Universidad Miguel Hernández de Elche

Programa de Doctorado en Criminología

Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención

Tesis doctoral presentada por

Nieves Erades Pérez

Dirigida por la Profesora Dr. Dª. Esther Sitges Maciá

Codirigida por el Profesor Dr. D. Steven Kemp

-2024-

La presente Tesis Doctoral titulada *Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención* se presenta bajo la modalidad de tesis convencional con los siguientes indicios de calidad:

- Kemp, S., & Erades Pérez, N. (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact. *International journal of environmental research and public health*, 20(7), 5404. https://doi.org/10.3390/ijerph20075404

- Erades, N., Sitges-Macia, E. & Segura-Cuenca, M.C (2022). Uso de las TIC y cibervictimización de personas adultas mayores: un estudio exploratorio. *Revista General de Derecho Penal*, 38.

La Dra. Dña. *Esther Sitges Maciá*, directora, y el Dr. D. *"Steven Kemp"*, codirector de la tesis doctoral titulada **"Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención"**

INFORMAN:

Que Dña. *Nieves Erades Pérez* ha realizado bajo nuestra supervisión el trabajo titulado **"Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención"** conforme a los términos y condiciones definidos en su Plan de Investigación y de acuerdo al Código de Buenas Prácticas de la Universidad Miguel Hernández de Elche, cumpliendo los objetivos previstos de forma satisfactoria para su defensa pública como tesis doctoral.

Lo que firmamos para los efectos oportunos, en Elche a 26 de julio de 2024

Directora de la tesis	Codirector de la tesis
Dra. Dña. *Esther Sitges Maciá*	Dr. D. Steven Kemp

El Dr. D. Fernando Miró Llinares, Coordinador del Programa de Doctorado en Criminología

INFORMA:

Que Dña. *Nieves Erades Pérez* ha realizado bajo la supervisión de nuestro Programa de Doctorado el trabajo titulado "Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención." conforme a los términos y condiciones definidos en su Plan de Investigación y de acuerdo al Código de Buenas Prácticas de la Universidad Miguel Hernández de Elche, cumpliendo los objetivos previstos de forma satisfactoria para su defensa pública como tesis doctoral.

Lo que firmo para los efectos oportunos, en Elche a 26 de julio de 2024

Prof. Dr. D. Fernando Miró Linares

Coordinador del Programa de Doctorado en Criminología

ÍNDICE DE CONTENIDOS

Listado de Tablas

Resumen

El envejecimiento poblacional es un fenómeno global que está transformando la estructura demográfica de las sociedades contemporáneas, imponiendo desafíos significativos en múltiples sectores. Este hecho, sumado a una gran digitalización en múltiples áreas de la vida cotidiana supone un verdadero reto para proporcionar un acceso inclusivo y seguro a todos los sectores de la población.

En este contexto, la tesis doctoral titulada *Exploración de la adaptación y victimización digital en personas adultas mayores: riesgos y estrategias de prevención*, aborda la adaptación de las personas adultas mayores a las tecnologías digitales y los riesgos asociados a la victimización en línea en este grupo etario, con un enfoque focalizado en la victimización por fraude en línea.

La investigación se sustenta en una metodología mixta, combinando enfoques cuantitativos y cualitativos para ofrecer una comprensión profunda de cómo las personas mayores interactúan con las Tecnologías de la Información y la Comunicación y cómo estas interacciones pueden resultar en una situación de vulnerabilidad digital.

Los resultados de la investigación señalan que, a pesar de una creciente adaptación tecnológica por parte de este grupo, las personas adultas mayores siguen siendo un grupo proclive a encontrarse en situaciones de vulnerabilidad en relación con la digitalización, debido a factores como la falta de alfabetización digital o la brecha digital, entre otros.

En términos de contribuciones prácticas, esta tesis doctoral propone un conjunto de recomendaciones para mitigar estos riesgos. Se sugiere la implementación de programas de educación digital específicos para personas adultas mayores, diseñados para fortalecer sus competencias digitales y concienciarles sobre las estrategias de prevención de fraudes y otros ciberdelitos. Además, se aboga por políticas públicas que fomenten la inclusión digital segura y efectiva de este colectivo, subrayando la importancia de un enfoque multidisciplinar que involucre a profesionales de diversas áreas.

Palabras clave: Adaptación; Cibervictimización; Prevención; Personas adultas mayores; TIC

Abstract

Population ageing is a global phenomenon transforming the demographic structure of contemporary societies, posing significant challenges across multiple sectors. This reality, coupled with extensive digitalisation in various aspects of daily life, presents a substantial challenge in providing inclusive and secure access for all population sectors.

In this context, the doctoral thesis titled "Exploration of Digital Adaptation and Victimisation in Older Adults: Risks and Prevention Strategies" addresses the adaptation of older adults to digital technologies and the associated risks of online victimisation within this age group, with a particular focus on online fraud victimisation.

The research is grounded in a mixed-methods approach, combining quantitative and qualitative methodologies to offer a deep understanding of how older adults interact with Information and Communication Technologies (ICT) and how these interactions can lead to digital vulnerability.

The research findings indicate that despite increasing technological adaptation within this group, older adults remain prone to vulnerability in the context of digitalisation due to factors such as digital illiteracy or the digital divide, among others.

In terms of practical contributions, this doctoral thesis proposes a set of recommendations to mitigate these risks. It suggests the implementation of specific digital education programmes for older adults, designed to enhance their digital competencies and raise awareness of fraud prevention strategies and other cybercrimes. Additionally, it advocates for public policies that promote the safe and effective digital inclusion of this group, emphasising the importance of a multidisciplinary approach involving professionals from various fields.

Keywords: Adaptation; Cybervictimisation; Prevention; Older adults; ICT

Resum

L'envelliment poblacional és un fenomen global que està transformant l'estructura demogràfica de les societats contemporànies, imposant desafiaments significatius en múltiples sectors. Este fet, sumat a una gran digitalització en múltiples àrees de la vida quotidiana suposa un verdader repte per a proporcionar un accés inclusiu i segur a tots els sectors de la població.

En este context, la tesi doctoral titulada Exploració de l'adaptació i victimització digital en persones adultes majors: riscos i estratègies de prevenció, aborda l'adaptació de les persones adultes majors a les tecnologies digitals i els riscos associats a la victimització en línia en este grup d'edat, amb un enfocament focalitzat en la victimització per frau en línia.

La investigació se sustenta en una metodologia mixta, combinant enfocaments quantitatius i qualitatius per a oferir una comprensió profunda de com les persones majors interactuen amb les Tecnologies de la Informació i la Comunicació i com estes interaccions poden resultar en una situació de vulnerabilitat digital.

Els resultats de la investigació assenyalen que, malgrat una creixent adaptació tecnològica per part d'este grup, les persones adultes majors continuen sent un grup procliu a trobar-se en situacions de vulnerabilitat en relació amb la digitalització, a causa de factors com la falta d'alfabetització digital o la bretxa digital, entre altres.

En termes de contribucions pràctiques, esta tesi doctoral proposa un conjunt de recomanacions per a mitigar estos riscos. Se suggerix la implementació de programes d'educació digital específics per a persones adultes majors, dissenyats per a enfortir les seues competències digitals i conscienciar-los sobre les estratègies de prevenció de fraus i altres ciberdelictes. A més, s'advoca per polítiques públiques que fomenten la inclusió digital segura i efectiva d'este col·lectiu, subratllant la importància d'un enfocament multidisciplinari que involucre a professionals de diverses àrees.

Paraules clau: Adaptació; Cibervictimización; Prevenció; Persones adultes majors; TIC

INTRODUCCIÓN

El fenómeno del envejecimiento poblacional se asienta como una constante en las proyecciones demográficas contemporáneas. Según datos de las Naciones Unidas, se espera que la población mundial de personas mayores de 60 años casi triplique su número para el año 2050, alcanzando los 1.500 millones de personas y superando a los adolescentes y jóvenes de 15 a 24 años (Naciones Unidas, 2019). Esta tendencia, eminentemente global, se deriva de la interacción de dos variables fundamentales: una reducción sustancial de las tasas de fertilidad y un incremento notable en la esperanza de vida. El resultado es una transformación estructural de la pirámide poblacional, donde la proporción de individuos que superan los 65 años de edad se amplifica de manera significativa. Además, esta tendencia mundial se observa todavía de forma más acusada en Europa, con una representación en torno al 20% de la población total (Eurostat, 2020). Es evidente que esta transición demográfica impone repensar de forma crítica y estratégica en múltiples sectores sociales y económicos, además de la necesidad de promover un enfoque de envejecimiento activo y saludable, incentivando la participación continua de los adultos mayores en una sociedad altamente cambiante, para mitigar los impactos negativos que se deriven de situaciones de vulnerabilidad, promoviendo una mayor calidad de vida.

Nuestra sociedad en los últimos años ha experimentado una rápida digitalización, con un aumento en el uso de dispositivos electrónicos, el acceso a Internet de alta velocidad y las tecnologías digitales, encontrándose estos omnipresentes en nuestra vida cotidiana. Según las estimaciones de la Unión Internacional de Telecomunicaciones, aproximadamente 5.400 millones de personas (67% de la población mundial) utilizarán Internet a lo largo del año 2023 (UIT, 2023). España no es ajena a este fenómeno de la digitalización de la sociedad; según el Instituto Nacional de Estadística, en 2022, el 96,1% de los hogares españoles tenía acceso a Internet (INE, 2022). Esta revolución tecnológica facilita un flujo ininterrumpido de información, optimiza los procesos operativos y cataliza la innovación en diversos ámbitos, desde el sector empresarial hasta la gestión pública. Sin embargo, su penetración y difusión heterogénea también genera desafíos

considerables en términos de accesibilidad y seguridad. La alfabetización digital se posiciona como una competencia esencial en este entorno tecnológicamente saturado, sin embargo, se observa una disparidad significativa en su adquisición y dominio, particularmente entre la población adulta mayor, siendo una de las variables determinantes que limitan su capacidad para interactuar eficientemente con tecnologías emergentes (Zhang, 2023).

Ligado a este aumento de la digitalización, en los últimos años, el cibercrimen, definido como cualquier conducta criminal que se lleve a cabo en el ciberespacio, aprovechando sus características únicas (Miró-Llinares, 2012), ha experimentado un crecimiento exponencial paralelo al avance digital, incrementado todavía más durante la pandemia por COVID-19 en el año 2020 (Interpol, 2020). Las personas adultas mayores emergen como un segmento poblacional que puede ser particularmente vulnerable a esta forma de criminalidad, dada su relativa inexperiencia y falta de familiaridad con las prácticas de seguridad en línea (Czaja et al., 2006; James et al., 2014), además de la presencia de algunos factores psicológicos y personales que pueden ser relevantes en este contexto (Whitty, 2018), como se analizará a largo de este trabajo. Por tanto, los delitos cometidos en el contexto digital, como fraudes, estafas, phishing y otras modalidades de cibercrimen representan amenazas tangibles que se ciernen también sobre la población de más edad, pudiendo comprometer su seguridad financiera y personal.

Indudablemente, nos encontramos en una encrucijada histórica donde el envejecimiento demográfico y la proliferación digital se entrelazan de manera compleja y suponen un reto, en la que la investigación empírica se erige como un pilar fundamental para abordar estos desafíos y desarrollar estrategias efectivas que permitan la inclusión digital efectiva y segura de este grupo poblacional.

Por lo expuesto anteriormente, esta tesis doctoral se centra en la interacción de las personas adultas mayores con el entorno digital, explorando no solo los patrones de uso sino también las posibles susceptibilidades a la cibervictimización. El propósito primordial de este estudio es elucidar los mecanismos mediante los cuales las personas de este grupo etario se adaptan a la esfera digital, identificando simultáneamente vulnerabilidades específicas y estrategias de mitigación efectivas contra el fraude y otros tipos de crímenes cibernéticos. A través de una

metodología híbrida, que combina un enfoque cuantitativo y cualitativo, se aspira a aportar una base de conocimiento que sirva de fundamento para el desarrollo de líneas futuras de investigación, políticas públicas asociadas y programas preventivos orientados a esta demografía.

La estructura de esta tesis se articula en dos partes principales. En primer lugar, la Parte I, Contexto y Marco Teórico, sienta las bases conceptuales y revisa la literatura pertinente sobre el envejecimiento, la digitalización y el cibercrimen. El Capítulo 1 introduce el contexto de la digitalización global, el envejecimiento demográfico y la intersección de ambas variables, ofreciendo una visión panorámica de los desafíos y beneficios asociados en este contexto. En el Capítulo 2, se profundiza en el fenómeno del cibercrimen, con un énfasis particular en cómo afecta este grupo etario. El Capítulo 3 aborda las teorías criminológicas que pueden aplicarse a la cibervictimización, en este caso con especial énfasis en las teorías ambientales. Por último, en el Capítulo 4 se delinean las estrategias de prevención e intervención necesarias para mitigar la cibervictimización en personas adultas mayores.

En segundo lugar, la Parte II, Aproximación Empírica, presenta la investigación empírica llevada a cabo para evaluar cómo las personas adultas mayores se adaptan y son afectadas por la digitalización y la cibervictimización. El capítulo 5 presenta un estudio cuantitativo en el que se explora el uso de internet y estrategias de afrontamiento en personas adultas mayores. En los Capítulos 6 y 7, se profundiza en el uso de las herramientas digitales y la cibervictimización en las personas adultas mayores. El sexto capítulo se centra en evaluar cómo las interacciones digitales pueden exponer a las personas mayores a riesgos específicos en línea y qué estrategias emplean para mitigar tales riesgos, mediante una metodología cuantitativa. El séptimo capítulo analiza las dinámicas emocionales y adaptativas frente a la digitalización a través de una metodología cualitativa, incluyendo la exploración del miedo al ciberdelito y examinando las respuestas emocionales y comportamentales que la creciente digitalización evoca en este grupo poblacional. Finalmente, en el Capítulo 8 se analizan las posibles consecuencias de la cibervictimización en este grupo etario.

Por último, se esbozan conclusiones generales que buscan sintetizar las contribuciones teóricas y empíricas desarrolladas a lo largo del estudio. Así mismo, se delinean líneas futuras de investigación que podrían explorar más a fondo las dinámicas de cibervictimización y adaptación tecnológica en diferentes contextos.

PARTE I. CONTEXTO Y MARCO TEÓRICO

CAPÍTULO 1. DIGITALIZACIÓN Y PERSONAS ADULTAS MAYORES

1.1 UNA SOCIEDAD ALTAMENTE DIGITALIZADA

El ciberespacio se ha convertido en una realidad sólidamente afianzada en la época moderna, siendo un entorno digital interconectado a través de la compleja infraestructura de Internet. Esta nueva realidad no sólo ha provocado una metamorfosis en la manera en la cual accedemos a la información, sino que también ha reformulado de raíz nuestras relaciones, economía y, de forma más holística, la sociedad en su totalidad. El concepto de ciberespacio engloba un ámbito virtual que se extiende más allá de nuestras pantallas y actualmente está presente en prácticamente todos los aspectos de la vida cotidiana. Su origen se ubica en las décadas de 1960 y 1970, cuando ilustres visionarios en el campo tecnológico, como J.C.R. Licklider y Leonard Kleinrock, comenzaron a concebir la idea de una red global de comunicaciones. Estos pioneros establecieron los fundamentos para ARPANET, precursor del internet actual. ARPANET, que hizo su debut en 1969, entrelazó a cuatro instituciones académicas en los Estados Unidos, y marcó el hito inaugural de la creación de un ciberespacio global. Los protocolos primordiales, a saber, el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), sentaron las bases técnicas para la comunicación a larga distancia entre sistemas informáticos.

Sin embargo, esto fue tan solo el comienzo, ya que, desde entonces, la evolución del ciberespacio se erige como una auténtica revolución que progresa al unísono con el avance tecnológico y los cambios sociales. La eclosión de la World Wide Web a principios de la década de 90 del siglo pasado, representó un hito sumamente significativo, al hacer visibles las posibilidades de la conectividad global y la democratización del acceso a la información, revolucionando radicalmente el modo en el que las personas obtienen acceso a la información y se comunican. Durante la década de los 90 se presenció el nacimiento de navegadores web, como el ya desaparecido Netscape Navigator, que simplificaron la navegación en Internet y la

hicieron accesible para el público en general. La web se transformó en un espacio propicio para la compartición de datos, el intercambio de conocimientos y la construcción de redes sociales. En este contexto, la irrupción del correo electrónico transformó la comunicación, permitiendo a los individuos enviar mensajes de forma instantánea salvando extensas distancias, mientras que los motores de búsqueda, como Google, propiciaron el acceso a la información de una forma sin precedentes. Por supuesto, esta "ciber revolución" también tuvo un impacto en el ámbito económico. La creación de plataformas de comercio electrónico y venta en línea permitió a las empresas alcanzar audiencias globales, algo inimaginable sin esta estructura. Adicionalmente, las redes sociales, tales como Facebook y Twitter, han producido cambios en la forma en que las personas se conectan, expresan sus opiniones y acceden a información de actualidad. También los movimientos sociales e ideologías políticas han encontrado un nuevo contexto disponible y se ha empleado el ciberespacio para comunicar pensamientos e ideales y, en esta misma línea, la cultura popular se ha visto moldeada por medio de memes, videos virales o comunidades en línea lo que ha llevado a que podamos afirmar que el ciberespacio ha desencadenado una verdadera revolución social al mismo nivel que otras grandes revoluciones que ha vivido la humanidad como la Revolución Industrial a mediados del siglo XVIII.

Esta creciente digitalización de la sociedad, a pesar de los innumerables beneficios y avances que conlleva, también suscita riesgos y desafíos que influyen en numerosas áreas de nuestro día a día. Uno de los desafíos más apremiantes lo constituye la ciberseguridad. A medida que organizaciones y particulares somos cada vez más dependientes de la tecnología digital, aumenta nuestra situación de vulnerabilidad al vernos expuestos a ataques cibernéticos, cada día más sofisticados con ciberdelincuentes que planean la sustracción de datos personales y financieros, hasta ataques de gran envergadura contra infraestructuras críticas, como los sistemas de energía y salud. Estos hechos vienen avalados con los datos que revelan que las tasas de delincuencia en línea se han incrementado en los últimos años, en mayor medida que los delitos convencionales, perpetrados sin asistencia tecnológica (Buil-Gil et al., 2021; Caneppele & Aebi, 2019; Miró-Llinares, 2012;2013).

La elevada digitalización implica un aumento de la exposición y también una pérdida de privacidad lo que lleva a que se recopile un volumen considerable de datos personales con fines diversos, incluyendo su venta. Asimismo, la prolífica difusión mediante las redes sociales y la recolección masiva de información han avivado inquietudes en torno a la manipulación de la opinión pública y la erosión de la privacidad en línea. También, la digitalización ha creado nuevas formas de desigualdad ya que no todas las personas gozan de un acceso equitativo a las tecnologías digitales, lo cual puede agravar las diferencias económicas y sociales que ya existen. En los últimos años, la automatización y la inteligencia artificial también plantean desafíos a medida en que desplazan empleos convencionales y suscitan cuestiones éticas relativas a la toma de decisiones autónoma. Dada la importancia de este aspecto, tanto en este capítulo como en los siguientes procederemos a examinar minuciosamente estas dimensiones, con el propósito de comprender los desafíos que plantea este contexto altamente digitalizado y su implicación en personas adultas mayores.

1.2 PERSONAS ADULTAS MAYORES EN LA ACTUALIDAD

1.2.1 La gerontología: el estudio del envejecimiento como parte de una ciencia multidisciplinar

La Gerontología, entendida como el estudio científico de los procesos de envejecimiento y las particularidades de las personas mayores (Birren, 1961), es un campo multidisciplinar que ha evolucionado a lo largo de los años, adaptándose a las cambiantes realidades demográficas y sociales. El envejecimiento es una experiencia universal, inherente al ser humano, que ha intrigado a filósofos, médicos y sociólogos a lo largo de los siglos. En la antigua Roma, por ejemplo, Marco Tulio Cicerón, en su libro “De Senectute”, proporcionó una visión exhaustiva de la vejez, utilizando a Catón el Viejo como un ejemplo de envejecimiento activo y sabiduría acumulada a lo largo de los años. En esta obra, Cicerón no solo aborda aspectos físicos y biológicos del envejecimiento, sino que también se sumerge en discusiones filosóficas y éticas, explorando cómo la vejez puede ser una etapa de reflexión, entendimiento y aceptación de la mortalidad, siempre y cuando se

mantenga un estilo de vida equilibrado y una mente activa. Al igual que Hipócrates, que hizo énfasis en la dieta y el ambiente, Cicerón también realza la importancia de mantener un espíritu fuerte y una actividad cognitiva para enfrentar los desafíos que trae consigo el avanzar de la edad.

Pese a los estudios previos centrados en la vejez, el establecimiento de la Gerontología como disciplina científica se suele establecer a partir de la creación de la Asociación Gerontológica Americana en 1945. Esta organización, ahora conocida como Asociación Gerontológica de América (AGA), desempeñó un papel fundamental en la promoción de la investigación y el desarrollo de programas académicos en esta área, observándose una expansión y diversificación considerables en sus enfoques y metodologías. El surgimiento de una variedad de teorías y paradigmas han enriquecido el análisis y la comprensión del envejecimiento. La integración de distintas perspectivas y disciplinas ha permitido que la gerontología avance hacia una comprensión más profunda y matizada de los procesos asociados con el envejecimiento, consolidándose como una disciplina científica robusta y multifacética.

Desde una perspectiva biológica, la gerontología ha profundizado en el estudio de los mecanismos y procesos que subyacen al envejecimiento. Se ha otorgado prioridad a la exploración detallada de los procesos celulares y moleculares que participan en el desarrollo de diversas patologías potencialmente asociadas con el envejecimiento, una estrategia que ha facilitado la orientación de intervenciones prácticas hacia la optimización de la salud y la extensión de la longevidad. La transición evolutiva de estas perspectivas se manifiesta claramente al considerar la progresión histórica de las teorías científicas en este dominio. Originalmente, predominaba una concepción más negativa de la vejez, percibida predominantemente en términos de declive y deterioro. Sin embargo, esta visión ha sido progresivamente reemplazada por un paradigma más esperanzador y constructivo. Este cambio paradigmático refleja un enfoque renovado que enfatiza la posibilidad de mejorar la calidad de vida durante el envejecimiento. Un ejemplo ilustrativo de esta transición en el campo gerontológico puede observarse al analizar y comparar la "Teoría de los Radicales Libres" con la reciente propuesta, en esta misma línea, del gerontólogo biomédico Aubrey de Grey. La "Teoría de los

Radicales Libres", articulada inicialmente por Denham Harman en 1956, representa una de las premisas pioneras en el campo biológico de la gerontología donde se afirmaba que el envejecimiento es un proceso intrínsecamente mediado por los efectos destructivos de los radicales libres, moléculas inestables que inducen daño celular y molecular acumulativo a lo largo del tiempo. Aubrey de Grey, en su obra "Ending Aging" publicada en 2007, presentó la premisa, tan innovadora como controvertida, de que el envejecimiento puede ser efectivamente combatido a través de intervenciones terapéuticas dirigidas a la reparación y mantenimiento del daño molecular y celular acumulado, considerando la vejez una enfermedad y por tanto con posibilidad de “cura”. Este nuevo concepto representa un avance significativo en el campo gerontológico en su vertiente más biológica redirigiendo la atención hacia el desarrollo de terapias regenerativas y promueve una visión de envejecimiento saludable centrado en los aspectos más fisiológicos.

En el ámbito de la psicología gerontológica, el objeto de estudio ha recaído principalmente sobre los cambios cognitivos y emocionales que se manifiestan durante el proceso de envejecimiento. Un marco teórico notable dentro de esta disciplina fue propuesto por Erik Erikson en 1959, quien desarrolló una teoría del desarrollo psicosocial que identificaba etapas específicas y crisis asociadas a lo largo del ciclo vital. Erikson propuso ocho etapas del desarrollo humano, cada una caracterizada por una crisis o conflicto psicosocial, ocurriendo la última etapa, denominada "Integridad vs. Desesperación", durante la vejez. Erikson sugiere que las personas en esta etapa reflexionan sobre sus vidas, evaluando y analizando sus logros y fracasos. Aquellos que miran atrás con un sentido de satisfacción y cumplimiento experimentan integridad, mientras que aquellos que sienten remordimiento o decepción pueden enfrentar desesperación y desilusión. Esta teoría destaca la importancia crucial de la salud mental durante la etapa de envejecimiento, una consideración esencial que ha guiado las investigaciones y prácticas subsiguientes en gerontología y psicología del envejecimiento.

Desde una perspectiva sociológica, la gerontología examina meticulosamente cómo factores sociales y culturales omnipresentes influencian el proceso individual del envejecimiento, en una compleja interacción. Una de las teorías fundamentales en este ámbito es la "Teoría del Curso de la Vida" (Elder et al., 1994), cuya premisa

sostiene que el envejecimiento individual no es un proceso aislado, sino que está intrínsecamente entrelazado con el contexto histórico y social en el cual un individuo se desarrolla y envejece. El argumento central de esta teoría es que las transiciones y trayectorias de vida están profundamente influenciadas por las condiciones sociales y culturales, incluyendo oportunidades económicas, normas culturales y eventos históricos significativos. En esta misma línea, la gerontología también incorpora el análisis de las políticas públicas y la planificación de servicios para ajustarse a las demandas emergentes de una demografía que avanza hacia una edad más avanzada. Académicos y especialistas en el área han resaltado la función primordial de las políticas públicas, las cuales modelan activamente la estructura social relacionada con el envejecimiento. Estas políticas ejercen una notable influencia y determinan las oportunidades que están al alcance de las personas mayores y los desafíos que deben enfrentar de manera inevitable en sus vidas (Estes, 2001). Las políticas bien concebidas y estratégicamente implementadas pueden catalizar entornos de apoyo, potenciar el acceso a servicios esenciales, y facilitar ambientes en los cuales los adultos mayores pueden afrontar los retos del envejecimiento con dignidad y resiliencia. Por ende, en la confluencia de la investigación gerontológica y la política pública, prevalece una búsqueda de estrategias y soluciones a las necesidades y aspiraciones de una sociedad en constante evolución.

Por tanto, la Gerontología, en su evolución y expansión actual, se ha consolidado como una ciencia multidisciplinar, cuya riqueza reside en los diversos campos de estudio y especializaciones que convergen para explorar, analizar y entender las múltiples facetas del envejecimiento. Dentro de ella, la biología, la psicología, la sociología O ~~y~~ las políticas públicas, entre otras disciplinas, coexisten y colaboran, conformando una ciencia diversa, que permite una comprensión holística del proceso de envejecimiento. Esta integración multidisciplinar no solo ha ampliado los horizontes de la Gerontología, sino que también ha fortalecido su capacidad para desarrollar intervenciones, estrategias y políticas más efectivas e inclusivas, acorde con complejidad de las experiencias de envejecimiento en nuestra sociedad.

1.2.2 Calidad de vida en la vejez

La calidad de vida (CV) en esta etapa del ciclo vital es una preocupación central en la Gerontología, y al igual que esta, es un constructo influenciado por diversas disciplinas y enfoques teóricos. Por tanto, este concepto ha sido meticulosamente examinado desde múltiples perspectivas, y está formado por una diversidad de componentes que varían desde lo objetivo hasta lo subjetivo, y desde lo macrosocial hasta lo microindividual, incorporando variantes tanto positivas como negativas que interactúan de una forma dinámica (Tesch-Römer et al., 2001).

1.2.2.1 Factores objetivos de la calidad de vida

Los factores objetivos mensurables y externamente observables, hacen referencia a condiciones tangibles que circundan la vida de una persona.

Uno de ellos es el contexto social y residencial en el que conviven las personas adultas mayores (PAM), el cual modula sus interacciones, experiencias y oportunidades de acceso a recursos vitales. Explorar el contexto residencial nos lleva a un examen meticuloso de las características físicas y ambientales como las especificidades del hogar y el vecindario, así como su relación con la seguridad o la adaptabilidad de espacios. En este sentido, la seguridad no es solo una medida preventiva contra los peligros externos, sino que también es un facilitador de la movilidad, la socialización y la participación activa de los adultos mayores en las actividades comunitarias (Lawton, 1985). Además, la presencia y accesibilidad de espacios verdes y áreas recreativas son fundamentales. Estas zonas no solo contribuyen a la promoción de estilos de vida activos y saludables mediante el estímulo de la actividad física, sino también fomentan el bienestar psicológico y social, proporcionando lugares para el encuentro, la relajación y la conexión con la naturaleza (Takano et al., 2002). A su vez, la proximidad y facilidad de acceso a servicios esenciales, como un servicio médico adecuado, tiendas de alimentos u otros recursos comunitarios se erigen como componentes objetivos, siendo esenciales para la autonomía (Cho & Kwon, 2023) e influyendo en la CV. Concretamente, el acceso a los servicios de salud, que abarca desde la atención médica y preventiva hasta los servicios de rehabilitación, se configura como una

infraestructura clave que sostiene la salud y el bienestar de esta población. La disponibilidad y accesibilidad de estos servicios son cruciales y deben estar adaptados y ser pertinentes a las necesidades y condiciones específicas de los adultos mayores (Starfield et al., 2005), ya que les facilita mantener un nivel óptimo de salud física y funcional, permitiéndoles participar activamente en diversas actividades de la vida diaria y mantener un nivel de independencia y autonomía.

Así mismo, el sustento económico, puede funcionar como un facilitador, o un obstáculo, en el acceso a una variedad de recursos y experiencias que contribuyen a la CV, ya que permite desde satisfacer las necesidades básicas hasta acceder a oportunidades que enriquecen la vida y potencian la realización personal y la satisfacción. Los ingresos, pensiones y otros activos económicos, ofrecen posibilidades de elegir, participar y comprometerse en un amplio espectro de actividades y experiencias. Estos recursos económicos son vitales tanto para asegurar una nutrición adecuada y una vivienda confortable y segura, como para facilitar oportunidades de participar en actividades recreativas y culturales (Kahneman & Deaton, 2010).

En cuando a la red de apoyo social, desde una perspectiva objetiva, comprende las relaciones y conexiones interpersonales, incluyendo familiares, amigos y la participación en grupos o comunidades. Disponer de una red de apoyo social adecuada contribuye a la construcción de un sentido de comunidad y continuidad, proporcionando fuentes de interacción y compromiso que enriquecen la experiencia de vida (Barrón, 1996; Barrón & Sánchez, 2001, Berkman et al., 2011; Mirowsky & Ross, 1989). Además, este tejido social opera como un sistema de amortiguación y mitiga el impacto de las adversidades y desafíos que puedan surgir durante el envejecimiento (Wu & Sheng, 2019).

En cuanto a la salud, podemos analizarla tanto como una medida objetiva como subjetiva de la calidad de vida, ya que incluye tanto variables objetivas como la autonomía personal, la presencia de enfermedades crónicas o el estado nutricional, como subjetivas, como la propia autopercepción de salud que presenta la persona (Rodriguez Marin et al., 1993). Desde una perspectiva objetiva, existen indicadores tangibles y mensurables que nos permiten evaluar y monitorear la salud física.

Entre estos se destacan la autonomía personal, entendida como la capacidad de la persona para llevar a cabo actividades básicas e instrumentales de la vida diaria, manifestando un nivel de independencia funcional (Lawton & Brody, 1969). Este aspecto es relevante, ya que una mayor autonomía está asociada con un mejor bienestar y una mayor participación en diversas facetas de la vida. La presencia de enfermedades crónicas también emerge como una medida objetiva de la salud física, ofreciendo información valiosa acerca de las condiciones médicas que puedan afectar el bienestar físico y funcional y como estas pueden impactar en la capacidad de los individuos para mantener un estilo de vida activo y saludable. En los últimos años, por ejemplo, han surgido diversos estudios que muestran la evidencia de una relación entre una alimentación saludable y la probabilidad de desarrollar este tipo de enfermedades, que afectan directamente a la calidad de vida de la persona (Mastronuzzi & Grattagliano, 2019; Shlisky et al., 2017; Yang et al., 2022).

En cuanto al factor subjetivo de esta variable, la salud autopercibida, ha ganado un reconocimiento significativo en diversas áreas de investigación, ya que se ha obtenido evidencia de que no solo correlaciona con factores objetivos de salud, sino que a menudo anticipan a estos, como sucede con la esperanza de vida, siendo un posible predictor de esta (Machón et al., 2016). Además, en el contexto del deterioro cognitivo subjetivo, cambios autoinformados en la salud cognitiva se han vinculado con un aumento en el riesgo de demencia, incluso entre individuos cuyas evaluaciones clínicas se categorizan como normales (Mitchell et al., 2014).

1.2.2.2 Factores subjetivos de la calidad de vida

Siguiendo con los factores subjetivos, estos son consecuencia de la experiencia individual y perceptual del bienestar y juegan un rol de igual magnitud que los objetivos. Estos elementos surgen de la interacción de percepciones, sentimientos y evaluaciones personales que los individuos sostienen sobre su propia vida y bienestar. La literatura existente ha resaltado diversas dimensiones subjetivas que juegan un papel relevante ~~s~~ en la construcción de la calidad de vida en la vejez,

incluyendo la satisfacción vital, el bienestar emocional, las expectativas y aspiraciones personales, la autoeficacia y el sentido de pertenencia.

La satisfacción vital es un concepto que se define como la evaluación global que los individuos hacen de sus vidas, una reflexión introspectiva y evaluativa que incorpora múltiples dominios, como la salud, las relaciones sociales y la situación económica (Diener, 1984). En el contexto de los adultos mayores, la satisfacción vital puede verse afectada por la congruencia entre las expectativas de vida y las experiencias reales, así como por la habilidad para mantener una funcionalidad y participación significativa en diversas actividades de la vida (Ferring et al., 2004).

El bienestar emocional, hacer referencia a la prevalencia de afectos positivos sobre los negativos. Constituye una variable intrínsecamente interconectada con la satisfacción vital, ya que ambas participan en un intercambio recíproco y continuo de influencias y repercusiones. Por un lado, las emociones calificadas como placenteras, como la satisfacción, la alegría y el afecto positivo, han sido asociadas con beneficios para la salud. La presencia regulada y constante de estas emociones se ha relacionado con una menor prevalencia de enfermedades crónicas, una recuperación acelerada frente a enfermedades agudas, y una fortaleza y resiliencia elevada ante situaciones de estrés, lo que afecta directamente a la satisfacción vital de la persona (Fredrickson & Joiner, 2002). Por otro lado, las emociones que residen en el espectro de lo displacentero, como pueden ser la tristeza o la ansiedad, se han asociado con impactos adversos significativos sobre la salud y la satisfacción vital. Estas emociones se asocian con un mayor riesgo de desarrollar enfermedades crónicas, un deterioro en el funcionamiento cognitivo y un menor nivel de satisfacción con la vida, además de una reducción en la motivación, en la inclinación hacia la participación en actividades sociales y en las prácticas de autocuidado. (Carstensen et al., 2011).

En cuanto a las expectativas y aspiraciones personales son componentes subjetivos esenciales que influencian significativamente la calidad de vida (CV) de los adultos mayores. Las expectativas personales están profundamente arraigadas en los sistemas de creencias y valores de un individuo, funcionando como normas internas que guían las evaluaciones continuas de los logros y las experiencias de vida. Las personas comparan constantemente sus circunstancias actuales y logros

con sus expectativas y aspiraciones personales, lo que resulta en una evaluación subjetiva de satisfacción o insatisfacción en diversas áreas de la vida (Carr et al., 2001).

Otra variable fundamental en los aspectos subjetivos de la Calidad de Vida es la percepción de eficacia personal o Autoeficacia percibida, término propuesto por Albert Bandura en 1977, en su libro "*Self-efficacy: toward a unifying theory of behavioral change*". Este constructo psicológico, arraigado en la teoría social cognitiva, consiste en el conjunto de creencias de una persona acerca de su capacidad para organizar y ejecutar las acciones necesarias para manejar situaciones específicas, como alcanzar metas o salvar obstáculos (Bandura, 1977). En el ámbito del envejecimiento, la Autoeficacia Percibida (AP) juega un papel estratégico, siendo esencial para permitir la adaptabilidad y aportar estrategias de afrontamiento efectivas frente a los diversos desafíos que emergen en esta etapa de la vida. Los adultos mayores, con elevados niveles de AP tienden a mostrar una mayor resiliencia, manejando con más efectividad los estresores y adaptándose proactivamente a los cambios y las transiciones asociadas con el envejecimiento (Bandura, 1997). Y es que, la AP, influye no sólo en las acciones directas de los individuos, sino también su capacidad para gestionar sus pensamientos, emociones y la motivación intrínseca. Esta confianza en las propias capacidades puede fortalecer las habilidades de los adultos mayores para enfrentar y superar obstáculos, tales como la pérdida de seres queridos, las enfermedades crónicas o una disminución de la funcionalidad física, entre otros, contribuyendo significativamente a una CV más satisfactoria. Un alto sentido de Autoeficacia también puede promover comportamientos saludables y decisiones proactivas hacia el bienestar personal, incluyendo la participación en actividades físicas, sociales y cognitivas que son fundamentales para mantener y mejorar la CV en la vejez (Lachman, 2006).

Por último, el sentido de pertenencia y la creación de significado a través de las relaciones sociales y comunitarias emergen como aspectos esenciales para comprender la CV y además es uno de los aspectos que se han evidenciado como importante predictor de la CV en personas adultas mayores. Mantener conexiones sociales que las personas adultas mayores evalúen como significativas contribuye a

una mejor CV y a un envejecimiento más saludable (Holt-Lunstad et al., 2010; Tomaka et al., 2006). Las PAM, al interactuar y conectarse con sus comunidades y redes sociales, encuentran espacios de reciprocidad y reconocimiento. Estas interacciones favorecen la construcción de un sentido de pertenencia, esencial para el bienestar emocional y psicológico. Este sentido se nutre de la percepción de ser valorado, aceptado y apoyado por un sistema social, fortaleciendo así la resiliencia y la capacidad de adaptación a los cambios y desafíos que puedan presentarse durante el envejecimiento (Fuller-Iglesias et al., 2008).

Por tanto, la evaluación integral de la calidad de vida (CV) en la población de adultos mayores demanda una consideración meticulosa de una conjunto complejo e interconectado, que incluye variables tanto objetivas como subjetivas. Esta riqueza multifactorial en la conceptualización de la CV alimenta una comprensión más holística y matizada, permitiendo una aproximación a la complejidad y diversidad de las experiencias individuales en la vejez. Cada componente, desde factores objetivos como la salud física, hasta elementos subjetivos como la autoeficacia, opera en una intrincada red de interrelaciones, influyendo y siendo influenciado en un continuo dinámico (Netuveli & Blane, 2008). Además, el entrelazamiento de estos componentes fomenta una interdependencia, donde el fortalecimiento de un área, como el soporte social, puede influir positivamente, potenciando otros aspectos como la percepción de salud y bienestar (Berkman et al., 2000). Así, para una comprensión holística de la CV en la población de personas adultas mayores, es fundamental adoptar un enfoque que aprecie e incorpore esta red intrincada y multifactorial de componentes y sus interacciones. Este enfoque promueve una representación más precisa y fiel de las experiencias y realidades de los adultos mayores, respetando su diversidad y complejidad.

1.2.3 El desarrollo del concepto de Envejecimiento Activo: teorías y sus implicaciones teórico-prácticas

La percepción de la vejez, o del propio proceso de envejecimiento, ha evolucionado desde una concepción fundamentalmente negativa hasta una visión más holística y positiva, derivando en el término ampliamente aceptado de "Envejecimiento

saludable". Inicialmente, el enfoque del envejecimiento saludable estaba profundamente arraigado en la ausencia de enfermedad y discapacidad. Sin embargo, investigadores como Rowe y Khan (1987) jugaron un papel crucial en la redefinición y enriquecimiento de este concepto, articulando un marco teórico robusto que ha moldeado las investigaciones posteriores sobre el envejecimiento saludable. Estos autores propusieron que el "envejecimiento exitoso" o "saludable" no solo debe ser visto en términos de la evitación de enfermedades y la minimización de la discapacidad, sino también incluir aspectos como el mantenimiento de relaciones sociales saludables, el compromiso con actividades que fomentan el crecimiento personal y llevar una vida cognitivamente estimulante y desafiante. El trabajo de Rowe y Khan, por tanto, propone una visión más positiva del envejecimiento, que considera múltiples dimensiones, y reconoce el potencial para la mejora continua y el desarrollo a lo largo del curso de la vida. Esta conceptualización de la vejez no solo ha evolucionado en el ámbito académico, sino que también se ha observado un cambio en los discursos políticos relacionados con el envejecimiento. En las dos últimas décadas, han coexistido dos modelos teóricos divergentes. Predominantemente, prevaleció una orientación productivista, cuyo núcleo central radicaba en la prolongación y extensión de la vida laboral activa. Esta concepción ha ocupado un espacio preeminente dentro de los debates y estrategias políticas. En contraposición, también ha emergido y se ha manifestado un enfoque más holístico y comprehensivo del envejecimiento activo, una perspectiva apoyada por organismos internacionales preeminentes como la Organización Mundial de la Salud (OMS) y la Organización de las Naciones Unidas (ONU). Este enfoque más inclusivo y diversificado encapsula una visión del envejecimiento que trasciende las dimensiones ocupacionales y productivistas, incluyendo variadas facetas y dimensiones intrínsecas al proceso de envejecimiento (Foster & Walker, 2015). En esta línea, los avances hacia la adaptación y optimización de los entornos comunitarios, con el objetivo de facilitar la accesibilidad de las personas adultas mayores, se han incrementado en los últimos años debido a la influencia de diferentes estudios que destacan los beneficios de envejecer en el hogar, convirtiéndose en un objetivo político prioritario dentro de esta área (Del Barrio Truchado et al., 2018). Esta perspectiva refleja las preferencias y aspiraciones expresadas intrínsecamente por individuos

de edad avanzada y ha servido como un catalizador para la iniciación y proliferación de investigaciones académicas, que buscan conocer los componentes residenciales y ambientales menos accesibles para mejorar sus condiciones para un mayor beneficio integral, tanto individual como social (Eibich et al., 2016; Hans-Werner & Gerstorf, 2018; Hybels et al., 2006)

Con el tiempo, esta conceptualización evolucionó aún más, encuadrando al sujeto dentro de una estructura social indispensable para el transcurso de su envejecimiento, culminando en el paradigma del "Envejecimiento Activo", incorporado por la Organización Mundial de la Salud (OMS), y defendiéndolo como el "proceso de optimización de las oportunidades para el bienestar físico, social y mental a lo largo del ciclo vital para extender la esperanza de vida saludable" (OMS, 2002). El término presenta nuevamente una perspectiva multifacética que aúna consideraciones políticas, éticas y científicas. Muestra de ello, en la Segunda Asamblea Mundial de las Naciones Unidas sobre el Envejecimiento, celebrada en abril de 2002 en Madrid (España) la OMS presentó el documento "Envejecimiento activo: un marco político". La versión preliminar de este documento, publicada en 2001 con el título de "Salud y envejecimiento: Un documento para el debate", se tradujo a varios idiomas, ampliando su divulgación y facilitando las aportaciones de diversos expertos que permitieron completar la versión final. Este texto fue diseñado para guiar y orientar en la formulación de políticas y programas relativos al envejecimiento. En él se sostiene la idea de que enfrentar los retos derivados del envejecimiento poblacional requiere una acción colaborativa y coordinada entre diversos organismos y entidades. Para ello se establecen los tres pilares fundamentales que deben guiar las estrategias y políticas de los diferentes países en esta área: participación, salud y seguridad. Estos pilares representan las áreas críticas que necesitan atención y desarrollo para facilitar una concepción del proceso de envejecimiento como una etapa en la que se promueva no sólo estar libre de enfermedad, sino activo.

El pilar de "Participación" enfatiza la importancia de mantener a las personas adultas mayores integradas y activas dentro de sus comunidades y sociedades, promoviendo su involucración en actividades sociales, económicas y culturales, contribuyendo así a su bienestar general y calidad de vida. En cuanto a la "Salud",

se subraya la necesidad de promover estilos de vida saludables, prevención de enfermedades y gestión de condiciones crónicas existentes para mantener una vida con un nivel óptimo de bienestar físico y mental. Por último, el pilar de “Seguridad" se centra en la protección de este grupo de edad, asegurando que vivan en ambientes que se adapten a sus necesidades, además de promover sistemas de apoyo para proteger sus derechos y bienestar.

Atendiendo estos principios que guían la conceptualización del envejecimiento saludable, se desarrollaron diversas teorías que intentan describir los determinantes para conseguir éxito en dicho proceso. Entre ellas podemos destacar el Modelo de Envejecimiento Saludable, Positivo y con Éxito, desarrollado por Rocío Fernández-Ballesteros, en él, la autora destaca cuatro criterios esenciales que caracterizan este tipo de envejecimiento (Fernandez-Ballesteros, 2008):

1) Las condiciones de salud, haciendo referencia tanto a un estado de bienestar físico como mental.
2) El funcionamiento óptimo, tanto a nivel físico como cognitivo, permitiendo a la persona mantener una independencia y autonomía significativas.
3) Predisposición afectiva positiva y equilibrada, crucial para la adaptación y gestión emocional en la tercera edad.
4) Participación social efectiva, que facilite el sentido de pertenencia y contribución continua en la sociedad.

Como resultado práctico, se han desarrollado diversos programas que incorporan estos conceptos, derivando en estrategias orientadas a prolongar la independencia de las personas mayores, promoviendo su permanencia en el hogar y estimulando una participación social enriquecedora. Actualmente, existen numerosos programas a nivel tanto internacional como nacional que se focalizan en la temática del envejecimiento y el bienestar de las personas mayores. Un ejemplo es el programa "Ageing Better in Camden", que se implementó entre los años 2015 y 2022. Este programa enfrentó desafíos significativos durante su puesta en marcha, especialmente debido a la pandemia de COVID-19. Compuesto por diferentes proyectos comunitarios, se creó con el objetivo de mitigar el aislamiento y aumentar la resiliencia de las personas mayores en el Reino Unido, basándose en tres 'pilares de pertenencia' esenciales: el lugar, las personas y las actividades.

Durante la confluencia del programa con la pandemia, estos pilares experimentaron perturbaciones severas; los espacios físicos tuvieron que ser clausurados, las reuniones personales fueron limitadas, y las actividades presenciales fueron suspendidas. En este contexto de adversidad, los líderes del proyecto se vieron abocados a innovar y reestructurar sus estrategias para continuar brindando soporte y acompañamiento a los miembros y usuarios de los servicios. Ante la imposibilidad de utilizar espacios físicos, que muchos describían afectuosamente como un "segundo hogar", se recurrió a la virtualidad como una plataforma alternativa. Inspirados por otras instituciones, como escuelas y lugares de trabajo, los proyectos realizaron una transición hacia el dominio digital, facilitando actividades y clases mediante plataformas en línea, como Zoom, para mantener la continuidad y la cohesión de la comunidad.

En España, el Instituto de Mayores y Servicios Sociales (IMSERSO), que, tras la última reestructuración de los departamentos ministeriales acontecida en enero de 2020, está adscrito al Ministerio de Derechos Sociales y Agenda 2030 a través de la Secretaría de Estado de Derechos Sociales. Esta entidad desempeña un papel crucial en la articulación y ejecución de políticas y estrategias orientadas al bienestar de las personas mayores y de otros grupos vulnerables, como personas con diversidad funcional. Centrando su misión en la promoción del envejecimiento activo, el IMSERSO trabaja para garantizar que las personas mayores tengan acceso a servicios y oportunidades que enriquezcan su calidad de vida y faciliten su integración y participación activa en la sociedad. además, juega un papel vital en la promulgación de investigaciones, estudios y análisis que facilitan una comprensión más profunda de las necesidades y desafíos que enfrentan las personas adultas mayores y otros grupos, permitiendo así la adaptación y mejora continua de las políticas y servicios ofrecidos. Es esencial destacar que el IMSERSO trabaja en colaboración estrecha con diferentes niveles de gobierno, así como con entidades privadas y organizaciones no gubernamentales, buscando sinergias que potencien el impacto y alcance de sus iniciativas. A través de su labor, el IMSERSO refuerza el compromiso social y estatal hacia el bienestar y la dignidad, consolidando una sociedad más inclusiva e igualitaria.

En cuanto al sistema universitario, desde finales del siglo XX se implementaron en España los Programas Universitarios para Mayores (PUM), cuya finalidad es permitir el acceso de las poblaciones de mayor edad, habitualmente a partir de los 55 años, a la educación universitaria. Son concebidos como vehículos que facilitan la educación continua y a lo largo de la vida, encaminados hacia la promoción de una participación, formación e integración social robusta dentro de este grupo etario. Dichos programas están impregnados de una riqueza y diversidad temática y cuya estructura esta diseñada para propiciar un ambiente educativo que favorezca la participación activa, incentivando no solo la adquisición de conocimientos, sino también el intercambio cultural y generacional y desarrollo personal y social de los participantes.

En definitiva, podemos afirmar que la promoción del envejecimiento activo se erige como el pilar fundamental sobre el que desarrollar políticas, estrategias de acción y el desarrollo de intervención durante el proceso de envejecimiento para optimizar esta etapa.

1.3 BENEFICIOS Y DESAFÍOS DEL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN POR PERSONAS ADULTAS MAYORES

Es indiscutible que la dinámica de interacción de los distintos grupos sociales ha experimentado una transformación significativa a raíz del desarrollo y proliferación de las plataformas de redes sociales y el uso herramientas digitales destinadas a ello. Estas herramientas no solo han revolucionado la forma en que las personas se comunican y se relacionan entre sí, sino que también han ampliado considerablemente las posibilidades de gestionar una amplia variedad de actividades sin la necesidad de desplazamientos físicos antes indispensables. Esta evolución tecnológica ha demostrado ser particularmente beneficiosa para aquellos individuos que tienen limitaciones en su movilidad o que residen en localidades distantes de los centros donde se llevan a cabo dichas actividades, permitiéndoles superar estos obstáculos y acceder a una gama extensa de recursos y servicios. En este contexto, las personas con diversidad funcional, así como aquellas que se encuentran en situaciones de aislamiento geográfico, pueden aprovechar las ventajas que ofrecen estas plataformas digitales para integrarse

más efectivamente en la sociedad y participar en la economía digital, superando así las limitaciones físicas o logísticas que anteriormente restringían su participación activa.

En lo que respecta específicamente a la población de adultos mayores, la concepción del envejecimiento activo, que se ha analizado previamente, no puede ser plenamente comprendida ni implementada sin considerar el impacto y la importancia de la digitalización en el mundo actual. La integración de las Tecnologías de la Información y la Comunicación (TIC) en la vida diaria de los adultos mayores no solo es fundamental para su inclusión y participación social, sino que también contribuye significativamente a su bienestar emocional y calidad de vida, al proporcionarles medios para mantenerse conectados con su entorno, acceder a servicios esenciales y continuar con su desarrollo personal y aprendizaje a lo largo de la vida. Por tanto, la incorporación de las TIC en la cotidianidad de las personas adultas mayores ha surgido como un vector crucial en diversas áreas. Una de ellas es el fortalecimiento de sus redes sociales y la mejora de su bienestar emocional. Es evidente que estas herramientas pueden ofrecer un puente sobre la brecha de la distancia física, permitiendo a este colectivo mantener o generar nuevos vínculos afectivos, pudiendo mitigar la sensación de aislamiento, fomentando un sentido de pertenencia y conexión social que es vital para su integración y participación en la sociedad (Berkley et al, 2023). Además, la posibilidad de acceder a nuevas redes sociales y comunidades en línea es un recurso indispensable para aquellos cuya movilidad física se encuentra restringida o que enfrentan condiciones de aislamiento. De esta forma, mediante estas herramientas es posible fomentar la autonomía, ya que las PAM pueden gestionar sus intereses de manera independiente y expresar libremente sus opiniones y experiencias, realizando una participación activa. Por tanto, el uso efectivo de estas herramientas tiene el potencial de fomentar el desarrollo de diversos factores, como la autoeficacia, definida como la creencia en la propia capacidad para ejecutar comportamientos necesarios para producir resultados específicos, significativamente influenciada por el uso efectivo de las TIC. Los adultos mayores que se involucran activamente con estas tecnologías reportan una mayor sensación de control sobre su vida cotidiana, lo que a su vez fortalece su autoestima y promueve una mayor autonomía (Lozoya et al., 2022). Adicionalmente, debemos

tener en cuenta que tanto una mayor comunicación y participación activa en comunidades en línea, no sólo disminuye el aislamiento social, sino que también supone una estimulación cognitiva que puede desacelerar el declive cognitivo, permitiendo mantenerse durante más tiempo en mejores condiciones tanto la salud emocional, como la cognitiva y la física (Morikawa et al., 2023). Además, innovaciones como los sistemas de teleasistencia y monitoreo remoto de la salud permiten a los adultos mayores vivir con mayor independencia, proporcionando a la vez a los cuidadores y profesionales de la salud herramientas efectivas para supervisar y responder a las necesidades de salud de esta población. Estas tecnologías no solo mejoran la capacidad de los adultos mayores para gestionar condiciones crónicas desde la comodidad de sus hogares, sino que también ofrecen una vía para la intervención temprana en caso de emergencias, lo que resulta en mejores resultados de salud y reducción de la necesidad de atención institucional (Doyle & Walsh, 2015).

Por tanto, las TIC pueden entenderse como un instrumento crucial para mejorar la autoeficacia, la independencia y la calidad de vida de los adultos mayores, pudiendo transformar significativamente su envejecimiento y permitiendo que este se desarrolle de forma más saludable, independiente y satisfactoria. Sin embargo, existen diversas causas por las que no todas las personas adultas mayores implementan la tecnología en sus actividades rutinarias, entre ellas los estereotipos y el edadismo.

1.3.1 Barreras en el uso de TIC por parte de personas adultas mayores: estereotipos y edadismo

Los estereotipos, conceptualizados como percepciones erróneas derivadas de razonamientos ilógicos y rígidos acerca de un grupo específico, ejercen una notable influencia en diversos aspectos sociales y personales. Particularmente en el caso de las personas adultas mayores, dichos estereotipos afectan tanto su autoconcepto como la percepción del proceso de envejecimiento, influyendo en su comportamiento y dando lugar a la profecía autocumplida, mediante la cual las acciones individuales refuerzan los sesgos asociados a su propio grupo (Sitges-

Maciá et al., 2020). Asimismo, estos estereotipos inducen en el resto de la sociedad actitudes negativas y prejuicios que pueden culminar en conductas discriminatorias, egoísmo y maltrato, entre otras formas de comportamiento adverso (Fernández, 2003; Fernández-Ballesteros, 1992; Levy & Banaji, 2002; Montorio et al., 2002; Montoro, 1998; Pinazo, 2013).

Del seno de estos estereotipos surge el concepto de edadismo, término acuñado por Butler en 1980, que alude a la visión peyorativa basada en la edad cronológica avanzada de un individuo, implicando una percepción estereotipada y despectiva de las personas adultas mayores. Esta visión fomenta en el individuo la creencia de que el deterioro de su estado de salud esta intrínsecamente ligado al envejecimiento (McGuire et al., 2008), y puede suscitar en la sociedad conductas que van desde la agresión hasta prácticas profesionales discriminatorias (Losada-Baltar, 2004; Meisner, 2012; Pinazo, 2013). Es conveniente tomar conciencia de estos estereotipos vinculados a la edad y combatir las actitudes y comportamientos negativos prevalentes en nuestra sociedad (Molina, 2002).

Precisamente con el propósito de alcanzar esta meta, la American Psychological Association (APA) elaboró en 2003 un documento que delineaba las directrices para erradicar los estereotipos asociados a la vejez. Entre las estrategias destacadas se incluyen la sensibilización social, la formación y capacitación de especialistas, y la incorporación de más contenidos sobre la vejez y el envejecimiento humano en los planes de estudio. Además, es fundamental la implementación de dinámicas intergeneracionales para la eliminación de los estereotipos negativos sobre la vejez, dado que los efectos positivos del contacto entre generaciones están mediados por un proceso de recategorización, reduciendo el antagonismo intergrupal y provocando cambios en la percepción de los miembros de los grupos (Pinazo, 2013).

En el área tecnológica, el edadismo puede manifestarse en el diseño de productos, la comercialización, y el soporte técnico, los cuales a menudo ignoran las necesidades y capacidades de los usuarios adultos mayores (Ayalon, 2018). Este prejuicio tiene consecuencias directas en la disposición y capacidad de las personas mayores para adoptar nuevas tecnologías. Adicionalmente, las actitudes edadistas pueden llevar a las personas mayores a percibir la tecnología como algo

que no es para ellos, lo que crea una barrera psicológica significativa para la adopción tecnológica. Esto se ve exacerbado por interfaces de usuario que no consideran limitaciones físicas o cognitivas que pueden ser más comunes en la vejez, como la disminución de la visión, la audición o la destreza manual (Czaja et al., 2006). Sumado a esto, debemos tener en cuenta que el edadismo es un factor que favorece la brecha digital generacional, como se analizará a continuación.

1.3 ANÁLISIS DE LA BRECHA DIGITAL Y FACTORES CLAVE EN LA ADOPCIÓN DE LAS TIC POR PERSONAS ADULTAS MAYORES

Cuando hablamos de brecha digital nos estamos refiriendo a la disparidad existente entre individuos, empresas o áreas geográficas con respecto a su acceso a TIC, así como su uso y conocimiento de estas. Este fenómeno no solo se centra en la disponibilidad de infraestructura tecnológica, sino también en aspectos relacionados con las habilidades digitales, la motivación para usarla, el uso efectivo de la tecnología y las oportunidades derivadas de su uso, pudiendo ser categorizada en diferentes tipos según los factores que contribuyen a su existencia y persistencia. Es, por tanto, un fenómeno complejo que se puede manifestar en varios niveles, pese a que estos no son excluyentes (Van Dijk, 2006). La *brecha digital primaria* se refiere al acceso físico a las TIC, destacando como factores determinantes aspectos socioeconómicos, geográficos y de infraestructura, ya que estos impactan directamente en la disponibilidad de tecnología, tanto para individuos como para comunidades. Sin embargo, pese a superar el desafío del acceso, también puede existir una *brecha digital secundaria*, relacionada con las habilidades para utilizar de manera efectiva las tecnologías de la información. Este nivel abarca la capacidad de los individuos para entender y utilizar las TIC de forma efectiva, beneficiándose de ellas en su vida cotidiana (Hargittai, 2002). Factores como diferencias en la educación, edad o el contexto cultural son determinantes en este nivel. Por último, *la brecha digital terciaria*, hace referencia a las desigualdades resultantes del uso de las TIC pues, por ejemplo, aunque dos individuos tengan el mismo acceso y habilidades similares digitales, el beneficio real que obtienen del uso de la tecnología puede diferir significativamente. En palabras de DiMaggio & Hargittai, (2001), esta dimensión aborda cómo las

personas utilizan las TIC para mejorar su situación económica, cultural y social, y cómo dichas tecnologías pueden ampliar o reducir las desigualdades que ya existían previamente o crear otras. A la vista de lo expuesto, podemos afirmar que la brecha digital es un fenómeno multifacético que requiere un enfoque holístico para su comprensión y superación, que no solo implica proporcionar acceso universal a las TIC, sino también garantizar que todos los individuos posean las habilidades necesarias para utilizar estas tecnologías de manera efectiva y que puedan obtener beneficios reales de su uso, contribuyendo así a una sociedad más equitativa e inclusiva.

Concretamente, el análisis de la incidencia de la brecha digital en la población de adultos mayores revela contrastes significativos en comparación con las cohortes más jóvenes. La existencia de una persistente percepción social que cataloga a las personas adultas mayores como analfabetas digitales, prevalece a pesar de la evidencia que señala un incremento notable en la adopción y el uso TIC por parte de este segmento demográfico los últimos años (Schreurs et al., 2017). Es cierto que, pese a notables avances en la inclusión digital de las personas adultas mayores, aún persiste una brecha generacional marcada en términos de acceso, competencia y uso efectivo de estas herramientas tecnológicas. La brecha generacional en el uso de las TIC no solo se refleja en la diferencia cuantitativa de uso entre generaciones más jóvenes y mayores, sino también en la calidad y profundidad de este uso. Las generaciones más jóvenes tienden a utilizar una gama más amplia de aplicaciones y servicios digitales, y a integrar las TIC de manera más profunda en sus vidas cotidianas, tanto para el ocio como para actividades productivas. En contraste, aunque cada vez más personas mayores se familiarizan con las TIC, su uso tiende a ser más limitado, centrado en aplicaciones y servicios específicos que perciben como directamente relevantes para sus necesidades e intereses, tales como la comunicación con familiares y amigos, la adquisición de información o el entretenimiento.

En España, el uso de la tecnología en personas jóvenes es notablemente alta, superando el 98% de acceso a internet, lo cual ha facilitado de manera considerable su adaptación a modelos educativos a distancia cuando ha sido necesario, entre otros. Sin embargo, la integración de la tecnología entre las

personas mayores de 74 años presenta un escenario diferente, ya que pese a aumentar su uso, el uso de internet se encuentra alrededor del 30%. Según datos del Ministerio de Asuntos Económicos y Transformación Digital y del Instituto Nacional de Estadística, la edad constituye un factor determinante en el uso de la tecnología, que no sólo se manifiesta en la capacidad de manejo de tecnologías informáticas sino también en la confianza depositada en Internet. Mientras el 68,5% de los jóvenes informa de una alta confianza en la red, esta proporción se reduce al 50% entre los adultos mayores de 65 a 74 años. Además, el nivel educativo profundiza aún más esta brecha, con un uso de Internet casi universal (93%) entre poseedores de doctorados, en marcado contraste con aquellas personas sin estudios o con educación primaria, donde los porcentajes descienden al 6% y 19%, respectivamente. La brecha de ingresos también es notable, con un 55% de uso de Internet en hogares de ingresos altos frente a solo un 14% en hogares de ingresos bajos. En cuanto a los diferentes tipos de uso, la actividad en línea de los adultos mayores se centra principalmente en la comunicación y la adquisición de información. La mensajería instantánea, las llamadas y videollamadas, así como el correo electrónico, son las principales herramientas que utiliza este grupo. Además, un segmento considerable accede a noticias y revistas en línea, y busca información de salud a través de la red. Sin embargo, la participación en actividades como la banca digital, las redes sociales y la gestión trámites es menor que en otros grupos etarios. La confluencia de esta variabilidad de factores pone en relieve la necesidad enfoques inclusivos y estrategias dirigidas a mitigar estas desigualdades, con el fin de fomentar una integración tecnológica más equitativa (Ministerio de Asuntos Económicos y Transformación Digital, 2022).

Uno de los problemas asociados a la brecha digital generacional es la transición hacia la digitalización de servicios, especialmente en el ámbito de la salud y el bienestar, la cual se ha promovido como una estrategia para aumentar la accesibilidad de dichos servicios para toda la población. Sin embargo, esta premisa, aunque popular, ha sido cuestionada por su efectividad en la práctica. Equiparar la oferta de servicios en línea con una mayor accesibilidad es una simplificación que no toma en cuenta las complejidades inherentes a la diversidad de usuarios (Randall y Berlina, 2019). Esta observación es particularmente relevante en el

contexto de las PAM, quienes pueden enfrentar obstáculos significativos al interactuar con sistemas digitales, no solo debido a limitaciones tecnológicas sino también a barreras relacionadas con la salud y la edad.

Adicionalmente, la inaccesibilidad a estos sistemas puede comprometer la dignidad de los adultos mayores, y la necesidad de solicitar ayuda para utilizar sistemas básicos, como los relacionados con la salud puede incrementar la sensación de vulnerabilidad entre este grupo poblacional, afectando negativamente (Raja et al., 2023). Este impacto negativo en la dignidad es crítico, pero, además, la sustitución excesiva de la atención sanitaria presencial por alternativas digitales podría tener implicaciones adversas en la inclusión social de este grupo poblacional, sugiriendo que la tecnología podría estar aislando en lugar de integrar (Raja et al., 2023). Por tanto, a menudo, son las personas más jóvenes y con mayor nivel de educación las que más provecho sacan de estos servicios altamente digitalizados, aprovechando las oportunidades que ofrecen para mejorar su calidad de vida. En contraste, los adultos mayores, especialmente aquellos con menores ingresos o educación, se enfrentan a obstáculos significativos para acceder y utilizar eficazmente estas tecnologías. Esta brecha no solo limita su capacidad para interactuar con servicios sociales esenciales, sino que también puede aislarlos de la sociedad digital moderna, aumentando las desigualdades existentes y limitando su participación en una sociedad cada vez más digitalizada (Olson & Viscovi, 2023).

Por tanto, la alfabetización digital emerge como un componente esencial para empoderar a la población de adultos mayores (PAM) en el uso efectivo de tecnologías digitales. Sin embargo, tal y como se ha señalado anteriormente, para reducir esa brecha digital hemos de tener en cuenta factores que pueden ser determinantes en el uso de estas herramientas, en especial en la población de PAM. Por un lado, se enfatiza la importancia de la práctica y el apoyo del entorno cercano, como familiares o amigos, para fomentar una mayor confianza y competencia en el uso de estas herramientas. Este apoyo es particularmente crucial para los adultos mayores, quienes pueden requerir una red de soporte más sólida que otros grupos demográficos para utilizar estas herramientas (Schreurs et al., 2017), ejerciendo la influencia social un efecto positivo en la interacción con las TIC (Macedo, 2017). Por otro lado, encontramos otros factores que pueden ser

determinantes, como la usabilidad percibida de las aplicaciones tecnológicas y el nivel educativo, como se ha mencionado previamente, el cual ha demostrado tener un una relación directa y positiva en el uso de tecnología entre los adultos mayores (Özsungur, 2022). La intersección de estos factores revela una complejidad inherente en la adopción de las TIC por parte de las personas adultas mayores, que se distingue marcadamente de las dinámicas observadas en otros grupos de edad. Dicha complejidad subraya la importancia de recurrir a un marco conceptual que facilite una comprensión más profunda de este fenómeno.

En este contexto, resulta pertinente recurrir a la Teoría Unificada de la Aceptación y Uso de la Tecnología (UTAUT), desarrollada por Venkatesh et al., en el año 2003. Esta teoría propone un modelo explicativo cuyo objetivo es esclarecer los procesos mediante los cuales los individuos deciden adoptar y hacer uso de las TIC y en la que se destaca su capacidad para explicar la intención del usuario y el uso subsiguiente de la tecnología en una variedad de contextos organizacionales y personales. Este marco teórico sintetiza elementos de modelos previos que también intentaban explicar la aceptación de la tecnología, incluyendo la Teoría de Acción Razonada (Fishbein & Ajzen, 1975), el Modelo de Aceptación de Tecnología (Davis, 1989), la Teoría de Comportamiento Planificado (Ajzen, 1991).

Siguiendo el modelo UTAUT, hay cuatro elementos clave que señala como predictores directos de la intención de uso y del uso efectivo de una tecnología. En primer lugar, *la expectativa de rendimiento*, refiriéndose a la medida en que una persona cree que el uso de la tecnología le ayudará a mejorar el desempeño de sus tareas. Este constructo está claramente influido por la percepción de eficacia que el usuario anticipa de la adopción tecnológica, lo que significa que, si los individuos perciben que una herramienta tecnológica puede facilitar su trabajo o mejorar de alguna forma su día a día, es más probable que tengan la intención de utilizarla y efectivamente la usen. En segundo lugar, *la expectativa de esfuerzo*, como la percepción de facilidad de uso de la tecnología. Si un individuo cree que es fácil de aprender y utilizar una determinada tecnología, entonces es más probable que desarrolle una intención positiva hacia su uso. La expectativa de esfuerzo está relacionada con la usabilidad percibida pero también con la facilidad con la que el usuario cree que puede incorporar la tecnología en su rutina diaria. En tercer lugar,

la influencia social, entendida como el grado en que un individuo percibe que personas importantes para él (como familiares, amigos o personas relevantes de su círculo cercano) creen que debe usar la nueva tecnología. La influencia social juega un papel crítico, especialmente en las etapas iniciales de adopción de la tecnología, donde el apoyo o la presión del entorno social pueden motivar al individuo a adoptar la tecnología o desistir de su uso. En cuarto lugar, *las condiciones facilitadoras*, definidas como la percepción del individuo sobre los recursos y el soporte disponibles para utilizar la tecnología. Esto incluye tanto las infraestructuras tecnológicas existentes como el acceso a ayuda o asistencia técnica en caso de ser necesario. Si las personas creen que tienen el soporte necesario para utilizar la tecnología, es más probable que la adopten y la utilicen efectivamente, mientras que si consideran que el soporte será escaso o de difícil acceso no estarán tan inclinados a hacer uso de la herramienta. Además de estos cuatro constructos principales, la UTAUT también reconoce el papel moderador de variables como la edad, el género o la experiencia, que pueden afectar a las expectativas y la intención de uso de la tecnología.

Esta teoría en su inicio se desarrolló pensando en un contexto organizacional por lo que en el año 2012 se revisó el modelo y formulando La Teoría Unificada de la Aceptación y Uso de la Tecnología 2 (UTAUT2), que representa una extensión del modelo UTAUT original, adaptándolo al contexto de los consumidores y su interacción con la tecnología en ambientes no organizacionales (Venkatesh et al., 2012). Esta revisión surgió de la necesidad de comprender las dinámicas de adopción tecnológica en la vida cotidiana, donde los factores motivacionales pueden diferir sustancialmente de aquellos presentes en entornos empresariales o institucionales. Así, la UTAUT2 añade tres constructos clave al modelo original para abordar aspectos específicos del comportamiento del consumidor hacia la tecnología: *la expectativa de hedonismo*, el cual destaca el placer y el disfrute derivados del uso de la tecnología y reconoce que las decisiones de los consumidores no se basan únicamente en evaluaciones utilitarias, sino también en el valor intrínseco del entretenimiento o la satisfacción que la tecnología puede proporcionar; *la expectativa de precio*, identificando el coste como un factor crucial en la decisión de adoptar tecnologías; y *el hábito*, que subraya la importancia de las rutinas y comportamientos previos en la adopción y el uso continuado de la

tecnología. Se reconoce que, una vez establecida, la tendencia a usar tecnología puede persistir más allá de las evaluaciones conscientes de su utilidad o facilidad de uso.

Esta teoría ha sido ampliamente aplicada y validada en múltiples estudios y contextos (Nikolopoulou et al., 2020; Oliveira et al., 2013; Raman & Don, 2013; Tak & Panwar, 2017), demostrando su robustez para explicar la aceptación tecnológica en diferentes grupos, entre los que se incluyen las personas adultas mayores. Gracias a su enfoque integral es posible identificar factores clave que deben ser considerados al diseñar e implementar herramientas tecnológicas, así como los programas y políticas asociados a estos, con el objetivo de maximizar su aceptación y uso efectivo entre los potenciales usuarios.

CAPÍTULO 2: CIBERCRIMEN Y PERSONAS ADULTAS MAYORES

2.1 INTRODUCCIÓN AL CIBERCRIMEN

El cibercrimen es un fenómeno complejo que resiste las limitaciones de una única definición (Phillips et al., 2022) y su amplitud y diversidad han llevado a un continuo debate entre académicos, profesionales de la ciberseguridad y legisladores sobre cómo delinear con precisión este panorama en constante evolución. Para comprender a qué nos referimos con cibercrimen, es necesario adentrarse en las distintas perspectivas que se han desarrollado a lo largo del tiempo. Inicialmente llegó a argumentarse que el crimen que se producía en red era fundamentalmente el mismo que se producía de forma tradicional, simplemente cambiando el entorno en el que se llevaba a cabo (Grabosky, 2001). Sin embargo, se han presentado argumentos que contradicen esta afirmación, considerando que puede presentar formas distintivas, con características sustancialmente diferentes a las presentes en los delitos convencionales, que generen nuevos desafíos (Yar, 2006). La complejidad en hallar una única definición referente al cibercrimen comienza con la diversidad de terminología para referirse a este fenómeno. Esto se evidencia en el uso de un extenso repertorio de términos. La proliferación y aplicación arbitraria de multitud de términos, como “delitos informáticos", "delitos electrónicos" o "crimen facilitado por tecnología”, entre otros, contribuye no solo a una notable superposición conceptual sino también a la existencia de vacíos significativos en la definición de lo que constituye un delito en el contexto digital. Adicionalmente, encontramos que la conceptualización del cibercrimen varía significativamente según la amplitud con la que se defina el término, pudiendo encontrar dos perspectivas predominantes: una concepción amplia y una concepción restringida.

Bajo una concepción amplia, el término cibercrimen engloba cualquier forma de comportamiento delictivo que se manifieste en el ciberespacio. En este sentido, se considera que el cibercrimen no lo es por su forma sino por el medio en el que se comete (Grabosky, 2001), lo que incluiría dentro de los cibercrímenes delitos tradicionales que se adaptan a este nuevo contexto. Bajo esta óptica, el fraude, el acoso y la suplantación de identidad no son esencialmente diferentes en línea, pero

su ejecución y alcance se ven transformados por la tecnología digital. Esta perspectiva no solo contempla las actividades delictivas cuyo núcleo ilícito impacta directamente en los intereses o bienes fundamentales presentes en el ambiente digital (como el hackeo o la distribución de malware), sino también aquellos delitos de naturaleza tradicional que se ven transformados o facilitados por el uso de las Tecnologías de la Información y la Comunicación (TIC). Siguiendo esta perspectiva, en su obra *Cybercrime: The Transformation of Crime in the Information Age*, David Wall (2007) examina el cibercrimen abarcando tanto las transformaciones inducidas por la tecnología en formas tradicionales de criminalidad que ya existían previamente, como la emergencia de delitos únicamente posibles dentro del contexto digital. Wall argumenta que el cibercrimen no debe entenderse meramente como una extensión de la criminalidad en el espacio físico hacia el digital, sino como una evolución que refleja cambios fundamentales en cómo se conceptualizan y perpetran los delitos en la era moderna. A través de su análisis, Wall destaca la importancia de reconocer tanto la continuidad como la innovación en el cibercrimen, insistiendo en que las respuestas legales y sociales deben ser dinámicas y adaptativas para abordar efectivamente tanto los desafíos tradicionales transformados por la tecnología como los nuevos paradigmas delictivos.

En contraste, autores como Yar (2006) abogan por una conceptualización más restringida del cibercrimen, limitándose a aquellos delitos que son intrínsecamente digitales, es decir, aquellos comportamientos delictivos que, por su propia naturaleza, solo pueden tener lugar dentro del ciberespacio. Esta aproximación enfoca su atención en los delitos que emergen específicamente como resultado de la tecnología digital y que no encontrarían un equivalente directo fuera del este contexto. Yar enfatiza que estas nuevas modalidades de delito requieren enfoques teóricos y prácticos específicos para su prevención, detección y sanción, desafiando así a los sistemas jurídicos y a la sociedad a adaptarse a las realidades de la criminalidad en la era digital.

Salvando estas perspectivas, una de las definiciones más ampliamente aceptadas es la propuesta por Gordon y Ford en 2006 quienes articulan el concepto de cibercrimen sobre una amplia gama de actividades delictivas, definiéndolo como

"cualquier delito que se facilita o se comete utilizando un ordenador, red o dispositivo de hardware" (Gordon & Ford, 2006, pp.14). Por tanto, esta definición resalta el papel instrumental de la tecnología en la perpetración de delitos, subrayando tanto la utilización de dispositivos tecnológicos para facilitar actividades delictivas tradicionales como la comisión de delitos exclusivamente posibles dentro del entorno digital. Además, Gordon y Ford introdujeron una distinción pionera dentro del estudio del cibercrimen, proponiendo la categorización de estos delitos dentro de un espectro. En un extremo de esta categorización se encuentran los delitos tipo I, caracterizados por su naturaleza eminentemente técnica y dependiente de la tecnología, entre los que se incluirían actividades como la piratería. En el otro extremo encontramos los delitos de tipo II, que implican un mayor grado de interacción humana, como el fraude online. Lo interesante de esta clasificación es que subraya el debate existente entre concebir el cibercrimen bajo categorías fijas o entenderlo como un espectro donde los extremos representan la integración o la necesidad tecnológica en la comisión del delito, sugiriendo una conceptualización más matizada que la que aportan categorías estancas.

2.1.1 Clasificación del cibercrimen

En cuanto a la categorización del cibercrimen, un aporte notable fue el realizado por McGuire y Dowling en 2013, quienes ofrecen una distinción esencial entre dos categorías de cibercrimen: los crímenes ciberdependientes y los crímenes ciberhabilitados. La primera categoría engloba aquellos delitos que sólo pueden realizarse a través de un dispositivo electrónico o cualquier otra forma de tecnología de la información, refiriéndose a delitos intrínsecamente ligados al entorno digital. La segunda, en cambio, comprende delitos tradicionales cuya escala o alcance se ven significativamente aumentados por el uso de estas herramientas, aunque también podrían realizarse sin ellas.

Una de las categorizaciones más aceptadas es la de Miró-Llinares (2012), que distingue entre ataques puros, ataques réplica y ataques de contenido. Los ciberataques puros abarcan un amplio espectro de actividades delictivas que se

ejecutan exclusivamente en el mundo virtual. Entre ellos, destaca el hacking, una práctica donde un individuo, sin autorización, accede a sistemas o equipos informáticos de forma remota, permitiéndose explorar o extraer información a su antojo. Dentro de este tipo de ciberdelitos, otro desafío significativo proviene de las infecciones de malware y sabotajes cibernéticos, que engloban la infección de dispositivos con virus u otros métodos destructivos. Estas infecciones pueden tener fines industriales o, en otros casos, están diseñadas para causar daño individual. En esta línea se encontraría a proliferación del ransomware, en el cual los delincuentes cifran datos, bloqueando el acceso al usuario a su dispositivo o cuenta y exigen un rescate para su liberación. De forma similar, el uso de redes sociales sin autorización del titular plantea cuestiones complejas relacionadas con la privacidad y la seguridad de los datos. Por último, dentro de estos ciberataques puros, encontramos el concepto de antisocial networks para hacer referencia a la manipulación de las redes sociales con el objetivo de facilitar comportamientos criminales posteriores. Esto puede incluir la creación de perfiles falsos o la difusión de información engañosa con fines delictivos, desencadenando una serie de desafíos en la era digital. En contraste, los ciberataques de réplica no dependen exclusivamente de la tecnología ya que podrían efectuarse sin esta, pero aprovechan su alcance y facilidad de ejecución en el mundo digital. En esta categoría, los ciberfraudes son especialmente notorios, utilizando las TIC como herramientas para obtener ganancias a expensas de las víctimas. Esto incluye, entre otros, las estafas de inversión, ventas en línea fraudulentas, phising y los ataques de scam, mediante el que se envían mensajes o correos electrónicos que prometen beneficios financieros a cambio de una inversión inicial. Así mismo, el robo de identidad y la suplantación de identidad son preocupantes modalidades de fraude en las que los delincuentes adquieren datos personales con el propósito de cometer actos delictivos. Estos delitos no solo conllevan un prejuicio patrimonial, sino que pueden afectar a otros bienes jurídicos. Así mismo, dentro de los ciberataques de réplica encontramos el ciberespionaje, cuyo objetivo es la obtención de datos relevantes, ya sea de una empresa o de individuos, como mensajes privados o fotografías. Puede llevarse a cabo mediante la intrusión directa de un hacker en el sistema informático o a través de la distribución de software o spyware que se descarga en el dispositivo de la víctima sin su

conocimiento. En este mismo ámbito, el ciberblanqueo de capitales se convierte en una preocupación significativa, donde las actividades como el juego en línea y la extorsión se utilizan como medios para solicitar pagos económicos a cambio de no ser víctimas de un ciberataque. En cuanto al ciberacoso, abarca un amplio espectro de comportamientos que, a través de diversas herramientas de comunicación en línea, buscan atentar contra la libertad y la integridad de otras personas, presentando un desafío en términos de protección y seguridad en línea, ya que a diferencia de lo que ocurre en el contexto físico, cuando el acoso se da en línea la víctima se ve expuesta sin tener en cuenta las limitaciones de tiempo espacio. Por último, los ciberataques de contenido implican estrategias maliciosas centradas en la manipulación o explotación del contenido digital para propósitos delictivos. Estos ataques pueden abarcar desde la difusión de desinformación y noticias falsas, diseñadas para engañar o manipular la opinión pública, hasta la creación de materiales digitales alterados, como los deepfakes, que buscan desacreditar o extorsionar a individuos. Además, la integridad de sitios web y plataformas puede ser comprometida para incluir contenido malintencionado o alterar el ya existente.

Pese a las diferentes clasificaciones que podamos de los ciberdelitos, es un hecho que estas no pueden ser categorías estrictamente estancas ya que los ciberdelincuentes demuestran una notable capacidad de adaptación a los avances tecnológicos, como lo evidencia la reciente integración de la inteligencia artificial, y a los cambios en el contexto social, tal como se observó durante la pandemia de COVID-19 (Alawida et al., 2020). Los fraudes constituyen uno de los tipos de ciberdelitos que más rápidamente se ajustan a estos cambios. Se entiende por fraude cualquier engaño o intento de engaño que un individuo dirige hacia otro, prometiendo bienes, servicios o valores que no existen o que están significativamente distorsionados. Por tanto, el elemento esencial del fraude es el engaño (Titus, 2001), cuyo propósito es obtener un beneficio de la víctima, ya sea en forma de dinero, datos financieros o información personal. Holtfreter et al. (2016) resaltan que el fraude se caracteriza por requerir una comunicación entre víctima y delincuente, interacción que, como Cross (2013) apunta, puede conducir a que la víctima experimente sentimientos de autoculpabilidad. Aunque el fraude es un delito presente tanto en ambientes físicos como digitales, en el ámbito cibernético adopta formas particulares, como sucede en el fraude romántico, en el

cual la víctima es engañada a través de lo que cree que es una relación amorosa genuina, pese a no haber establecido interacción física con la persona que realiza la estafa.

2.2.2 Desafíos en la legislación y la medición del cibercrimen

Como se ha analizado previamente, la propia dinámica global del cibercrimen plantea desafíos significativos para un marco legal unificado. La Convención de Budapest (2001) se erige como un hito en el intento de establecer un terreno común para el enfrentamiento del cibercrimen, siendo el primer tratado internacional destinado a abordar esta problemática desde una perspectiva transfronteriza. Este Convenio tiene como objetivo principal armonizar las leyes nacionales en materia de ciberdelincuencia, mejorar las técnicas de investigación utilizadas por las autoridades nacionales, y aumentar la cooperación internacional en la lucha contra la ciberdelincuencia y establece medidas y procedimientos específicos para la detección, investigación y enjuiciamiento de delitos informáticos. Una parte crucial del documento reside en su énfasis en la cooperación internacional para combatir la ciberdelincuencia. Sin embargo, la eficacia de dicho tratado se ve comprometida por la ausencia de adhesión por parte de actores internacionales clave, como Rusia y China, evidenciando una fragmentación en la cooperación internacional que impide un abordaje efectivo y unificado del cibercrimen a nivel global (Gercke, 2015). Esta situación no solo genera vacíos legales, sino que también obstaculiza la cooperación internacional, esencial para la investigación y persecución del ciberdelito, siendo una de sus características que no cuentan con limitaciones físicas.

Además, la diversidad en la conceptualización del cibercrimen ya no sólo entre diversos países, sino dentro de la misma comunidad, añade otra capa de complejidad a la implementación de medidas legales unificadas. Esta disparidad no solo entorpece la implementación de estrategias conjuntas, sino que también limita la capacidad de las naciones para responder de manera efectiva a las amenazas cibernéticas que evolucionan y se adaptan a los cambios de forma constante. Es evidente que la velocidad sin precedentes a la que avanza la tecnología presenta un reto formidable para la creación y actualización de marcos legales. La legislación,

por su naturaleza, requiere de tiempos de desarrollo y procesos de aprobación que no se corresponden con el ritmo de innovación tecnológica, resultando en normativas que se vuelven obsoletas casi tan pronto como son promulgadas. Es precisamente esta discordancia entre la evolución tecnológica y la capacidad de adaptación legal uno de los factores que puede ser, y de hecho lo es, explotado por los ciberdelincuentes, dificultando aún más la persecución y sanción de estas actividades delictivas una vez se han llevado a cabo (Clough, 2015).

Más allá del ámbito legislativo, la medición del cibercrimen desde una perspectiva metodológica se enfrenta a obstáculos significativos que desafían nuestra capacidad para comprender completamente su alcance y naturaleza. Entre los métodos comúnmente utilizados, las encuestas de victimización y los informes generados por empresas de ciberseguridad destacan por sus contribuciones, pero también por sus limitaciones intrínsecas. Las encuestas de victimización dependen en gran medida de la auto-notificación de las víctimas, un enfoque que plantea varios desafíos (Button et al., 2014). Por un lado, la auto-notificación puede no ser exhaustiva, fallando en capturar la gama completa y la complejidad de los cibercrímenes. Esto se debe a varios factores, incluyendo el desconocimiento de las víctimas sobre su situación, es decir, muchas personas afectadas por cibercrímenes pueden no ser conscientes de su victimización debido a la sofisticación o el sigilo de los ataques. Por otro lado, el estigma asociado a ser víctima de ciertos cibercrímenes puede inhibir a las personas de reportar o reconocer que han sido afectadas, contribuyendo a una subestimación significativa de la prevalencia de estos delitos. Además, los informes de empresas de seguridad cibernética, aunque valiosos, tienden a estar sesgados hacia incidentes que son más fáciles de detectar o más propensos a ser reportados. Estos informes raramente proporcionan una visión completa de la diversidad de tácticas y objetivos empleados por los ciberdelincuentes, ya que las empresas pueden no tener acceso a información sobre ataques no detectados o técnicas emergentes que todavía no se han generalizado.

Por tanto, la variabilidad en las herramientas y métodos de detección utilizados por diferentes organizaciones agrava este problema, dificultando la comparación de datos y la construcción de un cuadro coherente del paisaje del cibercrimen. Otro

aspecto crítico que complica la medición del cibercrimen es la heterogeneidad de las metodologías de investigación. La falta de un estándar unificado para la recolección y análisis de datos sobre cibercrímenes hace que la comparación de resultados entre diferentes estudios sea particularmente desafiante. La variabilidad en las definiciones operacionales de lo que constituye un "cibercrimen", junto con diferencias en las poblaciones de estudio, intervalos de tiempo, y técnicas de muestreo, pueden llevar a interpretaciones divergentes sobre la magnitud y características del problema.

2.2 CIBERVICIMIZACIÓN Y PROBLEMÁTICA DE LA CIFRA NEGRA

2.2.1 Victimología y cibervictimización

El término "Victimología" constituye un neologismo derivado de la palabra inglesa “Victimology”, cuyo origen se data de la década de 1940. Desde su concepción inicial, esta disciplina ha sido entendida y desarrollada como el estudio científico centrado en las víctimas, abordando tanto sus dinámicas personales como las interacciones y consecuencias derivadas de su condición asociada a la victimización (Wallace & Roberson, 2015). Desde una perspectiva rigurosamente terminológica, el psiquiatra y criminólogo estadounidense Frederick Wertham fue pionero en introducir el término "victimología" dentro del ámbito científico, especialmente a través de su obra *The Show of Violence*. Posteriormente, en 1948, Benjamin Mendelsohn en su libro *The Criminal and His Victim* enriqueció el campo con el desarrollo de un enfoque más participativo sobre la relación entre la víctima y el victimario. Mendelsohn articuló el concepto de "victimización", proponiendo una perspectiva donde la víctima desempeña un rol activo en la creación y configuración de su agresor, centrándose en características específicas —como ser mujer o de edad avanzada— que podrían incrementar su vulnerabilidad. Por tanto, las primeras teorías referentes a la victimología sostenían que las víctimas desempeñaban un papel importante en la comisión del delito, ya que, aunque fuera de forma inconsciente, propiciaban una situación adecuada para que se llevase a cabo el acto delictivo (Fattah, 1991). Así, Von Hentingen (1948) clasificaba la vulnerabilidad de la víctima en términos personales, relacionales y contextuales y

consideraba que la víctima, de una forma u otra, podía evitar su victimización al modificar su comportamiento o al interactuar de una forma diferente con el delincuente (Fisher y Lab, 2010). Sin embargo, estas teorías iniciales también fueron objeto de críticas, particularmente por su tendencia a culpabilizar a las víctimas. Se identificaron limitaciones significativas en estos enfoques, tales como una excesiva dependencia de ideologías, arbitrariedad en sus planteamientos, déficits en la descripción fenomenológica de la victimización, circularidad argumentativa y una marcada carencia de solidez empírica. Además, se argumentó que la base teórica de estas primeras formulaciones de la victimología podía, inadvertidamente, legitimar la victimización y facilitar su aceptación social, presentando así desafíos éticos y metodológicos significativos dentro de la disciplina.

En la actualidad, la victimología se concibe como una ciencia multidisciplinar enfocada en el estudio de los procesos de victimización, abarca el análisis de cómo una persona puede convertirse en víctima y examinando las distintas dimensiones de la victimización —primaria, secundaria y terciaria— junto con las estrategias para su prevención y mitigación y se ocupa del estudio de las respuestas sociales, legales y asistenciales dirigidas hacia la reparación y reintegración social de las víctimas (Baca et al., 2006). En el contexto español, la Sociedad Española de Victimología, fundada en 2004, estableció en sus estatutos una clara diferenciación entre una visión amplia de la "victimología" y una perspectiva más limitada, optando por una definición de carácter ecléctico (Baca et al., 2006). Desde la perspectiva más restringida se define como víctima a cualquier persona que, de manera directa o indirecta, haya experimentado las consecuencias de un acto delictivo, independientemente de que haya sido formalmente reconocida como tal por un órgano jurisdiccional. De forma más amplia, se extiende el término a aquellas personas afectadas por las secuelas de guerras, enfrentamientos armados, catástrofes naturales o accidentes, reflejando un enfoque inclusivo que trasciende los límites del delito para abarcar otras formas de sufrimiento y daño. Por tanto, actualmente, debido a la complejidad inherente al término "victimización", se distinguen tres categorías principales: victimización primaria, secundaria y terciaria.

La victimización primaria se refiere a aquellos daños, tanto físicos como psicológicos, que una persona experimenta directa o indirectamente como resultado de un delito o un evento traumático. La victimización secundaria, por otro lado, alude a las consecuencias adversas que experimenta la víctima derivada de su interacción con el sistema penal y el proceso de enjuiciamiento. Este concepto engloba los efectos negativos resultantes de prácticas como interrogatorios por parte de la policía o el poder judicial, exámenes médico-forenses, o el enfrentamiento directo con el ofensor durante el juicio. Por último, la victimización terciaria se relaciona con los costes y consecuencias de la penalización del delito, ya sea para la persona directamente afectada, terceros, o la sociedad en su conjunto. Este concepto subraya la importancia de considerar tanto los costes sociales del delito como aquellos derivados de la penalización del infractor, incluyendo, por ejemplo, los estudios sobre los niveles de ansiedad de los reclusos, el impacto en los hijos de mujeres encarceladas, o las repercusiones económicas y emocionales para aquellos que dependen de alguien que ha sido encarcelado (Echeburúa et al., 2006).

Los diferentes modelos teóricos referidos a la victimología, se han ocupado del estudio en torno a diversos factores críticos que son esenciales para describir y evaluar los procesos de victimización. Estos elementos se pueden clasificar en varias categorías principales (Echeburúa et al., 2006):

- Factores individuales: Esta categoría abarca las diferencias personales significativas, como la edad, el género y las características de la personalidad, que pueden influir en cómo un individuo responde a un evento traumático. La personalidad, por ejemplo, puede afectar la manera en que una persona adapta estrategias frente a situaciones traumáticas, potencialmente incrementando el riesgo de victimización repetida y, en algunos casos, conduciendo a una victimización crónica. Dentro de estos factores también se incluyen aquellos riesgos que se adquieren a través del aprendizaje, como la indefensión aprendida o la adopción de roles específicos.

- Comportamiento de la víctima: Este aspecto se centra en cómo el estilo de vida de la víctima y sus comportamientos pueden exponerla a mayores riesgos de victimización. La exposición a situaciones peligrosas, la adopción de comportamientos de riesgo, las asociaciones diferenciales y las adicciones (como al alcohol y a las drogas) se consideran factores significativos que pueden aumentar la vulnerabilidad de una persona a ser víctima y su resistencia a desmitificar tales situaciones.

- Los ofensores: Las características del ofensor, la relación entre ofensor y víctima, y las motivaciones para seleccionar a una víctima específica son, en ciertos casos, fundamentales para entender la victimización. La elección de víctimas se explica, en parte, por estas consideraciones, junto con la oportunidad, sugiriendo que ciertos incidentes de victimización pueden ser entendidos a través del análisis de estos elementos.

- Oportunidad: Los factores de oportunidad representan elementos externos que explican significativamente la ocurrencia de la victimización. De particular interés son la ausencia o escasez de recursos de seguridad y la peligrosidad de ciertos lugares y momentos, que aumentan las probabilidades de ser víctima de un delito.

- Factores sociales: Esta categoría engloba todos aquellos riesgos derivados de la estructura social, incluyendo los elementos ambientales, la privación, la estigmatización, o la marginación de ciertos grupos, lo que facilita su identificación como blancos potenciales de agresión. La reacción del entorno frente al delito también juega un rol crucial, donde el grado de reconocimiento y apoyo emocional pueden moderar el impacto del delito en la víctima.

A pesar de que las clasificaciones modernas tienen como objetivo eliminar la responsabilidad de la víctima en el delito, persiste esta percepción en ciertas categorías delictivas, entre los que encontramos en el fraude (Cross, 2015). Ciertos estereotipos negativos en la sociedad fomentan la percepción de las víctimas de fraude como personas codiciosas y fácilmente “engañables”, contribuyendo así a

una cierta culpabilización. Este estigma no solo perdura entre el público general sino también entre quienes han sufrido fraude, lo que indica una internalización del discurso que les asigna culpa (Cross, 2013; 2015). Estas concepciones pueden exacerbar el daño causado por el delito y reducir la posibilidad de que los incidentes de fraude sean notificados (Cross, 2015; Cross et al., 2016), incrementando así la cifra negra en ciertos delitos.

En el ámbito del Cibercrimen, pese al esfuerzo de desvincular a la víctima de responsabilidad debemos tener en cuenta que en el ciberespacio la víctima juega un papel crucial tanto en la explicación como en la prevención del delito por tres razones fundamentales (Miró-Llinares, 2012). La primera es la decisión de la víctima de utilizar determinadas herramientas tecnológicas, ya que esto puede incrementar su situación de vulnerabilidad frente a determinados riesgos. Es evidente que los que no son usuarios de Internet no pueden ser objetivo de ciberdelitos. En segundo lugar, el nivel de interacción con las nuevas tecnologías y su integración en la vida cotidiana, que determina el grado de riesgo que la persona asume. Y, por último, en el contexto del cibercrimen, las víctimas tienen la responsabilidad exclusiva de establecer medidas de protección contra estos delitos, dada la ausencia de barreras físicas o sistemas institucionales de seguridad globales. Respecto a este último punto, a pesar del aumento en el uso de las TIC, encontramos un gran número de personas que no implementan medidas de protección adecuadas, lo que podría deberse tanto a una preocupación limitada por el cibercrimen (Miró-Llinares, 2012), como al nivel de conocimiento sobre el funcionamiento del cibercrimen y la implementación de medidas de seguridad, algo especialmente relevante en PAM (Cross, 2017).

2.2.2 Prevalencias y cifra negra

En la última década, hemos observado un incremento notable en la prevalencia del cibercrimen, con los adultos mayores emergiendo como uno de los grupos afectados por este tipo de delitos. De hecho, las estadísticas demuestran una tendencia inquietante, incrementada tras la pandemia debido a la COVID-19: mientras otros delitos realizados en el ámbito físico han mostrado una

disminución, los ciberdelitos muestran un incremento. Más que una mera transición de los delincuentes del ámbito físico al ciberespacio lo que se ha observado es una adaptación de los cibercriminales a las emergentes oportunidades delictivas presentadas tras la situación derivada de la COVID-19. Adicionalmente, se ha producido una reorientación de las oportunidades delictivas hacia el ciberespacio, impulsada por un aumento significativo en el tiempo y en la cantidad de actividades realizadas en línea, fenómeno que podría haber contribuido a una escalada en la prevalencia de determinados ciberdelitos (Miró-Llinares, 2021). Dentro del amplio espectro de la ciberdelincuencia, las estafas y los fraudes son consistentemente identificados como los delitos más prevalentes. Este patrón se observa en diversos contextos internacionales, evidenciando la adaptabilidad y persistencia de estas formas de criminalidad en el entorno digital. Los estudios indican que estos tipos de delitos no solo son comunes, sino que también muestran una tendencia creciente, exacerbada por factores como el aumento en la digitalización de las actividades económicas y sociales y la proliferación de plataformas en línea que facilitan interacciones anónimas o poco reguladas. Por ejemplo, en España, el estudio más reciente realizado en 2022 por el Ministerio del Interior sobre cibercriminalidad indica que el fraude en línea es más común de los delitos que se producen en el ciberespacio, llegando a representar el 89,7% de todos los ciberdelitos (Ministerio de interior, 2022). Debemos tener en cuenta que, si consideramos que la sociedad actual es marcadamente distinta a la de hace unas décadas, observamos que los delincuentes que cometen fraudes simplemente se adaptan a estos cambios y utilizan las herramientas disponibles. Este comportamiento sigue una dinámica similar a otros cambios observados en el ámbito del cibercrimen a lo largo del tiempo. Una razón plausible para el incremento constante en el número de delitos relacionados con el fraude en línea es la rápida difusión de información sobre cómo perpetrar estos actos. El nivel de conocimientos informáticos requerido para ejecutar estas estafas está disminuyendo, y las herramientas necesarias se han vuelto más accesibles (Miró Llinares, 2012). Este entorno facilita que los delincuentes transformen y actualicen los delitos tradicionales, adaptándolos al mundo digital y afectando a múltiples víctimas en un breve periodo de tiempo. Adicionalmente, otro factor que contribuye a la proliferación de fraudes informáticos es la facilidad con la que se

puede obtener información personal almacenada en dispositivos electrónicos ya que frecuentemente, datos personales como números de identificación o cuentas bancarias están almacenados en ordenadores personales o dispositivos móviles con conexión a internet, facilitando a los ciberdelincuentes el acceso a esta información.

Si nos centramos en la población adulta mayor, este aumento en la cibervictimización en comparación con décadas anteriores se puede atribuir, entre otros factores, al crecimiento exponencial en la adopción de internet por parte de este grupo etario. En cuanto a su mayor o menor probabilidad de convertirse en víctimas de fraude online, pese al debate existente en la literatura académica respecto a si las personas adultas mayores son más susceptibles a ser víctimas de fraude en comparación con los grupos más jóvenes (Ross et al., 2014), si existe un consenso generalizado sobre el hecho de que el fraude es el tipo de delito más frecuentemente experimentado por este grupo etario (Smith & Budd,2009).

La realidad es que la situación de vulnerabilidad de los adultos mayores respecto al ciber fraude es un fenómeno complejo y multifacético, donde varios factores interrelacionados juegan un papel crucial. Por un lado, el posible deterioro cognitivo, que provoca disminuciones en diversas capacidades conforme avanza la edad, afecta a áreas cruciales como la memoria, la velocidad de procesamiento de la información, la resolución de problemas, las habilidades matemáticas y el funcionamiento ejecutivo (Nyberg & Bäckman, 2011). Conjuntamente, se ha identificado que en algunos casos se da una disminución de la materia blanca y gris, que cuando se asocia con deterioro en la corteza prefrontal ventromedial, puede influir negativamente en la toma de decisiones relacionadas con el riesgo, además de asociarse con una mayor credulidad y sugestión (Asp et al., 2013). Adicionalmente, las evaluaciones forenses indican que el deterioro cognitivo leve es un factor que incrementa directamente el riesgo de ser defraudado, sugiriendo una conexión directa entre la capacidad cognitiva reducida y la mayor incidencia de fraude (DeLiema, 2018; Ueno et al., 2021; Wood et al., 2014) Esta situación puede verse agravada por la tendencia de los adultos mayores a confiar excesivamente, así como por su vulnerabilidad psicológica y su posible aislamiento social, factores

que se combinan para crear un entorno propicio para la victimización (Shao et al., 2019).

Por tanto, los factores emocionales y sociales ejercen una influencia considerable en la susceptibilidad al fraude, afectando significativamente la capacidad de los individuos para procesar información y tomar decisiones informadas. En particular, la excitación emocional puede debilitar sustancialmente la capacidad de los adultos mayores para discernir anuncios engañosos, disminuyendo notablemente su habilidad para identificar fraudes, especialmente en contextos que generan inseguridad y desorientación (Kircanski et al., 2016). Este fenómeno es particularmente preocupante ya que la capacidad para identificar tales engaños es crítica y por tanto para evitar la victimización en un ambiente cada vez más digitalizado y lleno de información potencialmente engañosa. Adicionalmente, el aislamiento social, reflejado en la escasez de relaciones cercanas, amplifica esta vulnerabilidad, ya que, sin un sistema de apoyo robusto, estos individuos pueden ser más susceptibles a las influencias de operadores fraudulentos que buscan explotar su soledad y desconexión para fines maliciosos (DeLiema, 2018), siendo la soledad auto percibida otro factor que contribuye a este incremento de la vulnerabilidad (Alves & Wilson, 2008). Finalmente, debemos tener en cuenta que la naturaleza del fraude varía con la situación económica que presenta la víctima, en este caso las personas adultas mayores. Aquellos con mayor riqueza pueden ser especialmente susceptibles a fraudes vinculados con inversiones, mientras que aquellos con menos recursos inmobiliarios pueden tener una mayor vulnerabilidad relacionada con fraudes que prometen premios (DeLiema et al., 2020). Además, no podemos olvidar, que este contexto puede complicarse todavía más debido a la falta de conocimientos adecuados sobre la prevención de fraudes, lo que subraya la importancia de abordar la problemática del fraude contra adultos mayores de forma holística, considerando tanto los aspectos cognitivos, emocionales y sociales, como económicos.

En cuanto a los delitos más prevalentes dentro de esta categoría entre las personas mayores, encontramos el phishing y la suplantación de identidad (identity theft), las estafas de soporte técnico, las estafas relacionadas con compras y los fraudes románticos. Referido al phishing y la suplantación de identidad, ambos delitos

buscan obtener acceso a información personal y financiera de forma fraudulenta, siendo esta forma de fraude particularmente insidiosa porque a menudo utiliza señuelos relacionados con instituciones financieras o servicios gubernamentales conocidos. En lo que respecta a las estafas de soporte técnico, estos delitos implican a criminales que se hacen pasar por técnicos de grandes compañías de software para ganar acceso a los sistemas informáticos de las víctimas. Dentro de los fraudes más comunes relacionados con las compras en línea encontramos la adquisición de productos que nunca son entregados y los anuncios falsos que a menudo aparecen en redes sociales o como anuncios emergentes en diferentes sitios web, prometiendo curas milagrosas para diversas dolencias o mejoras significativas en la salud con poco o ningún fundamento científico. Sin embargo, en muchos casos, los productos nunca son entregados o, si lo son, resultan ser completamente diferentes a lo que se prometía, careciendo de las propiedades o beneficios anunciados. Por último, los fraudes románticos son especialmente devastadores, no solo por las pérdidas económicas, sino también por el profundo impacto emocional en las víctimas. En este tipo de fraude, los estafadores estudian los perfiles de sus víctimas, seleccionando a aquellos que se encuentran en una posible situación de vulnerabilidad, como la viudez. Una vez que se establece la comunicación, los estafadores fingen interés romántico, comprensión y, a veces, promesas de un futuro juntos, lo cual puede ser particularmente efectivo con adultos mayores cuya soledad percibida es alta (Whitty, 2015). Posteriormente, los estafadores solicitan dinero a la víctima utilizando diversas situaciones, como emergencias médicas, problemas legales o aduaneros, planes de viaje o inversiones.

Es evidente que este tipo de delitos, los ciber fraudes, ocasionan un impacto significativo en diversas áreas como es en el ámbito económico. Los datos presentados por el Centro de Denuncias de Delitos en Internet (IC3) del Federal Bureau of Investigation (FBI) muestran un aumento significativo en las pérdidas económicas atribuibles a fraudes cibernéticos, particularmente entre personas de 60 años o más. Entre 2019 y 2022, las pérdidas monetarias en este grupo etario casi se triplicaron, y su participación en las pérdidas totales por delitos cibernéticos aumentó del 29% al 37%. Sin embargo, debemos tener en cuenta que las consecuencias de estos fraudes no se limitan a pérdidas económicas, también

pueden manifestarse como efectos físicos y psicológicos significativos, incluyendo alteraciones emocionales (Golladay & Holtfreter, 2017). El impacto psicológico no está necesariamente correlacionado con la magnitud de la pérdida económica; en algunos casos, incluso pérdidas financieras mínimas pueden desencadenar trastornos emocionales significativos que persisten a lo largo del tiempo. De forma similar a lo que ocurre con otros tipos de delitos, la respuesta emocional de las víctimas de fraudes muestra una amplia variabilidad y puede incluir una gama de síntomas como ansiedad, depresión y una disminución en la confianza sobre la capacidad propia, lo que puede afectar profundamente la calidad de vida y el bienestar general de las víctimas. Esta diversidad en las reacciones emocionales subraya la necesidad de adoptar intervenciones psicológicas individualizadas que reconozcan y aborden la singularidad de cada experiencia de victimización (Kemp & Moneva, 2020).

Sin embargo, a pesar de que el daño emocional y psicológico sufrido por las víctimas de fraude es comparable al de víctimas de otros delitos a los que se les da más visibilidad, estas víctimas no reciben el mismo nivel de atención por parte de los sistemas de justicia y de la sociedad en general. Esta discrepancia en la atención puede atribuirse, en parte, a las complejidades inherentes a la investigación de estos delitos. Los criminales frecuentemente operan desde el extranjero o utilizan métodos que dificultan su rastreo, lo que añade significativas barreras a la labor de las autoridades (Cross, 2020; Cross et al., 2014). El anonimato de los victimarios, junto con la dificultad de identificar a las víctimas, juega un papel crucial en complicar aún más la identificación y captura de los perpetradores. Además, en muchas ocasiones, especialmente en estafas de menor envergadura, los bancos optan por reembolsar los montos a sus clientes, lo que reduce la probabilidad de que se presenten denuncias formales. Esta práctica, aunque beneficia a las víctimas a corto plazo, puede contribuir a un ciclo de impunidad y falta de seguimiento legal, perpetuando la invisibilidad de estos delitos en el ámbito judicial y en la conciencia pública.

Adicionalmente, en el contexto de estos delitos, se observan actitudes que tienden a culpar a la víctima, tanto en personas que han sido víctimas como en otras personas del entorno. Esta tendencia no solo puede intensificar el impacto

emocional y psicológico de ser defraudado, sino que también puede suprimir la revelación de tales incidentes y actuar como un obstáculo significativo para obtener el apoyo necesario (Cross, 2015; Cross, et al., 2016). La estigmatización de las víctimas y la percepción de que deberían haber sido capaces de evitar el fraude por sí mismas desincentiva a muchos afectados de reportar los crímenes, buscar ayuda legal o incluso compartir su experiencia con otros, contribuyendo a un aislamiento que puede agravar su sufrimiento. Por tanto, este factor puede ser clave y afectar directamente a la cifra negra del fraude en línea, un fenómeno que ha capturado la atención de la literatura científica debido a la considerable discrepancia entre el número real de delitos cometidos y aquellos que son notificados o denunciados oficialmente. Esta discrepancia revela la verdadera extensión de un problema que afecta a toda la población, dado que muchas víctimas no informan de estos incidentes por diversas razones.

En línea con esta información, la Federal Trade Commission (FTC), que basa sus conclusiones en informes no verificados de usuarios acerca de fraudes económicos en línea, ha publicado recientemente un informe donde revela que en 2022 las pérdidas medias por fraude aumentan con la edad, pero curiosamente, la frecuencia de notificaciones disminuye. Así, el grupo de 30 a 39 años fue el que más informó de este tipo de delitos, mientras que las mayores pérdidas económicas se observaron en ciudadanos de 60 años o más.

Una de las principales razones detrás de la cifra negra en el fraude en línea, especialmente entre las personas mayores, es la ocultación motivada por vergüenza y culpa, ya que a menudo experimentan estas emociones tras haber sido engañadas en un fraude cibernético, lo que las lleva a mantener estos incidentes en secreto (Cross, 2015). La humillación de haber sido estafadas puede ser tan abrumadora que las víctimas evitan compartir su experiencia con amigos, familiares o autoridades, perpetuando así la subestimación de la verdadera magnitud de este problema. En un estudio realizado por Cross en 2016, se observó que las narrativas de las personas mayores respecto a su victimización por ciberfraude a menudo reflejan una percepción de deficiencia personal. Esto fomenta auto-discursos que actúan como una barrera significativa para la divulgación de la victimización a familiares y amigos, la subnotificación del fraude

a las autoridades y, en consecuencia, como un obstáculo para acceder a los servicios de apoyo necesarios para ayudar en la recuperación, tanto de daños financieros como no financieros.

2.3 PERCEPCIÓN DE SEGURIDAD EN LÍNEA Y MIEDO A LA CIBERVICTIMIZACIÓN

El miedo al crimen es un fenómeno multidimensional que ha suscitado atención a nivel global desde hace décadas que no se limita únicamente a las experiencias directas de victimización, sino que también incluye las reacciones emocionales subjetivas ante amenazas percibidas y diversos contextos que pueden generar inseguridad (Ferraro, 1995). Diversos estudios indican que el miedo al crimen, tanto en el entorno físico como en el digital, afecta a un sector significativo de la población, con variaciones según grupos de edad y género, entre otros factores. Sabemos que el miedo al crimen trasciende las experiencias individuales y puede impactar de forma negativa en el bienestar social, la educación, la economía y el acceso a recursos. A lo largo de este capítulo, se analizarán estos aspectos del miedo, abordando las causas y consecuencias de este fenómeno.

2.3.1 Miedo funcional y disfuncional al delito

El miedo al crimen es una preocupación omnipresente en muchas sociedades contemporáneas y su estudio resulta esencial para entender las dinámicas de seguridad y bienestar social. El término ha avanzado a lo largo de las últimas décadas, surgiendo en los últimos años una bifurcación del concepto y distinguiendo entre dos tipos principales: el miedo funcional y el miedo disfuncional.

La investigación sobre el miedo al crimen se originó en la década de 1960 en Estados Unidos y, desde entonces, ha sido un tema de estudio relevante en el campo de la criminología. En los años siguientes, países como Alemania y el Reino Unido comenzaron a llevar a cabo sus propias encuestas de victimización, considerando el miedo al crimen como un asunto criminológico de interés e incorporando preguntas destinadas a su medición (Lee & Mythen, 2018). Desde la aparición del término, se han propuesto múltiples definiciones, como la de Ferraro

(1995), quien lo definió como una respuesta emocional de ansiedad o nerviosismo tanto frente al crimen como a símbolos y contextos que podían asociarse a este. No obstante, a pesar de ser un término de uso frecuente en la criminología, se caracteriza por su notoria complejidad. Esta complejidad radica en la ausencia de una definición universalmente aceptada y en la falta de un entendimiento completo de todos los elementos que lo conforman, lo que complica significativamente su evaluación. Asimismo, la comparación de datos entre diversos estudios científicos resulta ardua debido a la variabilidad en las herramientas empleadas para su cuantificación, lo que plantea la posibilidad de que no se esté midiendo el mismo fenómeno en todos los casos. Adicionalmente, la dificultad para abordar esta variable se torna aún más acentuada cuando se traslada al ámbito digital, ya que este entorno constituye un fenómeno relativamente novedoso en la ecuación del temor al crimen. La creciente integración de la tecnología en la vida cotidiana y la evolución constante de las amenazas cibernéticas plantean desafíos adicionales en la definición y medición del temor a la ciberdelincuencia. Una dificultad añadida es la existencia de múltiples modalidades de cibercrimen, cada una de las cuales puede interactuar de manera diferente con la emoción del miedo (Castro Toledo, 2018). A su vez, la diversidad y los rápidos cambios intrínsecos al cibercrimen complica la tarea de desarrollar una comprensión integral del miedo al crimen en el contexto digital, ya que cada tipo de cibercrimen puede evocar diferentes niveles y formas de miedo. Además, la naturaleza intangible y a menudo anónima de las amenazas que pueden darse en el mundo digital puede intensificar el miedo, ya que los usuarios pueden sentirse indefensos frente a agresores invisibles y a menudo desconocidos.

Pese a esta complejidad, el miedo al crimen se define generalmente como una respuesta emocional negativa ante la posibilidad de ser víctima de un delito. Dentro de concepto se pueden incluir tres componentes principales: un factor emocional, que se refiere a la frecuencia e intensidad de la emoción; un componente cognitivo, basado en la percepción del riesgo de victimización; y un componente conductual, que se refiere a las precauciones tomadas para evitar el crimen. Por tanto, podemos afirmar que el miedo al crimen es una emoción subjetiva que implica múltiples variables y que no necesariamente correlaciona con la probabilidad objetiva de convertirse en víctima (Warr, 1987). Aunque

investigaciones previas sostenían que la victimización reciente estaba altamente correlacionada con la intensidad del miedo al crimen (Skogan, 1987), estudios más recientes no han encontrado esta relación (Chockalingam & Srinivasan, 2009), lo que genera resultados contradictorios. En cuanto a las diferencias por edad y género, las mujeres y las personas adultas mayores informan de niveles más altos de miedo pese a ser los hombres jóvenes más frecuentemente víctimas de delitos, subestimando estos últimos el nivel de riesgo o siendo más reacios a admitirlo debido a convenciones sociales (Sutton & Farral, 2005). Por tanto, actualmente podemos afirmar que la victimización directa no es el único factor que influye en el miedo al crimen ya que, además del elemento subjetivo, encontramos elementos del entorno, como una mayor presencia de grafitis o una menor iluminación, y sociales, como la influencia de los medios de comunicación y el discurso político, que juegan roles significativos en la amplificación de este miedo.

A pesar de que el concepto inicialmente tenía una connotación negativa, en las últimas décadas se ha subdividido en dos variantes distintas: un miedo disfuncional, que reduce la calidad de vida, y un miedo funcional, que permite tomar las precauciones necesarias para evitar el posible daño sin restringir excesivamente la libertad individual (Jackson & Gray, 2010).

Por un lado, cuando el miedo al crimen adopta una variante disfuncional, puede convertir a la persona en una víctima indirecta, limitando su capacidad para llevar a cabo ciertos comportamientos en diversas áreas de su vida (Narváez Mora, 2009). Las personas que experimentan este tipo de miedo pueden evitar salir de sus hogares, restringir sus actividades diarias y vivir en un estado constante de ansiedad y estrés. Por tanto, esta variante del miedo al crimen se caracteriza por una percepción exagerada del riesgo de victimización, que puede llevar a comportamientos irracionales y contraproducentes. Gabriel y Greve (2003) señalan que el miedo disfuncional puede conducir al aislamiento social, lo cual puede tener repercusiones negativas en la salud mental y física de los individuos a largo plazo. La literatura sugiere que esta variante del miedo al crimen puede perpetuar un ciclo vicioso donde el temor al crimen genera comportamientos que, paradójicamente, aumentan la sensación de inseguridad y la posibilidad de victimización (Ferraro, 1995). Este tipo de miedo también puede estar influenciado

por factores mediáticos, ya que la cobertura sensacionalista de los medios sobre crímenes violentos puede amplificar el temor al delito, creando una percepción distorsionada de la realidad que sobreestima la ocurrencia de actos delictivos. Por tanto, el consumo excesivo de noticias sobre crimen puede llevar a una sobreestimación del riesgo real, exacerbando el miedo disfuncional (Dowler, 2003).

Por otro lado, en el caso del miedo funcional, las personas adoptan precauciones para protegerse y, al hacerlo, experimentan una mayor sensación de seguridad, sin que su miedo tenga un impacto negativo en su calidad de vida (Jackson & Gray, 2010). Esta variante se traduce en comportamientos beneficiosos y proactivos para la persona, donde incorporan medidas preventivas en su rutina diaria que disminuyen la probabilidad de convertirse en víctimas, como podría ser instalar un sistema de seguridad en su hogar. Por tanto, el miedo funcional fomenta una actitud que esta enfocada a la realización de conductas o prácticas que incrementan la seguridad personal y reducen el riesgo de victimización sin que ello restrinja excesivamente la libertad y el bienestar de los individuos. Este enfoque permite que las personas mantengan un alto nivel de calidad de vida mientras se sienten protegidas, logrando así un equilibrio entre precaución y libertad. Por ende, el miedo funcional puede ser una herramienta efectiva para la prevención del delito si se canaliza a través de políticas públicas y estrategias de prevención adecuadas (Castro Toledo, 2019).

Si adaptamos estos conceptos al entorno digital, encontramos que los individuos que experimentan la variante funcional del miedo al ciberdelito implementarán prácticas de protección efectivas. Estas prácticas incluyen el uso de contraseñas robustas, la instalación de software de detección de virus informáticos, la actualización regular del software en los diferentes dispositivos con los que se accede a internet y la cautela al compartir información personal por medios digitales. En contraste, el miedo disfuncional puede llevar a la evitación del uso de tecnología, ya que estas personas pueden llegar a desconfiar tanto de las plataformas en línea que evitan participar en actividades digitales que podrían mejorar su calidad de vida, como transacciones bancarias en línea, compras por internet o el uso de redes sociales. En este contexto, es pertinente mencionar la Teoría de la Motivación de Protección (TMP) (Maddux & Rogers, 1983; Rogers,

1975), la cual se ha empleado recientemente como marco teórico para estudios sobre el uso seguro de Internet (Briggs et al., 2017; Giwah, 2018; Martens et al., 2019). Tal como asume esta teoría, la motivación de un individuo para protegerse depende tanto de su evaluación de la amenaza como de la percepción de su capacidad para enfrentar dicha amenaza. La evaluación de la amenaza consta de dos componentes principales: en primer lugar, la gravedad percibida de la amenaza; y, en segundo lugar, la vulnerabilidad percibida del individuo ante esa amenaza. Por su parte, la evaluación de la capacidad de afrontamiento involucra tres factores: primero, la capacidad percibida del individuo para responder a la amenaza; segundo, la eficacia percibida de esta respuesta frente a la amenaza; y, finalmente, el costo asociado a la respuesta. Es evidente que existe un notable solapamiento entre las construcciones que conforman la TMP y la teoría del autocontrol, desarrollada por Gottfredson y Hirschi en 1990. La teoría del autocontrol postula que los individuos con bajo autocontrol tienden a actuar de manera impulsiva, sin considerar adecuadamente las consecuencias a largo plazo de sus acciones. Por tanto, un individuo con bajo autocontrol tiende a no evaluar con precisión los riesgos potenciales y a sobreestimar su capacidad para responder a ellos, por lo que su motivación para protegerse no es adecuada frente a las amenazas que enfrenta. Esto implica que, a pesar de reconocer la amenaza, la falta de autocontrol impide una respuesta efectiva y adecuada, lo que subraya la importancia de considerar tanto la evaluación de la amenaza como la capacidad de afrontamiento en la promoción de comportamientos protectores o el fomento del miedo funcional.

La integración de estos marcos teóricos proporciona una comprensión más profunda de cómo el miedo al ciberdelito y las habilidades de afrontamiento interaccionan, influyendo directamente en la conducta de protección y pudiendo adoptar una variante funcional o disfuncional. Esta perspectiva teórica no solo ayuda a explicar las variaciones en la respuesta al ciberdelito, sino que también ofrece una base sólida para diseñar intervenciones que mejoren la seguridad digital y promuevan comportamientos protectores efectivos.

2.3.2 Definiciones de inseguridad

En este punto, resulta oportuno distinguir el miedo al crimen de una variable concomitante: la inseguridad. La percepción de inseguridad constituye una variable subjetiva que generalmente se relaciona con el contexto o el entorno físico y se ve influida por factores personales, sociales y ambientales (Valera & Guàrdia, 2014). Es un concepto más amplio que el miedo al delito ya que no se centra únicamente en el temor a convertirse en víctima, sino que también abarca el sentirse inseguro y carecer de control en un entorno específico, aunque esto no implique una posible victimización.

Basado en el trabajo de Fernández y Corraliza (1997), se ha desarrollado un modelo que marco comprensivo para entender cómo diversos elementos interactúan para formar la percepción de inseguridad en los individuos comprende tres factores principales vinculados a la percepción de inseguridad: 'Competencias personales para afrontar', 'Representación del espacio' y 'Entorno peligroso' (Carro et al., 2010). En cuanto a las *competencias personales para afrontar* estas están directamente relacionadas con la vulnerabilidad personal y las estrategias de afrontamiento disponibles para el individuo. Este factor se desglosa en varios componentes clave:

- Vulnerabilidad personal: Este componente abarca variables demográficas tales como el género, la edad y el estado de salud. Por ejemplo, las mujeres y las personas de edad avanzada suelen reportar mayores niveles de inseguridad debido a percepciones incrementadas de vulnerabilidad.

- Estrategias de afrontamiento cognitivas y sociales: Se refiere a las habilidades que los individuos perciben tener para gestionar situaciones potencialmente complejas o riesgosas. Esto incluye tanto la autopercepción de habilidades para afrontar la situación (como la confianza en la propia capacidad de respuesta) como el apoyo social disponible (redes de apoyo de familiares y amigos).

- Control emocional: Este componente está vinculado con la capacidad del individuo para manejar sus emociones en situaciones desafiantes. Un mayor control emocional puede mitigar la percepción de inseguridad.

- Control conductual: Incluye la capacidad de autodefensa activa y las medidas preventivas que el individuo puede tomar ante situaciones desafiantes.

Referido al segundo factor, *la representación del espacio*, este engloba las experiencias y percepciones que los individuos tienen sobre un entorno determinado. Al igual que el factor anterior, se descompone en varios elementos:

- Experiencias previas en el espacio: Las experiencias anteriores de los individuos en un área o contexto específico pueden influir significativamente en su percepción de inseguridad.

- Representaciones previas del espacio: Estas son las percepciones y creencias preexistentes sobre un entorno concreto, que pueden estar influidas por información mediática, estereotipos y narrativas sociales.

- Influencia social: Las percepciones del entorno también están moldeadas por la información y las opiniones compartidas dentro de la comunidad y los medios de comunicación.

En cuanto al último de los factores, *entorno peligroso*, está directamente relacionado con las características físicas y sociales del entorno, así como con los indicadores de peligrosidad presentes en este.

Al trasladar este modelo al entorno digital, se puede observar cómo estos factores tienen la capacidad de influir en la percepción de inseguridad en línea. Algunos autores sugieren que uno de los aspectos relacionados con una mayor o menor percepción de inseguridad en la red es el desarrollo tecnológico a nivel nacional (Cook et al., 2022). Este planteamiento sugiere que las naciones que invierten tanto en infraestructura tecnológica como en ciberseguridad pueden experimentar una disminución del temor en la población en relación con la ciberdelincuencia

económica, contribuyendo a la percepción de un entorno en línea más seguro y protegido. Adicionalmente, la percepción de inseguridad en el entorno digital puede estar influenciada por la calidad de la educación en ciberseguridad que reciben los usuarios. La alfabetización digital y el conocimiento sobre prácticas seguras en línea son fundamentales para mitigar el miedo al ciberdelito. Asimismo, la falta de habilidades digitales puede incrementar la tanto la inseguridad como la vulnerabilidad percibida y, en consecuencia, el miedo al ciberdelito (Van Deursen & Van Dijk, 2014). Por tanto, programas que busquen fomentar las capacidades tecnológicas y el conocimiento en ciberseguridad, adaptados a las poblaciones concretas a las que se dirigen, pueden empoderar a los usuarios, reduciendo su percepción de riesgo y aumentando su capacidad de respuesta ante amenazas digitales. Asimismo, el entorno regulatorio y las políticas de protección de datos juegan un papel crucial. La implementación de leyes estrictas de protección de datos y la existencia de agencias dedicadas a la ciberseguridad pueden aumentar la confianza de las personas usuarias de plataformas digitales. Un marco legal robusto que proteja a los ciudadanos contra el cibercrimen puede actuar como un factor disuasorio para los delincuentes, pero también ofrecer un sentido de seguridad a los usuarios (González-Granadillo et al., 2020).

Por lo tanto, como se ha analizado a lo largo de este capítulo, la existencia de un miedo disfuncional al ciberdelito y la percepción de inseguridad puede desincentivar el uso de herramientas digitales, representando un desafío significativo para la adopción de TIC entre las personas adultas mayores (Brands & Van Doorn, 2022; Chen & Zahedi, 2016; Vroman et al., 2015). Abordar estas preocupaciones e inseguridades requiere no solo la mejora de la formación en habilidades digitales entre los grupos vulnerables, sino también la concienciación sobre las amenazas más relevantes y sobre dónde y cómo conseguir apoyo para utilizar las TIC de forma segura. Esto podría minimizar significativamente los obstáculos hacia la inclusión digital y fomentar una interacción segura y efectiva con la tecnología.

CAPÍTULO 3: FUNDAMENTACIÓN TEÓRICA DEL CIBERCRIMEN

El estudio de la criminología ha experimentado una evolución significativa desde sus inicios, reflejando cambios profundos en la comprensión de las causas del crimen y en la formulación de políticas de prevención. El génesis de las teorías criminológicas modernas puede rastrearse hasta el trabajo del llamado “padre de la criminología”, Cesare Lombroso, un ilustre médico y criminólogo italiano del siglo XIX. Lombroso es ampliamente reconocido por su teoría del "criminal nato", la cual postulaba que ciertos individuos estaban biológicamente predispuestos al comportamiento criminal. Esta teoría se sustentaba en observaciones antropométricas y características físicas, argumentando que los delincuentes poseían rasgos atávicos que los diferenciaban de las personas no delincuentes (Lombroso, 1876). Lombroso sostenía que estos rasgos físicos, que incluían mandíbulas prominentes, brazos desmesuradamente largos y orejas de gran tamaño, eran indicadores de una regresión evolutiva a un estado primitivo. Su enfoque determinista sugería que el crimen era el resultado de factores biológicos inherentes, desatando una serie de debates sobre la dicotomía naturaleza versus crianza en la criminología. Aunque sus teorías fueron criticadas y eventualmente desacreditadas por su falta de rigor científico y sesgo racial, la labor de Lombroso sentó las bases para el desarrollo de la criminología como una disciplina científica. A medida que la criminología evolucionaba, las explicaciones biológicas y deterministas fueron gradualmente suplantadas por enfoques más multifacéticos que consideraban factores sociales, económicos y ambientales. Este cambio reflejaba una comprensión más compleja y matizada de las causas del crimen, reconociendo la importancia de las circunstancias contextuales en la conducta delictiva. Un desarrollo clave en este período fue la introducción de las teorías sociológicas, que subrayaban la influencia de factores externos sobre el comportamiento criminal. Entre estas teorías, una de las más destacadas es la teoría de la anomia de Robert K. Merton (1938). Merton postulaba que la estructura social de una sociedad puede inducir a los individuos a cometer delitos cuando existe una disyuntiva entre las metas culturalmente prescritas y los medios legítimos para lograrlas. Según Merton, en una sociedad que valora el éxito material y la prosperidad, pero que restringe el acceso a los medios legítimos para

alcanzarlos, los individuos pueden recurrir a medios ilícitos para cumplir con estas expectativas culturales. Merton identificó cinco modos de adaptación a esta disyuntiva entre metas y medios: conformidad, innovación, ritualismo, retraimiento y rebelión. La conformidad representa la aceptación tanto de las metas culturales como de los medios institucionales. La innovación, que es de particular relevancia para la criminología, implica la aceptación de las metas culturales, pero el rechazo de los medios institucionales, llevando a los individuos a buscar métodos alternativos, a menudo ilegales, para alcanzar el éxito. El ritualismo se refiere a la aceptación de los medios institucionales mientras se rechazan las metas culturales. El retraimiento implica el rechazo tanto de las metas como de los medios. Finalmente, la rebelión implica la sustitución de las metas y los medios culturales por otros nuevos. La teoría de la anomia de Merton ha sido fundamental para entender cómo las tensiones estructurales dentro de una sociedad pueden generar conductas desviadas. Por ejemplo, investigaciones sobre delitos económicos y de cuello blanco han demostrado que la presión para alcanzar el éxito financiero puede llevar a individuos a cometer fraudes y otras actividades ilegales cuando perciben que los medios legítimos están cerrados para ellos (Passas, 1990; Messner & Rosenfeld, 2007).

No obstante, con el paso del tiempo, los enfoques centrados en factores estructurales y socioeconómicos dieron lugar a un interés creciente en las teorías ambientales de la criminología. Estas teorías, que surgieron en la segunda mitad del siglo XX, enfatizan la influencia del entorno físico y social en la perpetración del crimen. Las teorías ambientales postulan que ciertos entornos pueden facilitar o inhibir el comportamiento delictivo, prestando atención a factores como el diseño urbano, la vigilancia natural y la gestión del espacio público. Más allá de las estadísticas sobre su prevalencia, las diversas manifestaciones del cibercrimen y las respuestas tecnológicas para combatirlo, una comprensión profunda del cibercrimen requiere una inmersión en las teorías que nos permiten desentrañar las raíces y los mecanismos subyacentes de esta forma de delincuencia. La importancia de este enfoque teórico radica en su capacidad para identificar no solo el "qué" y el "cómo" del cibercrimen, sino también el "por qué". A lo largo de este capítulo, se examinará cómo la criminología aborda el crimen desde esta perspectiva ambiental y cómo estos enfoques pueden adaptarse al entorno digital.

3.1. TEORÍAS AMBIENTALES

Estas teorías parten de la premisa de que el fenómeno delictivo trasciende la mera existencia del individuo que comete el delito y se orientan primordialmente hacia la prevención del crimen. En esencia, no buscan explicar por qué un individuo específico comete actos delictivos, sino que se enfocan en elucidar cómo y dónde ocurren los eventos delictivos. De este modo, la criminología ambiental centra su atención en el evento delictivo en sí, desplazando su interés hacia el conjunto de factores que convergen para facilitar la ocurrencia de un delito, incluyendo la presencia de una víctima potencial, la ausencia de un guardián capaz de prevenir el delito y el contexto específico en el que se desarrolla la conducta delictiva. Por tanto, las teorías ambientales no son teorías etiológicas en el sentido estricto de la palabra, ya que su propósito fundamental no es explicar por qué un individuo en particular delinque, sino más bien por qué se produce el evento delictivo, cómo se produce y dónde se produce, centrándose en el evento delictivo y no en el delincuente. El foco de atención no es el infractor, sino la idea de que, para que ocurra un delito, debe existir también una víctima y debe estar ausente un guardián, y que todo esto se producirá en un momento y lugar específicos, determinando todos estos elementos el crimen de una forma conjunta. Debido a esto, al otorgar menor importancia al que suele ser el elemento central de estudio en la criminología, el infractor, se convierten en teorías complementarias y compatibles con otros enfoques teóricos más biológicos o sociológicos, adoptando una perspectiva integradora. Es decir, las teorías ambientales no niegan que la razón por la cual alguien comete un delito, ya sea en el espacio físico o en el ciberespacio, está relacionada con factores psicológicos o sociológicos, sino que añaden que más allá de estas características, el crimen se cometerá en contextos de oportunidad cuando este converja con una víctima en un lugar sin un vigilante capaz de evitarlo. Estas teorías parten de la premisa de que, si se pretende prevenir el crimen, es mucho más eficaz centrarse en medidas enfocadas a la reducción de oportunidades en el lugar donde se comete el delito, en este caso en el ciberespacio, que intentar modificar elementos inherentes a la persona que comete el delito. Cabe señalar en este punto que, aunque estas teorías se formularon inicialmente para aplicarlas al espacio físico, también son aplicables al espacio

digital, ya que lo determinante no es el espacio en el que se produzca el delito, sino la interacción entre un agresor y una víctima en ausencia de métodos de prevención eficaces (Clarke, 2018; Miró-Llinares & Johnson, 2018).

Dentro de las teorías ambientales del crimen, se pueden discernir varios marcos teóricos significativos. Por su relevancia, se examinarán cuatro enfoques principales: la teoría de los estilos de vida, la teoría del patrón delictivo, la teoría de la acción racional y la teoría de las actividades rutinarias. Aunque estas perspectivas son complementarias, cada una aborda la noción de oportunidad delictiva de manera distinta. Finalmente, se introducirá una teoría específicamente formulada para el entorno digital, subrayando su pertinencia en el análisis de la cibercriminalidad.

3.1.1 Teoría de los estilos de vida

La teoría de los estilos de vida, concebida por Hindelang, Gottfredson y Garofalo en 1978 proporcionando una perspectiva renovadora sobre el fenómeno de la victimización al vincularlo indisolublemente con las actividades cotidianas y los comportamientos habituales de los individuos. En su núcleo, esta teoría postula que la victimización no se distribuye de manera aleatoria en el tiempo y el espacio, sino que existen espacios y periodos concretos de alto riesgo. El modelo propuesto vincula la probabilidad de ser víctima de un delito con el concepto de estilo de vida, que abarca una serie de factores exógenos de riesgo asociados a un modus vivendi arriesgado. En este sentido, se posterga la relevancia de los factores personales de la víctima potencial, ya sean biológicos o psicológicos, en favor de una priorización de los factores sociales.

El estilo de vida, con su concreto contenido de actividades, se configura a partir de las adaptaciones y compromisos del individuo frente a las expectativas sociales y determinaciones estructurales de tipo económico, familiar, educativo y legal. Precisamente en estas expectativas y determinaciones sociales inciden los factores demográficos que, en otras épocas, se consideraban determinantes de la victimización, tales como la condición sexual o la edad, entre otros. Siguiendo esta teoría, la probabilidad de ser victimizado depende esencialmente del margen vital

de exposición a lugares y situaciones de riesgo, así como de las asociaciones con individuos potencialmente delictivos, moldeando ambas variables de riesgo - la exposición y la asociación - en el marco del concreto estilo de vida.

La teoría de los estilos de vida se cimienta en varios principios fundamentales que elucidan cómo y por qué las personas se convierten en víctimas de delitos. En primer lugar, la exposición al riesgo: esta teoría sostiene que las personas que se exponen más frecuentemente a situaciones de riesgo tienen una mayor probabilidad de convertirse en víctimas de delitos. En segundo lugar, las asociaciones con potenciales delincuentes: las interacciones y asociaciones con individuos que poseen comportamientos delictivos incrementan la probabilidad de victimización. Por tanto, las personas que mantienen relaciones con amigos o familiares involucrados en actividades delictivas serán más propensas a ser victimizadas debido a su proximidad con estas conductas de riesgo. El tercer principio es el compromiso en actividades de riesgo, ya que participar en actividades que implican un alto nivel de riesgo, como el consumo de drogas o las apuestas, por ejemplo, incrementa la probabilidad de ser víctima de un delito. Estos comportamientos no solo exponen a las personas a situaciones peligrosas, sino que también las colocan en contacto con individuos que pueden tener intenciones delictivas. Finalmente, la teoría considera los factores demográficos: variables como la edad, el género, la educación y el estado civil influyen en los estilos de vida y, por ende, en la probabilidad de victimización.

Esta teoría proporciona una base fundamental para entender la victimización desde una perspectiva comportamental y situacional. A medida que exploramos cómo las actividades diarias y las interacciones sociales influyen en el riesgo de victimización, se hace evidente que los patrones delictivos no son completamente aleatorios, sino que siguen ciertos principios lógicos y predecibles.

En el contexto actual, la teoría de los estilos de vida ha sido adaptada para analizar la victimización en el ámbito digital, proporcionando una perspectiva renovada sobre los riesgos inherentes a las actividades en línea. La exposición al riesgo, en este nuevo entorno, se refiere a actividades digitales que incrementan la vulnerabilidad de los usuarios, tales como el acceso a conexiones de Internet inseguras y la divulgación de información personal en plataformas de redes

sociales (Akdemir & Lawless, 2020). Asimismo, las relaciones establecidas en el entorno digital desempeñan un papel crucial. La interacción en foros, redes sociales y otros espacios virtuales donde se promueven actividades ilícitas aumenta la probabilidad de ciber-victimización. Esto se debe a la proximidad y exposición constante a conductas delictivas (Marttila et al., 2020). Actividades como el streaming ilegal de contenido, la descarga de software ilegal o el uso de servicios de intercambio de archivos peer-to-peer no solo infringen la ley, sino que también incrementan la probabilidad de que los usuarios sean víctimas de malware, phishing y otros cibercrímenes. Dichos comportamientos crean un entorno favorable para que los ciberdelincuentes operen con mayor facilidad y dirijan sus esfuerzos hacia individuos involucrados en estas actividades (Dearden & Parti, 2021). Paralelamente, los factores demográficos mantienen su relevancia en el ciberespacio, al igual que en el contexto físico. La edad, el género, la educación y el estado civil influyen significativamente en cómo los individuos utilizan la tecnología y, por ende, en su riesgo de victimización. La edad es un factor crítico en la victimización digital, los jóvenes, debido a su mayor uso de tecnología y redes sociales, tienen una mayor exposición a riesgos en línea. Sin embargo, esta misma familiaridad con la tecnología puede ser una espada de doble filo, ya que la falta de conciencia sobre prácticas de seguridad digital adecuada hace a estos usuarios particularmente vulnerables a ataques cibernéticos como el phishing y el malware (Staksrud et al., 2013). Así mismo, el nivel educativo y la formación relacionada con la ciberseguridad influye directamente en el conocimiento y la implementación de prácticas de seguridad en este contexto. La falta de educación en ciberseguridad puede dejar a ciertos grupos demográficos expuestos a una mayor probabilidad de victimización (Dearden & Parti, 2021).

Se profundiza en estos conceptos en las teorías ambientales subsecuentes, las cuales argumentan y desarrollan esta perspectiva desde diferentes puntos de vista, destacando todas ellas la importancia del contexto y las condiciones ambientales en la ocurrencia de delitos.

3.1.2 Teoría del patrón delictivo

La teoría del patrón delictivo, desarrollada Paul y Patricia Brantingham, busca explicar la distribución espacial y temporal de los delitos mediante la integración de conceptos de la ecología del comportamiento humano y la criminología ambiental. Los autores se basan en la premisa de que los delitos no ocurren al azar, sino que siguen patrones discernibles influenciados por el entorno físico y social y argumentan que los delincuentes toman decisiones racionales basadas en la oportunidad, los costes y los beneficios presentes en un contexto espacial específico.

Un concepto central en esta teoría es el de los "espacios de vida" (activity spaces), que se refiere a las áreas geográficas que las personas frecuentan regularmente en sus actividades cotidianas, como el hogar, el trabajo, la escuela y áreas de ocio. Según los Brantingham, los delincuentes suelen cometer delitos en estos espacios de vida o cerca de ellos, debido a su familiaridad con estos lugares y la percepción de menor riesgo al encontrarse en una zona de confort. Esta noción está respaldada por estudios empíricos que demuestran que la muchos de los delitos ocurren en áreas cercanas a los lugares que los delincuentes visitan regularmente. Ya en el año 1985, Rengert y Wasilchick afirmaron que una considerable proporción de los actos de hurto perpetrados en el ámbito urbano eran, en esencia, respuestas inmediatas a oportunidades fortuitas que emergían en el transcurso de las actividades cotidianas. Por ende, tales conductas delictivas podían ser categorizadas como delitos de naturaleza situacional.

De igual forma, esta teoría establece una distinción crucial entre "generadores de delitos" y "atractores de delitos". Los generadores de delitos son ubicaciones que, debido a motivos legítimos, congregan a grandes cantidades de individuos, tales como centros comerciales, estaciones de transporte o eventos deportivos. Esta elevada afluencia de personas incrementa las oportunidades delictivas debido a la alta concentración de potenciales víctimas. Contrariamente, los atractores de delitos son lugares específicos ampliamente reconocidos por ofrecer oportunidades propicias para la comisión de crímenes, como barrios marginales o zonas donde se realizan actividades relacionadas con la prostitución o el comercio de sustancias ilegales. Dichos lugares específicos pueden ejercer una influencia significativa en la distribución espacial de los delitos, propiciando una mayor

concentración de estos, dirigidos tanto contra la propiedad como contra las personas (Brantingham & Brantingham, 1995).

Finalmente, otro componente esencial de la teoría es la relevancia de los "nodos" y "caminos". Los nodos representan puntos de convergencia donde las personas se agrupan, como domicilios, lugares de trabajo, instituciones educativas y centros comerciales. Los caminos, por su parte, son las rutas empleadas para desplazarse entre estos nodos, incluyendo arterias principales, trayectos de transporte público y carreteras. Según los autores, la incidencia delictiva tiende a concentrarse en los nodos y a lo largo de los caminos, dado que en estos contextos los delincuentes encuentran mayores oportunidades para identificar víctimas potenciales y la confluencia entre ambos, delincuente y víctima, es más probable en estas áreas. Tal como presenta la teoría del patrón delictivo, existe una conexión intrínseca entre el lugar donde se comete el delito y la persona que lo comete, minimizando la percepción de riesgo en las zonas que le son familiares al delincuente.

En el ciberespacio, la aplicación de esta teoría es incipiente y deben tenerse en cuenta algunas adaptaciones debido a las características concretas del ciberespacio. Los *espacios de vida* pueden traducirse en los entornos en línea frecuentados regularmente por los usuarios, tales como redes sociales, foros y sitios de comercio electrónico. Estos espacios virtuales se convierten en áreas de familiaridad donde los delincuentes pueden operar con una percepción reducida de riesgo, por lo que, siguiendo esta teoría, los ciberdelincuentes son más proclives a realizar sus ataques mediante plataformas que visitan frecuentemente, aprovechando su conocimiento de las vulnerabilidades específicas de estos entornos (Yar & Steinmetz, 2019). De la misma forma, los conceptos de *generadores de delitos* y *atractores de delitos* son aplicables al entorno digital. Los generadores de delitos en el ciberespacio son sitios web y plataformas que atraen grandes volúmenes de visitas, como redes sociales, plataformas de juegos en línea y mercados digitales. La alta afluencia de usuarios en estos sitios crea numerosas oportunidades delictivas, como el phishing, el malware y el robo de identidad. En cuanto a los atractores de delitos harían referencia a sitios específicos conocidos por sus actividades ilícitas, como foros de la dark web y mercados de venta de datos robados. Estos espacios digitales son frecuentados tanto por delincuentes

como por potenciales víctimas, facilitando la comisión de delitos debido a la concentración de actividades delictivas. En el contexto digital, los *nodos* representan los puntos de convergencia en el ciberespacio donde los usuarios interactúan mientras que los *caminos* son las rutas de navegación que los usuarios toman para moverse entre estos nodos, incluyendo enlaces, redes de pares y gestores de búsqueda en línea. Al adaptar esta teoría al ciberespacio y referir la evaluación de riesgos y beneficios es evidente que los ciberdelincuentes evalúan las oportunidades delictivas basándose en la familiaridad con las plataformas y la percepción de seguridad, similar a cómo los delincuentes tradicionales operan en espacios físicos conocidos, aunque en este entorno a menudo perciben un riesgo menor al cometer delitos en comparación con el espacio físico (Miró-Llinares & Moneva, 2020).

Precisamente, estos conceptos centrales presentes en la teoría del patrón delictivo, la evaluación de riesgo y beneficio, fundamentan otra de las teorías ambientales: la teoría de la elección racional.

3.1.3 Teoría de la elección racional

La teoría de la elección racional, desarrollada en la década de 1980 por Derek Cornish y Ronald Clarke, postula que los delincuentes actúan de manera racional, ponderando cuidadosamente los beneficios y costes antes de cometer un delito. Según esta teoría, las personas cometen actos ilícitos en un lugar basado en el cálculo realizado sobre el beneficio esperado de dicha actividad superior al coste asociado. Esto no implica que el delincuente carezca de emociones, sino que estas interactúan en un entorno específico que proporciona claves y estímulos para la delincuencia. Así, incluso en los casos más emocionales y aparentemente impredecibles, existen una serie de decisiones que se toman con cierto nivel de planificación y racionalidad, las cuales suelen relacionarse con la selección de la víctima y el lugar del crimen.

Por ende, la teoría de la elección racional se fundamenta en varios principios clave que explican el comportamiento delictivo como resultado de decisiones calculadas

y conscientes, y que se podrían aplicar tanto a un entorno físico como al ciberespacio. El elemento central es la toma de decisiones racionales por parte del delincuente, quien evalúa las posibles recompensas del delito frente a los riesgos y costes asociados. Este proceso de toma de decisiones incluye la consideración de factores como la probabilidad de éxito, el valor del objetivo y la severidad de las posibles sanciones. Los beneficios pueden incluir ganancias financieras, satisfacción emocional o estatus social, mientras que los costes pueden abarcar el riesgo de arresto, el castigo legal y el esfuerzo requerido. Así mismo, la teoría reconoce que las decisiones delictivas están influenciadas por factores situacionales específicos, como la presencia de medidas de seguridad, la vigilancia policial y la accesibilidad del objetivo. Estos factores pueden alterar la percepción de los costes y beneficios, influyendo en la decisión final del potencial delincuente. Sin embargo, pese a que se asume que los delincuentes actúan de forma racional, también se reconoce la existencia de una "racionalidad limitada", por lo que las decisiones asociadas al acto delictivo pueden no ser perfectamente lógicas debido a la falta de información completa, sesgos cognitivos o emociones asociadas. Por último, uno de los avances significativos en la teoría ha sido la distinción entre "elección inicial" y "elección continuada".

Por un lado, la elección inicial se refiere a la decisión de involucrarse en el delito por primera vez, mientras que la elección continuada se refiere a las decisiones repetidas de continuar cometiendo delitos. La decisión de cometer un delito por primera vez a menudo está motivada por factores situacionales y contextuales, como la disponibilidad de oportunidades delictivas y la influencia de pares delincuentes (Wright & Decker, 2020). Así mismo, los delincuentes novatos utilizan técnicas de neutralización para justificar sus acciones y reducir la disonancia cognitiva asociada con la violación de normas sociales. Estas técnicas incluyen la negación de la responsabilidad, la negación del daño y la apelación a lealtades superiores, y juegan un papel crucial en la superación de las barreras morales iniciales al comportamiento delictivo (Piquero et al., 2014)

Por otro lado, la elección continuada se refiere a las decisiones repetidas de continuar cometiendo delitos después de la primera ofensa. Este proceso está influenciado por la experiencia previa del delincuente, las percepciones

cambiantes de riesgo y recompensa, y la adaptación de estrategias y tácticas para maximizar el éxito y minimizar el riesgo de captura. Estudios sobre delincuentes que reinciden han mostrado cómo estos individuos desarrollan un "conocimiento delictivo" basado en sus experiencias pasadas, lo que les permite cambiar sus habilidades y ajustar sus comportamientos para evitar la detección (Wright et al., 2014).

Desde esta concepción del criminal como un sujeto racional que toma decisiones basadas en la evaluación de costes y beneficios, Cornish y Clarke delinearon cinco categorías fundamentales de prevención situacional del delito. Estas categorías comprenden: técnicas para aumentar el esfuerzo, que buscan dificultar la comisión del delito; técnicas para aumentar el riesgo, que incrementan la probabilidad de detección y arresto del criminal; técnicas para disminuir las ganancias, que reducen el atractivo de los objetivos; técnicas para reducir las provocaciones, que minimizan las incitaciones al comportamiento delictivo; y, finalmente, técnicas para eliminar las excusas, que privan al delincuente de justificaciones para sus acciones.

En primer lugar, las técnicas destinadas a aumentar el esfuerzo delictivo se centran en la implementación de controles de acceso, tanto físicos como digitales, con el objetivo de restringir la entrada a determinados espacios. La vigilancia de los puntos de salida resulta igualmente crucial para prevenir huidas rápidas en el caso del entorno físico. La deflexión de los infractores, lograda a través de la configuración del entorno o señales disuasorias, redirige a los posibles delincuentes lejos de objetivos vulnerables. La protección de los objetivos se realiza mediante la implementación de medidas de seguridad, como sistemas de alarma y dispositivos que dificulten el acceso no autorizado. Por último, el control de herramientas y armas implica restringir el acceso a instrumentos que faciliten la comisión de delitos.

En segundo lugar, las técnicas para aumentar el riesgo de detección y detención del delincuente incluyen la extensión y fortalecimiento de la vigilancia, utilizando cámaras de seguridad y sistemas de monitoreo. Mejorar la calidad y eficacia de estos sistemas es fundamental, al igual que aumentar la capacidad de intervención inmediata por parte del personal de seguridad. El refuerzo de los controles de

entrada y salida asegura un monitoreo estricto, dificultando la huida de los delincuentes. Asimismo, la creación de defensas naturales, como una mejor iluminación, aumenta la visibilidad y la vigilancia natural.

En tercer lugar, las técnicas para disminuir las ganancias implican la reducción del valor de los objetivos potenciales. Esto incluye eliminar ciertos bienes o información de la disponibilidad pública, identificar claramente la propiedad mediante marcas o registros para hacerla menos atractiva para los ladrones, y reducir la tentación disminuyendo la visibilidad y accesibilidad de objetos valiosos. Denegar beneficios asegura que las ganancias del delito sean mínimas o inexistentes, mientras que neutralizar las mercancías robadas, mediante tecnologías de rastreo o bloqueos remotos, las hace inutilizables.

En cuarto lugar, las técnicas para reducir las provocaciones buscan moderar las condiciones que podrían incitar a un ataque. Esto incluye reducir las frustraciones y el estrés, evitar conflictos y tomar medidas preventivas para evitar actos de venganza. Limitar la visibilidad de comportamientos delictivos que puedan ser imitados y controlar el uso de alcohol y drogas restringiendo su acceso también son medidas importantes para limitar el comportamiento delictivo. Disuadir la revancha implica implementar medidas preventivas para evitar actos de venganza.

Por último, las técnicas para eliminar las excusas del delincuente se centran en privarlo de justificaciones para sus acciones. Establecer y publicitar reglas y sanciones claras asegura que las normas y consecuencias del comportamiento delictivo sean conocidas. Aumentar la conciencia de los riesgos informa a los potenciales delincuentes sobre los peligros y consecuencias de sus acciones. Promover la responsabilidad individual y social, evitando la justificación del delito, y fomentar una cultura de desaprobación hacia el comportamiento delictivo mediante la presión social y comunitaria son también esenciales.

Estas medidas proporcionan un enfoque para la prevención situacional del crimen, aplicable a diversos contextos y entornos, ajustándose a las especificidades de cada uno de ellos (Clarke, 1197; Ekblom, 2011; Welsh & Farrington, 2009; Wortley, 2001). En su aplicabilidad al cibercrimen, la Teoría del patrón delictivo se presenta como un enfoque prometedor, aunque todavía poco explorado en este contexto. A

pesar de su éxito en otros ámbitos delictivos en el entorno físico, su aplicación al ciberespacio no ha sido extensamente desarrollada y la investigación existente muestra una integración limitada de las técnicas específicas propuestas por Cornish y Clarke en la prevención de delitos cibernéticos, siendo necesario un enfoque que reconozca y aborde la diversidad y especificidad de los desafíos del cibercrimen (Ho et al., 2022).

Todos los conceptos previamente expuestos se encuentran representados, de una u otra forma, en la siguiente y última teoría que abordaremos dentro del marco de las teorías ambientales: la teoría de las actividades cotidianas. Esta teoría complementa y enriquece las teorías anteriores al incluir el contexto (tal como postula la teoría del patrón delictivo), las actividades rutinarias (en consonancia con la teoría de los estilos de vida) y la presencia de un delincuente motivado (de forma similar a la teoría de la elección racional). Por tanto, en conjunto, estas teorías ofrecen una visión integral y matizada de cómo los patrones de la vida diaria, las interacciones sociales y las evaluaciones racionales de riesgo y beneficio influyen en la distribución y ocurrencia delictiva.

3.1.4 Teoría de las actividades cotidianas

La formulación de la teoría de las actividades cotidianas debe entenderse en el contexto de las transformaciones sociales y económicas que caracterizaron a Estados Unidos en las décadas de 1960 y 1970. Durante este período, las tasas de criminalidad experimentaron un aumento significativo, lo cual generó un interés renovado en la búsqueda de explicaciones teóricas que fueran más allá de las características individuales de los delincuentes. Cohen y Felson observaron que estos aumentos en la criminalidad coincidían con cambios estructurales importantes, entre los que se encontraba la incorporación masiva de mujeres al mercado laboral y una mejora en la economía. Cohen y Felson observaron que, a pesar de las mejoras económicas y sociales, las tasas de delincuencia experimentaron un aumento. Llegaron a la conclusión de que este fenómeno se

debía a los cambios que se habían producido en las actividades cotidianas de la población, que generaban mayores oportunidades para la comisión de delitos. Estos cambios generaron un contexto en el cual los hogares permanecían vacíos durante largos periodos del día, incrementando así las oportunidades para delitos como el robo. Por tanto, factores tales como pasar más tiempo fuera del hogar, incrementar las transacciones bancarias y una mayor interacción social, potenciados por la mejora de las condiciones económicas y la modernización, contribuyeron a elevar el número de delitos (Cohen & Felson, 1979).

El artículo seminal de Cohen y Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach", publicado en 1979 en la American Sociological Review, marcó un punto de inflexión en las teorías criminológicas. En este trabajo, los autores propusieron que el cambio en las actividades rutinarias de las personas influye directamente en las oportunidades para la comisión de delitos. Este enfoque situacional fue innovador, pues desviaba la atención del perfil del delincuente hacia las circunstancias específicas que facilitan la ocurrencia del crimen, planteando una relación directa entre los patrones de vida cotidiana y la victimización.

Este paradigma enfatiza la importancia de considerar el contexto situacional y los elementos estructurales que facilitan la comisión del delito, más allá de las características intrínsecas del delincuente. Dentro de este marco, los delitos son entendidos como eventos con una naturaleza ecológica, influenciados por la interacción dinámica de diversos componentes en términos de espacio y tiempo. La estructura social y las actividades cotidianas no delictivas ejercen una influencia directa sobre la manera en que se cometen los delitos. La adopción de ciertas prácticas, como el uso prevalente de automóviles en lugar del transporte público, puede incrementar las oportunidades para delitos específicos bajo condiciones adecuadas.

3.1.4.1 Elementos clave

La teoría de las actividades cotidianas postula que la convergencia espacial y temporal de un agresor potencial con una víctima susceptible, en ausencia de

guardianes efectivos capaces de prevenir el acto delictivo, constituye una condición sine qua non para la materialización del delito. En consecuencia, esta teoría se centra en tres elementos clave cuya presencia simultánea en un contexto específico propicia el incremento de las tasas de criminalidad: un delincuente motivado y provisto de las herramientas necesarias para perpetrar el delito; una víctima apropiada, definida por su situación de vulnerabilidad y falta de protección; y la ausencia de protectores eficaces, entendidos como aquellos ciudadanos capaces de autodefenderse o de proteger a otros en esa situación concreta. Procedamos, pues, a analizar cada uno de estos conceptos clave con mayor detalle.

El primer elemento crucial en la teoría es la figura del delincuente motivado, sustentada en la premisa de que siempre existirán individuos con inclinaciones delictivas, movidos por una combinación de factores económicos, psicológicos y sociales. La teoría de las actividades cotidianas asume que estos individuos están dispuestos a cometer un delito si se presentan las condiciones adecuadas. Los factores que impulsan a un individuo a convertirse en delincuente son variados y complejos. Entre ellos destacan:

- Factores Económicos: La necesidad de recursos financieros constituye uno de los motivadores más comunes. En situaciones de crisis económica, pobreza, desempleo y carencia de otras vías mediante las que obtener sustento, la motivación para delinquir puede aumentar significativamente (Wright & Decker, 1994).

- Factores Psicológicos: Algunos individuos pueden hallar en el delito una fuente de emoción, desafío o gratificación psicológica. La búsqueda de adrenalina o la necesidad de probarse a sí mismos pueden ser motivadores significativos.

- Factores Sociales: La presión de los pares y la influencia de subculturas delictivas también juegan un papel crucial en la motivación del delincuente. La pertenencia a grupos que valoran y promueven la conducta delictiva puede aumentar la propensión de un individuo a cometer delitos (Felson & Boba, 2010).

El segundo elemento esencial en la teoría es la presencia de una víctima adecuada o un objetivo deseable. La teoría sostiene que no todos los posibles objetivos son igualmente atractivos para los delincuentes; algunos presentan mayores niveles de vulnerabilidad o valor que otros. Las características que hacen que una víctima sea considerada adecuada incluyen la Visibilidad, el Valor otorgado al objetivo, la Inercia y la Accesibilidad. Todas estas características se analizarán en el siguiente apartado, tanto en su definición inicial como en su posible adaptación al ciberespacio.

Aunque Cohen y Felson asignaron importancia a cada uno de estos elementos, su análisis otorgó especial atención a la ausencia de mecanismos protectores, considerando que este factor ofrece un mayor margen para el control y la prevención del crimen. La presencia de guardianes efectivos es un factor necesario para la prevención del crimen, ya que actúan como un disuasivo visible para los delincuentes potenciales. Los guardianes pueden clasificarse en tres categorías principales:

- Guardianes Formales: Estos incluyen a las fuerzas y cuerpos de seguridad y los sistemas de seguridad tecnológica, como cámaras de vigilancia y alarmas.

- Guardianes Informales: referidos a miembros de la comunidad, vecinos y familiares.

- Medidas de seguridad ambiental: Estas incluyen diseños urbanos que promueven la vigilancia natural y reducen las oportunidades para el crimen.

Al aplicar esta teoría al contexto actual, caracterizado por avances tecnológicos significativos, se observa cómo esta digitalización ha facilitado la acción de los delincuentes, proporcionando herramientas rápidas y efectivas no disponibles anteriormente. Además, las modificaciones en las actividades cotidianas y las formas de interacción social han creado nuevos blancos y potenciales víctimas que se vuelven más vulnerables ante el crimen. Aunque existen reservas sobre la aplicabilidad de esta teoría al ámbito del ciberespacio (Leukfeldt & Yar, 2016),

otros investigadores argumentan que la convergencia entre víctima y delincuente es plausible en el ciberespacio, considerándolo un sustituto del espacio físico (Miró Llinares, 2011; Reyns, 2011), como se expone a continuación.

3.1.4.2 Adaptación al ciberespacio

Tal como se ha expuesto, todas las teorías ambientales poseen una naturaleza esencialmente geográfica y están diseñadas para el análisis del espacio físico, lo que podría sugerir superficialmente que su aplicación al contexto digital es inapropiada. Sin embargo, el núcleo de estas teorías no reside en el lugar específico donde se perpetra el crimen (Clarke,2004), sino en la convergencia de agresores y víctimas en ausencia de guardianes específicos, una situación que puede darse tanto en un entorno físico como digital.

Además, la relación entre el crimen y el lugar es significativa desde la perspectiva de que el criminal elige dónde y cuándo actuar, y esto se extiende también al ciberespacio. Basándonos en las teorías analizadas previamente, el lugar es significativo porque las personas cometen crímenes en los espacios de actividad cotidiana en los que interactúan: lugares de ocio, de trabajo y otros entornos del día a día, tal como lo argumenta la teoría de los estilos de vida. Es evidente que hoy en día esto también ocurre en el ciberespacio, que ha absorbido muchas de las actividades diarias de los ciudadanos. Asimismo, el lugar es relevante porque ciertos espacios, por el tipo de actividades que en ellos se desarrollan, propician conductas delictivas. Esto se observa igualmente en el ciberespacio, donde lugares concretos ofrecen servicios ilegales. De igual modo, hay lugares que, debido a la concentración de personas, generan oportunidades propicias para la comisión de delitos y este fenómeno también se manifestará en el ciberespacio. Adicionalmente, la teoría de la elección racional postula que el delincuente considera los beneficios y costes asociados al acto delictivo, priorizando aquellos que son menos costosos y más beneficiosos, un proceso que también se da en el ciberespacio.

Por tanto, aunque el ciberespacio no comparte todas las características del espacio físico y presenta diferencias intrínsecas, esto no impide la aplicación de las teorías mencionadas a este contexto. Esta postura es precisamente defendida por el

Catedrático en Derecho Penal y experto en cibercriminalidad, Fernando Miró Llinares. Este autor sostiene que, al ser el ciberespacio un ámbito distinto del espacio físico se modifican las dinámicas tradicionales del crimen, lo que no limita su explicación mediante las teorías ambientales, particularmente mediante la Teoría de las actividades cotidianas (Miró-Llinares, 2011; 2012).

En su adaptación de la Teoría de las actividades cotidianas al ciberespacio, el autor plantea que, dado que lo esencial para la comisión de un delito es la convergencia de agresor y víctima en ausencia de guardianes eficaces, es evidente que este fenómeno también se produce en el entorno digital. Sin embargo, esta convergencia se manifiesta de forma distinta. Para comprender estas diferencias, es pertinente analizar los factores que singularizan el ciberespacio en comparación con el espacio físico.

Entre estos factores, encontramos primero una serie de elementos extrínsecos, es decir, aquellos que podrían modificarse con el tiempo. Por ejemplo, el ciberespacio es actualmente un ámbito popular y universal, utilizado masivamente por una gran parte de la población y en constante evolución, lo cual lleva a afirmar que actualmente es un entorno donde el contacto físico no es posible, aunque esto podría cambiar en el futuro. Más allá de estos factores extrínsecos, hay dos elementos fundamentales que diferencian al ciberespacio del espacio físico: las dimensiones espacial y temporal.

Desde una perspectiva espacial, el ciberespacio es un entorno donde la distancia tal como se concibe en el espacio geográfico no existe. Todos los sujetos están virtualmente en el mismo lugar, lo que crea una contracción del espacio en términos de distancia y una expansión de las posibilidades comunicativas. En el espacio físico, la comunicación requiere proximidad entre emisor y receptor; en el ciberespacio, la distancia deja de ser un obstáculo, y el coste de la realización de una acción es el mismo sin importar la ubicación física del sujeto destinatario.

Además, el ciberespacio implica una contracción del tiempo necesario para la comunicación social: se reduce el tiempo necesario para llevar a cabo una tarea y se extienden las relaciones sociales. Al no requerirse recorrer una distancia física para la comunicación, aumentan las posibilidades de contacto con múltiples

sujetos y se reduce el tiempo necesario para ello. En última instancia, Internet disminuye los costes temporales asociados a la comunicación interpersonal en el espacio físico.

Otro cambio significativo relacionado con el tiempo en el ciberespacio es que las conductas ejecutadas, especialmente aquellas consistentes en la difusión de contenidos, pueden permanecer por tiempo indeterminado, desplegando efectos duraderos aunque su ejecución haya sido instantánea. Mientras que en el espacio físico las acciones producen efectos en un momento específico, en el ciberespacio estos efectos pueden perdurar y afectar a diferentes agentes en distintos momentos.

En consecuencia, las coordenadas espacio-temporales en el ciberespacio se ven alteradas: se comprimen las distancias y el tiempo necesario para recorrerlas, y se expanden las posibilidades comunicativas y los efectos de las acciones, que apenas están limitados espacial o temporalmente. Esto significa que cualquier agente en el ciberespacio, salvo la imposibilidad del contacto físico directo, enfrenta menos restricciones espaciales y temporales para sus actos que en el espacio físico. Estas cualidades particulares modifican la naturaleza de las interacciones, incluyendo aquellas entre agresores y víctimas. En primer lugar, aumentan los objetivos potenciales. En segundo lugar, reducen el coste espacio-temporal de cometer un delito, tanto en términos de alcanzar el objetivo como de asegurar la huida una vez cometido el delito. Este campo de oportunidad más amplio y la falta de coincidencia en el mismo espacio físico con la víctima pueden llevar a una menor valoración del daño causado y a un incremento en la motivación del delincuente para cometer el delito.

Como se ha expuesto previamente, en la Teoría de las actividades cotidianas (TAC) se identifican cuatro factores relevantes para evaluar la idoneidad de una víctima u objetivo: Valor, Inercia, Visibilidad y Accesibilidad. Tal como afirma el Profesor Miró-Llinares, el único de estos elementos que no resulta aplicable al ciberespacio, debido a su naturaleza esencialmente física, es el de inercia. En la teoría clásica, el concepto de inercia se refiere a la capacidad del objetivo para resistirse al ataque, dificultando su desplazamiento y el ataque del agresor, características intrínsecamente físicas. Sin embargo, en el ciberespacio, los bienes no se

diferencian significativamente entre sí por sus condiciones intrínsecas en términos de resistencia física. La propuesta del autor consiste en sustituir la idea de inercia por la de Introducción y matizar los otros factores, como se analizará a continuación (Figura 1).

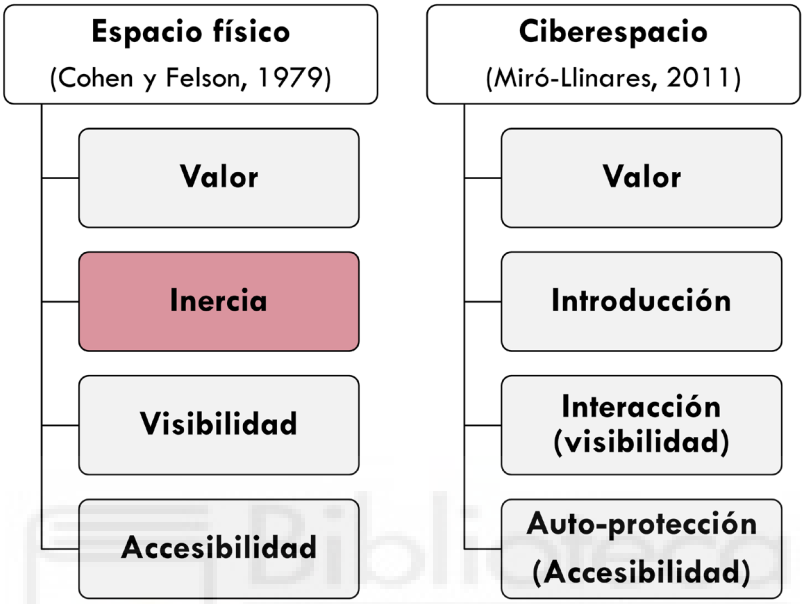


Figura 1. Aplicación TAC al ciberespacio 1

- Valor

En relación con el valor del objetivo, es evidente que, a mayor valor intrínseco del mismo, mayor es la probabilidad de que sea objeto de ataque, y esto se aplica igualmente en el ciberespacio. Independientemente de la naturaleza del objetivo, ya sea patrimonial o de libertad sexual, entre otros, en el ciberespacio se presenta la particularidad de que elementos con escaso valor intrínseco pueden adquirir una significancia considerable. Esta transformación se debe a la facilidad con la que se puede obtener información, correlacionarla con otros datos obtenidos, y así convertirla en un objeto de riesgo significativo.

- Inercia vs Introducción

En la TAC, la Inercia se definía como las propiedades intrínsecas de los objetivos que pueden hacer que ofrezcan resistencia, en distintos grados, al ataque. El contacto entre objetivo y agresor en el espacio físico se caracteriza, generalmente, por un contacto físico directo e inmediato, donde todos los bienes personales de la víctima que lleve consigo están expuestos y se convierten en potenciales objetivos para el ataque del agresor. Sin embargo, en el espacio virtual o ciberespacio, la naturaleza del contacto entre individuos es sustancialmente diferente, lo que limita claramente la aplicación de este concepto, siendo más adecuado sustituirlo por el de Introducción (Miró-Llinares, 2012). Este nuevo concepto hace referencia al hecho de que en el contexto digital la persona no coloca todos sus bienes al alcance de otros usuarios o potenciales agresores, sino que selecciona aquellos que decide situar en este entorno. Esta selección permite, al menos inicialmente, la posibilidad de excluir del ataque aquellos bienes que no se han incorporado al ámbito digital. Esta diferencia fundamental altera significativamente la dinámica delictiva, dado que el agresor solo tiene acceso a los bienes que la víctima ha elegido exponer en el ciberespacio, modificando así la evaluación de los objetivos y las estrategias de ataque.

- Visibilidad

Conforme a la teoría original, dicho factor postulaba que aquello que no es percibido por el agresor no puede constituir su objetivo. En el contexto del ciberespacio, la visibilidad de un individuo se manifiesta a través de sus interacciones con otros sujetos y diversos servicios digitales. A medida que aumenta la cantidad de interacciones, tanto con personas como con sitios web y otros servicios, incrementa la probabilidad de ser visible para otros usuarios en el ciberespacio, incluyendo a posibles agresores.

- *Accesibilidad*

La teoría original alude a este factor como la capacidad del agresor para contactar con un objetivo y sustraerlo de la escena del crimen. En el ciberespacio, la contracción de las distancias implica que todos los objetivos presentes en este

entorno son, en cierto modo, accesibles. No obstante, el mero hecho de establecer contacto con el individuo no garantiza el acceso a sus datos o bienes, ya que esto depende de los sistemas de protección que el propio sujeto haya implementado para salvaguardarse.

Finalmente, en la adaptación de esta teoría al ciberespacio, es necesario abordar la noción de los guardianes capaces, ya que su presencia impide la perpetración del delito incluso cuando existe una convergencia entre agresor y víctima. En el entorno digital, se puede diferenciar entre el guardián propiamente dicho, que actúa directamente sobre el objetivo potencial, y el gestor del lugar, que se encarga de prevenir daños en áreas específicas del ciberespacio. La problemática central radica en la ausencia de mecanismos de control centralizados que se extiendan a nivel global y proporcionen una protección significativa en el vasto contexto digital (Miró-Llinares, 2012). Adicionalmente, en este caso, cuando se habla de guardianes capaces, es el propio usuario quien debe autoprotegerse. Esto se logra, por ejemplo, mediante la instalación de programas que permitan la detección de virus o la implementación de contraseñas seguras que dificulten el acceso a sus bienes. Esta diferencia es fundamental, ya que el concepto de auto-guardián recae en el individuo, un rol que en el entorno físico solían desempeñar personas cercanas al objetivo o a la víctima, así como las fuerzas y cuerpos de seguridad.

Como hemos presentado, los conceptos derivados de las teorías ambientales pueden aplicarse al ámbito digital, aunque con ciertas limitaciones evidentes inherentes a la naturaleza de este entorno. La exposición al riesgo en línea es un factor crucial en la victimización cibernética por lo que las personas que pasan más tiempo en internet, especialmente en plataformas vulnerables a ataques como redes sociales, foros y sitios de comercio electrónico, están más expuestas a riesgos como el phishing, el hacking y el ciberacoso. Es cierto que, en el entorno digital, las personas más jóvenes tienden a ser usuarios más activos de las TIC y las redes sociales, por lo que pueden estar más expuestos a ciertos tipos de ciberdelitos. Sin embargo, no debemos olvidar que las personas adultas mayores, aunque pueden estar menos expuestos debido a un menor uso de la tecnología, a menudo carecen de las habilidades necesarias para protegerse adecuadamente, lo que los hace

vulnerables a ataques específicos, en su mayoría financieros, como se ha expuesto previamente. Así mismo, el contacto en este entorno con individuos o grupos que participan en actividades delictivas también aumentan el riesgo de victimización. Adicionalmente, realizar actividades digitales que pueden suponer un riesgo, como el intercambio de información personal en redes sociales sin medidas de privacidad adecuadas, incrementa la probabilidad de ser víctima de ciberdelitos ya que estas conductas pueden exponer a los individuos a riesgos adicionales, como el robo de identidad y el fraude financiero. En este ámbito es adecuado subrayar la importancia de entender cómo los patrones de comportamiento digital y las rutinas diarias influyen en la exposición a riesgos en el ciberespacio, siendo esencial que las estrategias de prevención del cibercrimen deben adaptarse a los diferentes estilos de vida y perfiles demográficos de los usuarios.

No obstante, es pertinente en este punto hacer referencia a una teoría específicamente diseñada para abordar las particularidades del contexto digital, la cual será detallada en el siguiente apartado. Esta teoría proporciona un marco conceptual que se adapta a las dinámicas y características únicas del ciberespacio, superando algunas restricciones de las teorías tradicionales.

3.1.5 La teoría de la Transición Espacial de K.Jaishankar

La teoría propuesta por K. Jaishankar en 2008, denominada Teoría de la Transición Espacial, representa una innovación conceptual al referirse exclusivamente al ámbito digital. Esta teoría postula que los individuos manifiestan comportamientos divergentes en el entorno digital en comparación con el espacio físico. Jaishankar sostiene que el ciberespacio altera las reglas del comportamiento social, facilitando y, en ciertos casos, exacerbando conductas que, en el ámbito físico, permanecen reprimidas debido a las normas sociales y los mecanismos de control presentes en dicho entorno. Jaishankar introduce esta noción a través de siete postulados que examinan la naturaleza del comportamiento humano en relación con el crimen en el contexto digital. Estos postulados destacan que el ciberespacio proporciona

características únicas, tales como la flexibilidad de la identidad y la posibilidad de anonimato, las cuales permiten a ciertos individuos explorar comportamientos que no se atreverían a manifestar en el mundo físico. A continuación, se expone cada uno de estos postulados y se analizan sus implicaciones para la comprensión del comportamiento delictivo en el entorno digital.

- Comportamientos criminales reprimidos

  El primer postulado establece que los individuos con comportamientos delictivos reprimidos en el espacio físico tienden a manifestar dichas conductas en el ciberespacio. Este fenómeno se explica debido a la reducción de barreras sociales y personales que normalmente inhiben tales comportamientos y que se encuentran presente en el espacio físico. Jaishankar argumenta que en el entorno digital las restricciones sociales tradicionales se debilitan considerablemente. En el espacio físico, el estatus social y la posición de un individuo actúan como frenos conductuales debido al miedo, la vergüenza, el juicio social y las repercusiones legales. Sin embargo, en el ciberespacio, estas barreras se erosionan, permitiendo a los individuos actuar de manera más libre y, en algunos casos, delictiva. Si asumimos que ciertos individuos están predispuestos a manifestar comportamientos delictivos cuando las barreras sociales son reducidas, las medidas preventivas pueden enfocarse en recrear estas barreras en el entorno digital.

- Flexibilidad de la identidad, anonimato disociativo y falta de factores disuasorios

  Este postulado subraya tres características fundamentales del ciberespacio que facilitan la comisión de delitos. En primer lugar, en el ciberespacio encontramos flexibilidad de la identidad, ya que los individuos pueden adoptar múltiples identidades o cambiar su identidad con facilidad. Este fenómeno, conocido como identidad flexible, permite a los usuarios ocultar su verdadera identidad detrás de pseudónimos, avatares o perfiles falsos, creando una barrera que dificulta la identificación y rastreo del delincuente. en segundo lugar, cierto anonimato en línea disocia la identidad del

individuo de sus acciones ya que reduce la percepción de responsabilidad personal y las consecuencias sociales de las acciones, permitiendo que las personas actúen de manera que no lo harían si su identidad real estuviera expuesta.por último, en internet encontramos menos factores disuasorios, la ausencia de vigilancia efectiva y la percepción de baja probabilidad de ser sancionado cuando se delinque en el ciberespacio eliminan los factores disuasorios que normalmente inhiben el comportamiento delictivo en el mundo físico. Por tanto, la falta de una estructura de control y aplicación de una ley coherente y global en este entorno contribuye a esta percepción de impunidad.

Estas afirmaciones encuentran respaldo en diversos estudios de psicología y criminología que han explorado el fenómeno del comportamiento desinhibido en contextos anónimos o semi-anónimos (Francisco et al., 2023; Martín-Martín et al., 2023; Suler, 2004). Estudios sobre el comportamiento en redes sociales, foros y otros entornos digitales han documentado una prevalencia significativa de conductas como el ciberacoso, la suplantación de identidad y el fraude, que son mucho menos comunes en contextos donde la identidad del individuo es conocida y fácilmente rastreable (Lapidot-Lefler & Barak, 2012)

- Importación y Exportación de Comportamientos Delictivos

  Este postulado afirma que el comportamiento delictivo manifestado en el ciberespacio puede influir y ser importado al espacio físico, y viceversa. Esta interacción bidireccional entre los dos entornos sugiere que las acciones delictivas en uno pueden tener repercusiones directas en el otro. Jaishankar sugiere que los individuos no operan de forma aislada dentro de un solo entorno, sino que sus comportamientos y experiencias en el ciberespacio pueden trasladarse al mundo físico, y los comportamientos desarrollados en el entorno físico pueden ser exportados al ciberespacio. Esta teoría es especialmente relevante en un mundo cada vez más interconectado donde las líneas entre lo digital y lo físico se desdibujan constantemente. Investigaciones sobre el ciberacoso han revelado que aquellos que acosan

en línea a menudo también muestran comportamientos agresivos en sus interacciones cara a cara (Hinduja & Patchin, 2008). De igual manera, alguien que participa en actividades delictivas en el mundo físico, como el tráfico de drogas, puede extender sus operaciones al ciberespacio mediante el uso de criptomonedas y mercados en la dark web (Holt & Bossler, 2014).

- Oportunidad de evasión en el ciberespacio

  Este postulado sugiere que las incursiones intermitentes de los delincuentes en el ciberespacio, combinadas con la naturaleza dinámica y espaciotemporal del mismo, proporcionan una oportunidad única para evadir la captura y las responsabilidades legales, destacando la capacidad de este entorno para ofrecer múltiples formas de ocultación y movilidad que no son posibles en el entorno físico. Jaishankar argumenta que el ciberespacio, debido a su vastedad y constante evolución, permite a los delincuentes navegar y actuar en diferentes plataformas y espacios virtuales sin dejar rastros fácilmente identificables. La ausencia de barreras físicas y la posibilidad de cambiar rápidamente de ubicación virtual facilitan la evasión de las autoridades y la continuidad de las actividades delictivas. Tecnologías como las redes privadas virtuales (VPNs), la navegación anónima a través de Tor y el uso de criptomonedas (Aldridge & Decary-Hétu, 2014) para transacciones ilícitas son ejemplos de cómo los delincuentes pueden aprovechar las características dinámicas del ciberespacio para evadir la detección y la captura (Clough, 2015; Holt & Bossler, 2016).

- Colaboración delictiva en el ciberespacio

  El quinto postulado se centra en la capacidad del ciberespacio para facilitar la colaboración entre individuos con intenciones delictivas, superando las barreras físicas que tradicionalmente han limitado este tipo de actividades. Jaishankar afirma que el ciberespacio ofrece una plataforma sin precedentes para la interacción y cooperación entre individuos que, de otro modo, no se conocerían ni tendrían la oportunidad de colaborar en

actividades delictivas. La naturaleza global y desmaterializada del ciberespacio permite a estos individuos superar las limitaciones geográficas y temporales, facilitando la planificación y ejecución de delitos a través de canales de comunicación digitales seguros y anónimos. Este postulado se desglosa en dos componentes: la unión de extraños en el ciberespacio para cometer delitos en el espacio físico y la colaboración entre asociados del espacio físico para cometer delitos en el ciberespacio. Es evidente que el ciberespacio permite que individuos con intereses delictivos comunes se encuentren y colaboren. Foros clandestinos, redes sociales, y la dark web actúan como puntos de encuentro para estos individuos, donde pueden compartir información, estrategias y recursos para la comisión de delitos en el espacio físico. Así mismo, este contexto facilita que individuos que ya tienen una relación en el espacio físico extiendan su colaboración a actividades delictivas en línea. Esto puede incluir la planificación de delitos informáticos, como el hacking, o la coordinación de estafas en línea. La facilidad de comunicación, la superación de la barrera del lenguaje y la capacidad de compartir datos en tiempo real amplifican la eficiencia y el alcance de estas actividades delictivas.

La colaboración delictiva facilitada por el ciberespacio ha sido documentada en diversas áreas de interés para la criminología. En esta línea, la investigación sobre la comunidad de hackers afirma que estos individuos a menudo forman grupos en línea para compartir conocimientos técnicos y coordinar ataques cibernéticos. Estos grupos, que pueden operar de forma descentralizada, utilizan diversas plataformas para comunicarse y planificar sus actividades (Perkins et al., 2023; Roque et al., 2023). Así mismo, estudios sobre terrorismo y radicalización en línea, muestran cómo las plataformas digitales permiten que individuos aislados se conecten con organizaciones terroristas, reciban instrucción y coordinen ataques. La investigación ha demostrado que el uso de redes sociales y foros es decisivo para la difusión de ideologías extremistas y la organización de actos terroristas (Iftikhar, 2024; Rahimi, 2011).

- Influencia del origen social en la propensión a cometer delitos en el ciberespacio

  En este postulado, Jaishankar, sostiene que individuos provenientes de sociedades cerradas tienen una mayor propensión a cometer delitos en el ciberespacio en comparación con aquellos provenientes de sociedades más abiertas, resaltando cómo el contexto social y cultural influye en el comportamiento delictivo en línea. El autor argumenta que las restricciones y limitaciones impuestas en sociedades cerradas fomentan un deseo reprimido de libertad y exploración que puede manifestarse en el ciberespacio al no poder hacerlo en el espacio físico. En estas sociedades, las normas estrictas y la vigilancia constante inhiben comportamientos que los individuos pueden sentirse tentados a explorar una vez que entran en un entorno más libre y anónimo como el ciberespacio. El ciberespacio, con su capacidad para reducir las barreras normativas, proporciona un entorno propicio para que estos individuos actúen de manera que no podrían en su entorno físico restringido. Investigaciones sobre el uso de internet en países con más normas orientadas a la censura muestran que los usuarios a menudo recurren a medios en línea para acceder a contenido prohibido, expresar opiniones contrarias al régimen y participar en actividades ilícitas (Akdeniz, 2016; Tsatsou, 2016).

- Conflicto de normas y valores entre el espacio físico y el ciberespacio

  El séptimo y último postulado plantea que el conflicto entre las normas y valores del espacio físico y del ciberespacio puede conducir a la comisión de ciberdelitos, debido a la disonancia normativa y ética que surge cuando las reglas sociales del mundo físico no se alinean con las del entorno digital. El entorno digital, al ser relativamente nuevo y en constante evolución, carece de un conjunto unificado de normas y valores que regulen el comportamiento de sus usuarios a nivel global, creando esta falta de cohesión normativa un espacio donde los individuos pueden actuar de forma contraria a las expectativas del mundo físico sin enfrentar las mismas consecuencias. Este conflicto normativo se ve exacerbado por la naturaleza

global del ciberespacio, donde interactúan usuarios de diversas culturas y sistemas legales, ya que lo que es considerado legal y ético en una jurisdicción puede ser ilegal e inmoral en otra, creando un entorno donde las normas están en constante conflicto.

La teoría de la Transición Espacial, aunque innovadora en su enfoque sobre el cibercrimen, presenta varias limitaciones significativas. En primer lugar, la teoría puede ser criticada por su falta de evidencia empírica robusta, ya que muchos de sus postulados no han sido suficientemente validados a través de estudios cuantitativos y cualitativos extensivos. Además, la teoría tiende a simplificar excesivamente las motivaciones detrás de los ciberdelitos, ignorando factores complejos como la psicología individual y las dinámicas socioeconómicas, factores que afectan al cibercrimen (Wall, 2007). Asimismo, su aplicabilidad universal es cuestionable, dado que las diferencias culturales y legales entre distintas jurisdicciones pueden influir en la relevancia y eficacia de sus postulados (Yar, 2005). En consecuencia, la teoría requiere una mayor investigación y adaptación para abordar las especificidades del comportamiento delictivo en el ciberespacio. Pese a estas limitaciones, puede servir como un complemento valioso a las teorías ambientales y otras teorías criminológicas, proporcionando una perspectiva adicional que ayuda a entender las dinámicas del comportamiento delictivo en el entorno digital. Esta integración puede enriquecer el análisis criminológico al incorporar factores específicos del ciberespacio que no son completamente abordados por las teorías tradicionales.

Tras la revisión de las teorías previamente expuestas, en el capítulo siguiente procederemos a integrar los contenidos analizados previamente con el objetivo de exponer las características con las que deberían contar las estrategias diseñadas para prevenir, o al menos reducir, la victimización de personas adultas mayores en el ciberespacio. Estas estrategias estarán fundamentadas en las diversas bases teóricas abordadas, orientando su desarrollo y aplicación efectiva en la protección

de esta población que puede encontrarse en una situación de vulnerabilidad mayor en el entorno digital.

CAPÍTULO 4: HACIA LA REDUCCIÓN DE LA CIBERVICTIMIZACIÓN EN PAM: ESTRATEGIAS DE PREVENCIÓN E INTERVENCIÓN

A pesar de que muchas de las técnicas de prevención situacional derivadas de las teorías previamente expuestas fueron formuladas originalmente para aplicarse en el espacio físico, estas también encuentran aplicabilidad en el entorno digital, con las modificaciones pertinentes.

Al centrar la atención en el perpetrador del delito, en lo relativo al incremento del esfuerzo percibido, es posible implementar medidas tales como el uso de firewalls, la constante actualización de los sistemas operativos, la instalación de programas antivirus, el fortalecimiento de las contraseñas y la implementación de la autenticación en dos pasos. En cuanto al aumento del riesgo percibido, se pueden emplear estrategias como la reducción del anonimato en diversas plataformas y sitios web, incrementando así la percepción de vigilancia por parte del potencial delincuente. Así mismo, para la eliminación de excusas, es recomendable la implementación de políticas claras que establezcan explícitamente las consecuencias de las acciones delictivas en línea, así como programas educativos que informen a los usuarios sobre la ilegalidad y las repercusiones de sus actos, incluyendo la perspectiva de la víctima, en el ciberespacio. Además, la promoción de normas éticas y comportamientos responsables en línea puede contribuir a la internalización de las expectativas de conducta y a disuadir el comportamiento delictivo.

Enfocándonos en la víctima, dada la relevancia de su rol como auto-guardián en el entorno digital, encontramos medidas diseñadas para reducir la esfera de influencia potencial del ciberdelincuente y su conducta. Estas medidas abarcan tanto la disminución de los objetos sobre los que puede realizarse la acción criminal, como la mitigación de los efectos lesivos de la misma en el ciberespacio (Miró-Llinares, 2011; Miró-Llinares, 2012). El papel de la víctima es clave, ya que, en el espacio digital, es necesario que la víctima realice una acción para que se produzca la victimización, como acceder a un sitio web no fiable, descargar un archivo infectado o proporcionar datos personales, entre otros. Por tanto, es necesario que la prevención atienda a la perspectiva de la decisión de la víctima, pues será ella quien, en muchos casos, determine si el riesgo creado por el ofensor

motivado se convierte en un daño real. Por tanto, en este caso no se trata de implementar medidas que reduzcan la percepción de los beneficios que el ciberdelincuente puede obtener, sino más bien de llevar a cabo acciones previas que disminuyan los objetos disponibles para el cibercrimen y que impidan la propagación de sus efectos si este se produce.

Sin embargo, no podemos obviar que la prevención situacional del cibercrimen, especialmente en las medidas en las que intervenga la propia víctima, pueden provocar un desplazamiento del objetivo elegido por el ciberdelincuente: este seleccionará aquel objetivo que le exija un menor esfuerzo criminal, que conlleve un menor riesgo de ser identificado y que pueda aumentar sus beneficios (Miró-Llinares, 2021). Este fenómeno es parte del paradigma del desplazamiento, definido como la respuesta de los delincuentes al bloqueo de las oportunidades criminales (Reppetto, 1976). En esencia, la prevención situacional no reduce la motivación interna para la comisión del delito, sino únicamente la oportunidad concreta de ejecutarlo en un ámbito determinado o contra un objetivo concreto, lo que lleva al delincuente a desplazarse hacia donde si pueda cometer el delito (Guerette & Bowers, 2009).

En el contexto específico del cibercrimen, se produce una adaptación tipológica, donde los delincuentes responden al bloqueo de un tipo específico de acto delictivo cometiendo delitos totalmente diferentes; una adaptación técnica, donde el ciberdelincuente mejora su ataque y utiliza nuevos instrumentos para superar las barreras; y una adaptación de objetivo, donde los ciberdelincuentes desechan el ataque a objetivos bien protegidos y centran sus esfuerzos en otros más vulnerables (Miró-Llinares, 2021). En este último punto es precisamente dónde la situación concreta de las PAM puede aumentar especialmente su situación de vulnerabilidad debido a su menor alfabetización digital (Loges & Jung, 2001) y, por tanto, una menor capacidad para implementar medidas de protección efectivas en este contexto, convirtiéndose en un objetivo ideal para los ciberdelincuentes.

Basándonos en esta información, y la expuesta en otros capítulos, es posible detallar algunos aspectos que deberían incluirse en las estrategias enfocadas tanto en la prevención del ciberdelito en personas adultas mayores como en el fomento

del uso de estas herramientas de una forma efectiva y segura, permitiendo que puedan beneficiarse de ellas.

4.1. Estrategias para fomentar un uso seguro y funcional de TIC en PAM

4.1.1 Programas para disminuir la cibervictimización capacitando a la persona usuaria como auto-guardián

A la luz de los factores previamente presentados, resulta patente la necesidad de implementar un enfoque holístico para enfrentar los diversos aspectos y riesgos inherentes a la ciberseguridad dentro de la población de adultos mayores. Dada la mayor incidencia de vulnerabilidades asociadas al fraude online en este grupo demográfico, cualquier programa de formación dirigido a estas personas debe integrar conocimientos específicos sobre la identificación de comunicaciones fraudulentas, la gestión segura de las transacciones financieras y una comprensión exhaustiva de las tácticas de ingeniería social utilizadas para manipular a los usuarios, ya sea para que divulguen información personal o realicen transferencias bancarias.

Asimismo, es pertinente que los adultos mayores aprendan a reconocer las señales de alerta que sugieren intentos de suplantación de identidad. Esto incluye un análisis minucioso de correos electrónicos que solicitan información personal de forma encubierta, llamadas telefónicas no solicitadas con ofertas de asistencia técnica y propuestas que aparentan ser demasiado ventajosas para ser verídicas. Para ilustrar estos peligros, es esencial utilizar ejemplos prácticos y simulaciones que permitan a los individuos experimentar de manera segura la presentación de estas prácticas engañosas, mejorando así su capacidad para identificar intentos de fraude y responder adecuadamente. Adicionalmente, la educación en seguridad en línea debe subrayar la importancia de mantener un escepticismo saludable frente a cualquier comunicación que demande alguna acción por parte del usuario, lo cual permitirá el desarrollo de un juicio crítico (Jampen et al., 2020), especialmente al considerar hacer clic en un enlace o descargar un archivo, particularmente si estos provienen de fuentes desconocidas o si el emisor subraya la urgencia de la acción.

Otro aspecto crucial en esta formación es la gestión de contraseñas, que requiere una atención especial. Es fundamental educar a este grupo demográfico sobre la

creación de contraseñas seguras y únicas para sus cuentas en línea, evitando el uso de información personal que sea fácil de adivinar. Esta instrucción debe incluir la utilización de administradores de contraseñas, los cuales permiten almacenar y organizar de manera segura estas contraseñas, eliminando la necesidad de recordar cada una de ellas y disminuyendo el riesgo de emplear contraseñas débiles por conveniencia (Chaudhary et al., 2019). Además, se debe enfatizar la importancia de la autenticación de dos factores (2FA) como una capa adicional de seguridad. La 2FA añade una barrera extra al requerir una segunda forma de verificación, como un código enviado al teléfono móvil, lo que aumenta significativamente la seguridad de las cuentas en línea. Es apropiado explicar de forma clara y detallada cómo funciona este mecanismo y por qué es eficaz para proteger las cuentas, incluso en caso de que la contraseña sea robusta.

Adicionalmente, es recomendable que la formación transmita un mensaje claro de autoeficacia, desafiando la noción preconcebida de que constituyen un grupo intrínsecamente vulnerable y subrayando su capacidad para gestionar las herramientas digitales de manera segura. La importancia de la autoeficacia percibida en la adopción de medidas preventivas ha sido resaltada en diversos estudios (Van Bavel et al., 2019). Por ende, es beneficioso que los programas formativos no solo impartan conocimientos técnicos, sino que también refuercen la percepción de competencia y empoderamiento entre los participantes. Al enfatizar que son perfectamente capaces de administrar su seguridad en línea, se fomenta una mayor confianza en sus habilidades digitales, lo cual es fundamental para la implementación efectiva de prácticas de seguridad recomendadas, tales como el uso de contraseñas robustas y la adopción de mecanismos de autenticación de dos factores.

No obstante, la instrucción en el ámbito de la ciberseguridad para este grupo enfrenta una serie de barreras de aprendizaje, ligadas fundamentalmente al diseño de las herramientas y a la alfabetización digital de este grupo, que afectan significativamente su capacidad para interactuar con la tecnología de forma eficaz y segura, por lo que es esencial que se incida también en estos aspectos.

4.1.2 Programas para fomentar el uso efectivo de las TIC en PAM

La falta de familiaridad y comprensión de la terminología digital constituye uno de los principales obstáculos, ya que genera inseguridad al utilizar estas herramientas, debido al temor de cometer errores (Olphert & Damodaran, 2013). Términos como «enlace» o «nube», entre otros, pueden resultar confusos y, sin una explicación clara y personalizada, pueden aumentar los sentimientos de exclusión y analfabetismo digital cuando se les proporciona información relacionada el entorno digital. Esta situación se ve exacerbada por la rápida evolución tanto del lenguaje tecnológico como de las diversas herramientas digitales, lo que puede llevar a que incluso las personas usuarias que cuentan con ciertas habilidades digitales perciban que sus conocimientos pronto se vuelven obsoletos. demás de los desafíos relacionados con la terminología digital, existen dificultades técnicas inherentes al uso de dispositivos y software.

Adicionalmente, la interfaz de usuario de numerosos dispositivos y aplicaciones tecnológicas a menudo no está diseñada teniendo en cuenta a los usuarios de mayor edad (Xie, 2003), lo cual genera problemas como el tamaño reducido de la letra, botones poco intuitivos y configuraciones complejas que pueden resultar abrumadoras, incrementando así la inseguridad al interactuar con estas tecnologías. Asimismo, estas dificultades se agravan cuando se presentan limitaciones físicas comunes en los usuarios de mayor edad, tales como la disminución de la destreza manual, problemas de visión y una menor capacidad para retener información a corto plazo. Por lo tanto, la combinación de estas características específicas con un enfoque de formación insuficientemente adaptado puede exacerbar los sentimientos de inseguridad y perpetuar la percepción de que la tecnología es intrínsecamente compleja y fuera de su alcance.

En consecuencia, es pertinente que los programas de formación se estructuren con un enfoque inclusivo y accesible, tomando en cuenta no solo las barreras cognitivas y emocionales, sino también las limitaciones físicas inherentes a los usuarios de mayor edad. Esto requiere la creación de interfaces de usuario más amigables, con tipografías ampliadas, botones claramente identificables y configuraciones simplificadas. Además, es fundamental que el contenido de la formación se ajuste a

las necesidades y capacidades de este grupo demográfico, utilizando métodos de enseñanza claros, pausados y repetitivos para garantizar una comprensión sólida y duradera. Por ejemplo, en lugar de simplemente presentar los conceptos técnicos de forma abstracta, es beneficioso contextualizarlos dentro de experiencias y conocimientos previos de los usuarios. Este enfoque facilita una conexión más intuitiva y reduce la percepción de complejidad. Además, la implementación de sesiones prácticas donde los usuarios puedan aplicar directamente lo aprendido contribuye significativamente a la retención del conocimiento y al aumento de la confianza en el manejo de las tecnologías.

Adicionalmente, la implementación de herramientas de asistencia, tales como lupas digitales, teclados ergonómicos y software de reconocimiento de voz, puede ser sumamente beneficiosa para mitigar las limitaciones físicas y optimizar la experiencia de uso de la tecnología. Estas herramientas no solo facilitan la interacción con dispositivos digitales, sino que también fomentan una mayor autonomía y confianza en su utilización. El empleo de lupas digitales, por ejemplo, permite a los usuarios con problemas de visión leer textos en pantalla con mayor facilidad, mientras que los teclados ergonómicos pueden reducir la tensión en las manos y muñecas, favoreciendo a aquellos con destrezas manuales reducidas. Por su parte, el software de reconocimiento de voz posibilita la realización de tareas mediante comandos hablados, lo cual es particularmente útil para usuarios con dificultades para escribir o manipular dispositivos. De este modo, al integrar estas tecnologías de asistencia en los programas de formación y en el diseño de interfaces, se promueve una experiencia de uso más accesible y personalizada, contribuyendo a una inclusión digital más efectiva de las personas adultas mayores en la sociedad actual. Esto no solo mejora la competencia técnica, sino que también empodera a los adultos mayores, permitiéndoles participar activamente sin depender de otras personas en el proceso.

Otro aspecto esencial es la configuración de una red de apoyo robusta que involucre diversas áreas, incluidas las comunidades de aprendizaje y la adopción de políticas públicas orientadas a promover la inclusión digital efectiva y segura de las personas adultas mayores, lo cual constituye un componente fundamental en el proceso de digitalización de este grupo poblacional (Xie et al., 2020). Por un lado,

incentivar el contacto intergeneracional puede actuar como un catalizador positivo, considerando que la interacción entre generaciones representa un factor crucial en la atenuación de los estereotipos asociados con la edad (Levy, 2006). Esto, a su vez, contribuye significativamente a la mitigación del edadismo y a la desconstrucción de los prejuicios relacionados con el uso de TIC en este grupo etario, propiciando la colaboración y generando un entorno de comprensión y respeto mutuo entre diferentes grupos etarios. Este intercambio de conocimientos y experiencias enriquece a ambas partes y fomenta una cultura de inclusión y respeto hacia los individuos de todas las edades, contribuyendo así a una sociedad más equitativa y libre de discriminación etaria. Por otro lado, las comunidades de aprendizaje entre pares, donde personas adultas mayores actúan como formadores y apoyo para otros dentro del mismo grupo etario, pueden producir resultados sumamente positivos. La promoción de la formación de grupos de aprendizaje donde las PAM puedan compartir experiencias, conocimientos y soluciones, permite la creación de un entorno de apoyo mutuo que facilita la adquisición de habilidades digitales. Este enfoque colaborativo no solo refuerza el aprendizaje individual a través de la interacción social, sino que también contribuye a la reducción del aislamiento, potenciando la confianza y la motivación para enfrentarse a los desafíos tecnológicos. La eficacia de las comunidades de aprendizaje entre pares radica en su capacidad para adaptarse a las necesidades específicas de sus miembros, ofreciendo un espacio seguro para la exploración y la experimentación digital (Nicholson et al., 2021).

Además, la colaboración con entidades locales, tales como bibliotecas, ayuntamientos y asociaciones comunitarias, constituye un elemento crucial en el fortalecimiento de la red de apoyo digital para las PAM. Estas instituciones emergen como agentes de cambio esenciales en la provisión de talleres, conferencias y sesiones educativas enfocadas en la seguridad en línea y otras áreas relevantes de la digitalización (Lenstra, 2017). En este ámbito, es fundamental adoptar estrategias inclusivas y accesibles en la difusión de la formación digital, especialmente considerando que la divulgación de estos recursos a menudo se realiza a través de medios digitales, lo cual puede representar una barrera significativa para las PAM que aún no están familiarizadas con estas tecnologías.

Adicionalmente, los gobiernos, en colaboración con instituciones públicas y privadas, pueden liderar la creación de políticas y programas que promuevan la alfabetización digital y la seguridad en línea de los adultos mayores. Esto implica la inversión en la educación digital y en la infraestructura tecnológica necesaria para garantizar el acceso universal a servicios digitales seguros y confiables. Un aspecto a tener en cuenta es el desarrollo de estos programas, así como de la legislación asociada al ámbito digital, desde una perspectiva centrada en el usuario y todas las áreas implicadas, fomentando una comprensión holística que ayude a reducir la percepción de la edad como un factor determinante en el uso de TIC (Sourbati, 2009).

En definitiva, la construcción de una red de apoyo sólida, la promoción de comunidades de aprendizaje entre pares y la implementación de políticas públicas inclusivas, constituyen pilares fundamentales para la inclusión digital de las personas adultas mayores, asegurando así que puedan beneficiarse plenamente de las oportunidades que ofrece la tecnología en la sociedad contemporánea. Así mismo, sería beneficiosa la adopción de un enfoque participativo de este grupo etario en el proceso de diseño, tanto de las diversas herramientas como de las iniciativas relacionadas con la digitalización. Incorporar activamente las perspectivas del conjunto de la sociedad es esencial para asegurar que las TIC sean verdaderamente universales y respondan a las necesidades de todos los sectores de la población (Zhang, 2023). Esto requiere un compromiso con métodos de investigación cualitativa y cuantitativa que puedan capturar de forma efectiva las experiencias y expectativas de las personas adultas mayores, así como un enfoque interdisciplinario que promueva un diseño inclusivo del entorno digital.

PARTE II: APROXIMACIÓN EMPÍRICA AL ESTUDIO DE PERSONAS ADULTAS MAYORES EN EL CIBERESPACIO

OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS DE LA INVESTIGACIÓN EMPÍRICA

El objetivo general de la investigación empírica llevada a cabo en el marco de esta tesis doctoral radica en el análisis y la comprensión de la relación existente entre la población adulta mayor y las TIC. En última instancia se pretende determinar las áreas y dimensiones relevantes para la evaluación e intervención en el ámbito digital de este grupo etario. Para cumplir con estos objetivos, se establecen los siguientes objetivos específicos:

- Analizar características psicosociales y de afrontamiento ante una sociedad altamente digitalizada en personas adultas mayores usuarias de TIC, así como el tipo de uso y tiempo dedicado a estas herramientas.

- Detectar las diferencias entre las personas adultas mayores que implementan la tecnología a sus actividades diarias y aquellas que no lo hacen, incidiendo en las consecuencias emocionales, sociales y la posible presencia de miedo funcional y disfuncional en este grupo.

- Examinar la cibervictimización sufrida por las PAM, incluyendo su notificación, conductas de protección, percepción de vulnerabilidad y formación relacionada con las TIC.

- Analizar las consecuencias económicas y emocionales de la cibervictimización en este grupo etario.

En función de estos objetivos se presentan las investigaciones realizadas en los próximos capítulos.

CAPÍTULO 5: AFRONTAMIENTO Y USO DE TIC EN PERSONAS ADULTAS MAYORES

5.1 JUSTIFICACIÓN DEL ESTUDIO

Este estudio se explora cuál es la posible relación entre algunos factores psicosociales que podrían estar influyendo en el empleo de las TIC en la población de personas adultas mayores. Según lo expuesto en la parte teórica de esta tesis doctoral, sabemos que la gran digitalización que permea nuestra sociedad ha precipitado la necesidad de adaptación a las herramientas tecnológicas a todos los sectores poblacionales. Una adaptación que se extiende no solo a la esfera de las interacciones sociales, sino también al área laboral, de ocio y a los servicios fundamentales como la atención sanitaria, la banca o la educación. En este contexto de alta digitalización, es necesario confrontar los desafíos emergentes que la sociedad plantea, dado que una adaptación deficiente podría desencadenar problemas significativos en la dinámica social y personal de los usuarios de estas herramientas.

En esta línea, uno de los factores que puede conllevar una diferencia en la adaptación a entornos o situaciones que en inicio suponen un desafío es la Resiliencia, conceptualizada como la capacidad de un sistema, siendo este un individuo, un grupo o una cultura, para hacer frente de forma exitosa a los desafíos que amenazan su viabilidad, funcionamiento y desarrollo (Masten, 2001). Este rasgo adquiere especial relevancia en el grupo etario de las personas adultas mayores, pues las herramientas digitales, en muchos casos, suponen un reto no trivial (Bonanno et al., 2007). En oposición a la Resiliencia, encontramos la "Evitación experiencial", definida como la tendencia de un individuo a esquivar el enfrentamiento con experiencias internas que resultan desagradables, tales como sensaciones corporales, emociones, pensamientos o predisposiciones conductuales, intentando modificar la frecuencia o naturaleza de estos eventos y el contexto que los provoca (Hayes et al., 1996). Existen numerosas investigaciones que señalan una correlación positiva entre esta variable, la Evitación Experiencial, y el desarrollo de trastornos a largo plazo, relacionados con la ansiedad (Glick &

Orsillo, 2011; Kashdan et al., 2006; Santanello & Gardner, 2007), las tentativas de suicidio (Ellis & Rufino, 2016; Skinner et al.,2016) o la aparición de conductas problemáticas y desadaptativas (Chawla & Ostafin, 2007).

Adicionalmente, considerando las características diferenciales de este grupo demográfico, es relevante tener en cuenta el fenómeno de la soledad definida como la vivencia subjetiva de un déficit en las interacciones sociales (Peplau & Perlman, 1982). Una alta soledad percibida puede incrementar el riesgo de desarrollar patologías como la depresión o la ansiedad y, si se prolonga en el tiempo, podría derivar en problemas adicionales como la estigmatización y el aislamiento social (Hawkley & Cacioppo, 2010).

Tal y como la literatura indica en relación a la disposición al uso de las TIC, es esencial considerar la capacidad percibida en el uso de tecnología, un factor que, como se ha discutido en capítulos previos, podría influir de manera significativa en la adopción y utilización efectiva de las TIC, incidiendo tanto en la autoconfianza como en la disposición para enfrentar los desafíos inherentes a la digitalización. Al focalizarnos en constructos como la Resiliencia, la Evitación Experiencial, la percepción de soledad y la capacidad percibida en el uso de TIC, aspiramos a elucidar cómo estos factores se interrelacionan con el empleo de dichas herramientas en esta específica cohorte poblacional.

5.2 OBJETIVOS DEL ESTUDIO

El objetivo principal de este estudio es examinar la relación entre el uso de internet por parte de las PAM y su relación con la soledad, la resiliencia y la evitación experiencial.

Para lograr este objetivo principal, se definieron varios objetivos específicas, los cuales incluyeron:

- Caracterizar las características sociodemográficas, los patrones de uso de Internet, y los perfiles psicológicos (evitación experiencial, resiliencia, percepción de soledad) de las personas adultas mayores usuarias de

internet, y comparar cómo estas variables difieren entre distintos tipos y frecuencias de uso.

- Explorar las interacciones entre el uso de Internet y los factores psicológicos, y determinar cómo las variables de uso de Internet, la capacidad tecnológica autopercibida y las características sociodemográficas pueden predecir aspectos psicológicos como la evitación experiencial, la resiliencia y la percepción de soledad.

- Identificar perfiles distintos de usuarios de Internet en la población adulta mayor, basándose en sus características sociodemográficas y psicosociales.

Estos objetivos específicos fueron establecidos para proporcionar una comprensión de las dinámicas subyacentes que podrían estar influyendo en cómo los individuos de más edad se adaptan y responden a la integración de las tecnologías digitales en su vida cotidiana.

5.3 METODOLOGÍA

5.3.1 Procedimiento

La recolección de datos se llevó a cabo en línea mediante un cuestionario de Google Forms diseñado para el estudio. Se proporcionó acceso al cuestionario electrónico a los participantes a través de un enlace enviado por la aplicación WhatsApp, redes sociales (Facebook y Twitter) y mediante correos electrónicos enviados a la base de datos de las instituciones colaboradoras (universidades participantes en el estudio). Para iniciar la recolección de datos, se utilizó un muestreo por bola de nieve. Los criterios de inclusión para participar en el estudio eran ser mayor de 18 años y tener un dispositivo con acceso a internet a través del cual completar el cuestionario. En nuestro caso, seleccionamos posteriormente los participantes que tenían 65 años o más. El cuestionario

comenzaba con una descripción de los objetivos del estudio, la política de protección de datos, el consentimiento para participar en el estudio y un compromiso de confidencialidad. La difusión del cuestionario y la recolección de datos comenzaron el 18 de septiembre de 2021 y finalizaron el 10 de enero de 2022. El Comité de Revisión Interna de la Universidad que organizó el estudio aprobó previamente el procedimiento (ref. 436/20/26).

5.3.2 Variables e instrumentos

Los instrumentos y variables tenidas en cuenta en la obtención de los datos fueron los siguientes:

a) Variables sociodemográficas de los participantes: género, edad y estado civil.

b) Evitación experiencial (EE): Versión española del Cuestionario de Aceptación y Acción II (AAQ-II, Ruiz et al., 2013). El instrumento está compuesto por 7 ítems con una escala Likert de 7 puntos (1 = nunca verdadero; 7 = siempre verdadero), con puntuaciones que varían entre 7 y 49 puntos. Se ha informado que este instrumento tiene buenas propiedades psicométricas en diversas poblaciones (Bond et al., 2011). En la adaptación a la muestra española (Ruiz et al., 2013), se obtuvo una buena consistencia (entre 0.75 y 0.93). En el presente estudio, obtuvimos un α de Cronbach=0.904.

c) Resiliencia: Versión española (Tomás et al., 2012) de la Brief Resilient Coping Scale (Sinclair & Wallston, 2004). La escala consta de 4 ítems que se evalúan utilizando una escala Likert de cinco puntos, desde 1 (no me describe en absoluto) hasta 5 (me describe muy bien), con puntuaciones que varían entre 4 y 20. La versión original de Sinclair y Wallston (2004) tenía un α de Cronbach=0.69. En el presente trabajo, obtuvimos un α de Cronbach=0.762.

d) Percepción de soledad: Escala breve de soledad de UCLA de 3 ítems (Hughes et al., 2004). La escala consta de 3 ítems, con 1 correspondiente a "casi nunca", 2 a "algunas veces" y 3 a "a menudo", por lo tanto, las puntuaciones de la escala estarán entre 3 y 9 puntos. En el estudio de validación de la versión española de la escala (Pedroso-Chaparro et al., 2022), se obtuvo un α de Cronbach=0.78. En el presente estudio, obtuvimos un α de Cronbach=0.792.

e) Frecuencia de uso de internet, usos y capacidad percibida: Se midió el número de horas por día y el número de días por semana que las personas utilizaban internet, así como la capacidad percibida en el uso de la tecnología, mediante una escala Likert del 1 al 5, dónde 1 hacía referencia a "Nada competente" y 5 "Totalmente competente". Así mismo se incluyeron diferentes tipos de uso de internet (Relaciones sociales, búsqueda de información, gestiones bancarias y compras online, correos electrónicos), teniendo los participantes que indicar si realizaban estas conductas concretas por internet o no.

5.3.3 Muestra final

La muestra final estuvo compuesta por 274 personas entre 65 y 84 años (*M*= 70.46; *DE*= 4.42), de las cuales el 61.7% eran mujeres. La Tabla 1 describe las características sociodemográficas de la muestra con más detalle.

Tabla 1. *Características sociodemográficas*

	N, (%)
Estado civil	
Soltero/a	33 (12)
Casado/a o viviendo en pareja	151 (55.1)
Divorciado/a o separado/a	49 (17.9)

Viudo/a	41 (15)
Género	
Masculino	105 (38.3)
Femenino	169 (61.7)

5.3.4 Análisis de datos

En primer lugar, se llevaron a cabo análisis descriptivos para resumir las características principales de las variables sociodemográficas y las variables psicológicas (evitación experiencial, resiliencia, percepción de soledad) y de uso de internet (frecuencia de uso, tipos de uso, capacidad tecnológica autopercibida). Posteriormente, se realizaron correlaciones de Pearson para examinar las relaciones bivariadas entre las variables psicológicas y de uso de internet. Para comparar las medias de las variables psicológicas según los diferentes usos de internet, se emplearon pruebas t de Student para muestras independientes. Además, se llevaron a cabo análisis de regresión lineal múltiple para evaluar cómo las variables de uso de internet, la capacidad tecnológica autopercibida y las variables sociodemográficas (sexo, estado civil, edad) predicen la Evitación Experiencial, la Resiliencia y la percepción de soledad. Finalmente, se realizó un análisis de clusters para identificar grupos homogéneos dentro de la muestra basados en los patrones de uso de internet y las variables psicosociales. El análisis de clusters es una técnica exploratoria que agrupa casos similares para detectar estructuras subyacentes en los datos, permitiendo una mejor comprensión de los diferentes perfiles de usuarios y sus características asociadas. El conjunto de análisis estadísticos se llevó a cabo utilizando SPSS v28. En todos los análisis, se consideraron valores inferiores a 0.05 como estadísticamente significativos.

5.4 RESULTADOS

5.4.1 Análisis descriptivo

La Tabla 2 presenta los estadísticos descriptivos de las principales variables del estudio, incluyendo la evitación experiencial, la percepción de soledad, la resiliencia, y varias medidas relacionadas con el uso de Internet y la capacidad tecnológica autopercibida. El uso medio de Internet del grupo fue de 2.67 horas diarias y 18.53 horas semanales. En cuanto a la capacidad tecnológica autopercibida, pudiendo encontrarse esta en el rango de 1 a 5, la media fue de 3.61. Para la EE, las puntuaciones oscilaron entre 7 y 43 puntos, con una media grupal de 20.06 puntos. La resiliencia, con un rango posible de 4 a 20 puntos, presenta una media general de 15.35. En cuanto a la soledad percibida el rango posible fue de 3 a 9 puntos, siendo la media general 4.29.

Tabla 2. *Estadísticos descriptivos de variables continuas*

	M, (DE)
Evitación experiencial	20.06 (6.543)
Percepción de soledad	4.29 (1.425)
Resiliencia	15.35 (3.393)
Días semanales de uso de internet	6.56 (1.114)
Horas diarias de uso de internet	2.67 (1.746)
Capacidad tecnológica autopercibida	3.61 (.8)

M= media; *DE*= Desviación estándar

La Tabla 3 presenta los estadísticos descriptivos de las variables categóricas del estudio, en este caso los diferentes usos de Internet entre los participantes del. Se observa que la mayoría de los participantes utilizan Internet para relacionarse (90.1%) y para buscar información (91.9%). Un porcentaje significativo también utiliza Internet para realizar gestiones bancarias y compras online (78.0%), así como para enviar correos electrónicos (80.2%).

Solamente un pequeño porcentaje de los participantes informó que no usaba internet en absoluto (1.1%).

Tabla 3. *Descriptivos usos de internet*

	N, (%)
Relaciones sociales	
Si	246 (90.1)
No	27 (9.9)
Buscar información	
Si	251 (91.9)
No	22 (8.1)
Hacer gestiones bancarias y compras online	
Si	213 (78)
No	60 (22)
Enviar correos electrónicos	
Si	219 (80.2)
No	54 (19.8)

5.4.2 Correlación de Pearson

En cuanto a las correlaciones de Pearson entre las variables principales del estudio se observó una correlación negativa significativa entre la evitación experiencial y la resiliencia ($r = -0.333$, $p < 0.001$), lo que sugiere que mayores niveles de evitación experiencial se asocian con menores niveles de resiliencia. Asimismo, la evitación experiencial mostró una correlación positiva significativa con la percepción de soledad ($r = 0.500$, $p < 0.001$), indicando que mayores niveles de evitación experiencial están asociados con mayores niveles de soledad. La percepción de soledad también correlacionó negativamente con la resiliencia ($r = -0.135$, $p < 0.05$), sugiriendo que mayores niveles de soledad están asociados con menores niveles de resiliencia. No se encontraron correlaciones significativas entre la evitación experiencial y el uso de internet en horas por semana ($r = -0.022$, $p = 0.733$). Referido a la capacidad tecnológica autopercibida, se encontró una correlación negativa significativa con la evitación experiencial ($r = -0.129$, $p < 0.05$) y una correlación positiva

significativa con la resiliencia (r = 0.197, p < 0.001), lo que indica que una mayor capacidad tecnológica autopercibida se asocia con menores niveles de evitación experiencial y mayores niveles de resiliencia. En la tabla 4 se muestran la totalidad de resultados de estas correlaciones.

Tabla 4. *Correlaciones de Pearson*

Variables	1	2	3	4	5
1. Evitación experiencial	1	-0.333**	0.500**	-0.022	-0.129*
2. Resiliencia	-0.333**	1	-0.135*	0.062	0.197**
3. Soledad	0.500**	-0.135*	1	-0.073	-0.085
4. Horas internet a la semana	-0.022	0.062	-0.073	1	0.183**
5.Capacidad tecnológica autopercibida	-0.129*	0.197**	-0.085	0.183**	1

**p < 0.01, *p < 0.05.

5.4.3 Pruebas t de Student

Se realizaron pruebas t de Student para comparar las puntuaciones de evitación experiencial, soledad, resiliencia y capacidad tecnológica autopercibida entre los usuarios y no usuarios de diferentes herramientas de internet (relaciones sociales, búsqueda de información, gestiones bancarias/compras y correos electrónicos).

No se encontraron diferencias significativas en evitación experiencial entre usuarios y no usuarios de internet para relacionarse (t(271) = 1.427, p = 0.155), buscar información (t(271) = 0.657, p = 0.511), realizar gestiones bancarias/compras (t(271) = 1.062, p = 0.289) y enviar correos electrónicos (t(271) = 2.149, p = 0.033). Sin embargo, la evitación experiencial fue significativamente mayor en los usuarios de correos electrónicos en

comparación con los no usuarios (diferencia de medias = 2.125, IC 95% [0.178, 4.071]). Asimismo, no se encontraron diferencias significativas en la percepción de soledad entre usuarios y no usuarios de internet para relacionarse (t(269) = 1.173, p = 0.242), buscar información (t(269) = 0.471, p = 0.638), realizar gestiones bancarias/compras (t(269) = -0.101, p = 0.919) y enviar correos electrónicos (t(269) = -0.135, p = 0.893). En cuanto a la capacidad tecnológica autopercibida, tampoco se observaron diferencias significativas entre usuarios y no usuarios de internet para relacionarse (t(267) = -1.251, p = 0.212), buscar información (t(267) = -0.636, p = 0.526), realizar gestiones bancarias/compras (t(267) = -1.364, p = 0.174) y enviar correos electrónicos (t(267) = -1.488, p = 0.138). Por último, los análisis no mostraron diferencias significativas en resiliencia entre usuarios y no usuarios de internet para relacionarse (t(271) = -1.218, p = 0.224), buscar información (t(271) = -0.696, p = 0.487), realizar gestiones bancarias/compras (t(271) = -1.167, p = 0.868) y enviar correos electrónicos (t(271) = -0.392, p = 0.695).

5.4.4 Regresión lineal

Se realizaron análisis de regresión lineal para evaluar cómo las variables de uso de internet, capacidad tecnológica autopercibida y variables sociodemográficas (sexo, estado civil, edad) pueden predecir las variables psicosociales de interés en nuestro estudio (la evitación experiencial, la resiliencia y la percepción de soledad). Los resultados se presentan en las Tablas 5, 6 y 7.

Tabla 5*. Regresión lineal evitación experiencial*

Variable independiente	B	Error estándar	t	p
(Constante)	30.365	6.876	4.416	<0.001
Horas internet a la semana	-0.007	0.028	-0.237	0.813
Sexo	-0.123	0.819	-0.150	0.881
Edad	-0.109	0.094	-1.160	0.247
Estado civil	-0.086	0.466	-0.184	0.855
Capacidad tecnológica autopercibida	-0.737	0.520	-1.416	0.158

Variable dependiente = Puntuación total de evitación experiencial.

El modelo completo no fue significativo ($F(5, 241) = 0.752$, $p = 0.585$), indicando que las variables independientes incluidas en el modelo no explican significativamente la variabilidad en la evitación experiencial. El valor de R^2 fue 0.015, lo que sugiere que solo el 1.5% de la varianza en la evitación experiencial está explicado por las variables independientes.

Tabla 6. *Regresión lineal percepción soledad*

Variable independiente	B	Error estándar	t	p
(Constante)	4.548	1.477	3.079	0.002
Horas Internet a la semana	-0.005	0.006	-0.901	0.369
Sexo	0.540	0.176	3.069	0.002
Edad	-0.011	0.020	-0.538	0.591
Estado civil	0.429	0.100	4.292	<0.001
Capacidad tecnológica autopercibida	-0.218	0.112	-1.949	0.052

Variable dependiente = Puntuación total de soledad.

El modelo completo fue significativo ($F(5, 240) = 6.526$, $p < 0.001$), indicando que las variables independientes incluidas en el modelo explican significativamente la variabilidad en la percepción de soledad. El valor de R^2 fue 0.120, lo que sugiere que el 12% de la varianza en la percepción de soledad está explicado por las variables independientes. Las variables independientes que fueron predictores significativos de la percepción de soledad incluyen el sexo ($B = 0.540$, $p = 0.002$) y el estado civil ($B = 0.429$, $p < 0.001$). La capacidad percibida del uso de tecnología mostró una tendencia a ser significativa ($B = -0.218$, $p = 0.052$), mientras que las horas de uso de internet por semana ($B = -0.005$, $p = 0.369$) y la edad ($B = -0.011$, $p = 0.591$) no fueron predictores significativos.

Tabla 7. *Regresión lineal resiliencia*

Variable independiente	B	Error estándar	t	p
(Constante)	12.119	3.532	3.432	<0.001
Horas Internet a la semana	0.005	0.014	0.384	0.701
Sexo	0.075	0.421	0.179	0.858
Edad	-0.008	0.048	-0.176	0.860
Estado civil	0.350	0.239	1.465	0.144
Capacidad tecnológica autopercibida	0.811	0.267	3.033	0.003

Variable dependiente = Puntuación total de resiliencia

El modelo completo fue significativo ($F(5, 246) = 2.730$, $p = 0.020$), indicando que las variables independientes incluidas en el modelo explican significativamente la variabilidad en la resiliencia. El valor de R^2 fue 0.054, lo que sugiere que el 5.4% de la varianza en la resiliencia está explicado por las variables independientes. La capacidad percibida del uso de tecnología fue un predictor significativo de la resiliencia ($B = 0.811$, $p = 0.003$), lo que sugiere que una mayor capacidad tecnológica autopercibida se asocia con mayores niveles de resiliencia. Sin embargo, las horas de uso de internet por semana ($B = 0.005$, $p = 0.701$), el sexo ($B = 0.075$, $p = 0.858$), la edad ($B = -0.008$, $p = 0.860$) y el estado civil ($B = 0.350$, $p = 0.144$) no fueron predictores significativos.

5..4.5 Análisis de Clusters

Para identificar grupos homogéneos dentro de la muestra basados en los patrones de uso de internet y las variables psicológicas, se realizó un análisis de clusters utilizando el método K-means. Los resultados del análisis identificaron cuatro clusters distintos.

El Cluster 1, que comprende 83 casos, se caracteriza por un uso moderado de internet (24.51 horas por semana) y altos niveles de capacidad percibida en el

uso de tecnología. Las puntuaciones de soledad, evitación experiencial y resiliencia en este grupo son moderadas.

El Cluster 2, con 15 casos, muestra un uso mayor de internet (54 horas por semana), alta capacidad tecnológica percibida y puntuaciones moderadas en las variables soledad, evitación experiencial y resiliencia.

El Cluster 3, el grupo más grande (146 casos), se distingue por un uso bajo de internet (10.70 horas por semana) y una capacidad tecnológica autopercibida más baja. Las puntuaciones de soledad, evitación experiencial y resiliencia son similares a las de los otros clusters.

Finalmente, el Cluster 4, que contiene un solo caso, se caracteriza por un uso extremadamente alto de internet (144 horas por semana), alta capacidad tecnológica percibida, bajas puntuaciones de soledad y resiliencia ligeramente más alta.

5.5 DISCUSIÓN Y CONCLUSIONES

En la presente investigación, se delineó un perfil descriptivo de nuestra muestra para elucidar cómo las variables "uso de Internet", "soledad percibida", "Resiliencia" y "Evitación Experiencial" se interrelacionan entre sí en personas de 65 años o más, situados dentro de un contexto eminentemente digitalizado. Nuestro análisis reveló que el uso promedio de Internet entre los participantes es de 2.67 horas diarias y 18.53 horas semanales, y que la autoevaluación de competencia tecnológica arroja un nivel moderado dentro de este grupo, con una media de 3.61 en una escala de 1 a 5. Estos datos son consonantes con investigaciones anteriores que resaltan la pertinencia de la competencia tecnológica en los procesos de adaptación a la digitalización avanzada, teniendo en cuenta que todas las personas que participaron en el estudio eran usuarias de TIC (Golz et al., 2021; La Torre at al., 2019). En cuanto a los tipos de uso de internet se observó que su aplicación para establecer relaciones sociales y búsqueda de

información fue notablemente alto, lo que subraya la importancia de esta tecnología como un vehículo de integración social y acceso al conocimiento.

Respecto a la "Evitación Experiencial", las puntuaciones oscilaron entre 7 y 43 puntos, con una media de 20.06 puntos. La "Resiliencia", con un rango posible de 4 a 20 puntos, presentó una media de 15.35. En cuanto a la "Soledad "Percibida", con un rango posible de 3 a 9 puntos, la media fue de 4.29. Es pertinente destacar la ausencia de un punto de corte clínico establecido para las pruebas de resiliencia y soledad. En el caso del indicador de evitación experiencial, se ha establecido que la puntuación clínica media es de alrededor de 29 puntos, y nuestra muestra, teniendo en cuenta las puntuaciones medias, no alcanza este umbral, aunque si lo hacen individuos concretos. Es necesario señalar en este punto que el estudio inicial, como se ha señalado previamente, incluía a individuos desde los 18 años y se realizaron comparaciones por grupos de edad. A pesar de que los estudios sugieren que la soledad percibida aumenta con la edad (Hämmig, 2019; Nicolaisen & Thorsen, 2016), nuestros hallazgos parecen contradictorios a esta tendencia, ya que el grupo de adultos mayores fue el que menos puntuación obtuvo en esta variable, alineándose en cambio con otros estudios que cuestionan si la edad es un factor determinante en este aspecto (Ferreira-Alves et al., 2014; Nguyen et al., 2020).

Por último, es importante subrayar que este estudio se realizó justo después del confinamiento experimentado durante la pandemia de COVID-19, y los individuos más jóvenes enfrentaron este evento de manera más adversa que otros grupos poblacionales (Morales-Vives et al., 2020; Schlomann et al., 2022), por lo que sería prudente replicar el estudio fuera de este contexto. De hecho, la mayoría de los estudios realizados durante la pandemia por COVID-19 realizados en este ámbito señalaron a las personas adultas mayores como el grupo más resiliente y que mejor se había adaptado al periodo de confinamiento (Czeisler et al., 2020; García-Portilla et al., 2021; Kobayashi et al., 2021; Losada-Baltar et al., 20201,2; Nwachukwu et al., 2020). La interpretación de estos datos llevo a afirmar que la edad emerge como un factor clave en la respuesta a la pandemia, y probablemente a otros sucesos que requieran una adaptación, vinculado a una menor incidencia de síntomas graves y una capacidad de adaptación más robusta. Sin embargo, estos

datos contaban con un sesgo significativo: representan a aquellos adultos mayores con acceso y habilidades para utilizar las TIC, no a la totalidad de este colectivo. Esta distinción resulta particularmente esencial cuando se examina la población adulta mayor, puesto que no es posible extrapolar los resultados obtenidos de un subconjunto digitalmente competente al conjunto general, dada la marcada brecha digital existente y teniendo en cuenta que los usuarios de internet en este grupo etario no alcanzan las altas tasas que se manejan en otros grupos. La implicación de este sesgo en la interpretación de la adaptación y la salud mental es profunda: sugiere que podría haber una porción oculta de la población adulta mayor que, sin las competencias digitales necesarias, podría estar enfrentando niveles de estrés psicosocial y aislamiento significativamente mayores, con efectos potencialmente devastadores sobre su bienestar mental. En consecuencia, es necesario una reflexión crítica sobre las políticas de salud pública y las estrategias de intervención social para atender este desafío y mitigar las desigualdades en la salud mental que la brecha digital podría estar exacerbando en aquellas personas que no están utilizando estas herramientas.

En cuanto a las correlaciones entre las variables principales del estudio, se observó una correlación negativa significativa entre la evitación experiencial y la resiliencia, lo que respalda las afirmaciones de estudios que señalan que estas variables se mueven en direcciones opuestas, actuando la resiliencia como un factor facilitador (o protector) en la adaptación a contextos adversos, mientras que la evitación experiencial impide esta adaptación (Ruiz-Párraga & López-Martínez, 2015). Asimismo, la evitación experiencial mostró una correlación positiva significativa con la percepción de soledad, indicando que mayores niveles de evitación experiencial están asociados con mayores niveles de soledad. Estos resultados son consistentes con investigaciones previas que indican que una mayor evitación experiencial y, por tanto, una menor resiliencia, disminuye la capacidad de los individuos para manejar efectivamente las situaciones sociales (Amini et al., 2019; Martín-Rodríguez et al., 2021). Las personas que tienden a alterar la forma o la frecuencia de los eventos o contextos en los que no desean participar podrían ser menos activas en la expansión de sus relaciones sociales, llevando a una percepción reducida del apoyo social y a un aumento de la

sensación de soledad (Maitland, 2020). En cuanto a la capacidad tecnológica autopercibida, se encontró una correlación negativa significativa con la evitación experiencial y una correlación positiva significativa con la resiliencia, lo que indica que una mayor capacidad tecnológica autopercibida se asocia con menores niveles de evitación experiencial y mayores niveles de resiliencia.

En el presente estudio, se aplicaron modelos de regresión lineal para explorar el impacto de diversas variables —uso de Internet, competencia tecnológica autopercibida y factores sociodemográficos (sexo, estado civil, edad)— sobre constructos psicosociales clave como la evitación experiencial, la resiliencia y la percepción de soledad. Los hallazgos indican que, mientras el modelo para la evitación experiencial no alcanzó significación estadística, sugiriendo que las variables independientes no explican de manera significativa la variabilidad en la evitación experiencial, los modelos para la percepción de soledad y la resiliencia resultaron ser significativos. En particular, el modelo de la percepción de soledad explicó el 12% de la varianza, identificando el sexo y el estado civil como predictores significativos, y mostrando una tendencia a la significación para la competencia tecnológica autopercibida. Por otro lado, la resiliencia fue explicada en un 5.4% por la competencia tecnológica autopercibida, sin que otras variables como el tiempo de uso de Internet, el sexo, la edad y el estado civil mostraran efectos significativos. Así mismo, el análisis de clústeres identificó cuatro perfiles distintivos basados en patrones de uso de Internet y características psicosociales. Los clústeres con un uso moderado y alto de Internet mostraron puntuaciones moderadas en soledad, evitación experiencial y resiliencia, mientras que un clúster con uso extremadamente alto de Internet presentó bajas puntuaciones en soledad y ligeramente más alta en resiliencia, lo cual resalta la complejidad de estas relaciones y su posible no linealidad (Morizt, 2017). Sin embargo, el análisis sólo introdujo a un miembro en este clúster, por lo que sería necesario contar con una muestra más heterogénea para que la división aportarse información de calidad y más

En términos de limitaciones, los resultados del estudio no son representativos de toda la población adulta mayor, sino únicamente de aquellos que son usuarios activos de TIC. Este factor introduce un sesgo potencial, ya que los no usuarios

podrían presentar perfiles psicosociales diferentes y posiblemente más desafiantes, debido a que el uso de internet en este grupo etario contribuye al bienestar y al sentido de empoderamiento, afectando a sus interacciones interpersonales, promoviendo su funcionamiento cognitivo y contribuyendo a su experiencia de control e independencia (Shapira et al., 2007). Continuar la investigación en esta línea, incluyendo tanto a usuarios como no usuarios de TIC permitirá una visión más completa de las interacciones entre los diversos factores que pueden influir en el uso de las TIC, permitiendo enfrentar los retos emergentes que plantea una sociedad cada vez más digitalizada, de una forma que promueva la salud y el bienestar de los adultos mayores en un entorno tecnológicamente avanzado.

CAPÍTULO 6: USO DE TIC Y CIBERVICTIMIZACIÓN EN PAM: UN ESTUDIO EXPLORATORIO

6.1 JUSTIFICACIÓN DEL ESTUDIO

Como se ha expuesto previamente, desde mediados de los años setenta en España, al igual que otros países, ha experimentado cambios demográficos significativos, caracterizados por una disminución de la natalidad y un aumento de la esperanza de vida (INE, 2021). Como resultado, la proporción de personas adultas mayores (PAM) ha crecido sustancialmente. Este fenómeno, aunque indicativo de progreso social, plantea desafíos importantes en términos de integración y adaptación de las PAM a los rápidos avances tecnológicos. Las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un componente esencial para la participación activa de las PAM en la sociedad contemporánea, ofreciendo beneficios en áreas como la salud, la economía y las relaciones sociales (Concepción-Breton et al., 2020; Ces García, 2003). Sin embargo, la falta de formación en el uso de estas tecnologías expone a las PAM a un mayor riesgo de cibervictimización. El incremento en la cibervictimización de las PAM, especialmente en delitos relacionados con fraudes y estafas en el ciberespacio, es un fenómeno alarmante. En los últimos años el número de casos de ciber-victimización registrados entre las PAM ha aumentado (Ministerio del Interior, 2021), facilitado por las características propias del ciberespacio, como el anonimato y la eliminación de barreras geográficas (Cerezo et al., 2007; Clough, 2010; Miró-Llinares, 2011), sumado a un mayor uso de estas herramientas por parte de este grupo demográfico. Este estudio exploratorio se llevó a cabo con el objetivo de analizar el uso de las TIC por parte de las PAM, evaluar su percepción de vulnerabilidad ante ciberdelitos, y examinar las medidas de seguridad que emplean. Los resultados obtenidos proporcionan una base para el diseño de programas de formación adaptados a las características de este grupo poblacional, con el fin de reducir la brecha digital y mitigar su vulnerabilidad ante el cibercrimen. La necesidad de estudios como el presente radica en la creciente digitalización de la vida cotidiana, exacerbada por la pandemia de SARS-CoV-2, que

ha obligado a muchas PAM a incorporar las TIC en actividades diarias sin la formación adecuada (INE, 2021). La falta de conocimiento y habilidades digitales no solo limita el aprovechamiento de las oportunidades que ofrece el entorno digital, sino que también aumenta el riesgo de convertirse en víctimas de ciberdelitos (Miró-Llinares, 2013; Huey & Ferguson, 2022). Por tanto, este capítulo tiene como propósito principal analizar la relación entre el uso de las TIC y la cibervictimización en las PAM, presentando un análisis de sus hábitos digitales, su percepción de seguridad y las medidas de protección que emplean. Esta investigación es fundamental para desarrollar estrategias de intervención que mejoren la alfabetización digital y promuevan una participación segura y activa de las PAM en la sociedad digital. En el desarrollo de una sociedad inclusiva para todas las edades, consideramos pertinente dotar a las personas adultas mayores de las herramientas necesarias para realizar un uso efectivo de las TIC. Fomentar su empoderamiento social mediante la mejora de sus habilidades digitales, tanto para aprovechar los beneficios que ofrece el ciberespacio como para ser capaces de autoprotección, es fundamental para prevenir los delitos que puedan ocurrir en este nuevo entorno digital y para proporcionarles conocimiento sobre los riesgos que en él se encuentran.

6. 2 OBJETIVOS DEL ESTUDIO

El objetivo principal de este estudio es conocer la asociación entre las actividades cotidianas en línea de las PAM y la cibervictimización. Concretamente, pretendemos conocer, en primer lugar, la relación entre los hábitos en el uso de internet y la percepción de riesgo de sufrir algún tipo de ciberdelito y la victimización por ciberfraude. En segundo lugar, pretendemos conocer las medidas de protección adoptadas por las PAM y la percepción de riesgo de sufrir algún tipo de ciberdelito. En tercer lugar, se busca obtener datos sobre la victimización en línea y la denuncia o notificación de haber sido objetivo de este tipo de delitos.

Con el propósito adicional de realizar este análisis completo del impacto de la digitalización en los hábitos de las PAM y su victimización, esta investigación se complementa con un estudio cualitativo que compara los hábitos y percepciones de

dos grupos de PAM: uno que ha incorporado las TIC en sus actividades diarias y otro que no, que se presentará en el siguiente capítulo.

6.3 METODOLOGÍA

6.3.1 Procedimiento y selección de la muestra

Una vez aprobado el estudio por el Comité de Ética y debido a las restricciones de movilidad que estaban vigentes para las personas adultas mayores durante el período de recogida de datos, se elaboró una encuesta ad hoc utilizando la plataforma Google Forms para la recolección de datos. Los criterios de inclusión en la muestra fueron ser una persona mayor de 55 años y disponer de un dispositivo con acceso a internet para poder completar el cuestionario. El enlace de la encuesta se difundió a través de WhatsApp y correo electrónico, tanto entre los estudiantes de un programa universitario para mayores como entre otras PAM que cumplieran los criterios de inclusión mencionados, utilizando la técnica de bola de nieve. Antes de completar la encuesta, se solicitó a los participantes su consentimiento informado para participar en el estudio.

El formulario estuvo disponible desde el 14 de mayo de 2021 hasta el 7 de junio de 2021, obteniendo un total de 77 respuestas válidas, con edades comprendidas entre los 55 y 80 años (M = 66,2; DT = 6,2), de las cuales el 73,1% eran mujeres. La mayoría de los participantes (54,5%) tenía ingresos mensuales en el rango de 1000 a 2000€. Los datos sociodemográficos se detallan en la tabla 8.

Tabla 8. *Datos sociodemográficos*

Nivel educativo	*N (%)*
Sin estudios	0
Primarios (graduado escolar o equivalente)	8 (10,4)

Secundarios (bachillerato o equivalente)	27 (35,1)
Superiores (universitarios)	42 (54,5)
Ingresos mensuales	*N (%)*
Entre 0 y 499€	1 (1,3)
Entre 500 y 999€	11 (14,3)
Entre 1000 y 1999€	42 (54,5)
Más de 2000€	23 (29,9)
Convivencia	*N (%)*
Viven solos/as	26 (33,8)
En pareja	46 (59,7)
Con otro familiar o conocido	5 (6,5)
En una residencia	0
Edad	*M (DT)*
	66,2 (6,2)

M = media; *DT* = desviación típica

6.3.2 Variables del estudio

La selección de variables relacionadas con el uso de las TIC y los diferentes tipos de fraude que pueden afectar a las personas adultas mayores (PAM) que utilizan estas tecnologías se realizó a partir del cuestionario elaborado en el proyecto Protegi2.0+, llevado a cabo en 2017 con PAM de la provincia de Alicante. En dicho estudio se analizó la prevalencia de diversas formas de victimización por fraude que afectan a las PAM, así como las conductas de riesgo que estas llevan a cabo tanto en el entorno físico como en el digital. Los datos indicaron que la cibervictimización por fraude en PAM alcanzaba aproximadamente el 30%, mientras que en el entorno físico llegaba al 40%. Sin embargo, los autores destacaron la existencia de una gran cifra negra en los fraudes realizados online, y señalaron como una posible causa del menor

porcentaje de fraude online el menor uso de las TIC, dado que solo el 32,1% de la muestra era usuaria de internet. Debido al aumento del uso de las TIC por parte de las PAM y al incremento de la digitalización de las tareas cotidianas a raíz del confinamiento provocado por la pandemia de SARS-CoV-2, se consideró necesario realizar esta aproximación para evaluar la percepción de riesgo, el uso de medidas de protección y la cibervictimización, con el fin de observar la nueva realidad de las PAM en el ciberespacio. Basándonos en los resultados del proyecto mencionado anteriormente y en la bibliografía más reciente sobre formación, uso, protección y percepción de victimización de las PAM en el entorno digital, se elaboró una encuesta compuesta por 28 preguntas (Anexo I) estructuradas de la siguiente forma:

a) Variables sociodemográficas de los participantes: sexo, edad y nivel máximo de estudios alcanzado.

b) Uso de internet por parte de los usuarios (frecuencia y herramientas utilizadas).

c) Percepción de vulnerabilidad (referida a la probabilidad percibida de ser víctima de diferentes tipos de fraude online, medida a través de una escala Likert donde "0" = considera que no tiene ninguna probabilidad de convertirse en víctima de ese tipo de fraude y "3" = considera que la probabilidad de convertirse en víctima de ese tipo de fraude es alta).

d) Cibervictimización: se preguntó a los participantes si en los últimos 12 meses habían sido objeto de fraude en comportamientos como compras online, phishing, virus informáticos, usurpación de identidad, solicitud de dinero por parte de alguna persona conocida en internet, o si habían sufrido un perjuicio patrimonial en el contexto digital.

e) Uso de medidas de seguridad: se evaluaron, para cada tipo de fraude sufrido, las medidas de seguridad utilizadas para dificultar el mismo. Se indagó sobre la realización de conductas de protección, como el cambio de contraseñas o marcar los correos fraudulentos como spam, entre otras. La

escala de evaluación fluctuaba entre "0" = mínimo nivel de seguridad y "3" = nivel de seguridad óptimo, en función de las medidas adoptadas.

A continuación, se detallan las conductas evaluadas referentes a las medidas de seguridad y los diferentes niveles en esta área:

- Compras online:
  - No realiza ninguna medida de seguridad, compra donde sea más barato o en cualquier página que aparezca en el buscador (Nivel 0).
  - Pregunta a familiares y conocidos si es seguro realizar compras en la página (Nivel 1).
  - Busca información sobre el producto y el vendedor antes de realizar cualquier compra online (Nivel 2).
  - Realiza siempre las compras en una página de confianza (Nivel 3).

- Correos electrónicos u otros mensajes:
  - Sin medidas de seguridad, abre los enlaces que aparecen en estos correos o responde a los mensajes (Nivel 0).
  - Cuando un correo electrónico o mensaje parece sospechoso, busca información en internet sobre él (Nivel 1).
  - Marca los correos o mensajes sospechosos como spam (Nivel 2).
  - Elimina sin abrir los correos o mensajes que parecen sospechosos (Nivel 3).

- Virus informático:
  - Sin antivirus en ningún dispositivo (Nivel 0).
  - Con antivirus solo en el ordenador (Nivel 1).
  - Con antivirus en el móvil y la tablet (Nivel 2).
  - Con antivirus en todos mis dispositivos (Nivel 3).

- Usurpación de la identidad:
  - Sin medidas de seguridad, facilita sus datos personales a extraños diariamente (Nivel 0).
  - Facilita varias veces al mes sus datos personales a extraños (Nivel 1).

- Facilita menos de una vez al mes sus datos personales a extraños (Nivel 2).
- Nunca facilita sus datos personales a extraños (Nivel 3).

6.3.3 Análisis de datos

El análisis estadístico de los datos se llevó a cabo utilizando el programa SPSS v26. Se realizaron análisis descriptivos de las variables, incluyendo frecuencias y porcentajes para las variables categóricas, así como medias y desviaciones típicas para las variables cuantitativas, tanto en los datos sociodemográficos como en las variables de interés previamente descritas. Tras examinar la normalidad de los datos y comprobar que este supuesto no se cumplía, se emplearon pruebas no paramétricas. La relación entre la percepción de vulnerabilidad y el uso de medidas de seguridad se analizó mediante correlaciones de Spearman, dado que ambas se categorizaron como variables continuas. Para todos los análisis mencionados, se consideró un nivel de significación de $\alpha = .05$, el cual se utilizó para determinar la significancia de los resultados.

6.4 RESULTADOS

6.4.1 Hábitos y cambios relacionados con el uso de las TIC

En las Tablas 9 y 10 se presentan los resultados descriptivos sobre las rutinas relacionadas con el uso de internet realizadas por los participantes de nuestra muestra. Como se puede observar, el 84,6% utiliza internet más de una hora al día, y el 42,3% lo utilizaba, en el momento en que se realizó el estudio, más que antes de la situación de confinamiento provocada por el SARS-CoV-2. El 60,8% de los encuestados afirma utilizar contraseñas compuestas exclusivamente por números y letras, y el 36,7% no suele utilizar contraseñas diferentes para sus distintas cuentas. Se observa que el uso de internet es variado, siendo las herramientas más utilizadas el

navegador para buscar información cultural (94,9%), WhatsApp (89,95%) y el correo electrónico (87,3%). En cuanto al nivel formativo en el uso de las TIC, solo el 22,8% de la muestra (18 personas) había recibido algún curso en esta área.

Tabla 9*. Actividades realizadas en internet*

	N (%)
Frecuencia de uso de internet	
Menos de 1 hora diaria	12 (15,4)
Entre 1 y 3 horas diarias	49 (62,8)
Más de 3 horas diarias	17 (21,8)
Uso antes/después confinamiento	
Menos que antes del confinamiento	2 (2,5)
Igual que antes del confinamiento	43 (55,1)
Más que antes del confinamiento	33 (42,3)
Herramientas utilizadas	
Redes sociales	47 (59,5)
Correo electrónico	69 (87,3)
WhatsApp	71 (89,9)
Navegador para información cultural	75 (94,9)
Compras online	33 (41,8)
Banca online	62 (78,5)
Curso para el manejo de internet	
Si	18 (22,8)
No	61 (77,2)
Uso de contraseñas diferentes para cada cuenta	
Nunca	2 (2,5)
A veces	27 (34,2)
La mayoría de las veces	31 (39,2)
Siempre	19 (24,1)
Tipos de contraseñas utilizadas	
Sólo letras	0 (0)
Solo números	6 (7,6)

Letras y números	48 (60,8)
Letras, números y símbolos	25 (31,6)

A continuación, en la Tabla 10 se muestran los resultados relativos a las frecuencias de las conductas susceptibles de relacionarse con los distintos tipos de fraude analizados en el estudio.

Tabla 10. *Frecuencia actividades susceptibles de relacionarse con ciberfraude*

	N (%)
Realización de compras online	
Cada día	0 (0)
Varias veces al mes	9 (11,5)
Menos de una vez al mes	47 (60,3)
Nunca	22 (28,2)
Utilización de Correo electrónico	
Cada día	39 (50)
Varias veces al mes	34 (43,6)
Menos de una vez al mes	5 (6,4)
Nunca	0 (0)
Utilización de WhatsApp	
Cada día	74 (94,9)
Varias veces al mes	4 (5,1)
Menos de una vez al mes	0 (0)
Nunca	0 (0)
Utilización de redes sociales	
Cada día	38 (48,7)
Varias veces al mes	15 (19,3)
Menos de una vez al mes	5 (6,4)
Nunca	20 (25,6)
Descarga de contenido desde enlaces	
Cada día	5 (6,4)
Varias veces al mes	36 (46,2)
Menos de una vez al mes	31 (39,7)
Nunca	6 (7,7)

Compartir información personal con desconocidos	
Cada día	0 (0)
Varias veces al mes	1 (1,3)
Menos de una vez al mes	20 (25,6)
Nunca	57 (73,1)

Podemos observar que las conductas más realizadas diariamente por parte de la muestra son: la utilización del whatsapp (94,9%), del correo electrónico (50%) y de las redes sociales (48,7%). La conducta de descarga de contenidos desde enlaces es realizada varias veces al mes por parte del 46,2% de la muestra.

6.4.2 Victimización por fraude online y conducta de denuncia y/o notificación

En cuanto a la victimización por fraude online, el 84,6% de los encuestados afirmaron haber sido objetivo de al menos uno de los tipos de fraude analizados y el 15,6% había sido objetivo de, al menos, dos. Los tipos de fraude sufridos más comunes fueron: recibir un mensaje o un correo electrónico con contenido fraudulento, ofreciendo un premio, descuento, inversión o negocio falso (72,2%) y realizar una compra online y no recibir el producto, recibir otro o pagar un precio diferente al establecido (15,2%).

Se analizaron las conductas de denuncia realizadas por los sujetos que habían sido víctimas de fraude y se observa que sólo el 15,2% de ellos había denunciado ser objetivo de fraude a alguna entidad (tipo bancaria) o a los cuerpos de seguridad. El 45,6% de las personas que habían sido objetivo de algún tipo de fraude, no lo denunciaron ni lo comentaron con familiares o conocidos. En la Tabla 11 se muestran estos resultados.

Tabla 11. *Objetivo de cibervictimización y denuncia/notificación*

	N (%)
Victimización	
Compra online fraudulenta	12 (15,2)

Mensaje o correo electrónico fraudulento	57 (72,2)
Relación online en la que se pide dinero	7 (8,9)
Descargar archivos con virus informático	5 (6,3)
Sufrir prejuicio patrimonial	1 (1,3)
Suplantación de identidad	0 (0)
Denuncias	
No se lo dijo a nadie	36 (45,6)
Lo comentó con amigos y/o familiares	31 (39,2)
Denunció en una entidad	8 (10,1)
Denunció en la policía	4 (5,1)

6.4.3 Percepción de vulnerabilidad, medidas de seguridad y relación entre las variables

La percepción de vulnerabilidad de convertirse en víctima de un fraude, de forma general, obtuvo de media 1,6 sobre 4 (DT = ,5), lo que indica que existe una baja percepción de vulnerabilidad entre los encuestados, siendo esta más baja (1,5) en los dos tipos de fraude más prevalentes en la muestra: fraude en compras y fraude mediante mensajes o correos electrónicos. Los resultados se muestran en la Tabla 12.

Tabla 12*. Percepción de vulnerabilidad*

	"0" Ninguna	"1" Poca	"2" Moderada	"3" Alta	
Percepción de vulnerabilidad	*N* (%)	*N* (%)	*N* (%)	*N* (%)	*Media*
Fraude en compras	4 (5,1)	34 (44,2)	33 (42,9)	6 (7,8)	1,5
Fraude por correo o mensaje	1 (1,3)	40 (51,9)	32 (41,6)	4 (5,2)	1,5
Virus	1 (1,3)	28 (36,4)	44 (57,1)	4 (5,2)	1,7
Usurpación identidad	3 (3,9)	26 (33,8)	40 (51,9)	8 (10,4)	1,7

En cuanto los tipos de fraude en el que los participantes realizaban más conductas de autoprotección fueron los relacionados con la compra online (el 80,5% afirmaba comprar sólo en páginas de confianza) y el correo electrónico o mensaje (ya que el 89,6% afirmaba que borraba directamente los mensajes que consideraba sospechosos de fraude). Por su parte, *la protección contra virus* sería la medida que menos se realiza pues el 57,1% de los usuarios afirmaba no tener antivirus o tenerlo sólo en el ordenador. Estos datos se muestran en la Tabla 13.

Tabla 13*. Nivel de seguridad empleado (medidas de protección)*

	0	1	2	3	
Medidas de seguridad	*N* (%)	*N* (%)	*N* (%)	*N* (%)	*M (DT)*
Fraude en compras online	0 (0)	8 (10,4)	7 (9,1)	62 (80,5)	2,7
Fraude por correo o mensaje	4 (5,2)	1 (1,3)	3 (3,9)	69 (89,6)	2,78
Virus	13 (16,9)	32 (41,6)	6 (7,8)	26 (33,8)	1,58
Usurpación de identidad	0 (0)	1 (1,3)	16 (20,8)	60 (77,9)	3,16

La prueba de correlación de Spearman descartó una relación significativa entre la percepción de vulnerabilidad en los distintos tipos de fraude y un mayor o menor uso de medidas de seguridad por parte de las PAM, tal como se muestra en la Tabla 14.

Tabla 14. *Correlaciones de Spearman vulnerabilidad-protección*

	Uso de medidas de seguridad
Compras	
Percepción de vulnerabilidad	,163
Phishing	
Percepción de vulnerabilidad	,005
Virus informático	

Percepción de vulnerabilidad	-,051
Usurpación de identidad	
Percepción de vulnerabilidad	,077

** $p \leq .05$

6.5 DISCUSIÓN Y CONCLUSIONES

Este estudio tuvo como objetivo realizar un primer análisis exploratorio de las variables implicadas en la cibervictimización de las personas adultas mayores (PAM), la percepción de vulnerabilidad que tienen ante este tipo de delitos y las medidas de seguridad adoptadas para su prevención en los últimos 12 meses.

En relación con la frecuencia de uso de las TIC por parte de la muestra de PAM estudiada, se observa que los resultados son congruentes con los señalados en estudios a nivel nacional, que indican un aumento del uso de internet por parte de las PAM del 10,9% entre 2019 y 2021 (INE, 2021). En nuestro estudio, el 42,3% de la muestra manifestó haber incrementado el número de horas diarias dedicadas a las TIC tras el confinamiento, utilizándolas entre una y tres horas al día el 62,8% de los participantes, y más de tres horas diarias el 21,8%.

Estos datos sugieren que el uso de las TIC se está convirtiendo en una actividad cotidiana entre las PAM, confirmando el riesgo que estas conductas conllevan, ya que el 77,2% de los encuestados afirmó no haber recibido ningún tipo de formación relacionada con el uso de internet. Según la Teoría de las Actividades Cotidianas (TAC) y basándonos en estudios realizados con otros grupos poblacionales (Miró, 2013), podemos suponer, con un bajo riesgo de equivocarnos, que la cibervictimización por fraude aumentará en este grupo poblacional en los próximos años si no incrementamos su formación tanto en los diferentes tipos de delitos a los que pueden estar expuestos en el entorno digital como en el uso de medidas de protección para evitarlos.

El análisis de los datos mostró que, entre las actividades que los participantes realizaban diariamente en el ciberespacio, el correo electrónico era utilizado por el

50% de la muestra y WhatsApp por el 94,9%. Sabemos que estas actividades son altamente susceptibles de sufrir fraudes online, como el phishing, siendo este uno de los más comunes (Miró, 2012). En el momento del estudio, el 84,6% de los encuestados afirmó haber sido objetivo de al menos un tipo de fraude y el 15,6% de dos, confirmando, en la línea señalada por otros autores (Leukfeldt et al., 2017; Pratt et al., 2010; Savona & Mignone, 2004), que las PAM son un objetivo atractivo para los ciberdelincuentes. Asimismo, coincidiendo con estudios realizados en otros países (ActionFraud, 2020; CIFAS, 2020; Scamwatch, 2020), los tipos de fraude más identificados en nuestra muestra fueron los relacionados con compras online y phishing.

Por otro lado, al igual que en los trabajos de Cross (2015, 2016), en nuestro estudio, las PAM entrevistadas manifiestan una baja percepción de convertirse en víctimas de fraude, a pesar de que el 84,6% de ellas había sido objetivo de algunos de los tipos de fraude analizados. Esta baja percepción de vulnerabilidad puede deberse al desconocimiento respecto a los delitos que se pueden cometer en el ciberespacio. Quizás esta baja percepción está en la base de que el 57% de la muestra no utilice ningún antivirus en sus dispositivos como medida de protección. Cualesquiera que sean los motivos, es necesario responder a esta victimización diseñando una formación adecuada a las características de este sector poblacional acerca de los diferentes delitos a los que están expuestos en el entorno digital y las diversas situaciones que pueden aumentar su vulnerabilidad al utilizar nuevas herramientas digitales.

Es importante analizar en profundidad la ausencia de relación entre la percepción de vulnerabilidad a ser víctima de un ciberdelito y el uso de medidas de seguridad empleadas, de cara al diseño de futuras intervenciones. Es necesario conocer si la percepción de baja vulnerabilidad se debe a que las personas no cuentan con los conocimientos y herramientas necesarios para protegerse de los delitos que pueden sufrir, o a que desconocen los tipos de delitos que pueden ocurrir en el ciberespacio y el procedimiento para realizarlos, en línea con lo afirmado por Kemp y Moneva (2020). Sabemos que, en lo referente a la vulnerabilidad de ser víctima de un delito en el entorno digital, lo relevante no es solo contar con

antivirus o protectores similares, sino que la posible víctima juega un papel importante en la prevención del delito al actuar como un "autoguardián" e incorporar las medidas que considere necesarias en función de sus conocimientos (Miró, 2012). De esta forma, si la víctima se percibe vulnerable pero no cuenta con los conocimientos para protegerse, no podrá adoptar estas medidas de seguridad. Esta desinformación aumentaría la brecha digital, como apuntan otros autores (Loges & Jung, 2001; Hargittai, 2002; Warschauer, 2002), debido al desconocimiento de este entorno, y no por dificultades de acceso a herramientas digitales, como sucede en otras ocasiones. Por tanto, la formación en herramientas que permitan actuar como "autoguardianes" a las PAM es necesaria en el contexto altamente digitalizado en el que nos encontramos (Nicholson et al., 2021).

Por último, respecto a las conductas de denuncia realizadas por parte de los participantes que han sido objetivo de algún tipo de fraude online, observamos que, a pesar de que el 84,6% de los individuos había sido objetivo de alguno de los fraudes evaluados, el 45,6% no informó a nadie de lo que le había sucedido, ni siquiera a un conocido o familiar. Estos datos confirman que sigue existiendo una "cifra negra" de este tipo de delitos debido a la falta de denuncia, en línea con la literatura existente (Button & Cross, 2017; Caneppele & Aebi, 2017; Maras, 2017; Wall, 2007). Tal y como afirman Kemp et al. (2020), las razones para que no se produzca la denuncia pueden deberse a la falta de conciencia por parte de la víctima de su posible victimización, posiblemente por su falta de conocimiento sobre este tipo de delincuencia. Otra causa que explicaría la alta cifra negra podría ser el desconocimiento de dónde denunciar, de cómo hacerlo, o la percepción de que no compensa el tiempo y los recursos que debe emplear para realizar una denuncia, al ser poca la cantidad de dinero perdida o no haberse producido ninguna pérdida.

Tras lo expuesto en este capítulo podemos concluir que:

- Se ha producido un aumento en el uso de las TIC por parte de las personas adultas mayores (PAM) en numerosas actividades diarias tras el confinamiento. La digitalización de estas actividades ha llevado a cambios en la forma en que se cometen diversos delitos, incluidos los económicos.

Esto podría aumentar la vulnerabilidad de las PAM, como se ha señalado, entre otros, en el estudio teórico realizado por Cross en 2021.

- Sigue siendo insuficiente la formación en nuevas herramientas digitales dentro del grupo de PAM, lo que disminuye su percepción de riesgo al no ser conscientes de los posibles delitos que pueden ocurrir en el ciberespacio. En esta línea, una reciente revisión sistemática sobre el ciberfraude (Ahmad et al., 2022) concluye que ciertas variables pueden favorecer la victimización potencial de los ciberdelincuentes. Entre estas variables se encuentran algunas frecuentes en las PAM, como la escasa formación en nuevas tecnologías y la baja percepción de riesgo en el entorno digital, lo que disminuye su capacidad de autoprotección.

- Existe una considerable cifra negra respecto a las denuncias de delitos sufridos en el ciberespacio por parte de las PAM. Este aspecto debe ser considerado en futuros estudios, ya que, si nos basamos únicamente en estadísticas policiales para analizar los fraudes en el entorno digital, estaríamos ignorando gran parte de estos delitos (Kemp et al., 2020).

Sin embargo, no disponemos de una fuente de datos sólida y actualizada sobre los comportamientos y actitudes de las PAM en el ciberespacio, necesaria para diseñar políticas públicas adecuadas para la formación y uso de medidas de prevención para este grupo poblacional cada vez más numeroso. Es evidente que la formación en competencias digitales mejora la calidad de vida de las PAM al permitirles el acceso al universo digital en su propio hogar, eliminando las barreras del entorno físico. No obstante, si queremos reducir la victimización y favorecer su plena inclusión en el mundo digital, también debemos capacitarlas en el uso de herramientas de prevención y protección en el ciberespacio.

Respecto a las limitaciones del estudio, debemos señalar en primer lugar que, al tratarse de un diseño transversal, no podemos determinar una relación causal

entre las variables estudiadas. Asimismo, no podemos generalizar los resultados a la población general de PAM españolas debido al tamaño muestral, que no permite que los datos sigan una distribución normal, y al método de recolección de datos, que solo incluyó a PAM que utilizan internet. Con los datos obtenidos en este estudio, junto con los obtenidos a través de la investigación cualitativa realizada tanto con PAM que utilizan internet en su vida diaria como con aquellas que no lo hacen, tenemos dos estudios que abordan las variables relacionadas con los cambios en las actividades cotidianas de las PAM y el aumento del riesgo de su victimización. Nuestro objetivo próximo es realizar una investigación a nivel nacional sobre el uso de las TIC y la cibervictimización representativa de las PAM en nuestro país, disponiendo así de un instrumento validado para la detección de la vulnerabilidad de las PAM en el ciberespacio que nos permita diseñar intervenciones eficaces adaptadas a este grupo poblacional para reducir su brecha digital.

CAPÍTULO 7: PERCEPCIÓN DE LA DIGITILIZACIÓN Y MIEDO FUNCIONAL Y DISFUNCIONAL ASOCIADO A LAS TIC

7.1 JUSTIFICACIÓN DEL ESTUDIO

Debido al contexto actual de envejecimiento de nuestra sociedad, ya expresado en capítulos previos, es evidente que el estudio del envejecimiento de la población requiere conocer los factores que contribuyen al mantenimiento de una vida de calidad, activa y emocionalmente enriquecedora. El enfoque propuesto por la OMS (2002) denominado "Envejecimiento Activo", creó un marco para redefinir el envejecimiento, estableciendo como relevantes las áreas de la salud, la participación social y la seguridad como determinantes de un buen envejecimiento. Hoy en día, el uso de las TIC, como elemento que impregna todas las áreas de nuestra vida, se hace indispensable su estudio en esta importante y extensa etapa del ciclo vital. Además de los beneficios que estas reportan, no se debe olvidar que el uso inapropiado de la tecnología, como la exposición a información errónea o la falta de medidas de protección en línea, puede tener efectos perjudiciales en el bienestar psicológico y emocional (Borges do Nascimento et al., 2022; Diomidous et al., 2016). Adicionalmente, la brecha digital, particularmente presente en este grupo etario, tanto en términos de acceso como de competencias digitales, puede agravar las desigualdades sociales y aumentar la percepción de soledad entre las PAM, afectando su salud mental (Armitage & Nellums, 2020). Por todo ello, surge la necesidad de examinar las implicaciones emocionales y posibles repercusiones de esta alta digitalización en diferentes sectores de nuestra vida diaria en dos cohortes de personas adultas mayores: aquellos que han integrado las TIC en su vida diaria frente a los que se han mantenido al margen. Este estudio cualitativo busca identificar las barreras que podrían estar relacionadas con una utilización nula o escasa de estas tecnologías, considerando que esta no adaptación puede estar vinculada a vivencias negativas, considerando, así mismo, el miedo al cibercrimen y la inseguridad en los entornos digitales, factores que pueden afectar la participación de las PAM en la sociedad digital. La percepción de vulnerabilidad y la falta de medidas de protección adecuadas pueden incrementar el riesgo de victimización en línea, exacerbando el miedo y la inseguridad (Brands & Van Doorn, 2022; Miró-Llinares & Moneva, 2019). Por tanto, este estudio pretende no

solo contribuir a la literatura existente sobre el uso de las TIC y el miedo al cibercrimen entre las PAM, sino también ofrecer una base de partida para futuras investigaciones y el diseño de intervenciones que favorezcan un envejecimiento activo y enriquecedor en la era digital.

7.2 OBJETIVOS DEL ESTUDIO

El objetivo principal de este estudio fue explorar cómo el uso y la falta de uso de las TIC pueden afectar emocional y socialmente a las PAM. En particular, se pretende determinar las disparidades en las emociones predominantes, patrones emocionales y posibles consecuencias asociadas con la digitalización entre dos grupos de PAM con características sociodemográficas similares, pero con un uso distinto de las TIC en su vida diaria.

Para lograr este objetivo general, se plantean los siguientes objetivos específicos:

- Analizar las emociones predominantes, los patrones emocionales y las consecuencias para estos grupos en relación con la adopción (o la falta de esta) de las TIC en sus rutinas diarias.
- Comprender las repercusiones emocionales y sociales asociadas con la decisión de no uso de las TIC. Este objetivo se centra en explorar las razones detrás de la falta de uso de las TIC y cómo esta decisión puede impactar en la salud emocional y la participación digital de las PAM.
- Explorar si las PAM percibieron obligación relacionada con el aumento del uso de TIC durante la pandemia y cómo esta experiencia ha influido en el uso y percepción general de las TIC.
- Examinar el miedo y la inseguridad asociados con el uso de las TIC entre las PAM y los contextos o factores relacionados con estos factores. Este objetivo busca identificar los factores que contribuyen al miedo y la inseguridad en el uso de las TIC y cómo estos sentimientos influyen en el comportamiento de las PAM.
- Determinar las posibles consecuencias del miedo y la inseguridad en el uso de las TIC y las repercusiones emocionales y conductuales de no utilizar estas tecnologías.

Para abordar estos objetivos, se seleccionaron dos grupos de PAM, cada uno compuesto por 8 individuos con características equitativas en términos de edad, nivel educativo y género, diferenciados por su uso o no uso de las TIC. Se ha optado por un enfoque cualitativo mediante entrevistas semiestructuradas y análisis del discurso, utilizando técnicas como la codificación y la visualización, a través del software Atlas.ti, así como la realización de nubes de palabras. Este método permite profundizar en la comprensión de las emociones y percepciones de las PAM en relación con las TIC, aportando una visión holística y detallada en un área con investigación previa limitada.

7.3 METODOLOGÍA

7.3.1 Selección de la muestra

Los participantes de este estudio fueron personas adultas mayores (PAM) estudiantes durante el período académico 2019-2020 de un programa universitario (AUNEX) para personas adultas mayores ofrecido por la Universidad Miguel Hernández de Elche. Este programa docente está diseñado para individuos mayores de 55 años, teniendo la mayoría del estudiantado un nivel medio-alto de educación previa. Por tanto, estos programas educativos en el contexto universitario están dirigidos a personas adultas mayores con intereses culturales y que se consideran cognitivamente activas. Por esta razón, consideramos que este era un grupo ideal para nuestro estudio, ya que, por un lado, generalmente no tienen una formación formal previa específica en TICs debido a su edad, pero están interesados en el envejecimiento activo en su concepción más amplia, incluyendo las áreas física, psicosocial y cognitiva.

Es importante recalcar que durante el año académico 2020-2021, debido a las restricciones impuestas por la pandemia provocada por el virus SARS-COV-2, las actividades formativas se llevaron a cabo de forma virtual. Es importante resaltar que, en el año académico previo a la pandemia (2019-2020), este programa contaba con 353 estudiantes matriculados. Sin embargo, en el año académico siguiente (2020-2021), que se realizó de forma online, se

matricularon sólo 122 estudiantes. Esto significa que el 34.5% de los estudiantes que participaron en el año anterior a la pandemia continuaron su formación en línea, mientras que el 65.5% restante (231 estudiantes) optó por no inscribirse siguiendo esta modalidad. Esta variación, dentro del mismo grupo, en la implementación de las TIC en una actividad que previamente se realizaba de forma presencial nos brindó una oportunidad única para comparar y analizar las diferencias asociadas con el cambio en la adopción (o no) de las TIC dentro de un grupo de PAM.

La selección de la muestra se llevó a cabo en dos fases: en primer lugar, se obtuvieron porcentajes de las variables edad, sexo y nivel de estudios a partir de los datos totales de las personas matriculadas en el curso 2018/2019, antes de la pandemia. A continuación, se extrapolaron esos datos para conformar una muestra de 8 personas en cada grupo, asegurando así una representatividad adecuada en cuanto a las características mencionadas anteriormente. Estos dos subgrupos fueron homogéneos en las características sociodemográficas que se han especificado, diferenciados únicamente por la implementación (o no) de las TIC.

Una vez establecidas las características de la muestra procedimos a contactar a los posibles participantes que correspondían con el perfil demográfico requerido para el estudio. A estos individuos se les preguntó por su grado de interacción y frecuencia de uso de las TIC en su vida cotidiana. Aquellos que indicaron haber incorporado las TIC de manera habitual y se mostraron dispuestos a contribuir con el proyecto fueron adscritos al grupo A, designado como el conjunto de usuarios activos de dichas tecnologías. En cuanto a las personas que no habían integrado las TIC en sus rutinas diarias y accedieron a participar en el estudio, fueron asignados al grupo B, identificado como el colectivo no usuario de TIC. La muestra final estuvo compuesta por 16 personas, tal como se muestra en la Tabla 14.

Tabla 15*. Distribución de la muestra*

	Muestra 2019-2020, *N* (%)	Grupo A, *N*	Grupo B, *N*

Mujeres	270 (76,49)	6	6
Entre 65 y 74 años	190 (70,37)	4	4
Leer y escribir	0 (0)	0	0
Nivel educativo básico	50 (26,31)	1	1
Nivel educativo medio	80 (42,11)	2	2
Nivel educativo alto	60 (31,58)	1	1
Entre 75 y 84 años	73 (27,04)	2	2
Leer y escribir	3 (4,11)	0	0
Nivel educativo básico	17 (23,29)	0	0
Nivel educativo medio	30 (41,09)	1	1
Nivel educativo alto	23 (31,51)	1	1
85 años o más	7 (2,5)	0	0
Hombres	83 (23,51)	2	2
Entre 65 y 74 años	63 (75,9)	2	2
Leer y escribir	2 (3,18)	0	0
Nivel educativo básico	14 (22,22)	0	0
Nivel educativo medio	25 (39,68)	1	1
Nivel educativo alto	22 (34,92)	1	1
Entre 75 y 84 años	17 (20,49)	0	0
85 años o más	3 (3,61)	0	0

Por tanto, los grupos para realizar las entrevistas se distribuyeron de la siguiente forma, con un total de 16 participantes:

Grupo A (presencial, estudiantes que no continuaron con la formación en línea):

- 1 mujer con estudios básicos entre 65 y 74 años.
- 2 mujeres con educación intermedia entre 65 y 74 años.
- 1 mujer con educación superior entre 65 y 74 años.
- 1 mujer con educación intermedia entre 75 y 84 años.

- 1 mujer con educación superior entre 75 y 84 años.
- 1 hombre con educación intermedia entre 65 y 74 años.
- 1 hombre con educación superior entre 65 y 74 años.

Grupo B (en línea, estudiantes que continuaron con la formación en línea):

- 1 mujer con estudios básicos entre 65 y 74 años.
- 2 mujeres con educación intermedia entre 65 y 74 años.
- 1 mujer con educación superior entre 65 y 74 años.
- 1 mujer con educación intermedia entre 75 y 84 años.
- 1 mujer con educación superior entre 75 y 84 años.
- 1 hombre con educación intermedia entre 65 y 74 años.
- 1 hombre con educación superior entre 65 y 74 años.

7.3.2 Elaboración del instrumento y recogida de datos

La entrevista cualitativa con cada uno de los participantes consistió en una entrevista semiestructurada, ya que las preguntas se diseñaron con anticipación, pero el participante tenía relativa libertad para desarrollar sus respuestas. Se optó por la utilización de metodologías cualitativas y entrevistas semiestructuradas en este estudio debido a varias razones fundamentales. El enfoque cualitativo se consideró como el más apropiado debido a la naturaleza exploratoria de la investigación y a la existencia de amplias áreas de interés en el tema. Aunque el campo de estudio es prometedor, no contábamos con una bibliografía exhaustiva ni instrumentos estandarizados que abordaran las cuestiones específicas que deseábamos investigar en este grupo poblacional concreto. En vista de estas circunstancias, las entrevistas semiestructuradas nos permitirán adentrarnos en profundidad en las perspectivas y experiencias

individuales, capturando la riqueza de datos cualitativos en ausencia de recursos bibliográficos extensos y escalas previamente validadas.

Como se detalló al inicio de este capítulo la pandemia aceleró la digitalización. Sin embargo, muchas personas adultas mayores pueden no haber estado suficientemente preparados para navegar en entornos digitales, lo que significa que podrían sentirse inseguros y temer la victimización en línea. Por lo tanto, las entrevistas se dividieron en tres áreas principales que estaban compuestas por las siguientes preguntas (Anexo II):

Área 1: Cambio en el uso de las TIC y capacidad para enfrentar estos cambios.

- ¿Te has sentido obligado a hacer uso de las TIC? Si es así, ¿en qué áreas has sentido esta obligación (comunicación, banca, salud...)? ¿Cómo te hizo sentir esto? ¿Crees que la situación de COVID-19 ha influido en esto?

- ¿Sientes que tienes la preparación necesaria para usar las TIC? Si no, ¿cuáles crees que son las consecuencias de no tener esta formación?

Área 2: Inseguridad y miedo sobre el uso de las TIC

- ¿Cuáles son los usos de las TIC en los que te sientes más capaz? ¿Y en cuáles te sientes menos capaz?

- ¿Hay algo que te haga sentir inseguro al usar las TIC?

- ¿Alguna vez has tenido miedo de convertirte en víctima de un delito al usar las TIC? Si es así, ¿de qué tipo?

Área 3: Consecuencias de la inseguridad y el miedo y del no uso de las TIC

- ¿Alguna vez no has usado las TIC porque temías las consecuencias de usarlas? Si es así, ¿qué posibles consecuencias te han llevado a no usarlas?

- ¿Crees que no usar las TIC puede tener consecuencias para ti? ¿Cuáles?

- Si te sientes inseguro al usar las TIC, ¿qué consecuencias crees que puede tener para ti?

Antes de comenzar las entrevistas con los participantes, se realizó una prueba piloto con 2 personas mayores de 65 años para verificar que las preguntas fueran correctamente entendidas y estuvieran alineadas con los objetivos de la investigación. Los datos cualitativos se recopilaron estableciendo un clima de confianza y respetando la necesidad de los entrevistados de hablar.

Las entrevistas con los participantes se agendaron por teléfono y se realizaron en el verano de 2022, tanto de forma presencial en uno de los despachos de la Universidad Miguel Hernández de Elche, como en línea, dependiendo de la disponibilidad y preferencias de los participantes. Estudios previos han concluido que las diferencias entre los resultados obtenidos de entrevistas presenciales y en línea se relacionan principalmente con la calidad de la relación entre el entrevistador y el entrevistado cuando es necesario hablar sobre temas íntimos y además la relación se extiende en el tiempo (Davies et al., 2020). En nuestro caso, las entrevistas no indagaban en temas particularmente delicados y solo se realizaba una entrevista por participante, por lo que optamos por permitir a los participantes elegir la modalidad que prefirieran.

Una única investigadora fue la responsable de conducir las entrevistas, grabarlas y transcribirlas. Todos los participantes fueron informados del objetivo principal del estudio y se solicitó su consentimiento para la grabación de la sesión y para analizar sus respuestas en detalle. La duración promedio de las entrevistas fue de 25 minutos, siendo la duración de la más corta 15 minutos y la más larga 50 minutos, sin encontrarse diferencias significativas entre la duración de los formatos en línea y presencial. Una vez completadas las entrevistas, se transcribieron y se produjo un mapa conceptual basado en las diferentes categorías obtenidas, de acuerdo con los objetivos del estudio y las preguntas de investigación.

7.3.3 Estrategia analítica

De acuerdo con los objetivos del estudio, se realizaron análisis sobre las tres áreas de interés: cambio en el uso de las TIC y capacidad para enfrentar estos cambios; inseguridad y miedo sobre el uso de las TIC; consecuencias de la inseguridad y el miedo y del no uso de las TIC. Se llevó a cabo un análisis temático para identificar patrones (o temas) que se pueden identificar en la muestra de datos, permitiéndonos describir estos datos en detalle (Braun y Clarke, 2006). Este método permite organizar y describir en detalle los datos recopilados, proporcionando una comprensión rica y profunda de las experiencias, percepciones y comportamientos de los participantes en el estudio. El proceso de análisis temático comienza con la familiarización exhaustiva con los datos, lo que incluye la transcripción de las entrevistas y la lectura repetida de los datos para identificar ideas iniciales. Una vez familiarizado con los datos, se procede a generar códigos iniciales, que son etiquetas sistemáticas aplicadas a segmentos de datos relevantes. Estos códigos son esenciales para organizar la información de manera significativa ya que posteriormente los códigos se agrupan en temas potenciales, lo que implica una búsqueda minuciosa de patrones dentro de los datos. Cada grupo de códigos representa un tema, que encapsula un aspecto relevante del conjunto de datos. En la fase de revisión de temas, se verifica la coherencia interna de cada tema y su validez en relación con el conjunto de datos completo, asegurándose que los temas sean representativos y estén bien definidos. Posteriormente, se procede a definir y nombrar los temas. En esta etapa, se le asigna un nombre que refleje con precisión su contenido, que sea comprensible y útil para el análisis posterior. Este tipo de análisis es particularmente adecuado porque no está vinculado a ninguna teoría particular, lo que ofrece una forma de análisis más accesible, especialmente para la investigación cualitativa en áreas con investigación previa limitada (Braun y Clarke, 2006), como es el caso en este estudio.

Dado que una crítica general de los estudios cualitativos es la falta de información sobre el proceso y los detalles del análisis (Attride-Stirling, 2001), el presente estudio siguió la estructura propuesta por la guía QUAGOL

(Qualitative Analysis Guide of Leuven) (De Casterlé et al., 2012). Los fases a seguir en el análisis cualitativo guiado por QUAGOL, y que se tuvieron en cuenta en este estudio, son las siguientes:

1. Preparación para la codificación (trabajo con lápiz y papel):
   - (Re)leer las entrevistas en detalle;
   - Informe de la entrevista (resumen breve de las ideas de la entrevista);
   - Esquema conceptual de la entrevista (sustituir conceptos por experiencias concretas);
   - Verificar la adecuación del esquema (código) en el diálogo;
   - Comparación constante.

2. Proceso de codificación (con software):
   - Desarrollar una lista de conceptos como códigos preliminares;
   - Vincular todos los fragmentos relevantes a los códigos;
   - Análisis de los conceptos;
   - Extraer la estructura y descripción de los resultados.

Concretamente, en esta investigación se utilizó el software ATLAS.ti para realizar el análisis de las entrevistas semiestructuradas. ATLAS.ti es una herramienta especializada en el análisis cualitativo que facilita la organización, gestión y análisis de grandes volúmenes de datos no estructurados, en este caso las transcripciones de las entrevistas. Este software es ampliamente reconocido y utilizado en diversas disciplinas, debido a su capacidad para proporcionar un análisis detallado y riguroso. El proceso de análisis comenzó con la importación de las transcripciones de las entrevistas semiestructuradas en ATLAS.ti. Una vez importados los datos, se procedió a la codificación, lo que implicó la aplicación de etiquetas a segmentos específicos de texto que contenían información relevante para los objetivos de la investigación. Estos códigos permitieron organizar y categorizar los datos de manera sistemática, facilitando la identificación de patrones, temas y relaciones dentro del conjunto de datos. Una de las fortalezas de ATLAS.ti es su capacidad para visualizar las relaciones entre los códigos y los datos mediante mapas de red, diagramas de relaciones y gráficos. Estas herramientas de visualización facilitaron una

comprensión más profunda y matizada de los patrones complejos que emergieron de los datos.

7.4 RESULTADOS

Siguiendo los objetivos de la investigación, se crearon diferentes códigos a partir del análisis. Todos los códigos pueden agruparse en tres temas principales: miedo al cibercrimen e inseguridad en las TIC; uso de las TIC y percepción de las TIC. Dentro de los temas encontramos un total de 15 códigos, que se muestran en la Tabla 15, así como sus asociaciones entre sí, proporcionadas por el software Atlas.ti y representada en la Figura 2 (Anexo III). Cada una de las entrevistas fue codificada por la investigadora, creando códigos basados en las respuestas de los participantes. Las diferentes frases codificadas pueden pertenecer a un solo código o a varios, en cuyo caso el programa detecta estas asociaciones entre códigos. Por ejemplo, si ante la pregunta "¿Qué haces si te sientes inseguro al usar internet?", la persona responde, "Llamo a mi hijo", esta respuesta se codificará como "Actitud frente a la inseguridad" y "Necesidad de apoyo social/instrumental". Por lo tanto, los códigos no siguen un orden estricto ya que el análisis temático da lugar a un sistema que cambia a lo largo del proceso, pudiendo surgir nuevos códigos o unificando varios códigos en uno sólo.

Tabla 16. *Temas y códigos*

Temas principales	Códigos
Miedo al cibercrimen e inseguridad	Miedo al cibercrimen
	Cibervicimización previa
	Actitudes/comportamiento ante el miedo al cibercrimen
	Situaciones generadoras de inseguridad

	Actitudes/comportamiento ante la inseguridad
Uso de TIC	Autopercepción de alta eficacia
	Autopercepción de baja eficacia
	Formación relacionada con TIC
	Consecuencias de no usar las TIC
	Necesidad de apoyo social/instrumental
Percepción de las TIC	Consecuencias de la alta digitalización
	Impacto de COVID-19 en la digitalización
	Percepción de obligación en el uso
	Emociones relacionadas con el uso de TIC
	Evaluación de las TIC

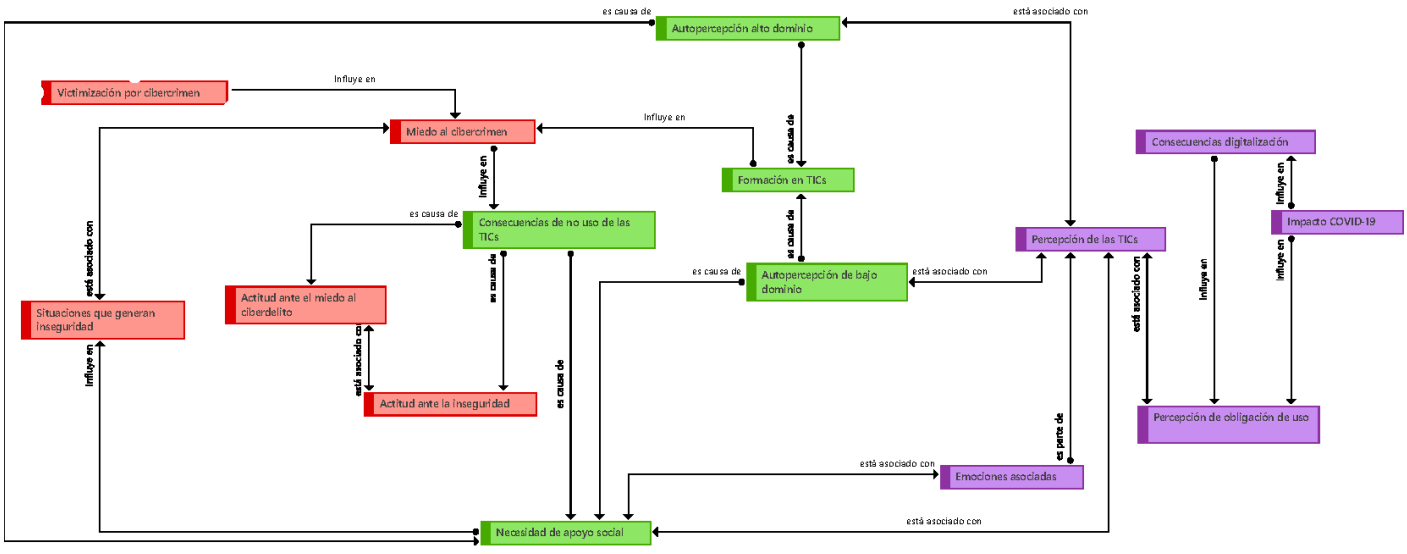


Figura 2. Códigos y sus asociaciones (Anexo III)

Las siguientes secciones detallan cada uno de estos temas principales y los códigos que los componen, así como algunas frases representativas de cada uno de estos códigos.

7.4.1 Temas principales y códigos

7.4.1.1 Miedo al cibercrimen e inseguridad asociada al uso de TIC

Este tema se compone de cinco códigos. En primer lugar, respecto al miedo al cibercrimen, se observa que en el grupo A (estudiantes que únicamente participaron en educación presencial) hay un mayor número de participantes que informaron de miedo respecto a la posibilidad de convertirse en víctimas de un ciberdelito, específicamente fraudes en línea, en comparación con el grupo B (estudiantes que únicamente participaron en educación en línea). Solo dos participantes de este grupo (A) manifestaron no haber experimentado este miedo al utilizar herramientas digitales, uno de ellos debido a que no había realizado transacciones bancarias en formato online nunca y el otro porque consideraba que las aplicaciones de banca en línea eran suficientemente seguras. Es importante mencionar que ambos participantes fueron los dos participantes masculinos del grupo A. En contraste, en el grupo B se encontró que la mayoría de los participantes no temían convertirse en víctimas de delitos al usar las TIC. Solo tres participantes en este grupo dijeron tener miedo a ser víctimas de cibercrimen, refiriendo específicamente el temor a ser víctimas al hacer transacciones en línea o compras en páginas web.

En segundo lugar, con respecto a haber sido víctima de cibercrimen, aunque esta cuestión no fue planteada directamente, algunos participantes se refirieron a experiencias previas durante la entrevista. En el grupo A, tres personas habían sido víctimas de cibercrimen relacionado con fraude. En el grupo B, solo una participante informó haber sido víctima de cibercrimen a través de un enlace en un correo electrónico, lo que provocó la infección por un virus de su ordenador, aunque esto no tuvo repercusiones financieras para ella. Por tanto,

ser víctima de un delito está asociado, como se observa en la Figura 1, con el miedo al cibercrimen. Sin embargo, esta relación presenta una baja asociación en nuestros datos.

En tercer lugar, en cuanto a la actitud/comportamiento frente al miedo al cibercrimen, encontramos que en ambos grupos las respuestas se centran en dos comportamientos principales. El primero de estos comportamientos es evitar el uso de herramientas o plataformas digitales en las que consideran que hay peligro de cibervictimización. En ambos grupos, varios participantes optaron por esta estrategia, pese a considerar útil la herramienta que dejaban de utilizar. Aquí se presentan algunos ejemplos de frases extraídas de las transcripciones de las entrevistas:

Grupo A: "Comprar en línea es muy cómodo, pero no lo uso porque me da miedo"; "Cuando recibo correos electrónicos que no sé de quién son, me asusto, no confío mucho en ellos. A veces los borro y luego me dicen que me los enviaron y no era nada malo".

Grupo B: "Si tengo miedo, lo borro directamente"; "Nunca he comprado en línea porque me da un poco de miedo que me estafen".

El segundo comportamiento que adoptaban los participantes frente al miedo y que se encontraba presente en los participantes de ambos grupos fue solicitar ayuda u opinión a personas cercanas: "Cuando tengo que comprar algo le pregunto a mis hijas, ellas lo compran por mí y les hago un bizzum" (grupo A); "Mi hijo lo hace por mí, pero me da un poco de vergüenza" (grupo B).

En cuarto lugar, se analizaron las situaciones que generan inseguridad al utilizar las TIC. Esta variable está estrechamente relacionada con el miedo al cibercrimen, ya que en muchas ocasiones tanto la inseguridad como el miedo al cibercrimen se presentan en situaciones específicas, especialmente aquellas relacionadas cualquier tipo de transacción que implica un pago. No se detectaron diferencias entre los dos grupos en este código, ya que ambos grupos dieron respuestas similares que seguían la misma línea. Varios participantes mencionaron la inseguridad generada por procedimientos que requerían realizar muchos pasos, ya que esto impedía saber si estaban

realizando correctamente el proceso o no. Otro factor que generaba inseguridad en ambos grupos era el desconocimiento de términos que se usan frecuentemente en contextos digitales (como “enlace” o “nube”) ya que no sabían a qué se referían exactamente.

Finalmente, se aborda la actitud/conducta hacia la inseguridad. Este código presentó una fuerte asociación con el código de necesidad de apoyo social o instrumental, que analizaremos más adelante. En el grupo A, se observa que la ausencia de este tipo de apoyo al usar las TIC era determinante, ya que esto unido a la sensación de inseguridad en ciertos entornos digitales provocaba que dejasen de utilizarlas, como se puede observar en este ejemplo: "Cuando me siento insegura, si no tengo a nadie cerca para ayudarme, no las uso. Si tan solo me lo explicaran y pudiera hacer un guion para las próximas veces sería diferente". En el grupo A, se encontraron varias respuestas en la misma línea, refiriéndose a la necesidad de apoyo en situaciones digitales que no saben manejar o con las que no están familiarizados. Sin embargo, aunque en el grupo B las respuestas fueron similares, en cuanto a la necesidad de apoyo, detectamos que la principal diferencia es que los individuos en este grupo cuentan con este tipo de apoyo en más ocasiones. No obstante, la mayoría de los participantes en ambos grupos coinciden en que si se sienten inseguros o tienen miedo de ser victimizados en línea y no tienen apoyo, prefieren dejar de usar las TIC.

7.4.1.2 Uso de TIC

Este tema se compone de 5 códigos.

En primer lugar, la autopercepción de alto dominio en el ámbito digital. Este código fue muy heterogéneo, tanto en general, teniendo en cuenta los dos grupos como conjunto, como dentro de cada uno de los grupos de nuestra muestra (Grupo A: presencial y Grupo B: en línea), sin que se encontraran diferencias entre ellos ni patrones significativos dentro de cada uno de los grupos. En general, los usos en los que consideraban que su habilidad era

mayor eran aquellos en los que más habían practicado, como por ejemplo la búsqueda de información en Google y el uso de WhatsApp y otras redes sociales.

En segundo lugar, en cuanto al bajo dominio autopercibido, al igual que sucedía en el código anterior, las respuestas fueron heterogéneas, aunque en el grupo A (presencial) hubo más respuestas referidas al bajo dominio percibido en compras y banca online.

En tercer lugar, la formación relacionada con las TIC. Las respuestas en este código fueron homogéneas tanto dentro de cada uno de los grupos como teniendo en cuenta a todos los participantes de la muestra total, ya que sólo uno de los participantes (en el grupo B - en línea) informó de que había recibido formación para utilizar las TIC de forma adecuada. En el resto de los participantes, la mayoría de los participantes nunca había recibido formación formal sobre herramientas digitales, y si habían recibido algún tipo de formación consideraban que no era suficiente para manejar las TIC de forma adecuada. Por lo tanto, la mayoría de las personas de nuestra muestra habían aprendido de forma autodidacta o con el apoyo de familiares, amigos u otras personas de su entorno cercano. En ambos grupos se hizo referencia al hecho de que los cursos centrados en el aprendizaje de una herramienta digital específica no les resultaban útiles, ya que la tecnología avanzaba muy rápido y todo lo aprendido quedaba pronto obsoleto, debido a rápidas actualizaciones que cambiaban la apariencia de la herramienta o sus funcionalidades, lo que impedían que siguieran usándola adecuadamente.

En cuarto lugar, las consecuencias de no utilizar las TIC. En este código encontramos una gran mayoría de respuestas referidas a consecuencias negativas en ambos grupos. Las personas del grupo A consideraban que no utilizar las TIC a menudo significaba que el acceso a recursos en diversas áreas era más limitado, por lo que se quedaban atrás en algunos aspectos. Adicionalmente, consideraban que no usar estas herramientas aumentaba su aislamiento, en comparación con las personas que sí utilizaban las TIC. Algunos ejemplos extraídos de las transcripciones de las entrevistas son: «Una de las consecuencias es ir por detrás de la gente que sí las utiliza, voy muy atrasada

pero no me queda otra» o «A veces me siento aislada». En el grupo B, aunque sí utilizaban las TIC, se imaginaban las consecuencias de no utilizarlas y todos los participantes informaron de consecuencias negativas, como se ilustra en estos ejemplos: «Tendría que renunciar a muchas cosas, sería terrible» o «Me sentiría completamente aislado».

En quinto lugar, la necesidad de apoyo social o instrumental. Ambos grupos se refirieron a esta variable como determinante en su interacción con las TIC. En el caso de las personas del grupo A (que no utilizaban herramientas digitales), consideraban que, si tuvieran una persona de apoyo que pudiera resolver sus dudas y decirles si iban por buen camino cuando estaban utilizando estas herramientas, harían un mayor uso estas. Algunos ejemplos: «Necesitaría una persona a mi lado porque cuando viene mi hijo, entonces sí las uso»; «No tener conocimientos o una persona a mi lado que me resuelva las dudas hace que no lo haga» o «Antes, uno de mis hijos vivía conmigo y me resolvía todos los temas de nuevas tecnologías. Pero ahora que se ha ido es como que no te queda más remedio que empezar a aprender y bueno...». En el caso del grupo B, también consideraron este apoyo como una variable determinante, ya que consultaban a familiares o personas de su entorno cuando se sentían inseguros al utilizar estas herramientas o querían asegurarse de que determinadas transacciones online no suponían una situación peligrosa.

7.4.1.3 Percepción de las TIC

Este tema se compone de 5 códigos.

En primer lugar, las consecuencias que los participantes percibían debido a la alta digitalización en multitud de áreas que pueden ser determinantes para actividades de la vida diaria. En este código encontramos una clara diferenciación entre las respuestas dadas por el grupo A y las del grupo B. En el caso del grupo A, consideraban que el proceso de alta digitalización en estas áreas era un hecho negativo, ya que discrimina a diferentes grupos de personas, entre las que incluían a personas adultas mayores y personas con diversidad funcional, por ejemplo. Además, las respuestas aludían con frecuencia a la

incomprensión de las herramientas digitales, ya que la mayor parte de su vida el contexto en el que habían vivido no era digitalizado y, por tanto, desconocían muchos términos y procesos que otras personas daban por sentados, lo que dificultaba la adaptación a estas herramientas. Sin embargo, en el caso del grupo B, la mayoría de los participantes pensaban que la digitalización era un cambio al que había que adaptarse y no lo percibían como algo negativo, ya que aunque lo consideraban un reto también tenían la percepción de la alta digitalización como un contexto que les proporcionaba una oportunidad para tener acceso a un mayor número de recursos, que no estarían disponibles en el contexto físico. Este código se analizará con más detalle en el punto 5.1.4.3 de este capítulo.

En segundo lugar, la influencia de la COVID-19 en el proceso de digitalización. La mayoría de los participantes en ambos grupos consideró que la situación derivada de la pandemia había acelerado el proceso y había ayudado a algunas industrias, como la banca y los servicios sanitarios, a digitalizar procesos y prescindir de trabajadores.

En tercer lugar, la percepción de la obligación de utilizar las TIC. Dentro de este código había una clara diferenciación entre los dos grupos. Mientras que la mayoría de los participantes del grupo A se sentían obligados a utilizar las TIC, no ocurría lo mismo en el grupo B, donde sólo dos participantes lo consideraban una obligación. Este sentimiento de obligación estaba muy correlacionado con las emociones expresadas por los participantes sobre el uso de las TIC, como se describe a continuación.

En cuarto lugar, las emociones relacionadas con las TIC. Este código estaba relacionado con la percepción de obligación, ya que los participantes del grupo A que manifestaron sentirse obligados a utilizar las TIC relacionaron esta obligación con emociones negativas: «Esto me ha hecho sentir muy mal y la primera sensación es que me da mucha rabia porque ¿por qué me tienen que obligar a hacer cosas que no quiero hacer?». Como se desprende de este ejemplo, para los participantes del grupo A, estas emociones negativas estaban provocadas por el hecho de no tener una alternativa a la opción digital. En este grupo, incluso en los casos en los que no se percibía ninguna obligación,

encontramos emociones negativas, en su mayoría asociadas a la tristeza. Sin embargo, en el grupo B, las emociones asociadas eran mayoritariamente positivas, ya que percibían las TIC como una oportunidad para hacer cosas nuevas o ahorrar tiempo en algunas tareas. Este apartado se analizará más detalladamente en el siguiente apartado.

Por último, la valoración de las TIC. De nuevo, observamos diferencias entre los dos grupos: mientras que el grupo A valoraba mayoritariamente las TIC de forma negativa, el grupo B las valoraba de forma positiva. Sin embargo, este código está influido directa o indirectamente por los cuatro códigos anteriores, así como por otros códigos que se encuentran dentro de otros temas, como podemos ver en la Figura 1. Variables como el apoyo disponible o la percepción de obligación son importantes en la valoración de las TIC.

7.4.2 Emociones predominantes

La realización de nubes de palabras proporciona una visión visual y concisa de las emociones predominantes experimentadas por los participantes en el estudio. Estas representaciones visuales destacan las palabras clave más relevantes y frecuentes asociadas con la experiencia de uso de las TIC en cada uno de los grupos estudiados (Figura 3 y 4).

Observando las nubes de palabras generadas, se identificaron las emociones predominantes experimentadas por las personas participantes en el estudio al utilizar las TIC en cada uno de los grupos. Las palabras clave más destacadas en las nubes de palabras indicaron las emociones más frecuentes y relevantes asociadas a esta experiencia.

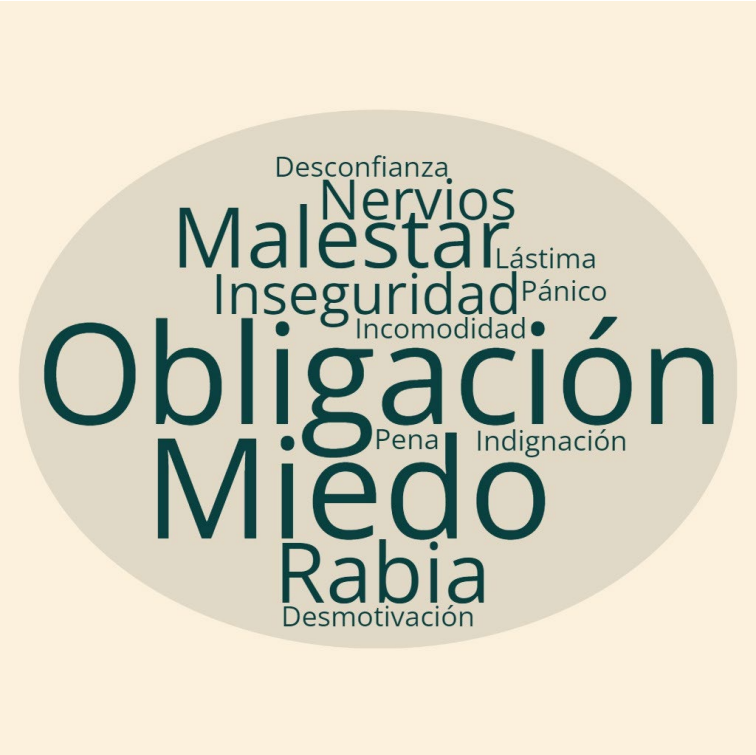


Figura 3. Emociones predominantes A

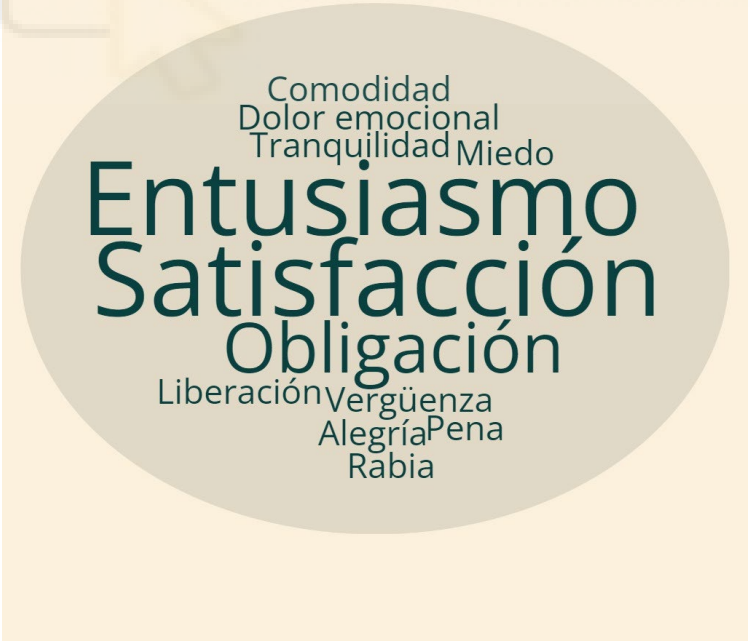


Figura 4. Emociones predominantes B

A continuación, se presentan algunos ejemplos narrativos extraídos de las transcripciones literales de las entrevistas en relación a algunas de las diferentes emociones detectadas en cada uno de los grupos.

Grupo B: “Me ha dado vida, me ha dado alegría, estoy contactando con gente de otros países… ¡Es que estoy loca! Y lo de la universidad online… eso ya me ha hecho super feliz. Yo es que estoy super bien, no puedo decir nada más que buenas cosas, de momento.”; “He visto a compañeros que no se han podido o no se han atrevido a matricularse online, veo a gente en los cajeros que protesta y se enfada, sobre todo gente mayor... entonces me duele.”

Grupo A: “Te da rabia porque te molesta no poder estar al tanto de ciertas cosas por la barrera. Para mí es una barrera a veces infranqueable”; “Pues me hace sentir muy mal, un bicho raro y una analfabeta. Yo digo que soy una analfabeta tecnológica y creo que me siento como se podrían sentir hace años los analfabetos, las personas que no sabían ni leer ni escribir supongo que ante ciertas cosas se sentirían muy mal porque no poder… y yo ahora me siento así muchas veces.”

7.4.3 Dinámicas Emocionales y Adaptativas ante las TIC

Al analizar las nubes de palabras, se identificaron patrones emocionales relacionados con el uso de las TIC en nuestra muestra, que proporcionaron una comprensión más profunda de las experiencias de este grupo de población ante estas herramientas. Se observó un patrón emocional positivo en el grupo B (uso cotidiano de las TIC) relacionado con el entusiasmo y la satisfacción al utilizar las TIC tanto para comunicarse con sus seres queridos como para el acceso a recursos no disponibles fuera del entorno digital.

Ejemplos narrativo grupo B: “Me ha abierto una puerta al mundo estando en mi casa tranquilamente.”; “Estas navidades pasadas cené sola en mi casa, pero con mi hija, mi yerno y mi nieta a través de a través del ordenador. Estuvimos cada uno en su casa con el ordenador al lado de la mesa e hicimos la reunión.

También me permite, pues como tengo bastante familia, bueno bastante no, tengo toda mi familia por parte mía, fuera de España entonces pues me permiten estas aplicaciones estar en contacto."

Sin embargo, aunque la mayoría de las palabras clave reflejaban emociones positivas, también se encontraron algunas palabras relacionadas con la inseguridad y la necesidad de apoyo por parte de otras personas ante esta emoción, la inseguridad.

Ejemplos narrativos grupo B respecto a esta cuestión fueron: "Cuando no se hacer algo doy mil vueltas y lo hago de otra manera. O llamo a mi hijo y me lo explica bien, vuelvo a meterme y vuelvo a hacerlo."; "Yo vivo sola y me conecto con mis hijas y me enseñan cosas. Lo utilizo en el día a día."; "Si alguna vez me siento inseguro en algo nada más que tengo que levantar el teléfono y llamo a mi hijo"; "Hay cosas que me cuestan, como configurar un móvil nuevo, mi hijo sí que me lo me lo hace, aunque me da un poco de vergüenza."

En relación al grupo A, se observó un patrón de frustración y percepción de obligación de uso. Esto estuvo estrechamente vinculado con la dificultad percibida al utilizar ciertas herramientas y la falta de alternativas disponibles a la herramienta digital. Además, se detectó una percepción de falta de apoyo en la mayoría de los discursos de los participantes, lo que dificultaba aún más su adaptación a las diferentes herramientas digitales, especialmente cuando no tenían control sobre la herramienta utilizada.

Ejemplo narrativo grupo A: "Esto me ha hecho sentir muy mal y la primera sensación es que me da mucha rabia porque ¿por qué tienen que hacerme pasar a mí por cosas que no quiero hacerlas? Tienen que poner servicios para todos, también para los que no sabemos utilizar las nuevas tecnologías."; "No tener conocimientos ni una persona a mi lado que me resuelva las dudas hace que no lo haga. Necesitaría a una persona a mi lado porque cuando viene mi hijo, entonces sí lo hago."

7.4.4 Consecuencias del no uso de las TIC

En este caso, ambos grupos coincidían en la mayoría de las consecuencias que consideraban que tenía para ellos no hacer uso de las TIC (el grupo B indicaba posibles consecuencias en el hipotético caso de que no hiciesen uso de estas herramientas y el grupo A indicaba las consecuencias que ya experimentaban). Las palabras clave destacadas (Figura 5 y 6) revelan un impacto negativo en diferentes aspectos de sus vidas como el aislamiento social y una limitación de acceso a recursos e información necesaria en el día a día.

Figura 5. Consecuencias grupo A

Figura 6. Consecuencias grupo B

A continuación, se muestran algunos ejemplos narrativos de ambos grupos.

Grupo A: "Tiene unas consecuencias tremendas, muy duras. Tienes que anular muchas cosas, tienes que dejar de hacer muchas cosas, tienes que valerte de tus familiares más jóvenes y lo pasas muy mal."; "Personas como yo que viven solas tienen que hacer los pedidos por internet y cosas así y todo el mundo no sabe manejar internet, ya tienes que depender de otra persona y pedir ayuda."

Grupo B: "Para mis las consecuencias serían catastróficas. Sobre todo, no me podría comunicar con mucha gente porque no solamente es el ordenador, son los móviles, son los WhatsApp, es todo. Y bueno, yo socialmente las utilizo mucho a esos niveles, un poco pobres, bueno quitando que haces alguna videollamada y entonces los ves, a mis hijos. Pero bueno, sería horrible, no los podría ver, no podría ver a mi nieta, no podría tener información, no podría hacer los cursos de la universidad, no podría ver en mi saldo si me queda

dinero o no, son muchas cosas. Ya te he dicho que es la época de las tecnologías y ya no podemos vivir sin ellas, esto está ya así."

7.5 DISCUSIÓN

El principal objetivo de este estudio fue explorar cómo el uso y la falta de uso de las TIC pueden afectar emocional y socialmente a las PAM. En particular, se pretendía examinar cuestiones como los factores o contextos asociados con la inseguridad en línea o el miedo al cibercrimen y cómo esto podría influir en su percepción de las TIC. Adicionalmente, se buscaba determinar las disparidades en las emociones predominantes, patrones emocionales y posibles consecuencias asociadas con la digitalización entre dos grupos de PAM con características sociodemográficas similares, pero con un uso distinto de las TIC en su vida diaria.

En nuestra muestra encontramos que el temor al ciberdelito, especialmente el de naturaleza económica, era más prevalente en los adultos mayores que no emplean las TIC (grupo A), alineándose con investigaciones previas (Brands & Van Wilsem, 2021; Virtanen, 2017). Este temor puede motivar la evitación de actividades en línea, como se observa en aquellos con escasa familiaridad con las TIC. Además, esta evitación, generada por el miedo, podría ampliar la brecha digital ya existente entre los adultos mayores y otros grupos etarios (Bouma et al., 2007; Heinz et al., 2013; Olejniczak-Szuster & Dziadkiewicz, 2020). Algunas teorías desarrolladas para entornos tradicionales fuera de línea, como la teoría de la percepción de la vulnerabilidad sugieren que la incapacidad percibida para enfrentar situaciones aumenta la vulnerabilidad y las conductas de evitación (Hale, 1996), lo que también podría suceder en este entorno. Por lo tanto, la capacitación en TIC para PAM debería dirigirse tanto a mitigar el impacto del ciberdelito como a fortalecer su capacidad para lidiar con los riesgos que se encuentran en este contexto. Adicionalmente, es esencial priorizar la capacitación en contextos digitales críticos para la participación en la sociedad, como la banca en línea y las compras en línea, donde se observa un mayor temor o inseguridad. En contraste con el grupo A, la mayoría de los usuarios habituales de TIC (grupo B) no experimentan temor al ciberdelito. Sin embargo, la falta de capacitación en seguridad digital en toda la

muestra podría llevar a una subestimación de los riesgos y aumentar el peligro de victimización en línea en este grupo (Back & LaPrade, 2019; Choi, 2008; Shibata et al., 2022), por lo que es necesario que reconozcan los riesgos digitales para sean capaces por sí mismos de poner en práctica medidas de seguridad adecuadas (Miró-Llinares, 2011).

En cuanto a la inseguridad, debemos tener en cuenta que la falta de habilidades digitales puede generar incertidumbre al realizar actividades en línea, de forma similar a lo que sucede en el entorno físico (Valera & Guàrdia, 2014). La falta de alfabetización digital puede llevar a la interrupción del uso de las TIC, al sentirse perdidos o desorientados al enfrentarse a interfaces digitales poco intuitivas o al intentar comprender términos técnicos específicos. A este respecto, Schepers y Wetzels (2007) señalan la importancia de crear herramientas sencillas y adaptadas que faciliten el uso de las tecnologías, especialmente para las PAM. Además, la rapidez con la que evolucionan estas herramientas puede dificultar aún más la tarea, lo que puede generar sentimientos de frustración y desmotivación. Como hemos observado, en estos casos el apoyo social e instrumental puede ser un factor clave al ofrecer orientación y retroalimentación (Goetz & Boehm, 2020).

En cuanto a otras emociones prevalentes las nubes de palabras realizadas indican que los individuos del Grupo A manifiestan sentimientos adversos relacionados con la digitalización, tales como “sensación de obligación” y un marcado “sentimiento de incompetencia”. Este patrón de respuesta emocional negativa hacia las TIC se alinea con las conclusiones de Mitzner et al. (2010), quienes identificaron que las personas que experimentan sentimientos como ansiedad o frustración al interactuar con dispositivos tecnológicos muestran menos inclinación hacia la adopción y el uso efectivo de dichas herramientas, en comparación con quienes abordan la tecnología con una perspectiva más optimista. Esto se considera especialmente significativo frente a la problemática de la exclusión digital, que no solo incrementa el riesgo de aislamiento social, sino que también puede afectar la autoestima negativamente (Eshet-Alkalai & Chajut, 2010). Adicionalmente este tipo de exclusión puede tener consecuencias devastadoras para la salud mental a largo plazo, aumentando el riesgo de depresión, ansiedad y otros trastornos psicológicos (Choi & DiNitto, 2013, Santini

et al., 2020). Teniendo en cuenta estas particularidades, consideramos necesario desarrollar intervenciones que tengan en cuenta las emociones que pueden generar la alta digitalización en este sector de la población. Es fundamental que, para que cualquier intervención en esta área sea efectiva, se atiendan las necesidades y circunstancias particulares de estos grupos (Schlomann et al., 2020; Seifert et al., 2017).

En contraste, la mayoría de participantes del grupo B percibe la digitalización como una oportunidad de aprendizaje y una vía para acceder a nuevas herramientas y/o recursos y para establecer conexiones sociales. En esta misma línea, Melenhorst et al. (2001) exploraron los beneficios percibidos del empleo de TIC entre PAM, y sus resultados indicaron que las emociones positivas relacionadas con la tecnología, como satisfacción y disfrute, guardaban una estrecha relación con un mayor interés y participación en el uso de las TIC de forma continuada. Además, este grupo, al percibir la digitalización como una oportunidad de aprendizaje tiene acceso a nuevas herramientas, recursos y conexiones sociales, una ventaja que puede contribuir significativamente a su bienestar emocional y mental (Cotten et al., 2013).

Por último, referido a las consecuencias asociadas al no uso de las TIC por parte de las PAM, la mayoría de participantes de ambos grupos mencionaron como consecuencias negativas un mayor aislamiento al tener un menor número de contactos sociales y un acceso reducido a recursos disponibles. En la misma línea, Berkowsky et al. (2017) señalaron que el no uso de las TIC por parte de las personas mayores limitaba su acceso a recursos y servicios importantes en su vida diaria, como información de salud, servicios bancarios en línea y oportunidades de aprendizaje, pudiendo afectar directamente a su calidad de vida. En este punto, es relevante considerar la evidencia que correlaciona la soledad con un deterioro de la salud mental en edades avanzadas (Courtin & Knapp, 2017), así como el incremento en la prevalencia de la soledad entre los adultos mayores tras la pandemia de COVID-19 (Van Tilburg et al., 2021). Nuestros resultados coindicen con investigaciones como las realizadas por Czaja et al. (2018) quienes hallaron que el no uso de las TIC por parte de PAM se asociaba con un mayor riesgo de aislamiento social y una menor participación en actividades sociales.

Adicionalmente, la soledad, concebida como la percepción subjetiva de aislamiento social o carencia de vínculos emocionales con otros individuos (Cacioppo et al., 2006), puede inducir en las personas adultas mayores (PAM) una serie de estados emocionales adversos, tales como tristeza, ansiedad, depresión y una reducción en la percepción de calidad de vida (Hawkley & Cacioppo, 2010). Además, se ha establecido una asociación significativa entre la experiencia de la soledad y un incremento en el riesgo de desarrollar problemas de salud tanto físicos como mentales, incluyendo trastornos cardiovasculares, deterioro cognitivo y una mayor tasa de mortalidad (Cacioppo et al., 2006; Hawkley & Cacioppo, 2010).

7.6 CONCLUSIONES

La creciente digitalización, acelerada como consecuencia de las medidas de restricción social impuestas por la COVID-19, sitúa a las personas mayores en una situación complicada. Aunque el uso de las TIC por parte de este grupo poblacional es un espectro (Loos, 2012), en este estudio se tuvieron en cuenta las dos posibilidades situadas en los extremos. Por un lado, usuarios que han implementado las TIC en su vida diaria, pero sin la formación adecuada para ello y, por lo tanto, sin habilidades suficientes para protegerse, lo que aumenta su probabilidad de convertirse en víctima de delitos en línea. Por otro lado, los adultos mayores que no utilizan las TIC y por tanto no pueden acceder a los recursos que estas herramientas ofrecen, pudiendo aumentar todavía más la soledad a la que algunos ya están expuestos, con las consecuencias asociadas (Armitage et al, 2020).

Es cierto que el uso de las TIC puede tener beneficios en diferentes contextos para las PAM (Sourbati, 2008; Vivian Miller et al., 2021; Yang et al., 2018) pero no debemos olvidarnos de los problemas que pueden estar asociados a su uso, aunque estos han sido más estudiados en otros grupos poblacionales (Orosco & Pomasunco, 2020; Romero & González, 2018; Shensa et al., 2017; Spraggins, 2009; Tsitsika et al., 2014). Dado que los datos sobre inseguridad, miedo al cibercrimen y uso de las TIC en esta franja etaria son más limitados que en este grupo de edad, los resultados de nuestro estudio sugieren que es necesario continuar con esta

línea de investigación. Comprender la inseguridad, el miedo, las consecuencias de la exclusión digital y otros factores relevantes en este ámbito dentro de este grupo poblacional nos permitirá implementar políticas y estrategias de formación inclusiva y de calidad que promueva una relación positiva con el entorno digital y permita a los ciudadanos adultos mayores protegerse de los diversos peligros en línea mientras acceden a los beneficios que este entorno ofrece.

Además, los datos presentados se quiere destacar la necesidad de proporcionar un respaldo tanto social como instrumental para facilitar la plena integración de las PAM en nuestra sociedad altamente digitalizada. Este respaldo no solo actuaría como orientación en el uso adecuado de las herramientas digitales, sino que también requeriría la implementación de programas formativos adaptados a las características educativas específicas de las PAM destinatarias de dichas herramientas. Es necesario considerar su nivel previo de alfabetización digital y su comprensión de la terminología asociada. Asimismo, se recomienda el diseño de herramientas digitales más intuitivas, tomando en cuenta las capacidades funcionales de las personas a las que van dirigidas. La usabilidad y accesibilidad emergen como aspectos esenciales a considerar en este proceso de diseño, tal como lo respaldan investigaciones previas (Lee & Coughlin, 2015). Por último, en consonancia con las observaciones de Chu et al. (2009), resulta imperativo considerar la gestión emocional asociada al empleo de estas tecnologías. Dichos autores identificaron la ansiedad tecnológica y el temor a cometer errores como factores emocionales que pueden incidir en la adopción y utilización de las TIC en este grupo demográfico. En este sentido, resulta fundamental el diseño de tecnologías accesibles, intuitivas y centradas en el usuario, con el fin de asegurar una experiencia positiva y gratificante durante su uso. A través de estas medidas, se fomentará el bienestar emocional y social de las PAM, contribuyendo así a mejorar su calidad de vida en la era digital. Por tanto, este enfoque holístico contribuiría a mejorar la experiencia de las personas mayores con las tecnologías digitales, optimizando así los beneficios que estas pueden ofrecer para mejorar su calidad de vida.

Al reconocer las limitaciones inherentes a nuestro estudio cualitativo, debemos señalar las propias de un estudio cualitativo. Aunque el tamaño de la muestra es

pequeño (n = 16) es similar al de otros estudios en el campo de la criminología (Cross, 2016; Heap, 2021; Huber, 2022). Una segunda limitación es el ámbito geográfico del estudio, que se llevó a cabo exclusivamente en la provincia de Alicante, España. Esto significa que los resultados no necesariamente pueden generalizarse a una población más amplia. Las narrativas personales y las experiencias compartidas, si bien son valiosas para obtener una comprensión en profundidad, deben ser interpretadas con precaución al intentar aplicarlas a un espectro más amplio de la población. Por lo tanto, cualquier conclusión o recomendación derivada de esta investigación debe ser considerada de forma preliminar y sujeta a futuras investigaciones que aborden una gama más amplia de contextos y participantes.

Sin embargo, los resultados de este estudio proporcionan una visión más completa del miedo al ciberdelito y la inseguridad en este grupo poblacional, además de otras emociones, la necesidad de apoyo mientras se utilizan las TIC y las consecuencias asociadas al uso y no uso de estas herramientas. Estos hallazgos respaldan la importancia de desarrollar estrategias y programas de alfabetización digital adaptadas al contexto real del heterogéneo grupo de personas mayores con el fin de mejorar su competencia tecnológica y reducir las posibles consecuencias negativas asociadas a la alta digitalización.

Por último, en la síntesis de nuestras conclusiones, es relevante enfatizar la necesidad de integrar en futuros estudios y políticas públicas las experiencias y realidades de aquellos adultos mayores que no utilizan las TIC. Su ausencia en la conversación digital no solo perpetúa la brecha tecnológica, sino que también invisibiliza los desafíos únicos que enfrentan, como se ha explicado previamente. Así pues, un compromiso con la inclusión digital exige que atendamos diligentemente a esta población, comprendiendo sus reticencias y barreras, y desarrollando soluciones inclusivas que promuevan un acceso equitativo.

CAPÍTULO 8. CONSECUENCIAS DE LA CIBERVICTIMIZACIÓN EN PAM

8.1 JUSTIFICACIÓN DEL ESTUDIO

En los últimos años, la digitalización ha traído consigo un aumento significativo en el cibercrimen, un incremento particularmente notable durante la pandemia de COVID-19 en 2020, informando de un aumento significativo en las pérdidas económicas debido a fraudes cibernéticos, especialmente entre personas de 60 años o más (FBI, 2023).

El porqué de esta mayor victimización de este grupo etario no tiene una única respuesta, debido a su heterogeneidad. En primer lugar, una mayor implementación de las TIC a las rutinas diarias predice per se un aumento de la tasa de cibervictimización, basándonos en la Teoría de las Actividades Cotidianas de Cohen y Felson (1979), tal como se ha presentado anteriormente. Pero, además, las PAM cuentan con ciertas características que también pueden aumentar su situación de vulnerabilidad.

La situación de vulnerabilidad de este grupo a diversas formas de fraude se encuentra profundamente enraizada en una interacción compleja de factores cognitivos, económicos, y sociales. El deterioro cognitivo, los cambios en la regulación emocional y motivacional, una naturaleza excesivamente confiada, vulnerabilidad psicológica, y el aislamiento social contribuyen significativamente a la susceptibilidad al fraude en este grupo etario (Shao et al., 2019). De hecho, incluso un deterioro cognitivo leve se encuentra directamente relacionado con un mayor riesgo de victimización por fraude (Ueno et al., 2021). Estudios específicos han demostrado que, aunque los inversores de mayor edad pueden poseer conocimientos financieros equivalentes a los de los inversores más jóvenes, tienden a ser menos eficaces en la práctica, lo cual se refleja en un aumento del riesgo de ser víctimas de fraude (Korniotis & Kumar, 2011). Adicionalmente, contamos con evaluaciones forenses que afirman que muchas víctimas de fraude y explotación financiera entre las personas adultas mayores muestran deficiencias notables en pruebas de funcionamiento cognitivo y toma de decisiones financieras,

lo que podría aumentar la situación de vulnerabilidad a este tipo de delitos (DeLiema, 2018; Wood et al., 2014).

Así mismo, desde una perspectiva emocional y social, la inducción de excitación emocional puede incrementar la susceptibilidad de las personas adultas mayores a anuncios engañosos, debilitando su capacidad para discernir entre publicidad legítima y fraudulenta (Kircanski et al., 2016). De la misma forma, la percepción de soledad y el aislamiento social, reflejado en la falta de una red de amigos o familiares de confianza, también aumenta su vulnerabilidad al fraude, al dejarles sin un sistema de apoyo que podría ayudar a proteger sus activos (DeLiema, 2018; Alves & Wilson, 2008). Finalmente, el estado económico de los adultos mayores influye en la naturaleza del fraude al que son más susceptibles. Una mayor riqueza se ha asociado con una susceptibilidad incrementada al fraude relacionado con inversiones, mientras que una menor riqueza inmobiliaria, combinada con síntomas de depresión, ha sido vinculada a una mayor vulnerabilidad ante fraudes asociados a premios o loterías (DeLiema et al., 2020).

8.2 OBJETIVO DEL ESTUDIO

El objetivo de este estudio es evaluar el impacto del cibercrimen económico en personas adultas mayores en comparación con otros grupos de edad.

Basados en este objetivo se plantearon los siguientes objetivos específicos:

- Evaluar la prevalencia de distintos delitos económicos entre personas adultas y otros grupos de edad, así como una posible diferencia en la vulnerabilidad a ser víctimas de este tipo de delitos.

- Analizar la notificación de ciberdelitos económicos entre personas adultas mayores y otros grupos etarios, y los factores que influyen en su decisión de notificar.

- Examinar el impacto financiero y emocional de los ciberdelitos económicos en personas adultas mayores en comparación con otros grupos de edad.

8.3 MÉTODO

8.3.1 Procedimiento

La base de datos utilizada para abordar estas interrogantes procede de la encuesta "Estafas y fraudes experimentados por los consumidores", realizada por la Comisión Europea en el año 2019. El análisis de este estudio se centra en los datos provenientes de los residentes en los 28 Estados miembros de la UE, con un total de 26,735 sujetos. Las entrevistas se realizaron telefónicamente, con asistencia mediante ordenador e implementando un muestreo aleatorio estratificado para asegurar una muestra representativa. Con el fin de garantizar la representatividad, las muestras fueron ajustadas utilizando un método de ponderación posterior a la estratificación que integraba variables demográficas como edad, sexo y posesión de teléfono. Posteriormente, se efectuó una ponderación poblacional para que el tamaño de la muestra ponderada reflejara de manera proporcional el tamaño de la población elegible. Para aquellos encuestados que informaron haber sido víctimas de más de un tipo de fraude, se aplicó un método de respuesta mínima, enfocándose no en la última incidencia de fraude experimentada, sino en aquella para la cual existían menos respuestas al momento de la entrevista. Con el fin de ajustar proporcionalmente los perfiles y las proporciones de incidencia, se introdujo una fase adicional de ponderación para la submuestra de individuos que habían sido víctimas de fraude. Las ponderaciones necesarias fueron provistas junto con el conjunto de datos por los administradores de la encuesta, y las muestras ajustadas se emplearon en el análisis.

Dado el contexto de nuestro estudio, los análisis se realizaron con la submuestra española, contando con un total de 1010 sujetos y habiéndose recolectado estos datos entre el 22 de julio de 2019 y el 18 de septiembre de 2019.

8.3.2 Variables

A continuación, se detallan los ítems seleccionados en función de los objetivos del estudio y las variables de interés, así como su codificación.

- Datos sociodemográficos: edad (continua y categorizada en base de datos original en 3 grupos: 18-34 años, 35-54 años y 55 o más años); género (femenino, masculino, otro); nivel educativo (categorizado en base de datos original ordinalmente en tres niveles en función de la respuesta del participante: bajo, medio y alto).

- Uso de internet y compras online
    - Ítem D6 (variable ordinal): ¿Con qué frecuencia utiliza Internet para fines privados?
        - Todos los días o casi todos los días (1)
        - Al menos una vez a la semana (pero no todos los días) (2)
        - Al menos una vez al mes (pero no todas las semanas) (3)
        - Menos de una vez al mes (4)
        - Casi nunca (5)
        - Nunca (6)
        - No sé (7)

    - Ítem D6b (variable ordinal): En los últimos 2 años, ¿con qué frecuencia ha comprado productos o servicios en línea?
        - Al menos una vez a la semana (1)
        - Al menos una vez al mes (2)
        - Menos de una vez al mes (3)

- Casi nunca (4)
- Nunca (5)
- No sé (6)

- Objetivo de crimen económico

  Ítem Q1 (variable binomial en cada subcategoría: si/no): En los últimos 2 años, ¿ha experimentado personalmente alguno de los siguientes al comprar bienes o servicios, ya sea en línea o fuera de línea? Por favor, diga sí a cada uno que le aplique.
  Instrucción para el entrevistador: Marque sí en cualquier instancia de que el encuestado haya experimentado estas cosas, incluso si no actuó sobre la solicitud – por ejemplo, aunque no haya proporcionado la información personal solicitada o pagado la tarifa solicitada.

  - Estafa de compra:
    - Se solicitaron productos o servicios que se promocionaban como gratuitos o de bajo coste, pero que terminaron implicando una costosa suscripción mensual no anticipada. (Estafa de compra/Trampa de suscripción)
    - Se adquirió lo que se creía era una oferta favorable, pero los bienes o servicios nunca fueron entregados o eran fraudulentos o inexistentes. (Estafa de compra)
    - Se recibió una factura no solicitada y falsa por productos que el consumidor nunca había pedido, con la solicitud de cubrir el coste. (Estafa de compra o venta - Facturación falsa).

  - Robo de identidad:
    - Alguien lo contactó - por teléfono, en persona, por correo electrónico o por otro medio - fingiendo ser de una organización legítima como un banco, proveedor de servicios telefónicos o de internet, o un departamento

gubernamental, y le pidió que proporcionara (o confirmara) información personal (Robo de identidad – phishing)

- Fue abordado - por teléfono, en persona, por correo electrónico, por otro medio - o accedió a un sitio web y se le informó que tenía un problema con su ordenador o internet. Luego, le pidieron sus detalles personales y los datos de su tarjeta de banco o crédito para solucionar el problema (Robo de identidad - Estafas de acceso remoto)

- Fraude monetario
  - Le prometieron que recibiría un bien, un servicio, un reembolso o una ganancia importante en inversiones si transfería o invertía dinero (Estafa de inversión - Estafa de reembolso)
  - Compró entradas para un evento, concierto o viaje, pero resultó que los boletos no eran reales y/o nunca los recibió (Fraude entradas)
  - Alguien fingiendo ser de una organización legítima, como un banco, proveedor de internet o gobierno, afirmó que había problemas con su cuenta u otra documentación y lo amenazó con daño si no pagaba para resolver el problema (Amenazas y extorsión)
  - Recibió una notificación de un premio de lotería o una ganancia de concurso, pero se le informó que necesitaba pagar una tarifa o comprar un producto para reclamar su premio (Ganancia inesperada)

- Medio usado para el crimen económico

  Ítem Q3 (variable binomial en cada subcategoría: si/no) : ¿A través de qué canal experimentó esto?
  - Correo electrónico

- Mensaje de texto/SMS
- Una llamada telefónica en su móvil
- Una llamada telefónica en su teléfono fijo
- Fax
- WhatsApp, Facebook Messenger u otros canales de mensajería móvil
- Un anuncio en línea en un sitio web de redes sociales, blog o foro, como Facebook
- Un anuncio en línea en un sitio web no relacionado con redes sociales
- Un anuncio en una revista o periódico
- Una carta postal
- En persona a través de alguien que se le acercó en su casa
- En persona a través de alguien que se le acercó en otro lugar
- De alguna otra forma

Este ítem se utilizó en los análisis para categorizar los delitos económicos como online (correo electrónico, sms, llamada en teléfono móvil, mensajería móvil, anuncio en línea en redes sociales, anuncio en línea en página web) u offline (llamada en teléfono fijo, fax, un anuncio en revista o periódico, una carta, en persona en casa o en otro lugar). Pese a que las llamadas a un teléfono móvil se consideran frecuentemente como offline, en este trabajo se consideraron como online por dos motivos fundamentales: la diferenciación entre llamadas a teléfono móvil y teléfono fijo y el contexto específico de fraude en el que se engloba este trabajo, ya que pueden considerarse como un medio online especialmente cuando se emplean tecnologías como VoIP o VoLTE que requieren conexión a Internet. Este aspecto es crucial en contextos de fraude, donde los estafadores aprovechan las capacidades avanzadas de las llamadas basadas en Internet para enmascarar su identidad y manipular los números de teléfono desde los que llaman. Utilizando estas tecnologías, pueden realizar acciones fraudulentas a gran escala y a través de fronteras internacionales con menos restricciones legales y a un coste significativamente menor. Este uso de llamadas online ofrece a los criminales una herramienta potente y flexible,

diferenciándola significativamente de las llamadas a teléfonos fijos, que están más limitadas por las redes tradicionales y por su naturaleza más estática y rastreable. En los casos en los que el participante contesto "de alguna otra forma" se categorizó como "No especificado".

- Denuncia o notificación del delito económico

- Ítem Q6 (variable binomial en cada subcategoría: si/no): La experiencia de la que estamos hablando puede categorizarse como 'fraude'. Por favor diga sí, cada vez que le aplique a usted. Usted notificó el fraude a:
    - La policía
    - Una autoridad de protección al consumidor
    - Banco o compañía de tarjeta de crédito
    - Asociación de consumidores
    - Regulador de la industria (por ejemplo, autoridad de telecomunicaciones, autoridad de supervisión bancaria)
    - Amigos/familia
    - Otro

- Motivos por los que sí se notifica/denuncia

  Q7b (variable binomial en cada subcategoría: si/no): ¿Cuál fue la razón principal por la que notificó el fraude?

    - Sabía a quién notificarlo
    - Sentía que habría una diferencia
    - Tenía tiempo
    - Sufrió un daño emocional o financiero significativo
    - Robaron su identidad
    - No pudo seguir trabajando en su dispositivo
    - Para intentar evitar que suceda de nuevo ya sea a usted o a otras personas.
    - No sé

- Motivos por los que no se notifica/denuncia (o sólo se informa a familiares):

  Q7a (variable binomial en cada subcategoría: si/no): ¿Cuál fue la razón principal por la que no denunció el fraude? ¿Cuál fue la razón principal por la que no notificó del fraude a alguien más que a familiares/amigos?

  - No sabía a quién denunciarlo
  - Sentía que no habría diferencia
  - Me sentía avergonzado
  - No tenía tiempo
  - No hubo, o fue poco, el daño financiero o emocional
  - No se robaron detalles de mi identidad
  - Pude seguir trabajando en mi dispositivo
  - No sé

- Preferencia de vía de denuncia/notificación

  Ítem Q17 (variable binomial en cada subcategoría: si/no): Voy a leer seis opciones. Por favor, dígame a través de qué canal preferiría informar de un fraude.

  - Un sitio web gubernamental
  - Un sitio web no gubernamental
  - Un número de teléfono gratuito gubernamental
  - Un número de teléfono gratuito no gubernamental
  - Un puesto en una ubicación central en mi país
  - Vía email

- Consecuencias (financiaras y emocionales)
  - Ítem Q9 (variable ordinal): ¿Cuál fue la pérdida financiera total, si hubo alguna, que experimentó como resultado de este fraude? Por favor, incluya cualquier dinero que tuvo que gastar

obteniendo un nuevo portátil, software u otro equipo debido al Malware.

- 0€ (1)
- Menos de 50€ (2)
- Más de 50€ pero menos de 500€ (3)
- Más de 500€ pero menos de 2000€ (4)
- Más de 2000€ (5)

- Ítem Q10 (variable binomial en cada subcategoría: si/no): Aparte de la pérdida financiera, ¿qué otros efectos negativos tuvo el fraude en usted? Leeré algunos elementos, por favor diga sí a cada uno de los que le sucedió. Usted se sintió...
  - Enfadado
  - Irritado
  - Avergonzado
  - Estresado
  - Percibí un efecto negativo en mi salud física

- Comportamiento

  Ítem Q14 (variable categórica): Me gustaría preguntarle un poco más sobre su comportamiento en línea y fuera de línea. ¿Podría decirme si hace cada una de las siguientes cosas: siempre (1), a veces (2) o nunca (3)? (se incluyen en el estudio sólo las que se consideran exclusivamente online)
  - Evita hacer clic en enlaces en correos electrónicos o mensajes de texto a menos que conozca al remitente (online)
  - Se suscribe a un servicio específico para evitar llamadas comerciales
  - Instala software anti-spam o antivirus (online)
  - Transfiere dinero a alguien que no conoce (por ejemplo, a través de Western Union)
  - Realiza verificaciones sobre la credibilidad del vendedor

- Lee cuidadosamente los términos y condiciones
- Solo proporciona su tarjeta de identidad o información de su identificación en persona o en un sitio web seguro
- Solo realiza compras en línea con tarjeta de crédito (para recuperar su dinero si algo sucede) (online)
- Desconfía de cartas o correos electrónicos que contengan errores ortográficos y gramaticales
- Desconfía de personas desconocidas cuando se acercan a usted en persona, por teléfono, correo electrónico u otro medio

- Campañas informativas sobre fraude
  Ítem Q15: En los últimos 2 años, ¿ha visto algún anuncio u otra campaña para advertirle o informarle sobre el fraude? (Si/No)

8.3.3 Análisis de datos

Para realizar todos los análisis descritos en este estudio se utilizó el software estadístico SPSS v.27 (Statistical Package for the Social Sciences) y el software R (para el modelo de regresión logística). Para una visión general de la muestra de estudio, se realizaron análisis descriptivos que incluyeron el cálculo de frecuencias y porcentajes para las variables categóricas, tales como género, nivel educativo, frecuencia de uso de Internet, compras en línea, concienciación sobre fraudes, haber sido objetivo de delito económico, los medios utilizados para la distribución del delito, la notificación, las consecuencias de esta victimización y el comportamiento en línea. Para las variables continuas, en este caso la edad, se calculó la media y la desviación estándar. Dado que los objetivos se centran en evaluar las diferencias entre diferentes grupos de edad, tanto estos análisis como los análisis de correlación (en este caso pruebas chi cuadrado), se realizaron teniendo en cuenta la agrupación de los datos en tres categorías de edad: 18-34 años, 35-54 años, y 55 años o más.

Para evaluar si la probabilidad de victimización en delitos económicos realizados de forma digital variaría entre personas mayores si estas utilizaran internet con la misma frecuencia que los jóvenes, realizamos un análisis contrafactual utilizando una simulación basada en modelos. Dado que, en nuestra muestra original, al igual que en la población general, las personas adultas mayores utilizan internet con menor frecuencia que los jóvenes, y que esta diferencia podría influir en la probabilidad de ser víctimas de ciberdelitos, era necesario controlar esta variable para obtener conclusiones más precisas. Primero, construimos un modelo de regresión logística para predecir el uso frecuente de internet basado en variables sociodemográficas como edad, género y nivel educativo. Este modelo nos permitió calcular la probabilidad de uso frecuente de internet para cada individuo en la muestra. Para simular un escenario en el que las personas mayores usan internet con la misma frecuencia que los jóvenes, ajustamos estas probabilidades a un nivel constante, equivalente a la probabilidad media de uso frecuente de internet observada en las personas más jóvenes. Posteriormente, utilizamos estas probabilidades ajustadas para realizar una simulación, asignando de manera aleatoria el uso frecuente de internet a cada individuo en función de la probabilidad ajustada. Esto nos permitió crear un conjunto de datos contrafactuales en el que la frecuencia de uso de internet no varía significativamente con la edad. Finalmente, aplicamos un modelo de regresión logística sobre los datos simulados para analizar la relación entre la edad y la probabilidad de victimización en delitos cibernéticos, incluyendo una interacción entre edad y uso de internet. Este análisis nos permitió evaluar si, bajo un uso de internet constante, las personas mayores tendrían una mayor, menor o igual probabilidad de ser víctimas de ciberdelitos en comparación con los jóvenes.

8.4 RESULTADOS

8.4.1 Estadísticos descriptivos

La muestra total estuvo formada por 1010 sujetos, siendo su edad media 49.57 con una desviación estándar de 17.41. Las características sociodemográficas se detallan en la Tabla 17.

Tabla 17*. Variables sociodemográficas*

Variable	N, (%)
Edad	
18-34	233 (23.1)
35-54	394 (39.0)
55 o +	383 (37.9)
Género	
Femenino	483 (47.8)
Masculino	527 (52.2)
Nivel educativo	
Bajo	84 (8.3)
Medio	347 (34.5)
Alto	576 (57.2)

Teniendo en cuenta los objetivos de este estudio, la edad del individuo constituye la principal variable predictiva, categorizada de manera que divide a los encuestados en tres grupos etarios: de 18 a 34 años, de 35 a 54 años y de 55 años en adelante. Teniendo en cuenta esta agrupación, se presentan los resultados descriptivos en la Tabla 18, relacionados con las variables de frecuencia de uso de Internet, compras en línea y concienciación sobre fraudes.

Tabla 18*. Estadísticos descriptivos uso de internet*

Variable	**18-34 años (*N,%*)**	**35-54 años (*N, %*)**	**55 años o + (*N,%*)**
Frecuencia uso de internet			
Cada día o casi cada día	193 (82.8)	322 (81.7)	164 (42.8)
Al menos una vez a la semana	33 (14.2)	45 (11.4)	64 (16.7)

Al menos una vez al mes	3 (1.2)	13 (3.3)	56 (14.6)
Menos de una vez al mes	2 (.9)	2 (.5)	28 (7.3)
Casi nunca	2 (.9)	7 (1.8)	35 (9.1)
Nunca	0	5 (1.3)	36 (9.4)
Compra online			
Al menos una vez a la semana	44 (18.9)	67 (17.0)	13 (3.4)
Al menos una vez al mes	108 (46.4)	163 (41.4)	86 (22.5)
Menos de una vez al mes	60 (25.8)	105 (26.6)	94 (24.5)
Casi nunca	19 (8.2)	35 (8.9	101 (26.4)
Nunca	2 (.9)	24 (6.1)	89 (23.2)
Concienciación sobre fraude			
Si	133 (57.1)	233 (56.6)	213 (55.6)
No	98 (42.1)	163 (41.4)	160 (41.8)
No lo recuerda/No sabe	2 (.8)	8 (2.0)	10 (2.6)

Los datos muestran que los jóvenes de 18 a 34 años y los adultos de 35 a 54 años realizan un uso mayor de Internet, con más del 80% de ellos utilizando Internet diariamente. En contraste, solo el 42.8% de los adultos mayores de 55 años utilizan Internet con la misma frecuencia. A medida que la frecuencia de las compras online disminuye, observamos un incremento en la proporción de adultos mayores que casi nunca o nunca compran en línea, alcanzando el 26.4% y el 23.2% respectivamente. En cuanto a la conciencia sobre el fraude parece ser relativamente uniforme entre los distintos grupos de edad, con más del 55% de los encuestados en cada grupo indicando estar al tanto de las campañas informativas sobre fraude.

En la tabla 19 se presentan los estadísticos descriptivos referidos a las diferentes conductas realizadas de forma online, mostrando los resultados una clara variación en las conductas online de seguridad entre diferentes grupos de edad. Por ejemplo, más del 65% de los jóvenes y adultos de mediana edad evitan enlaces desconocidos, lo que sólo hace el 59% de las

personas mayores de 55 años. En cuanto a la instalación de software antivirus o anti-spam, un 30.3% de los adultos mayores nunca lo instalan.

Tabla 19*. Conductas realizadas online*

Variable	**18-34 años (*N,%*)**	**35-54 años (*N, %*)**	**55 años o + (*N,%*)**
Evitar enlaces desconocidos			
Siempre	155 (66.5)	271 (68.8)	226 (59.0)
A veces	61 (26.2)	84 (21.3)	64 (16.7)
Nunca	17 (7.3)	38 (9.6)	85 (22.2)
No aplicable			8 (2.1)
Instalar anti-virus o anti-spam			
Siempre	103 (44.2)	222 (56.3)	184 (48.0)
A veces	83 (35.6)	68 (17.3)	65 (17.0)
Nunca	46 (19.7)	100 (25.4)	116 (30.3)
No aplicable	1 (.4)		18 (4.7)
Compras online sólo con tarjeta			
Siempre	74 (31.8)	216 (54.8)	145 (37.9)
A veces	120 (51.5)	116 (29.4)	111 (37.9)
Nunca	39 (16.7)	57 (14.5)	115 (30.0)
No aplicable		5 (1.3)	12 (3.1)

En cuanto a la prevalencia de victimización, dentro del grupo de edad 18-34 años experimentaron algún tipo de delito económico el 50.2% de los participantes (N=117), siendo la mayoría de estos distribuidos por un medio electrónico (94%). En cuanto a las categorías delictivas, dentro de este grupo 41 participantes (17.6% de la muestra de este grupo etario) fueron víctimas de fraude relacionado con compras, 36 participantes (15.5%) fueron víctimas de robo de identidad y 40 participantes (17.2%) víctimas de fraude económico.

En el grupo de edad 35-54 años experimentaron algún tipo de delito económico el 67.3% (N=265), siendo también mayoritarios los distribuidos por medios electrónicos (89.4%). Dentro de este grupo etario 91 participantes (23.1% de la muestra del grupo) fueron víctimas de fraude relacionado con las compras, 91 (23.1%) robo de identidad y 83 (21.1%) sufrieron fraude económico.

Por último, el 48% del grupo de personas de 55 o más informó haber sido objetivo de alguno de los delitos evaluados (N=184), siendo también la mayoría de estos delitos distribuidos de forma electrónica (71.2%). Referido a las categorías delictivas, 54 (14.1% de la muestra de este grupo etario) fueron víctimas de fraude relacionado con compras, 62 (16.2%) sufrieron robo de identidad y 68 participantes (17.8%) experimentaron fraude económico.

A continuación, se presentan en la tabla 20 los estadísticos descriptivos de haber sido objetivo de los distintos tipos de delito económico evaluados. Es importante señalar en este apartado que los porcentajes que se presentan en las vías utilizadas para la distribución del delito están referidos al total de las personas que confirmaron haber sido objetivo de uno de los delitos evaluados (N=117 para el grupo entre 18 y 34 años; N=265 para el grupo entre 35 y 54 años; y N=184 para el grupo de 55 años o más). Así mismo, en este desglose de las tres tipologías delictivas cada participante podía haber sido objetivo de más de uno de estos delitos.

Tabla 20*. Delitos económicos y su notificación*

Variable	**18-34 años (*N,%*)**	**35-54 años (*N, %*)**	**55 años o + (*N,%*)**
Estafa de compra			
Productos gratuitos = suscripción	32 (13.7)	77 (19.5)	41 (10.7)
Productos que no se reciben	29 (12.4)	56 (14.2)	21 (5.5)
Factura falsa	13 (5.6)	44 (11.2)	23 (6.0)
Robo de identidad			
Solicitando datos	34 (14.6)	97 (24.6)	68 (17.8)

Solicitando un pago (para solucionar un problema)	45 (19.3)	106 (26.9)	47 (12.3)
Fraude económico			
Ganancia-reembolso	21 (9.0)	73 (18.5)	60 (15.7)
Entradas fraudulentas	12 (5.2)	5 (1.3)	3 (.8)
Solicitud pago-amenazas	15 (6.4)	46 (11.7)	18 (4.7)
Pago para reclamar premio	54 (23.2)	136 (34.5)	95 (24.8)
Vía de transmisión del delito			
Correo electrónico	46 (39.3)	120 (45.3)	70 (38.0)
SMS	9 (7.7)	10 (3.8)	11 (6.0)
Llamada móvil	8 (6.8)	41 (15.5)	27 (14.7)
WhatsApps u otros	2 (1.7)	7 (2.6)	3 (1.6)
Anuncio redes sociales	19 (16.2)	26 (9.8)	9 (4.9)
Anuncio web	26 (22.2)	33 (12.5)	11 (6.0)
Método offline	7 (6.1)	28 (10.5)	53 (28.9)
No especificado	1 (.9)	6 (2.3)	6 (3.3)

En cuanto a la notificación y/o denuncia de estos delitos la mayoría de los participantes informaron no decírselo a nadie (con porcentajes por encima del 40% en todos los grupos etarios) o comentarlo sólo con amigos y/o familiares. Entre las personas que habían sido objetivo de uno de los delitos evaluados los canales más comunes de notificación y denuncia fueron la policía o la entidad bancaria, pero sólo un 9.4% (grupo 18-34 años), 18.5% (grupo 35-54 años) y un 7.1% (grupo 55 o más años) informaron o denunciaron a través de estos canales. Debido al interés de nuestro estudio se incluirán a partir de este momento sólo la victimización sufrida por métodos electrónicos (cibervictimización)

Referido a las opciones que los participantes consideraban más adecuadas para informar o denunciar de los diferentes delitos económicos, se muestra la distribución de los datos en la Tabla 21. Estos datos reflejan como

opciones preferentes el uso de un teléfono gratuito o una página web gubernamental. Además, se observa una mayor disposición por parte de las personas de 55 años a utilizar medios físicos, como la asistencia en una ubicación presencial.

Tabla 21*. Preferencia métodos de denuncia/notificación*

Variable	**18-34 años (*N,%*)**	**35-54 años (*N, %*)**	**55 años o + (*N,%*)**
Página web gubernamental	70 (30.0)	123 (21.2)	76 (19.8)
Página web no gubernamental	27 (11.6)	42 (10.7)	23 (6.0)
Teléfono gratuito gubernamental	73 (31.3)	135 (34.3)	179 (46.7)
Teléfono gratuito no gubernamental	21 (9.0)	23 (5.8)	43 (11.2)
Emplazamiento físico	18 (7.7)	38 (9.6)	54 (14.1)
Email	24 (10.3)	33 (8.4)	8 (2.1)

En cuanto a las motivaciones para no informar o denunciar el delito, el desconocimiento acerca de a quién hacerlo fue un factor significativo, especialmente en los extremos del espectro etario; un 22,4% de los jóvenes entre 18 y 34 años y un 21,4% de los mayores de 55 años indicaron esta razón, mientras que solo un 8.4% de los individuos entre 35 y 54 años lo mencionaron este factor. La percepción de ineficacia del sistema de justicia también es prominente, con más del 27,8% en cada grupo de edad creyendo que notificar/denunciar el delito no supondría ninguna diferencia. Los factores emocionales, en este caso la vergüenza, es más predominante entre el grupo de 55 años o más (12,5%), y se establece alrededor del 6% en los otros dos grupos etarios.

En contraste, entre los motivos para denunciar/notificar el intento de prevenir futuros delitos para sí mismos o para otros fue la razón más predominante en todos los grupos de edad (entre el 46 y el 54%). Además, la experiencia de daños financieros o emocionales significativos también se

destacó como una razón importante para denunciar. En el grupo más joven, el 23,1% de las personas indicó haber sufrido tales daños, cifra que también es notable en el grupo de 35 a 54 años con un 18,5%. En el grupo de 55 años o más, tanto los daños significativos como la creencia en la eficacia de la denuncia, fueron elegidos por el 19,2% de los encuestados.

Para finalizar esta sección, relacionada con los análisis descriptivos, se presentan tanto las consecuencias económicas como emocionales y físicas relacionadas con la victimización (Tabla 22).

Tabla 22*. Consecuencias de la cibervictimización*

Variable	**18-34 años (*N,%*)**	**35-54 años (*N, %*)**	**55 años o + (*N,%*)**
Consecuencias financieras			
0€	69 (62.7)	166 (70.1)	97 (74.0)
Menos de 50€	19 (17.3)	29 (12.2)	20 (15.3)
Más de 50€ y menos de 500€	20 (18.2)	33 (13.9)	11 (8.4)
Más de 500€ y menos de 2000€	2 (1.8)	7 (3.0)	2 (1.5)
Más de 2000€	0 (0.0)	2 (.8)	1 (.8)
Consecuencias emocionales y físicas			
Enfado	72 (65.5)	161 (67.9)	86 (65.6)
Irritación	67 (60.9)	146 (61.6)	68(51.9)
Verguenza	22 (20.0)	50 (21.1)	27 (20.6)
Estrés	31 (28.2)	81 (34.2)	29 (22.1)
Efectos negativos en salud física	3 (2.7)	19 (8.0)	10 (7.6)

La mayoría de los consumidores en la muestra analizada (69.46%) que experimentaron algún tipo de delito económico no informaron pérdidas financieras resultantes del incidente. Adicionalmente, entre aquellos que sí enfrentaron un impacto económico, la mayor parte sufrió pérdidas menores a 500 euros, y solo el 2.93% de las víctimas registraron pérdidas superiores a 500 euros. Sin embargo, en relación con las consecuencias no financieras del delito, se observan prevalencias mayores en todos los grupos de edad.

La mayoría de las víctimas informó sentir enfado (66,74%) o irritación (58,79%). En cuanto a las consecuencias físicas en la salud física, sólo el 2.7% de los jóvenes lo experimentaron, mientras que el grupo de más edad lo sufrió un 7.6%.

8.4.2 Pruebas chi-cuadrado referido a las consecuencias de la cibervictimización

Se llevaron a cabo análisis de chi-cuadrado para detectar posibles relaciones entre los grupos de edad y las consecuencias financieras, emocionales y físicas de la cibervictimización. Los resultados indican que no hay una relación significativa entre el grupo de edad y las consecuencias financieras, ya que el valor del chi-cuadrado de Pearson fue 12.553 con un p-valor de 0.250. Esto sugiere que las diferencias observadas en las consecuencias financieras entre los diferentes grupos de edad no son estadísticamente significativas.

En cuanto a las consecuencias emocionales, los análisis no mostraron relaciones significativas entre los grupos de edad y los sentimientos de enfado ($\chi^2(2) = 0.304$, $p = .859$), irritación ($\chi^2(2) = 3.539$, $p = .170$), y vergüenza ($\chi^2(2) = 0.056$, $p = .972$). Sin embargo, el análisis del sentimiento de estrés debido a la victimización mostró una relación marginalmente significativa con el grupo de edad ($\chi^2(2) = 6.000$, $p = .050$). Esto implica que las diferencias en los niveles de estrés entre los grupos de edad están en el límite de ser estadísticamente significativas, lo que sugiere que podría haber una tendencia a que ciertos grupos de edad experimenten más estrés que otros.

Por último, las consecuencias en la salud física debido a la victimización tampoco mostraron una asociación significativa con el grupo de edad ($\chi^2(2) = 3.620$, $p = .164$), indicando que las diferencias observadas en las consecuencias en la salud física entre los diferentes grupos de edad no son estadísticamente significativas. Estos resultados indican que, en general, las consecuencias financieras y emocionales de la victimización no difieren

significativamente entre los grupos de edad, con la posible excepción del estrés.

8.4.3 Regresión logística

El objetivo principal de este análisis fue determinar si la probabilidad de victimización en delitos cibernéticos variaría entre diferentes grupos de edad si todos utilizaran internet con la misma frecuencia. Para ello, primero se calculó un modelo de propensión para predecir el uso frecuente de internet. Utilizamos una regresión logística con las variables edad, género y nivel educativo para predecir la probabilidad de uso frecuente de internet (definido como usar internet al una vez a la semana). Posteriormente, simulamos un escenario donde todos los individuos tienen la misma probabilidad de uso frecuente de internet que el grupo de jóvenes (18-34 años). Calculamos la probabilidad media de uso frecuente de internet para este grupo y asignamos esta probabilidad a todos los individuos del estudio. Luego, generamos una variable simulada de uso de internet basada en esta probabilidad constante. Con esta variable simulada, ajustamos un modelo de regresión logística para evaluar la probabilidad de cibervictimización, incluyendo las variables de edad, género, nivel educativo y la interacción entre edad y uso simulado de internet.

Los resultados mostraron que ninguna de las variables consideradas tuvo un efecto estadísticamente significativo en la probabilidad de victimización. Específicamente, los grupos de edad 35-54 años (B = 15.65, SE = 441.35, z = 0.04, p = .97) y 55+ años (B = 2.20, SE = 1.63, z = 1.34, p = .18) no mostraron diferencias significativas en comparación con el grupo de referencia (18-34 años). Además, no se encontraron diferencias significativas en la probabilidad de victimización en función del género (B = -0.04, SE = 0.13, z = -0.27, p = .79) ni del nivel educativo.

Los resultados indican que, manteniendo constante el uso de internet entre los diferentes grupos de edad, no existen diferencias en la

cibervictimización. Este resultado es relevante, ya que los resultados descriptivos apuntaban a una menor prevalencia en el grupo de más de 55 años.

Puesto que estos resultados indican que hay otras variables relacionadas con la cibervictimización económica se llevó a cabo una regresión logística binaria para evaluar la relación entre diversas conductas de seguridad online y la probabilidad de ser víctima de los delitos económicos evaluados. Las variables incluidas en el modelo fueron: evitar hacer clic en enlaces desconocidos, instalar software anti-virus o anti-spam, y realizar compras online únicamente con tarjeta de crédito. Los resultados muestran que evitar hacer clic en enlaces desconocidos no tiene un efecto significativo en la probabilidad de ser víctima de ciberdelitos ($B = -0.113$, $p = 0.234$). Sin embargo, la instalación de software anti-virus o anti-spam se asocia significativamente con una reducción en la probabilidad de ser víctima de ciberdelitos económicos ($B = -0.296$, $p < 0.001$), indicando que aquellos que instalan software de seguridad tienen un 25.6% menos de probabilidad sufrir este tipo de victimización ($Exp(B) = 0.744$). Asimismo, realizar compras online únicamente con tarjeta de crédito también se asocia significativamente con una reducción en la probabilidad de ser víctima ($B = -0.451$, $p < 0.001$). Los individuos que utilizan esta medida de seguridad tienen un 36.3% menos de probabilidad de ser víctimas de ciberdelitos ($Exp(B) = 0.637$).

8.5 DISCUSIÓN Y CONCLUSIONES

El presente estudio tuvo como objetivo principal analizar la prevalencia de los delitos económicos online en personas adultas mayores en comparación con otros grupos de edad, así como la notificación de estos delitos y el impacto financiero y emocional resultante.

En cuanto al uso de Internet, solo el 42.8% de las personas mayores de 55 años de nuestra muestra hacía uso de internet de forma frecuente (a diario o casi a diario),

en comparación con más del 80% en los grupos más jóvenes. Este resultado es consistente con investigaciones previas que han señalado una significativa brecha digital entre las generaciones, tal como se ha mencionado previamente en este trabajo. Adicionalmente, se debe tener en cuenta que los datos de este estudio se recogieron durante el año 2019, por lo que todavía no se había incrementado la digitalización en este grupo etario como consecuencia de la pandemia por COVID-19. Actualmente, las personas mayores de 55 años que hacen uso de internet de forma frecuente en España representan un porcentaje más alto, alrededor del 81,1% (INE, 2023). Sin embargo, seguimos observando una brecha en el acceso a la tecnología, si observamos los datos de acceso en otros grupos de edad, por encima del 90%. Esta disparidad puede atribuirse a múltiples factores, incluidos la alfabetización digital limitada, percepciones sobre la utilidad de la tecnología y barreras económicas (Berkowsky et al., 2018). Así mismo, la menor actividad en el entorno digital puede reducir la exposición a fraudes en línea, pero no necesariamente les protege contra fraudes diseñados específicamente para explotar su falta de experiencia digital (Pratt et al., 2010; Reising & Holtfreter).

En cuanto a la prevalencia en los distintos tipos de delitos económicos evaluados, los más prevalentes en este grupo fueron los fraudes económicos, específicamente las solicitudes de pago para reclamar premios inexistentes, afectando al 24.8% de los participantes mayores de 55 años. La detección de una mayor prevalencia en tipologías específicas de fraude presenta una importancia capital para el diseño de campañas de sensibilización y prevención destinadas a la población adulta mayor ya que las instituciones encargadas de implementar programas de protección para este segmento demográfico deben mantenerse informadas sobre las amenazas más prevalentes y pertinentes que confrontan estas personas. Además, es imperativo que dichas entidades adopten una postura proactiva en la monitorización de la evolución de estas amenazas a lo largo del tiempo, ajustando sus estrategias de intervención conforme a los cambios detectados en el panorama delictivo. Aunque la mayoría de estos delitos económicos ser realizaron de forma digital, en este grupo demográfico se encontró la mayor prevalencia de delitos económicos realizados mediante medios tradicionales (28.9%), en comparación con el 10.5% en el grupo de 35 a 54 años y el 6.1% en el grupo de 18 a 34 años. Este resultado es coherente con la teoría de los estilos de vida (Hindelang et al., 1978), la cual

defiende que la exposición a delitos está influenciada por las rutinas diarias y los estilos de vida de los individuos. En el caso concreto de las personas adultas mayores, su estilo de vida y rutinas pueden contribuir significativamente a su vulnerabilidad frente a delitos económicos realizados de forma tradicional. Por ejemplo, es más probable que realicen transacciones financieras en persona en lugar de utilizar servicios en línea. Esta preferencia por las interacciones cara a cara incrementa las oportunidades para los delincuentes que buscan perpetrar fraudes económicos, ya que los adultos mayores se encuentran en situaciones donde el contacto directo con potenciales estafadores es más frecuente.

En cuanto a las preferencias en los medios de notificación/denuncia, entre los adultos mayores se centran en métodos más tradicionales, como una llamada telefónica a un número gubernamental o la visita a una ubicación física. Por tanto, para garantizar la difusión efectiva de la información relacionada con la notificación o prevención de los ciberdelitos, es fundamental que los programas de prevención empleen una multiplicidad de canales de comunicación para alcanzar a todos los segmentos dentro del grupo demográfico de 65 años o más. Esta estrategia multicanal debe incluir medios tradicionales, como folletos impresos y charlas presenciales, así como plataformas digitales, como correos electrónicos y redes sociales, para asegurar que la información crítica sobre prevención de fraudes llegue de manera efectiva y comprehensiva a su audiencia objetivo (Mears et al., 2016).

Un dato preocupante es que solo el 7.1% de las personas mayores de 55 años que fueron víctimas de un ciberdelito económico acudieron a la policía, en comparación con el 9.4% en el grupo de jóvenes y el 18.5% en el grupo de edad media. Este bajo nivel de notificación puede explicarse por varios factores, que indicaron los participantes como principal motivo para no realizar la notificación o denuncia. Entre los mayores de 55 años, el motivo más citado fue la percepción de que no habría una diferencia, mencionado por el 24.1%, reflejando un escepticismo sobre la efectividad de la denuncia y su posible impacto (Cross, 2016). Otro motivo prevalente fue la falta de daño financiero o emocional significativo (21.4%) y la falta de conocimiento sobre el procedimiento (21.4%). Encontramos en este grupo etario una mayor prevalencia de sentirse avergonzado

como motivo de no hablarle a nadie (ni notificar) el ciberdelito, representando el motivo principal para el 12.5% de los mayores de 55 años (y situándose en otros grupos de edad esta prevalencia alrededor del 6%). Estudios previos han investigado cómo las personas mayores, incluidas aquellas que han sido víctimas de fraude, tienden a utilizar etiquetas como codiciosos, crédulos o ingenuos, lo que refleja una atribución de un cierto grado de responsabilidad a las propias víctimas por su victimización, sugiriendo una percepción interna de culpabilidad o de deficiencia en el juicio crítico que contribuye a su susceptibilidad frente a estos engaños (Cross, 2015; Segal et al., 2021).

Referido a la probabilidad de cibervictimización, los análisis revelaron que, al controlar la variable de uso de Internet, todos los grupos de edad mostraron una probabilidad similar de ser victimizados. Esto sugiere que la exposición a riesgos cibernéticos está más relacionada con las conductas específicas en línea que con la edad per se. Inicialmente, los análisis descriptivos parecían indicar que los adultos mayores tenían una menor probabilidad de ser víctimas, probablemente debido a su menor uso de Internet. Sin embargo, este efecto desaparece al considerar cómo utilizan la tecnología. En consonancia con la teoría de las actividades rutinarias de Cohen y Felson (1979), se identificó que las conductas preventivas en Internet son cruciales para reducir la victimización. Los resultados mostraron que aquellos que instalan software de seguridad tienen un 25.6% menos de probabilidad de sufrir ciberdelitos económicos y realizar compras online únicamente con tarjeta de crédito se asocia significativamente con una reducción en la probabilidad de ser víctima, presentando un 36.3% menos de probabilidad de ser victimizados. Esto sugiere que establecer "guardianes efectivos", como medidas de seguridad cibernética, puede ser altamente efectivo en la prevención de estos delitos.

En cuanto a las consecuencias físicas y emocionales de ser víctima de un ciberdelito económico, los resultados mostraron que estas fueron similares entre todos los grupos de edad, sin diferencias significativas. Este hallazgo subraya que el impacto psicológico de la victimización por fraudes financieros es uniformemente severo, independientemente de la edad. Investigaciones previas han documentado que la victimización por fraudes puede conducir a estrés significativo, ansiedad y una sensación de vulnerabilidad que afecta

profundamente la calidad de vida (Cross, 2015). Este efecto homogéneo indica la necesidad de proporcionar apoyo psicológico y recursos de recuperación a todas las víctimas de fraudes financieros, sin importar su edad, aunque sería beneficioso que estas intervenciones se encontraran adaptadas a las características de la muestra a la que van dirigidas.

A pesar de los hallazgos, que suponen un aporte para la comprensión de la relación entre las herramientas digitales y las personas adultas mayores, este estudio presenta varias limitaciones que deben ser consideradas al interpretar los resultados. En primer lugar, los datos utilizados corresponden al año 2019, un periodo previo a la acelerada digitalización impulsada por la pandemia de COVID-19, lo que podría implicar que los patrones de uso de Internet y la prevalencia de ciberdelitos entre los adultos mayores hayan sufrido transformaciones significativas desde entonces. Además, la naturaleza transversal del estudio limita la capacidad para establecer relaciones causales entre las variables analizadas. Es imperativo realizar estudios longitudinales que permitan un seguimiento a lo largo del tiempo para entender mejor las dinámicas cambiantes de la victimización cibernética en este grupo etario. Asimismo, aunque se ha abordado una gama de factores relevantes, es necesario evaluar un espectro más amplio de variables potencialmente asociadas con la vulnerabilidad a los delitos económicos, tales como la competencia digital, la percepción de riesgo y las redes de apoyo social. La inclusión de estas variables en futuras investigaciones proporcionaría una comprensión más holística y matizada del fenómeno en estudio. Adicionalmente, la muestra utilizada en este estudio, aunque representativa, se limita a la población de España, lo cual restringe la generalización de los resultados a otros contextos geográficos y culturales. Es crucial llevar a cabo investigaciones comparativas en diferentes países para identificar posibles variaciones en los patrones de victimización y desarrollar estrategias de prevención adaptadas a diversas realidades sociodemográficas.

GENERAL CONCLUSIONS

The overarching aim of this doctoral thesis lies in the analysis and understanding of the relationship between the older adult population and ICTs. The ultimate goal was to identify relevant areas and dimensions within this age group for assessment and intervention in the digital realm. To achieve this general objective, throughout PART I, the underlying theoretical foundations were established and the current state of research in this field was analysed. CHAPTER 1 provided a contemporary view of older adults, as well as the benefits and challenges they may face in a highly digitalised society, including the digital divide and cyber-victimisation. Throughout CHAPTER 2, cybercrime was described, along with the issue of dark figures in these types of crimes and the importance of considering both online security and the potential fear of cyber-victimisation in this age group. The theoretical basis underpinning this doctoral thesis focuses on environmental theories and is presented throughout CHAPTER 3. Considering the aspects presented in the previous three chapters, CHAPTER 4 introduces various prevention and intervention strategies that should be considered for this age group to promote effective and safe digital inclusion. These chapters establish the theoretical basis for the empirical study conducted and presented in PART II. Based on the literature reviewed, CHAPTERS 5, 6, 7, and 8 aim to elucidate the areas of interest identified in this work through a mixed methodology, applying both quantitative and qualitative analyses. In these general conclusions, the findings obtained through empirical research will be grouped and discussed, based on the specific objectives underlying this work.

SPECIFIC OBJECTIVE 1: Analyse the psychosocial characteristics and coping strategies in the face of a highly digitalised society among older adults who are ICT users, as well as the type of use and time dedicated to these tools.

Throughout the various empirical studies conducted, we have observed that the majority of older adults using ICT predominantly engage in activities related to socialization, information gathering, email communication, and, to a lesser extent,

banking transactions. Moreover, their self-assessment of technological competence is moderate, and those with higher perceived technological competence also showed greater resilience, being the most frequent internet users, whereas those with lower perceived competence tended to exhibit greater experiential avoidance. These findings are aligned with Bandura's (1997) self-efficacy theory, which suggests that individuals with high levels of perceived self-efficacy tend to exhibit greater resilience, effectively managing stressors and proactively adapting to changes, including increased digitalization.

Consequently, in line with findings from recent studies conducted during the COVID-19 pandemic (Czeisler et al., 2020; García-Portilla et al., 2021; Kobayashi et al., 2021), our study categorizes older individuals as the most resilient and adequately adapted age group compared to others. However, it is necessary to highlight an inherent bias in these data, derived from the fact that they represent exclusively those older adults who are active ICT users, as data collection was carried out through online questionnaires. This method inevitably excludes a considerable segment of this demographic that does not interact with such technological tools, potentially leading to a partial and possibly erroneous interpretation of the overall adaptive capacity of the older population in adverse contexts.

These results highlight the need to formulate public policies and social intervention strategies that transcend mere provision of access to ICT. It is essential that such strategies are committed to promoting digital competencies among older individuals, paying special attention to their idiosyncratic psychosocial characteristics and including the heterogeneity of this entire age group. The recent COVID-19 pandemic has served as an unexpected catalyst, clearly demonstrating the crucial importance of digital competence, especially for older adults, due to the variability in adaptability that characterizes their interaction with ICT. Therefore, it would be advisable for the implemented policies not to be limited to closing the digital divide in terms of access and usage, but to focus on in-depth and personalized training that fosters self-efficacy and resilience in the digital context. Adopting a holistic and multidisciplinary perspective is essential to ensure that the integration of ICT in the lives of older adults is not only

effective but also empowering, allowing them an active social participation in our increasingly digitalized society.

SPECIFIC OBJECTIVE 2: Detect the differences between older adults who integrate technology into their daily activities and those who do not, focusing on the emotional and social consequences and the possible presence of functional and dysfunctional fear within this group.

Regarding the heterogeneity among older adults in relation to ICT, significant differences emerge between users of these technologies and those who, whether by choice or circumstance, remain on the sidelines. This study has identified significant discrepancies, which find theoretical grounding in the UTAUT model (Venkatesh et al., 2003), which posits that ICT adoption is intrinsically linked to performance and effort expectations, social influence, and facilitating conditions, as previously analyzed in this work.

ICT users generally express a positive perception of these tools, valuing the ability to establish and maintain social relationships effectively, as well as access to educational resources and other digital media that would otherwise be out of their reach. Moreover, incorporating these technologies provides increased autonomy, furnishing this age group with the necessary tools to manage their daily needs independently through online transactions and health information access, which not only enhances their self-efficacy but also their social and emotional integration (Wu & Sheng, 2019; Lozoya et al., 2022). It is also essential to consider that intensifying communication and active participation in online communities not only contributes to reducing social isolation but also acts as catalysts for cognitive stimulation, which can slow cognitive decline. This enables older adults to maintain an optimal state longer in their emotional, cognitive, and physical health (Morikawa et al., 2023). Undoubtedly, these digital tools serve as bridges that span the gap of physical distance, facilitating the maintenance or creation of new emotional bonds for individuals in this age group, which can mitigate the feeling of isolation and foster a sense of belonging and essential social connection for their

effective integration and participation in society (Berkley et al., 2023). This aligns with the principles of Active Ageing proposed by the World Health Organization in 2002, particularly the fundamental pillar of "Participation," which underscores the critical importance of keeping older adults integrated and active within their communities.

However, it is necessary to recognize that equating the provision of online services with greater accessibility represents an oversimplification that ignores the complexities inherent in user diversity (Randall and Berlina, 2019), as observed in the non-users of these tools. Within this group, we find that non-users face significant barriers that limit their capacity to interact with essential services and isolate them from the modern digital society, exacerbating pre-existing inequalities and reducing their participation in an increasingly digitalized society (Olson & Viscovi, 2023). This situation not only compromises their dignity but can also increase their vulnerability, particularly when the inaccessibility of these systems forces them to rely on others for basic services, such as those related to health, thus increasing their perception of vulnerability (Raja et al., 2023). Additionally, non-users reported experiencing emotions from the negative spectrum, such as anxiety, insecurity, stress, and a palpable sense of obligation. This range of negative emotions is particularly relevant since, under certain circumstances, these individuals are forced to interact with digital tools, which can generate negative consequences for this group. Negative emotions, such as sadness and anxiety, have consistently been linked to significant adverse effects on health and general well-being. Furthermore, these emotions are associated with an increased risk of developing chronic diseases, as well as with a deterioration in cognitive functioning and a decrease in life satisfaction levels. Additionally, they lead to a reduction in motivation and the propensity to participate in social activities and self-care practices, crucial elements for maintaining a healthy and active life (Carstensen et al., 2011).

Regarding security, we observe that users who feel insecure turn to acquaintances or family members for help. This support is crucial for older adults, who may require a stronger support network than other demographic groups to use these tools (Schreurs et al., 2017; Macedo, 2017). However, this could also pose a danger

in the digital context where values and norms are blurred, and could lead to those individuals, who in principle are there to help, taking advantage of the situation to commit a crime (Jaishankar, 2008). For instance, a family member or caregiver assisting an elderly person with little or no supervision might abuse their access to personal and financial information. The anonymity and lack of regulation in cyberspace facilitate these abuses, as the norms and values that typically regulate behavior in the physical world do not apply in the same way in the digital environment. This context highlights the need to implement measures for supervision and monitoring, as well as the importance of educating older adults about safe practices when delegating digital tasks. Additionally, in the case of non-users, they often did not have this support, so they preferred not to use the tool, generating a sense of social exclusion and isolation.

Finally, regarding the fear of cybercrime, we find a notable absence of functional fear in the two groups analyzed. Among ICT users, the majority did not exhibit fear of becoming victims, resulting in a lack of adequate protective measures in this digital environment, likely due to poor digital literacy in this area. It is relevant to note that according to the Protection Motivation Theory (Maddux & Rogers, 1983; Rogers, 1975), an individual's motivation to protect themselves is based both on their assessment of the threat and their perception of their ability to cope with it, which is influenced by knowledge about the necessary security measures and awareness of the potential risks present in the digital environment. On the other hand, among non-users, we identified dysfunctional fear that dissuaded them from using these technological tools. When fear of crime manifests in a dysfunctional manner, it can lead to social isolation, which in turn has potential long-term detrimental effects on individuals' mental and physical health (Gabriel and Greve, 2003). Additionally, dysfunctional fear can cause these avoidance behaviors to increase even more the emotion of fear, generating a loop (Ferraro, 1995).

SPECIFIC OBJECTIVE 3: Examine the cyber victimization experienced by older adults, including its reporting, protective behaviors, perception of vulnerability, and ICT-related training.

In the different samples analyzed, between 71.2% and 84.6% of respondents over the age of 55 indicated that they had been targeted by at least one of the types of cybercrimes examined, with economic frauds emerging as the most prevalent. Although the majority of these economic crimes were perpetrated digitally, primarily via email, it was observed that traditional methods of committing economic crimes are more prevalent in this demographic group than in others. This finding is consistent with the lifestyle theory of Hindelang et al. (1978), which postulates that exposure to crime is significantly influenced by individuals' daily routines and lifestyles, thereby contributing to their greater vulnerability to traditional economic crimes.

Despite a significant proportion having been victims of cybercrime, more than 40% of those affected chose not to report their experience to anyone, not even acquaintances or family members. This phenomenon supports the existence of a "dark figure" of unreported or unnotified crimes, which persists due to the reluctance to report these incidents (Button & Cross, 2017; Caneppele & Aebi, 2017; Maras, 2017; Wall, 2007). The tendency not to report incidents of economic cybercrimes in this age group was attributed more than in participants of other ages to shame. This emotion can be exacerbated by negative stereotypes that frame fraud victims as greedy or easily deceived, which promotes victim-blaming (Cross, 2013; 2015). Moreover, this stigmatization not only persists among the general public but is also internalized among those who have been defrauded, exacerbating the damage caused by the crime and decreasing the likelihood of incidents being reported (Cross, 2015; Cross et al., 2016). Additionally, this negative self-perception not only worsens emotional suffering but also acts as a barrier to accessing the support resources necessary for recovery.

Regarding preferences for notification and reporting methods, older individuals lean towards more traditional reporting methods, such as calls to government toll-free numbers or visits to physical locations, highlighting the need for cybercrime prevention programs to use a multiplicity of communication channels. This multi-channel strategy should span from traditional media, like printed pamphlets and in-person talks, to digital platforms, like emails and social networks, to ensure that

crucial information on the prevention and reporting of various cybercrimes is effectively and comprehensibly distributed to the entire target audience (Mears et al., 2016).

In terms of the perception of vulnerability to fraud, especially those perpetrated via email, scores were low, and no significant relationship was identified between the perception of vulnerability in different types of fraud and the use of security measures by older adults. This finding could be attributed both to limited concern about cybercrime and to the level of knowledge about the functioning of cybercrime and the implementation of security measures, a crucial aspect in the population of older adults (Cross, 2017). According to the Routine Activity Theory (Cohen and Felson, 1979), victimization occurs when three elements converge: a suitable target, a motivated offender, and the absence of a capable guardian. In this context, the limited digital skills of older adults make them suitable targets for cybercriminals since the convergence in cyberspace with potential offenders in the absence of adequate protective measures can increase their vulnerability situation.

Regarding the likelihood of becoming a victim of economic cybercrime based on age, analyses showed that, when adjusted for the variable of Internet use, all ages showed a similar probability of victimization, suggesting that cyber victimization is more related to specific online behaviors than to age itself. Following this line, the analyses showed that security behaviors reduced the probability of being a victim of cybercrime by about 30%, indicating that training in tools that allow acting as "self-guardians" is essential in a highly digitalized context (Nicholson et al., 2021).

SPECIFIC OBJECTIVE 4: Analyze the economic and emotional consequences of cyber victimization in this age group.

In our study, the majority of individuals over the age of 55 did not report significant financial losses after being targeted by economic cybercrimes; however, most did face emotional consequences. Additionally, the results did not reveal substantial differences in terms of both emotional and financial consequences based on age.

Although the financial losses resulting from cyber victimization may appear minor in numerous cases, it is crucial not to underestimate their impact, particularly when evaluated in conjunction with the emotional and psychological consequences that accompany such events. The data reveal that the psychological and emotional impact of cyber victimization is considerable, with the most common emotional responses being anger (65.6%), irritation (51.9%), embarrassment (20.6%), and stress (22.1%). These negative emotions can persist over time, significantly influencing the mental health and well-being of the affected individuals. But the impact of cyber victimization is not limited to emotional and psychological effects; it can also manifest in the physical health of victims. The study data indicate that a small but significant percentage of victims over the age of 55 (7.6%) experienced negative effects on their physical health.

These findings confirm that frauds not only manifest through economic losses but also induce a spectrum of significant physical and psychological effects (Golladay & Holtfreter, 2017), underscoring the need for implementing individualized psychological interventions that recognize and address each victimization experience specifically (Kemp & Moneva, 2020).

Additionally, in the context of cybercrimes, there is a worrying trend of victim-blaming, an attitude that is not only adopted by the social environment of those who have suffered fraud but also, unfortunately, by the victims themselves. This culture of blame not only intensifies the emotional and psychological impact experienced by defrauded individuals but can also have paralyzing effects on victims' willingness to disclose these incidents. According to Cross (2015; Cross et al., 2016), this tendency toward blame attribution acts as a considerable barrier, hindering the process of seeking and receiving necessary support after victimization. Moreover, elevated levels of stress, anxiety, and distrust in the future use of digital technologies significantly increase after being victimized. These effects can lead to a reluctance to use the Internet and other digital resources, exacerbating social isolation and reducing the quality of life, as previously discussed.

DISCUSION

Firstly, it is deemed necessary to broaden the conceptualization of what it means to be a "cyber-victim". Current research and policies predominantly focus on individuals suffering from cybercrimes. However, it is essential to recognize that digitalization has a considerably broader scope, capable of creating victims in various ways. Therefore, this process affects not only those who experience direct victimization online but also those who are excluded from the digital society as a whole. This expanded concept of "digital victim" would include people who, for various reasons, lack access to digital tools, whether due to economic, geographical, or educational limitations. It also includes those who, by personal choice or cultural reasons, opt not to use digital technologies and, as a consequence, are deprived of accessing resources available only in digital mode. Therefore, it is reasonable for future research and policies in this field to address this broader social dimension and explore its associated consequences. It is evident that digitalization, instead of being a source of exclusion, should be a means of empowerment and enrichment for all people, regardless of their age, gender, or personal circumstances. Therefore, the psychosocial impact of ICT use, as well as the negative consequences of exclusion from the digital society and its relationship with the quality of life of older adults, must be thoroughly investigated. This approach should be a priority line of research aimed at determining the psychological and social benefits of regular ICT use and the strategies that must be implemented to mitigate the negative effects that digital exclusion produces. This will promote the empowerment of older adults and contribute to the development of active, healthy, and inclusive aging.

In terms of access and availability of ICT, it is essential to assess the physical accessibility to technological devices and internet infrastructure. Many older adults face economic, geographical, and technical barriers that limit their access to ICT. Public policies in this area should focus on facilitating the acquisition of devices and technological services at affordable prices, ensuring that all individuals can benefit from the advantages of digitalization. Likewise, training and digital literacy are crucial aspects to ensure that older adults can use ICT safely. It is necessary to develop educational programs that enhance digital literacy, offering workshops

and courses adapted to different levels of knowledge and technological skills. Intergenerational collaboration can be especially useful in facilitating learning and the adoption of new technologies, promoting an exchange of knowledge and experiences between generations.

Regarding cyber victimization, it is a growing problem that affects older adults in various ways. Identifying the most common forms of cyber victimization and developing strategies for protection and prevention is essential. Older adults must have the training and tools necessary to protect themselves against fraud and online abuse. Assessing the perception of vulnerability and the effectiveness of the adopted security measures will contribute to improving prevention and security strategies in cyberspace.

FUTURE LINES OF RESEARCH

Research on the adaptation and digital victimisation of older adults has revealed various areas that require more in-depth and specific study to effectively address emerging challenges. One of the key areas for future research is the development and validation of reliable and valid questionnaires and measurement instruments that assess cyber victimisation and digital exclusion among older adults. These questionnaires should be adapted to different cultural and socio-economic contexts to ensure their relevance and accuracy, enabling comprehensive studies with high reliability and validity, which will guarantee access to precise and useful data, allowing for a more detailed assessment of risks and vulnerabilities. Additionally, it is necessary to evaluate the psychosocial impact of ICT use and the negative consequences of exclusion from the digital society. This approach should be a priority line of research aimed at determining not only the psychological and social benefits of regular ICT use but also the potential negative effects of digital exclusion, with the aim of intervening to mitigate these effects. As outlined throughout this work, promoting the empowerment of older adults and contributing to the development of active, healthy, and inclusive ageing is essential to improving the quality of life for this demographic group. In this same vein, it is necessary to develop specific intervention programmes tailored to the

characteristics of this age group, designed to address the particular needs of older adults in relation to ICT. Additionally, it is necessary to evaluate the impact of the interventions carried out to understand their long-term effectiveness, including improvements in digital literacy, reduction of cyber victimisation, and increased digital inclusion of older adults.

REFERENCIAS BIBLIOGRÁFICAS

ActionFraud (2020). C*yber experts shine light on online scams as British public flag over 160,000 suspect emails*, recuperado de: www.actionfraud.police.uk/news/cyber-experts-shine-light-on-onlinescams-as-british-public-flag-over-160000-suspect-emails

Ahmad, Rahayu & T., Ramayah. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1133

Akdemir, N. & Lawless, C.J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research*, Vol. 30 No. 6, pp. 1665-1687. https://doi.org/10.1108/INTR-10-2019-0400

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University*. Computer and information sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Aldridge, J. & Decary-Hétu, D. (2014). Not an "eBay for Drugs": The cryptomarket "Silk Road" as a paradigm shifting criminal innovation. *SSRN Electronic Journal*.

Alves, L. M., & Wilson, S. R. (2008). The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of elder abuse & neglect*, 20(1), 63–85. https://doi.org/10.1300/J084v20n01_04

American Psychological Association. (2003). Guidelines for Psychological Practice with Older Adults. Washington, DC: American Psychological Association.

Amini, S., Dehghani C., Salehi, A. & Soltani, Z. (2019). The role of experiential

avoidance and psychological capitals in predicting feeling loneliness by mediating meaning in life in the elderly. *Journal of psychologicalscience*, 18(74), 223-234.

Armitage R., & Nellums L.B. (2020). COVID-19 and the consequences of isolating the elderly, *The Lancet Public Health*, Volume 5, Issue 5, ISSN 2468-2667, https://doi.org/10.1016/S2468-2667(20)30061-X

Ayalon, L. (2018). Contemporary Perspectives on Ageism (Liat. Ayalon & Clemens. Tesch-Römer, Eds.; 1st ed. 2018.). *Springer Nature*. https://doi.org/10.1007/978-3-319-73820-8

Baca Baldomero, E. (Coord.), & Alonso Rimo, A. [et al.] (2006). *Manual de victimología.* Valencia: Tirant Lo Blanch.

Bandura A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review,* 84(2), 191–215. https://doi.org/10.1037//0033-295x.84.2.191

Bandura, A. (1997). Self-efficacy: The exercise of control. *W H Freeman/Times Books/ Henry Holt & Co*.

Barrón, A. (1996). *Apoyo social. Aspectos teóricos y aplicaciones.* Madrid: Siglo XXI

Barrón, A. & Sánchez, E. (2001) Estructura social, apoyo social y salud mental. *Psicothema*, ISSN 0214-9915, Vol. 13, Nº. 1, pags. 17-23.

Birren, J. E. (1961). A brief history of the psychology of aging. Vol I / 2. *The Gerontologist*, 1, 69-77.

Berkley, P., Najmeh, K., Caitlin, R., Murphy, K., Sawchuk., N., Beers, P., Karen, Z., H., Li., & Shannon, H. (2023). The association between information and communication technologies, loneliness and social connectedness: A

scoping review. *Frontiers in Psychology,* 14. https://doi.org/10.3389/fpsyg.2023.1063146

Berkman, L. F., & Syme, S. L. (1979). Social networks, host resistance, and mortality: A nine-year follow-up study of Alameda County residents. *American Journal of Epidemiology,* 109(2), 186-204. https://doi.org/10.1093/oxfordjournals.aje.a112674

Berkman, L. F., Glass, T., Brissette, I., & Seeman, T. E. (2000). From social integration to health: Durkheim in the new millennium. *Social science & medicine* (1982), 51(6), 843–857. https://doi.org/10.1016/s0277-9536(00)00065-4

Berkowsky, R. W., Sharit, J., & Czaja, S. J. (2018). Factors Predicting Decisions About Technology Adoption Among Older Adults. *Innovation in aging*, 2(1), igy002. https://doi.org/10.1093/geroni/igy002

Brantingham, P.J. & Brantingham, P.L. (1984) *Patterns in Crime*. MacMillan, New York.

Brantingham, P.J. & Brantingham, P.L. (1995). Criminality of place. *Eur J Crim Policy Res* 3, 5–26. https://doi.org/10.1007/BF02242925

Bonanno, G. A., Galea, S., Bucciarelli, A., & Vlahov, D. (2007). What predicts psychological resilience after disaster? the role of demographics, resources, and life stress. *Journal of Consulting and Clinical Psychology,* 75(5), 671-682. https://doi.org/10.1037/0022-006X.75.5.671

Brands, J., & Van Doorn,J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review, *Computers in Human Behavior,*Volume 127. https://doi.org/10.1016/j.chb.2021.107082

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for

cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behavior change research and theory: Psychological and technological perspectives* (pp. 115–136). Elsevier Academic Press. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. & Díaz-Castaño, N. (2021), 'Cybercrime and Shifts in Opportunities During COVID-19: A Preliminary Analysis in the UK', *European Societies*, 23: S47–59.

Butler, R. (1980). Ageism: A foreword. *Journal of Social Issues*, 36, 8-11.

Button, C., & Cross, C. (2017). Cyber frauds, scams and their victims. Abingdon: *Routledge*.

Caneppele, S. & Aebi, M. F. (2019), 'Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes', *Policing: A Journal of Policy and Practice*, 13: 66–79. https://doi.org/10.1093/police/pax055

Carr, A. J., Gibson, B., & Robinson, P. G. (2001). Is quality of life determined by expectations or experience?. Bmj, 322(7296), 1240-1243. https://doi.org/10.1136/bmj.322.7296.1240

Carro, D., Valera, S., & Vidal, T. (2010). Perceived insecurity in the public space: Personal, social and environmental variables. *Quality and Quantity*. 44. https://doi.org/10.1007/s11135-008-9200-0

Carstensen L. L. (1992). Motivation for social contact across the life span: a theory of socioemotional selectivity. *Nebraska Symposium on Motivation*, 40, 209–254.

Carstensen, L. L., Turan, B., Scheibe, S., Ram, N., Ersner-Hershfield, H., Samanez-

Larkin, G. R., & Nesselroade, J. R. (2011). Emotional experience improves with age: Evidence based on over 10 years of experience sampling. *Psychology and Aging*, 26(1), 21-33. https://doi.org/10.1037/a0021285

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

Castro Toledo, F. J. (2019). *Sociedad tecnológica y miedo al crimen*. Edisofer.

Cerezo, A., Lopez, J. & Patel, A. (2007). International Cooperation to Fight Transnational Cybercrime. Proceedings - *2nd International Annual Workshop on Digital Forensics and Incident Analysis,* WDFIA 2007. 13-27. https://doi.org/10.1109/WDFIA.2007.4299369

Ces García, E.M. (2003). Una sociedad inclusiva para una población que envejece: el desafío del empleo y la protección social. *Revista Del Ministerio de Trabajo y Asuntos sociales*, 37(42), 209–225

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M. & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features, *Computer Science Review*, Volume 33, 69-90. https://doi.org/10.1016/j.cosrev.2019.03.002

Chawla, N. & Ostafin, B. (2007). Experiential avoidance as a functional dimensional approach to psychopathology: An empirical review. *Journal of clinical psychology*, 63(9), 871-890.

Chen, Y., & Zahedi, F.M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS* Q. 40, 1 https://doi.org/10.25300/MISQ/2016/40.1.09

Cho, M. S., & Kwon, M. Y. (2023). Factors Associated with Aging in Place among

Community-Dwelling Older Adults in Korea: Findings from a National Survey. *International journal of environmental research and public health,* 20(3), 2740. https://doi.org/10.3390/ijerph20032740

Chockalingam, K., & Srinivasan, M. (2009). Fear of Crime Victimization: A Study of University Students in India and Japan. *International Review of Victimology,* 16(1), 89–117. https://doi.org/10.1177/026975800901600105

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2, 308.

Christiansen, J., Qualter, P., Friis, K., Pedersen, S. S., Lund, R., Andersen, C. M. & Lasgaard, M. (2021). Associations of loneliness and social isolation with physical and mental health among adolescents and young adults. *Perspectives in public health*, 141(4), 226-236.

CIFAS (2020). *COVID-19 weekly threat summary*. Recuperado de www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas-COVID-19%20Weekly%20Threat%20Summary%2031_07_2020.pdf

Clarke, R. V. (1997) *Situational crime prevention: Successful case studies.* (2nd ed.). New York, NY: Harrow & Heston.

Clarke, R.V. (2004) Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research* 10, 55–63. https://doi.org/10.1023/B:CRIM.0000037557.42894.f7

Clarke, R. V. (2018). Book Review. *Journal of Criminal Justice Education*, 29(1), 157–159. https://doi.org/10.1080/10511253.2016.1258031

Clarke, R.V. & Felson M. (1993) Introduction: Criminology, routine activity and rational choice. In: R.V. Clarke and M. Felson (Eds), *Routine Activity and Rational Choice*, Vol. 5, pp. 259-294. New Brunswick: Transaction Publisher.

Clough, J. (2015). *Jurisdiction. In Principles of Cybercrime* (pp. 473–474). chapter, Cambridge: Cambridge University Press.

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

Concepción-Breton, A., Corrales-Camacho, I., Córdoba, M. E., Acosta-Hernández, M. E., Larancuent-Cueto, O. I., & De La Cruz-Morel, Y. L. (2020). Sondeo de casos en personas mayores sobre actividades cotidianas y utilización de tecnologías de la información y la comunicación (TIC) en tiempos de pandemia. *Revista Docentes* 2.0, 9(2), 132-150.

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

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Springer-Verlag.

Cross, C. (2013). Nobody's holding a gun to your head: Examining current discourses surrounding victims of online fraud. In Richards K and Tauri J (eds) *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*: 25-32. Brisbane: Queensland University of Technology.

Cross C., Richards, K. & Smith, R.G. (2016). *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support: Final Report*. Canberra: Criminology Research Grant Scheme, Australian Institute of Criminology. Available at http://crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud.

International Review of Victimology, 21 (2), 187-204. https://doi.org/10.1177/0269758015571471

Cross, C. (2016). 'They're very lonely': Understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy* 5(4): 60-75. https://doi.org/10.5204/ijcjsd.v5i4.268

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychology and aging*, 21(2), 333–352. https://doi.org/10.1037/0882-7974.21.2.333

De Grey, A. & Rae, M. (2007). *Ending Aging: The Rejuvenation Breakthroughs That Could Reverse Human Aging in Our Lifetime*

Dearden, T.E. & Parti, K. (2021). Cybercrime, Differential Association, and Self-Control: Knowledge Transmission Through Online Social Learning. *Am J Crim Just* 46, 935–955. https://doi.org/10.1007/s12103-021-09655-4

Dedel, K. (2003). *Financial Crimes Against the Elderly; Problem-Oriented Guides for Police*; Guide No.20; U.S. Department of Justice: Washington, DC, USA,

DeLiema M. (2018). Elder Fraud and Financial Exploitation: Application of Routine Activity Theory. *The Gerontologist*, 58(4), 706–718. https://doi.org/10.1093/geront/gnw258

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Financial Fraud Among Older Americans: Evidence and Implications. *The journals of gerontology. Series B*, Psychological sciences and social sciences, 75(4), 861–868. https://doi.org/10.1093/geronb/gby151

Diener, E. (1984). Subjective well-being. *Psychological Bulletin*, 95(3), 542–575.

https://doi.org/10.1037/0033-2909.95.3.542

DiMaggio, P., & Hargittai, E. (2001). *From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases.* https://doi.org/10.31235/osf.io/rhqmu

Dowler, K. (2003). Media consumption and public attitudes toward crime and justice: The relationship between fear of crime, punitive attitudes, and perceived police effectiveness. *Journal of Criminal Justice and Popular Culture*. 10. 109-126.

Doyle, J. & Walsh, L. (2015). Independent Living Applications. In: Hannah, K., Hussey, P., Kennedy, M., Ball, M. (eds) Introduction to Nursing Informatics. *Health Informatics*. Springer, London. https://doi.org/10.1007/978-1-4471-2999-8_9

Eibich, P., Krekel, C., Demuth, I., & Wagner, G. G. (2016). Associations between Neighborhood Characteristics, Well-Being and Health Vary over the Life Course. *Gerontology*, 62(3), 362–370. https://doi.org/10.1159/000438700

Ekblom, P. (2011). C*rime Prevention, Security and Community Safety Using the 5Is Framework*. Palgrave Macmillan.

Elder, G. H. (1994). Time, Human Agency, and Social Change: Perspectives on the Life Course. *Social Psychology Quarterly*, 57(1), 4–15. https://doi.org/10.2307/2786971

Ellis, T. E., & Rufino, K. A. (2016). Change in experiential avoidance is associated with reduced suicidal ideation over the course of psychiatric hospitalization. *Archives of Suicide Research*, 20(3), 426-437.

Erikson, E. H. (1959). *Identity and the Life Cycle*. New York, NY: W.W. Norton.

Estes, C. L. (2001). *Social policy & aging: A critical perspective*. SAGE Publications, Inc., https://doi.org/10.4135/9781452232676

Eurostat (2020). *Estructura demográfica y envejecimiento de la población*. Recuperado el 15 de septiembre de 2023 de https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=Archive:Estructura_demogr%C3%A1fica_y_envejecimiento_de_la_poblaci%C3%B3n&oldid=510186

Fattah, E.A. (1991). *Understanding Criminal Victimization*, Scarborough, Ont.: Prentice Hall.Canadá

Fernández, C. (2003). Estereotipos sobre la vejez y niveles de dependencia. *Geriátrika*, 19, 32-38.

Fernández-Ballesteros, R. (1992). *Mitos y realidades en torno a la vejez y la salud.* Barcelona,SG.

Fernández-Ballesteros, R. (2008). *Active aging. The contribution of psy-chology.* Gottingën: Hogrefe & Huber. Traducción española: Pirámide

Fernández, B., & Corraliza, J.A. (1996) Aspectos físicos y sociales en los lugares peligrosos. Miedo al delito en un espacio institucional. *Rev Psicol Social* 11(2), 219–234.

Ferraro, K.F. (1995). *Fear of Crime. Interpreting Victimization Risk.* Albany, NY: State University of New York Press

Ferreira-Alves, J., Magalhães, P., Viola, L. & Simoes, R. (2014). Loneliness in middle and old age: Demographics, perceived health, and social satisfaction as predictors. A*rchives of gerontology and geriatrics*, 59(3), 613-623.

Ferring, D., Balducci, C., Burholt, V., Wenger, C., Thissen, F., Weber, G., & Hallberg, I.

(2004). Life satisfaction of older people in six European countries: findings from the European study on adult well-being. *European Journal of Ageing*, 1, 15-25.

Fisher B. & Lab S. P. (2010). *Encyclopedia of victimology and crime prevention.* SAGE Publications.

Fredrickson, B. L., & Joiner, T. (2002). Positive emotions trigger upward spirals toward emotional well-being. *Psychological Science*, 13(2), 172-175. https://doi.org/10.1111/1467-9280.00431

Friemel, T.N. (2014). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, 16 (1), 176-183. https://doi.org/10.1177/1461444814538648

Foster, L., & Walker, A. (2015). Active and Successful Aging: A European Policy Perspective, *The Gerontologist*, Volume 55, Issue 1, Pages 83–90. https://doi.org/10.1093/geront/gnu028

Francisco, S. M., da Costa Ferreira, P., Veiga Simão, A. M., & Pereira, N. S. (2023). Measuring empathy online and moral disengagement in cyberbullying. *Frontiers in psychology*, *14*, 1061482. https://doi.org/10.3389/fpsyg.2023.1061482

Fuller-Iglesias, H., Sellars, B., & Antonucci, T. C. (2008). Resilience in old age: Social relations as a protective factor. *Research in Human Development*, 5(3), 181-193. https://doi.org/10.1080/15427600802274043

Gabriel, U. & Greve, W. (2003). The Psychology of Fear of Crime. Conceptual and Methodological Perspectives. *British Journal of Criminology*, 43, 600-614. https://doi.org/10.1093/bjc/43.3.600

García-Portilla, P., de la Fuente Tomás, L., Bobes-Bascarán, T., Jiménez Treviño, L.,

Zurrón Madera, P., Suárez Álvarez, M., Menéndez Miranda, I., García Álvarez, L., Sáiz Martínez, P. A., & Bobes, J. (2021). Are older adults also at higher psychological risk from COVID-19?. *Aging & mental health*, 25(7), 1297–1304. https://doi.org/10.1080/13607863.2020.1805723

Gercke, M. (2015). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* ITU.

Giwah, A. (2018). User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory. *SoutheastCon,*1-5. https://doi.org/10.1109/SECON.2018.8479178

Glick, D. M., & Orsillo, S. M. (2011). Relationships among social anx¬iety, self-focused attention, and experiential distress and avoidance. *Journal of Cognitive and Behavioral Psychotherapies*, 11(1), 1–12

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

Golz, C., Peter, K. A., Müller, T. J., Mutschler, J., Zwakhalen, S. M. G., & Hahn, S. (2021). Technostress and Digital Competence Among Health Professionals in Swiss Psychiatric Hospitals: Cross-sectional Study. JMIR mental health, 8(11), e31408. https://doi.org/10.2196/31408

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*; 21(14):4759. https://doi.org/10.3390/s21144759

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime.

Journal in computer virology, 2, 13-20.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime* . Stanford, CA: Stanford University Press.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, 10(2), 243–249. https://doi.org/10.1177/a017405

Gray, E., Jackson, J. & Farrall, S. (2011). Feelings and functions in the fear of crime: Applying a new approach to victimisation insecurity. *British Journal of Criminology,* 51(1), 75–94.

Guerette, R. T. & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology*, 47(4), 1331-1368.

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

Hämmig, O. (2019). Health risks associated with social isolation in general and in young, middle and old age. *PLoS One*, 14(7), e0219663.

Hans-Werner, W. & Gerstorf, D. (2018). A conceptual framework for studying Context Dynamics in Aging (CODA), *Developmental Review*,Volume 50, Pages 155-176, https://doi.org/10.1016/j.dr.2018.09.003

Hargittai, E. (2002). Second-Level Digital Divide: Differences in People's Online Skills. *First Monday*, 7(4). https://doi.org/10.5210/fm.v7i4.942

Harman, D. (1956). Aging: a theory based on free radical and radiation chemistry. *Journal of gerontology*, 11(3), 298–300. https://doi.org/10.1093/geronj/11.3.298

Hawkley, L. C. & Cacioppo, J. T. (2010). Loneliness matters: a theoretical and empirical review of consequences and mechanisms. *Annals of behavioral medicine : a publication of the Society of Behavioral Medicine,* 40(2), 218–227. https://doi.org/10.1007/s12160-010-9210-8

Hayes, S. C., Wilson, K. G., Gifford, E. V., Follette, V. M. & Strosahl, K. (1996). Experiential avoidance and behavioral disorders: A functional dimensional approach to diagnosis and treatment. *Journal of Consulting and Clinical Psychology*, 64(6), 1152– 1168. https://doi.org/10.1037/0022-006X.64.6.1152

Heart, T. & Kalderon, E. (2013). Older adults: are they ready to adopt health-related ICT? *International journal of medical informatics*, 82(11), e209-e231.https://doi.org/10.1016/j.ijmedinf.2011.03.002

Hindelang, M. J., Gottfredson, M. R. & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization.* Cambridge, MA: Ballinger Publishing Company.

Hinduja, S. & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*(2), 129–156. https://doi.org/10.1080/01639620701457816

Ho, H., Ko, R. & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review, *Computers & Security*, Volume 115. https://doi.org/10.1016/j.cose.2022.102611

Holt, T. J. & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. & Bossler, A. (2015). *Cybercrime in Progress: Theory and prevention of technology-enabled offenses* (1st ed.). Routledge. https://doi.org/10.4324/9781315775944

Holtfreter, K., Reisig, M. & Blomberg, T. (2006). Consumer fraud victimisation in Florida: An empirical study. *St Thomas Law Review* 18(3): 761-789.

Holt-Lunstad, J., Smith, T. B. & Layton, J. B. (2010). Social relationships and mortality risk: A meta-analytic review. *PLoS Medicine*, 7(7), e1000316. https://doi.org/10.1371/journal.pmed.1000316

Huey, L. & Ferguson, L. (2022). What Do We Know About Senior Citizens as Cybervictims? A Rapid Evidence Synthesis. *CrimRxiv.* https://doi.org/10.21428/cb6ab371.e6b80803

Hybels, C. F., Blazer, D. G., Pieper, C. F., Burchett, B. M., Hays, J. C., Fillenbaum, G. G., Kubzansky, L. D., & Berkman, L. F. (2006). Sociodemographic characteristics of the neighborhood and depressive symptoms in older adults: using multilevel modeling in geriatric psychiatry. *The American journal of geriatric psychiatry : official journal of the American Association for Geriatric Psychiatry*, 14(6), 498–506. https://doi.org/10.1097/01.JGP.0000194649.49784.29

Iftikhar S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ. *Computer science,* 10, e1772. https://doi.org/10.7717/peerj-cs.1772

Internet Crime Complaint Center (2021). *Internet Crime Report*.

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

Instituto Nacional de Estadística. (2021). *Equipamiento y uso de TIC en los hogares* Recuperado el día 15 de septiembre de 2023 de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

Jackson, J. & Gray, E. (2010). Functional fear and public insecurities about crime. *British Journal of Criminology,* 50, 1-22.

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. Internet Journal of Criminology.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. Journal of elder abuse & neglect, 26(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

Jampen, D., Gür, G., Sutter, T. & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. H*uman-centric Computing and Information Sciences*. 10. https://doi.org/10.1186/s13673-020-00237-7

Kahneman, D. & Deaton, A. (2010). High Income Improves Evaluation of Life But Not Emotional Well-Being. *Proceedings of the National Academy of Sciences of the United States of America*. https://doi.org/10.1073/pnas.1011492107

Kashdan, T. B., Barrios, V., Forsyth, J. P. & Steger, M. F (2006). Experiential avoidance as a generalized psychological vulnerability: comparisons with coping and emotion regulation strategies. *Behaviour Research and Therapy,* 44(9),1301–1320. https://doi.org/10.1016/j.brat.2005.10.003

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola,

G., Carstensen, L. L., & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and aging,* 33(2), 325–337. https://doi.org/10.1037/pag0000228

Kemp, S. (2020). *Fraud against individuals in the Internet era: trends, victimisation, impact and reporting*.

Kemp, S. & Moneva, A. (2020) Fraude online vs. offline: factores predictores de victimización y su impacto. *InDret: revista para el análisis del derecho*. 424-444.

Kemp, S., Miró-Llinares, F. & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *Eur J Crim Policy Res* 26, 293–312. https://doi.org/10.1007/s10610-020-09439-2

Kobayashi, L. C., O'Shea, B. Q., Kler, J. S., Nishimura, R., Palavicino-Maggio, C. B., Eastman, M. R., Vinson, Y. R., & Finlay, J. M. (2021). Cohort profile: the COVID-19 Coping Study, a longitudinal mixed-methods study of middle-aged and older adults' mental health and well-being during the COVID-19 pandemic in the USA. *BMJ open*, 11(2), e044965. https://doi.org/10.1136/bmjopen-2020-044965

Korniotis, G. & Kumar, A. (2011). Do Older Investors Make Better Investment Decisions?. *The Review of Economics and Statistics* 2011; 93 (1): 244–265. https://doi.org/10.1162/REST_a_00053

La Torre, G., Esposito, A., Sciarra, I., & Chiappetta, M. (2019). Definition, symptoms and risk of techno-stress: a systematic review. *International archives of occupational and environmental health*, 92(1), 13–35. https://doi.org/10.1007/s00420-018-1352-1

Lachman, M. E. (2006). Perceived Control Over Aging-Related Declines: Adaptive

Beliefs and Behaviors. *Current Directions in Psychological Science*, 15(6), 282-286. https://doi.org/10.1111/j.1467-8721.2006.00453.x

Lapidot-Lefler, N. & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. Comput. Hum. Behav., 28, 434-443.

Lawton, M. P. (1985). The Elderly in Context: Perspectives from Environmental Psychology and Gerontology. *Environment and Behavior*, 17(4), 501-519. https://doi.org/10.1177/0013916585174005

Lawton, M. P. & Brody, E. M. (1969). Assessment of older people: self-maintaining and instrumental activities of daily living. *The Gerontologist*, 9(3), 179–186.

Lee, M. & Mythen, G. (2018). *The Routledge international handbook on fear of crime*. Abingdon, UK: Routledge.

Lenstra,N. (2017).The Community-Based Information Infrastructure of Older Adult Digital Learning: A Study of Public Libraries and Senior Centers in a Medium-sized City in the USA. *Nordicom Review*,38(s1) 65-77. https://doi.org/10.1515/nor-2017-0401

Leukfeldt, E. R. & Yar, M. (2016), 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior,* 37: 263–80.

Leukfeldt, E. R., Lavorgna, A. & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of Criminal Policy and Research*, 23(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Levy, S. R. (2016). Toward Reducing Ageism: PEACE (Positive Education about Aging and Contact Experiences) Model. *The Gerontologist*, gnw116. https://doi.org/10.1093/geront/gnw116

Levy, B.R. & Banaji, M.R. (2002). Implicit ageism. T.Nelson, (ED). *Agism: stereotypes and prejudice against older person*. (pp.49-75).

Loges, W.E. & Jung, J.Y. (2001). Exploring the Digital Divide: Internet Connectedness and Age. Communication Research, 28(4), 536-562. DOI: http://dx.doi.org/10.1177/009365001028004007

Lombroso, C. (1876). L'Uomo Delinquente: *Studiato in Rapporto All'Antropologia, Alla Giurisprudenza Ed Alla Psichiatria* (2a ed.). Torino, Italia: Fratelli Bocca Editori.

Losada-Baltar, A. (2004). Edadismo: consecuencias de los estereotipos, del prejuicio y la discriminación en la atención a personas mayores. Algunas pautas para la intervención. *Informes Portal Mayores*, 14.

Losada-Baltar, A., Márquez-González, M., Jiménez-Gonzalo, L., Pedroso-Chaparro, M. D. S., Gallego-Alberto, L. & Fernandes-Pires, J. (2020). Differences in anxiety, sadness, loneliness and comorbid anxiety and sadness as a function of age and self-perceptions of aging during the lock-out period due to COVID-19]. *Revista española de geriatría y gerontología,* 55(5), 272–278. https://doi.org/10.1016/j.regg.2020.05.005

Lozoya, S.V., Guirado, M.A., Zapata González, A. & Lopez, A.B. (2022). Use of Technologies and Self-Efficacy in Older Adults. IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, 17, 125-130.

Macedo, I. M. (2017). Predicting the acceptance and use of information and communication technology by older adults: An empirical examination of the revised UTAUT2. *Computers in Human Behavior,* 75, 935–948. https://doi.org/10.1016/j.chb.2017.06.013

Machón, M., Vergara, I., Dorronsoro, M., Vrotsou, K. & Larrañaga, I. (2016). Self-

perceived health in functionally independent older people: associated factors. B*MC geriatrics*, 16, 1-9. https://doi.org/10.1186/s12877-016-0239-9

Maddux, J. E. & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Maitland, D. W. (2020). Experiential avoidance and fear of intimacy: A contextual behavioral account of loneliness and resulting psychopathology symptoms. *Journal of Contextual Behavioral Science.*

Maras, M. H. (2017). *Cybercriminology.* New York: Oxford University Press.

Martens, M.B., Wolf, R.D., & Marez, L.D. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Comput. Hum. Behav.*, 92, 139-150.

Martín-Martín, M. & Bueno-Álvarez, J. A. (2023). Social networks and aggressive attitudes: who is who. Scoping review of the scientific production on their relationships. *Frontiers in psychology*, 14, 1249907. https://doi.org/10.3389/fpsyg.2023.1249907

Martín-Rodríguez, A., Tornero-Aguilera, J. F., López-Pérez, P. J. & Clemente-Suárez, V. J. (2021). *The effect of loneliness in psychological and behavioral profile among high school students in Spain.*

Masten, A. S. (2001). Ordinary magic: Resilience processes in development. *American Psychologist*, 56(3), 227–238. https://doi.org/10.1037//0003-066x.56.3.227

Mastronuzzi, T. & Grattagliano, I. (2019). Nutrition as a health determinant in elderly patients. *Current medicinal chemistry,* 26(19), 3652-3661. https://doi.org/10.2174/0929867324666170523125806

McGuire, M. & Dowling, S. (2013). Cybercrime: A review of the evidence: Summary of key findings and implications. *Home Office Research Report* 75. London: Home Office, October.

Mears, D. P.; Reisig, M. D.; Scaggs, S. & Holtfreter, K. (2016). Efforts to Reduce Consumer Fraud Victimization Among the Elderly: The Effect of Information Access on Program Awareness and Contact. *Crime & Delinquency*, 62 (9), 1235–1259. https://doi.org/10.1177/0011128714555759

Messner, S. F. & Rosenfeld, R. (2007). *Crime and the American Dream. Wadsworth.*

Merton, R. K. (1938). "Social Structure and Anomie." *American Sociological Review,* 3(5), 672-682.

Miller, D., Rabho, L.A., Awondo, P., De Vries, M., Duque, M. & Garvey, P. (2021). *The Global Smartphone: Beyond a Youth Technology*. London: UCL Press

Ministerio de Asuntos Económicos y Transformación Digital (2022). *Uso de tecnología en los hogares españoles*. Madrid.

Ministerio de Interior (2022). *Informe sobre la cibercriminalidad en España*. Madrid

Miró-Llinares F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, Nº 13, págs. 1- 55.

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

Miró-Llinares, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica.* https://doi.org/11.10.46381/reic.v11i0.77

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 Llinares, F. & Johnson, S. D. (2018). *Cybercrime and place: Applying environmental criminology to crimes in cyberspace.*

Miró-Llinares, F. & Moneva, A. (2020). Environmental Criminology and Cybercrime: Shifting Focus from the Wine to the Bottles. In: Holt, T., Bossler, A. (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_30

Mirowsky, J. & Ross, C. (1989). *Social causes of psychological distress.* Nueva York: Aldine de Gruyter

Mitchell, A. J., Beaumont, H., Ferguson, D., Yadegarfar, M. & Stubbs, B. (2014). Risk of dementia and mild cognitive impairment in older people with subjective memory complaints: meta-analysis. *Acta psychiatrica Scandinavica,* 130(6), 439–451. https://doi.org/10.1111/acps.12336

Montorio, I., Izal, M., Sánchez, M. & Losada, A. (2002). Dependencia y autonomía funcional en la vejez. La profecía que se autocumple. *Revista multidisciplinar de Gerontología*, 2 (12), 61-68.

Montoro, J. (1988). Actitudes hacia las personas mayores y discriminación basada en la edad. *Revista multidisciplinar de Gerontología*, 8 (1), 21-30.

Morales-Vives, F., Dueñas, J. M., Vigil-Colet, A. & Camarero-Figuerola, M. (2020). Psychological variables related to adaptation to the COVID-19 lockdown in Spain. *Frontiers in Psychology*, 11, 565634.

Morikawa, M., Lee, S., Makino, K., Harada, K., Katayama, O., Tomida, K., Yamaguchi, R., Nishijima, C., Fujii, K., Misu, Y., & Shimada, H. (2023). Information and Communication Technology Use for Alleviation of Disability Onset in Socially Isolated Older Adults: A Longitudinal Cohort Study. *Gerontology,* 69(5), 641–649. https://doi.org/10.1159/000528134

Moritz, B. (2017). *Digital inequalities: differentiated internet use and social implications.* University of Zurich, Faculty of Arts.

Naciones Unidas. (2019). World Population Prospects 2019: Highlights. Recuperado https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf

Narváez Mora, M. I. (2009). *Inseguridad ciudadana subjetiva/miedo al delito: límites para la viabilidad de la transferencia de políticas de seguridad.*

Netuveli, G. & Blane, D. (2008). Quality of life in older ages. *British medical bulletin,* 85, 113–126. https://doi.org/10.1093/bmb/ldn003

Nguyen, T. T., Lee, E. E., Daly, R. E., Wu, T. C., Tang, Y., Tu, X. & Palmer, B. W. (2020). Predictors of loneliness by age decade: study of psychological and environmental factors in 2,843 community-dwelling Americans aged 20-69 years. *The Journal of clinical psychiatry,* 81(6), 15111.

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L. & McGlasson, J. (2021). Training and embedding cybersecurity guardians in older communities. In *CHI '21 : proceedings of the 2021 CHI Conference on Human Factors in*

Computing Systems: Making Waves, Combining Strengths. Article 86 Association for Computing Machinery, Inc. https://doi.org/10.1145/3411764.3445078

Nicolaisen, M. & Thorsen, K. (2016). What are friends for? Friendships and loneliness over the lifespan—from 18 to 79 years. Int J *Aging Hum Dev* 84(2):126–158. https://doi.org/10.1177/0091415016655166

Nikolopoulou, K., Gialamas, V. & Lavidas, K. (2020). Acceptance of mobile phone by university students for their studies: An investigation applying UTAUT2 model. E*ducation and Information Technologies*, 25, 4139-4155.

Nwachukwu, I., Nkire, N., Shalaby, R., Hrabok, M., Vuong, W., Gusnowski, A., Surood, S., Urichuk, L., Greenshaw, A. J., & Agyapong, V. I. O. (2020). COVID-19 Pandemic: Age-Related Differences in Measures of Stress, Anxiety and Depression in Canada. I*nternational journal of environmental research and public health,* 17(17), 6366. https://doi.org/10.3390/ijerph17176366

Oliveira, T., Thomas, M.A., Baptista, G. & Campos, F. (2013). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Comput. Hum. Behav.*, 61, 404-414.

Olphert, W. & Damodaran, L. (2013). Older people and digital disengagement: a fourth digital divide?. *Gerontology*, 59(6), 564–570. https://doi.org/10.1159/000353630

Olsson, T. & Viscovi, D. (2023). Digitalised Welfare: Access, Usage, and Outcomes Among Older Adults. *Media and Communication*, 11(3), 18-28. https://doi.org/10.17645/mac.v11i3.6694

Organización Mundial de la Salud (2002). *Envejecimiento activo: un marco político*.

Özsungur, F. (2022). A research on the effects of successful aging on the acceptance

and use of technology of the elderly. *Assistive Technology*, 34(1), 77–90. https://doi.org/10.1080/10400435.2019.1691085

Passas, N.I. (1990). Anomie and corporate deviance. *Contemporary Crises*, 14, 157-178.

Peplau, L. A. & Perlman, D. (1982). *Perspectives on loneliness. Loneliness: A sourcebook of current theory, research and therapy,* 1-18.

Perkins, R. C., Ouellet, M., Howell, C. J. & Maimon, D. (2023). The Illicit Ecosystem of Hacking: A Longitudinal Network Analysis of Website Defacement Groups. *Social Science Computer Review*, *41*(2), 390-409. https://doi.org/10.1177/08944393221097881

Phillips, K., Davidson, J.C, Farr, R.R, Burkhardt, C., Caneppele, S. & Aiken, M.P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci*, 2 , 379-398. https://doi.org/10.3390/forensicsci2020028

Pinazo, S. (2013). Envejecimiento active y solidaridad intergeneracional. *Infomació Psicològica,* 105, 4-13.

Piquero, A. R., Farrington, D. P. & Blumstein, A. (2014). The criminal career paradigm. *Crime and Justice*, 39(1), 359-506.

Pratt, Holtfreter & Reisig (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. https://doi.org/10.1177/0022427810365903

Rahimi, B. (2011). The agonistic social media: cyberspace in the formation of

dissent and consolidation of state power in postelection Iran. *The Communication Review.*2011;14(3):158–178. https://doi.org/10.1080/10714421.2011.597240

Raja, M., Kymre, I. G., Bjerkan, J., Galvin, K. T. & Uhrenfeldt, L. (2023). National digital strategies and innovative eHealth policies concerning older adults' dignity: a document analysis in three Scandinavian countries. *BMC health services research*, 23(1), 848. https://doi.org/10.1186/s12913-023-09867-w

Raman, A. & Don, Y. (2013). Preservice teachers' acceptance of learning management software: An application of the UTAUT2 model. International *Education Studies*, 6(7), 157-164.

Randall, L. & Berlina, A. (2019). *Governing the digital transition in Nordic Regions : The human element*. https://doi.org/10.30689/R2019:4.1403-2503

Repetto, T.A. (1976). Crime prevention and the displacement phenomenon. *Crime and delincuenci.* 22 , 166 - 177.

Redondo, S. & Garrido, V. (2013). *Principios de Criminología*. Valencia: Tirant lo Blanch.

Reiboldt, W. & Vogel,R. (2003) A critical analysis of telemarketing fraud in a gated Senior community. *Journal of Elder Abuse and Neglect* 13(4): 21-38. https://doi.org/10.1300/J084v13n04_02

Reisig, M. D. & Holtfreter, K. (2013). Shopping Fraud Victimization among the Elderly. *Journal of Financial Crime*, 20 (3), 324–337. https://doi.org/10.1108/JFC-03-2013-0014

Rengert, G.F. & Wasilchick, J. (1985). *The use of space in burglary. In Suburban*

Burglary: A Time and a Place for Everything (53-75). Springfield, IL: Charles C. Thomas.

Reyns, B. W., Henson, B. & Fisher, B. S. (2011), 'Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization', *Criminal Justice and Behavior*, 38: 1149–169. https://doi.org/10.1177/0093854811421448

Rodriguez Marin, J., Pastor, M. A. & LopezRoig, S. (1993). Afrontamiento, apoyo social, calidad de vida y enfermedad . *Psicothema,* 5(Sup), 349-372.

Rogers R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of psychology,* 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Roque, C., Canudo, M., Moreira, S. & Guedes, I. S. (2023). Hacking: Evolution, Conceptualization, and the Perpetrators. In N. Mateus-Coelho & M. Cruz-Cunha (Eds.), *Contemporary Challenges for Cyber Security and Data Privacy* (pp. 83-107). IGI Global. https://doi.org/10.4018/979-8-3693-1528-6.ch006

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

Rowe, J. W. & Kahn, R. L. (1987). Human aging: usual and successful. *Science* (New York, N.Y.), 237(4811), 143–149. https://doi.org/10.1126/science.3299702

Ruiz-Párraga, G. T. & López-Martínez, A. E. (2015). The role of experiential

avoidance, resilience and pain acceptance in the adjustment of chronic back pain patients who have experienced a traumatic event: a path analysis. *Annals of Behavioral Medicine*, 49(2), 247-257.

Santanello, A. W. & Gardner, F. L. (2007). The role of experiential avoidance in the relationship between maladaptive perfectionism and worry. *Cognitive Therapy and Research*, 30(3), 319–332. https://doi.org/10. 1007/s10608-006-9000-6

Savona, E. U., & Mignone, M. (2004). The fox and the hunters: how IC technologies change the crime race. *European Journal on Criminal Policy and Research,* 10(3), 3–26. https://doi.org/10.1023/B:CRIM.0000037562.42520.d7

Scamwatch (2020). *Current COVID-19 (coronavirus) scams*. Recuperado de www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

Schlomann, A., Bünning, M., Hipp, L., & Wahl, H. W. (2022). Aging during COVID-19 in Germany: a longitudinal analysis of psychosocial adaptation. *European journal of ageing*, 19(4), 1077-1086.

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).

Segal, M., Doron, I. & Mor, S. (2021). Consumer Fraud: Older People's Perceptions and Experiences. *Journal of Aging & Social Policy,* 33(1), 1–21. https://doi.org/10.1080/08959420.2019.1589896

Shao, J., Zhang, Q., Ren, Y., Li, X. & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. J*ournal of Elder Abuse & Neglect*. 31. 1-

19. https://doi.org/10.1080/08946566.2019.1625842

Shapira, N., Barak, A., & Gal, I. (2007). Promoting older adults' well-being through Internet training and use. *Aging & mental health*, 11(5), 477–484. https://doi.org/10.1080/13607860601086546

Shlisky, J., Bloom, D. E., Beaudreault, A. R., Tucker, K. L., Keller, H. H., Freund-Levi, Y., Fielding, R. A., Cheng, F. W., Jensen, G. L., Wu, D., & Meydani, S. N. (2017). Nutritional Considerations for Healthy Aging and Reduction in Age-Related Chronic Disease. *Advances in nutrition* (Bethesda, Md.), 8(1), 17–26. https://doi.org/10.3945/an.116.013474

Sitges-Maciá, E., Bautista-Ortuño, R., & Lorente-Martínez, R. (2020). Fundamentos teóricos y de investigación en gerontología. En J. Rodríguez-Marín & E. Sitges-Maciá (Eds.), *Perspectivas de estudio en gerontología y salud en el siglo XXI* (pp. 19-100). Tirant lo Blanch.

Skinner, K. D., Rojas, S. M. & Veilleux, J. C. (2016). Connecting eating pathology with risk for engaging in suicidal behavior: The mediating role of experiential avoidance. *Suicide and Life-Threatening Behavior*, 47(1), 3–13. https://doi.org/10.1111/sltb.12249

Skogan, W. G. (1987). *The Impact of Victimization on Fear. Crime & Delinquency*, 33(1), 135–154. https://doi.org/10.1177/0011128787033001008

Smith, R.G. & Budd, C. (2009). Consumer fraud in Australia: Costs, rates and awareness of the risks. *Trends & Issues in Crime and Criminal Justice* (382). Canberra: Australian Institute of Criminology.

Sourbati, M. (2009). «It could be useful, but not for me at the moment»: older people, internet access and e-public service provision. *New Media & Society,* 11(7), 1083-1100. https://doi.org/10.1177/1461444809340786

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior,* 29(1), 40–50. https://doi.org/10.1016/j.chb.2012.05.026

Starfield, B., Shi, L. & Macinko, J. (2005). Contribution of primary care to health systems and health. *The Milbank quarterly,* 83(3), 457–502. https://doi.org/10.1111/j.1468-0009.2005.00409.x

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Sutton, R. & Farrall, S. (2005). Gender, Socially Desirable Responding and the Fear of Crime: Are Women Really More Anxious About Crime? *British Journal of Criminology*, 45: 212-224

Tak, P. & Panwar, S. (2017). "Using UTAUT 2 model to predict mobile app based shopping: evidences from India", *Journal of Indian Business Research*, Vol. 9 No. 3, pp. 248-264. https://doi.org/10.1108/JIBR-11-2016-0132

Takano, T., Nakamura, K., & Watanabe, M. (2002). Urban residential environments and senior citizens' longevity in megacity areas: the importance of walkable green spaces. *Journal of epidemiology and community health,* 56(12), 913–918. https://doi.org/10.1136/jech.56.12.913

Tesch-Römer, C., von Kondratowitz, H.J. & Motel-Klingebiel, A. (2001). Quality of life in the context of intergenerational solidarity. In: Daatland SO, Herlofson K (eds) *Ageing, intergenerational relations, care systems and quality of life*. Nova, Oslo, pp 63–73

Titus, R. (2001). Personal fraud and its victims. *In Shover N and Wright J* (eds) Crimes of Privilege: 57-66. New York: Oxford University Press

Tomaka, J., Blascovich, J., Kibler, J. & Ernst, J. M. (1997). Cognitive and physiological antecedents of threat and challenge appraisal. *Journal of Personality and Social Psychology,* 73(1), 63-72. https://doi.org/10.1037/0022-3514.73.1.63

Ueno, D., Daiku, Y., Eguchi, Y., Iwata, M., Amano, S., Ayani, N., Nakamura, K., Kato, Y., Matsuoka, T. & Narumoto, J. (2021). Mild Cognitive Decline Is a Risk Factor for Scam Vulnerability in Older Adults. Frontiers in psychiatry, 12, 685451. https://doi.org/10.3389/fpsyt.2021.685451

Valera, S. & 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 Bavel, R., Rodríguez-Priego, N., Vila, J. & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

van Deursen, A. J. & van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507-526. https://doi.org/10.1177/1461444813487959

Van Dijk, J.A. (2006) Digital Divide Research, Achievements and Shortcomings. *Poetics,* 34, 221-235. https://doi.org/10.1016/j.poetic.2006.05.004

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* 27(3), 425–478. https://doi.org/10.2307/30036540

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

Von Hentig (1948). *The Criminal & His Victim: Studies in the Sociobiology of Crime*. Yale University Press

Vroman, K.G., Arthanat, S. & Lysack, C. (2015), «Who over 65 is online? Older adults' dispositions toward information communication technology», *Computers in Human Behavior,* Vol. 43, pp. 156-166. https://doi.org/10.1016/j.chb.2014.10.018

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* POLITY.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police practice and research*, 8(2), 183-205.

Wallace, H. & Roberson, C. (2015). V*ictimology: Legal, Psychological, and Social Perspectives* (4th ed.). Pearson.

Warschauer, M. (2002). Reconceptualizing the Digital Divide. *First Monday,* 7(7). https://doi.org/10.5210/fm.v7i7.967

Warr, M. (1987). Fear of victimization and sensitivity to risk. *Journal of Quantitative Criminology*, 3(1):29-47.

Welsh, B. C. & Farrington, D. P. (2009). Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis. *Justice Quarterly,* 26(4), 716–745. https://doi.org/10.1080/07418820802506206

Whitty. (2015). The Scammers Persuasive Techniques Model Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology.*, 53(4), 665–684.

Whitty M. T. (2018). Do You Love Me? Psychological Characteristics of Romance

Scam Victims. Cyberpsychology, behavior and social networking, 21(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Wood, S., Rakela, B., Liu, P. J., Navarro, A. E., Bernatz, S., Wilber, K. H., Allen, R. & Homeier, D. (2014). Neuropsychological profiles of victims of financial elder exploitation at the los angeles county elder abuse forensic center. *Journal of elder abuse & neglect,* 26(4), 414–423. https://doi.org/10.1080/08946566.2014.881270

Wortley, R. (2001). A Classification of Techniques for Controlling Situational Precipitators of Crime. *Secur J* 14, 63–82 (2001). https://doi.org/10.1057/palgrave.sj.8340098

Wright, R. T. & Decker, S. H. (2020). *Criminals in the Making: Criminality Across the Life Course* (2nd ed.). SAGE Publications.

Wright, K. A., Kim, B., Chassin, L., Losoya, S. H. & Piquero, A. R. (2014). Ecological context, concentrated disadvantage, and youth reoffending: identifying the social mechanisms in a sample of serious adolescent offenders. *Journal of youth and adolescence,* 43(10), 1781–1799. https://doi.org/10.1007/s10964-014-0173-0

Wu, F. & Sheng, Y. (2019). Social support network, social support, self-efficacy, health- promoting behavior and healthy aging among older adults: A pathway analysis, *Archives of Gerontology and Geriatrics,* Volume 85, https://doi.org/10.1016/j.archger.2019.103934

Xie, B. (2003). Older adults, computers, and the Internet: Future directions. *Gerontechnology*, 2(4), 289-305.

Xie, B., Charness, N., Fingerman, K., Kaye, J., Kim, M. T., & Khurshid, A. (2020). When Going Digital Becomes a Necessity: Ensuring Older Adults' Needs for Information, Services, and Social Inclusion During COVID-19. *Journal of*

aging & social policy, 32(4-5), 460-470. https://doi.org/10.1080/08959420.2020.1771237

Yang, Y., Piao, W., Huang, K., Fang, H., Ju, L., Zhao, L. & Ma, Y. (2022). Dietary pattern associated with the risk of hyperuricemia in Chinese elderly: result from china nutrition and health surveillance 2015–2017. *Nutrients*, 14(4), 844. https://doi.org/10.3390/nu14040844

Yar, M. (2006). *Cybercrime and society*. SAGE Publications Ltd, https://doi.org/10.4135/9781446212196

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

Zhang, M. (2023). Older people's attitudes towards emerging technologies: A systematic literature review. *Public Understanding of Science,* 0(0). https://doi.org/10.1177/09636625231171677

ANEXOS

ANEXO I

CUESTIONARIO FRAUDE ONLINE

Desde la Universidad Miguel Hernández de Elche se esta llevando a cabo un estudio sobre el fraude online en personas mayores de 55 años.
Por favor, lea detenidamente las preguntas y señale la respuesta que más se ajusta a su situación. Recuerde que no hay respuestas correctas ni incorrectas, solo queremos saber su opinión, por lo que le agradecemos que sea lo más sincero/a posible.
Se trata de una encuesta anónima, que no le llevará más de 10 minutos completar y nos aportará datos de gran interés. Si está de acuerdo continúe con la realización del cuestionario.

Muchas gracias por su participación

A) Datos sociodemográficos

1. ¿Fue alumno de las AUNEX en el curso 21/22?

2. Edad

3. Sexo
- Hombre
- Mujer

4. Nivel de estudios
- Sin estudios
- Primarios
- Secundarios

- Superiores

5. Situación de convivencia actual
- Solo/a
- En pareja
- Con otro familiar o conocido
- En una residencia

6. Ingresos mensuales
- Entre 0 y 500€
- Entre 500 y 1000€
- Entre 1000 y 2000€
- Más de 2000€

B) Datos sobre el uso de internet

7. ¿Con qué frecuencia utiliza internet?
- Nunca
- Menos de una hora al día
- Entre una y tres horas al día
- Más de tres horas al día

8. Respecto al uso que hacía de internet antes de la situación de confinamiento, ¿cuál es su uso actual?
- Menos que antes del confinamiento
- Igual que antes del confinamiento
- Más que antes confinamiento

9. ¿Para qué suele utilizar Internet? (marque todas las opciones que considere correctas)
- No utilizo nunca a Internet
- Redes sociales (Facebook, Twitter…)
- Correo electrónico

- WhatsApp
- Para buscar información (cultural, noticias, recetas de cocina...)
- Para realizar compras online
- Para banca online

10. ¿Ha recibido algún curso para aprender a manejar internet?
- Si
- No

11. ¿Utiliza contraseñas diferentes para cada una de sus cuentas?
- Nunca
- A veces
- La mayoría de las veces
- Siempre

12. ¿Cuál tipo de contraseña que utiliza normalmente?
- 14393738 (sólo números)
- mariA232 (letras y números)
- maría (sólo letras)
- *Maria748373? (letras, números, símbolos y mayúsculas)

13. ¿Ha experimentado usted alguna de las siguientes situaciones en internet en los últimos 12 meses? Señale todas las opciones que considere correctas.

- No utilizo nunca internet
- Comprar un producto por internet y no recibirlo, recibir algo diferente o que le cobren un precio que no era el establecido.
- Recibir un mail ofreciéndole un premio, descuento o un negocio del que sospechaba que pudiera ser engañoso.
- Recibir un correo o mensaje de una entidad conocida que usted consideraba era falso (por ejemplo, hacerse pasar por una entidad bancaria, por Hacienda, etc.)

- Entablar una relación de amistad con alguien que ha conocido a través de Internet y que en un momento determinado esta persona le solicite ayuda económica.
- Abrir enlaces o descargar archivos infectados con un virus informático.
- Sufrir un perjuicio patrimonial debido a un premio, inversión o negocio que resultó ser falso.
- Que alguien haya adoptado su identidad en Internet sin su consentimiento.
- Ninguna de las anteriores

14. Si su respuesta ha sido afirmativa en alguno de los casos anteriores, ¿lo denunció?

- No
- Si, en la policía u otra autoridad pública
- Si, en una institución (banco, etc)
- Sólo lo comenté con un familiar o conocido

C) Compra online

C1) Rutinas

15. ¿Con qué frecuencia realiza compras online?

- Nunca
- Menos de una vez al mes
- Varias veces al mes
- Cada día

C2) Percepción de vulnerabilidad

16. ¿Cuánta probabilidad cree usted que tiene de que le estafen mediante una compra online?

- Ninguna
- Poca
- Moderada

- Alta

C3) Medidas de protección

17. En relación a las compras online ¿Cuál de estas conductas lleva a cabo?
- Las realiza siempre en una página de confianza
- Busca información sobre el producto y el vendedor antes de realizarla
- Pregunto a conocidos o familiares si es una página dónde es fiable realizar mis compras.
- La realizo en el sitio que este más barato
- La realizo en cualquier página que aparezca en el buscador y tenga el producto que quiero.

D) Email

D1) Rutinas

18. ¿Con qué frecuencia utiliza su correo electrónico?
- Nunca
- Menos de una vez al mes
- Varias veces al mes
- Cada día

19. ¿Con qué frecuencia utiliza WhatsApp?
- Nunca
- Menos de una vez al mes
- Varias veces al mes
- Cada día

20. ¿Con que frecuencia utiliza redes sociales (Facebook, Instagram…)?
- Nunca
- Menos de una vez al mes
- Varias veces al mes
- Cada día

D2) Percepción de vulnerabilidad

21. ¿Cuánta probabilidad cree usted que tiene de que le estafen mediante un correo electrónico o un mensaje (WhatsApp, mediante redes sociales…)?

- Ninguna
- Poca
- Moderada
- Alta

D3) Medidas de protección

22. Con relación a su correo electrónico, ¿Cuáles de las siguientes conductas lleva a cabo? Marque todas las opciones que considere.

- Marco los emails sospechosos como spam
- Elimino sin abrir los emails que me parecen sospechosos
- Cuando un email me parece sospechoso busco información en internet sobre él.
- Abro los enlaces de los mails que recibo, aunque no conozca su procedencia
- Cuando recibo un mail que es sospecho contesto que no para que no me envíen más o para solicitar más información.

E) Virus

E1) Rutinas

23. ¿Con que frecuencia accede a enlaces o descarga archivos desde un dispositivo electrónico?

- Nunca
- Menos de una vez al mes
- Varias veces al mes
- Cada día

E2) Percepción de vulnerabilidad

24. ¿Cuánta probabilidad cree usted que tiene de que sus dispositivos se infecten con un virus?

- Ninguna
- Poca
- Moderada
- Alta

E3) Medidas de protección

25. ¿Tiene instalado un antivirus en sus dispositivos electrónicos?

- Si, en todos
- Solo en el ordenador
- Sólo en el móvil o Tablet
- No, no tengo antivirus

26. ¿Con qué frecuencia realiza análisis en sus dispositivos para localizar posibles virus?

- Diariamente
- Semanalmente
- Varias veces al mes
- Una vez al mes
- Menos de una vez al mes
- Nunca

F) Información personal

F1) Rutinas/ medidas de seguridad

27. ¿Con qué frecuencia introduce datos personales (número de cuenta, dni, claves, etc) mediante sus dispositivos electrónicos?

- Nunca
- Menos de una vez al mes

- Varias veces al mes

F2) Percepción de vulnerabilidad

28. ¿Cuánta probabilidad cree usted que tiene de que utilicen sus datos personales sin su consentimiento?

- Ninguna
- Poca
- Moderada
- Alta

ANEXO II

Área 1: Cambio en el uso de las TIC y capacidad para enfrentar estos cambios.

- ¿Te has sentido obligado a hacer uso de las TIC? Si es así, ¿en qué áreas has sentido esta obligación (comunicación, banca, salud...)? ¿Cómo te hizo sentir esto? ¿Crees que la situación de COVID-19 ha influido en esto?

- ¿Sientes que tienes la preparación necesaria para usar las TIC? Si no, ¿cuáles crees que son las consecuencias de no tener esta formación?

Área 2: Inseguridad y miedo sobre el uso de las TIC

- ¿Cuáles son los usos de las TIC en los que te sientes más capaz? ¿Y en cuáles te sientes menos capaz?

- ¿Hay algo que te haga sentir inseguro al usar las TIC?

- ¿Alguna vez has tenido miedo de convertirte en víctima de un delito al usar las TIC? Si es así, ¿de qué tipo?

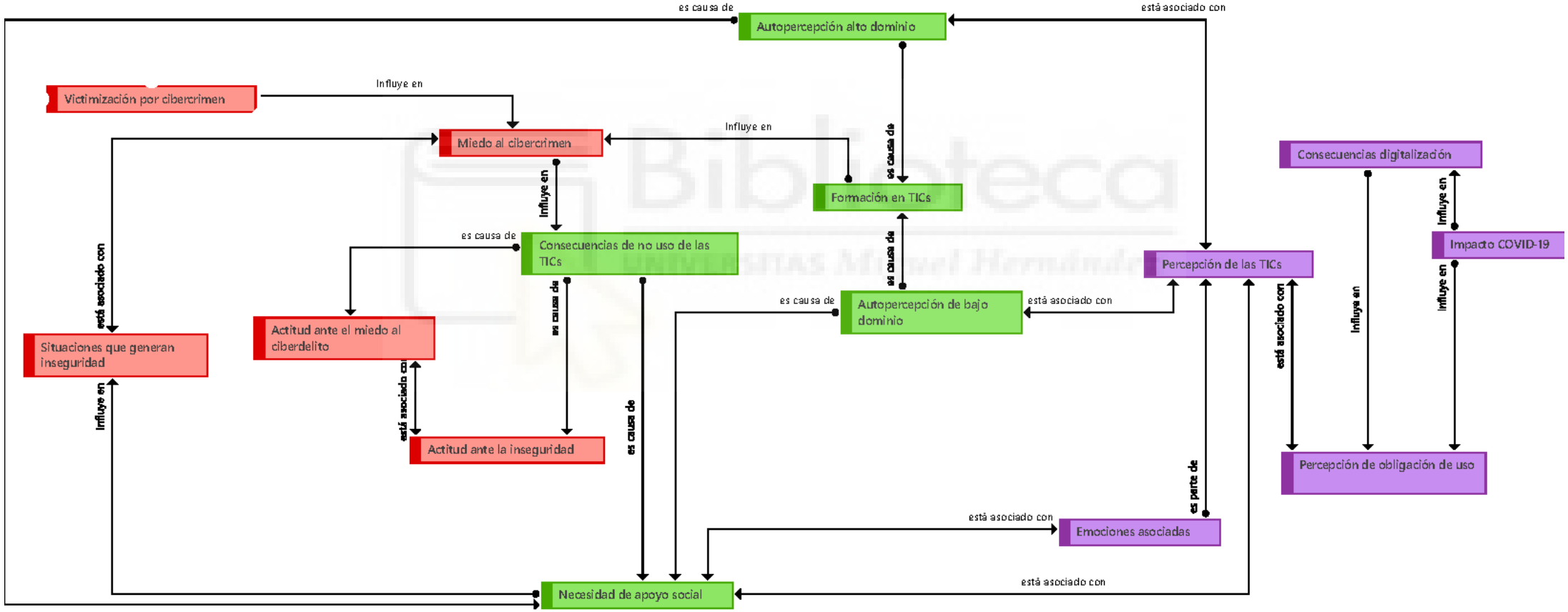
Área 3: Consecuencias de la inseguridad y el miedo y del no uso de las TIC

- ¿Alguna vez no has usado las TIC porque temías las consecuencias de usarlas? Si es así, ¿qué posibles consecuencias te han llevado a no usarlas?

- ¿Crees que no usar las TIC puede tener consecuencias para ti? ¿Cuáles?

- Si te sientes inseguro al usar las TIC, ¿qué consecuencias crees que puede tener para ti?

ANEXO III


es causa de
Autopercepción alto dominio
está asociado con
Victimización por cibercrimen
Influye en
Miedo al cibercrimen
Influye en
es causa de
Formación en TICs
Consecuencias digitalización
Influye en
Impacto COVID-19
Influye en
es causa de
Consecuencias de no uso de las TICs
es causa de
Percepción de las TICs
está asociado con
Situaciones que generan inseguridad
Actitud ante el miedo al ciberdelito
es causa de
Autopercepción de bajo dominio
está asociado con
está asociado con
Influye en
está asociado con
Actitud ante la inseguridad
es causa de
Influye en
está asociado con
Percepción de obligación de uso
es parte de
está asociado con
Emociones asociadas
está asociado con
Necesidad de apoyo social

Agradecimientos

Al llegar al final de este largo y enriquecedor viaje académico, que espero que suponga el inicio de otro, me gustaría dedicar unas palabras de agradecimiento a todas aquellas personas y seres que, de una forma u otra, han sido fundamentales en la culminación de esta tesis doctoral.

En primer lugar, quiero expresar mi más profundo agradecimiento a mi directora de tesis, la Dra. Esther Sitges Maciá. Esther, tu confianza inquebrantable en mí y tu guía paciente y sabia han sido fundamentales en este proceso. Gracias por creer en mi potencial y por impulsarme a superar mis propios límites.

A mi codirector de tesis, el Dr. Steven Kemp, mis más sinceros agradecimientos por todos tus valiosos consejos y por ser una fuente constante de conocimiento. Tus observaciones siempre precisas y oportunas han sido esenciales para la evolución de este trabajo.

En este punto no puedo dejar de mencionar al Dr. Fernando Miró, ha sido un honor y un privilegio contar con tu cercanía y sabiduría. Tu ejemplo y tus aportaciones en este campo han enriquecido profundamente esta investigación.

A mis amigas, a todas, pero especialmente a Maica y Lourdes. Maica, gracias por ser ese soplo de aire fresco que tanto necesitaba en los momentos de tensión, sin ti todo esto habría sido mucho más difícil. Lourdes, gracias por estar siempre ahí, incluso cuando te hablaba de cosas que seguro te sonaban a klingon. Vuestra amistad ha sido un pilar fundamental para mí, prometo que ya no os hablaré más de este trabajo, aunque sabéis que tendréis que aguantarme con los siguientes.

A mi familia, especialmente a mi padre y a mi madre. Aunque siguen sin entender del todo qué es una tesis doctoral, su apoyo incondicional y su fe en mí han sido el motor que me ha impulsado a seguir adelante. Gracias por estar siempre ahí, sin importar las circunstancias, os quiero.

A mi compañero de vida, Miguel Ángel, por su comprensión y apoyo y por formar siempre equipo a mi lado. Aunque sé que la jerarquía universitaria y los términos académicos no siempre resultan claros, tu apoyo ha sido vital para mantenerme firme en este camino.

Y, por supuesto, a mis compañeros de cuatro patas: Izzy, Mystika y Tayler. Aunque no vais a entender nada de esto, vuestra compañía silenciosa ha sido fundamental en los momentos en que sentía que esto podía superarme, en los que sólo quedábamos vosotros y yo, y vuestras miradas inquisitivas a altas horas de la madrugada me proporcionaban un recordatorio de que la vida es más que solo trabajo y estudio. Este logro es, en parte, gracias a vosotros. Si algún día se llega a traducir esta tesis al "lenguaje de los ladridos y maullidos", sabed que sois una parte esencial de esta historia.

A todos vosotros, gracias de corazón. Esta tesis es el resultado de un esfuerzo colectivo, donde cada uno ha aportado su granito de arena para que hoy pueda presentar este trabajo.