Prisma Social revista de ciencias sociales , No. 53
Abril 2026 e-ISSN 1989-3469. pp 95-112
DOI: https://doi.org/10.65598/rps.6015

Aproximación educativa a percepciones sobre riesgos online y protección de datos personales

Educational approach to perceptions of online risks and personal data protection

María-Jesús Gallego-Arrufat[1], Norma Torres-Hernández[2], María del Mar García-Ruiz[3], Antonio Teba-López[1]
[1]Universidad de Granada, España
[2]Universidad de Jaén, España
[3]Centro de Magisterio La Inmaculada, España

KEYWORDS

Digital education
Online risks
Online frauds and scams prevention
Personal data protection
Safe and responsible use of the Internet

ABSTRACT

Online risks associated with scams or fraud involving technological devices and personal data are becoming increasingly common, so it is important to understand how citizens perceive these risks. Some studies point to training as one of the main challenges that will help address the risks and problems arising from the use of technology, which is necessary in both urban and rural areas. In this quasi-experimental mixed-method study, a risk perception scale is applied and 15 items on the perceptions of 239 citizens and their experiences focused on relationships and communication, online fraud and scams, and personal data are analyzed. The results show that citizens perceive a lot and/or too much risk in most actions and, in general, little risk in online purchases. They report problems of identity theft due to lost mobile phones, phishing, personal data processing, and others. Some of them are associated with good practices and strategies to deal with them and thus consciously avoid adopting risky behaviors in everyday situations that are increasingly common in the digital society.

PALABRAS CLAVE

Educación digital
Riesgos online
Prevención de fraudes y estafas online
Protección de datos personales
Uso seguro y responsable de Internet

RESUMEN

Los riesgos online asociados a las estafas o fraudes con dispositivos tecnológicos y a los datos personales, son cada vez más frecuentes, por lo que es importante comprender la percepción del riesgo que sobre ellos tienen los ciudadanos. Algunos estudios señalan a la formación como uno de los principales retos que ayudarán a afrontar riesgos y problemas derivados del uso de la tecnología y necesarios tanto en zonas urbanas como rurales. En este estudio cuasi experimental de tipo mixto se aplica una escala de percepción de riesgo y de ella, se analizan 15 ítems sobre percepciones de 239 ciudadanos y sus experiencias centradas en relaciones y comunicación, problemas de fraudes y estafas online y datos personales. Los resultados muestran que los ciudadanos perciben mucho y/o demasiado riesgo en la mayor parte de las acciones y en general poco riesgo en las compras online. Narran problemas de suplantación de identidad por extravío de móvil, phishing, tratamiento de datos personales y otros. Algunos de ellos asociados a buenas prácticas y estrategias para afrontarlos y así evitar conscientemente adoptar conductas de riesgo en situaciones cotidianas cada vez más habituales en la sociedad digital.

RECIBIDO: 23/01/2026
ACEPTADO: 26/02/2026

Cómo citar este artículo / Referencia normalizada: (Norma APA 7ª)
Gallego-Arrufat, M.J., Torres-Hernández, N., García-Ruiz, M.M., Teba-López, A. (2026). Aproximación educativa a percepciones sobre riesgos online y protección de datos personales. *Prisma Social revista de ciencias sociales*, *53*, 95-112. https://doi.org/10.65598/rps.6015

1. Introducción

Una parte importante de los ciudadanos usuarios de Internet se han enfrentado a la ciberdelincuencia con más frecuencia en los últimos años. Constantemente están apareciendo nuevos tipos de fraudes y estafas por Internet. *Phishing*, *Vishing*, *Smishing*, *Pharming*, *Hacking*, *Carding*, *Sim Swapping*, *Whaling*, *Pig butchering* o *infostealers* o *stealers* son algunos de los numerosos métodos de ciberdelitos denunciados, según recogen sistemas estadísticos de criminalidad gestionados por entidades y organismos de todo el mundo. Son abundantes, heterogéneos y se producen en muy diversos contextos: pago de todo en lugar de una parte al adquirir productos, por la reserva de vivienda inexistente en alquiler; pago de trámites para el acceso a un empleo en el extranjero; falsas compañías de telecomunicaciones que informan de problemas informáticos que piden conexiones remotas; establecimiento de relaciones amistosas o sentimentales con engaños; viajes y servicios inexistentes; llamadas telefónicas, mensajes o emails informando que alguien cercano está en apuros y necesitan urgentemente dinero; ofertas de servicios muy baratos que empresas fantasma exigen pagar; acceso a links con publicidad engañosa que advierte de que nuestros equipos han sido infectados y sugieren compra de programas antivirus. También se reciben mensajes vía correo electrónico donde avisan de problemas en cuentas bancarias, tenga o no la persona relación con esas entidades. Es frecuente que muchas personas reciban mensajes que anuncian la obtención de lotería, herencia o premio sin haber jugado, o sobre la entrega de paquetes a cambio de pagos, entre otros muchos fraudes y estafas comunes.

En este contexto, es el ciudadano usuario de Internet el que más potencial riesgo tiene cada vez que cliquea un sitio en Internet. El núcleo de la situación pandémica dio lugar a la formación de una nueva cultura de relaciones y compras online. El uso permanente de los dispositivos tecnológicos (sobre todo el teléfono móvil) para contactar con personas, hacer pagos con tarjetas de crédito, obtener servicios o productos, o necesitar registrarnos en páginas web para el acceso a diversos servicios esenciales son factores determinantes del aumento del grado de exposición de los datos personales y proporcionalmente del incremento de fraudes y estafas online a través de la telefonía móvil y los correos electrónicos (Reynolds & Parker, 2018). Hoy millones de ciudadanos usuarios y consumidores de todo el mundo con independencia del contexto poblacional donde habitan, sufren victimización en línea y con ello pérdidas económicas, problemas psicológicos, emocionales y/o sociales. Datos post-pandemia del COVID-19 señalan que, del total de ciberdelitos denunciados en España, un 88% correspondía a fraudes online debido principalmente a las desigualdades digitales que representan un importante factor de riesgo de vulnerabilidad (Dodel & Mesch, 2018; Beaunoyer et al., 2020). En el año 2022 hubo un incremento al 89.7% (Muniesa et al., 2022) del total de los delitos informáticos (374.737) registrados por fuerzas y cuerpos de seguridad españoles. Estos datos informan de la importancia que este tema tiene para la formación de la ciudadanía digital.

Consideramos que es esencial enfocar la educación digital de la ciudadanía hacia la prevención de fraudes y estafas online como una línea que contribuye a promover la cultura de la prevención de la cibercriminalidad especialmente en grupos vulnerables. En respuesta a ello, este estudio plantea como objetivo identificar y describir la vulnerabilidad de riesgo para fraudes y estafas online de ciudadanos españoles de cuatro poblaciones de Andalucía en cuatro actividades de carácter social y/o económico, una de ellas sobre Fraudes y estafas online (Torres-Hernández et al., 2023). Se analiza su percepción a través de un cuestionario y se describen sus reflexiones sobre sus experiencias sobre estos problemas.

1.1. Marco conceptual

En el Consejo de Europa se definió el fraude online como aquel acto deliberado e ilegítimo que causa perjuicio patrimonial al introducir, alterar, borrar o suprimir datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático con intención fraudulenta o delictiva (Council of Europe, 2001). Un delito informático es cualquier acción en el ciberespacio ilegal, delictiva, antiética o no autorizada que debe ser tratada legalmente. De acuerdo con Mayer (2018) en él pueden coexistir tres acciones ilícitas: el sabotaje, el espionaje y el fraude online,

considerándose en cualquier caso infracción la serie de acciones realizadas con el propósito de burlar los sistemas de seguridad (invasiones a ordenadores, emails o sistemas de datos). Se caracteriza por el engaño, ocultamiento o violación de la confianza y es perpetrado por individuos y organizaciones para obtener dinero, propiedades o servicios, evitar pagos y asegurar un beneficio económico. Cross et al. (2014) definen el fraude online como la experiencia de un individuo que ha respondido mediante el uso de Internet a una invitación, solicitud, notificación u oferta deshonesta proporcionando información personal o dinero que le ha llevado a sufrir una pérdida financiera o de otro tipo. La estafa se refiere al acto de una persona que, con ánimo de lucro, utiliza el engaño con perjuicio valiéndose de una manipulación informática o artefacto similar para conseguir una transferencia patrimonial no consentida.

Existe acuerdo en considerar que tanto los fraudes como las estafas online son delitos informáticos de acuerdo con la Convención sobre el Cibercrimen de Budapest (Council of Europe, 2001). Al ritmo que avanza la transformación digital, aumentan los problemas relacionados con el uso de Internet. Para atenderlos, se diseñan políticas, iniciativas y programas para la educación y la prevención. Esa es la razón por la que el enfoque educativo para un uso seguro y responsable es pertinente y necesario para la ciudadanía en la sociedad digital. Ribble et al. (2004) insisten en la necesidad de información sobre los riesgos y cómo prevenirlos para la ciberciudadanía. Formar personas conocedoras de los límites de sus derechos con respecto a los de otros y de sus propias obligaciones implica prestar atención a lo que sucede con las personas y sus actitudes y no solo evitar los riesgos a los usuarios, sino aumentar su confianza desarrollando la competencia. Lo anterior conlleva un uso responsable de la tecnología, por lo que se pone de manifiesto la necesidad de la formación para la mejora de las competencias digitales para el desarrollo de una ciudadanía digital plena y responsable, demanda que surge de la práctica y que promueven organismos supranacionales, como el programa *Council of Europe's Digital Citizenship Education* (DCE) el cual adopta un *framework* conceptual que agrupa los dominios digitales en *being online*, *well-being online* y *rights online* (Council of Europe, 2019).

La ciudadanía digital descansa en la alfabetización mediática basada en el papel y las responsabilidades de las personas. Implica la coexistencia de múltiples acciones relacionadas con el acceso digital tales como el comercio digital, la comunicación y la colaboración, la netiqueta, la salud y el bienestar, los derechos y la responsabilidad digitales, así como la seguridad, la protección de datos y la privacidad. Todas ellas exigen un desarrollo permanente de normas de uso apropiado, responsable y empoderado (European Commision, 2021; Levin & Mamlok, 2021). Asimismo, es necesaria la formación para el manejo de la información, el aprendizaje independiente y la responsabilidad social como estándares para la construcción de la ciudadanía digital. Por tanto, es difícil pensar en construir una ciudadanía digital, sin considerar al uso de la tecnología y la educación como ejes interrelacionados para el desarrollo de la sociedad digital. Las necesidades de interrelación personal, las oportunidades para vender y comprar, la transformación digital de las administraciones, organizaciones sociales y entidades exigen a las personas competencia digital para dominar diversas cantidades de información y resolver problemas que las relaciones mediadas generan. Internet ha transformado la vida de quienes habitamos la sociedad digital y con ello prácticamente se puede estar en cualquier parte del mundo, realizar pagos en línea o comprar lo inimaginable haciendo solo un clic (Williams et al., 2017; Wang et al., 2017).

El confinamiento causado por la pandemia del COVID-19 dio paso a una nueva cultura de relaciones sociales, un uso más frecuente de Internet, compras online, pagos con tarjeta y registro en páginas para contactar con otras personas con fines de amistad o pareja (Ma & McKinnon, 2022). Debido a este crecimiento se amplía en la misma proporción el problema de los fraudes y estafas online (Norris & Brookes, 2021). En EEUU, la Federal Trade Commission (FTC) informa que en 2022 de los 2.6 millones de consumidores que reportan incidentes, una gran parte de los problemas son fraudes de impostores, compras en línea, estafas por premios, loterías y sorteos en cuyos casos el medio más común es el email. Por grupos de edad los de 30-39 años son los más vulnerables y le siguen los diferentes grupos de edad de mayores de 40 años. En Australia, según Australian Bureau of Statistics (ABS), el 57% de usuarios mayores de 55 años estuvieron expuestos

al menos a una estafa y de ellos el 4% perdió dinero, información personal o ambas cosas. En España, el Instituto Nacional de Ciberseguridad (INCIBE-CERT) registró en 2023 del total de los incidentes registrados (83,517) el 69% afectó a la ciudadanía. De ellos, el 33% fueron por fraudes online, el 12% por suplantación de identidad y en menor medida por compras fraudulentas y fraudes de mensajería instantánea. Sin embargo, los estudios no aportan resultados concluyentes sobre la relación entre los riesgos online y la edad de los ciudadanos. Los datos tienden a considerar que el grupo más vulnerable podría ser el de adultos, a quienes se les atribuye menores competencias en el manejo de la tecnología. Norris et al. (2019) estiman que en Reino Unido los adultos mayores sufren altos porcentajes de incidentes de fraude y uso indebido de ordenadores. Sin embargo, Ross et al. (2014) sugieren que la edad puede ser un factor de protección en el sentido de que es menos probable que las personas mayores usen Internet para realizar ciertas transacciones financieras, argumento apoyado por el estudio de Hussain et al. (2018). Por otro lado existen estudios en los que los llamados nativos digitales se auto perciben con altas competencias en la alfabetización informacional pero cuando se enfrentan a la seguridad online sus competencias son escasas. Se afirma que los más jóvenes y usuarios de social media estiman que los efectos de los riesgos son más elevados en otros intervalos de edad que en el propio (Wei et al., 2019).

1.2. Antecedentes

Con la adopción de las tecnologías digitales en la vida cotidiana, muchas facetas de la sociedad se han trasladado a Internet, desde las compras o las interacciones sociales hasta los negocios, la industria y, por desgracia, también la delincuencia. Las investigaciones previas muestran que, desde antes de la pandemia, los estudios sobre fraudes y estafas han sido foco de interés en la investigación. En esta área de interés se ha desarrollado una importante cantidad de literatura con enfoques diferentes, lo que permite tener una visión holística del problema y en algunos casos su repercusión y consecuencias para la ciudadanía, en especial en los adultos considerados en diferentes estudios como el grupo más vulnerable.

La literatura aporta evidencias de la exposición de los ciudadanos a diferentes tipos de fraudes y estafas relacionados principalmente con aspectos financieros (Cook, 2020; Fenge & Lee, 2018; Harrell & Langton, 2013; Phiri et al., 2024), relaciones amorosas (Coluccia et al., 2020; Kirwan et al., 2018; Koop et al., 2015; Sorell & Whitty, 2019), falta de competencias digitales (Kaspersky 2020; Kumaran & Lugani, 2020; Purkait et al, 2014; Segura, 2017), comercio electrónico o robo de datos o información (Al-Qahtani & Cresci, 2022; Harrell & Langton, 2013; Whittaker et al., 2023) o el juego online (Crowne-Mohammed & Andreacchi, 2009). Los estudios de Mitchel et al. (2006), Norris & Brookes (2021) y Zhang & Ye (2022) abordan estos problemas de Internet desde una visión clínica analizando factores psicosociales que afectan la vida de las personas o planteando la atención a los problemas de fraudes online desde su base jurídica en contextos sociales diferentes. Otros han relacionado la posibilidad de victimización con variables como edad, género, ingresos o nivel educativo (Purkait et al., 2014). Quienes consideran que los perfiles son muy diversos, concluyen finalmente que cualquier ciudadano podría ser estafado (Button & Cross, 2017; Hu et al., 2019).

La diversidad de estudios sobre este tema dificulta afirmar con precisión cuáles son las variables que hacen a una persona usuaria de Internet más susceptible de sufrir conductas delictivas online, pues en ello pueden influir otro tipo de variables como el riesgo percibido, existiendo conceptualizaciones desde el enfoque del consumidor o del usuario (Mitchell, 1999; Byrne et al., 2016). La facilidad con que un delincuente o estafador engaña a los ciudadanos es uno de los más grandes problemas que se tiene al navegar por Internet. Una gran cantidad de estafas se producen principalmente en la contratación de servicios y en la compraventa online (Wang et al., 2017), pero en muchos casos se deben al uso y tratamiento de datos personales debido a aceptar cookies o al hackeo de datos. En general, con independencia de la perspectiva adoptada, los resultados suelen ser cuestionables sobre la relación entre los riesgos online y la edad de los ciudadanos. Los datos tienden a considerar que el grupo más vulnerable podría ser el de los adultos a quienes se les atribuye menores competencias digitales en el manejo de la tecnología junto a otros factores psicosociales que inciden en un mayor número de casos en este grupo

poblacional. Norris et al. (2019) estiman que en Reino Unido los adultos mayores sufren altos porcentajes de incidentes de fraude y uso indebido de ordenadores. Sin embargo, Ross et al. (2014) sugieren que la edad puede ser un factor de protección en el sentido de que es menos probable que las personas mayores usen Internet para realizar ciertas transacciones financieras, argumento apoyado por el estudio de Hussain et al., (2018) porque las personas usuarias mayores suelen preferir no usar Internet para hacer compras u operaciones bancarias. Byrne et al. (2016) en su estudio concluyen que uno de cada 18 adultos mayores suele ser víctimas de un fraude o estafa financiera cada año. También existen estudios en los que los llamados nativos digitales se auto perciben con altas competencias en la alfabetización informacional pero cuando se enfrentan a la seguridad online sus competencias son escasas. Sin embargo, los más jóvenes perciben mayor riesgo en los demás intervalos de edad y no en el propio (Wei et al., 2019).

2. Metodología

El estudio se realiza mediante una investigación cuasi experimental de tipo mixto. Los objetivos son:

- Objetivo 1. Identificar y describir los niveles de percepción de riesgo, las estafas y fraudes online y la protección de datos personales en actividades socio-económicas de ciudadanos según diferentes intervalos de edad.
- Objetivo 2. Analizar las experiencias de los ciudadanos relacionadas con fraudes y estafas online identificando las dimensiones que, desde su punto de vista, representan mayor preocupación.

2.1. Características de la muestra

Con un muestreo no probabilístico y por conveniencia, se eligen individuos por su proximidad y participación en talleres formativos de un programa de educación digital para la ciudadanía, parte del proyecto de investigación Desarrollo y optimización de acciones educativas intergeneracionales para la promoción del uso responsable de Internet (EduACD) que contó con la colaboración de la red denominada Guadalinfo de centros públicos andaluces de innovación abierta y acceso a Internet. La muestra es de 239 participantes. El estudio se lleva a cabo en cuatro poblaciones de Andalucía.

Las edades de los participantes están comprendidas entre 15 y 68 años de edad. De ellos, 149 son mujeres (62.3%) y 90 hombres (37.7%). El conjunto de la muestra se distribuyó en seis grupos de edad en la que los participantes de 42-50 años representan el más elevado (30.5% de ciudadanos). Los demás grupos de mayor edad (51-59 años y 60-68 años) suponen 23.8% y 13.4% respectivamente. Y los de menor edad (24-32 años y 33-41 años), el 11.7% y el 10.9% respectivamente.

2.2. Trabajo de campo

La recogida de información se realizó en trece talleres intergeneracionales (Torres-Hernández et al., 2023) en los que la ciudadanía comparte sus percepciones y experiencias sobre problemas y riesgos en Internet. Considerando que las estafas y fraudes online ofrecen una línea de interés para la investigación actual y su prevención requiere de estrategias educativas eficaces para evitar el aumento de estos problemas en la población de adultos mayores, los diferentes talleres se sustentan entre otros ejes temáticos en la formación para la prevención de fraudes y estafas online. Se dirigen al ciudadano mayor de 18 años y en ellos se adopta un enfoque holístico, entendiendo que cualquier persona puede ser cebo de los ciberdelincuentes a través de Internet (Chatterjee et al., 2019).

2.3. Instrumentos

Se utilizan dos instrumentos para recoger datos cuantitativos y cualitativos. Para la parte cuantitativa, un cuestionario sobre el riesgo percibido con 50 ítems (Torres-Hernández et al., 2022) tipo escala Likert (entre nada arriesgado y extremadamente arriesgado) donde se valoran

diferentes acciones de riesgo en Internet. Las propiedades psicométricas informan de un Alfa de Cronbach α =.937. Un análisis factorial confirmatorio revela una escala con tres factores que explican el 68.1% de varianza, un índice de ajuste comparativo =.996; índice de bondad de ajuste (GFI) =.984; índice de bondad de ajuste (AGFI) = .982; y la media cuadrática de los valores residuales (SRMR) =.042. Es una escala para su uso en investigaciones sobre los riesgos de Internet en personas adultas. Para este estudio, se presentan resultados de 15 ítems sobre prácticas consideradas de riesgo para casos de fraudes o estafas online (Tabla 1).

Tabla 1.
Acciones de riesgo por uso de Internet de los ciudadanos con potencial exposición a fraudes y estafas online.

# Códigos	Prácticas y riegos online
1BPSI	Acceder a sitios online para encontrar pareja
2DDBTC	Dar mis datos bancarios o de tarjetas de crédito en páginas de apuestas o juegos
3CSO	Comprar en sitios web conocidos como Amazon u otros
4BOCO	Buscar opiniones de consumidores o usuarios sobre productos y que al acceder me soliciten datos personales
5ACN	Aceptar cookies para seguir navegando en Internet
6RPCE	Recibir publicidad sin consentimiento a través de correo electrónico o redes sociales
7TO	Hacer transferencias online en webs o apps de entidades como *Western Union, PayPal* o *Bizum*
8APP	Aceptar políticas de privacidad al registrarse en redes sociales o apps
9CIDP	Compartir información o datos personales (nombre, edad, número de teléfono, ubicación…) en Internet
10DDCE	No leer con detenimiento qué datos personales gestionan y comparten las empresas cuando se aceptan cookies
11URWF	Usar redes WIFI públicas
12NCSCO	No cerrar sesión al terminar de usar cuentas o perfiles
13ACS	Abrir correo electrónico basura (spam)
14DPVE	Desconocer qué hacer cuando aparecen ventanas emergentes o anuncios en Internet
15CENS	Hacer clic en enlaces sin saber si son seguros

Fuente: elaboración propia

Los participantes en los talleres cumplimentaron voluntariamente el cuestionario antes de su inicio. Se proporcionó un enlace para acceder al mismo, donde también se solicitó el consentimiento informado. Se informó acerca de la protección de datos de carácter personal, de que no se recogía ningún dato de este tipo y también se solicitó su autorización correspondiente para la grabación de audio. Todo ello garantizando el cumplimiento de la Ley Orgánica de Protección de datos y garantía de los derechos digitales en España.

Para la parte cualitativa los datos se extraen de transcripciones producto del desarrollo de la metodología de análisis de casos basada en los incidentes críticos. De ellas se obtienen registros que se complementan con comentarios emitidos a través del chat y de notas del equipo de investigación registradas, con observaciones previas y posteriores al taller. Para generar las

opiniones, experiencias, consejos o comentarios de los participantes, se parte del contenido de vídeos producidos por la administración pública y fragmentos de reportajes televisivos sobre esta temática.

2.4. Análisis de datos

El análisis de los datos se realiza con los programas estadísticos SPSS y MAXQDA. Para este estudio, se realizan análisis estadísticos descriptivos y análisis de correlaciones por grupo de edad tras la agrupación en intervalos de edad de los 239 participantes para averiguar si existen diferencias significativas según grupos de edad. Se aplica la prueba estadística chi cuadrado para analizar la asociación entre las variables grupo de edad y acciones de riesgo. Así se analiza la relación entre los niveles de percepción de riesgo y la edad. Para las intervenciones de los talleres se realiza un análisis de contenido. Se extraen las siguientes dimensiones: descripción de experiencias, emociones que generan, narrativas sobre formas de identificación y difusión entre los ciudadanos y en los medios de comunicación de hechos o sucesos relacionados con los problemas, consecuencias de las estafas y fraudes online y soluciones compartidas por los ciudadanos.

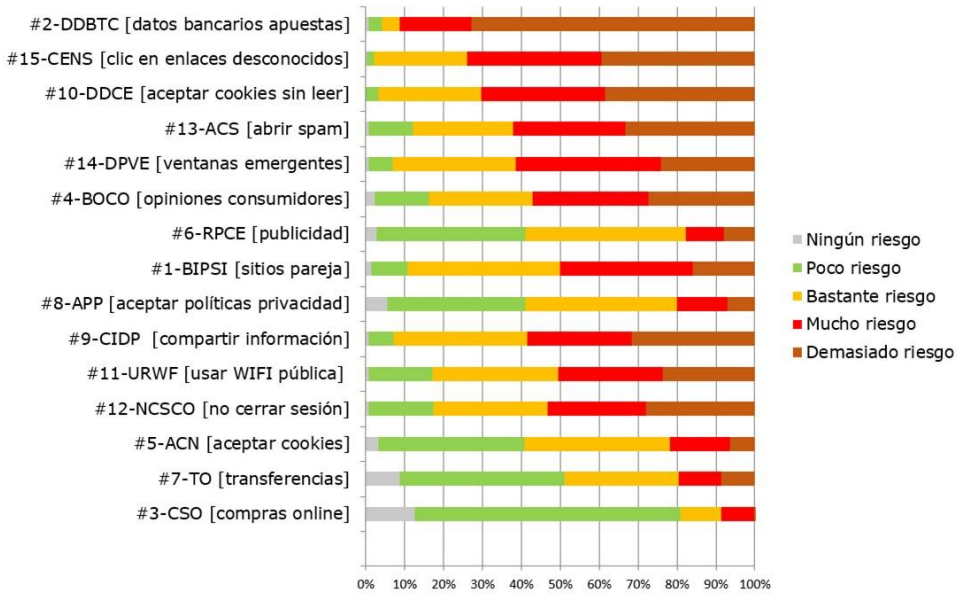
3. Resultados

Se presentan según los dos objetivos del estudio.

Objetivo 1. Identificar y describir los niveles de percepción de riesgo y problemas asociados a las estafas y fraudes online en actividades socio-económicas de ciudadanos en general, según diferentes intervalos de edad.

Con relación a este objetivo, se presentan resultados que muestran la percepción de las prácticas asociadas a fraudes y estafas online (Figura 1) y posteriormente se describen los resultados en función del grupo de edad al que pertenecen.

Figura 1.



Percepción general de riesgos asociados a fraudes y estafas online.

3.1. Percepción de riesgos

El conjunto de los ciudadanos percibe el riesgo más extremo en las siguientes acciones: En primer lugar, proporcionar datos bancarios o de tarjetas de crédito en páginas de apuestas o juegos (#2-DDBTC) (73%). También se aprecia demasiado riesgo (39%, 38% y 33% respectivamente)

en las siguientes prácticas: hacer clic en enlaces sin saber si son seguros (15-CENS); no leer con detenimiento qué datos personales gestionan y comparten las empresas cuando se aceptan cookies (#10-DDCE) y abrir mensajes que llegan como correo spam (#13-ACS). Como acciones de mucho riesgo aparecen (37% y 30% respectivamente), desconocer qué hacer cuando aparecen ventanas emergentes o anuncios en Internet (#14-DPVE) y buscar opiniones en Internet en páginas donde para acceder hay que proporcionar datos personales (#4-BOCO).

En cuanto a los valores medios, el 41% de ciudadanos encuestados coinciden en considerar prácticas de bastante riesgo la recepción de publicidad sin consentimiento del interesado (#6-RPO). El 39% percibe el acceso a sitios online para buscar pareja (#1-BPSI) y el aceptar políticas de privacidad durante el registro en redes sociales, páginas u otras aplicaciones (#8-APP) como acciones de bastante riesgo. Junto a ello, el resto de los valores medios corresponde a acciones como el compartir datos personales sensibles, es decir nombre, número de teléfono o ubicación (#9-CIDP) u otras de tipo técnico como usar redes WIFI públicas (#11-URWF) o mantener sesiones abiertas en dispositivos (#12-NCSCO), con 32% y 29% bastante riesgo respectivamente. Un valor menor (38% poco riesgo y 37% bastante riesgo) aparece en aceptar cookies para seguir navegando en Internet (5#-ACN).

Por otra parte, los riesgos como consumidores parecen suscitar escasa preocupación: la compra online en sitios como Amazon (#3-CSO) y las transferencias online a través de sitios ajenos a la banca online (#7-TO) se perciben por la mayoría de los ciudadanos como acciones de poco riesgo (68% y 42% respectivamente).

3.2. Asociación entre niveles de percepción y grupos de edad.

Los datos cuantitativos obtenidos en la escala también permiten indagar si existe asociación entre los niveles de percepción y los grupos de edad en cada acción de riesgo como se aprecia en la tabla 2.

Tabla 2.

Percepción de riesgo de cada ítem según grupos de edad y resultado de prueba Chi cuadrado.

# Códigos	Grupos de edad	Niveles de riesgo percibidos en % (Correlaciones)					Prueba X^2	
		Ningún riesgo	Poco riesgo	Bastante riesgo	Mucho riesgo	Demasiado riesgo	(X^2)	*P*
1-BIPSI [sitios pareja]	15-23	0	17.4	30.4	47.8	4.3	25.667706	.177
	24-32	0	14.3	39.4	39.3	7.1		
	33-41	3.8	11.5	34.6	34.6	15.4		
	42-50	2.7	4.1	39.7	30.1	23.3		
	51-59	1.8	5.3	35.1	28.1	29.8		
	60-68	0	3.1	56.3	25.0	15.6		
2-DDBTC [datos bancarios apuestas]	15-23	0	0	0	34.8	65.2	18.218673	.232
	24-32	3.6	3.6	3.6	21.4	67.9		
	33-41	0	7.7	7.7	11.5	73.3		
	42-50	1.4	1.4	8.2	9.6	79.5		
	51-59	0	1.8	1.8	12.3	84.2		
	60-68	0	6.3	6.3	21.9	71.9		
3-CSO [compras online]	15-23	13.0	78.3	4.3	4.3	0	24.233242	.573
	24-32	14.3	53.6	14.3	17.9	0		
	33-41	19.2	65.4	7.7	7.7	0		
	42-50	8.2	71.2	15.1	4.1	1.4		
	51-59	8.8	71.9	15.8	3.5	0		
	60-68	12.5	68.8	6.3	12.5	0		
4-BOCO [opiniones de consumidores]	15-23	4.3	17.4	39.1	30.4	8.7	25.093338	.198
	24-32	7.1	10.3	21.4	35.7	25.0		
	33-41	0	26.9	23.1	23.1	26.9		
	42-50	1.4	11.0	27.4	28.8	31.5		
	51-59	1.4	11.0	27.4	28.8	31.5		
	60-68	0	7.0	21.1	31.6	40.4		
	15-23	0	26.1	43.5	2.7	8.7		

Tabla 2.

Percepción de riesgo de cada ítem según grupos de edad y resultado de prueba Chi cuadrado.

# Códigos	Grupos de edad	Niveles de riesgo percibidos en % (Correlaciones)					Prueba X^2	
		Ningún riesgo	Poco riesgo	Bastante riesgo	Mucho riesgo	Demasiado riesgo	(X^2)	*P*
5-ACN [aceptar cookies]	24-32	0	28.6	39.3	25.0	7.1	31.417348	0.05
	33-41	0	42.3	26.9	23.1	7.7		
	42-50	1.4	37.0	37.0	17.8	6.8		
	51-59	1.8	43.9	38.6	8.8	7.0		
	60-68	15.6	40.6	32.3	12.5	0		
6-RPCE [publicidad]	15-23	4.3	39.1	39.1	4.3	13.0	30.800701	.050
	24-32	0	21.4	57.1	14.3	7.1		
	33-41	0	23.1	57.1	11.5	7.7		
	42-50	0	43.8	35.6	12.3	8.2		
	51-59	3.5	38.6	36.8	12.3	8.8		
	60-68	9.4	62.5	21.9	3.1	3.1		
7-TO [transferencias]	15-23	8.7	26.1	47.8	8.7	8.7	23.635643	.259
	24-32	7.1	32.1	35.7	17.9	7.1		
	33-41	15.4	54.8	15.4	7.7	7.7		
	42-50	5.5	34.2	35.6	15.1	9.6		
	51-59	3.5	50.9	22.8	14.0	8.8		
	60-68	12.5	56.3	18.8	3.1	9.4		
8-APP [aceptar políticas de privacidad]	15-23	4.3	35.8	43.5	17.4	0	19.294421	.503
	24-32	7.1	28.6	32.1	21.4	10.7		
	33-41	0	38.5	42.3	7.7	11.5		
	42-50	2.7	30.1	42.5	15.1	9.6		
	51-59	7.0	42.1	33.3	7.0	10.5		
	60-68	12.7	37.5	40.6	9.4	0		
9-CIDP [compartir información personal]	15-23	0	0	30.8	43.5	26.1	25.658662	.177
	24-32	0	3.6	39.3	28.6	28.6		
	33-41	3.8	11.5	26.9	15.4	42.3		
	42-50	1.4	4.1	42.5	20.5	31.5		
	51-59	0	12.3	22.8	22.8	42.1		
	60-68	0	6.3	43.8	31.3	18.8		
10-DDCE [aceptar cookies son leer contenido]	15-23	0	0	17.4	43.5	39.1	13.283337	.580
	24-32	0	0	42.9	25.0	32.1		
	33-41	0	7.7	26.9	23.1	42.3		
	42-50	0	4.1	17.8	34.2	43.8		
	51-59	0	5.3	21.1	35.1	38.6		
	60-68	0	3.1	31.3	31.3	34.4		
11-URWF [usar WiFi públicas]	15-23	0	13.0	43.5	13.0	30.4	32.950489	.034
	24-32	0	7.1	39.3	32.1	21.4		
	33-41	0	11.5	34.6	19.2	34.6		
	42-50	2.7	12.3	17.8	41.1	26.0		
	51-59	1.8	17.5	29.8	28.1	22.8		
	60-68	0	37.5	28.1	28.1	6.3		
12-NCSCO [no cerrar sesiones en dispositivos]	15-23	0	30.4	21.7	26.1	21.7	23.006969	.288
	24-32	0	25.0	28.6	21.4	25.0		
	33-41	0	3.8	42.3	19.2	34.6		
	42-50	1.4	8.2	30.1	24.7	35.6		
	51-59	0	14.0	21.1	29.8	35.1		
	60-68	3.1	18.8	31.3	31.3	15.6		
13-ACS [abrir spam]	15-23	0	34.8	26.1	26.1	13.0	40.694463	.04
	24-32	0	10.7	35.7	32.1	21.4		
	33-41	0	0	15.4	23.1	61.5		
	42-50	0	5.5	17.8	32.9	43.8		
	51-59	1.8	10.5	28.1	28.1	31.6		
	60-68	3.1	6.3	31.3	31.3	28.1		
14-DPVE [aparición de ventanas emergentes]	15-23	0	8.7	21.7	43.5	26.1		.112
	24-32	0	0	28.6	50.0	21.4		
	33-41	0	0	26.9	46.2	26.9		

Tabla 2.

Percepción de riesgo de cada ítem según grupos de edad y resultado de prueba Chi cuadrado.

# Códigos	Grupos de edad	Niveles de riesgo percibidos en % (Correlaciones)					Prueba X^2	
		Ningún riesgo	Poco riesgo	Bastante riesgo	Mucho riesgo	Demasiado riesgo	(X^2)	*P*
	42-50	1.4	5.5	37.0	26.0	30.1	27.881515	
	51-59	0	15.8	26.3	29.9	28.1		
	60-68	3.1	6.3	50.0	28.1	12.5		
15-CENS [clic en enlaces desconocidos]	15-23	0	0	21.7	30.4	47.6	27.996284	.109
	24-32	0	0	21.4	39.3	39.3		
	33-41	0	0	15.4	57.7	26.9		
	42-50	1.8	5.5	20.5	34.2	39.7		
	51-59	0	1.8	24.6	17.5	54.5		
	60-68	0.4	3.1	40.6	28.1	28.1		

En general los resultados muestran que en el ítem #2-DDBTC (dar datos bancarios o de tarjetas de crédito en páginas de apuestas o juegos) se concentra la percepción de mayor riesgo para todos los grupos de edad, seguido de aceptar cookies sin leer (#10-DDCE), acceder a enlaces desconocidos (#15-CENS), usar la WiFi pública (#11-URWF), recibir spam en correo electrónico (#13-ACS).

La mitad de los grupos de edad perciben poco riesgo en realizar compras online (#3-CSO), recibir publicidad (#6-RPCE) y hacer transferencias (#7-TO). Los grupos de edad de mayores de 40 años perciben mucho riesgo en confiar en las opiniones de consumidores en Internet (#4-BOCO), usar las WiFi públicas (#11-URWF), no cerrar sesiones de sitios en dispositivos tecnológicos (#12-NCSCO). La práctica donde todos los grupos coinciden en percibir como de poco riesgo son las compras online (#3-CSO). Los grupos de menores de 40 años perciben mucho riesgo en buscar pareja en Internet (#1-BIPSI), no cerrar ventanas emergentes (#14-DPVE) y acceder a sitios mediante enlaces desconocidos (#15-CENS).

En conjunto, los porcentajes en los seis grupos de edad son menores del 20% del total de cada uno de los grupos de edad al percibir poco o ningún riesgo en las 15 prácticas analizadas.

3.3. Asociación entre ítems

La Tabla 2 muestra los resultados de la prueba Chi cuadrado. Expresados en porcentajes informan de las correlaciones entre cada ítem y los grupos de edad. Para cada ítem se analizó la existencia o no de asociación entre cada uno de los niveles de percepción de riesgo con los diferentes grupos de edad. Contiene los porcentajes que resultan del análisis comparativo de los grupos de edad y los niveles de percepción de riesgo. Los resultados solo muestran ítems y porcentajes e intervalos en donde se han encontrado evidencias sustanciales de dicha asociación.

Los ciudadanos de todas las edades coinciden en percibir el riesgo más elevado si piensan en proporcionar sus datos bancarios o de tarjetas de crédito en páginas de apuestas o juegos (#2-DDBTC). En este caso, no se encontraron diferencias entre percepción de riesgo y los diferentes grupos de edad (X2 (1)= 18.21, $p > 0.05$).

También hacer clic en enlaces sin saber si son seguros (#15-CENS) es percibida como una acción que conlleva demasiado riesgo en todos los intervalos de edad excepto en el de mayores, dado que 40.6% de 60-68 años perciben riesgo medio. En este ítem, no se encontraron diferencias en percepción de riesgo (X2 (1)= 27.99 $p > 0.05$). La percepción de riesgo se distribuye y concentra principalmente en la opción demasiado riesgo (con proporción de más del 39.7%) en los grupos de edad 15-23, 24-32, 42-50 y 51-59.

Con valores elevados, todas las edades consideran acciones de mucho o demasiado riesgo no leer con detenimiento qué datos personales gestionan y comparten las empresas cuando se aceptan cookies (#10-DDCE), ninguno percibe un riesgo 0, aunque los ciudadanos de 24-32 años coinciden en percibir el riesgo como medio (42.9%). Según el resultado del test chi-cuadrado, en este ítem no se encontraron diferencias en percepción de riesgo (X2 (1)= 13.28, p > 0.05). La percepción de riesgo se distribuye principalmente entre las opciones bastante riesgo, mucho riesgo y demasiado riesgo con proporciones de más de 38.6% en los grupos de edad mayores de 33 años.

Con relación a la práctica incluida en el ítem #1-BPSI (acceder a sitios online para encontrar pareja) los resultados muestran que en el grupo de edad de 15-23 años las personas coinciden en percibir mucho riesgo; en los siguientes intervalos perciben con porcentajes similares mucho y bastante riesgo; y a partir del intervalo 42-50 años el mayor porcentaje percibido es bastante riesgo (56.3% en 60-68 años). En este no se encontraron diferencias en percepción de riesgo y los diferentes grupos de edad (X2 (1)= 26.66, p > 0.05). Según muestran los resultados, solo quienes tienen entre 15-23 años consideran esta práctica de mucho riesgo (47.8%).

Por otra parte, el ítem #8-APP (aceptar políticas de privacidad al registrarse en redes sociales o apps) es percibido como una acción de bastante riesgo en todas las edades, excepto en 51-59 años, quienes perciben poco riesgo (42.1%). En él, no se encontraron diferencias en percepción de riesgo (X2 (1)= 19.29, p > 0.05). La percepción de riesgo se distribuye principalmente en la opción bastante riesgo entre las opciones poco riesgo y bastante riesgo con proporción superior a 32.1% en cinco de los seis grupos de edad, salvo el grupo de 51-59.

En cuanto al ítem #9-CIPD (compartir información o datos personales como nombre, edad, número de teléfono, ubicación… en Internet) aparece distribuido en tres intervalos de edad como acción de mucho o demasiado riesgo y en otros tres de bastante riesgo, con porcentajes similares que oscilan entre 39.3% y 43.8%. Para este, no se encontraron diferencias en percepción de riesgo (X2 (1)= 25.65, p > 0.05), distribuyéndose principalmente entre las opciones bastante riesgo, mucho riesgo y demasiado riesgo.

Los ítems #14-DPVE (desconocer qué hacer cuando aparecen ventanas emergentes o anuncios en Internet) y #11-URWF (usar redes WIFI públicas) son riesgos técnicos que revelan un resultado diferente, dado que los tres intervalos de menor edad coinciden en percibir mucho riesgo en #14-DPVE y solo un riesgo medio en #11-URWF. En este caso, la percepción aparece dividida entre el valor extremo y el medio en el intervalo 33-41 años, y va disminuyendo a medida que aumenta la edad (mucho, bastante y poco riesgo respectivamente en los tres intervalos de mayor edad). En #14 la percepción de riesgo se concentra principalmente en la opción mucho riesgo (con proporción de más del 29.9%) en los grupos de edad de 15-23, 24-32, 33-41 y 42-50. El resultado de la prueba de X2 muestra que para el ítem #14-DPVE no se encontraron diferencias en percepción de riesgo (X2 (1)= 27.88 p > 0.05). En el ítem #11-URWF se encontraron diferencias en grado de percepción de riesgo y los diferentes grupos de edad (X2 (1)= 32.95, p < 0.05). La percepción de riesgo se distribuye entre cuatro opciones de riesgo, con más del 29.8% pero con tendencia hacia la opción de bastante riesgo en los grupos de edad más jóvenes (15-23, 24-32, 33-41).

También resultan con valores medios las acciones #5-ACN (aceptar cookies para seguir navegando en Internet), #6-RPCE (recibir publicidad sin consentimiento a través de correo electrónico o redes sociales) y #7-TO (hacer transferencias online en webs o apps de entidades como Western Union, PayPal o Bizum), aumentando entre los ciudadanos de mayor edad la

percepción de poco riesgo, sobre todo en el ítem #6-RPCE. También resaltamos que no existen ciudadanos en los intervalos de menor edad que perciban ningún riesgo en el ítem #5-ACN. Los valores de significación resultado del test chi-cuadrado son similares en los dos primeros (p=.05 y p=.058) y p=.259 para el ítem #7-TO por lo que se rechazan las hipótesis nulas y se aceptan las hipótesis alternativas que señalan una asociación significativa entre el nivel de percepción de estos riesgos riesgo con los grupos de edad. El resultado de prueba X2 muestra que en el ítem #5-ACN se encontraron diferencias en grado de percepción de riesgo y los diferentes grupos de edad ($X2 (1)= 31.41, p < 0.05$). La percepción de riesgo tiene una mayor proporción en la opción poco riesgo (con proporción de más de 37%) en los grupos de edad de más 33 años. En el ítem #6-RPCE se encontraron diferencias en grado de percepción de riesgo y los diferentes grupos de edad ($X2 (1)= 30.80, p <0.05$). La percepción de riesgo se distribuye entre las opciones poco riesgo y bastante riesgo con proporción superior a 38.6% en todos los grupos de edad. Para el ítem #7-TO no se encontraron diferencias en percepción de riesgo ($X2 (1)= 23.63, p > 0.05$). La percepción de riesgo se distribuye entre las opciones poco riesgo para grupos de edad de 33-41, 51-59 y 60-68 y bastante riesgo para edades de 15-23, 24-32 y 42-50 con proporción superior a 35.6%.

En último lugar, el único ítem en el que coinciden los ciudadanos en percibir poco riesgo, independientemente de su edad, es #3CSO (Comprar en sitios web conocidos como Amazon u otros), con porcentajes similares (los más jóvenes 78.3% y los mayores 68.8%). El resultado del test chi-cuadrado para este caso muestra que no se encontraron diferencias en percepción de riesgo y los diferentes grupos de edad ($X2 (1)= 24.23, p > 0.05$). La percepción de riesgo tiene una mayor proporción en la opción poco riesgo en todos los grupos de edad.

Objetivo 2. Analizar las experiencias de los ciudadanos relacionadas con fraudes y estafas online identificando las dimensiones que, desde su punto de vista, representan mayor preocupación.

3.4. Principales preocupaciones de ciudadanos

El análisis de la experiencia de los ciudadanos se presenta a partir de un análisis cualitativo de intervenciones y comentarios de los ciudadanos en talleres de formación online sobre fraudes y estafas online. Se realiza mediante análisis de contenido (Hsieh & Shannon, 2005) a partir del sistema de categorías creado en el programa MAXQDA 2022©. En este estudio dar la voz a los ciudadanos permite presentar narrativas en los segmentos identificados y agrupados en seis dimensiones: experiencias, emociones, formas de identificación, difusión, consecuencias y soluciones compartidas por los participantes. Los resultados obtenidos responden al objetivo dos de la investigación.

Experiencias sobre estafas y fraudes online. Los registros corresponden en su mayoría a esta dimensión y en ella los participantes describen experiencias y vivencias que conocen en primera persona o de círculos cercanos. Para ellos, los fraudes más comunes son los avisos de la recogida pendiente de paquetes, las clonaciones de tarjetas de crédito, el phishing, y la suplantación de identidad por extravío del móvil. En palabras de los ciudadanos […] ya sea por correo electrónico o mensaje de texto mandaban que estaba pendiente de recibir un paquete y te pedían clicar un enlace y algunos datos (P41M) Hay personas que creyeron que les iban a entregar el paquete porque habían comprado algo y dieron datos (P58M) […] el caso del paquete que comentaban, yo creo que ese lo hemos recibido casi todo el mundo (P133H). Otros explican […] lo que hicieron fue entrar en su cuenta del banco y en todos los correos […] con lo cual le vaciaron la cuenta y un préstamo pre concedido […] (P34H) […] a un compañero de trabajo antes del confinamiento le duplicaron la tarjeta del móvil y lo que notó fue que el móvil no funcionaba, creía que se le

había estropeado y era que se la habían duplicado (P4H) Y también […] ¿ejemplos de phishing? sólo tienes que meterte en tu carpeta de spam y los ves (P3H).

Emociones de los ciudadanos. Las emociones y sentimientos son variados e incluyen la culpa, la impotencia, el hartazgo o el miedo. En ocasiones claramente se identifica así […] nos ha hablado de sensaciones como impotencia o sentirnos mal por cosas que nosotros realmente no deberíamos sentirnos culpables (P70H) Tampoco uso mucho las compras por Internet porque me da miedo (P9H) No uso mucho el móvil porque le tengo miedo y respeto sinceramente […] (P92H) Estamos cansados de ver muchos problemas con fotografías fuera de lugar o compartir historias con chantajes y abusos que a mí me da miedo de mis nietos (P81M) Somos un poquito ingenuos y picamos (P1M) […] a mí me fue suplantado un correo electrónico y he actuado, pero me he quedado con la sensación de temor, de miedo, de pensar qué información han podido buscar de mis contactos. Creo que es importante que tengamos en cuenta las emociones porque también afectan a nuestra salud (P9H).

Formas de identificar estafas y fraudes online. El andamiaje o los consejos que aportan los participantes son una manera de colaboración y ayuda para mejorar la percepción del problema. Adoptan expresiones como […] hay veces que tienen errores ortográficos y pueden ser más evidentes pero los mensajes de otros ciberdelincuentes son muy elaborados y que pueden parecer ciertos (P22M) […] puede coincidir que no esperemos ningún paquete o que nos escriban de un banco en el que ni siquiera tenemos una cuenta y entonces sea fácil detectar ese ciberataque (P213H) […] si has recibido un correo o un mensaje con un enlace y tienes duda, sería quizá una buena estrategia frente a ese tipo de ciberataques intentar buscar un teléfono (de la empresa, organismo oficial, etc.) para confirmarlo (P29M).

Difusión de problemas. Las estrategias de comunicación e información generan redes de colaboración y protección que se evidencian en comentarios como los siguientes: […] en el pueblo me consta que el mensaje sobre el fraude del paquete nos llegó a varios ciudadanos. Nos dimos cuenta de que era fraude porque salió en las noticias de TV. Es verdad que se extendió mucho ese mensaje (P33H) En las comunidades sociales online también se difunden: Por un grupo de WhatsApp nos ha llegado alguna vez que se ha concedido no sé qué premio por un sorteo (P5M).

Consecuencias de las estafas y fraudes online. Las consecuencias de los fraudes y estafas dan una idea de la problemática que se genera. Todas implican una pérdida de dinero. Manifiestan […] le habían duplicado la tarjeta con la intención de entrar en su cuenta del banco y todos los correos de doble seguridad y le vaciaron la cuenta directamente (P4H) […] yo escuché sobre una persona que había sido víctima de un fraude. Con sus datos habían abierto una cuenta en el banco. Y ahora tenía un juicio para demostrar que no había sido responsable y era víctima de un fraude (P92M) […] entregó los datos y perdió aproximadamente unos 1000 euros, el valor del paquete que iba a recibir (P53M).

Soluciones. Los participantes plantean posibles maneras de actuar en caso de ser víctima de fraude o estafas online. Son soluciones que han aprendido debido a la experiencia, aunque antes desconocían el procedimiento a seguir. Algunas de ellas son intuitivas y de sentido común, y en cualquier caso reflejan la integridad de los usuarios. En la mayoría de las ocasiones realizan una acción individual […] llamar para que bloqueen el dispositivo de teléfono o ponerse en contacto rápidamente con la entidad bancaria (P2M) A mí el problema que me pasó fue con la tarjeta en Amazon, lo reclamé al banco y me hicieron una tarjeta nueva y ya se solucionó todo (P43M) […] poner una denuncia en la Guardia Civil (P2M) […] ir a la compañía para que le arreglaran la tarjeta del móvil (P4H) Me robaron el móvil en el metro, recurrí a la policía y me pidieron un

número que viene en la caja del móvil, se lo di e hicieron ese bloqueo (P67H) En otras ocasiones el apoyo es de la comunidad: Nosotros tenemos un grupo de WhatsApp y a través de él alertamos a los miembros de que si les llega un mensaje de correos sobre un paquete, no abran ni pinchen el enlace, pues es una estafa (P79M) En todos los casos, son interesantes las expresiones de los ciudadanos enfocadas a la prevención del fraude o estafa: Cuando veo que hay un mensaje nuevo si es de un banco y no tengo cuenta en él o si es una multa y no conduzco, sé que eso es un fraude y directamente lo elimino (P231H) […] Cuando reviso mi correo y veo que en la carpeta de spam hay mensajes con asuntos o de personas que no conozco, los selecciono y los borro sin abrirlos (P114M) Y cuando veo algo raro digo: ¡Esto no me conviene! O cuando me pide insertar el número de teléfono u otro dato, no lo hago y digo: ¡Esto no me interesa! (P5160M).

4. Discusión

Los problemas asociados a Internet en la actualidad son riesgos tan posibles como reales. Riesgos y problemas que, precisamente por producirse en el entorno digital, no siempre son fáciles de detectar y que crecen exponencialmente. En este estudio se evidencia que los comportamientos adecuados de seguridad en Internet de los ciudadanos se basan en su percepción de riesgo y que compartirlos es un enfoque apropiado que forma parte de la mejora de su competencia digital. Aunque en ocasiones se requiere la adopción de conductas preventivas mediante la intermediación de personal técnico especializado, en otras funciona perfectamente la aproximación educativa from the bottom up basada en una comunidad intergeneracional diversa e inclusiva que comparte percepciones, experiencias y emociones (Ribble et al., 2004; Dodel & Mesch, 2018; Council of Europe, 2019). Indudablemente, la educación digital enfocada a la inclusión y el aprendizaje a lo largo de la vida desaconseja la restricción del uso y al mismo tiempo considera deseable la disminución de las emociones negativas. La reflexión realizada en la cumplimentación de la escala antes de los talleres y en los comentarios durante los mismos puede aumentar el avance en el aprendizaje y en el desarrollo de oportunidades digitales.

Por ello es fundamental apoyar la alfabetización digital y las habilidades de ciudadanía digital y no solo atender a las consecuencias negativas del uso de Internet. Se ha despertado un creciente interés hacia una nueva era para la educación orientada a tratar las oportunidades pero también los desafíos de compartir una vida digital dando más valor a la confianza digital. El análisis de varios casos de fraude surgidos en los talleres es de gran importancia en su prevención. La puesta en práctica de consejos y soluciones compartidas es propicia para mejorar el efecto educativo contra el fraude en Internet. En esa línea coincide el estudio de Hu et al. (2019).

Existen fraudes de muchos tipos, desde falsas ofertas de empleo, préstamos falsos, promociones de viaje ficticios, anuncios de alquileres o venta de productos y viviendas inexistentes. Las temáticas esenciales en la educación sobre fraudes y estafas online dirigidas a nuestras redes sociales y aplicaciones de mensajería instantánea pueden centrarse en: concursos y promociones falsos, secuestro de la cuenta de WhatsApp, cuentas falsas en redes sociales (de empresas, famosos, etc.), sextorsión y amores en línea, o anuncios chollo de tiendas fraudulentas, como se sugiere en campañas de organismos estatales como el Instituto Nacional de Ciberseguridad (INCIBE-CERT).

Es cada más frecuente la aparición de campañas preventivas en períodos puntuales, pero igualmente se desconoce el alcance real que tienen los mensajes preventivos a la ciudadanía y en especial a grupos de edad más adulta que hoy en día es más susceptible de ser víctima de un fraude o una estafa. En este sentido, es posible que en los resultados presentados puedan estar influyendo distintas variables: los niveles competenciales de los mayores de 50 años, la falta de

información y la zona donde habitan, lo que plantea una nueva línea de investigación hasta ahora no explorada.

Otra limitación de carácter metodológico reside en que este estudio se limita al análisis cualitativo en nuestra investigación considerando únicamente a los tipos de ciberamenazas que han formulado los ciudadanos participantes en los talleres online, por entender que el compromiso digital es mayor en estos casos, aunque posiblemente se han podido exacerbar algunas cuestiones como consecuencia de las emociones presentes en las reflexiones analizadas.

5. Conclusiones

La educación digital del ciudadano se debe construir en un espacio académico formal pero también y sobre todo en el ciberespacio informal o dependiente de centros municipales o estatales, donde es preferible educar digitalmente a los ciudadanos. El incremento de fraudes y estafas online en muchos países americanos, asiáticos y europeos ha incorporado en las últimas décadas la educación para la concienciación contra el fraude en políticas y estrategias nacionales e internacionales (Council of Europe, 2001; 2019). A través de diversas formas de sensibilización se ofrece formación para reforzar la conciencia de las personas sobre el fraude en Internet para obtener información confidencial, como datos personales o financieros, y salvaguardar legítimos derechos de los usuarios. Los canales más utilizados son las llamadas telefónicas, el correo electrónico, las aplicaciones de mensajería o las propias redes sociales.

Los resultados obtenidos en esta investigación no son concluyentes sobre la percepción de riesgo en relación con los intervalos de edad y no se aprecia un aumento en el caso de las personas mayores (Ross et al., 2014; Button & Cross, 2017; Hussain et al., 2018) aunque sería interesante profundizar en la relación riesgo-beneficio percibido (Byrne et al., 2016; Wei et al., 2019). Los llamados nativos digitales se auto perciben con altas competencias pero cuando se enfrentan a la seguridad online sus percepciones no difieren de los mayores sobre la aceptación de cookies sin leer o las políticas de privacidad. Las principales diferencias se encuentran en el riesgo de usar una WIFI pública, abrir spam o buscar opiniones de consumidores proporcionando datos personales. Por su parte, coinciden todos los ciudadanos de cualquier edad en la percepción de riesgo máximo al proporcionar datos bancarios en sitios de apuestas y juegos y en estimar poco riesgo en la realización de compras online.

En esta sociedad hiperconectada en la que aumenta la dependencia de los usuarios del mundo digital son esenciales cuatro elementos íntimamente relacionados: las redes digitales, los datos personales, la información y el conocimiento (Norris et al., 2019). En todo caso, las futuras campañas de concienciación deben enfatizar que la búsqueda de apoyo es parte de la solución y deben evitar colocar la responsabilidad completamente sobre la víctima (De Kimpe et al., 2020). También es importante vincular el problema a la solución y, sobre todo, a la adopción de medidas de protección, siendo un pilar esencial la existencia de servicios de información sobre fraudes online. Proporcionar confianza digital es tarea de todos: organismos, servicios, empresas y, sobre todo, los propios ciudadanos.

Referencias

Al-Qahtani, A. & Cresci, S. (2022). The COVID'19 scamdemic: A survey of phishing attacks and their countermeasures during COVID'19. *IET Information Security, 16*(5), 324–345. https://doi.org/10.1049/ise2.12073

Australian Bureau of Statistics (2022). *Personal Fraud. Reference period: 2020-21 financial year*. http://sl.ugr.es/0e1r

Beaunoyer, E., Dupéré, S. & Guitton, M. J. (2020). COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. *Computers in Human Behavior,* 111, 106424. https://doi.org/10.1016/j.chb.2020.106424

Button, M. & Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. Routledge. https://doi.org/10.4324/9781315679877

Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A. & Sanchez, D. (2016). From the User's Perspective: Perceptions of Risk Relative to Benefit Associated with Using the Internet. *Computers in Human Behavior, 59*, 456-468. https://doi.org/10.1016/j.chb.2016.02.024

Chatterjee, S., Kar, A.K., Dwivedi, Y.K. & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology & People, 32*(5),1153-1183. https://doi.org/10.1108/ITP-05-2018-0251

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A. & Gualtieri, G. (2020). Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. *Clinical Practice & Epidemiology in Mental Health, 1*, 24-35. http://doi.org/10.2174/1745017902016010024

Cook, A. (2020). *COVID-19: Companies and verticals at risk for cyber attacks*. Reliaquest. http://sl.ugr.es/0e1y

Council of Europe (2001). *Convention on Cybercrime*. European Treaty Series, 185. https://rm.coe.int/1680081561

Council of Europe (2019). *Digital Citizenship Education Handbook*. https://rm.coe.int/168093586f

Cross, C., Smith, R.G. & Richards, K. (2014). Challenges of responding to online fraud victimization in Australia. *Trends and issues in crime and criminal justice*, (474), 1-6. http://sl.ugr.es/0e1z

Crowne-Mohammed, E., & Andreacchi, R. (2009). The (Un)availability of Commons Law Remedies for Victims of Online Gambling Fraud. *Gaming Law Review and Economics, 13*(4). http://doi.org/10.1089/gire.2009.13405

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L. & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in human behavior, 108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Dodel, M. & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors, *Information, Communication & Society, 21*(5), 712-728. https://doi.org/10.1080/1369118X.2018.1428652

European Commission (2021). *2030 Digital Compass: the European way for the Digital Decade. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. http://sl.ugr.es/0e1q

Fenge, L.A., & Lee, S. (2018). Understanding the Risks of Financial Scams as Part of Elder Abuse Prevention. *The British Journal of Social Work 48*(4), 906–923. https://doi.org/10.1093/bjsw/bcy037

Federal Trade Commissión [FTC]. (2023). As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

Harrell, E. & Langton L. (2013). *Victims of identity theft*. Bureau of Justice Statistics. http://www.bjs.gov/content/pub/pdf/vit12.pdf

Hsieh, H. & Shannon, S. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. https://doi.org/10.1177/1049732305276687

Hu, L., Jiang, Y. & Li, Y. (2019). Optimization Design of Internet Fraud Case Based on Knowledge Graph and Case Teaching. In *Proceedings of the 7th International Conference on Information and Education Technology*, 301-305. https://doi.org/10.1145/3323771.3323806

Hussain, D., Ross, P. & Bednar, P. (2018). The Perception of the Benefits and Drawbacks of Internet Usage by the Elderly People. In C. Rossignoli, F. Virili, & S. Za (Eds.), *Digital Technology and Organizational Change. Lecture Notes in Information Systems and Organisation,* 23,199-212. Springer. https://doi.org/10.1007/978-3-319-62051-0_17

Kaspersky. (2020). *Kaspersky Security Bulletin Statistics*. http://sl.ugr.es/0e1w

Kirwan, G., Fullwood, C. & Brendan, R. (2018). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. *Cyberpsychology, Behavior, and Social Networking,* 123-128. http://hdl.handle.net/2436/620689

Kopp C., Layton R., Sillitoe J. & Gondal, I. (2015). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology,* 9(2), 205-217. http://sl.ugr.es/0e1t

Kumaran, N., & Lugani, S. (2020). *Protecting businesses against cyber threats during COVID-19 and beyond*. Google Cloud Bolg http://sl.ugr.es/0e1v

Levin, I. & Mamlok, D. (2021). Culture and society in the digital age. *Information*, *12*(2) 68. https://doi.org/10.3390/info12020068

Ma, K.W.F. & McKinnon, T. (2022). COVID-19 and cyber fraud: emerging threats during the pandemic, *Journal of Financial Crime,* 29 (2), 433-446. https://doi.org/10.1108/JFC-01-2021-0016

Mayer, L. (2018). Criminological Elements for the Criminal Legal Analysis of Cybercrime. *Ius et Praxis, 24*(1), 159-206. http://dx.doi.org/10.4067/S0718-00122018000100159

Mitchell,K., Finkelhor, D. & Becker-Blease, K.A. (2006). Classification of Adults with Problematic Internet Experiences: Linking Internet and Conventional Problems from a Clinical Perspective. *CyberPsychology & Behavior, 10*(3), 381–392. https://doi.org/10.1089/cpb.2006.9941

Mitchell, V. (1999). Consumer perceived risk: conceptualisations and models. *European Journal of Marketing, 33*(1/2),163-195. https://doi.org/10.1108/03090569910249229

Muniesa, P., Herrera, D., Guerrero, O., Martínez, F., Rubio, M., Gil, V., Santiago, A. & Gómez, M. (2022). *Informe sobre la cibercriminalidad en España*. Ministerio del Interior. http://sl.ugr.es/0e1p

Norris, G. & Brookes, A. (2021). Personality, Emotion and Individual Differences in Response to Online Fraud. *Personality and Individual Differences, 169*, 109847. https://doi.org/10.1016/j.paid.2020.109847

Norris, G., Brookes, A. & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5

Phiri, J., Lavhengwa, N. & Segooa, M. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management, 26*(1), https://doi.org/10.4102/sajim.v26i1.1763

Purkait, S., Kumar De, S. & Suar, D. (2014). An Empirical Investigation of the Factor that Influence Internet User's Ability to Correctly Identify a Phishing Website. *Information Management & Computer Security, 22(3)*, 194-234. https://doi.org/10.1108/IMCS-05-2013-0032

Reynolds, L. & Parker, L. (2018). *Digital resilience: Stronger citizens online*. Institute for Strategic Dialogue. http://sl.ugr.es/0cGT

Ribble, M., Bailey, G. & Ross, T. (2004). Digital Citizenship, addressing appropriate technology behavior. *Learning & Leading with Technology, 32*(1). https://files.eric.ed.gov/fulltext/EJ695788.pdf

Ross, M., Grossmann, I. & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science, 9*(4), 427-442. https://doi.org/10.1177/1745691614535935

Segura, J. (2017). *Compromised LinkedIn accounts used to send phishing links via private message and InMail*. Malwarebytes Labs http://sl.ugr.es/0e1x

Sorell, T. & Whitty, M. (2019). Online Romance Scams and Victimhood. *Security Journal, 32*(3), 342–361. https://doi.org/10.1057/s41284-019-00166-w

Torres-Hernández, N., Gallego-Arrufat, M.J., & García-Ruiz, M.M. (2023). Citizens' reflections on an open, distance intergenerational program for online risk prevention. *Digital Education Review. Universidad de Barcelona. 41*, 35-53. https://revistes.ub.edu/index.php/der/article/download/41067/41068/124507

Torres-Hernández, N., García-Martínez, I., & Gallego-Arrufat, M.-J. (2022) Internet Risk Perception. Development and Validation of a Scale for Adults. *Eur. J. Investig. Health Psychol. Educ.* 12, 1581–1593. https://doi.org/ 10.3390/ejihpe12110111

Wang, Q., Wang, L., Zhang, X., Mao, Y. & Wang, P. (2017). The impact research of online reviews' sentiment polarity presentation on consumer purchase decisions. *Information Technology & People, 30*(3), 522-541. https://doi.org/10.1108/ITP-06-2014-0116

Wei. R., Liu., X.S. & Liu, X. (2019). Examining the Perceptual and Behavioral Effects of Mobile Internet Fraud: A Social Network Approach. *Telematics and Informatics, 41*,103-113. https://doi.org/10.1016/j.tele.2019.04.002

Whittaker,J., Edwards, M.,Cross, C. & Button, M. (2023). I Have Only Checked after the Event. Consumer Approaches to Safe Online Shopping, *Victims & Offenders, 18*(7), 1259-1281. https://doi.org/10.1080/15564886.2022.2130486

Williams, E.J., Beardmore, A. & Joinson, A. (2017). Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computer in Human Behavior, 72*, 412-421. https://doi.org/10.1016/j.chb.2017.03.002

Zhang Z. & Ye Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. *Frontiers in Psychology, 13*, 1030670. https://doi.org/10.3389/fpsyg.2022.1030670