EL PAPEL DE LOS MEDIOS FRENTE AL FRAUDE INFORMÁTICO. DIFUSIÓN, PREVENCIÓN Y ALFABETIZACIÓN

DRA. MARÍA MENDOZA MICHILOT
https://orcid.org/0000-0001-7293-5110
tmendoza@ulima.edu.pe
Universidad de Lima, Perú

DRA. MARIELA DEJO-VÁSQUEZ
https://orcid.org/0000-0003-1726-2106
mcdejo@ulima.edu.pe
Universidad de Lima, Perú

MAG. ROSARIO NAJAR-ORTEGA
https://orcid.org/0000-0002-7247-3021
Rnajar@ulima.edu.pe
Universidad de Lima, Perú

Recibido: 31 de mayo del 2024 / Aceptado: 5 de febrero del 2025
doi: https://doi.org/10.26439/contratexto2025.n43.7160

RESUMEN. El fraude informático es un delito que se incrementó en la coyuntura de la pandemia de COVID-19 en el mundo, y el Perú no fue la excepción. Por ello, nos interesó recoger las perspectivas de los peruanos sobre el uso de la prensa y de los medios sociales en la difusión y, eventualmente, su participación en una estrategia de alfabetización financiera digital como medida de prevención para evitar más pérdidas económicas y de datos por este delito. Una encuesta a 429 residentes en Lima Metropolitana y 25 entrevistas a víctimas del fraude informático permitieron conocer que Facebook y la televisión convencional son las plataformas más utilizadas para informarse sobre el *modus operandi* de la delincuencia. De los resultados, también se obtuvo que la mayoría no comparte sus experiencias en los medios, porque desconfía de ellos o percibe que no contribuyen a esclarecer sus denuncias. Por ello, el estudio plantea una estrategia informativa mínima que la prensa podría considerar en su quehacer cotidiano para orientar a las personas sobre cómo prevenir, denunciar y hallar una solución a los fraudes informáticos; además, evitar la impunidad del delito y, al mismo tiempo, ir construyendo ciudadanía.

PALABRAS CLAVE: delito cibernético / periodismo de soluciones / medios sociales / usuarios digitales / alfabetización financiera digital

THE ROLE OF THE MEDIA AGAINST COMPUTER FRAUD. DISSEMINATION, PREVENTION AND LITERACY

ABSTRACT: Computer fraud is a crime that increased in the context of the Covid-19 pandemic in the world, and Peru was no exception. Therefore, we were interested in gathering Peruvians' perspectives on the use of the press and social media in the dissemination and, eventually, their participation in a digital financial literacy strategy, as a preventive measure to avoid further losses from this crime. A survey of 429 residents in Metropolitan Lima and interviews with 25 victims of computer fraud revealed that Facebook and conventional television are the platforms most used to learn about the modus operandi of crime; that the majority do not share their experiences in the media because they distrust them or perceive that they do not contribute to clarifying their complaints. The study proposes a minimum informative strategy that the press could consider in its daily work, to guide people on how to prevent, denounce and find a solution; to avoid the impunity of crime and, at the same time, to build citizenship.

KEYWORDS: cybercrime / solutions journalism / social media / digital users / digital financial literacy

O PAPEL DA MÍDIA NO COMBATE À FRAUDE DE COMPUTADOR. DISSEMINAÇÃO, PREVENÇÃO E ALFABETIZAÇÃO

RESUMO. A fraude informática é um crime que aumentou no contexto da pandemia de Covid-19 no mundo, e o Peru não foi exceção. Portanto, estávamos interessados em coletar as perspectivas dos peruanos sobre o uso da imprensa e das mídias sociais na divulgação e, eventualmente, sua participação em uma estratégia de alfabetização financeira digital como medida preventiva para evitar mais perdas com esse crime. Uma pesquisa com 429 residentes na região metropolitana de Lima e entrevistas com 25 vítimas de fraude de computador revelaram que o Facebook e a televisão convencional são as plataformas mais usadas para aprender sobre o modus operandi do crime; que a maioria não compartilha suas experiências na mídia, porque não confia nela ou percebe que ela não contribui para esclarecer suas reclamações. O estudo propõe uma estratégia mínima de informação que a imprensa poderia considerar em seu trabalho diário, para orientar as pessoas sobre como prevenir, denunciar e encontrar uma solução; para evitar a impunidade do crime e, ao mesmo tempo, para construir a cidadania.

PALAVRAS-CHAVE: crimes cibernéticos / jornalismo de soluções / mídias sociais / usuários digitais / alfabetização financeira digital

INTRODUCCIÓN

Los fraudes informáticos son ciberdelitos que aumentaron en el mundo durante el estallido de la pandemia de COVID-19 y después de ella. Sin considerar el subregistro de casos, el peligroso y atípico crecimiento de estas formas de criminalidad ha marchado de la mano con el uso intensificado de internet durante la crisis pandémica (Interpol, 2022; Kemp et al., 2021; Van de Weijer et al., 2023). Tales formas delictivas son de este siglo y han sustituido a otras no informáticas (García-Juárez, 2016; Kshetri, 2013). Hoy son el cuarto riesgo global más importante después de las enfermedades infecciosas, la crisis alimentaria y los fenómenos meteorológicos extremos, según *The Global Risk Report* (World Economic Forum, 2022).

Una de las formas delictivas más comunes es el delito cibernético-financiero (en adelante, fraude informático o fraude en línea). Es un conjunto de actos ilegales que se basa en el mal uso de las tecnologías para suplantar la identidad de las personas y sustraer ilícitas ganancias financieras (Loggen et al., 2024). El fraude informático ha sido abordado antes, durante y después de la pandemia de COVID-19 desde diferentes tópicos: consecuencias financieras, modalidades del delito, culpabilidad del infractor y el control tecnológico (Arief & Bin Adzmi, 2015; Button et al., 2014; Buzzio-García et al., 2021; Drew, 2020; Hakak et al., 2020; Holt, 2023; Ibrahim, 2016; López Gorostidi, 2020; Mayer Lux & Calderón, 2020; Mendivil et al., 2022¸ Nuredini, 2014; Sánchez Henríquez et al., 2022).

Este artículo, que propone aproximarse a la consecuencia social del delito cibernético-financiero (Button et al., 2014; Ikbal et al., 2022; Nicholls et al., 2006), recoge el punto de vista de la víctima, el eslabón más débil de la ciberseguridad (Cain et al., 2018). Esto se debe a que la víctima juega un papel crucial e involuntario en la trama delictiva (Rodríguez-Rodríguez et al., 2020), ya que el delincuente necesita de su concurso para sustraer sus bienes de manera inconsulta (Carter, 2023), pues se aprovecha cuando la víctima actúa de buena fe, por ejemplo al instalar *softwares* dudosos o compartir datos personales (Proofpoint, 2019).

Para este estudio, se ha tomado como referencia el caso peruano. Según la herramienta Google Trends, el fraude informático ha sido uno de los intereses de búsqueda más destacados de los cibernautas peruanos durante el 2019, así como estafa por internet, ciberdelito, delito informático y *phishing*, tanto en noticias como en otros contenidos. El *phishing* (que significa 'suplantación a través del enlace a una página adulterada') destacó entre marzo y abril del 2020, al estallar la pandemia en el Perú, y en enero del 2021, y coincidió con el aumento de denuncias ante la Policía Nacional del Perú (2022a, 2022b) y el Ministerio Público (Consejo Nacional de Política Criminal, 2020).

Del mismo modo, en este artículo se analizó si los ciudadanos afectados han socializado sus experiencias a través de los medios de comunicación, con qué objetivos lo hicieron y qué resultados obtuvieron. También se analizó qué tipo de apoyo,

respaldo o información recibieron las víctimas en la interacción mediática, qué repercusión tuvieron los medios para las víctimas, como espacios de difusión de los delitos, y qué tareas podrían cumplir en los procesos que vive una víctima de fraude informático.

Con esta información, y aplicando la metodología del periodismo de soluciones (Fundación Gabo, 2020), se ha propuesto una dieta informativa (McIntyre, 2019) basada en la agenda pública, es decir, en asuntos que las víctimas quisieran que se discutan o debatan para promover no solo la prevención de la delincuencia en línea, sino alfabetizarse frente a esta modalidad del crimen organizado (Jiang et al., 2024). Además, se presentaron contenidos de un programa de formación o de higiene cibernética propuestos por algunos autores (Cain et al., 2018).

Alfabetización digital o higiene cibernética

Entendemos la alfabetización digital como una forma de educación digital financiera que, durante la pandemia, se planteó de manera urgente ante el uso indebido de los datos personales o información privada de las personas en medios digitales, la elaboración de perfiles digitales falsos, otros delitos cibernéticos y riesgos derivados de activos y servicios tecnológicos complejos (Van Zeeland & Pierson, 2024). Alfabetizar es la prevención del delito menos onerosa y forma parte de la seguridad cibernética. Es un concepto aceptado globalmente, sinónimo de confianza en los sistemas digitales de las naciones ante el mundo y sus socios comerciales (World Economic Forum, 2022).

En el ámbito de la comunicación, este tipo de alfabetización podría inscribirse dentro de una estrategia informativa que reformule los problemas sociales, enfocándose en sus posibles soluciones (McIntyre, 2019). En este marco, orientar a las personas en las prácticas de la ciberseguridad desde el periodismo significa darles información suficiente sobre los delitos informáticos frecuentes (Waqas et al., 2023) o ilustrarlas respecto al quehacer periodístico para que interactúen con las dinámicas del trabajo noticioso (Sencan & Soydal, 2023) y puedan difundir sus casos si son víctimas. Entonces, para brindar una educación antifraude y mejorar la resiliencia de las personas frente a un delito que es global, se requiere de la ciberhigiene (Baraković & Baraković-Husic, 2023; Vilks et al., 2022), porque provee herramientas —conocimientos y habilidades— para que las personas ganen competitividad, desarrollen sus capacidades de respuesta y tomen decisiones acertadas para identificar las prácticas delictivas y los riesgos (Kshetri, 2013; Li et al., 2024; Pham et al., 2021).

La ciberhigiene, inspirada en la salud pública, ha merecido múltiples interpretaciones en lo que va del presente siglo. No obstante, hay consenso en definirla como el conjunto de prácticas de ciberseguridad que puede aplicar un consumidor en línea o una organización para proteger sus activos y cautelar la seguridad e integridad de su información en internet ante cualquier amenaza criminal cibernética externa (Maennel et al., 2018; Ngo et al., 2024). Algunas prácticas de ciberhigiene son lanzar

alertas, aplicar estrategias de protección frente a diferentes modalidades fraudulentas, manejar contraseñas seguras y no compartirlas, mejorar la confianza en el entorno digital, sopesar si determinados rasgos humanos propios pesan en nuestro comportamiento frente a la ciberseguridad, entre otras (Jurevičienė et al., 2021; López et al., 2023; Ngo et al., 2024; Vishwanath et al., 2020). Entonces, se plantea que estas prácticas varían según los contextos, pero pueden conducir a una mejor comprensión de las amenazas y contribuir a evitarlas (Maennel et al., 2018). Son útiles para medir si subsisten riesgos desde el almacenamiento de la información hasta la transmisión y navegación (Esparza et al., 2020; Fandakly & Caporusso, 2020).

Desde la ciberhigiene, los sistemas informáticos son sociotécnicos (Latour, 2008). Esto quiere decir que se componen de múltiples piezas interconectadas, incluidos los actores humanos y no humanos (la tecnología y sus procesos). En esta alianza sociotécnica, los ciudadanos bien intencionados aportan a la ciberseguridad de las organizaciones y se convierten en parte de la solución del problema (Zimmermann & Renaud, 2019).

Agenda y periodismo de soluciones

La comunicación aporta en este proceso, primero, con dar cuenta del entramado de riesgos, actores y actantes involucrados; y, segundo, al articular a todos los protagonistas: recoge los problemas, los introduce en la agenda política y, eventualmente, promueve políticas que solucionen asuntos de interés público (Grau et al., 2010; Lahera, 2004).

La prensa es un intermediario en la construcción de una agenda mediática que conecte a todos los elementos de la información, en la *network agenda-setting* (Valenzuela & McCombs, 2019) y un actante de la función alfabetizadora. Se trate de medios estatales o privados, tradicionales, digitales o sociales, que funcionen bajo regímenes democráticos e incluso autoritarios, las audiencias mantienen interés en las noticias siempre que respondan a sus necesidades y urgencias (Kaspar & Fuchs, 2021; Katz et al., 1985).

En los últimos treinta años, el *public* o *civic journalism* Glasser & Craft, 1998; Nichols et al., 2006; Rosen, 1997) emergió como una opción para el funcionamiento de la democracia, mejorar las habilidades cívicas de los ciudadanos, influir en la formulación de políticas públicas y elevar el voluntariado. Surgió en un momento clave: la web había irrumpido, la relación de públicos y periodistas estaba cambiando y la prensa padecía una crisis de credibilidad. Como se preguntó Jay Rosen (1997), uno de los propulsores de la idea, "What type of relationship do we have with the community we 'serve'? [¿qué tipo de relación tenemos [los periodistas] con la comunidad a la que servimos?]" (p. 86).

En este siglo, el papel de la prensa ha sido medular frente al sostenimiento de la democracia. A pesar de ello, el periodismo profesional afronta una nueva crisis mundial provocada, en parte, por la erosión de las audiencias de los medios ante el desarrollo

de las redes sociales, servicios de mensajería personal y otras plataformas digitales abiertas (Altay et al., 2024; Pew Research Center, 2023; Reuters Institute, 2024); y su dificultad para responder a un entorno sociocultural en evolución y a las necesidades de públicos que no se sienten representados (Drok et al., 2018; Vásquez-Herrero, 2021).

Ante tal reto, organizaciones académicas y periodísticas postulan el periodismo constructivo (Casares, 2021; Codina, 2022) y el periodismo de soluciones (Lough & McIntyre, 2021; Thier & Namkoong, 2023) frente al rechazo a las noticias negativas (46 % de la población mundial prefieren noticias que propagan salidas y no problemas, según Reuters Institute [2024]). No se trata de publicar "buenas" noticias, sino de definir problemas, investigar sus causas, consecuencias y cómo los enfrentaron las víctimas, proponer alternativas y explorar en las lecciones aprendidas, ya sean exitosas o fallidas. Al exponer situaciones-límite de los protagonistas, con evidencia y antecedentes, se infiere que sus soluciones podrían replicarse (Solutions Journalism Network, 2024).

Hasta ahora, se ha hallado lo siguiente: primero, esta propuesta constructiva puede acercar la noticia a los públicos si los periodistas presentan y discuten sobre las salidas a los problemas; segundo, reduce el impacto de las noticias negativas y aumenta el interés de los usuarios, su conocimiento e, incluso, el deseo de participar en el tema; tercero, el público valora esta función periodística tanto como otras (Murray & Stroud, 2019). Entonces, de esta forma, las noticias pueden mostrar el capital social comunicativo que integra a las personas en la búsqueda de consensos, pueden crear oportunidades y contactos en torno a la información recibida como medio de vigilancia y pueden fomentar el compromiso cívico frente a la criminalidad (Boczkowski & Mitchelstein, 2015; Bourdieu, 1986, 1999; Putnam, 1995; Rojas et al., 2011).

Las redes, la televisión y la ciberseguridad

Se documenta que las personas valoran la inmediatez e interactividad de las plataformas sociales, la multidireccionalidad de sus mensajes y la posibilidad de generar contenido (Ben-Asher et al., 2024; Castells, 2010). En tanto, la televisión aparece como fuente confiable y su información es fidedigna (Martynov & Bundin, 2020; Silveira & Gancho, 2021).

En América Latina, la popularidad de las redes sobre otras plataformas institucionalizadas es ostensible. La excepción es la televisión, que sigue dominando la inversión publicitaria (CPI Research, 2023). Ambas plataformas se complementan, sobre todo en un contexto de crisis. Y es que, en materia de ciberseguridad, el predominio de los medios sociales puede facilitar una interacción más cooperativa, abierta y atractiva entre las comunidades virtuales. Su uso extendido las convierte en canales propicios para el intercambio de conocimientos y experiencias de higiene cibernética (Pham et al., 2021), tal como sucede en otros ámbitos de interés ciudadano (medio ambiente, salud, discapacidad y mitigación de discriminación) (Gómez-Marí et al., 2021; Primo et al., 2021; Rodríguez, 2024).

No se ha podido garantizar la eficacia de las redes en campañas sociales orientadas a consolidar actitudes o comportamientos saludables ni cambios en materia de prevención (Faus et al., 2022, p. 9). Por ello, como señalan algunos autores, es necesario ahondar en las ventajas de su uso, sobre todo en su relación con la televisión. Como segunda pantalla, los usuarios comparten mensajes sobre los programas, práctica que ha revolucionado las estrategias de la publicidad televisiva (Brubaker, 2010; Cremonesi et al., 2013; Kitsa & Mudra, 2018; Zhang & Liu, 2024). Además, gran parte de la innovación televisiva se da en espacios virtuales y en las redes sociales, con informes en vivo y servicios a pedido (Imre & Wenger, 2020).

METODOLOGÍA

Esta investigación de alcance exploratorio y descriptivo forma parte de un proyecto mayor sobre el problema del fraude informático en el debate público desde la perspectiva de la víctima, la autoridad y la prensa, a partir de la pandemia de COVID-19. En este artículo, exponemos los resultados referidos al uso de los medios de comunicación por las personas afectadas y sus percepciones sobre el papel que cumplen frente al delito. Enmarcado en un enfoque mixto, se han combinado elementos cuantitativos y cualitativos mediante dos instrumentos de recolección de datos (encuesta y entrevista) elaborados para este estudio.

Los objetivos específicos de esta investigación fueron los siguientes:

Objetivo 1: analizar el uso de los medios de comunicación por parte de las víctimas de fraude informático.

Objetivo 2: estudiar las percepciones de las víctimas sobre el papel que podrían cumplir los medios antes, durante y después de perpetrado el delito tras la experiencia vivida.

Universo

Personas residentes de Lima Metropolitana de los niveles socioeconómicos (NSE) alto (A), medio (B), bajo (C), muy bajo (D) y extrema pobreza (E); de uno u otro sexo, entre 18 y 70 años de edad e inscritas en el Registro Nacional de Identidad y Estado Civil (Reniec) para las Elecciones Regionales y Municipales 2022. El universo de estudio ascendió a 8 423 852 electores.

Marco muestral

Se basa en la información estadística sobre población electoral del Perú, elaborada por la Unidad de Planificación y Estadística del Reniec (2022); y el estimado de la población distribuida por NSE de Lima Metropolitana de la Asociación Peruana de Empresas de Investigación de Mercados (Apeim, 2021). Y, para cumplir las exigencias

de un marco muestral adecuado y actualizado, se trabajó con material de la cartografía a nivel de distrito, manzana y calle. Esta información fue obtenida de las páginas web del Instituto Nacional de Estadística e Informática (INEI) y la Guía de calles del Perú.

Diseño muestral

Para conocer la incidencia del fraude electrónico en los pobladores de Lima Metropolitana, se elaboró una muestra estadística centrada en los niveles socioeconómicos A, B y C, pues en ellos se observó mayor incidencia del tipo de fraude en estudio. El diseño muestral fue multietápico, probabilístico y estratificado por NSE.

Procedimiento de selección

Las unidades muestrales en cada etapa fueron las siguientes:

- Primera etapa: selección de 39 conglomerados de manzanas de viviendas en Lima Metropolitana de manera aleatoria.
- Segunda etapa: selección al azar de manzanas de viviendas al interior de cada conglomerado.
- Tercera etapa: selección de viviendas mediante el empleo de un salteador sistemático.
- Cuarta etapa: selección de las personas a encuestar mediante la aplicación de un filtro y cuotas de sexo y edad.

Muestra 1

Se calculó bajo el supuesto de la máxima dispersión ($p = q = 0{,}5$) y resultó un tamaño de 390 ciudadanos elegidos de forma aleatoria con base en una distribución demográfica con afijación proporcional (véanse las tablas 1 y 2). El máximo margen de error fue de $\pm$ 5 %, con un nivel de confianza de 95 %.

Tabla 1

Estructura de la muestra según zona

Zona	Distritos	Encuestas
1	Puente Piedra, Comas, Carabayllo	10
2	Independencia, Los Olivos, San Martín de Porres	20
3	San Juan de Lurigancho	16
4	Cercado, Rímac, Breña, La Victoria	55
5	Ate, Chaclacayo, Lurigancho, Santa Anita, San Luis, El Agustino	60
6	Jesús María, Lince, Pueblo Libre, Magdalena, San Miguel	30

(*continúa*)

(*continuación*)

Zona	Distritos	Encuestas
7	Miraflores, San Isidro, San Borja, Surco, La Molina	110
8	Surquillo, Barranco, Chorrillos, San Juan de Miraflores	30
9	Villa El Salvador, Villa María del Triunfo, Lurín, Pachacámac	20
10	Callao, Bellavista, La Perla, La Punta, Carmen de la Legua, Ventanilla, Mi Perú	39
Total		390

Tabla 2

Estructura de la muestra según nivel socioeconómico y género

NSE	Encuestas
Alto (A)	100
Medio (B)	85
Bajo (C)	205
Total	390
Género	Encuestas
Masculino	194
Femenino	196
Total	390

Muestra 2

Mediante un muestreo intencional, se contactaron a los encuestados que dejaron referencias personales, quienes nos acercaron a más informantes a través de la técnica de la bola de nieve. Se construyó una base de 71 personas de diferentes NSE y edades, hombres y mujeres en número equitativo, dispuestas a relatar sus historias. Aplicamos 25 entrevistas recurriendo al principio de saturación y según estos criterios de inclusión: las personas entrevistadas sufrieron un fraude; el delito se perpetró en agravio suyo cuando utilizaron sus tarjetas de crédito y débito (a octubre del 2023, casi siete millones de peruanos tenían una tarjeta de crédito, según la Asociación de Bancos [2022]); las víctimas tenían niveles educativos diferentes; las víctimas siguieron algún proceso de denuncia del delito ante una institución con injerencia en el problema (en el Perú son organismos estatales o independientes de control, reguladores y de sanción del fraude informático como: la Superintendencia de Banca, Seguros y AFP, el Instituto de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, el Defensor del cliente financiero, el Organismo Supervisor de Inversión Privada en Telecomunicaciones y el Poder Judicial) (véanse las tablas 3, 4 y 5).

Tabla 3

Perfil de las víctimas de fraude informático por zonas geográficas

Zona geográfica (Lima-Metropolitana)	Cantidad de entrevistas
Zona 1: Carabayllo	1
Zona 2: Los Olivos, San Martín de Porres	2
Zona 3: San Juan de Lurigancho	3
Zona 4: La Victoria	3
Zona 5: Ate, Santa Anita	3
Zona 7: Surco, La Molina	3
Zona 8: Chorrillos, Surquillo, San Juan de Miraflores	4
Zona 9: Villa El Salvador	2
Zona 10: Callao	2
Otros (Ancón y Lima)	2
Total	25

Nota. Adaptado de *Niveles socioeconómicos 2021*, de Asociación Peruana de Empresas de Investigación de Mercados, 2021, p. 26 (https://apeim.com.pe/wp-content/uploads/2022/08/2021-APEIM-NSE-Presentacion_Comite-Vfinal2.pdf).

Tabla 4

Perfil de las víctimas de fraude informático por modalidad

Modalidad	Cantidad de entrevistas
Presencial	17
Virtual	8
Total	25
Fechas	25 de octubre del 2023 al 2 de diciembre del 2023

Tabla 5

Perfil de las víctimas de fraude informático por nivel socioeconómico y edad

Nivel socioeconómico		Edad	
Alto	2	22-30	6
Medio	8	31-40	7
Medio bajo	3	41-50	7
Bajo	12	51-67	5
Total	25	Total	25

Técnicas de recopilación de datos

El cuestionario de veintidós preguntas se estructuró en cuatro secciones: experiencias personales o cercanas; seguimiento y sanción; panorama general; y fraude informático y uso de medios de comunicación, componente que se aborda en este artículo. Por el enfoque del estudio y la forma en que fueron construidos los ítems, la validez del cuestionario se hizo a través del coeficiente de la V de Aiken (Aiken, 1980; Navarrete, 2024), para lo cual fue sometido al juicio de tres expertos que evaluaron el nivel de pertinencia de los ítems y la redacción. La mayoría de ítems obtuvo un valor de V superior a 0,75, considerado adecuado para la validez del contenido. Los ítems con valores inferiores a 0,75 fueron revisados y modificados siguiendo las recomendaciones de los expertos. Luego, se aplicó una prueba piloto de diez encuestas a sujetos informantes con las características del perfil de personas a encuestar.

En cuanto a la entrevista, la guía de indagación constó de treinta y tres preguntas semiestructuradas y abiertas (nueve referidas a las percepciones sobre el papel de los medios) y se elaboró para el estudio a partir de una matriz cualitativa de categorías e indicadores derivados de los objetivos. La guía comprende cuatro temas: experiencia personal, impacto, afectación, emociones y sentimientos experimentados por las víctimas; nivel de conocimiento del fraude informático; respuesta y recuperación; y percepción sobre los medios de comunicación y sociales, cuyos resultados se presentan en este artículo.

La guía fue validada también por la V de Aiken, tras recabar los juicios de cuatro expertos, quienes evaluaron y aprobaron la pertinencia y la redacción de las preguntas. La mayoría de preguntas obtuvo un valor V superior a 0,85. Igualmente, aquellas con valores inferiores fueron revisadas y modificadas. Además, los expertos aprobaron la matriz de objetivos, categorías e indicadores y el acta de validación del instrumento y el consentimiento informado para que los entrevistados autoricen la grabación y difusión de sus declaraciones (se acordó mantener en reserva sus identidades).

Técnica de análisis de datos

Después de aplicar las encuestas se cumplieron estos pasos: el 100 % de cuestionarios se editaron para detectar posibles omisiones o errores sistemáticos; fueron digitados en una base de datos para su procesamiento, aplicando un plan de cuadros; los datos se editaron y digitalizaron en el *software* SPSS versión 28.0; y se realizó el análisis de las distribuciones de frecuencia expresadas en porcentajes en los cuadros estadísticos.

Los datos fueron objeto de un análisis descriptivo. Este artículo ha incluido los resultados relacionados con el uso de los medios de comunicación, que se operacionalizó en estas categorías: tipos de medios utilizados para informarse; tipos de

medios utilizados para difundir una queja, reclamo o denuncia; calificación del medio (más independiente y menos independiente); y nivel de confianza en el medio.

Los datos de la entrevista tuvieron una codificación cualitativa basada en dos estrategias descriptivas de Wolcott (1994): la técnica de ordenamiento del investigador o narrador y la técnica de efecto Rashomon. La primera permitió ordenar las reflexiones de los entrevistados según el marco analítico de la investigación, la revisión de la literatura y el orden cronológico de los eventos. La segunda facilitó el recojo de los testimonios, siguiendo los temas y categorías del estudio, para dar cuenta de la diversidad de versiones sobre el hecho, determinar patrones significativos y organizar la información para su posterior análisis sobre la finalidad del uso de los medios (información, denuncia, otro), resultados del uso de los medios (difunde agenda pública pendiente, experiencias, procesos, soluciones) y funciones atribuibles a los medios en la cobertura del delito (acompañar, representar, mediar, prevenir, educar, alfabetizar). En la revisión de la literatura, se siguieron los criterios del periodismo de soluciones que incluyeron la exposición periodística de problemas y soluciones; evidencias y antecedentes; implementación experta; resultados e inconvenientes; y lecciones aprendidas (McIntyre, 2019; Murray & Stroud, 2019; Solutions Journalism Network, 2024).

RESULTADOS

En este acápite, exponemos los hallazgos derivados del análisis del uso que las víctimas hacen de los medios de comunicación, el para qué y el porqué (objetivo 1); y del estudio de sus percepciones sobre la agenda ciudadana pendiente, es decir, sobre el papel que debieran cumplir las plataformas informativas frente al fraude informático (objetivo 2). Para ello, se triangularon los hallazgos provenientes de los datos estadísticos obtenidos de la encuesta con la información cualitativa recabada de las víctimas en las entrevistas. Y, sobre la base de esos resultados, se propusieron lineamientos de una estrategia informativa.

Uso de los medios

Sobre el uso de los medios por parte de las víctimas (objetivo 1), la encuesta reveló que Facebook, seguido de la televisión de señal abierta, fue el medio más utilizado por los ciudadanos para informarse sobre el fraude informático. En ambas plataformas, el mayor consumo se dio en los sectores socioeconómicos medios y bajos, que son los más afectados por la suplantación de identidad en compras fraudulentas por internet. Respecto, a las variables sexo y edad, hubo diferencias: los hombres y los jóvenes se informaron más por Facebook, mientras que las mujeres y los mayores de cuarenta años lo hicieron por televisión (véase la Tabla 6).

Tabla 6

*Porcentaje de plataformas utilizadas para informarse sobre el fraude informático**

Medio	Total	NSE			SEXO		EDAD			
		Alto	Medio	Bajo	Masculino	Femenino	18-27	28-37	38-47	48-70
Facebook	46,6	33	49,4	46,3	51,1	42,2	56,7	59,8	47,3	29,2
TV en señal abierta	44,5	22	43,5	45,5	41,7	47,3	35,2	36,0	45,0	57,0
WhatsApp	21,3	15	18,8	22,1	24,4	18,3	20,4	20,1	20,2	23,6
Conversaciones personales	18,4	22	29,4	15,6	16,6	20,2	12,8	16,4	15,6	26,0
TikTok	17,5	15	18,8	17,2	13,0	21,8	23,7	25,2	13,5	10,4
Televisión por cable	9,3	25	16,5	7,0	5,8	12,7	7,5	6,9	10,2	11,5
YouTube	7,8	8	9,4	7,4	8,6	7,0	5,6	11,4	8,4	6,2
Periódicos impresos	5,3	2	7,1	4,9	6,6	3,9	7,0	2,4	3,3	7,7
Instagram	5,0	12	9,4	3,7	5,3	4,7	9,5	7,6	2,1	2,1
Medios digitales	4,8	19	5,9	4,1	4,5	5,1	8,8	4,6	2,8	3,7
X (antes Twitter)	3,9	15	4,7	3,3	4,0	3,7	9,8	3,3	2,4	1,1
Emisoras de radio	3,8	4	5,9	3,3	3,0	4,6	1,5	1,5	2,9	7,8

Nota. * Base total de encuestados que sufrieron —o algún familiar o amigo— un fraude en los últimos cinco años.

La entrevista a las víctimas confirmó su preferencia por la televisión y las redes sociales, y les reconoció once funciones frente al fraude. Los entrevistados valoraron que la televisión en señal abierta difundiera más información que otras plataformas tradicionales, aunque en ocasiones se circunscribe solo a fuentes policiales y fraudes millonarios. No obstante, destacaron más a las redes, porque ofrecen una voz al ciudadano, celeridad, intermediación ante la autoridad y prevención del delito (véase la Tabla 7).

Tabla 7

*Funciones de los medios frente al fraude**

Funciones	Televisión	Medios sociales
Informan sobre fraudes/estafas informáticas	5	9
Difunden con celeridad		5
Alertan sobre los riesgos	1	3
Exponen modalidades de fraude	1	3
Exponen grandes casos mediáticos	1	
Recogen más denuncias/casos no atendidos	1	5

(*continúa*)

(*continuación*)

Funciones	Televisión	Medios sociales
Recogen testimonios de las víctimas		2
Recogen información de fuentes policiales	2	
Intermedian con la autoridad		1
Realizan campañas publicitarias	1	
Realizan campañas de prevención del delito		1
Total	12	29

Nota. * Según respuestas de las víctimas entrevistadas.

Plataformas para denunciar

Saber qué difunden las diferentes plataformas y, eventualmente, utilizarlas para informarse no implica que los ciudadanos recurran a ellas para exponer sus casos al ser víctimas de un fraude. Y es que la tendencia prevaleciente en la mayoría de encuestados fue no denunciar en ninguna plataforma, sobre todo en segmentos populares que no presentaron quejas. Esta postura se constató en hombres y mujeres de todos los grupos etarios, con énfasis en mayores a cincuenta años. Quienes socializaron sus casos en el espacio público lo hicieron por Facebook (véase la Tabla 8).

Tabla 8

*Medio de difusión de queja**

Medio	Total	Edad			
		18-27	28-37	38-47	48-70
No difundió	65,9	67,6	60,8	61,9	71,5
Facebook	16,2	13,9	19,2	26,1	7,9
WhatsApp	3,6	5,8	4,8	0,0	3,9
TV en Señal abierta	2,2	0,0	14,0	1,4	4,8
Medios digitales	1,3	3,9	2,1	0,0	0,0
TikTok	1,2	1,5	1,0	2,7	0,0
X (antes Twitter)	0,6	1,7	0,1	0,0	0,7
Emisoras de radio	0,5	0,0	1,0	0,0	0,7
Periódicos impresos	0,0	0,0	0,0	0,1	0,0
No sabe	8,0	5,6	8,2	7,8	9,7
No contesta	0,5	0,0	1,4	0,0	0,7

Nota. * Base total de encuestados que sufrieron —o algún familiar o amigo— un fraude en los últimos cinco años.

Factores de independencia, credibilidad e impotencia

El uso de los medios como plataformas de denuncia depende de la independencia y credibilidad que ofrecen al público. En opinión de los encuestados, las redes sociales (38,8 %) y la televisión (23,6 %) fueron más independientes que el resto de plataformas informativas. En cuanto a la credibilidad, la encuesta arrojó que 74,8 % confía poco o no confía en la información sobre el fraude informático que propalan los medios de comunicación en general.

Al buscar una explicación a estas preferencias, las entrevistas permitieron concluir que las víctimas sí estaban dispuestas a denunciar por otras razones. Por ejemplo, ante la falta de respuestas de los entes responsables de atender el problema, la queja en las redes sociales se puede convertir en una tabla de salvación para agilizar los procesos. Los usuarios sostuvieron que las entidades financieras, principalmente, temen al escrutinio público en los medios sociales. Igualmente, estas plataformas son espacios amigables, de libre expresión ciudadana y con poder: ejercen presión sobre los organismos reguladores o responsables de atender la queja, reclamo o denuncia; visibilizan el caso y a la víctima. Para otros usuarios, que temen al aislamiento, la represalia o la condena pública, la queja mediática deviene en una acción extrema. He aquí algunas respuestas:

- No confío en las redes, pero tampoco niego que tengan algún éxito (C. M. F.).
- Veo que algunos llegan a ese extremo [denunciar por las redes], pues no tienen respuestas a sus reclamos de la comisaría, del banco ni de nadie (R. C. T.).
- Obtenemos respuesta más rápida del banco y más personas se unen a nuestros reclamos. Creo que, para cautelar su buena imagen, nos hacen caso cuando denunciamos por las redes (A. O. G.).
- Cualquier denuncia a través de una red social se hace más visible y ayuda al proceso del reclamo (D. G. A.).
- Expuse mi caso en Facebook, muchos comentaron que les había pasado lo mismo y me dieron su opinión. Lo hice por impotencia cuando acudí a una entidad reguladora en busca de respaldo y no lo encontré (S. H. C.).

La agenda ciudadana pendiente

El trabajo de campo arrojó que las víctimas eran hombres y mujeres peruanos de todos los grupos etarios, casi en las mismas proporciones: víctimas principalmente de *phishing*, durante y después de la pandemia de COVID-19. Aseguraron estar informados y muy informados sobre el delito, mas no diferenciaron sus modalidades ni lo denunciaron en las instancias correspondientes. La encuesta, además, aportó indicadores a considerar respecto a sus percepciones sobre los medios (objetivo 2).

Nivel de conocimiento

El 42,1 % de encuestados sabía que la ciberdelincuencia englobaba los delitos cometidos por internet o medios informáticos. Pero, un porcentaje ligeramente superior (43,4 %) declaró estar poco o nada informado sobre los fraudes informáticos. La mayoría pertenecía a sectores populares, son varones y se ubicaban en dos grupos etarios: jóvenes (18 a 27 años) y adultos mayores (48 a 70 años). Desconocían los mecanismos requeridos para administrar información sensible.

Procesos

La mayoría de encuestados ignoraba los procesos para presentar una queja o hacer un seguimiento de las denuncias. Algunos nunca presentaron un reclamo (21,6 %) y un porcentaje similar solo lo hizo ante la entidad comercial o financiera involucrada (21,4 %). Otros resultados: el 17,1 % asumió las obligaciones del fraude y apenas 14,1 % recuperó el monto sustraído de sus cuentas.

Instancias

La mayoría desconocía las instancias a las cuales acudir en estos casos. Solo el 14,9 % hizo seguimiento de sus denuncias ante bancos y el 6 % ante la policía. Las entrevistas revelaron que las víctimas demandaban mayor atención de los medios y de las redes informativas digitales de las entidades involucradas: bancos, financieras, la policía, entes reguladores. Estos organismos, afirmaron los entrevistados, no responden a sus demandas, reaccionan parcialmente ante la denuncia en las redes sociales e institucionales y no realizan campañas de comunicación, orientación ni prevención:

- Los bancos responden en sus redes sociales, pero no siempre. Ante ello, algunas personas etiquetan a los funcionarios en LinkedIn y consiguen su atención. Nadie quiere ver mellado su prestigio (V. S. C.).
- Todas las comisarías deberían producir y difundir videos de orientación en sus cuentas de TikTok o de Instagram sobre qué hacer, a fin de que sus seguidores sepan dónde acudir y ponerse a su servicio. Hoy no lo hacen (R. C. U.).
- Por las redes, las autoridades podrían publicar tutoriales de cómo prevenir un fraude. Eso sería más efectivo y más rápido (P. R. P.).
- Se necesita un mix: exposición de casos reales y participación de los bancos para darle soporte. Ello repercutiría en una mejor imagen del banco (R. C. T.).
- Más que denunciar a través de sus redes sociales, los bancos y entidades reguladoras, deberían comunicar toda la información que necesitamos para cuidarnos de las estafas. Hoy ofrecen diversos productos, pero no dicen cómo protegernos (S. S. C.).

Asimismo, los entrevistados solicitaron a los medios que asumieran el rol de un defensor del consumidor o de un alfabetizador mediático digital. Así, podrían exigir de las entidades involucradas respuestas sobre los casos expuestos, especialmente de las víctimas más desprotegidas. Para las víctimas, la estrategia mediática debía ser digital a través de las redes sociales, porque les dan voz, impactan y ofrecen mayor confianza:

- Como el problema ocurre en internet, la educación de las personas debe brindarse en ese entorno digital para que todos sepan manejarse en la virtualidad. Quizá deberían enfocarse en los grupos etarios mayores, los más susceptibles a sufrir un fraude, aunque los menores también pueden ser víctimas (A. O. P.).
- Hay personas que aprenden a cuidarse gracias a los testimonios de las víctimas que difunden sus experiencias (S. S. C.).
- Los testimonios de las víctimas impactan. Cuando ves y escuchas a una persona como tú con ese problema, tomas conciencia del peligro al que estamos expuestos (V. K. T.).
- Las redes son una ventana, porque los medios de comunicación son empresas privadas, cuyos dueños poseen otras empresas con intereses que defenderán (C. G. C.).

Lineamientos de una estrategia informativa

A la luz de los hallazgos, esta investigación alcanzó lineamientos de una estrategia informativa que, según la información recabada en el trabajo de campo, debería considerar cuatro funciones:

1. Escuchar: hay un público que espera ser atendido, exponer su caso a las partes involucradas y a los medios.
2. Denunciar: desde la perspectiva del ciudadano, esta función recae en el periodismo de investigación.
3. Mediar: solicitar información a las entidades involucradas sobre las denuncias de las víctimas.
4. Orientar: desarrollar una agenda de ciberhigiene, principalmente en los medios digitales.

En aplicación de un periodismo de soluciones, los medios debieran exponer los problemas, tales como modalidades de fraude, vacíos en la información financiera y la eventual responsabilidad de las instituciones y organizaciones involucradas; las evidencias (como la estadística del delito y amenazas futuras), tales como canales de atención para ejercer el derecho al reclamo y a la denuncia, las normas y sanciones

(que obran en manos de bancos, organismos reguladores y estamentos judiciales); y las soluciones, es decir, los testimonios de quienes evitaron caer en las manos del suplantador o que salieron airosos o no de un fraude, los mecanismos de la prevención que aplicaron, los inconvenientes que afrontaron para cautelar su identidad y cambiar la forma en que suelen administrar su información personal, y las lecciones aprendidas (Cancela et al., 2021; Walth et al., 2019).

DISCUSIÓN Y CONCLUSIONES

El papel de los medios informativos y de los medios sociales es crucial no solo en la difusión del fraude en línea, sino en la alfabetización o educación financiera de las personas para que sepan prevenir el delito. Pero, respondiendo al objetivo general de esta investigación, podría afirmarse que la percepción de las víctimas es que la prensa peruana no socializa de manera suficiente las experiencias que recoge en sus plataformas informativas; tampoco proporciona orientación suficiente, oportuna, constructiva, receptiva ni solidaria. O sea, aún esperan la ejecución de un programa de higiene cibernética (Cain et al., 2018) que exponga y explique el alcance de prácticas de ciberseguridad, alfabetizadoras y que ahonden en las amenazas, las soluciones y la prevención (Van Zeeland & Pierson, 2024).

Ello confirma la necesidad de brindar a los públicos de conocimientos y habilidades a través de la fijación de una agenda de servicio, amplia e interconectada (Valenzuela & McCombs, 2019). Se trata de información que no está llegando a los usuarios y que demanda abrir espacios para la interacción, la creación de redes y comunidades, de consensos y soluciones. De esta forma, el medio no solo cumpliría el rol que los ciudadanos le reclaman —como mediador ante las partes involucradas y con compromiso cívico frente a la criminalidad—, sino en la consolidación de un capital social comunicativo (Putnam, 1995; Rojas et al., 2011).

Una agenda enfocada en los ciudadanos puede atraer otra vez la atención de los jóvenes a las noticias (Drok et al., 2018; Ha et al., 2018). A la larga, puede redefinir la relación de la prensa con el público (Rosen, 1997) y reducir la brecha que hoy separa al público de los medios. Dicha brecha afecta tres funciones básicas del periodismo: la fijación de la agenda, el servicio público y la creación de espacios para la deliberación (Boczkowski & Mitchelstein, 2015).

Respecto al primer objetivo específico de este estudio, cabe señalar que el uso frecuente de las redes sociales y de la televisión por parte de las víctimas revela no solo la preferencia por dos plataformas más populares en el Perú. En primer lugar, hay un reconocimiento hacia la labor que estas cumplen, desde la perspectiva de los encuestados y entrevistados, en materia de información y en su revalorización como personas, después de haber sido objeto de ataques de la delincuencia y de sufrir los

embates de la llamada ingeniería social criminal (ataques persuasivos que buscan engañar apelando al miedo, la emoción o la confianza de la víctima) (Kshetri, 2013). El estudio ratifica que, como en otros países, en el Perú todos los grupos etarios carecen de experiencia para identificar los niveles de riesgo, anticipar y prevenir los daños, y que la capacidad de la víctima para evaluar críticamente la situación y elegir el comportamiento adecuado será decisiva (Vilks et al., 2022).

En segundo lugar, da cuenta de la relación hombre-máquina (Latour, 2008) que las víctimas han entablado con las redes y la televisión, y que coloca la tecnología al servicio de las necesidades de un grupo de personas afectadas por la criminalidad. En esta alianza sociotécnica, aprenden de la experiencia y de los resultados positivos y negativos de manera flexible, y generan comunicación, colaboración y resiliencia (Zimmermann & Renaud, 2019).

La preferencia por las redes sociales (en menores de 40 años) y por la televisión (en mayores de 40 años) deja por fuera a otras plataformas informativas cuyo concurso en una estrategia de ciberseguridad es prioritaria. Según las entrevistas, se trata de medios que actualmente no generan credibilidad ni confianza, que aparecen como poco independientes respecto al poder de entidades involucradas. Se trata de perspectivas propias del contexto peruano que confirman que no hay dos campañas de concientización y capacitación iguales, que cada esfuerzo de alfabetización financiera dependerá de las realidades locales en donde se perpetró el delito y de los públicos involucrados (Maennel et al., 2018).

No obstante, respecto al segundo objetivo específico del estudio, sobre las percepciones de las víctimas respecto a una agenda de ciberseguridad, se podría concluir que apelan, en primer lugar, a los principios elementales del periodismo (veracidad y actualidad), también a la relevancia social, el análisis de las consecuencias en la vida de las personas y empatía, y ponerse en la cabeza del público. Tareas que demandan mayor investigación y esfuerzo, así como un periodismo con mayor sensibilidad social. En segundo lugar, ponen de manifiesto la necesidad de usar nuevos lenguajes en el abordaje de una estrategia que debe ser prioritariamente virtual y generadora de contenidos, producidos con un público especial y para él.

La labor que se solicita no es solo informativa, sino que responde a una función mayor. Desde la ciberhigiene, se trata de contribuir a la mejora del conocimiento y de las habilidades de la población para enfrentar el delito, señalar la necesidad de un cambio de comportamiento sobre la información personal sensible, valorar la defensa de nuestros derechos y deberes, y felicitar los esfuerzos individuales frente al abuso de terceros. Desde lo periodístico, los ciudadanos le piden a la prensa denunciar sus casos, mediar ante los organismos involucrados e indiferentes ante las pérdidas, y defender los derechos de los consumidores financieros.

Según la literatura revisada, se trata de funciones aplicables en países donde las víctimas no están capacitadas para enfrentar al delito, sea porque carecen de información para adelantarse al riesgo o de habilidades para prevenirlos críticamente (Vilks et al., 2022). Pero el aumento de la comisión del delito del fraude informático constituye uno de los más complejos y acuciantes de la sociedad actual; por ello, amerita un análisis más profundo sobre la labor del periodismo como generador de políticas públicas. Este tema, que no fue abordado en este estudio, podría ser motivo de otra investigación basada en fuentes expertas, organismos reguladores del sistema financiero, autoridades públicas y privadas involucradas en la prevención de este delito.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORES

Conceptualización, M. M. M.; metodología, M. M. M., R. N. O. y M. D. V.; análisis de datos, M. M. M., R. N. O. y M. D. V.; resultados, M. M. M., R. N. O. y M. D. V.; escritura (borrador original) M. M. M; escritura (revisión y edición) M. M. M., R. N. O. y M. D. V.

AGRADECIMIENTO

Este artículo se desarrolló como parte del proyecto "El fraude informático en el debate público desde la perspectiva de la víctima, la autoridad y la prensa", financiado por el Instituto de Investigación Científica de la Universidad de Lima (IDIC). Fue revisado y aprobado por el Comité de Integridad y Ética de la Facultad de Comunicación de la Universidad de Lima.

REFERENCIAS

Aiken, L. (1980). Content validity and reliability of single items or questionnaires. *Educational and Psychological Measurement*, *40*(4), 955-959. https://doi.org/10.1177/001316448004000419

Altay, S., Fletcher, R., & Nielsen, R. K. (2024, 14 de mayo). News participation is declining: Evidence from 46 countries between 2015 and 2022. *New Media & Society*. https://doi.org/10.1177/14614448241247822

Arief, B., & Bin Adzmi, M. A. (2015). Understanding cybercrime from its stakeholders perspectives: Part 2-defenders and victims. *IEEE Security & Privacy*, *13*(2), 84-88. https://doi.org/10.1109/MSP.2015.44

Asociación de Bancos. (2022, 27 de octubre). *Tarjetas de crédito de bancos*. https://www.asbanc.com.pe/estadisticas-del-sector

Asociación Peruana de Empresas de Investigación de Mercados. (2021). *Niveles socioeconómicos 2021*.

Baraković, S., & Baraković Husic, J. (2023). Impact of COVID-19 pandemic circumstances on cyber hygiene of university students. *International Journal of Human-Computer Interaction, 40*(19), 5961-5979. http://doi.org/10.1080/10447318.2023.2247577

Ben-Asher, S., Ben-Atar, E., & Lavi, Tamar (2024). Time and ethics in delivering bad news in institutionalized and social media. *Journal of International Crisis and Risk Communication Research*, *7*(1), 113-139. http://doi.org/10.56801/jicrcr.V7.i1.4

Boczkowski, P., & Mitchelstein, E. (2015). *La brecha de las noticias: la divergencia entre las preferencias informativa de los medios y el público*. Manantial.

Bourdieu, P. (1986). The forms of capital. En J. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241-258). Greenwood.

Bourdieu, P. (1999). *Meditaciones pascalianas*. Anagrama.

Brubaker, J. (2010). Internet and television are not substitutes for seeking political information. *Communication Research Reports*, *27*(4), 298-309. https://doi.org/10.1080/08824096.2010.518906

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Journal of Crimimology*, *47*(3), 391-408. https://doi.org/10.1177/0004865814521224

Buzzio-García, J., Salazar-Vilchez, V., Moreno-Torres, J., & Leon-Estofanero, O. (2021). Review of cybersecurity in Latin America during the COVID-19 pandemic. A brief overvie. En *IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)*. IEEE. http://www.doi.10.1109/ETCM53643.2021.9590693

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45. https://doi.org/10.1016/j.jisa.2018.08.0022

Cancela, P., Gerber, D., & Dubied, A. (2021). "To me, it's normal journalism": Professional perceptions of investigative journalism and evaluations of personal commitment. *Journalism Practice*, *15*(6), 878-893. https://doi.org/10.1080/17512786.2021.1876525

Carter, E. (2023). Confirm not command: Examining fraudsters' use of language to compel victim compliance in their own exploitation. *The British Journal of Criminology*, *63*(6), 1405-1422. https://doi.org/10.1093/bjc/azac098

Casares, A. (2021). *La hora del periodismo constructivo*. Astrolabio.

Castells, M. (2010). *Comunicación y poder*. Alianza Editorial.

Codina, L. (2022, 23 de septiembre). *Periodismo de soluciones: definiciones y guía de recursos*. https://www.lluiscodina.com/periodismo-de-soluciones/

Consejo Nacional de Política Criminal. (2020). *Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú*. Ministerio de Justicia y Derechos Humanos; Observatorio Nacional de Política Criminal. https://cdn.www.gob.pe/uploads/document/file/5948093/5270009-diagnostico-situacional-multisectorial-sobre-la-ciberdelincuencia-en-el-peru.pdf

CPI Research. (2023). *Evolución de la inversión publicitaria en las plataformas tradicionales y digitales. Nivel nacional 2018/2022*. https://cpi.pe/images/upload/paginaweb/archivo/26/MARKET%20REPORT_2023_2-1.pdf

Cremonesi, P., Pagano, R., Pasquali, S., & Turrin, R. (2013). TV program detection in tweets. En *EuroITV '13: Proceedings of the 11th European conference on interactive TV and video* (pp. 45-53). Association for Computing Machinery. https://doi.org/10.1145/2465958.2465960

Drew, J. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, *6*(1), 17-33. https://doi.org/10.1108/JCRPP-12-2019-0070

Drok, N., Hermans, L., & Kats, K. (2018). Decoding youth DNA: The relationship between social engagement and news interest, news media use and news preferences of Dutch millennials. *Journalism*, *19*(5), 699-717. https://doi.org/10.1177/1464884917703469

Esparza, J., Caporusso, N., & Walters, A. (2020, 4 de julio). Addressing human factors in the design of cyber hygiene self-assessment tools. En I. Corradini, E. Nardelli & T. Ahram (Eds.), *Advances in human factors in cybersecurity* (pp. 88-94). https://doi.org/10.1007/978-3-030-52581-1_12

Fandakly, T., & Caporusso, N. (2020). Beyond passwords: Enforcing username security as the first line of defense. En I. Corradini, E. Nardelli & T. Ahram (Eds.), *Advances in human factors in cybersecurity* (pp. 48-58). Springer. https://doi.org/10.1007/978-3-030-20488-4_5

Faus, M., Alonso, F., Javadinejad, A., & Useche, S. (2022). Are social networks effective in promoting healthy behaviors? A systematic review of evaluations of public health campaigns broadcast on Twitter. *Front. Public Health*, *10*. https://doi.org/10.3389/fpubh.2022.1045645

Fundación Gabo. (2020, 6 de noviembre). *Contar una historia con números: de las políticas públicas al enfoque de soluciones. Periodismo de soluciones*. https://

fundaciongabo.org/es/blog/periodismosoluciones/contar-una-historia-con-numeros-de-las-politicas-publicas-al-enfoque-de

García-Juárez, P. (2016). *Riesgos informáticos enfocados en la banca* [Sesión de conferencia]. Conferencia del Centro de Estudios de Seguridad, Perú, Lima.

Glasser, T., & Craft, S. (1998). Public journalism and the search for democratic ideals. En T. Liebes & J. Curran (Eds.), *Media, ritual and identity* (pp. 203-218). Routledge.

Gómez-Marí, I., Sanz-Cervera, P., & Tárraga-Mínguez, R. (2021). Hoy es mi día: análisis del impacto de las campañas de sensibilización sobre diversidad funcional en prensa, Google y Twitter. *International Journal of Environmental Research and Public Health*, *18*(15), 7789. https://doi.org/10.3390/ijerph18157789

Grau, M., Íñiguez-Rueda, L., & Subirats, J. (2010). La perspectiva sociotécnica en el análisis de políticas públicas. *Psicología Política*, (41), 61-80. https://www.uv.es/garzon/psicologia%20politica/N41-4.pdf

Ha, L., Xu, Y., Yang, C., Wang, F., Yang, L., Abuljadail, M., Hu, X., Jiang, W., & Gabay, I. (2018). Decline in news content engagement or news medium engagement? A longitudinal analysis of news engagement since the rise of social and mobile media 2009-2012. *Journalism*, 19(5), 718-739. https://doi.org/10.1177/1464884916667654

Hakak, S., Zada Khan, W., Imran, M., Choo, R., & Shoaib, M. (2020). Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access*, *8*, 124134-124144. https://doi.org/10.1109/ACCESS.2020.3006172

Holt, T. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*. https://doi.org/10.1016/j.chb.2022.107493

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ikbal, M., Rosidi, R., & Andayani, W. (2022). Critical dramaturgy approach: Research epistemology in the field of fraud action study. *Economic Alternatives*, *4*, 788-808. https://doi.org/10.37075/EA.2022.4.12

Imre, I., & Wenger, D. (2020). Where newsroom leaders see technology facilitating innovation in local TV news. *Electronic News*, *14*(4), 151-167. https://doi.org/10.1177/1931243120963705

Interpol. (2022, 10 de noviembre). *COVID-19 cyberthreats*. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

Jiang, X., Liu, L., Wu-Ouyang, B., Chen, L., & Lin, H. (2024). Which storytelling people prefer? Mapping news topic and news engagement in social media. *Computers in Human Behavior*, 158. https://doi.org/10.1016/j.chb.2024.108248

Jurevičienė, A., Brilingaitė, A., & Bukauskas, L. (2021). Digital human in cybersecurity risk assessment. En D. D. Schmorrow & C. M. Fidopiastis (Eds.), *Augmented Cognition* (pp. 418-432). Springer Nature. https://doi.org/10.1007/978-3-030-78114-9_29

Kaspar, K., & Fuchs, L. A. M. (2021). Who likes what kind of news? The relationship between characteristics of media consumers and news interest. *Sage Open*, *11*(1), 1-12. https://doi.org/10.1177/21582440211003089

Katz, E., Blumer, J. G., & Gurevitch, M. (1985). Usos y gratificaciones de la comunicación de masas. En M. Moragas (Ed.), *Sociología de la comunicación de masas* (Vol. 2, pp. 127-171). Gustavo Gili.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501. https://journals.sagepub.com/doi/pdf/10.1177/10439862211027986

Kitsa, M., & Mudra, I. (2018). Social media tools for TV programmes promotion. *Communication Today*, *9*(2), 56-72.

Kshetri, N. (2013). Global Cybersecurity: Issues and Concerns. *Journal of Global Information Technology Management*, *16*(4), 1-5. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Global_2013.pdf

Lahera, E. (2004). *Política y políticas públicas*. Comisión Económica para América Latina y el Caribe. https://repositorio.cepal.org/entities/publication/e77dfbfc-ea99-4cdb-90cd-c8280b645b8a

Latour, B. (2008). *Reensamblar lo social. Una introducción a la teoría del actor-red*. Manantial.

Li, P., Li., Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics and Finance*, *91*, 364-377. https://doi.org/10.1016/j.iref.2024.01.056

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, *52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

López Gorostidi, J. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Estudios de Deusto*, *68*(1), 201-221. http://www.doi.10.18543/ed-68(1)-2020pp201-221

López, A., Ventura, R., Prieto, M., & Salazar, R. (2023). Cybersecurity among university students from generation Z: A comparative study of the undergraduate programs in administration and public accounting in two Mexican universities. *TEM Journal*, *12*(1), 503-511. https://doi.org/10.18421/TEM121-60

Lough, K., & McIntyre, K. (2021). A systematic review of constructive and solutions journalism research. *Journalism*, *24*(5), 1069-1088. https://doi.org/10.1177/14648849211044559

Maennel, K., Mäses, S., & Maennel, O. (2018). Cyber hygiene: The big picture. En N. Gruschka (Ed.), *Secure IT Systems* (pp. 291-305). Springer. https://link.springer.com/chapter/10.1007/978-3-030-03638-6_18

Martynov, A., & Bundin, M. (2020). Policy & regulation against fake news: Case of Russia. En S.-J. Eom & J. Lee (Eds.), *Dg.o '20: The 21st Annual International Conference on Digital Government Research* (pp. 346-347). https://doi.org/10.1145/3396956.3397866

Mayer Lux, L., & Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151-184. https://doi.org/10.5354/0719-2584.2020.57149

McIntyre, K. (2019). Solutions journalism: The effects of including solution information in news stories about social problems. *Journalism Practice*, *13*(8), 1029-1033, https://doi.org/10.1080/17512786.2019.1640632

Mendivil, J., Sanz, B., & Gutiérrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit. Revista de Medios y Educación*, (63), 197-225. https://dialnet.unirioja.es/servlet/articulo?codigo=8272071

Murray, C., & Stroud, N. J. (2019). *The keys to powerful solutions journalism.* The University of Texas at Austin, Center for Media Engagement. https://mediaengagement.org/research/powerful-solutions-journalism/

Navarrete, J. (2024). Content validation of a satisfaction survey for a training activity for a company based on empirical comparison by expert judgment. En J. A. de Carvalho, J. Sousa, J. Coelho, F. García-Peñalvo & A. García-Holgado (Eds.), *Proceedings of TEEM 2023* (pp. 1168-1177). Springer Natura. https://doi.org/10.1007/978-981-97-1814-6_114

Ngo, F. T., Agarwal, A., & Holman, K. (2024). Cyber hygiene and cyber victimization among limited English proficiency (LEP) internet users: A mixed-method study. *Victims & Offenders*, 1-22. https://doi.org/10.1080/15564886.2024.2329765

Nichols, S., Friedland, L., Rohas, H., & Cho, J. (2006). Examining the effects of public journalism on civil society from 1994 to 2002: Organizational factors, project features, story frames, and citizen engagement. *Journalism & Mass Communication Quarterly*, *83*(1). http://www.doi.org/10.1177/107769900608300106

Nuredini, A. (2014). Challenges in commbating the cyber crime. *Mediterranean Journal of Social Sciences*, *5*(19), 592-599. http://dx.doi.org/10.5901/mjss.2014.v5n19p592

Pew Research Center. (2023, 14 de septiembre). *Network news fact sheet*. https://www.pewresearch.org/journalism/fact-sheet/network-news/

Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. *Australasian Journal of Information Systems*, *25*. https://doi.org/10.3127/ajis.v25i0.2177

Policía Nacional del Perú. (2022a). *Anuario estadístico PNP.* https://www.policia.gob.pe/estadisticopnp/documentos/anuario-2022/anuario-estadistico-policial-2022.pdf

Policía Nacional del Perú. (2022b). *Boletín Estadístico Policial 2022 - II Trimestre. Sistema de denuncias policiales.* https://www.policia.gob.pe/estadisticopnp/documentos/boletin-2022/II%20BOLETIN%202022%20DIRTIC%20PNP.pdf

Primo, F., Romanovsky, A., De Mello, R., García, A., & Missier, P. (2021). A customisable pipeline for the semi-automated discovery of online activists and social campaigns on Twitter. *World Wide Web*, *24*, 1235-1271. https://doi.org/10.1007/s11280-021-00887-2

Proofpoint. (2019). *2019 human factor: Today's cyber attacks target people – How to keep them safe*. https://www.proofpoint.com/us/resources/webinars/human-factor-2019

Putnam, R. (1995). Bowling alone: America's declining social capital. *Journal of Democracy*, *6*(1), 65-78. https://doi.org/10.1353/jod.1995.0002

Reuters Institute. (2024). *Digital news report 2024*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024

Rodríguez, J. (2024). Impacto de la comunicación en Twitter en el movimiento ambientalista durante la COP15. *Revista de Comunicación*, *23*(1), 485-505. https://doi.org/10.26441/RC23.1-2024-3383

Rodríguez-Rodríguez, V., Pérez-Garinb, D., Recio-Saboya, P., & Rico-Gómez, A. (2020). Fraudes financieros, salud y calidad de vida: un estudio cualitativo. *Gaceta Sanitaria, 34*(3), 268-275. https://doi.org/10.1016/j.gaceta.2019.11.006

Rojas, H., Shah, D., & Friedland, L. A. (2011). A communicative approach to social capital. *Journal of Communication*, *61*(4), 689-712, http://www.doi.org/10.1111/j.1460-2466.2011.01571.x

Rosen, J. (1997). In quest of journalism. *Index on Censorship*, *26*(3), 81-89. https://doi.org/10.1177/030642209702600315

Sánchez Henríquez, J., Neira Cortes, P., & Severino González, P. (2022). Fraude: una mirada global a su desarrollo conceptual. *Revista Venezolana de Gerencia*, *27*(99), 884-910. https://doi.org/10.52080/rvgluz.27.99.3

Sencan, I., & Soydal, I. (2023). Haber okuryazarlığı eğitimi alan öğrencilerin haber algısı. *Bilgi Dünyası*, *24*(2), 1-31. https://doi.org/10.15612/BD.2023.717

Silveira, P., & Gancho, S. (2021). University students engagement with fake news: the portuguese case. *Revista Observatório*, *15*(1), 23-37. http://dx.doi.org/10.15847/obsOBS15120211696

Solutions Journalism Network. (2024). *Responses to problems are newsworthy*. https://www.solutionsjournalism.org/

Thier, K, & Namkoong, K. (2023). Identifying major components of solutions-oriented journalism: A review to guide future research. *Journalism Studies*, *24*(12), 1557-1574. https://doi.org/10.1080/1461670X.2023.2230314

Unidad de Planificación y Estadística del Reniec. (2022). *Población electoral, año 2022*. Registro Nacional de Identificación y Estado Civil. https://identidad.reniec.gob.pe/estadisticas

Valenzuela, S., & McCombs, M. (2019). The agenda-setting role of the news media. En D. W. Stocks, M. B. Salwen & K. C. Eichhorn (Eds.), *An integrated approach to communication theory and research* (3.ª ed., pp. 99-112). Routledge.

Van de Weijer, S., Leukfeldt, R., & Monevaa, A. (2023). Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Computers & Security*, *139*, 103693. https://doi.org/10.1016/j.cose.2023.103693

Van Zeeland, I., & Pierson, J. (2024). Changing the whole game: effects of the COVID-19 pandemic's accelerated digitalization on Europa bank staff's data protection capabilities. *Financial Innovation*, *10*(29). https://doi.org/10.1186/s40854-023-00533-y

Vásquez-Herrero, J. (2021). Nuevas narrativas en los cibermedios: de la disrupción a consolidación de formatos y características. *Estudios sobre el Mensaje Periodístico*, *27*(2), 685-696. https://dx.doi.org/10.5209/esmp.70222

Vilks, A., Kipane, A., Kudeikina, I., Palkova, K., & Grasis, J. (2022). Criminological aspects of current syber security. *Law, State and Telecommunications Review*, *14*(2), 94-108. https://doi.org/10.26512/lstr.v14i2.41411

Vishwanath, A., Seng Neo, L., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*. https://doi.org/10.1016/j.dss.2019.113160

Walth, B., Dahmen, N. S., & Thier, K. (2019). A new reporting approach for journalistic impact: Bringing together investigative reporting and solutions journalism. *Newspaper Research Journal*, *40*(2), 177-189. https://doi.org/10.1177/0739532919834989

Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. *Sage Open*, *13*(4). https://doi.org/10.1177/21582440231217720

Wolcott, H. (1994). *Transforming qualitative data: Description, analysis, and interpretation*. Sage Publications.

World Economic Forum. (2022). *The Global Risk Report* (17.ª ed.). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Zhang, J., & Liu, F. (2024). Second screen synergy: Exploring the socio-economic impact of dual screen engagement in television consumption. *Journal of the Knowledge Economy*, *15*, 20196-20228. https://doi.org/10.1007/s13132-024-01945-6

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005


FONDO
EDITORIAL
ULIMA