ISBN: 978-628-95207-4-3. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2023.1.1.1274

Victimization study of cybercrime related fraud and scams in the city of Mar del Plata, Argentina

Ana Haydée Di Iorio, Eng[1], Santiago Trigo, Eng.[2], Bruno Constanzo, Eng.[3], Julieta Elvira Campero Mateos, Lic.[4]
[1,2,3] *Facultad de Ingeniería Universidad FASTA, Mar del Plata, Argentina*
diana@ufasta.edu.ar, santiagotrigo@ufasta.edu.ar, bconstanzo@ufasta.edu.ar
[4] *Facultad de Periodismo y Comunicación Social, Universidad FASTA, Mar del Plata, Argentina* julietacampero@ufasta.edu.ar

Abstract–.The digital transformation of organizations, accelerated by the COVID 19 pandemic, forced millions of people to use different technological tools to continue carrying out their daily activities, such as making purchases, banking procedures or maintaining social interactions. This situation generated an increase in cybercrime, specifically cyber scams and cyber fraud, however, in Argentina there are no official statistics in this regard. This paper presents a victimization study carried out during the year 2021 in the city of Mar del Plata, Argentina in order to investigate and collect information on the commission of crimes mediated by technology, in order to contribute to the design of crime policies. public safety, as a first situational diagnosis.

Keywords- cybercrime - cyber fraud - cyber scams - victimization study - cybersecurity

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Estudio de victimización sobre la comisión de delitos informáticos vinculados a fraudes y estafas en la ciudad de Mar del Plata, Argentina

Ana Haydée Di Iorio, Eng[1], Santiago Trigo, Eng.[2], Bruno Constanzo, Eng.[3], Julieta Elvira Campero Mateos, Lic.[4]
[1,2,3] *Facultad de Ingeniería Universidad FASTA, Mar del Plata, Argentina*
diana@ufasta.edu.ar, santiagotrigo@ufasta.edu.ar, bconstanzo@ufasta.edu.ar
[4] *Facultad de Periodismo y Comunicación Social, Universidad FASTA, Mar del Plata, Argentina* julietacampero@ufasta.edu.ar

Resumen– La transformación digital de las organizaciones, acelerada por la pandemia de COVID 19 provocó que millones de personas se vieran obligadas a utilizar diferentes herramientas tecnológicas para continuar desarrollando sus actividades cotidianas, tales como realizar compras, trámites bancarios o mantener interacciones sociales. Esta situación generó un aumento de los delitos informáticos, específicamente de las ciber estafas y los ciberfraudes, sin embargo, en Argentina no hay estadísticas oficiales al respecto. Se presenta en este trabajo un estudio de victimización realizado durante el año 2021 en la ciudad de Mar del Plata, Argentina con el objeto de investigar y relevar información sobre la comisión de delitos mediados por la tecnología, a fin de aportar al diseño de políticas de seguridad pública, como un primer diagnóstico situacional.

Palabras claves: Delitos Informáticos - ciberfraude - ciberestafa - Encuesta victimización - Ciberseguridad

I. Introducción

"Los delitos informáticos o ciberdelitos pueden ser entendidos como todas aquellas conductas antijurídicas, ilícitas o ilegales que vulneran derechos o libertades de las personas y utilizan un dispositivo informático como medio para la comisión del mismo, o el mismo es el fin del delito."(Sain, G; 2021:1) [1].

La transformación digital de las organizaciones, acelerada por la pandemia de COVID 19 provocó que desde comienzos de 2020 millones de personas se vieran obligadas a utilizar diferentes herramientas tecnológicas para continuar desarrollando sus actividades cotidianas, tales como realizar compras, trámites bancarios o mantener interacciones sociales.

En ese marco el uso de la tecnología como medio o como fin para cometer delitos también ha aumentado exponencialmente.

No existen hasta el momento estadísticas oficiales en el Ministerio Público de la Provincia de Buenos Aires, Departamento Judicial de Mar del Plata, sin embargo, los funcionarios de las fiscalías que tratan estos temas coinciden que los delitos informáticos registraron un incremento de entre un 700% y 800% con respecto al año 2019 [4].

No obstante, se carece de datos precisos que permitan determinar las particularidades de este tipo de hechos, debido a que los mismos no se encuentran categorizados de manera detallada.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

predominando las bancarias; las extorsiones sexuales, la distribución de material de abuso sexual infantil, el grooming y actos de violencia, destacándose la violencia de género digital [5].

Los delitos informáticos o delitos cometidos a través de medios digitales, presentan una elevada cifra negra, es decir, que muchos de ellos no se denuncian, y por tal razón, no se encuentran asentados en las estadísticas oficiales [6, 7]. De acuerdo a Saín [8] existen varios factores que explican por qué estos hechos no se denuncian, entre las que se destacan:

1. El desconocimiento de las personas que están siendo víctimas de un delito informático.
2. El temor de las empresas ante la posibilidad de ver afectada su imagen y reputación y/o también evitar multas o sanciones penales o administrativas, ante la ocurrencia de un ciber incidente de seguridad.
3. Las resoluciones técnicas y administrativas de una gran cantidad de delitos, lo que evita la judicialización de los mismos.

Este estudio novedoso en la región, realizado por el Observatorio Universitario de la Ciudad de la Universidad FASTA, tuvo como objeto investigar y relevar información sobre la comisión de delitos mediados por la tecnología en la ciudad de Mar del Plata.

Para esto se encuestaron 500 personas residentes en la ciudad de Mar del Plata, de manera presencial con el fin de conocer su percepción de la seguridad, detectar potenciales víctimas, determinar los canales adecuados para prevención y concientización, conocer las medidas de seguridad adoptadas, cuantificar los tipos de delitos sufridos y explorar el nivel de cifra "negra" de los mismos. No hay registros sobre la realización de estudios de victimización de este tipo en la región.

Este trabajo fue realizado de manera conjunta por el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) y las Facultades de Ingeniería y de Ciencias Jurídicas y Sociales de la Universidad FASTA.

El informe se encuentra dividido en tres secciones. En la primera sección, se indaga sobre las medidas de seguridad que adoptan los ciudadanos al navegar o realizar trámites online y sobre si se sienten o no seguros al utilizar este tipo de herramientas. En segundo término, se presentan datos sobre cuáles son los medios que la sociedad utiliza para informarse

sobre este fenómeno a los efectos de direccionar los mecanismos de prevención y concientización. Por último, se indaga sobre si los encuestados fueron víctimas de algún delito y, se pregunta sobre las reacciones frente a esas circunstancias. Es importante destacar que, para en este estudio sólo se trabajó sobre los delitos informáticos relacionados a los fraudes bancarios, accesos indebidos, robos de identidad, estafas informáticas y defraudaciones en general dejando de lado para estudios posteriores todo lo relacionado a violencia digital.

II. Metodología

A. Diseño del Instrumento

En el trabajo de campo se utilizó como técnica la encuesta semi estructurada, dado que permite recolectar y obtener datos de forma sistemática. Como instrumentos se empleó un cuestionario dividido en 3 secciones troncales con 21 preguntas en total.

La primera de ellas indaga sobre las características del encuestado, tales como sexo, edad, estudio adquiridos y ocupación. Por otra parte, intenta conocer la frecuencia con la que los encuestados acceden a Internet, así como también desde qué lugar y qué dispositivos utilizan sumado a las actividades que realizan a la hora de utilizar los medios digitales. También se indaga por el grado de preocupación que tienen los encuestados sobre realizar ciertas actividades a través de medios digitales, como así también, las medidas que adoptan para que no se vean vulnerados sus activos digitales.

La segunda sección, indaga sobre los medios utilizados para informarse sobre este tipo de cuestión y qué nivel de confianza le asigna a cada uno de ellos.

Por último, la tercera sección, indaga sobre el grado de victimización de los encuestados, a saber, tentativas -intentos- de delitos informáticos que han recibido, pasando luego por la experiencia personal o de terceros que han sufrido delitos de esta índole, en los que se destacan los accesos indebidos, consumos con tarjetas indebidos, robos de identidad, robo de criptomonedas, entre otros. Esta misma sección, posteriormente indaga sobre el modus operandi, si lo conoce, por el cual fue víctima de un delito. Ya sea, recibiendo una llamada telefónica, conectándose por redes sociales con una cuenta supuestamente oficial, accediendo a un sitio de compra venta, entre otros.

Luego, se consulta sobre cuáles fueron las medidas realizadas una vez que, el encuestado, advirtió que fue víctima de un delito, destacándose el contacto con la red social, haciendo la denuncia, entre otras opciones, intenta determinar si los encuestados conocen los canales oficiales para denunciar este tipo de delitos informáticos.

B. Perfil de la muestra

La población de la ciudad de Mar del Plata según el censo del año 2022 es de 682.605 habitantes [9]. En esta línea se trabajó en base a una muestra integrada por 503 personas con al menos 18 años cumplidos, de las cuales el 56,3 % es femenino y el 43,7% masculino.

El porcentaje de encuestados se distribuyó de una manera lo más heterogénea posible con respecto al rango etario, para que los resultados reflejen o se aproximen a la realidad. Así el 5% de los encuestados tenía 20 años o menos, el 27% de 21 a 35 años, el 23% de 36 a 50 años, el 23% 51 a 65 años, el 19 % de 66 a 80 años y el 3% más de 80 años (ver Fig. 1).

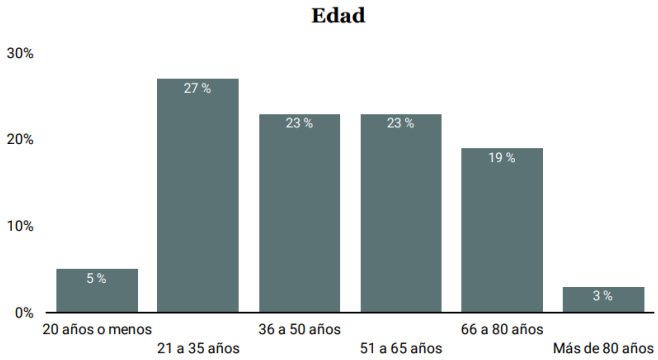

Fig. 1 Histograma de distribución de edades en la población muestreada.

Respecto al nivel de estudios, el 6,56% de los encuestados cuenta con nivel primario, el 35,59% nivel secundario y el 57,46% nivel universitario o mayor. Por otra parte, en cuanto a la ocupación, se destaca que un 20.6% de los encuestados es empleado, un 20% jubilado y, en los escalafones más bajos, se encuentra los comerciantes con un 5.6% y las amas de casas representando un 4.1% del total de la muestra.

III. Resultados y Discusión

Consultados respecto a la frecuencia con la que se accede a Internet, el 90,7% de los encuestados asegura acceder en forma diaria.

Al segmentar las respuestas por características sociodemográficas se destacan las siguientes conclusiones:

- No se observan diferencias significativas en relación al sexo.
- Existen diferencias significativas en la distribución por edades entre los menores y los mayores de 66 años. Los más propensos a usar Internet diariamente son los menores de 66 años. Se aprecia que a medida que la edad avanza, las personas son menos propensas a utilizar Internet diariamente.
- Si bien la frecuencia de acceso a Internet es elevada entre las personas más allá de su nivel educativo, se observa que su uso es ligeramente menor entre quienes sólo alcanzaron el nivel primario.

Los lugares desde donde los encuestados aseguran acceder a Internet con mayor frecuencia son en sus viviendas y *"en cualquier otro lugar con mis datos móviles"*. La mayor mención de estas opciones permite inferir una preferencia por el uso de conexiones particulares. En tercer y cuarto lugar se ubica el acceso a Internet en el lugar de trabajo o en cualquier otro lugar donde se provea una conexión de wi-fi pública.

Los dispositivos más utilizados para acceder a Internet son los smartphones, los cuales fueron mencionados con una

frecuencia del 96,2%. En segundo lugar, se ubican las computadoras personales (PC). En tercer lugar, aparecen los televisores. Otros dispositivos mencionados con menor frecuencia son las tablets y las consolas de juegos.

La actividad más popular en Internet es el uso de mensajería instantánea, la cual fue mencionada con una frecuencia del 94% por los encuestados. La segunda actividad más habitual, mencionada con una frecuencia del 87%, es el uso de servicios de entretenimiento (Netflix, Youtube, Spotify). Casi la misma proporción accede a Internet para usar redes sociales. Un poco menos de encuestados accede a Internet para enviar o recibir correos electrónicos. Con menor frecuencia aparecen realizar compras, gestiones en homebanking, asistir a videoconferencias, leer noticias o efectuar pagos por plataformas (ver Tabla I).

Se observan algunas diferencias significativas en cuanto a las actividades realizadas a través de Internet en función de las características sociodemográficas de los encuestados: sexo, edad y educación.

TABLA I
ACTIVIDADES EN INTERNET

Actividad	%
Mensajería instantánea (Whatsapp, Telegram, Facebook)	94%
Entretenimiento / Streaming (Netflix, Youtube, Spotify)	87%
Uso de las redes sociales (Instagram, Twitter, Facebook, etc.)	84%
Correo electrónico	76%
Compra de bienes o servicios (entradas espectáculos, boletos de transporte, indumentaria, electrodomésticos, delivery, etc)	68%
Homebanking	66%
Realización de videoconferencias (Zoom, Meet, Jitsi)	57%
Lectura de noticias (diarios, blogs, foros)	52%
Plataformas de pago (MercadoPago, PagoMisCuentas, etc)	49%
Gestión y pago de servicios públicos (AFIP, ARBA, Luz, Gas)	44%

En función del objetivo de este informe, se destacan:

1. Homebanking: No se observan diferencias significativas en cuanto al sexo, quienes realizan este tipo de operaciones con mayor frecuencia son las personas de entre 36 y 65 años y los individuos con estudios terciarios/universitarios. Entre los que las realizan con menor frecuencia están las personas de menos de 20 y los mayores de 65 años, y los individuos con estudios primarios.

2. Compra de bienes o servicios: Si bien no se observan diferencias significativas en cuanto al sexo, quienes realizan este tipo de actividad con mayor frecuencia son las personas de entre 21 y 35 años y quienes tienen estudios terciarios/universitarios. Los que menos las realizan son las personas de más de 80 años y las que sólo alcanzaron estudios primarios.

3. Venta de bienes o servicios: Quienes realizan este tipo de actividad con mayor frecuencia son los hombres, las personas de entre 21 y 50 años y los individuos con estudios secundarios. Los que menos las realizan son las mujeres, las personas de más de 66 años y las que sólo alcanzaron estudios primarios.

El 69% de las personas consultadas asegura que le genera algún tipo de preocupación realizar compras u operaciones bancarias a través de Internet. Se aprecia que la realización de estas actividades genera mayor preocupación entre las personas de mayor edad, en especial, entre las de más de 51 años, el 76% de los encuestados de entre 51 y 65 años, y el 81% de los encuestados de entre 66 y 80 años manifestó esta preocupación.

La estrategia mencionada por los encuestados con mayor frecuencia como medida para evitar una vulneración de la seguridad consiste en evitar publicar información personal y/o sensible en la web. Entre las más mencionadas también se destacan utilizar únicamente dispositivos propios, utilizar diferentes contraseñas en diferentes sitios, y no abrir correos electrónicos de origen desconocido.

Un dato no menor es el porcentaje de encuestados que, como medida de seguridad, ha elegido utilizar el doble factor de autenticación. Sólo un 33% de la muestra ha optado por esta medida, lo cual resulta muy bajo ya que esta medida se ha convertido en una de las más efectivas para evitar el robo de información y/o acceso indebido a sus cuentas.

El 26,5% de los encuestados considera estar bien o muy bien informado acerca de los riesgos del cibercrimen.

El 73,5% reconoce estar informado de manera deficiente, ya sea porque asume estar algo informado (38%), poco informado (26,8%) o nada informado (8,7%). En relación a la edad se advierte que la mayor proporción de quienes manifiestan tener algo de información se registra en el rango etario de 21 a 50 años. Consultados respecto a las fuentes de información a las que se les asigna mayor confianza para informarse sobre seguridad en Internet son familiares y/o amigos y expertos en informática.

Las fuentes a las que se les asigna menor confianza son las redes sociales y los funcionarios policiales y judiciales.

Considerando las estrategias que pueden dar origen a un fraude a través de Internet, los encuestados fueron consultados sobre sí experimentaron algunas de las siguientes situaciones de manera reciente.

En ese sentido se observa que:

- El 32,6% recibió correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla.
- El 34,4% recibió llamados telefónicos solicitando datos personales.
- El 73,8% recibió mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio.

Al segmentar los datos por variable sociodemográficas no se perciben diferencias significativas en cuanto a sexo. En relación

a la edad y al nivel de estudios se observa que reconocen con más frecuencia :

- Haber recibido correos o mensajes diciéndole que habían bloqueado su cuenta y que debía hacer clic en un link para volver a activarla las personas de entre 21 y 50 años y los individuos con estudios terciarios/universitarios.
- Haber recibido llamados telefónicos solicitando datos personales, las personas de entre 66 y 80 años.
- Haber recibido mensajes diciéndole que había ganado un premio o sobre el lanzamiento de una oferta o beneficio, las personas de entre 36 y 50 años y los individuos con estudios terciarios/universitarios.

Las modalidades de ciberdelito que más preocupan a los encuestados consisten en:

- Ser víctima de un fraude a través de tarjetas de crédito/débito.
- Ser víctima de un fraude a través del servicio de homebanking.
- Sufrir un robo de identidad mediante el uso de datos personales.

El 63% de los encuestados manifestó haber vivido o saber que algún allegado sufrió en el último año algunas de las modalidades de ciberdelito consideradas. Las tres modalidades mencionadas de manera más frecuentes son:

- Fraude a través de tarjeta crédito/débito.
- Hackeo de cuentas en redes sociales, mail, etc
- No haber recibido bienes o servicios en las condiciones adquiridas.

Por otro lado, el 37% de los encuestados asegura no haber vivido ni sabido de que algún allegado haya sufrido alguna de estas situaciones.

Entre quienes señalaron haber sufrido fraude a través de tarjeta crédito/débito el 29,3% recordó que antes de haberse dado cuenta de esa situación recibió una llamada telefónica solicitando datos personales para obligarlo a concurrir a un cajero automático y brindar un número o código de seguridad.

Entre quienes reconocen haber sido víctimas de fraude a través de Homebanking o Fintech, el 25,02% recordó que antes de haber detectado la situación inició alguna operación a través de una comunicación con la cuenta o el perfil de una empresa o institución en una red social.

El 61,03% de los encuestados que reconocen haber sido víctimas de fraude por no recibir bienes o servicios comprados/alquilados, que sean falsificados o diferentes a lo publicitado señaló haber realizado la operación a través de redes sociales, un marketplace o similar.

El 57,07% de los encuestados que reconocen haber sufrido fraude al vender un bien o servicio indicaron haber realizado estas operaciones mediante redes sociales, un marketplace o similar.

De los encuestados que reconocen haber sufrido un fraude por no recibir bienes o servicios comprados/alquilados, el 25.43% señaló haber sido víctima de esta situación al alquilar un inmueble, mientras que el 44.44% indicaron haber sufrido esta situación al recibir un comprobante de pago falso o que fue rechazado.

Tras haber detectado situaciones anómalas que potencialmente podrían ser el origen de un ciberdelito, la reacción mencionada con mayor frecuencia por los encuestados consistió en haberse contactado con el sitio web o proveedor con el cual se había interactuado.

La reacción más frecuente de los encuestados ante un ciberdelito consistió en haberse contactado con el banco cuando han sido han sido víctimas de un hecho de fraude con tarjeta de débito/crédito o a través de homebanking o fintech.

El 72,1% asegura desconocer dónde reportar mediante Internet un ciberdelito y el 17,1% no sabe o no contesta a la pregunta. Sólo el 10,8% afirma conocer dónde denunciar un caso. Entre quienes aseguran sí conocer dónde reportar la situación el 82,14% alude a las empresas proveedoras de servicios como Instagram, Facebook, Twitter o Gmail. En tanto que el 17,86% menciona al sitio web argentina.gob.ar

IV. Conclusiones y trabajo futuro

Este trabajo se comenzó a diagramar durante el año 2020 y se culminó su implementación en diciembre de 2021. Los datos fueron publicados en febrero de 2022.

Entre los datos presentados, y reforzando la hipótesis de la cifra negra, surge de esta encuesta que sólo el 10.8% declara conocer algún organismo para denunciar ciberdelitos. De ese porcentaje, las redes sociales como Instagram o Facebook han sido las más frecuentes a la hora de denunciar un ciberdelito. Sin embargo, estos no son los canales adecuados. Las redes sociales toman medidas sobre cuentas denunciadas, sin embargo son pocos los casos en los que reportan a la justicia para que se investigue. En el caso de Facebook, por ej. [10], se indica los pasos a seguir para recuperar la cuenta en caso de sospecha de hackeo, pero deja la denuncia a potestad del usuario.

Los canales adecuados para denunciar un ciberdelito son siempre los organismos del estado. El sitio de argentina.gob.ar provee mecanismos para denunciar este tipo de situaciones y aparece por debajo de las redes sociales con un porcentaje bastante bajo [11]. En la ciudad de Mar del Plata, los delitos pueden ser denunciados por correo electrónico directamente ante la Fiscalía General de esta ciudad a la casilla denunciasmardelplata@mpba.gov.ar.

Por otro lado, es importante destacar que se han realizado las encuestas correspondientes al período 2022, de los cuales ya se tiene la totalidad de los datos pero aún no ha finalizado su análisis.

Todas las preguntas diseñadas para este instrumento, fueron pensadas para medir el nivel de ciberdelito dada la inexistencia de estadísticas oficiales en la provincia de Buenos Aires. El sistema informático del Ministerio Público no permite diferenciar entre estafas cometidas por medios digitales de las que se realizaron por medios tradicionales, con lo cual, una estadística por estafa no distinguiría aquellas relacionadas al ciberdelito.

Los resultados de la presente encuesta de victimización, sumada a la posibilidad de contar con estadísticas oficiales, podrían estimar con cierto grado de certeza la "criminalidad aparente" del delito, entendida por Sozzo (2003:9) como "aquellas (conductas) que resultan concretamente calificadas como delitos por determinados agentes estatales o no estatales y sólo en el caso en que se hacen aparentes en virtud de haber sido registradas de alguna manera" [2]. Esto podría llevarnos a una "criminalidad real" aproximada, pero no a una criminalidad real precisa ya que es "dudosamente factible" (Sozzo, 2003:9) de conocer porque, como ya se mencionó, muchas personas no saben que han sido victimizadas o no lo ven como tal y por ende no lo informan.

Por último, Sain (2008:70) sostiene que toda política de seguridad pública consta de varios componentes pero uno de ellos es el "diagnóstico situacional" resultante de una recopilación y sistematización de información y de abordaje analítico, que debe dar cuenta de la situación general y específica del delito y la violencia existente en un tiempo y espacio determinado, su evolución, modalidades de manifestación, despliegue territorial, impacto social e institucional [3].

Entonces, se genera el siguiente interrogante ¿cómo es posible realizar estrategias, políticas de seguridad, prevención y otros factores en cuanto al ciberdelito si no existen mediciones, al menos aproximadas, de su ocurrencia en la sociedad? Este trabajo pretende dar alguna respuesta a este interrogante.

La necesidad de conocer los canales por los que los usuarios se informan es fundamental para dirigir las campañas de concientización. ¿De qué sirve concientizar por Twitter si el usuario detalla que ese canal no lo utiliza para informarse?

Conocer las medidas de seguridad adoptadas por los usuarios como las no adoptadas y que se consideran indispensables, es fundamental para diseñar estos planes de concientización. Por ejemplo, no utilizar el doble factor de autenticación en las cuentas es una gran debilidad que tiene la población de la ciudad de Mar del Plata.

Como resultado de este trabajo, el instrumento aquí presentado se ha replicado bajo la misma metodología en la ciudad de Salta, Argentina, a partir de un convenio con la Universidad Católica de Salta. Asimismo, está en vías de replicarse en la ciudad de Santa Fe, Argentina, a partir de un convenio con la Defensoría del Pueblo de la provincia de Santa Fe, y en San Pablo, Brasil, a partir de un convenio con el Colegio de Abogados de San Pablo.

Previo a la realización de este trabajo, sólo se contaba con algunas iniciativas esporádicas basadas en encuestas online, sin una metodología ni muestreos acordes, con lo cual se dificulta el control de la muestra así como la veracidad de los resultados. Este tipo de estudio de victimización, novedoso en la región, permite establecer un parámetro para medir este fenómeno, y a partir de esto, establecer políticas criminales adecuadas.

AGRADECIMIENTOS

Agradecemos la colaboración de los investigadores del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense y especialmente al Lic. Gabriel Coronello Aldao, director del Observatorio de la Ciudad de la Universidad FASTA, a la Lic. Mónica Pascual, Secretaria de Investigación y al Ing. Roberto Giordano Lenera, decano de la Facultad de Ingeniería de la Universidad FASTA por apoyar esta iniciativa.

REFERENCIAS

[1] Sain, G. Nuevas modalidades delictivas en materia de cibercrimen durante la pandemia del covid-19 en la república argentina; En Revista Temas de Derecho Penal y Procesal Penal, 2021, Erreius Online.

[2] Sozzo, M,; Contando el Delito. Análisis crítico y comparativo de las encuestas de victimización en Argentina; Azul, Argentina; 2003, Facultad de Derecho. Universidad Nacional del Centro de la Provincia de Buenos Aires,

[3] Sain, M. "El Leviatán azul. "Policía y política en la Argentina"; 2008, Siglo XXI Editores.

[4] https://www.lacapitalmdp.com/intentaron-estafar-al-fiscal-de-la-unidad-de-delitos-economicos/

[5] Informe anual sobre Pornografía Infantil en Internet y Grooming – Informe Anual 2021, Departamento de Delitos Conexos a la Trata de Personas, Pornografía Infantil y Grooming. Secretaría de Política Criminal, Coordinación Fiscal e Instrucción Penal Procuración General de la Suprema Corte de la provincia de Buenos Aires, La Plata, Septiembre 2022, disponible en: https://www.mpba.gov.ar/files/informes/Informe%20PI%202021.pdf consultado el 25 de febrero de 2023.

[6] Temperini, M., Borghello, C. Macedo, M. "La cifra negra de los delitos informáticos: Proyecto ODILA", disponible en https://www.odila.org/pdf/cifra_negra_delitos_informaticos.pdf consultado el 24 de febrero de 2023

[7] Reporte Fraude Electrónico 2021, disponible en https://www.odila.org/analisis-fraude consultado el 22 de febrero de 2023.

[8] Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos Aires : Erreius,2018. Disponible en https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf consultado el 27 de febrero de 2023.

[9] Instituto Nacional de Estadística y Censos -INDEC, Censo nacional de población, hogares y viviendas 2022 : resultados provisionales / 1a ed. - Ciudad Autónoma de Buenos Aires : Instituto Nacional de Estadística y Censos - INDEC, 2023, disponible en https://www.indec.gob.ar/ftp/cuadros/poblacion/cnphv2022_resultados_provisionales.pdf consultado el 26 de febrero 2023.

[10] Recuperar tu cuenta si crees que alguien hackeó tu cuenta de Facebook o la está usando sin tu permiso https://es-la.facebook.com/help/203305893040179

[11] Información oficial portal de gobierno para realizar denuncias de un ciberdelito en Argentina, disponible e https://www.argentina.gob.ar/justicia/convosenlaweb/denuncia consultado el 26 de febrero de 2023