SEGURIDAD | CIBERPREVENCIÓN | I.A. | CRIMINOLOGÍA | VICTIMOLOGÍA | GOBIERNO

Insight 21

Ciberdelincuencia y tendencias en Argentina

Desafíos emergentes para la ciberprevención y la gobernanza digital

Mgter. Nicolás Macchione
Director del Instituto de Seguridad y Criminología

UNIVERSIDAD SIGLO 21

Resumen ejecutivo

La presente investigación analiza el fenómeno de la ciberdelincuencia en Argentina desde una perspectiva criminológica y sociodigital, focalizándose en las dinámicas de victimización, percepción del riesgo y prácticas de ciberprevención desarrolladas por los usuarios. El estudio adopta un enfoque cuantitativo, descriptivo y transversal, basado en el análisis de encuestas de victimización realizadas a 1050 ciudadanos residentes en nuestro país.

Los resultados evidencian una expansión sostenida de modalidades delictivas digitales, en particular fraudes y suplantaciones de identidad, desarrolladas principalmente a través de plataformas de uso cotidiano como WhatsApp y demás redes sociales. Asimismo, se identificó una mayor incidencia de victimización en adultos económicamente activos, lo que podría sugerir una relación entre la intensidad de la interacción digital y la exposición al delito.

El análisis también permitió observar una persistente brecha entre la percepción del riesgo y la conducta preventiva. Si bien gran parte de los encuestados reconoce la existencia de amenazas digitales y adopta determinadas medidas de protección, continúan registrándose prácticas de vulnerabilidad, especialmente vinculadas a la provisión de datos personales y a la ausencia de cambios conductuales posteriores a experiencias de victimización.

En este marco, el estudio destaca la necesidad de fortalecer estrategias integrales de ciberprevención y alfabetización digital, orientadas al desarrollo de capacidades de autoprotección y a la formulación de políticas públicas adaptadas a las particularidades sociales y territoriales del fenómeno.

Información metodológica

Metodología
Cuantitativa

Tipo de investigación
Descriptiva

Técnica de recolección de datos
Encuesta telefónica

Instrumento de recolección de datos
Cuestionario estructurado

Población de estudio
Varones y mujeres con edades comprendidas entre los 18 y los 65 años, residentes en las siguientes ciudades argentinas: Ciudad de Buenos Aires, Comodoro Rivadavia, Córdoba, Corrientes, Mendoza, Rosario, y San Miguel de Tucumán.

Procedimiento de selección de la muestra
Probabilístico, aleatorio sistemático.

Tamaño de la muestra
1050 casos en cada año comparado

Error de la muestra
3,02 %

Nivel de confianza
95 %

Introducción al tema y problema

Los espacios cibernéticos y las herramientas digitales se caracterizan por su constante expansión y su creciente centralidad en la vida social, económica e institucional. Este desarrollo continuo se orienta a mejorar la calidad de vida, automatizar diversos procesos y generar nuevos espacios de interacción y ocio, entre otros avances. Sin embargo, en paralelo a dicha modernización, los delitos digitales se han expandido, lo que ha dado lugar a una estructura de modalidades y técnicas digitales que configuran prácticas de cibercrimen capaces de tomar desprevenidos tanto a ciudadanos como a organizaciones.

El presente trabajo se propone identificar este fenómeno en distintos puntos de Argentina, analizando las modalidades en que se manifiesta, su alcance sobre las víctimas y los métodos de prevención empleados. Para ello, se recurre al análisis de encuestas de victimización de carácter criminológico, que permiten evidenciar situaciones no contempladas en las estadísticas delictuales.

En este marco se destaca la necesidad no solo de contabilizar e interpretar la problemática, sino también de comprender las dinámicas de exposición y percepción de los usuarios para dar respuesta mediante la articulación de políticas públicas orientadas a la ciberprevención que garanticen la accesibilidad, la adaptabilidad y el desarrollo del usuario en el manejo de herramientas de comprensión ante los avances digitales que se dan día a día.

La relevancia del estudio radica, entonces, en la necesidad de comprender la ciberdelincuencia como un fenómeno en expansión y también como una problemática que interpela las formas tradicionales de abordar la seguridad y la prevención en entornos digitales. La creciente incorporación de tecnologías en la vida cotidiana, en ausencia de niveles homogéneos de alfabetización digital, expone a amplios sectores de la población a riesgos no siempre identificados y de difícil gestión.

A partir de lo expuesto, surge el interrogante: ¿Cómo se configuran las dinámicas de victimización y percepción del riesgo frente a la ciberdelincuencia

en Argentina y en qué medida inciden en la efectividad de las estrategias de ciberprevención?

En función de ello, se plantea como objetivo general de esta investigación analizar el fenómeno de la ciberdelincuencia en Argentina a partir de las dinámicas de exposición, percepción del riesgo y respuesta de los usuarios victimizados a la par que se describe su incidencia en las prácticas de ciberprevención adoptadas por ellos. Como objetivos específicos, se proponen: identificar las principales modalidades delictivas en entornos digitales, examinar el alcance del fenómeno en las víctimas, y analizar cuáles son las prácticas de ciberprevención adoptadas por los usuarios.

Desde esta perspectiva, el estudio se inscribe en un enfoque analítico de carácter criminológico y sociodigital articulado. Este enfoque permite abordar el fenómeno con una mirada integral, considerando tanto las condiciones objetivas de exposición como las dimensiones subjetivas que influyen en las conductas de los usuarios.

Diagnóstico y análisis

La ciberdelincuencia se presenta como un fenómeno complejo, dinámico y en constante expansión, que se distingue de la delincuencia convencional por su carácter transnacional, el anonimato de los actores y la desmaterialización del daño (INTERPOL, 2024; Sanchis, 2018). En el contexto argentino, informes como el de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI, 2024) evidencian un crecimiento exponencial de estas prácticas, particularmente en el fraude digital, la suplantación de identidad y las extorsiones a través de plataformas digitales, reflejo de una creciente exposición de los usuarios en su vida cotidiana.

Este fenómeno fue advertido por Miró Llinares (2011), quien reconoce el ciberespacio como un nuevo ámbito de oportunidad criminal en el que la reducción del espacio físico elimina la necesidad de proximidad entre agresor y víctima. Al adecuar la teoría de las actividades rutinarias (Cohen & Felson, 1979) a este medio, el autor sostiene que la convergencia entre la exposición de datos del usuario, el valor de esa información para el agresor y su nivel de interacción digital incrementan la posibilidad de victimización. Desde esta perspectiva criminológica, la victimización no depende únicamente de la ocurrencia del delito, sino de la interacción entre oportunidades delictivas, niveles de exposición y capacidades de protección disponibles para cada usuario.

En este marco, la percepción del riesgo –la forma en que los individuos interpretan y evalúan las amenazas– no siempre se corresponde con los niveles reales de exposición, y esa brecha entre riesgo objetivo y percibido incide en la adopción de prácticas preventivas, incluso en contextos de creciente conciencia digital (Slovic, 1987; Pew Research Center, 2017; Equipo de Respuesta ante Emergencias Informáticas de la República Argentina, 2022). A ello se suma la alfabetización digital –la capacidad de comprender, evaluar y gestionar información en entornos digitales (UNESCO, 2018; Van Deursen & Van Dijk, 2014)–, cuyos niveles dispares contribuyen a desigualdades en la exposición y victimización (OECD, 2022). Por ello, los debates actuales en torno al cibercrimen enfatizan la necesidad de enfoques integrales que articulen estrategias de ciberprevención accesibles y adaptables al usuario, orientadas a reducir la brecha entre percepción y conducta (Gobierno de Argentina, 2023; ENISA, 2018).

De cara a la recolección de datos, se llevó a cabo una encuesta de 21 preguntas de opción múltiple a 1050 personas, repartidas en 7 localidades del país, con una distribución equitativa por género y una amplia pluralidad etaria y de nivel educativo (con predominancia de escolaridad secundaria y estudios universitarios). Esta diversidad sociodemográfica permite abordar de manera más abarcativa las dinámicas de reproducción y prevención ciberdelictuales.

Los resultados muestran que un 24,9% de los encuestados han sido víctimas de algún tipo de delito cometido mediante el uso de herramientas digitales. Complementariamente, un 35,9% de los encuestados han logrado evitar los efectos de estos tipos de actos delictivos, mientras que el 56,7% reporta conocer a alguien cercano que haya sido víctima. Estos datos sugieren una elevada exposición social a estos modos de reproducción del delito. De cara al primer contacto, este se produce mayoritariamente por redes sociales y llamadas telefónicas, siendo los datos personales, como el Documento Nacional de Identidad y las claves de acceso bancarias, la información más solicitada (30% y 32,2%, respectivamente).

En cuanto a las estrategias de prevención, se destacan la desconfianza ante remitentes desconocidos (58,5% de los encuestados), el uso de medios y páginas oficiales como único canal de compra (37,5%) y el cambio regular de contraseñas (31,2%). Sin embargo, un 43,8% de quienes recibieron una solicitud de datos por canales digitales (del 49% de encuestados a quienes se les pidió información) manifestaron haber proporcionado total o parcialmente lo

requerido, lo que evidencia una tensión entre el uso cotidiano de herramientas tecnológicas y la efectividad real de las estrategias de prevención adoptadas.

En consecuencia, se procede al análisis sistematizado de los datos anteriormente presentados, separándolos en categorías operacionales acordes al propósito de la presente investigación:

1. Victimización según características sociodemográficas

El análisis de la victimización en función de variables sociodemográficas permite identificar patrones diferenciales de exposición al cibercrimen. En términos etarios, se observa mayor incidencia en los grupos de 30 a 49 años (36%) y 50 a 64 años (33%), lo que sugiere que la intensidad y el tipo de uso digital –vinculado a actividades laborales, financieras y administrativas– constituyen factores relevantes en la configuración del riesgo.

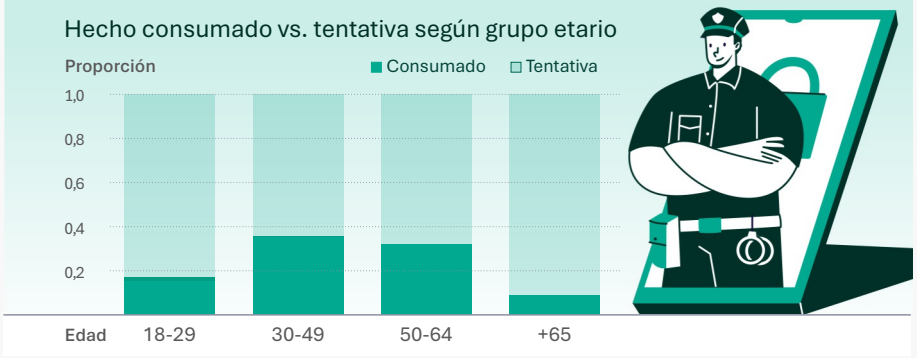
Respecto al género, la distribución resulta relativamente equilibrada (55% de mujeres y 45% de varones), lo que permite sostener el carácter transversal del fenómeno, sin una segmentación marcada. No obstante, esta paridad no excluye la posibilidad de diferencias en las modalidades o consecuencias del delito, lo que abre líneas de análisis complementarias.

En cuanto al nivel educativo, los mayores niveles de victimización se registran en personas con educación secundaria (35%) y universitaria (39%), lo que evidencia que el acceso a la educación formal no constituye, por sí mismo, un factor de protección frente al cibercrimen. Este dato refuerza la idea de que la alfabetización digital no se corresponde necesariamente con el nivel educativo alcanzado.

En términos ocupacionales, se destaca la proporción de empleados (48%), seguida por trabajadores independientes (22%), lo que sugiere que la exposición está estrechamente vinculada a la frecuencia de interacción con entornos digitales, particularmente en contextos laborales. En conjunto, estos resultados permiten comprender la victimización como un fenómeno socialmente distribuido, condicionado por las prácticas de uso y los niveles de exposición.

2. Hecho consumado vs. tentativa

Gráfico 1 | Hecho consumado vs. tentativa



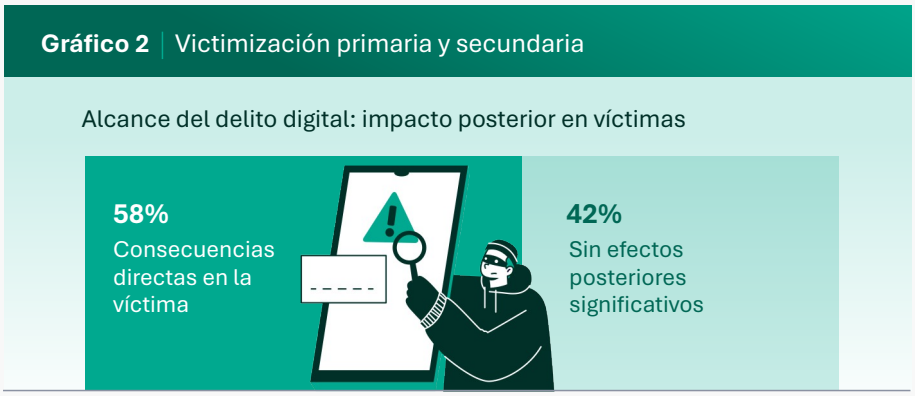
Nota. Elaboración propia a partir de los datos relevados en la encuesta.

El análisis del tipo de hecho evidencia que el 55% de los casos corresponden a delitos consumados, mientras que el 45% restante se configura como tentativa. Al incorporar la variable etaria, se observa que los grupos de 30 a 49 años (37%) y 50 a 64 años (34%) concentran la mayor proporción de hechos consumados.

Este patrón permite deducir dos aspectos que nos interesa destacar. Por un lado, la posibilidad de evitar la consumación del delito puede variar según la experiencia digital y los hábitos del usuario. Por otro lado, permite diferenciar entre exposición y efectividad del delito, aportando elementos para comprender quiénes son más vulnerables.

3. Victimización primaria y secundaria

Gráfico 2 | Victimización primaria y secundaria

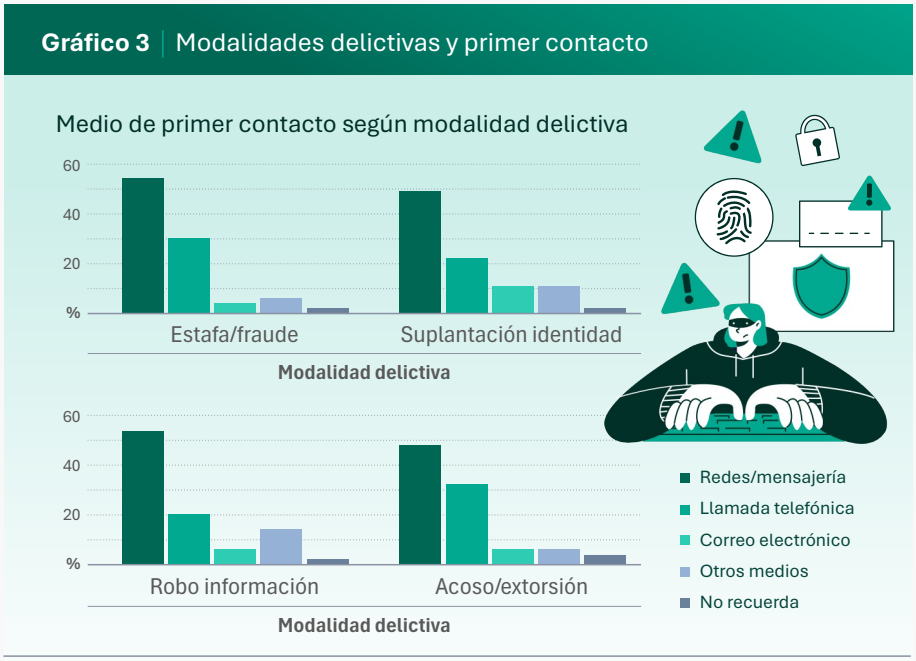


Nota. Elaboración propia a partir de los datos relevados en la encuesta.

El gráfico muestra que el 58% de las víctimas reportan haber sufrido consecuencias directas, mientras que un 42% indica no haber experimentado efectos posteriores significativos. Esta distribución confirma que la tipología delictual analizada presenta impactos que trascienden el momento en el que ocurre el hecho, proyectándose a futuro, incidiendo en la práctica digital, la gestión de la información y la confianza en entornos tecnológicos.

4. Modalidades delictivas y primer contacto

Gráfico 3 | Modalidades delictivas y primer contacto



Nota. Elaboración propia a partir de los datos relevados en la encuesta.

En relación con las modalidades delictivas, se observa una clara predominancia de los fraudes digitales (41%), seguidos por la suplantación de identidad (29%), lo que confirma la centralidad de prácticas orientadas a obtener información y recursos mediante engaño.

Otro aspecto que merece especial atención es la elevada incidencia de casos de suplantación de identidad que, desde una perspectiva criminológica y jurídico-penal, no siempre constituye un delito autónomo, sino que frecuentemente opera como medio comisivo para facilitar estafas, defraudaciones patrimoniales, accesos indebidos a cuentas o engaños a familiares y allegados de la víctima, al construir una apariencia de confianza que la convierte en una de las principales herramientas de la ingeniería social. Si bien la

encuesta no distingue si esta modalidad fue percibida como hecho principal o como medio para otros delitos, los resultados y la evidencia especializada disponible permiten inferir su creciente relevancia, por lo que se considera pertinente incorporar esta diferenciación en futuros relevamientos.

En este apartado, se evidencia que las redes sociales funcionan como primer contacto en la mayoría de los casos recopilados, independientemente de la modalidad delictiva. Este dato resulta en especial relevante, ya que indica que los delitos se insertan en los mismos espacios de comunicación cotidiana de los usuarios. Dicho canal concentra más del 50% de los casos de estafa (56,2%), robo de información financiera (54,8%) y suplantación de identidad (50,7%), lo que expresa la centralidad de las redes sociales como espacio predilecto de intervención entre víctima y victimario.

5. Modalidades delictivas según género y localidad

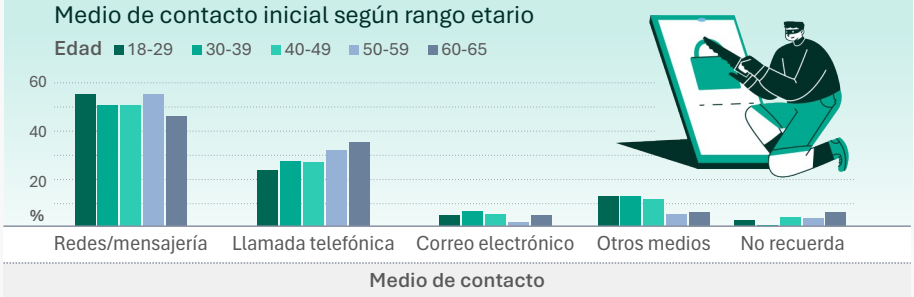
La Ciudad Autónoma de Buenos Aires concentra el mayor porcentaje de casos de ciberdelincuencia, lo cual se vincula con sus características sociodemográficas. No obstante, en Corrientes se registra un volumen superior de estafas, robo de información financiera y acoso/chantaje que en Córdoba o Rosario, pese a la mayor densidad poblacional e índices delictivos de estas últimas; Tucumán ocupa el segundo lugar en casos de acoso, chantaje o extorsión virtual (15,7%); y Comodoro Rivadavia exhibe los índices más bajos de ciberdelincuencia en general.

En cuanto a las diferencias por género, la distribución de las principales modalidades delictivas resulta relativamente equilibrada entre varones y mujeres, aunque el acoso, chantaje o extorsión virtual presentan una mayor incidencia entre los varones (62,7% frente a 37,3%), mientras que el robo de información personal o financiera muestra una leve predominancia entre las mujeres (52% frente a 48%).

6. Canales de contacto según edad y localidad

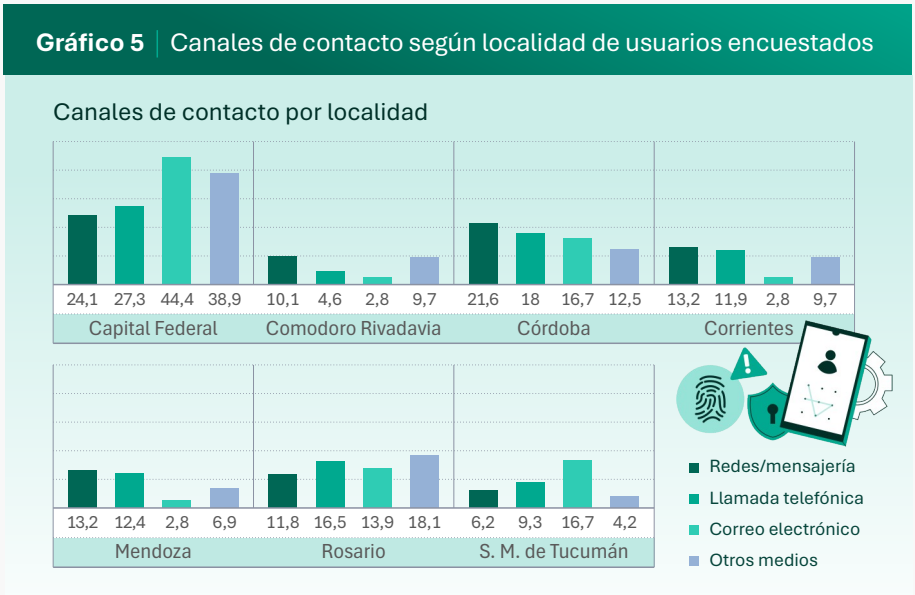
Los datos muestran que los canales de contacto varían según la edad: en los grupos más jóvenes predominan las redes sociales (42%), mientras que en los adultos se destaca WhatsApp (46%), lo que evidencia que la exposición al delito está mediada por las prácticas digitales de cada grupo etario.

Gráfico 4 | Canales de contacto según edad de los usuarios encuestados



Nota. Elaboración propia a partir de los datos relevados en la encuesta.

Gráfico 5 | Canales de contacto según localidad de usuarios encuestados



Nota. Elaboración propia a partir de los datos relevados en la encuesta.

A nivel territorial, ambos canales mantienen su centralidad, aunque con diferencias de intensidad que refuerzan la dimensión contextual del fenómeno.

7. Solicitud y provisión de información

El análisis revela que al 49% de los encuestados se les solicitó información personal relevante a través de canales digitales. De este grupo, un 24,6% afirmó haber proporcionado la totalidad de los datos requeridos, mientras que un 19,2% solo entregó parte de ellos. En contraste, el 56,3% manifestó no haber brindado ningún tipo de información.

8. Victimización y prácticas de prevención

El cruce entre la victimización y la adopción de medidas preventivas muestra una relación directa entre haber sufrido un ciberdelito y la conducta de autoprotección: el 90% de quienes fueron víctimas en más de una ocasión y el 86,6% de quienes lo fueron una vez implementan medidas de seguridad digital, frente al 71,2% de quienes nunca lo fueron. Esto sugiere que la exposición previa incrementa la disposición a protegerse. En contraste, entre quienes no adoptan medidas preventivas, el 87,6% nunca fue víctima, lo que podría reflejar una subestimación del riesgo.

9. Medidas de prevención según variables sociodemográficas

Finalmente, un 75,3% de los encuestados declara implementar alguna práctica preventiva, mientras que un 24,7% no adopta medidas, lo que evidencia un nivel considerable de conciencia sobre la seguridad digital, aunque persiste un segmento sin estrategias de protección. Entre las prácticas más adoptadas se destacan el uso de contraseñas seguras y su actualización periódica (31,2%), el uso de plataformas oficiales para compra o venta (37,5%) y la negativa a contestar llamadas, mensajes o correos de fuentes desconocidas (58,5%), lo que refleja un enfoque centrado en la autoprotección básica frente a fraudes y engaños digitales.

Sin embargo, estas prácticas presentan cambios según variables sociodemográficas, lo que indica que la adopción de conductas de protección no es uniforme. Factores como la edad, el nivel educativo y la ocupación inciden en la forma en que los usuarios gestionan su seguridad digital.

De cara a la categoría etaria, se observa que el rango etario con mayor porcentaje de prevención se encuentra entre los 60 y 65 años (81,5%), mientras que el rango etario de los 40 a 49 años presenta los menores valores (72,4%). En todos los grupos etarios se repite el patrón de que entre el 72% y el 82% toma medidas preventivas (18-29: 77,2%; 30-39: 74,5%; 40-49: 72,4%; 50-59: 74,6%; 60-65: 81,5%).

En referencia al apartado educativo, se observa que aquellos encuestados con estudios secundarios completos muestran una mayor inclinación a no tomar medidas preventivas, en comparación con quienes tienen nivel universitario.

En cuanto al apartado laboral, se observa un patrón de comportamiento similar entre a los encuestados laboralmente activos, dado que cada grupo (sin importar su rol o posición) muestra cierta tendencia a la adopción de medidas preventivas.

Este resultado refuerza la necesidad de diseñar estrategias de ciberprevención diferenciadas, orientadas a distintos perfiles de usuarios, en lugar de adoptar enfoques homogéneos.

Conclusiones

El presente estudio permitió analizar el fenómeno de la ciberdelincuencia en Argentina a partir de las dinámicas de victimización, la percepción del riesgo y las prácticas de prevención de los usuarios. Los resultados confirman que se trata de una problemática transversal, dinámica y en expansión, estrechamente vinculada con la creciente digitalización de la vida cotidiana.

Se identifica una predominancia de modalidades basadas en el engaño –fraudes digitales y suplantación de identidad–, con las plataformas de uso cotidiano (WhatsApp y redes sociales) como principal canal de contacto, lo que profundiza la inserción de la ciberdelincuencia en los espacios habituales de comunicación y complejiza la identificación temprana de amenazas. Uno de los hallazgos más relevantes es la persistente brecha entre percepción del riesgo y conducta preventiva: si bien gran parte de los encuestados reconoce las amenazas digitales y adopta ciertas medidas de protección, continúan registrándose conductas de vulnerabilidad –como la provisión de datos personales ante solicitudes sospechosas– que evidencian que la experiencia directa con el delito no siempre se traduce en prácticas sostenidas de autoprotección.

Estos resultados permiten problematizar la ciberdelincuencia como un fenómeno que excede las respuestas basadas únicamente en el control técnico o la intervención punitiva, y que plantea desafíos para la gobernanza digital y las políticas públicas de prevención. Frente a ello, el informe refuerza la necesidad de avanzar hacia estrategias integrales de ciberprevención centradas en el usuario, que articulen dimensiones tecnológicas, educativas y sociales,

entendiendo que la alfabetización digital es un componente clave para reducir vulnerabilidades y fortalecer capacidades de evaluación del riesgo –capacidades que, según muestra el estudio, no se distribuyen de manera homogénea entre la población–.

En consecuencia, se propone crear y robustecer políticas públicas de ciberprevención integrales, adaptadas a distintos perfiles poblacionales, que sean accesibles, territorialmente situadas e incorporen programas de alfabetización digital en ámbitos educativos, laborales y comunitarios. Asimismo, resulta fundamental consolidar mecanismos de articulación entre organismos estatales, instituciones educativas, empresas tecnológicas y organizaciones civiles, dado que la ciberdelincuencia es un fenómeno dinámico y transnacional que requiere respuestas coordinadas.

Finalmente, cabe destacar que estos resultados constituyen un diagnóstico correspondiente a un momento determinado, por lo que se recomienda actualizar periódicamente este relevamiento para monitorear la evolución de las modalidades delictivas y evaluar el impacto de las políticas implementadas. Del mismo modo, futuras ediciones del estudio deberían ampliar su alcance territorial, incorporando nuevas ciudades y áreas metropolitanas que permitan representar con mayor precisión la diversidad social y tecnológica del país, y así diseñar políticas públicas más inclusivas, equitativas y eficaces.

Referencias

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

European Union Agency for Cybersecurity (ENISA). (2018). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Jefatura de Gabinete de Ministros. (2023). Segunda Estrategia nacional de ciberseguridad: Consulta pública para la segunda estrategia. https://www.argentina.gob.ar/sites/default/files/2023/06/consulta_publica_segunda_estrategia.pdf

Ministerio de Justicia de la Nación. (2025). ¿Qué es el ciberdelito? https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

INTERPOL. (2024). Ciberdelincuencia. https://www.interpol.int/es/Delitos/Ciberdelincuencia

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología, 13(07), 1-55.

http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Organisation for Economic Co-operation and Development (OECD). (2022). Policy Framework on Digital Security. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

Pew Research Center. (2017). Americans and Cybersecurity. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Sanchis, E. G. de la B. (2018). Ciberdelincuencia, ciberterrorismo, ciberdelito y cibercrimen. Peritos Informáticos. https://peritos-informaticos.com/blog/ciberdelincuencia-ciberterrorismo-ciberdelito-cibercrimen/

Slovic, P. (1987). Perception of risk. Science, 236(4799), 280-285. https://pages.ucsd.edu/~aronatas/project/academic/risk%20slovic.pdf

Equipo de Respuesta ante Emergencias Informáticas de la República Argentina. (2023). Informe de Gestión CERT.ar 2022. Portal Oficial del Estado Argentino. https://www.argentina.gob.ar/noticias/informe-de-gestion-certar-2022

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (2024). Informe anual sobre ciberdelincuencia en Argentina. Recuperado de: https://www.mpf.gob.ar/ufeci/files/2025/06/UFECI_informe_anual_2024-1.pdf

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2018). A global framework of reference on digital literacy skills for indicator 4.4.2. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000265403

Van Deursen, A. J. A. M., & Van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. New Media & Society, 16(3), 507–526. https://www.dhi.ac.uk/san/waysofbeing/data/economy-crone-vandeursen-2014b.pdf

INFORME

Ciberdelincuencia y tendencias en Argentina

Desafíos emergentes para la ciberprevención y la gobernanza digital

SEPTIEMBRE 2026

Insight 21 THINK TANK

UNIVERSIDAD SIGLO 21