Revista Española
de Investigación Criminológica

2024, vol**22**(2) e887
https://doi.org/10.46381/reic.v22i2.887

Perfil de conducta digital, ciberdelitos y cifra negra: análisis de una muestra española

Digital behaviour profile, cybercrimes, and dark figure: analysis of a Spanish sample

Nieves Erades Pérez*, Esther Sitges Maciá

Universidad Miguel Hernández
*Corresponding author(s): nerades@umh.es

Recibido diciembre 2023 / Aceptado octubre 2024

Resumen

El objetivo de este estudio fue analizar la cibervictimización, la denuncia y los perfiles de conducta adoptados frente a preocupaciones en línea en la población española, utilizando datos de la Encuesta del Eurobarómetro 92.2 (N=1005). Se emplearon análisis descriptivos, análisis de componentes principales, correlaciones de Pearson y árboles de decisión para examinar las relaciones entre variables. Los resultados revelaron una preocupante falta de conocimiento (13.8%) sobre los procedimientos de denuncia de delitos cibernéticos, y una tasa de notificación de solo el 20% de las victimizaciones. Se identificó un perfil predominante de comportamiento pasivo-evitativo, asociado con la escasez de conocimiento y la no actividad laboral. Se encontró una correlación positiva entre el miedo, la inseguridad y el conocimiento en el ámbito de los ciberdelitos. Se destaca la urgencia de mejorar la comprensión general sobre los procedimientos de denuncia, la necesidad de clarificar términos para futuras investigaciones en ciberseguridad, así como la importancia de explorar variables psicológicas.

Palabras clave: Cibervictimización, denuncia, miedo funcional, miedo disfuncional, inseguridad.

Abstract

The aim of this study was to analyse cyber victimisation, reporting behaviours, and behavioural profiles adopted in response to online concerns within the Spanish population, using data from Eurobarometer Survey 92.2 (N=1005). Descriptive analyses, principal component analyses, Pearson correlations, and decision trees were employed to examine variable relationships. Results revealed a concerning lack of knowledge (13.8%) regarding procedures for reporting cybercrimes, with only a 20% victimisation reporting rate. A predominant passive-avoidant behavioural profile was identified, associated with limited knowledge and non-employment. A positive correlation was found between fear, insecurity, and knowledge within the realm of cybercrimes. Emphasising the urgent need to enhance general understanding of reporting procedures, the necessity for terminology clarification for future cybersecurity investigations, and the significance of exploring psychological variables.

Keywords: Cyber victimisation, reporting, functional fear, dysfunctional fear, insecurity.

1. Introducción

En las últimas décadas, el uso de internet ha experimentado una expansión significativa, abarcando múltiples áreas de actividad y convirtiéndose en una herramienta indispensable en la sociedad actual. Entre los años 2016 y 2021, se registró un aumento considerable del uso de internet a nivel global, llegando a 44.19 puntos porcentuales e incrementándose desde un 43% hasta un 62%, según la Unión Internacional de Telecomunicaciones (UIT, 2023). Siguiendo esta línea, los datos globales sugieren que aproximadamente 5.400 millones de individuos, equivalentes al 67% de la población mundial, contaban con conexión a Internet al finalizar el año 2023 (UIT, 2023). Este crecimiento ha sido especialmente notable en Europa, donde el acceso a Internet en los hogares de la Unión Europea alcanzó en torno a un 93% en el año 2021 (Eurostat, 2021). Adicionalmente, esta expansión se ve facilitada por el desarrollo de infraestructuras de banda ancha, la reducción de costes en el acceso y la proliferación de dispositivos digitales. Además del incremento en el acceso, también se han diversificado de forma significativa las distintas actividades que pueden realizarse en línea. Actualmente, los usuarios no solo utilizan Internet para consultas de correo electrónico o búsqueda de información, sino también para una amplia gama de servicios como transacciones bancarias, compras, educación y acceso a servicios públicos (Eurostat, 2021).

En el ámbito español, se evidencia un proceso equiparable al que se observa en el resto de Europa, alcanzando el 96.1% de acceso a Internet en hogares españoles en el año 2022, y siendo la actividad más frecuente, tanto para hombres como para mujeres, el uso de mensajería instantánea a través de plataformas como WhatsApp (INE, 2023). Además, la búsqueda de información en línea es una actividad predominante que abarca desde noticias hasta aspectos específicos relacionados con la salud, educación y servicios gubernamentales. En paralelo, el comercio electrónico ha experimentado un crecimiento considerable, con un número creciente de usuarios participando en compras en línea que abarcan una amplia gama de productos y servicios. En el año 2019, la proporción de compradores en línea en los últimos tres meses se situaba en el 46.9% de la población entre 16 y 74 años, ubicándose ligeramente por debajo de la media de la Unión Europea. Sin embargo, esta tendencia ha sido ascendente a lo largo de los años, y se ha visto aún más potenciada tras la pandemia de COVID-19 (INE, 2021). Por tanto, esta evolución tecnológica ha impulsado un flujo continuo de información, optimizando procesos operativos e impulsando la innovación en distintos sectores, desde el ámbito empresarial hasta la gestión pública.

No obstante, este progreso ha conllevado notables desafíos, especialmente en términos de accesibilidad y seguridad, y en los últimos años ha contribuido significativamente al aumento exponencial del cibercrimen, definido este como actividades ilícitas ejecutadas en el ciberespacio. Sin embargo, este es un fenómeno complejo tanto en su definición como en su legislación, ya que alberga tanto delitos existentes como nuevos tipos de delitos que son exclusivos de este entorno (Jewkes y Yar, 2011; Miró Llinares, 2012; Wall, 2017). Pese a que en los últimos años se ha evidenciado una tendencia en disminución de las actividades delictivas realizadas en el espacio físico (Caneppele y Aebi, 2017), diversos estudiosos han planteado que esta reducción señala un desplazamiento de la criminalidad hacia el contexto digital (Button y Cross, 2017; Caneppele y Aebi, 2017). Además de los desafíos inherentes al aumento del cibercrimen debido a este desplazamiento, encontramos limitaciones significativas que obstaculizan la prevención efectiva de estos delitos. En particular, se

observa una dependencia excesiva de las organizaciones para liderar los esfuerzos en ciberseguridad, centrando la mayoría de las medidas en aspectos técnicos y dejando de lado los factores humanos esenciales en la ecuación del delito cibernético. Estas prácticas, que suelen seguir estándares de la industria y basarse en experiencias anecdóticas, carecen de evidencia empírica que demuestre su eficacia en enfrentar específicamente los delitos cibernéticos (Ho et al., 2022). Por lo tanto, esta tendencia destaca la necesidad de adoptar un enfoque más holístico que integre una mejor comprensión de los factores humanos junto con las soluciones tecnológicas (Back y LaPrade, 2019)

En cuanto a los datos relativos al cibercrimen, la pandemia de COVID-19 constituyó un punto de inflexión, exacerbando todavía más las tendencias de aumento de cibercrimen que se observaban en años anteriores y en el año 2020 el coste de la ciberdelincuencia para la economía global fue de aproximadamente 5.5 billones de dólares, el doble que en 2015 (Comisión Europea, 2021). Es evidente que tras el año 2020 diversos factores, como la transición masiva hacia el teletrabajo, la educación en línea y el aumento de transacciones digitales crearon nuevas oportunidades para los delincuentes, facilitando un desplazamiento en el entorno dónde se realiza el delito, en este caso hacia el contexto digital (Miró Llinares, 2021). De acuerdo con el informe de Europol (2021), Europa ha sufrido un incremento notable en los ataques cibernéticos, abarcando modalidades como el phishing, el malware y los ataques a infraestructuras. En España, también encontramos este aumento del cibercrimen y los datos del Ministerio del Interior confirman que las cifras se alinean con las tendencias observadas en Europa. Específicamente, en el año 2022, se notificaron un total de 374.737 incidentes, representando un incremento del 22.7% con respecto al año anterior (2021). De esta cifra, el 89.7% corresponde a casos de fraudes informáticos (Ministerio de Interior, 2023). Sin embargo, a pesar del incremento de los ciberdelitos, probablemente la cifra real se encuentre por encima de los datos oficiales. La existencia de cifra negra en este tipo de delitos, definida como la discrepancia entre la cantidad real de delitos cometidos y los casos notificados oficialmente o denunciados a las autoridades, se ha confirmado en diversos estudios (Button y Cross, 2017; Kemp et al., 2020; Tcherni et al., 2016), por lo que es conveniente valerse de otras fuentes, como las encuestas de victimización (Mayhew y Dijk 2012). Sin embargo, estas encuestas también presentan limitaciones, como el subregistro, atribuible tanto a la dificultad de recordar incidentes menores como a la falta de conciencia sobre haber sido víctima o la reticencia a reconocerlo públicamente. Además, los cambios metodológicos y la diversidad de nomenclatura entre encuestas pueden dificultar la comparabilidad de los resultados.

1.1. Estado de la cuestión

Los motivos que pueden llevar a una víctima a no informar sobre su experiencia de victimización son diversos. Estos incluyen desde el desconocimiento de haber sido víctima o del procedimiento para denunciar, hasta sentimientos de vergüenza o la percepción de que la denuncia resultará inútil (Kemp et al., 2020). En este sentido, no deben tomarse en consideración únicamente las pérdidas económicas asociadas al cibercrimen, sino que debemos considerar también que este tipo de victimización lleva asociada consecuencias tanto físicas como emocionales, como la pérdida de relaciones personales o el desarrollo de sintomatología, por ejemplo, depresiva (Button et al., 2009; Cross et al., 2014; Golladay y Holtfreter, 2017). Además, las disparidades en el acceso a recursos de

ciberseguridad pueden exacerbar las desigualdades preexistentes, dejando a grupos vulnerables más expuestos a riesgos en línea (Van Dijk, 2005). Un ejemplo lo constituyen las personas adultas mayores, quienes pueden enfrentarse a dificultades para adquirir habilidades digitales debido a su falta de familiaridad con la tecnología (Schreuers et al., 2017), lo que limitaría la capacidad tanto de protegerse en este entorno como de acceder a recursos que le permitan notificar una victimización.

Una variable que puede verse afectada por el incremento de la ciberdelincuencia es el miedo a convertirse en víctima, en este caso de ciberdelitos. El miedo al delito constituye una variable de notable complejidad, cuya intricación se intensifica al ser examinada dentro del contexto digital, un dominio relativamente reciente en el estudio del miedo al crimen. La integración progresiva de la tecnología en nuestras vidas diarias, junto con el desarrollo constante de amenazas cibernéticas, presenta retos adicionales en la definición y medición del miedo a la ciberdelincuencia. Se añade a esto un obstáculo adicional: la existencia de múltiples formas de cibercrimen, cada una de las cuales puede interactuar de manera distinta con la emoción del miedo (Castro Toledo, 2018). En cuanto a su naturaleza aparentemente negativa, cabe señalar que en las últimas décadas se han diferenciado dos variantes: un miedo disfuncional, que afecta a la calidad de vida, y un miedo funcional que impulsa la implementación de medidas preventivas sin menoscabar la funcionalidad del individuo. Desde esta perspectiva, el miedo funcional puede motivar a las personas para protegerse, sin un impacto significativo en el acceso a diferentes recursos (Jackson y Gray, 2010; Yar y Steinmetz, 2019). Estas conductas proactivas abarcan una amplia gama de medidas, como podría ser cerrar la puerta con llave, si nos referimos al contexto físico o, la instalación de antivirus en dispositivos electrónicos, en el contexto digital. En este punto conviene distinguir el miedo al delito de una variable relacionada, como es la inseguridad. La percepción de inseguridad, al igual que el miedo, constituye una variable subjetiva estrechamente ligada al contexto o entorno físico, y se encuentra influenciada por una combinación de variables personales, sociales y ambientales (Valera y Guàrdia, 2014). Sin embargo, la percepción de inseguridad consiste en un concepto más amplio que el miedo específico al ciberdelito, ya que no solo se concentra en el temor a convertirse en víctima, sino también en experimentar inseguridad y percibir una falta de control en un entorno concreto. Por ende, la interacción entre ambas variables, inseguridad y miedo, en su aspecto negativo, podría motivar a los individuos a abstenerse de utilizar estas herramientas digitales, lo que representa un desafío significativo. Sin embargo, en su aspecto positivo, un cierto nivel de miedo podría impulsar a los usuarios a adoptar medidas de protección en el entorno digital, reduciendo así la probabilidad de ser víctimas. A pesar de que numerosas investigaciones han analizado estas variables en el ámbito físico, los estudios en el espacio digital son más limitados y suelen emplear diferentes términos como miedo, preocupación o inquietud. Además, con frecuencia se ven influenciados por datos obtenidos del crimen tradicional, a pesar de que el comportamiento en el entorno digital podría diferir (Brands y Van Doorn, 2022).

En consecuencia, este estudio se enfocó en la exploración y comprensión de las percepciones, comportamientos y factores que podrían estar asociados con diferentes patrones de conducta en la red. Se empleó una muestra de la población española, utilizando los datos obtenidos de la Encuesta del Eurobarómetro 92.2. El objetivo primordial consistió en identificar modelos, correlaciones y posibles factores determinantes que pudieran influir en la percepción de inseguridad digital, así como en la toma de decisiones respecto a la denuncia o no de incidentes relacionados con delitos cibernéticos.

2. Método

En línea con el objetivo principal del estudio, se realizaron las siguientes preguntas de investigación, referidas a nuestra muestra:

P1: ¿Cuál es la magnitud de las notificaciones de ciberdelitos, los canales utilizados para realizar dichas notificaciones y el nivel de conocimiento de los usuarios acerca de los procedimientos para efectuar estas denuncias?

P2: ¿Qué variables se relacionan con la decisión de notificar o abstenerse de informar de los incidentes de ciberdelitos?

P3: ¿Existe una asociación entre la victimización previa de delitos cibernéticos y un incremento en la percepción de inseguridad y miedo? ¿Qué otras variables muestran una relación con estos aspectos en el contexto de la ciberseguridad?

P4: ¿Cuáles son las variables determinantes que influyen en la adopción de un patrón de comportamiento evasivo basado en la preocupación frente a un patrón de comportamiento activo orientado a la protección en el contexto de la ciberseguridad?

Para responder a estas cuestiones este estudio se fundamentó en la base de datos de la Encuesta del Eurobarómetro 92.2, realizada en 2019 en los 28 países de la Unión Europea y publicada en 2021. La recopilación de datos se extendió desde el 8 de octubre de 2019 hasta el 22 de octubre de 2019. Su diseño muestral se fundamentó en un modelo de muestreo de probabilidad aleatoria en múltiples etapas, seleccionando un conjunto de puntos de muestreo con una probabilidad proporcional al tamaño de la población, asegurando una representación geográfica y demográfica adecuada y una cobertura nacional exhaustiva. En este estudio, los análisis se realizaron teniendo en cuenta la submuestra específica que representaba a la población española (n=1005).

Todos los análisis estadísticos se realizaron con el programa SPSS v27. Previo al análisis, se llevó a cabo un proceso de preprocesamiento y limpieza de los datos. Esto implicó la identificación y tratamiento de valores perdidos para mantener la integridad y la consistencia de la información utilizada. En nuestro conjunto de datos, la cantidad de valores perdidos resultó ser mínima, representando menos del 1% del total. Esta baja incidencia de datos ausentes permitió abordar el problema de manera eficiente mediante técnicas de imputación sencillas sin comprometer la integridad del análisis. En estos casos específicos, optamos por utilizar la imputación por la media para las variables afectadas. Este método consiste en sustituir los valores perdidos por el promedio de las respuestas existentes para cada variable, asegurando así la continuidad y coherencia de nuestros datos sin introducir sesgos significativos en los resultados finales del estudio. Esta técnica fue elegida debido a su simplicidad y efectividad en situaciones donde los valores perdidos son escasos y aleatoriamente distribuidos. Asimismo, realizamos un proceso de organización y ajuste de los datos para mejorar la claridad y consistencia de nuestros análisis. Este proceso incluyó la agrupación de ítems según la variable de interés. Además, en algunos casos fue necesario recalibrar la escala utilizada, es decir, ajustamos los valores de las variables para que siguieran la misma dirección en todos los casos. Esto fue esencial para asegurar que los resultados de diferentes análisis fueran comparables y coherentes. Detallaremos más sobre estas agrupaciones y los métodos de recalibración empleados en secciones posteriores.

El análisis se estructuró en tres bloques principales para examinar en profundidad las variables de interés, en consonancia con nuestras preguntas de investigación.

En primer lugar, se llevó a cabo un análisis descriptivo (frecuencias y porcentajes para variables categóricas y medias, medianas y desviaciones típicas para variables cuantitativas) de las variables sociodemográficas, cibervictimización previa, notificación y conocimiento del proceso de denuncia, lo que permitió obtener una panorámica global de estas variables. En segundo lugar, con el fin de examinar el solapamiento existente entre las variables miedo y preocupación e inseguridad y evaluar la posibilidad de integrarlas en un único constructo, se llevó a cabo un Análisis Factorial Exploratorio, utilizando como método de extracción el Análisis de Componentes Principales (ACP). Esta técnica estadística posibilita la reducción de la dimensionalidad en un conjunto de datos al identificar los componentes principales, representados como combinaciones lineales de las variables originales, con el objetivo de capturar la mayor proporción de variabilidad conjunta en un número reducido de factores. Posteriormente, para evaluar las asociaciones entre nuestras variables de interés, se utilizó el coeficiente de correlación de Pearson.

Por último, se llevaron a cabo árboles de decisión. Los árboles de decisión constituyen una técnica de minería de datos que explora y analiza los datos en busca de información subyacente. Esta metodología aborda problemas de predicción, clasificación y segmentación. Su funcionamiento se basa en la creación de un modelo de clasificación representado mediante diagramas de flujo. Estos modelos categorizan casos en grupos o anticipan valores de una variable dependiente (criterio), en función de los valores observados en variables independientes (predictoras) (Berlanga et al., 2013). El primer modelo, se focalizó en comprender los factores que influyen en la decisión de denunciar o no delitos cibernéticos después de haber experimentado al menos una victimización. En el segundo modelo de nuestro análisis, centramos nuestra atención en cómo las preocupaciones sobre la seguridad en línea pueden influir en el comportamiento en línea de los individuos. La variable dependiente en este modelo fue el perfil de cambio de conducta, clasificado en dos categorías principales: pasivo-evitativo y activo-protección. Esta categorización refleja las diferentes formas en que las personas pueden responder a las preocupaciones sobre su seguridad digital. Los detalles específicos sobre cómo se definieron y categorizaron estas respuestas se explicarán en secciones posteriores del estudio.

2.1. Variables

A continuación, se detallan los ítems empleados para la evaluación de las variables de interés

Preocupación en red

Ítem QC15: ¿Podría decirme en qué medida está de acuerdo o en desacuerdo con las siguientes afirmaciones? (Escala Likert de 1, totalmente en desacuerdo a 5, totalmente de acuerdo).

- Le preocupa que los sitios web no mantengan segura su información personal en Internet.
- Le preocupa que las autoridades públicas no mantengan segura su información personal en Internet.
- Evita dar información personal en Internet.

- Cree que el riesgo de ser una víctima de ciberdelito está aumentando.
- Es capaz de protegerse a sí mismo/a lo suficiente contra los ciberdelitos. (En este caso 1 Totalmente de acuerdo y 5 Totalmente en desacuerdo).

Miedo a la cibervictimización.

Ítem QC8: Los ciberdelitos incluyen distintos tipos de actividades delictivas. ¿Hasta qué punto le preocupa personalmente la posibilidad de sufrir o ser víctima de las siguientes situaciones? (Escala Likert de 1, Nada preocupado a 5, Muy preocupado).

- Correos electrónicos o llamadas de teléfono fraudulentas para pedirle sus datos personales (incluidos el acceso a su ordenador, sus nombres de usuario y contraseñas, su información bancaria o de pago).
- Fraude online en el que los productos comprados no son enviados, son falsificados o no son como se anuncian.
- No poder acceder a servicios online como servicios bancarios o servicios públicos a causa de ciberataques.
- La infección de dispositivos con software malicioso (virus, etc.).
- Robo de identidad (alguien roba sus datos personales y suplanta su identidad).
- Encontrar accidentalmente en Internet material que contenga abusos sexuales a niños.
- Material online que fomenta el odio racial o el extremismo religioso.
- Pirateo de cuentas en las redes sociales o de correo electrónico.
- Fraude bancario o con tarjeta bancaria por Internet.
- Que le exijan un pago a cambio de recuperar el control de su dispositivo.

Cambios en conducta debido a la preocupación

Ítem QC5: ¿La preocupación por cuestiones de seguridad le ha hecho cambiar la manera en cómo utiliza Internet en alguna de las siguientes formas?

Pasivas-evitación:

- Es menos probable que compre productos o servicios online.
- Es menos probable que utilice la banca online.
- Es menos probable que introduzca información personal en sitios web.
- Sólo visita sitios web que conoce y en los cuales confía.
- No abre correos electrónicos de gente que no conoce.

Activas-protección:

- Ha cambiado su configuración de seguridad (por ejemplo, en su navegador, redes sociales, motor de búsqueda).
- Utiliza contraseñas diferentes para sitios diferentes.
- Sólo utiliza su propio ordenador.
- Ha instalado un software antivirus.
- Ha cancelado una compra por Internet porque sospechaba del vendedor o del sitio web.

- Cambia sus contraseñas con regularidad.
- Usa contraseñas más complejas que en el pasado.
- Utiliza un administrador de contraseñas.
- Utiliza datos biométricos (p. ej., reconocimiento facial, huella dactilar).
- No se conecta a Internet a través de redes públicas no seguras.

Para garantizar una comparación justa y equitativa entre las dos categorías de comportamiento (pasivo-evitativo y activo-protección) aplicamos un proceso de normalización de las puntuaciones. Una vez normalizados los puntajes, realizamos una comparación entre el total de la puntuación normalizada de las conductas evitativas y las conductas de protección. La comparación de los resultados nos permitió identificar cuatro perfiles distintos de comportamiento en relación con la seguridad en línea, cada uno predominando por un tipo específico de conducta. Estos perfiles son:

- Perfil 1 (Sin cambios/No está preocupado): No muestra preocupación significativa por la seguridad en línea y no se observan cambios notables en su comportamiento.
- Perfil 2 (Combinado): No prevalece un tipo específico de conducta, sino que se observa una mezcla de comportamientos.
- Perfil 3 (Pasivo-evitativo): Predominan conductas de evitación, caracterizadas por una respuesta retraída frente a las preocupaciones de seguridad.
- Perfil 4 (Activo-protección): Las conductas activas de protección son las más prominentes, con una clara tendencia a tomar medidas proactivas ante las preocupaciones de seguridad en línea.

Conocimiento ciberdelitos

A través del ítem QC7: ¿En qué medida está usted informado/a sobre los riesgos de los ciberdelitos? (Escala Likert de 1, asociado a nada informado, 5, muy bien informado).

Victimización previa

Ítem QC9: En los últimos tres años, ¿con qué frecuencia ha experimentado personalmente o ha sido víctima de cada una de las siguientes situaciones? (mismas opciones de cibervictimización que en el ítem QC8).

Opciones de respuesta: nunca (0 punto), una sola vez (1 punto), dos o tres veces (2 puntos), más de tres veces (3 puntos).

Notificación de la victimización

Ítem QC13: ¿Conoce la existencia de alguna página web, dirección de correo electrónico, formulario online o número de contacto en España donde pueda denunciar un ciberdelito o cualquier otro comportamiento ilegal que se produzca en la red (p. ej., ciberataques, acoso o bullying online)?

- Si, un sitio web.
- Si, una dirección de correo electrónico.
- Si, un formulario online.

- Si, un número de contacto.
- Si, otro modo de denunciar un ciberdelito o cualquier otro comportamiento ilegal en la red.
- No, no conoce de su existencia.

En función de los resultados de esta variable se realizaron tres grupos: no conoce ningún método de denuncia, conoce un método de denuncia, conoce 2 o más métodos de denuncia.

Ítem QC14: ¿Alguna vez ha denunciado algún ciberdelito u otro comportamiento ilegal en la red (p. ej., ciberataque, acoso o bullying online)?

- Si, a la policía o autoridades.
- Si, a un proveedor de servicios.
- Si, a un sitio web.
- Si, a una organización de protección de consumidores.
- Si, a otra persona.
- No, nunca.

En función de las respuestas a este ítem se creó una nueva variable con dos categorías: alguna vez ha denunciado y nunca ha denunciado.

Ítem QC11: ¿Qué ha hecho usted en cada una de las situaciones que ha experimentado personalmente o en las que ha sido víctima?

Para cada uno de los diferentes tipos de cibervictimización contemplados, se crearon las siguientes opciones de respuesta: Nada; Se puso en contacto con la policía, Se puso en contacto con el sitio web o el vendedor; se puso en contacto con su proveedor de servicios de internet; Se puso en contacto con una organización para la protección del consumidor; Denunció la situación a través de un sitio web o correo electrónico oficiales; Otro.

3. Resultados

3.1. Análisis descriptivo

Variables sociodemográficas

La edad media de los participantes fue de 50,97 años (DE = 18,97; rango 15-93). Los estadísticos descriptivos de la muestra referentes a las variables sociodemográficas se encuentran en la Tabla 1.

Victimización previa y notificación

La Tabla 2 presenta los datos relacionados con la experiencia previa de cibervictimización, junto con los comportamientos asociados tanto a la notificación u omisión del incidente. Se presenta, además, los datos referentes al nivel de conocimiento que los encuestados tienen acerca de las diversas opciones disponibles para notificar incidentes en línea.

Tabla 1

Características sociodemográficas

Variable	N	%
Género		
Mujer	522	51.9
Hombre	483	48.1
Tipo de comunidad		
Área rural o pueblo	417	41.5
Ciudad pequeña o mediana	363	36.1
Ciudad grande	225	22.4
Estado civil		
Soltero/a	238	22.7
Casado/a o viviendo en pareja	613	61.0
Divorciado/a o separado/a	74	7.4
Viudo/a	89	8.9
Grupos de edad		
15-24 años	111	11.0
25-34 años	116	11.5
35-44 años	143	14.2
45-54 años	181	18.0
55-64 años	175	17.4
65-74 años	154	15.3
75 años o más	125	12.4
Situación laboral		
Autónomo/a	73	7.3
Directivos/as y otros (oficina)	137	13.7
Empleos manuales	244	24.3
Trabajo doméstico no remunerado	98	9.8
Desempleado/a	92	9.2
Retirado/a	284	28.3
Estudiante	77	7.7

Tabla 2

Victimización y denuncia

Variable	N	%
Al menos una victimización	283	28.2
Fraude por correo electrónico o llamadas	156	15.5
No hizo nada	94	60.0
Acudió a la policía	12	7.9
Informó utilizando otros medios	49	32.1
Fraude en compras online	48	4.8
No hizo nada	13	27.1
Acudió a la policía	9	18.8
Informó utilizando otros medios	25	52.1
No poder acceder a servicios por ciberataques	33	3.3
No hizo nada	13	40.0
Acudió a la policía	0	0.0
Informó utilizando otros medios	20	60.0

Variable	N	%
Software malicioso	164	16.3
No hizo nada	76	46.3
Acudió a la policía	12	7.4
Informó utilizando otros medios	76	46.3
Robo de identidad	38	3.8
No hizo nada	8	21.0
Acudió a la policía	14	36.9
Informó utilizando otros medios	16	42.1
Acceso accidental a material de pornografía infantil	22	2.2
No hizo nada	7	31.8
Acudió a la policía	8	36.4
Informó utilizando otros medios	7	31.8
Acceso accidental a material extremista	61	6.1
No hizo nada	34	55.8
Acudió a la policía	9	14.7
Informó utilizando otros medios	18	29.5
Pirateo de cuenta	38	3.8
No hizo nada	17	44.7
Acudió a la policía	5	13.2
Informó utilizando otros medios	16	42.1
Fraude bancario	29	2.9
No hizo nada	6	20.7
Acudió a la policía	12	41.4
Informó utilizando otros medios	11	37.9
Ransomware	30	3.0
No hizo nada	12	40.0
Acudió a la policía	7	23.3
Informó utilizando otros medios	11	36.7
Conocimiento de medios notificación online		
No conoce ninguno	866	86.2
Conoce una página web	80	7.9
Conoce una dirección de email	17	1.7
Conoce un formulario online	9	.9
Conoce un número de teléfono	27	2.7
Conoce otro método	22	2.2

Como podemos observar, del total de la muestra (n= 1005), el 28.2% de los individuos habían sido víctimas de los ciberdelitos evaluados en al menos una ocasión. Sin embargo, de esta cifra, únicamente 57 personas (20% de las que habían sido victimizadas) optaron por informar mediante cualquier medio. Además, se observó que la gran mayoría de los usuarios encuestados (86.2%) carecía de conocimiento sobre los procedimientos disponibles para notificar incidentes en el entorno digital. En cuanto a los ciberdelitos más predominantes, se destacaron la infección de dispositivos mediante software malicioso, experimentada por el 16.3% del total de la muestra, seguido por el fraude a través de correo electrónico y llamadas, afectando al 15% de los encuestados.

3.2. Análisis de Componentes Principales (ACP) y correlaciones

Debido al posible solapamiento, que la literatura analizada ha puesto de manifiesto, entre las variables relacionadas con la preocupación y el miedo a la cibervictimización (Danieli & Paz García, 2020; Hummelsheim et al., 2011; Reid et al., 2020; Valera & Guardià, 2014) se realizó un análisis de componentes principales con los 14 ítems que formaban estas variables. El determinante 6.3^{-9} y prueba Kaiser-Meyer-Olkin .957 con significación <0.01 en la prueba de esfericidad de Barlett, confirmó la alta correlación de las variables y su posibilidad de agrupación mediante este método. Tras el análisis, se obtuvo un factor que explicaba el 72.7% de la varianza del conjunto de variables, cuya matriz factorial se presenta en la tabla 3. De esta forma se creó la variable "Inseguridad", ya que el concepto puede abarcar tanto al miedo como a la preocupación en línea, al ser esta más global que las anteriores.

Tabla 3

Matriz factorial componente "Inseguridad"

Ítem	Componente
Preocupación en red	
Le preocupa que los sitios web no mantengan segura su información personal en Internet	.765
Le preocupa que las autoridades públicas no mantengan segura su información personal en Internet	.717
Cree que el riesgo de ser una víctima de ciberdelito está aumentando	.715
Es capaz de protegerse a sí mismo/a lo suficiente contra los ciberdelitos	.291
Miedo a la cibervictimización	
Cibervictimización por fraude correos y llamadas	.863
Cibervictimización por fraude en compras	.888
Cibervictimización al no poder acceder a servicios online como servicios bancarios o servicios públicos a causa de ciberataques	.881
Cibervictimización por software malicioso	.899
Cibervictimización por robo de identidad	.943
Cibervictimización al encontrar accidentalmente pornografía infantil	.924
Cibervictimización al encontrar material extremista	.912
Cibervictimización por pirateo de cuentas	.935
Cbiervictimización por fraude de banca online o tarjeta	.941
Cibervictimización al exigirle un pago a cambio de recuperar el control de su dispositivo (Ramsomware)	.928

Método de extracción: análisis de componentes principales.

Posteriormente se llevaron a cabo análisis de correlaciones de Pearson para examinar las relaciones lineales entre las variables específicas de interés, tal como se muestra en la Tabla 4.

Tabla 4

Correlaciones de Pearson.

	Edad	Conocimiento denuncia	Información ciberdelitos	Victimización previa	Inseguridad
Edad	1	-.158**	-.405**	-.224**	.-.502**
Conocimiento método denuncia		1	.298**	.167**	.197**
Información sobre ciberdelitos			1	.232**	.498**
Victimización previa				1	.167**
Inseguridad					1

** p ≤ .01

Cómo se puede observar los análisis mostraron una correlación significativa entre todas las variables analizadas. La inseguridad correlacionaba de forma positiva con el conocimiento sobre ciberdelitos y métodos de denuncia, así como con la victimización previa. Sin embargo, la edad correlacionaba de forma negativa con todas las variables analizadas. Por tanto, las personas que se sentían más inseguras tenían más conocimientos sobre ciberdelitos y métodos de denuncia, además habían sido víctimas de algunos de los ciberdelitos evaluados en los últimos 3 años y eran más jóvenes.

3.3. Árboles de decisión

Por último, se realizaron dos árboles de decisión, mediante el método de crecimiento CHAID, para profundizar en dos aspectos cruciales. El primer árbol se realizó centrándonos en la predicción de la preferencia a realizar denuncias como variable dependiente y el segundo árbol se enfocó en el tipo de conductas realizadas ante diferentes preocupaciones en la red, diferenciando entre un perfil de conducta funcional (conductas activas-de protección) y disfuncional (conductas pasivas-de evitación), con el objetivo de identificar elementos determinantes en la realización de un tipo de conductas u otras. Los árboles realizados se muestran en las Figuras 1 y 2.

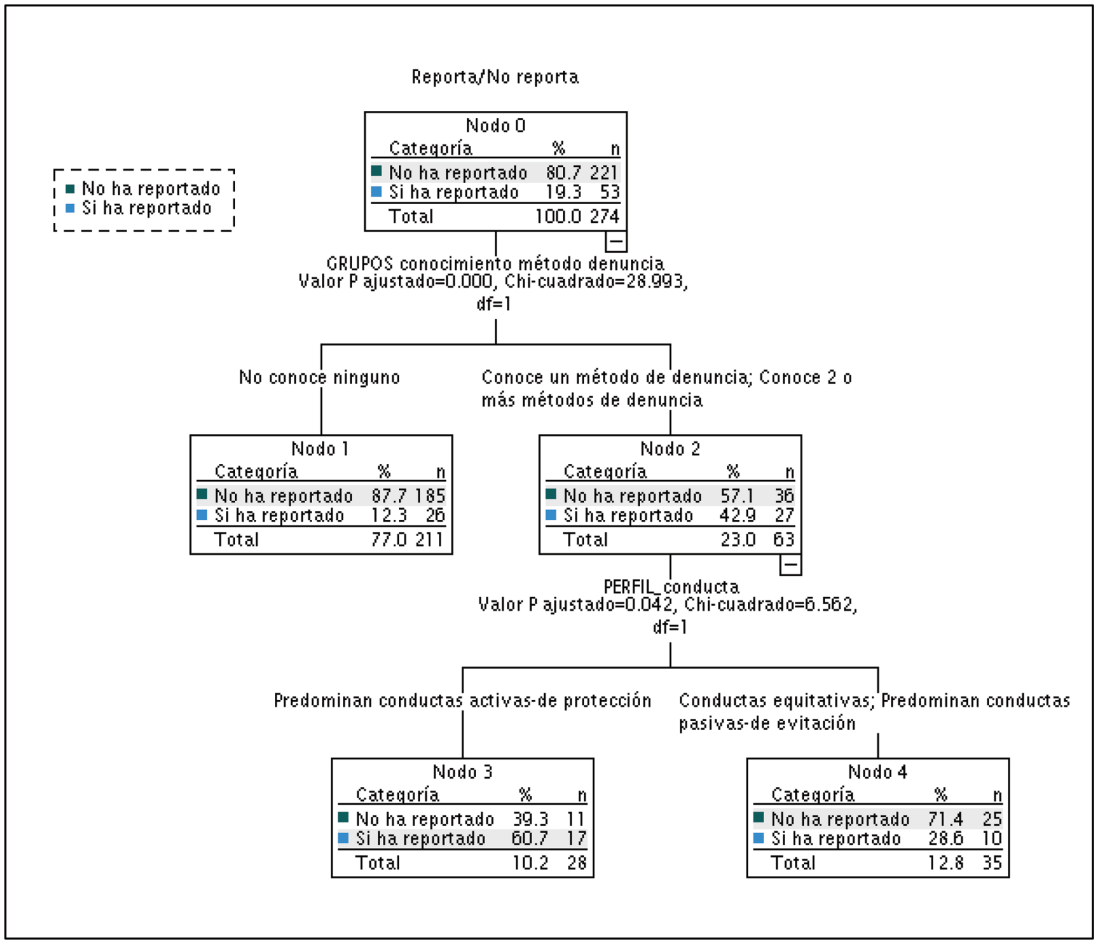
Notificación de cibervictimización

Para la realización de este árbol seleccionamos las 283 personas de la muestra que habían sufrido al menos una victimización en la red. Como variables predictoras utilizamos la edad, el sexo, la ocupación, el tipo de comunidad, el conocimiento sobre métodos de denuncia y el perfil predominante ante el miedo-preocupación.

Tal y como se muestra en la Figura 1, de todas estas variables, sólo el conocimiento de métodos de notificación y el perfil de conducta ante la preocupación en red fueron determinantes. El 71.4% de la no notificación de una victimización se encuentra explicado por un estilo evitativo (perfil disfuncional) sumado a un desconocimiento de métodos de notificación online. Este modelo clasifica correctamente al 82.8% de la muestra (estimación de riesgo = .172).

Figura 1

Notificación de cibervictimización.



Perfil de conducta: evitativo-protección

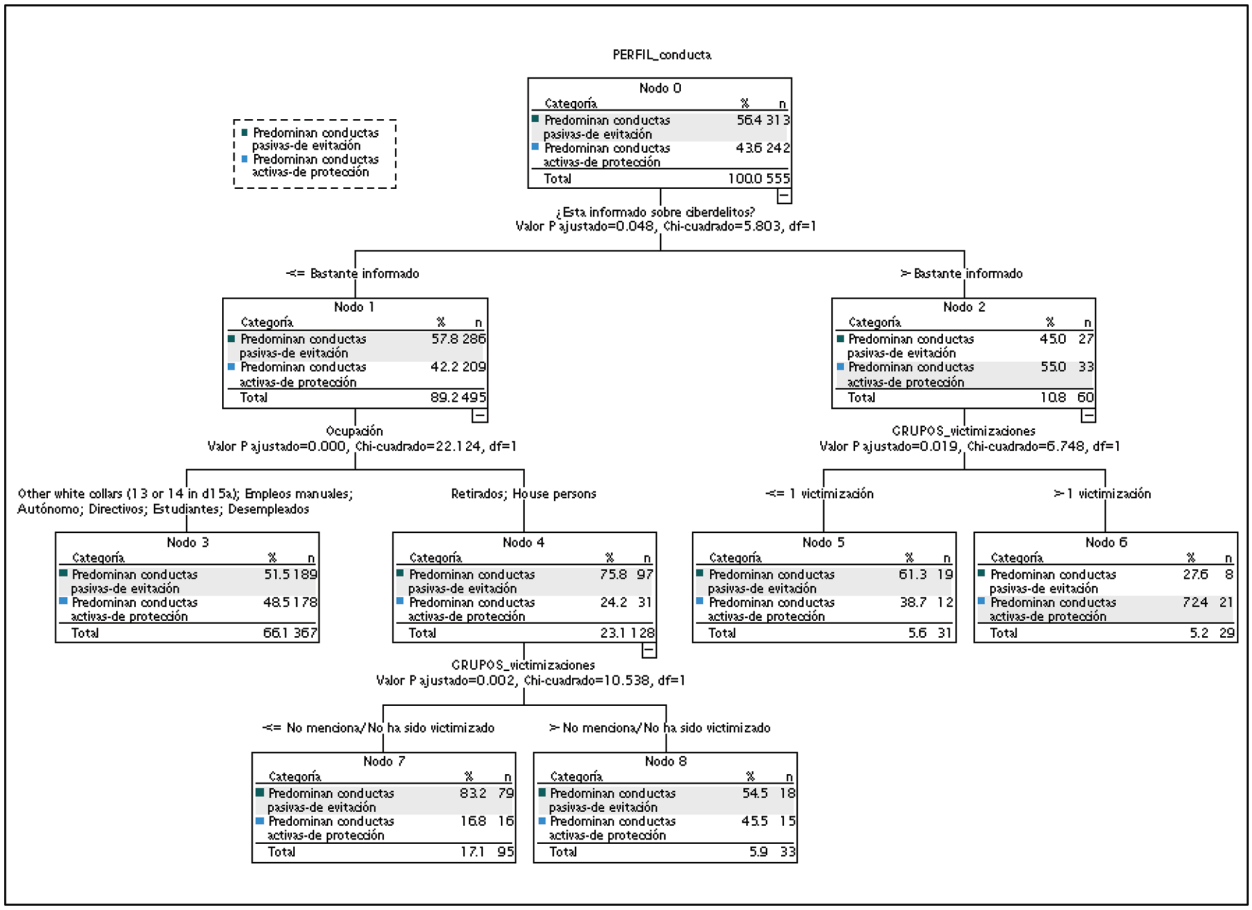
Para realizar este árbol de decisión seleccionamos los dos perfiles extremos de conducta ante preocupaciones al interaccionar con herramientas digitales: conductas pasivas (evitación, vertiente disfuncional) y conductas activas (protección, vertiente funcional). Como posibles variables predictoras en este modelo utilizamos la edad, estado civil, el género, la ocupación, el tipo de comunidad, conocimiento sobre ciberdelitos, victimizaciones previas y la inseguridad. Este modelo clasifica correctamente al 58.7% de la muestra (estimación de riesgo = .413). Tal como observamos en la Figura 2, el modelo incluyó las variables Estar informado sobre ciberdelitos, Victimización previa y Ocupación.

Los nodos determinantes para el perfil pasivo-evitación son los nodos 1, 4 y 7. Este perfil quedaría explicado por el modelo generado en un 83.2% por las variables correspondientes a no encontrarse muy informado sobre ciberdelitos, estar retirado o ser persona del hogar (por lo tanto, no activo laboralmente) y no haber sido victimizado previamente.

En cuanto al perfil activo-protección se asocia en mayor medida con los nodos 2 y 6, indicando el modelo que realizar conductas de protección ante la preocupación estaría asociada en un 72.4% por estar bastante informado sobre ciberdelitos y haber sufrido, al menos, una cibervictimización.

Figura 2

Perfil de conducta.



4. Discusión y conclusiones

Nuestro estudio se enfocó en abordar aspectos fundamentales relacionados con la incidencia de ciberdelitos, su notificación, la percepción de inseguridad y los patrones conductuales ante las preocupaciones en línea. Conviene señalar que este estudio incluye factores que pueden mostrar diferencias clave entre la victimización por delitos tradicionales y cibernéticos, un aspecto que ha recibido atención limitada en investigaciones previas. Mientras que el impacto directo de los delitos tradicionales ha sido extensamente documentado, los ciberdelitos presentan desafíos únicos que afectan a las víctimas de forma diferente, influenciando tanto su percepción de seguridad como sus respuestas comportamentales (Borwell et al., 2021). Respecto a la prevalencia de la cibervictimización, el 28.2% de nuestra muestra informó haber sido víctima de alguno de los ciberdelitos evaluados en los últimos 3 años, siendo los más frecuentes la infección de dispositivos mediante malware y los fraudes mediante correo electrónico o llamada. La baja tasa de conocimiento sobre métodos que permiten la notificación en línea de algún tipo de ciberdelito, reflejada por el escaso 13.8% de los participantes que tenían conocimiento de estos procedimientos, es un hallazgo inquietante. Este dato pone de manifiesto una significativa carencia en el conocimiento generalizado de los protocolos para informar de delitos digitales. Por otra parte, la baja tasa de notificación, mediante diferentes medios, de la victimización sufrida, revela una alta cifra negra en los datos oficiales,

que podría alcanzar el 80%, tal como señalan investigaciones previas realizadas en España, que sugieren que la tasa de notificación de delitos que se producen en la red es aproximadamente un 20% (Kemp et al., 2020). El análisis de las opciones de notificación reveló que la policía fue el canal menos empleado para informar de la mayoría de los delitos cibernéticos, con una preferencia más marcada por medios alternativos como sitios web o la comunicación directa con el proveedor de servicios. Únicamente en casos de acceso accidental a material de pornografía infantil y fraude bancario, hubo una mayor prevalencia de denuncia a las autoridades policiales, lo que podría estar relacionado con una percepción de mayor gravedad en estos delitos. Es evidente que la complejidad jurisdiccional que enfrentan las fuerzas policiales al investigar delitos cibernéticos que trascienden fronteras limita significativamente su capacidad para llevar a cabo acciones efectivas. Tal limitación puede llevar a las víctimas a considerar la inutilidad de la denuncia, dado que la persecución efectiva de los ciberdelincuentes se ve obstaculizada por barreras tanto geográficas como jurisdiccionales (Cross, 2020). En respuesta a esta problemática, es incuestionable la necesidad de establecer vías de acceso a la justicia que sean rápidas y efectivas para las víctimas de ciberdelitos. Estas vías deberían facilitar la notificación de los delitos y reducir la sensación de impunidad. Siguiendo esta línea, algunos países como el Reino Unido, Australia y Nueva Zelanda han implementado mecanismos centrales de denuncia que buscan simplificar el proceso y mejorar la experiencia de las víctimas al presentar informes. Además, estos sistemas permiten unificar y mejorar la recopilación de información por parte de las autoridades policiales (Cross, 2018), lo que facilita su posterior análisis y podría mejorar la eficacia en investigaciones transfronterizas, así como la creación de contramedidas asociadas a la problemática detectada.

En relación con la baja notificación de victimización, nuestro modelo de decisión tenía como objetivo detectar variables clave en la comunicación de este tipo de delitos. Los resultados indican que el conocimiento del procedimiento para realizar la notificación juega un papel fundamental en este proceso. Por tanto, la capacitación en seguridad cibernética podría aumentar la disposición de los usuarios a notificar incidentes, siendo necesarias estrategias que no solo informen sobre los riesgos cibernéticos, sino que también ofrezcan herramientas prácticas y habilidades concretas para abordar estas situaciones (Adorjan y Ricciardelli, 2019). Por tanto, se resalta como crucial la capacitación en seguridad cibernética del usuario, lo que requiere el establecimiento de programas de formación, y el apoyo de políticas asociadas, que no solo informen sobre los riesgos, sino que también proporcionen herramientas prácticas para manejar y prevenir ciberdelitos por parte del usuario.

En cuanto a la correlación positiva entre el miedo y la inseguridad con el conocimiento sobre ciberdelitos, métodos de denuncia y la victimización previa, puede dar lugar a dos interpretaciones potenciales. Inicialmente, los resultados parecen confirmar que es más probable que personas que han experimentado una cibervictimización previa informan de un mayor miedo a este tipo de delitos, resaltando la importancia de experiencias previas en la configuración del miedo y la percepción de seguridad futura. Este patrón sugiere que las intervenciones preventivas deben ser personalizadas para abordar no solo el conocimiento general sobre cibercrimen, sino también las experiencias específicas de las víctimas, lo que puede influir significativamente en la eficacia de las estrategias de prevención (Lee y Kim, 2023) Siguiendo con la posible interpretación de los resultados referidos a las correlaciones mencionadas, se podría sugerir que un mayor nivel de miedo e inseguridad motiva a las personas a buscar activamente información y conocimiento sobre cómo prevenir y enfrentarse a estos delitos. Esta idea respalda la noción de que la percepción de riesgo elevado impulsa a

las personas a adquirir herramientas para protegerse en el entorno digital. Por otro lado, también podría considerarse que el conocimiento adquirido sobre el funcionamiento de estos delitos genera un mayor miedo en el individuo. Es decir, a medida que las personas adquieren más información sobre los ciberdelitos y sus mecanismos, podrían desarrollar una mayor conciencia sobre los riesgos involucrados, lo que a su vez aumentaría su nivel de preocupación y percepción de amenaza. Sin embargo, determinar el orden causal entre el miedo, la inseguridad y el conocimiento en este contexto específico requiere de investigaciones adicionales y más detalladas. Además, estudios recientes sugieren que una mayor conciencia o percepción de vulnerabilidad no siempre se traduce en un comportamiento preventivo activo, subrayando la complejidad de las respuestas humanas ante el riesgo cibernético (De Kimpe et al., 2022). Por tanto, se necesitan estudios que aborden esta problemática en un contexto que permita discernir si el miedo e inseguridad conducen a la búsqueda de conocimiento o si es el conocimiento adquirido lo que amplifica el miedo y la inseguridad en relación con los ciberdelitos. Esta distinción en el orden causal sería fundamental para comprender mejor cómo estas variables se interrelacionan y cómo se podría intervenir de manera efectiva para promover una mayor conciencia y protección en el ámbito de la ciberseguridad. Además, dado que la investigación previa en este ámbito concreto es limitada, puede ser apropiado adoptar un enfoque mixto, combinando el análisis cuantitativo con investigaciones cualitativas, que permiten una narrativa no limitada por variables restringidas para el análisis en profundidad de conceptos (Wright y Bouffard, 2016). Observamos además una correlación negativa entre la edad y todas las variables examinadas, posiblemente influenciado por el menor uso de herramientas digitales entre grupos de mayor edad. Sin embargo, es crucial reconocer que esta tendencia puede estar cambiando, particularmente después de la pandemia por COVID-19, donde se ha observado un aumento significativo en el uso de tecnología por parte de personas mayores (INE, 2022). La correlación negativa entre las variables edad e inseguridad se encontraría en consonancia con un reciente estudio llevado a cabo en el año 2022 por Cook et al., que evidencia una relación curvilínea entre la edad y el temor a la ciberdelincuencia económica. Los resultados de este estudio muestran que el miedo aumenta de manera constante después de alcanzar la mayoría de edad, llegando a su punto culminante a los 45 años en hombres y a los 35 años en mujeres. A partir de estas edades, el temor comienza a disminuir, lo que sugiere que los adultos jóvenes y de mediana edad presentan una mayor inquietud en comparación con las personas de mayor edad en lo que respecta a la ciberdelincuencia económica. A nuestro juicio, este fenómeno podría explicarse, al menos en parte, por el hecho de que estos grupos demográficos son quienes hacen mayor uso de las herramientas en línea para realizar gestiones económicas, lo que les expone de manera más frecuente a los riesgos asociados. Por otro lado, algunas investigaciones recientes han sugerido que la falta de miedo al cibercrimen en personas mayores podría estar relacionada con su menor conocimiento sobre tecnologías de la información y la comunicación (TIC) y los distintos tipos de delitos en línea, los que les hace no ser consciente del riesgo que supone ciertas conductas en el entorno digital (Pino Juste et al., 2015).

En referencia a los patrones de conducta frente a las preocupaciones en línea, observamos un perfil pasivo-evitativo predominante, representado por conductas relacionadas con la limitación de uso de herramientas digitales ante la preocupación en línea, explicado en más del 80% por el modelo de decisión realizado. Este perfil se asoció con individuos que no estaban activos laboralmente, no habían sido victimizados previamente y carecían de conocimiento sobre ciberdelitos. Este resultado subraya, una vez más, la importancia de la información y la concienciación sobre

ciberdelitos para influir en las actitudes y comportamientos de las personas frente a las amenazas digitales. En consonancia con la Teoría de la Percepción de Vulnerabilidad propuesta por Hale en 1996, en el contexto físico, la percepción de incapacidad para enfrentar ciertas situaciones puede incrementar la sensación de vulnerabilidad percibida y, a su vez, adoptar comportamientos de evitación como una estrategia para reducir el posible riesgo de daño. Sin embargo, en nuestro estudio no se encontró que el nivel de inseguridad fuese determinante para adoptar un patrón de conducta u otro. Sería adecuado incluir en los estudios relacionados con la victimización en línea, no sólo variables referidas al miedo o a la tasa de notificación, sino evaluar también características como la gestión emocional, la autoestima, el apoyo social o la percepción de control, ya que estos factores podrían estar asociados no sólo a un mayor o menor riesgo de convertirse en víctima de ciberdelitos, como se ha comprobado en otros estudios (Alvarez-García et al., 2015; Helweg-Larsen et al., 2012; Wilsem, 2013; Zhang y Ye, 2022), sino también con la adopción de un perfil de conducta funcional o disfuncional ante las preocupaciones en línea.

Consideramos necesario destacar el uso indiscriminado de términos que podrían estar relacionados con miedo, preocupación e inseguridad tanto en los cuestionarios como en la bibliografía analizada, así como una fuerte correlación en los ítems que evaluaban estas cuestiones en nuestro análisis, lo que sugiere la necesidad de una revisión terminológica en estudios futuros para una mejor comprensión de estas experiencias. En este contexto, se destaca que los sentimientos/emociones como el miedo y los pensamientos/cogniciones como las percepciones de riesgo a menudo se entrelazan y confunden. En el uso de medidas subjetivas, como las referidas a preocupaciones y miedos uno de los mayores desafíos es que estos términos pueden presentar confusión incluso por parte de los sujetos que realizan el cuestionario, que tienden a proyectar su respuesta no hacía el sentimiento experimentado con anterioridad sino a la probabilidad de tenerlo en un futuro (Jackson y Gouseti, 2013). Por tanto, la falta de exactitud y unificación en los términos puede llevar a que la interpretación de los resultados no sea la adecuada.

Por último, nuestro estudio presenta ciertas limitaciones que deben considerarse al interpretar los resultados. En primer lugar, pese a ser una muestra representativa, la muestra se limitó exclusivamente a la población española, lo que puede restringir la generalización de los hallazgos a otros países. Sería relevante y esencial realizar investigaciones adicionales que abarquen múltiples países para comprender las diferencias y similitudes en variables analizadas. Parece que las características individuales son insuficientes para predecir el temor a la ciberdelincuencia por lo que sería adecuado tener en cuenta variables externas relacionadas con el entorno, así como los diferentes medios que permiten la notificación de delitos electrónicos y las leyes vigentes relacionadas con ciberdelitos en cada país. Puesto que el miedo al cibercrimen económico varía en función del país y el desarrollo tecnológico de este, no sólo por variables individuales y asociadas a las rutinas de los usuarios, podría suceder lo mismo con otro tipo de ciberdelitos (Cook et al., 2022). Es necesario replicar también estos estudios con datos post-COVID-19 ya que el aumento del trabajo desde casa y los cambios en los perfiles de uso de las herramientas digitales podrían haber cambiado el contexto y la relación entre las variables (Rennie Naidoo,2020). En esta misma línea, una investigación reciente que utilizó la misma base de datos de nuestro estudio identificó que la tasa de penetración de Internet es el único predictor que se asocia positivamente con la victimización por delitos cibernéticos (Lee & Wang, 2024). Este hallazgo subraya que, en países con una elevada integración de Internet, como España, la cibervictimización se configura como un problema

clave, por lo que es imperativo considerar la cibervictimización en el desarrollo de políticas públicas, estrategias de prevención y en la formulación de programas educativos que busquen mitigar los riesgos asociados al uso extensivo de tecnologías digitales. Adicionalmente, consideramos que es crucial destacar la importancia de los gestores de contenido como guardianes efectivos en el ciberespacio. Los gestores de contenido, al actuar como guardianes competentes, desempeñan un papel fundamental no solo supervisando y controlando las actividades dentro de sus plataformas, sino también implementando estrategias preventivas que reduzcan la probabilidad de incidentes delictivos. Esta estrategia es coherente con la teoría de las actividades cotidianas, la cual sostiene que la presencia de un guardián efectivo reduce las oportunidades para la comisión de delitos (Cohen y Felson, 1979; Miró y Johnson, 2018), en este caso en el ciberespacio. De la misma forma, esta problemática requiere una atención particular en la investigación académica y en las iniciativas de cooperación internacional, con el fin de diseñar respuestas efectivas que protejan a los usuarios en el entorno digital. Además, sería recomendable ampliar el rango de ciberdelitos estudiados, agrupándonos en categorías preestablecidas y siguiendo un marco común, ya que se ha observado que la relación entre la victimización por ciberdelitos y el miedo puede variar según el tipo de delito y su impacto percibido, por lo que distintos tipos de ciberdelitos deberían ser considerados de forma individual (Virtanen, 2017). Pese a ello, este estudio ofrece implicaciones relevantes tanto para la sociedad como para la comunidad científica en el campo de la ciberseguridad. En términos sociales, la investigación subraya la urgente necesidad de implementar contramedidas efectivas y accesibles en seguridad cibernética para el público en general, que aumenten tanto el conocimiento sobre los riesgos digitales como la capacitación de los individuos para protegerse de ellos y notificar en caso de que detecten algún delito en línea o sean victimizados. Además, abre la vía a futuras investigaciones que permitan explorar con detalle las variables psicológicas que influyen en los diferentes patrones de conducta adoptados en la red. Asimismo, resalta la necesidad de mejorar las metodologías de investigación en este campo, considerando la confusión en términos y la subjetividad en la interpretación como aspectos cruciales a atender para garantizar la precisión y validez de los resultados.

Referencias

Adorjan, M., & Ricciardelli, R. (2019). Student perspectives towards school responses to cyber-risk and safety: the presumption of the prudent digital citizen. *Learning, Media and Technology*, 44(4), 430-442. https://doi.org/10.1080/17439884.2019.1583671

Álvarez-García, D., Pérez, J. C. N., González, A. D., & Pérez, C. R. (2015). Risk factors associated with cybervictimization in adolescence. *International Journal of clinical and health psychology*, 15(3), 226-235. https://doi.org/10.1016/j.ijchp.2015.03.002

Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 1-4. https://www.doi.org/10.52306/02020119KDHZ8339

Berlanga Silvente, V., Rubio Hurtado, M. J., Vilà Baños, R. (2013). Cómo aplicar árboles De decisión en SPSS. REIRE, *Revista d'Innovació i Recerca en Educació*, 6 (1), 65-79.Accesible en: http://www.ub.edu/ice/reire.htm

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. Journal of Digital Social Research, 3(3), 85-110. https://doi.org/10.33621/jdsr.v3i3.66

Brands, Jelle & van Doorn, Janne. (2021). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*. 127. 107082. https://doi.org/10.1016/j.chb.2021.107082

Button, C., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Abingdon: Routledge. https://doi.org/10.4324/9781315679877

Button, M., Lewis, C. & Tapley, J. (2009). *A better deal for fraud victims: research into victims' needs and experiences*.

Caneppele, S. & Aebi, M. (2017). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing*. Online First. https://doi.org/10.1093/police/pax055

Castro Toledo, F. (2018). Miedo al crimen en la era tecnológica: nuevos horizontes metodológicos, nuevo alcance ontológico. https://doi.org/10.13140/RG.2.2.33071.28327

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Comisión Europea. (2021). Top cyber threats in the EU. Recuperado de https://www.consilium.europa.eu/en/infographics/

Cook, S., Giommoni, L., Pareja, N., Levi, M. & Williams, M. (2022). Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory. *The British Journal of Criminology*. Volume 63, Issue 2, March 2023, Pages 384–406, https://doi.org/10.1093/bjc/azac021

Cross C, Smith R & Richards K 2014. Challenges of responding to online fraud victimisation in Australia. *Trends & issues in crime and criminal justice* no. 474. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi474

Cross, Cassandra. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*. 55. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 358–375. https://doi.org/10.1177/1748895819835910

Danieli, N.E. & Paz-García, A.P. (2020). Public opinion on security: psycho-social analysis dimensions around fear of crime and its media treatment. *Comunicación y sociedad*, 17, e7586. https://doi.org/10.32870/cys.v2020.7586

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

European Commission and European Parliament, Brussels (2021). *Eurobarometer 92.2* (2019). GESIS Data Archive, Cologne. ZA7580 Data file Version 1.0.0, https://doi.org/10.4232/1.13657

Eurostat (2021). *Digital economy and society statistics - households and individuals*. Recuperado de https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Golladay K. y Holtfreter K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes, *Victims & Offenders*, 12(5), 741–760. https://doi.org/10.1080/15564886.2016.1177766

Hale, C. (1996). Fear of Crime: A Review of the Literature. *International Review of Victimology*, 4, 79-150.

Helweg-Larsen, K., Schütt, N., & Larsen, H. B. (2012). Predictors and protective factors for adolescent internet victimization: Results from a 2008 nationwide Danish youth survey. *Acta Paediatrica, 101*(5), 533–539. https://doi.org/10.1111/j.1651-2227.2011.02587.x

Hummelsheim, D., Hirtenlehner, H., Jackson, J., & Oberwittler, D. (2011). Social Insecurities and Fear of Crime: A Cross-National Study on the Impact of Welfare State Policies on Crime-related Anxieties. *European Sociological Review*, 27, 327-345.

Ho, M. H., Ko, P. R., & Mazerolle, P. L. (2022). Situational Crime Prevention (SCP) Techniques to Prevent and Control Cybercrimes: A Focused Systematic Review. Computers & Security, 102611. https://doi.org/10.1016/j.cose.2022.102611

Instituto Nacional de Estadística (INE) (2021). *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares*. Recuperado de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735573113

Interpol (2020). *Cybercrime: Covid-19 impact*. Recuperado 15 septiembre de 2023 de https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Jackson, J., & Gouseti, I. (2013). Fear of crime: An entry to the Encyclopedia of theoretical criminology. In J. Mitchell Miller (Ed.), *Encyclopedia of theoretical criminology*. Oxford: Wiley-Blackwell (in press). URL (accessed 7 April 2021): SSRN: https://ssrn.com/abstract=2118663

Jackson, J., and Gray, E. (2010). Functional fear and public insecurities about crime. *British Journal of Criminology*, 50, 1-22. https://doi.org/10.1093/bjc/azp059

Jewkes, Y., & Yar, M. (2011). *Handbook of internet crime*. Abingdon: Routledge. https://doi.org/10.4324/9781843929338

Kemp, S., Miró Llinares y F., Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: evidence from Spain. *European Journal on Criminal Policy and Research*, vol. 26, núm. 4. https://doi.org/10.1007/s10610-020-09439-2

Lee, C. S., & Kim, J. H. (2023). How victims perceive fear of cybercrime: importance of informed risk. Criminal Justice Studies, 36(3), 206–227. https://doi.org/10.1080/1478601X.2023.2254099

Lee, C. S., & Wang, Y. (2024). Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis. Crime & Delinquency, 70(4), 1196-1223. https://doi.org/10.1177/00111287221118880

Mayhew, P., & Dijk, J. (2012). Assessing crime through international victimization surveys. In D. Gadd, S. Karstedt, & S. F. Messner (Eds.), *The SAGE handbook of criminological research methods* (pp. 253–267). London: SAGE Publications Ltd.. https://doi.org/10.4135/9781446268285

Ministerio de Interior (2023). *Informe sobre cibercriminalidad.*

Miró-Llinares, F. (2012), E*l cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons

Miró Llinares, F. (2021). «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos». IDP. *Revista de Internet, Derecho y Política*, n.º 32, https://doi.org/10.7238/idp.v0i32.373815

Miró, F., & Johnson, S.D. (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. En G.J.N. Bruinsma & S.D. Johnson (Eds.), The Oxford Handbook of Environmental Criminology. Oxford University Press.

Pino Juste, M., Soto Carballo, J., and Rodríguez López, B. (2015). Las personas mayores y las TIC. Un compromiso para reducir la brecha digital. Pedagogía social. *Revista Interuniversitaria*, núm. 26, 2015, pp. 337-359 Sociedad Iberoamericana de Pedagogía Social Sevilla, España

Reid, I. D., Appleby-Arnold, S., Brockdorff, N., Jakovljev, I., & Zdravković, S. (2020). Developing a model of perceptions of security and insecurity in the context of crime. Psychiatry, *Psychology and Law*, 27(4), 620–636. https://doi.org/10.1080/13218719.2020.1742235

Rennie Naidoo (2020) A multi-level influence model of COVID-19 themed cybercrime, *European Journal of Information Systems*, 29:3, 306-321, https://doi.org/10.1080/0960085X.2020.1771222

Schreurs, K., Quan-Haase, A., & Martin, K. (2017). Problematizing the digital literacy paradox in the context of older adults' ICT use: Aging, media discourse, and self-determination. *Canadian Journal of Communication*, 42(2). https://doi.org/10.22230/cjc.2017v42n2a3130

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: is cyberspace hiding a crime wave? *Justice Quarterly*, 33(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Valera, S., and Guàrdia, J. (2014). Perceived insecurity and fear of crime in a city with low crime rates. *Journal of Environmental Psychology*. 38. https://doi.org/10.1016/j.jenvp.2014.02.002

Van Dijk, J. A. (2005). *The deepening divide: Inequality in the information society.* Sage Publications. https://doi.org/10.4135/9781452229812

Virtanen, S. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*. 24. 1-16. https://doi.org/10.1080/13218719.2017.1315785

Wall, D. S. (2017). Towards a conceptualisation of cloud (cyber) crime. *Human aspects of information security, privacy and trust*. HAS 2017. Cham: Springer. https://doi-org.ezproxy.leidenuniv.nl/10.1007/978-3-319-58460-7_37

Wilsem, J. V. (2013). Hacking and harassment: Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437-453. https://doi.org/10.1177/1043986213507402

Wright, K. A., and Bouffard, L. A. (2016). Capturing crime: The qualitative analysis of individual cases for advancing criminological knowledge. *International journal of offender therapy and comparative criminology*, 60(2), 123-145. https://doi.org/10.1177/0306624X145493

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications.

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