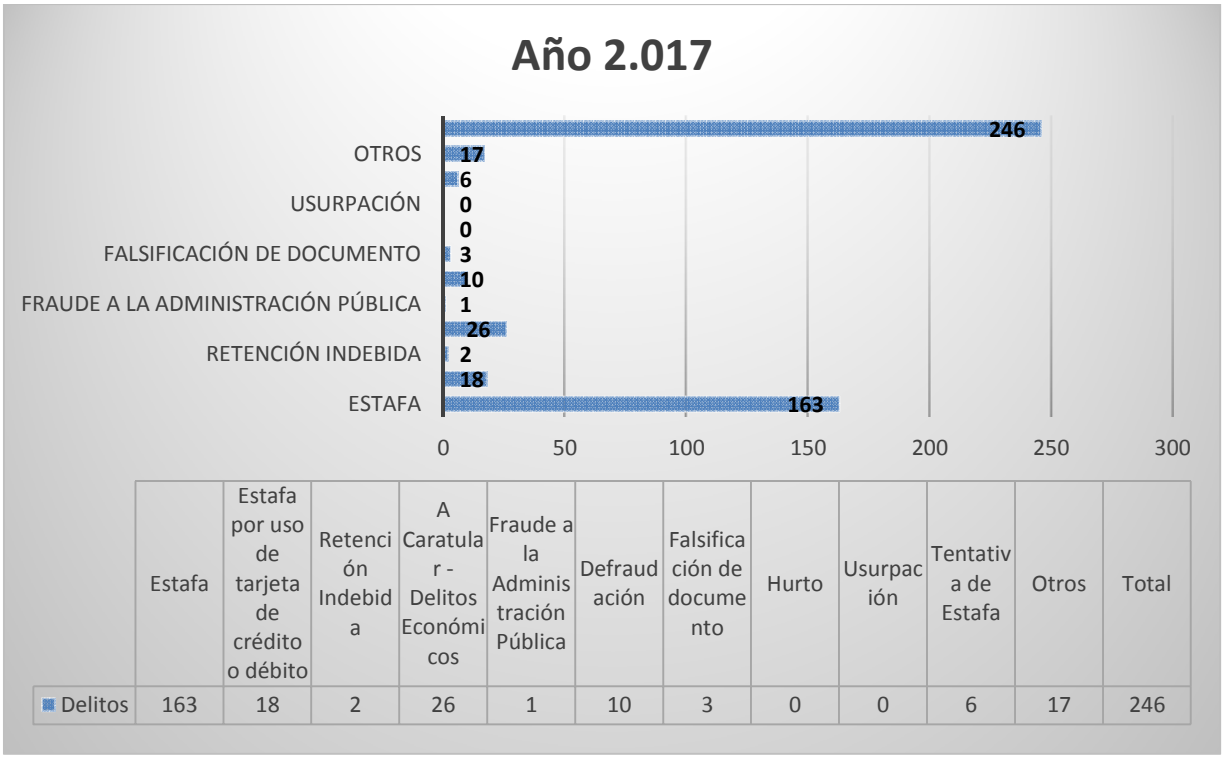
| Delitos | Cantidad |
|---|---|
| Estafa | 178 |
| Estafa por uso de tarjeta de crédito o débito | 19 |
| Retención Indebida | 5 |
| A Caratular - Delitos Económicos | 61 |
| Fraude a la Administración Pública | 1 |
| Defraudación | 3 |
| Falsificación de documentos | 2 |
| Hurto | 1 |
| Usurpación | 1 |
| Tentativa de Estafa | 2 |

| | |
|---|---|
| Otros | 2 |
| Total de Delitos Denunciados | 275 |

## ESTADISTICAS DE HECHOS DENUNCIADOS EN EL AÑO 2.017:



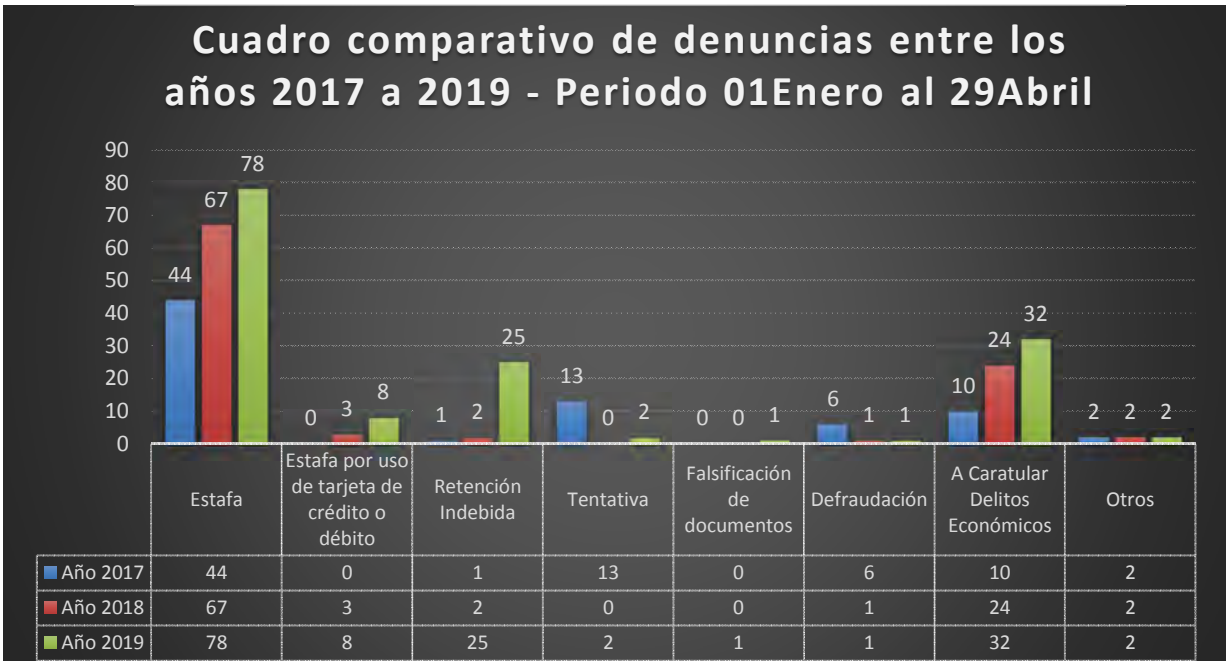

| | Estafa | Estafa por uso de tarjeta de crédito o débito | Retención Indebida | A Caratular - Delitos Económicos | Fraude a la Administración Pública | Defraudación | Falsificación de documentos | Hurto | Usurpación | Tentativa de Estafa | Otros |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cantidad | 178 | 19 | 5 | 61 | 1 | 3 | 2 | 1 | 1 | 2 | 2 |




| | Estafa | Estafa por uso de tarjeta de crédito o débito | Retención Indebida | A Caratular - Delitos Económicos | Fraude a la Administración Pública | Defraudación | Falsificación de documento | Hurto | Usurpación | Tentativa de Estafa | Otros | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Delitos | 163 | 18 | 2 | 26 | 1 | 10 | 3 | 0 | 0 | 6 | 17 | 246 |

**Cuadro comparativo de denuncias entre el periodo 01ENE al 29ABR entre los años 2.017 a 2.019**

| | Año 2017 | Año 2018 | Año 2019 |
|---|---|---|---|
| Estafa | 44 | 67 | 78 |
| Estafa por uso de tarjeta de crédito o débito | 0 | 3 | 8 |
| Retención Indebida | 1 | 2 | 25 |
| Tentativa | 13 | 0 | 2 |
| Falsificación de documentos | 0 | 0 | 1 |
| Defraudación | 6 | 1 | 1 |
| A Caratular Delitos Económicos | 10 | 24 | 32 |
| Otros | 2 | 2 | 2 |
| Total de Delitos Denunciados | 77 | 102 | 149 |




| | Estafa | Estafa por uso de tarjeta de crédito o débito | Retención Indebida | Tentativa | Falsificación de documentos | Defraudación | A Caratular Delitos Económicos | Otros |
|---|---|---|---|---|---|---|---|---|
| Año 2017 | 44 | 0 | 1 | 13 | 0 | 6 | 10 | 2 |
| Año 2018 | 67 | 3 | 2 | 0 | 0 | 1 | 24 | 2 |
| Año 2019 | 78 | 8 | 25 | 2 | 1 | 1 | 32 | 2 |

***Apreciaciones Generales:***

Desde mi experiencia personal como Oficial Subalterno de la Policía de la provincia de Salta, habiendo cumplido la función de “sumariante” y actualmente como Oficial Jefa, en el rol de Segunda Jefa de la División de Delitos Económicos, considero que las debilidades existentes están dadas por la falta de capacitación de los operadores a cargo de la investigación, pero no solo en lo que se refiere al personal policial a cargo de la instrucción de las actuaciones, sino también en quienes tienen a cargo el direccionamiento y supervisión de la investigación que se lleva a cabo.

Creo que desde el momento en que el ciudadano concurre a una dependencia policial a exponer un problema que, deviene con un perjuicio económico como lo es en el caso presentado, el encargado de recepcionar la denuncia debe estar correctamente instruído para comprender las circunstancias del hecho que se le expone y poder tipificar el delito, además de darla una respuesta pronta y favorable al ciudadano.

La denuncia, debe contener la información mínima y necesaria que le permita al sumariante poder iniciar una investigación preliminar e inmediata, sin tener que entrevistar nuevamente a la víctima para que deba relatarle el hecho.

Esta situación puede apreciarse frecuentemente en personal de comisarias con jerarquía de suboficiales que son sumariantes como también en los oficiales recientemente egresados o con cierta antigüedad, por cuanto a veces suele erróneamente confundirse la tipificación de un delito de “estafa” por “hurto”, o simplemente “a caratular”, en cuyo caso ni siquiera se logró identificar la conducta delictual o bien, el hecho denunciado no constituye delito.

En aquellos casos en que las denuncias son recibidas en unidad especiales, como lo son el Departamento Investigaciones, Brigadas de Investigaciones en el caso del interior de la provincia, Oficina de Orientación y Denuncia y en la propia División de Delitos Económicos, puede apreciarse los mismos errores de interpretación de las circunstancias de los hechos que se denuncian, o la imprecisión de información que permita realizar las primeras diligencias preliminares en pos de la identificación de los causante, ya que en algunos casos, esta situación genera demora y por ende puede resultar perjudicial para la investigación.

Para aseverar lo referido, a continuación se anexan capturas de imagen de fragmentos de una denuncia caratulada como “ESTAFA”, que fue recibida primeramente en la Comisaría y posteriormente, ampliación de la misma en la División de Delitos Económicos, puede apreciarse las circunstancias expuestas.

## DENUNCIA

CON PLENO CONOCIMIENTO DEL ART. 245 DEL C.P. (FALSA DENUNCIA), HACE SIMPLE PROMESA DE DECIR VERDAD DE TODO CUANTO SUPIERE Y LE FUERE PREGUNTADO, EXPRESANDO QUE:

EN LA FECHA SIENDO HS. 19:00 APROXIMADAMENTE RECIBIO UN LLAMADO TELEFONICO DE PARTE DEL SR. SEBASTIAN COLMAN, QUIEN SE IDENTIFICO SER EMPLEADO DEL BANCO MACRO, CONSULTANDOLE SI EL MISMO HABIA REALIZADO TRES TRANSFERENCIAS EN LA FECHA A DISTINTOS BANCOS, DESDE SU CUENTA BANCARIA A LO QUE EL DICENTE LE MANIFESTO QUE NO, CONSTATANDO A TRAVES DE LA COMPUTADORA QUE EFECTIVAMENTE SU CUENTA PRESENTABA EL FALTANTE DE DINERO. SE REALIZO UNA TRASFERENCIA DE ($45.000) CUARENTA Y CINCO MIL PESOS AL BANCO GALICIA AL CBU 0070199630004028210330 DESDE UNA IP: 5.62.59.81, LA SEGUNDA

AL BANCO GALICIA POR EL MONTO DE ($90.000) NOVENTA MIL AL CBU 0070116330004022680713 DESDE UNA IP: 5.62.59.83 Y LA TERCERA POR LA SUMA DE ($ 8500 ) OCHO MIL QUINIENTOS AL CBU 0720029888000037008918 DESDE UNA IP: 5.62.59.83 AL BANCO SANTANDER RIO. EL PERSONAL DEL

## AMPLIACIÓN DE DENUNCIA

EN LA CIUDAD DE BARCELONA, ESPAÑA. QUE AL MOMENTO DE QUE PERSONAS DESCONOCIDAS EFECTUARON LA OPERACIÓN, QUE EL DICENTE DESCONOCE TOTALMENTE, DE TRANSFERENCIA DE DINERO DESDE LAS CUENTAS DE CAJA DE AHORRO EN PESOS TENÍA UN SALDO DE PARA DÉBITO DE $ 5.000 PESOS Y EN LA OTRA EN OTRA $ 3.000 APROXIMADAMENTE. DESDE LA CUENTA DE CAJA DE AHORRO EN DÓLARES, TENÍA UN SALDO PARA DÉBITO DE U$S 12.700 (DOCE MIL SETECIENTOS DÓLARES) APROXIMADAMENTE. QUE LUEGO DE HABER RECIBIDO LA COMUNICACIÓN TELEFÓNICA DESDE LA CITADA ENTIDAD BANCARIA, ES DECIR, DE SEBASTIÁN COLMAN, QUIEN LE CONSULTÓ ACERCA DE LAS TRES TRANSFERENCIAS BANCARIAS, OBJETO DE LA PRESENTE DENUNCIA; PROCEDIÓ A REALIZAR UNA CONSULTA ACERCA DE SU ESTADO DE CUENTA POR INTERMEDIO DE LA APLICACIÓN DEL "HOME BANKING DEL BANCO MACRO", DÁNDOSE CON LA NOVEDAD DE QUE EFECTIVAMENTE, PERSONAS DESCONOCIDAS, HABÍAN REALIZADO TRASFERENCIA NO AUTORIZADA POR EL DICENTE DE DINERO Y CAMBIO DE MONEDA DE DÓLARES A PESOS. SI BIEN NO PUEDE PRECISAR, REFIERE QUE APARENTEMENTE LA TRANSFERENCIA POR EL MONTO DE $ 45.000 PESOS HABRÍA SIDO INHIBIDA AL IGUAL QUE LA DE $8.500,00 PERO LA OTRA RESTANTE, POR EL MONTO DE $90.000,00 SI AL NÚMERO DE CBU QUE YA FUE APORTADO OPORTUNAMENTE. PREGUNTADO: QUE MEDIO UTILIZA HABITUALMENTE PARA CONSULTAR LOS MOVIMIENTOS DE SUS CUENTAS YA MENCIONADAS, EXPRESA QUE HABITUALMENTE LO HACE DESDE SU TELÉFONO MÓVIL, COMPUTADORAS DE SU TRABAJO Y PERSONAL EN SU DOMICILIO; ADEMÁS DE AQUELLAS QUE SE ENCUENTRAN EN LA SUCURSAL Nº 133, SITO EN AV. BICENTENARIO DE LA PATRIA, EN DIAGONAL AL SHOPPING ALTO NOA. DESEA ACLARAR QUE SU ESPOSA, MARIA

**Soluciones:**

Para poder modificar estas circunstancias, considero que al menos una a dos veces de cada trimestre, los instructores a cargo de la recepción de denuncias, deberían tener un taller donde se evalúe la comprensión de texto y redacción escrita de cada uno de ellos, de manera tal que una vez que se observe los progresos satisfactorios, éstos puedan ser desafectados de dicho taller y tengan continuidad aquellos que evidencien tal necesidad. Esta capacitación podría estar a cargo de la Escuela Superior de Policía, o en su defecto, por los coordinadores de los sectores, quienes tienen una relación de directa del personal que le depende y podrán detectar fácilmente tal debilidad.

Asimismo, esto se podría reforzar en los cursos de capacitación que realiza el personal policial en condiciones de ascenso al grado superior inmediato y sería fundamental, que éstos talleres tengan mayor énfasis en las escuelas de formación.

Otra de las debilidades, son aquellos casos donde la primera intervención del operador no fue satisfactoria para la recolección de información o preservación de la escena, de acuerdo a la modalidad y tipo de delito que se investiga.

Esta situación podría salvaguardarse creando “protocolos de intervención” para hechos que son considerados de gravosos y complejos socialmente. Son considerados como tal, por el tipo de víctima (por ejemplo adultos mayores, capacidades diferentes, etc.), por el monto, por la repetición de conducta delictual y/o el impacto que causa en la comunidad en cuanto a la sensación de inseguridad que pudiera generar.

Estos protocolos deberán adecuarse de acuerdo a la modalidad en particular, para ello, se anexa un modelo de intervención para aquellos casos denominados operativamente como “Secuestros Virtuales”. (ANEXO 3)

Asimismo, considero que la herramienta más importante para poder prevenir cualquier tipo de delitos, son las recomendaciones que se puede hacer a través de los

medios masivos de comunicación. La difusión alcanza a todas las personas sin diferenciar clases sociales, edades, condiciones de instrucción, etc., pudiéndose impartir un mensaje claro, preciso, sintético e integrador, puesto que actualmente pueden utilizar otras herramientas que la sola entrevista, sino también videos interactivos que puedan ilustrar mejor a quienes va dirigido el mensaje como pueden ser personas de la tercera edad, personas con capacidades diferentes (ceguera o sordera), etc.

## CONCLUSIONES

En virtud de la nueva revolución tecnológica en la cual nos encontramos inmersos mundialmente; podemos concluir en que si bien a través de los medios de comunicación se ha ido difundiendo acerca de la existencia de los delitos cibereconómicos tales como skimming, pharming, malware, entre otros; es necesario que esta información sea frecuentemente recordada y no únicamente cuando se ha difundido la existencia de víctimas de delincuentes dedicados a este tipo de accionar delictivo.

Asimismo, debemos sumar a ello que muchas veces es el mismo sujeto pasivo, quien tampoco hace un uso adecuado, consciente y responsable de los medios tecnológicos para consigo o su entorno familiar más vulnerable, como pueden serlo los adultos mayores, adolescentes o niños, como es en el caso de grooming.

Es loable destacar que la modalidad delictual para la comisión de delitos cibereconómicos, telemáticos e informáticos no es pétrea ya que va mutando permanentemente al ir sofisticando las herramientas y conocimientos de quienes se dedican a pergeñar ideas en este ámbito, buscando tener anonimato su autor a través de la tecnología.

Además, debemos mencionar que no todos los delitos se perpetran de la misma forma ni está dirigido a las mismas víctimas; si bien podemos decir que existen patrones de coincidencia en algunos hechos denunciados con otros, como puede ser por ejemplo el uso de una página falsa o spam de “Mercado Libre”, “Plan Nacional de Viviendas”, “IPV”, etcétera; una vez que se inicia la investigación se van estableciendo parámetros y niveles de prioridad de acuerdo a la información que se vaya obteniendo de las evidencias digitales que pudieran existir y que posiblemente la víctima pudo haber preservado o probablemente, por desconocimiento, hubiera borrado.

Por todo ello, debemos concluir en que efectivamente es necesario y prioritario el perfeccionamiento y capacitación de los agentes encargados de investigar este tipo de delitos cibereconómicos e informáticos en general; por cuanto a través de ellos, en su carácter de auxiliar de justicia, serán el único camino que tendrá la justicia para poder determinar las conductas ilícitas en algún supuesto de los tipificados en nuestro Código Penal.

Amén de ello, como opinión personal, considero que nuestros legisladores deben ser capacitados también acerca de este tipo de delitos, de las distintas modalidades en que pueden cometerse y de las diferentes herramientas e inimaginables ardides que pueden utilizar las personas dedicadas a delinquir a través del uso de los medios tecnológicos; en virtud de que esta circunstancia hace que el grado de la víctima sea de mayor vulnerabilidad ante estas situaciones, sea por desconocimiento, confianza o simplemente porque no se encuentra en las mismas condiciones de igualdad en cuanto a capacidad en comparación con el sujeto activo.

Dicho ello, sostengo que por tal motivo debería considerarse como agravante el uso de los medios tecnológicos ante la comisión de este tipo de delitos, es decir, ante la existencia de un delito de ESTAFA y/o DEFRAUDACIÓN; teniendo en cuenta que ésta

es la única calificación legal prevista en nuestro Código Penal ante la existencia de un hecho delictivo que tenga como consecuencia el perjuicio económicos cometido, por ejemplo, mediante el uso de SKIMMING; o como es el caso de la modalidad delictiva, conocida socialmente como “PREMIOS VIRTUALES”, tipificado como ESTAFA, cuando en realidad nos encontramos ante un caso de SMISHING; no considerado de tal manera en nuestra legislación.

También se encuentra sumergida en esta laguna legal la falta de tipificación para el delito actualmente conocido y difundido a través de los medios masivos de comunicación por el área de la Dirección General de Investigaciones de la Policía de Salta como es la “SEXTORSION”, cuando en realidad se trata de un tipo de delito tecnológico, nominado como **PORNO VENGAZA** (**REVENGE PORN)** o **SEXTING**; encuadrado por nuestra legislación vigente únicamente como una EXTORSIÓN.

Concluyendo el presente trabajo, hago constar que efectivamente se confirma la hipótesis planteada, por cuanto de acuerdo a los estudios y análisis realizados, encuestas, como de los datos estadísticas que reflejan los hechos denunciados en materia de delitos económicos, se establece que necesariamente los operadores investigativos deben capacitarse permanentemente y actualizar los conocimientos ya adquiridos en materia de aquellos delitos que se cometieran mediante el uso de elementos informáticos y tecnológicos; por cuanto solo a través de ello, se podrá garantizar su esclarecimiento y evitar cualquier consecuencia que pudiera ocasionar la impunidad del accionar delictivo de quien comete este tipo de conductas.

Si bien, no debemos de dejar de considerar que al referirnos de “operadores investigativos”, es inevitable relacionar e identificar a los mismos únicamente con la figura de la fuerza de seguridad, en nuestro caso, con nuestra prestigiosa Policía de la Provincia de Salta, quienes en su función como “auxiliar de justicia”, realizan esta tarea

investigativa; pero la realidad y el estudio de este trabajo, ha llevado a determinar que estos “agentes”, no se limitan a los citados profesionales, sino también que deben capacitarse también quienes tienen a cargo dirigir este tipo de investigaciones y de juzgar las mismas y a quienes cometieron este tipo de conductas delictivas, es decir, la justicia, por cuanto todo debe complementarse y relacionarse entre sí, en beneficio de un solo objetivo, que es la protección de la sociedad.

También considero que al no existir una interpretación correcta en cuanto a los términos legales previstos en el artículo 173 inciso 16 de nuestro Código Penal, al referir en la tipificación de este tipo de delitos que prevé la figura de ***“quien defraudare a otro mediante cualquier técnica de manipulación informática…”***, y nos limitamos a interpretar como tal únicamente a las herramientas informáticas y no a las tecnológicas, como lo es un teléfono celular, el cual al poseer un software y por su función debiera ser incluido como tal en el citado supuesto legal, se proseguirá caratulando incorrectamente aquellas conductas de DEFRAUDACIÓN POR MEDIOS DEL USO DE ELEMENTOS INFORMÁTICOS (Art. 173 inc. 16) por el delito de ESTAFA (Art. 172). Si bien la pena es la misma en ambos casos, no permitirá proyectar a futuro a un legislador, que debiera considerarse como más gravosa el primer supuesto, debido a que el causante, valiéndose de herramientas que le permiten cierto anonimato, suplantación de identidad, en algunos casos no necesita encontrarse físicamente en el lugar del hecho por tiempo prolongados y se vale de elementos informáticos para la comisión de los mismos, puede exitosamente realizar su cometido y no ser identificado; lo que ocasiona socialmente una desprotección a la sociedad en este tipo de delitos informáticos.

Asimismo, al no existir fallos con condenas ejemplificativas para quienes fueron juzgados por éste tipo de delitos, sean ciudadanos argentinos o extranjeros, tampoco se podrá avanzar en este tipo de cuestiones judiciales.

Por último, hago constar que capacitando a nuestros miembros de la Institución Policial, podremos generar políticas de prevención dirigidas a la comunidad en general en lo que se refieren a delitos cibereconómicos, las que deberán ser difundidas a través de los medios de comunicación; además de crear protocolos de intervención proyectados a una eficiente y eficaz actuación por parte de nuestros efectivos policiales cuando la sociedad lo requiera en conductas ilícitas como las planteadas en el presente trabajo investigativo.

**Glosario.**

- **Cyberbulling:** es el uso de los medios telemáticos (internet, telefonía móvil y videojuegos online), para ejercer el acoso psicológico entre iguales. No se trata del acoso o abuso de índole estrictamente sexual ni los casos en los que las personas adultas intervienen.
- **Sexting o revenge porn** (porno vengativo): consistente en el contenido sexual explícito que se publica en internet sin el consentimiento del individuo que aparece representado. Mucho de este material es producido por la propia víctima y enviado al infractor a través de canales como whassapp, por ejemplo.
- **Grooming:** se trata de una serie de conductas y acciones emprendidas por un adulto con el objeto de ganarse la confianza de un menor de edad, creando una conexión emocional con el fin de disminuir las inhibiciones del menor y poder abusar sexualmente de él.
- **Pharming:** es la explotación de una vulnerabilidad en el software de los servidores DNS (o en el los equipos de los propios), que permite al atacante redirigir un nombre de dominio a otra computadora distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para el nombre de éste dominio.

- **Phishing:** Conocido también como suplantación de identidad. Es el modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.
- **Alterar:** del latín alterare, significa modificar, cambiar la esencia o forma de algo, trastornar, perturbar.
- **Sistema informático:** todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.
- **Transmisión de datos informáticos:** es toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.
- **Hacker:** es aquella persona especialista en alguna rama de la tecnología que es capaz de realizar intervenciones en redes, penetrando en bases de datos o sistemas informáticos que no son de acceso público. Si bien el término posee habitualmente una connotación socialmente negativa, ya que se lo emparenta con la figura de un pirata o un intruso, el hacker, al ser un especialista, trabaja también para desarrollar redes y sistemas más seguros.
- **Cracker:** el término “Cracker” literalmente traducido desde el inglés al español significa “romper o quebrar”. En este caso, se utiliza para referirse a las personas que rompen o vulnerar algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por un desafío personal. Mayormente, se enciende que los crackers se dedican a la edición desautorizada de software del propietario. Sin embargo, debe entenderse que si bien los ejecutables binarios son uno de los principales objetivos de estas personas, una aplicación web o

cualquier otro sistema informático representan otros tipos de ataques que de igual forma pueden ser considerados actos de cracking.

- **Keygens o key generators:** es un programa informático que al ejecutarse genera un código serial para que un determinado programa de software de pago en su versión de prueba pueda ofrecer los contenidos completos del programa ilegalmente y sin conocimiento del desarrollador. Normalmente los keygens son archivos ejecutables en formato *.exe, que se ejecutan sin necesidad de ser instalados. Suelen pesar muy poco, menos de 1 MB. Existen varios tipos de keygens, los normales pueden burlar la seguridad del programa pero también hay otros keygens que son más complejos y permiten desbloquear más aplicaciones.

  Si bien los keygen y crack se utilizan con el mismo objetivo, usan sistemas diferentes; mientras que el keygen es un ejecutable que genera un código o serial para poder desbloquear el programa, un crack simplemente hace una modificación sobre el programa para poder “completarlo”.

- **Piratería informática:** consiste en la distribución y/o reproducción ilegales de software.

- **Keylogger:** son un tipo de software que almacena todo registro ingresado a través de un teclado de computadora. Es un término derivado del inglés “key” que significa “tecla” y “logger” de “registro”. El objetivo de quien manipula este software es conocer los movimientos y la información que el usuario portador del malware registra en su ordenador personal.

- **Criptomoneda:** es un tipo de moneda digital pero no son únicas. Las criptomonedas son, un subconjunto de las monedas digitales basadas en la criptografía. El prefijo cripto, proviene de la palabra griega “kruptos” que significa oculto, secreto. Criptografía es el estudio de métodos de encriptación de información, principalmente utilizados para

enviar un mensaje de manera segura y privada, y la para la seguridad y autentificación de datos.

**Referencias / Bibliografía**


- Código Penal de la República Argentina.
- Ley de Delitos Informáticos Nº 26.388/08.
- Ley de Protección de Datos Personales Nº 25.326/00.
- Convenio sobre ciberdelincuencia.
- www.justiciasalta.gov.ar
- https://es.wikipedia.org/wiki.
- www.oroyfinanzas.com.
- www.xataca.com
- www.infotechonoly.com
- https://www.youtube.com
- http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa2.shtml
- Base de datos de la División Delitos Económicos.

**ANEXOS:**

- Anexo 1:

  Video ilustrativo acerca de una página de Mercado Libre mediante la cual se solicita a la víctima que reingrese datos personales. Datos que posteriormente serán utilizados por el sujeto activo que efectuó dicho programa.

- Anexo 2:

  Video ilustrativo acerca de la colocación de un dispositivo de skimming en un cajero automático del país de Chile.

- Anexo 3:

  Modelo de protocolo de intervención.

## ANEXO 3

## *"MODELO DE PROTOCOLO DE INTERVENCIÓN PARA SECUESTROS VIRTUALES".*

### *TEMA DE INVESTIGACIÓN: "SECUESTROS VIRTUALES"*

El presente trabajo está pensado desde una perspectiva analística, con la finalidad, de que pueda ser una herramienta de utilización en situaciones prácticas y reales, no solamente por especialistas en materia de seguridad pública o fuerzas de seguridad y/o policiales, sino también, dándole un ámbito de adecuación y practicidad desde la capacitación, a fin de que se instruya a los ciudadanos de cómo deben proceder ante una situación de la propuesta.

Basada en la premisa que a través de la capacitación por intermedio de un protocolo de intervención dirigido a las fuerzas policiales de seguridad y adecuado pedagógicamente para los establecimientos educativos, además de la difusión del mismo en los medios de comunicación a la ciudadanía en general, podremos evitar que personas de esta provincia o de otras, delincan en nuestra provincia y principalmente en nuestra ciudad, realizando "EXTORSIONES" mediante el uso de los teléfonos, conocidos como "SECUESTROS VIRTUALES"; se ha considerado proyectar la presente investigación.

Cabe mencionar que al tratarse el presente proyecto de un protocolo de intervención no posee hipótesis.

- Descripción de la situación problemática:

En los últimos tiempos, tanto en los medios de comunicación nacional como provincial, he podido observar que muchos ciudadanos fueron víctimas de hechos conocidos, consuetudinariamente, como “SECUESTROS VIRTUALES”, lo que en realidad son delitos legalmente configurados como “DELITO DE EXTORSIÓN”.

Este tipo delitos han originado que las víctimas, muchas veces actuando en estado de crisis o shock, por la situación planteada que es el ardid utilizado por parte de los delincuentes, llevan a que se puedan desencadenar otros hechos preterintencionales o culposos, ya que ante la desesperación para la obtención de dinero conducen con menores o en elevada velocidad, pueden atropellar alguna persona, al recibir la comunicación pueden sufrir algún tipo de ataque u ocasionárselo a otro familiar que se anoticie de ello, etc.; es por ello que lo considero el estudio de este tipo de delitos como una situación problemática que puede generar a veces desenlaces fatales o gravemente perjudiciales; o en su defecto, ser únicamente estadístico si es que la víctima se percata de la situación y corta la comunicación.

- Delimitación del problema:

La presente investigación está dirigida a establecer en el ámbito jurisdiccional de la ciudad de Salta, un protocolo de intervención que pueda ser destinado a la fuerza policial de seguridad, como así también, con una manera más pedagógica, a los establecimientos educativos con la finalidad de crear como medida de seguridad la “prevención” tanto en la seguridad pública como fomentando en quienes se encuentran en crecimiento y serán los futuros actores que se desempeñarán en nuestra sociedad.

Asimismo, a través de los medios masivos de comunicación, estaríamos también dirigiendo ésta importante herramienta a la comunidad y a la familia.

- Planteo del problema.

El problema planteado, consiste en que personas desconocidas, a través de una modalidad delictual debidamente definida por ellos, consistente en comunicarse telefónicamente a una vivienda elegida al azar, indagando sobre las personas que se encontrarían ausentes, por lo que realizan la misma en el horario comercial. Seguidamente se identifican como integrantes de algún organismo de emergencia, tales como las fuerzas de seguridad (policía, personal de tránsito) o de la salud, utilizando tal ardid para que la potencial víctima brinda datos, poniéndola en una situación de preocupación y nerviosismo, refiriéndole que alguno de los familiares ausentes habría sufrido algún tipo de accidente vial o fatalidad. Desde allí, al encontrarse la víctima en total vulnerabilidad, brinda toda la información requerida, la cual es utilizada maliciosamente por el delincuente, quien finalmente termina el relato de la situación conflictiva expresando que en realidad se trataría de “UN SECUESTRO”, coaccionando para la liberación del supuesto “secuestrado”, sumas de dinero.

- Objetivos de la investigación:

Objetivos generales:

- Crear una herramienta que permita evitar que las personas sean víctimas de delito de extorsión, cometido mediante el uso de los teléfonos.
- Elaborar un instructivo, dirigido a la comunidad en general, para proceder en caso de recibir un llamado telefónico extorsivo.

Objetivos específicos:

- Determinar el perfil delictual de la persona que se dedica a cometer este tipo de hechos.
- Características personales (sexo, edad, grado de instrucción, situación económica, etc) y fisonómicas y sociales de las personas que cometen este tipo de delitos.
- Determinar si son asociaciones ilícitas u organizaciones criminales.
- Determinar las características de la modalidad delictual
- Diferencias determinantes entre las características del resto de quienes delinquen y buscan una remuneración dineraria.
- Determinar el ámbito o sector de la población mayormente vulnerable en este tipo de hechos delictuosos.
- Establecer herramientas o mecanismos que permitan prevenir la comisión de este tipo de delitos.

➢ Fuentes del problema:

Para la investigación efectuada, se procedió a recopilar información en los registros existentes de la División Delitos Económicos de la Policía de la Provincia de Salta, respecto a la cantidad de hechos denunciados formal o verbalmente, sea en las dependencias policiales o al sistema de emergencia (9-1-1), de ciudadanos que hayan sido víctimas del delito de “extorsión”, específicamente cometidos mediante el uso de teléfonos, tanto celulares como fijos; dentro del periodo comprendido entre el mes de enero a diciembre del año 2.018 y ocurridos en la ciudad de Salta.

Con los datos obtenidos, se procedió a efectuar una recopilación sistemática de la información, determinándose que las personas que se dedican a realizar éste tipo de actividad delictual, utilizaban generalmente ambas líneas telefónicas de las víctimas, es decir, teléfono celular y fijo, a fin de impedir que éstos soliciten ayude; además de

tratarse de personas de sexo masculino, con voz con acento “porteño” o “cordobés”, que realizaban las llamadas desde “números privados”, identificándose siempre como integrante de algún organismos de seguridad o emergencia públicos, como lo son la policía de seguridad, tránsito o médicos del Samec y, mediante el engaño de que habría ocurrido algún siniestro vial protagonizado por algún integrante ausente del grupo familiar a la residencia donde efectuaron la llamada, pese a haber sido seleccionada la víctima al azar.

Al utilizarse este tipo de ardid por parte de éstos delincuentes, ocasiona en la víctima que ha recibido el llamado teléfono una situación de vulnerabilidad, de manera tal que inconscientemente brindará información personal sobre sí misma y su grupo familiar, la cual será utilizada maliciosamente por quien se encuentra cometiendo el delito en cuestión al referirle, tras la obtención de estos datos, que el accidente sería irreal y que “en realidad” se trataría de un “secuestro”, para lo cual procedería a extorsionarlo por la falaz liberación del familiar ausente a cambio de dinero; posicionándose así en una situación de “poder”, y manipulación respecto al primero, por lo que lE obliga a no cortar la comunicación y se le proporcione un número de teléfono celular para no interrumpir la comunicación y extorsión.

Al producirse este tipo de situaciones, generalmente, quien ha sido víctima de éste tipo de hechos y ha creído en la artimaña de la cual está siendo objeto, con la finalidad de que no se atente con la integridad física y vida de su ser querido y la premura de conseguir dinero y encontrándose en situación de crisis, suele salir de su vivienda sin rumbo definido peatonal o vehicularmente, atentando también en su proceder contra terceros que desconoce tal situación pudiendo ocasionarse una tragedia.

Con los datos obtenidos, ya se puede determinar un padrón respecto del artificio que utilizan éstas personas para cometer este tipo de delitos, como así también de un

posible perfil de los mismos; además de evaluarse la necesidad de encontrar una herramienta preventiva en el marco de la seguridad pública y ciudadana que pueda prevenir este tipo de problemáticas. Independientemente de ello, también se podrá analizar el efecto social que ocasionada la modalidad delictual planteada y conceptualizar desde lo general, la sociología criminal de quienes se dedican a esta actividad ilícita.

El enfoque metodológico seleccionado para utilizar, es el “combinado cualitativo/cuantitativo”; en virtud de que la metodología deductiva está prevista en que se está trabajando en algunos y casos determinados, sociales y empíricos, tendiente a teorizar, comprender y construir esquemas conceptuales adecuados a los hechos reales objetos del estudio; es decir, que se trabaja desde la realidad estudiada. No se está buscando explicar sino comprender porque las personas que delinquen en la modalidad estudiada lo hacen, cuál el al ámbito elegido para hacerlo y conceptualizar el perfil de los mismos.

Es también cuantitativo, en razón de estudiarse, analizarse, difundirse y practicarse un protocolo de intervención orientada a la prevención de la seguridad pública para los delitos de extorsión en lo que puntualmente respecta a los denominados “secuestros virtuales”, se podrá evitar que existan más víctimas objetos de éste ardid. Esta situación podrá demostrarse estadísticamente al valorarse los índices de denuncias formales y verbales registradas en las dependencias policiales o en el sistema de emergencia, si es que han disminuido considerablemente tras la implementación y difusión del protocolo o no.

• Selección del Universo:

La población objeto de estudio serán dos. Primeramente, se estudiarán los sujetos que utilizan están modalidad para delinquir, si actúan solos o en grupo u

organizaciones, el perfil personal y social del/los mismo/s en cuanto al sexo, edad, grado de instrucción, situación personal, lugar de residencia, estado financiero y económicos, etc.

En segundo lugar, las víctimas, si es que éstas fueron elegidas al azar o por la zona de residencia que puede ser indicador del poder adquisitivo o no, por el horario en que se efectúa la llamadas se busca que las personas se encuentran solas, para que se facilite la comisión del ardid, el perfil social de la víctima (grado de instrucción, vecindario).

•Unidades de análisis:

En virtud de que el enfoque metodológico es combinado cualitativo/cuantitativo, se procederá a seleccionar como objeto de estudio algunos casos que sean representativos en cuanto a su modalidad, víctima elegida y resultado, y además que por su contenido sean de interés para el estudio de la presente investigación.

Asimismo, desde el enfoque del estudio cuantitativo se tomarán números fidedignos de un determinado lapso donde se registraron hechos denunciados en la modalidad estudiada.

• Tipo de muestreo.

El tipo de muestreo seleccionado es el “muestreo teórico”, puesto que si bien se busca teorizar, también se colecciona, codifica y analiza los datos empíricos que serán previamente seleccionados y objeto de estudio. A través de éste se procederá a explorar en profundidad el perfil de las personas que se dedican a delinquir en esta modalidad, herramienta que también será útil para el protocolo a realizar. Será a través de este muestreo y del estudio probabilístico, los que determinarán con valores y resultados si a través de la implementación y capacitación con este protocolo se ha logrado disminuir, incrementar o sigue igual el índice de víctimas.

Para la realización del presente tema de investigación, he seleccionado como técnica de recolección de la información, la “ENCUESTA”.

Tal selección obedece a que la encuesta, es un procedimiento mediante el cual se podrá obtener de manera directa información por parte de los sujetos hacia el investigador, lo que traerá celeridad y premura los resultados que podrán ser posteriormente evaluados y poder concluir la investigación con datos empíricos pero por sobre todo, actualizados, es decir, que sean concordantes con la realidad diaria que está vivenciando la ciudadanía y no que sea solamente un trabajo que pueda ser considerado cuantitativamente o estadístico en este tipo de tareas.

Si bien la encuesta puede recopilar de manera indirecta datos cualitativos, éste no será el fin, puesto que con la información que se obtenga se pretende describir, analizar y establecer las relaciones existentes entre sectores particulares o no, de la comunidad que será objeto de la investigación, siendo en éste caso en particular, de quienes residen en la ciudad de Salta.

Así mismo, para la realización de la encuesta, se considerará como técnica de recopilación de datos a los cuestionarios, los cuales no solo permiten que la recolección sea de manera ágil, sino también que sea puntualizada puesto que se está dirigiendo hacia donde está especificando el aporte de la información que deban brindar los encuestados. Este proceder también favorece el análisis de la misma, puesto que se lo efectuará en menor tiempo, tendiendo a la eficacia y eficiencia en la elaboración del proyecto.

En razón de encontrarse determinado la extensión espacial o localización al cual está dirigido el presente proyecto, es decir, a quienes residen en la ciudad de Salta, se está determinando el grupo selecto y objeto del presente trabajo de investigación. Al estar definido tal situación se podrá dividir el mismo por sectores, de forma tal que se

planifique “dónde, cómo y cuándo”, o si será de manera simultánea, que los grupos habitacionales selectos para la realización de la encuesta lo realicen dentro del mismo lapso, con la finalidad de que las respuestas no varíen en cuanto a la temporalidad.

La problemática a resolver con el presente proyecto, surge en razón de tenerse como fuentes de información, datos de personas que han denunciado de manera formal o telefónica dando aviso al sistema de emergencia, que fueron víctimas del delito de extorsión mediante el uso del teléfono, conocido como “secuestros virtuales”; por lo que los cuestionarios serán dirigidos principalmente a éstos mismos denunciantes, de forma tal que ellos sean los primeros a quienes se está dirigiendo esta herramienta de prevención.

En este caso la encuesta sería “vía on line”, es decir, a través del uso de correos electrónicos, con la finalidad de que las personas seleccionadas a responder puedan realizarlo en algún momento libre o cuando sientan deseo de hacerlo, no demándales demasiado tiempo ni esfuerzo puesto que podrán ser respondidos por la misma vía; la cual será posteriormente cargada en una base de datos que su correspondiente análisis.

El cuestionario a realizarse será del tipo cerrados, puesto que se tratarán de alternativas o respuestas previamente delimitadas, por lo cual deberán circunscribirse a ellas; con la particularidad de que tendrá un acento de heterogéneo, puesto que entre los interrogantes, se les efectuará una del tipo abierta, por ejemplo: “ud. considera que existen otras herramientas preventivas, fuera de las propuestas por la fuerza de seguridad, para combatir esta problemática?. En caso afirmativo, fundamente.”; de manera tal que se puedan obtener infinidad de alternativas a tal respuesta y sirvan para que el análisis sea también proyectado a futuro, determinando para el presente trabajo sus fortalezas, debilidades, oportunidades y amenazas.

Para mayor ilustración, se anexa al presente un modelo del cuestionario a realizarse para el presente proyecto.

Conclusión:

Se concluye que mediante la prevención, difusión y concientización de todos los ciudadanos, se podrá neutralizar el accionar de las personas que se dedican a cometer este tipo de actividad ilícita hasta instaurar una conducta positiva en la sociedad que tienda a hacer desaparecer este tipo de delito.

Por ello, al instruirse a la ciudadanía convenientemente a través de un protocolo de intervención para este tipo de problemática, objetivo de estudio, se podrá evitar que personas que se dediquen a cometer este tipo de hecho utilizando factores tales como “sorpresa”, grado de instrucción respecto a éste tipo de modalidad, temor, vulnerabilidad, entre otros; atenten contra la tranquilidad y la paz social de la ciudadanía.

Así mismo, a través del estudio estadístico existente, se podrá ir evaluando a través de la misma fuerza de seguridad policial que brindo la fuente de información problemática (Policía de Salta), si la conducta delictual y el perfil de quienes cometen éstos delitos se ha modificado o no y de ser así, cuál sería su graduación en cuanto a las consecuencias sociales para poder crear los mecanismos de prevención y seguridad pública necesario; como así también determinar si ésta problemática empírica, ha disminuido en cuanto a sus denuncias o personas que hayan sido víctimas, pese a recibir otros llamados telefónicos por parte de éste tipo de delincuentes.

Si bien, se concluye favorablemente respecto al presente proyecto, se considera que no se puede dar por sentada una única difusión sino que deberá proyectarse a futuro que éste se renueve en caso de conocerse que la modalidad delictual vaya

mutando; pero también porque la memoria de las personas pueden ser frágiles y de no difundirse periódicamente esta herramienta de prevención a través de los medios de comunicación, seguirán existiendo personas que puedan ser víctimas de este tipo de delitos.

**ANEXO**

**Cuestionario:**

Edad: Sexo:

Barrio donde reside:

1. Sufrió o fue víctima alguna vez de un secuestro virtual?
2. Si lo fue, denunció el hecho?
3. Cómo? (En la comisaría o al sistema de emergencia 9-1-1)
4. Cuándo?
5. Conoce de alguien cercano a Ud. que lo haya sido?
6. Sabe si denunció el hecho? Cómo y cuándo?
7. Qué hizo cuando recibió este tipo de llamada?
8. Sabía que se estaban suscitando éste tipo de hechos en la comunidad?
9. Sabía cómo debía actuar?

10. Le dio conocimiento de ello a alguien?
11. Cómo actuó la policía respecto al planteo de su problema?
12. Cómo espera que esta fuerza de seguridad actúa?
13. Si tiene hijos, les enseñó qué hacer ante este tipo de situación?
14. Considera necesario que éstos sea difundido en los medios masivos de difusión?
15. Considera que los niños y jóvenes en edad escolar deben recibir este tipo de información?
16. Se concientiza en su hogar respecto del uso del teléfono y de la información que se debe y no debe brindar ante un desconocido?
17. Ud. como piensa que se puede evitar o contrarrestar la comisión de este tipo de hechos?