Consultoría y Estudios (CiE)

Ciberdelincuencia en personas mayores: prevención, detección y acompañamiento a la visibilización de la realidad

FUNDACIÓ PERE TARRÉS

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

Informe de resultados en el programa 101/2024/155/7/

Ciberdelincuencia en personas mayores: prevención, detección y acompañamiento a la visibilización de la realidad

FUNDACIÓN PERE TARRÉS

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

Autoría

David Lozano Arjona

Coordinación. Consultoría y Estudios.

Ares Cruz Hernández

Técnica de proyectos. Consultoría y Estudios.

Leire Franco Salazar

Técnica de proyectos. Consultoría y Estudios.

Sebastián Justicia Justicia

Técnico de proyectos. Consultoría y Estudios.

Caterina Guardiet Grande

Apoyo administrativo. Consultoría y Estudios.

Equipo colaborador:

Maria Lorenzo, Coordinadora pedagógica del departamento de Acción Social de la Fundació Pere Tarrés

Carles Pineda, Coordinador de proyectos del ámbito de gente mayor de Acción Social de la Fundació Pere Tarrés

Ana Aguilar, Coordinadora del Casal de Personas Mayores Penitents

Susana Barrios, Coordinadora del Espacio de Personas Mayores La Violeta

Federación de Asociaciones de Personas Mayores de Catalunya (FATEC)

Índice

Índice de tablas

Índice de figuras

1. Introducción

El avance constante de las tecnologías de la información y la comunicación (TIC) ha transformado profundamente la manera en que las personas se conectan, acceden a servicios y realizan gestiones cotidianas. Hoy en día, Internet permite a los usuarios interactuar con instituciones públicas, entidades financieras y numerosos servicios esenciales a través de una compleja y avanzada red digital. Esta realidad ha generado la necesidad de adaptación por parte de la ciudadanía, obligando a incorporar nuevas habilidades en su vida diaria. Sin embargo, no todas las personas han podido adaptarse igual de rápido y al mismo nivel que el resto de la sociedad, lo que ha llevado a que ciertos colectivos hayan quedado rezagados en este proceso de digitalización, lo que se ha denominado como “brecha digital”. A este problema de desconexión y falta de acceso a servicios hay que sumarle que la creciente digitalización ha posibilitado también nuevas formas de crimen y otras conductas perjudiciales, frente a las que precisamente este colectivo es más vulnerable debido a su falta de competencias. Es importante, pues, reconocer que la digitalización conlleva también una serie de riesgos que requieren ser identificados, comprendidos y abordados desde una perspectiva crítica y preventiva, con el fin de evitar situaciones de vulnerabilidad frente a los delitos informáticos (Solórzano et al., 2022).

En este contexto, la ciberseguridad se ha convertido en una de las principales preocupaciones para quienes navegan por el entorno digital. La protección de la información personal y sensible representa uno de los grandes desafíos de la era actual, y la formación en este ámbito resulta fundamental para todos los grupos poblacionales, independientemente de su edad. Capacitar a la ciudadanía en competencias digitales y en herramientas de prevención frente a amenazas cibernéticas emergentes es una condición indispensable para afrontar los retos de una sociedad cada vez más interconectada.

La pandemia de COVID-19 aceleró de forma significativa la transformación digital, evidenciando tanto los avances tecnológicos alcanzados como las importantes carencias estructurales y formativas existentes en el país. Esta situación hizo aún más visible la brecha digital y la necesidad de intervención por parte de los poderes públicos. Como respuesta, el Gobierno de España impulsó el **Plan Nacional de Competencias Digitales** dentro del marco de la **Agenda Digital 2025**, con el propósito de garantizar que toda la ciudadanía adquiera habilidades digitales básicas y avanzadas. Dicho plan presta especial atención a colectivos considerados prioritarios, como la población activa, las mujeres y, de forma destacada, las personas mayores, con el objetivo de promover una inclusión tecnológica real y reducir las desigualdades de acceso y uso.

El envejecimiento demográfico constituye un factor clave en el análisis de la relación entre la población mayor y el uso de las tecnologías digitales. España, al igual que otros países del entorno europeo, experimenta un aumento sostenido en el número de personas mayores, lo que plantea nuevos desafíos en materia de accesibilidad digital, formación continua y seguridad en línea. A medida que este colectivo se ve cada vez más involucrado en el uso de las TIC para realizar trámites, acceder a servicios esenciales o mantenerse comunicados, su exposición a los riesgos asociados a la ciberdelincuencia también se incrementa, posicionándolos como un objetivo habitual de este tipo de delitos.

En paralelo, el crecimiento exponencial de la digitalización en los sectores público y privado ha generado un entorno propicio para la expansión de los delitos informáticos. Las cifras evidencian una tendencia al alza: en 2019 se registraron 218.302 hechos delictivos relacionados con la cibercriminalidad, cifra que aumentó a 287.963 en 2020, a 305.477 en 2021, a 374.737 en 2022 y que alcanzó los 472.125 en 2023. Esto representa un crecimiento superior al 116% en apenas cuatro años (Muniesa et al., 2023), consolidando la ciberdelincuencia como una de las principales amenazas en materia de seguridad.

Dentro de este conjunto de delitos, el **fraude informático** representa el porcentaje más elevado, con un 90,5% de los casos registrados en 2023, seguido de las **amenazas y coacciones** (3,7%) y la **falsificación informática** (3,2%). También se observan incrementos notables en delitos como el **acceso e interceptación ilícita de comunicaciones** y la **interferencia en datos y sistemas**, reforzando la urgencia de implementar medidas eficaces de protección.

Aunque el número de esclarecimientos de delitos y de actuaciones policiales ha mejorado significativamente, pasando de 30.841 casos resueltos en 2019 a 60.197 en 2023, y de 8.914 a 17.173 detenciones e investigaciones en el mismo período, el ritmo de crecimiento de los delitos supera ampliamente los avances en su persecución. Esto pone de manifiesto la necesidad de reforzar estrategias preventivas, mejorar las capacidades de detección y promover una cooperación internacional más eficaz, dada la dimensión transnacional de muchas de estas actividades ilícitas.

En este escenario, es previsible que la ciberdelincuencia continúe creciendo y represente una porción cada vez mayor de la actividad delictiva en el país. La sensación de impunidad y la dificultad de rastrear a los responsables debido a la naturaleza global y descentralizada de internet (Cerezo Domínguez & García Cornejo, 2020) refuerzan este diagnóstico.

En cuanto al perfil de las víctimas, los datos muestran que los delitos informáticos afectan a todas las franjas de edad, si bien con distinta intensidad. En 2023 se registraron 354.610 victimizaciones, siendo los grupos entre 26 y 50 años los más afectados. En particular, el

tramo de 26 a 40 años concentró 92.830 víctimas, seguido por el grupo de 41 a 50 años con 81.840 casos. Estos datos evidencian que la exposición a los riesgos digitales está estrechamente relacionada con la frecuencia y el tipo de uso de las TIC.

Sin embargo, el colectivo de personas mayores de 65 años, pese a no ser el más afectado en términos absolutos, presenta un elevado nivel de vulnerabilidad. En 2023, se registraron 39.565 casos dentro de este grupo, de los cuales 38.041 correspondieron a fraudes informáticos. La incidencia de otros delitos, como la falsificación informática, las amenazas y el acceso ilícito a las comunicaciones, también resulta significativa, reflejando las dificultades que enfrenta este colectivo para desenvolverse con seguridad en el entorno digital. En este sentido, resulta relevante señalar que diversos autores/as coinciden en que, si bien las personas mayores no constituyen el grupo de edad más afectado por la ciberdelincuencia, ello podría explicarse por su menor presencia en entornos digitales (Bustillo et al., 2022; Hargittai, Piper & Morris, 2019; Burton et al., 2022; INE, 2024; ONTSI, 2024). En general, este colectivo presenta niveles más bajos de competencias digitales – un punto señalado por Bunbury et al. (2022) y por Kuong et al. (2025)-, lo que limita su participación en actividades en línea, pero, al mismo tiempo, incrementa su vulnerabilidad en caso de que decidan realizar gestiones a través de Internet (Ross et al., 2014; Burton et al., 2022). De este modo, la falta de habilidades digitales opera, paradójicamente, como un factor tanto protector como de riesgo frente a los delitos informáticos.

Por tanto, aunque la ciberdelincuencia impacta en todos los segmentos poblacionales, este informe centra su atención en las personas mayores, un grupo que enfrenta retos específicos en relación con la seguridad digital. La menor familiaridad con los entornos tecnológicos, la escasa formación en ciberseguridad y el incremento del uso de Internet para la gestión de trámites personales y financieros los convierte en un blanco preferente para los ciberdelincuentes. En este sentido, es fundamental reconocerles como un grupo activo, capaz de adquirir nuevas competencias y de desempeñar un papel relevante en la sociedad digital, siempre que cuenten con los apoyos y las herramientas necesarias.

Partiendo de lo expuesto anteriormente, desde la Fundación Pere Tarrés, se ha diseñado e implementado el programa 101/2024/155/7/ “Ciberdelincuencia en personas mayores: prevención, detección y acompañamiento a la visibilización de la realidad”, financiado a través de las subvenciones del Ministerio de Derechos Sociales, Consumo y Agenda 2030 a entidades que realicen actividades de interés social con cargo a la asignación tributaria del IRPF.

Dicho programa tiene como objetivo analizar los principales riesgos y tipologías de ciberdelincuencia que afectan a las personas mayores, explorar estrategias eficaces de

prevención y detección temprana, y proponer modelos de acompañamiento que fomenten la denuncia, la sensibilización y la visibilización de estas problemáticas.

Para la implementación del programa, se ha contado con la colaboración de diversas entidades, principalmente, la FATEC (Federació d'Associacions de Gent Gran de Catalunya) y la Asociación Cultural El Parlante, con experiencia en la comunicación y sensibilización social. Ambas tienen experiencia en la relación con personas mayores y en la lucha contra el edadismo. La participación de estas organizaciones, juntamente con la trayectoria de la FPT en la atención y apoyo al colectivo, especialmente a través de las áreas de personas mayores y de acción digital de la Fundación, ha dotado de calidad a la investigación, garantizando un abordaje integral y centrado en la persona.

Así, desde un enfoque integral e inclusivo, se aspira a contribuir al diseño de políticas públicas y acciones formativas que reduzcan la vulnerabilidad de este colectivo y promuevan un entorno digital más justo, accesible y seguro para todos. Entre otras acciones, se ha diseñado una guía de buenas prácticas orientadas a profesionales que trabajan con y para el colectivo, así como distintos materiales de sensibilización y concienciación que buscan mejorar las respuestas institucionales y actitudes sociales frente a las personas mayores, especialmente cuando estas han sido víctimas de ciberdelitos.

El siguiente informe constituye un resumen de las diferentes evidencias y hallazgos identificados a lo largo de la implementación, así como una memoria de las diferentes acciones desarrolladas.

2. Objetivos

Objetivo General 1. Diagnosticar los principales cibercrímenes, los factores de riesgo y protección y el impacto sobre las personas mayores para una mejor prevención y detección.

OE1.1: Analizar el impacto real del cibercrimen en las distintas dimensiones de la calidad de vida de las personas mayores.

OE1.2: Identificar los principales factores de riesgo y protección, los cuales son clave para minimizar el impacto de la ciberdelincuencia.

OE1.3: Analizar cómo se trabaja prevención y detección de la ciberdelincuencia en personas mayores.

OE.1.4. Identificar necesidades formativas para la prevención y detección de la ciberdelincuencia involucrando a las personas mayores y a los agentes que participan con y para ellas.

Objetivo general 2. Diseño, desarrollo e implementación de prueba piloto talleres participativos con personas mayores para combatir la ciberdelincuencia.

OE2.1: Diseñar una propuesta de talleres participativos con personas mayores que favorezca el aprendizaje de la prevención y detección de la ciberdelincuencia.

OE2.2: Desarrollar una propuesta de talleres participativos con personas mayores que facilite la participación de las personas mayores y ayude concienciarles sobre los beneficios del ciberespacio y el uso de las TIC y les apodere y capacite para su uso seguro.

OE2.3. Implementar talleres de acompañamiento participativo adaptado a las personas mayores que mejore el aprendizaje de este contenido en prevención a la delincuencia.

Objetivo General 3. Dar apoyo y asesoramiento a profesionales de la atención directa e indirecta de personas mayores sobre cómo prevenir y detectar casos de ciberdelincuencia y acompañar al colectivo para romper estigmas.

OE.3.1. Diseñar una propuesta de workshop con personas y agentes vinculados a las personas mayores que identifique como trabajan la ciberdelincuencia con el colectivo y les capacite a prevenir y detectar casos invisibilizados.

OE.3.2. Desarrollar e implementar una propuesta de workshop colaborativo adaptado que mejore el reconocimiento de las realidades de ciberdelincuencia, y el acompañamiento a ofrecer en caso de prevenir, o de detectar (recursos disponibles, servicios que atienden, etc.)

Objetivo General 4. Validación y escalado del contenido, creación de 2 videos formativos para canales TIC sobre ciberdelincuencia y personas mayores, presentación y difusión de resultados.

OE.4.1. Validación del contenido y diseño de los videos formativos para personas mayores sobre ciberdelincuencia.

O.E.4.2. Identificación de los canales clave para hacer difusión de los videos formativos surgidos protagonizados por personas mayores, para poder sensibilizar, escalando los resultados a la población.

OE.4.3. Difusión del contenido generado (informe, metodología, talleres, etc.)

3. Metodología

La metodología para la redacción del presente informe y ejecución del resto de actividades contempladas en el programa "101/2024/155/7 Ciberdelincuencia en personas mayores: prevención, detección y acompañamiento a la visibilización de la realidad" se basó en distintas técnicas de participación y de investigación cualitativa. Los datos obtenidos fueron analizados mediante la herramienta de software especializada en análisis cualitativo ATLAS.ti.

El programa contó con una primera fase de **revisión bibliográfica**, en la que se han explorado las siguientes bases de datos: PubMed, Scopus, Web of Science (WOS), y Google Scholar. Se han empleado los siguientes términos de búsqueda, tanto en castellano como en inglés, divididos en áreas temáticas:

- **Definición, tipos e incidencia de los cibercrímenes**: 'cibercrimen' o 'ciberdelito' y 'incidencia' o 'víctimas' o 'tipos' o 'estadísticas' / 'cybercrime' y 'incidence' o 'victims' o 'types' o 'statistics'.
- **Impacto emocional del cibercrimen**: 'cibercrimen impacto emocional' o 'ciberdelito impacto emocional' o 'fraude informático impacto emocional' y 'personas mayores' / 'emotional impact cybercrime' o 'cybercrime victimization' o 'online fraud emotional impact' y 'old people' o 'older people' o 'elder people' o 'old adults' o 'older adults' o 'elder adults'.
- **Respuesta actual al cibercrimen**: 'víctimas cibercrimen' o 'víctimas ciberdelito' o 'cibercrimen casos' o 'ciberdelito casos' y 'canales de atención' o 'respuesta institucional' o 'apoyo entidades bancarias' / cybercrime victims' o 'cybercrime cases' Y 'service channels' o 'institutional response' o 'banking institutions support'.
- **Estrategias y enfoques idóneos**: 'víctimas cibercrimen' o 'víctimas ciberdelito' y 'estrategias' o 'enfoques' o 'herramientas' o 'cuidado' o 'acompañamiento' o 'factores de riesgo' o 'factores de protección' / 'cybercrime victims' y 'strategies' o 'approaches' o 'tools' o 'care' o 'support' o 'risk factors' o 'protective measures'.

El resultado fue una selección de más de 40 artículos. Además de las publicaciones en sí, también se revisaron sus referencias bibliográficas con la técnica de *backward snowballing* (Wohlin, 2014) con el fin de encontrar otros artículos relevantes. Asimismo, se consultó la página web y publicaciones específicas de organismos relevantes, como el INCIBE, a medida que estos eran identificados. El conjunto de material académico recopilado ha sido sistematizado y explotado con la ayuda del gestor Mendeley.

En segundo lugar, se llevó a cabo una fase de contextualización, en la que se recabó información del estado de la situación actual de la ciberdelincuencia y su impacto en España, de páginas web gubernamentales como la del Ministerio del Interior. Se realizaron un total de

10 entrevistas[1] con profesionales de carácter multidisciplinar, entre las que se incluyen técnicos/as de la administración pública, expertos/as de universidades y ámbito académico, y trabajadores del tercer sector y de la industria privada.

En una tercera fase, se organizaron dinámicas participativas con personas mayores (un total de 10 talleres), que sirvieron para validar y mejorar los resultados obtenidos en las fases anteriores. Los talleres con personas mayores se realizaron en las propias aulas y espacios habilitados por la Fundación Pere Tarrés para desarrollar acción social enfocada al colectivo, y fueron dinamizados por dos profesionales que ya han impartido talleres similares. Así, el equipo del programa diseñó una propuesta educativa, que fue aplicada por profesionales con experiencia en el sector, quiénes, juntamente con las personas mayores, valoraron la información recibida e hicieron propuestas de mejora. En el apartado de Anexos de este informe se incluye la relación de los talleres realizados y el feedback recibido.

A partir de estas experiencias y del *feedback* obtenido se diseñó una breve guía con pautas y recomendaciones para una correcta relación con personas mayores que han sido víctima de ciberdelitos, incidiendo sobre todo en herramientas educativas y de concienciación.

Con el fin de aumentar la difusión e impacto del programa y de los materiales resultantes, se diseñó una infografía informativa (tríptico) que recoge los hallazgos más significativos y que transmiten de manera visual y comprensible las estrategias y herramientas destacadas. Estas infografías, están disponible en el apartado “Anexos” de este informe. Además, se contó con la colaboración de la Asociación Cultural El Parlante, responsable de la grabación un spot de 7 minutos, en el que, a partir de una situación ficticia de fraude informático, se busca concienciar sobre el impacto emocional de la ciberdelincuencia y reivindicar el papel de las personas mayores como personas que gozan de una ciudadanía plena y con plenas capacidades e interés por aprender a manejarse en un entorno cada vez más virtual.

Finalmente, esta guía y las conclusiones generales fueron compartidas con el personal profesional que trabaja con y para el colectivo mediante un workshop online, en el que se inscribieron 16 personas, de seis diferentes Comunidades Autónomas. Dicho workshop fue celebrado el día 1 de diciembre del 2025 de 11 a 13h. Asimismo, también se reprodujo el spot producido por El Parlante y se habilitó un espacio, al final de la sesión, para recoger el *feedback* de las personas participantes y atender a cualquier duda o comentario.

[1] Ver anexo 2

3.1. Limitaciones metodológicas y operativas.

Como es habitual en proyectos de investigación aplicada e intervención social, el programa presenta una serie de limitaciones que conviene explicitar de manera clara y transparente. Estas limitaciones se agrupan en dos grandes ámbitos: **limitaciones metodológicas**, vinculadas al diseño del estudio y al tipo de evidencia generada, y **limitaciones operativas**, derivadas de las condiciones concretas de ejecución del programa (duración, recursos y alcance territorial).

Disponibilidad y naturaleza de los datos

El proyecto se apoyó fundamentalmente en fuentes secundarias (estadísticas oficiales y literatura especializada) y en información cualitativa auto-reportada por las personas entrevistadas. No se dispuso de un muestreo probabilístico ni de encuestas cuantitativas específicas al conjunto del colectivo de personas mayores. Asimismo, la infra-denuncia de los ciberdelitos (especialmente elevada en este grupo de edad) sugiere que la incidencia real de algunos fenómenos puede estar infraestimada. La ausencia de datos longitudinales y de información sistemáticamente desagregada por edad para todos los tipos de ciberdelincuencia impide medir con precisión el impacto sostenido de las intervenciones en el medio y largo plazo.

Posibles sesgos en la participación

El carácter voluntario de las actividades puede haber generado sesgos de autoselección, al participar principalmente personas mayores con mayor interés o mayor autonomía digital. Asimismo, factores como la vergüenza, el temor al estigma o la normalización de determinadas estafas pueden haber limitado la comunicación abierta de experiencias negativas, especialmente en contextos grupales.

Alcance territorial y representatividad de la muestra

Aunque la ejecución del proyecto se ha desarrollado fundamentalmente en el ámbito local de la ciudad de Barcelona y con un volumen acotado de participantes (10 entrevistas a profesionales expertos y 10 talleres participativos con un total de 96 personas mayores), el diseño metodológico y el enfoque analítico del programa se han planteado desde el inicio con una **mirada de alcance estatal**. La selección de dimensiones de análisis, la tipología de agentes implicados y la sistematización de los resultados responden a problemáticas ampliamente reconocidas en el conjunto del territorio, lo que permite una **lectura homogénea y comparable más allá del contexto específico de intervención**.

Si bien la intervención presencial se concentró mayoritariamente en centros de personas mayores del entorno urbano de Barcelona, por razones logísticas y presupuestarias, el proyecto ha incorporado deliberadamente una **perspectiva transferible**, identificando factores estructurales comunes y dinámicas replicables en otros territorios. La realización de un workshop final en línea con profesionales de distintas comunidades autónomas, aun con una participación parcial, ha contribuido a contrastar los hallazgos con realidades diversas y a reforzar la coherencia interpretativa del modelo propuesto.

En este sentido, el programa debe entenderse como un **piloto de base local, pero con vocación de escalado**, cuyos resultados no pretenden ofrecer una representación exhaustiva del conjunto del colectivo de personas mayores, sino generar un marco conceptual, metodológico y operativo susceptible de **adaptación, validación y despliegue progresivo a nivel estatal.,** siempre que se cuente con los recursos necesarios para ampliar su alcance territorial y poblacional.

Duración temporal limitada

El proyecto tuvo una duración aproximada de un año, con una ejecución intensiva de las acciones presenciales concentrada en un periodo corto. Los diez talleres formativos se realizaron en un mismo mes, con sesiones de entre 1,5 y 2 horas, lo que permitió un alcance rápido, pero limitó la profundización de contenidos y la posibilidad de refuerzo progresivo de los aprendizajes. Esta temporalidad impidió, además, realizar un seguimiento post-intervención que permitiera evaluar cambios sostenidos en hábitos digitales o en conductas de denuncia.

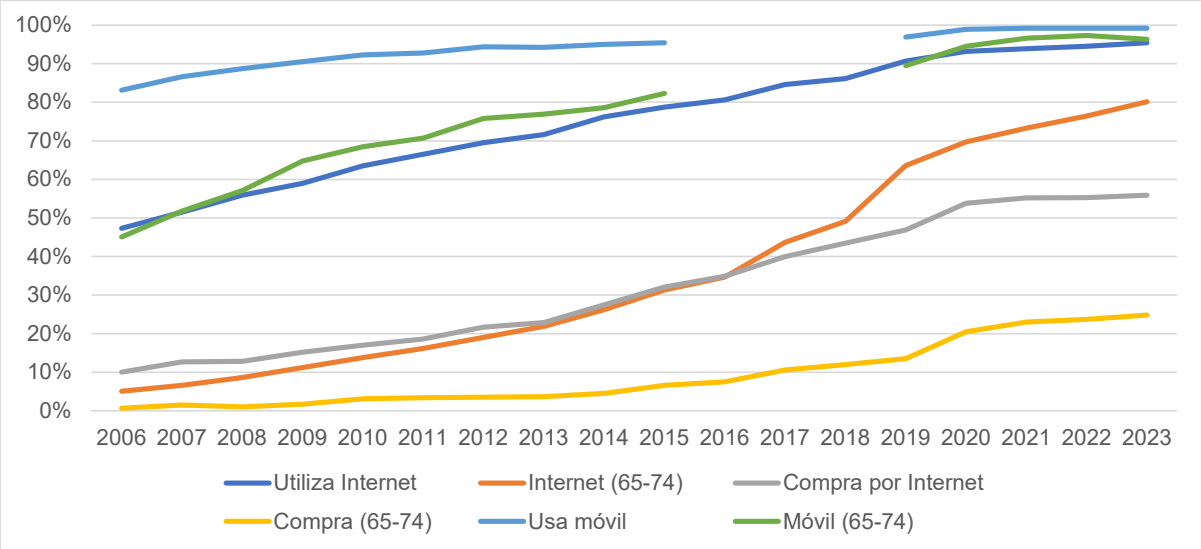
4. Articulación de la problemática social

4.1. Transformación digital: vivir, aprender y conectarse en la era tecnológica

En la era digital, el uso de las tecnologías de la información y la comunicación ha adquirido una relevancia fundamental, especialmente en aquellos colectivos que enfrentan mayores barreras para su acceso. Durante la pandemia de la COVID-19, estas herramientas fueron clave para favorecer la inclusión social y reducir el impacto del aislamiento en quienes tenían menos oportunidades de interacción. Sin embargo, a pesar del aumento en su uso, la situación evidenció la necesidad de reforzar las competencias digitales de las personas mayores, ya que aún persisten desigualdades asociadas al género, el nivel educativo y la edad.

La **transición digital**, entendida como el proceso de incorporación y adaptación a las tecnologías digitales en todos los ámbitos de la sociedad, requiere que toda la ciudadanía desarrolle competencias digitales básicas para interactuar con la administración, realizar transacciones y comunicarse con autonomía y seguridad. Si bien algunos sectores de la población ya disponen de estas habilidades, otros, como las personas mayores, las personas con bajos ingresos o las residentes en zonas rurales, enfrentan dificultades para acceder a los beneficios de la digitalización. Esto refuerza la necesidad de que la acción pública se enfoque en estos colectivos para evitar su exclusión y promover su integración digital a través de programas adaptados. En este sentido, resulta significativo que “el 80,1% de las personas entre 65 y 74 años utilizó internet en 2023, cuando en 2002 apenas lo hacía un 1,5%, según los datos que se pueden consultar en Eurostat” (Pérez et al., 2024, p.46).

Figura 1. *Datos de evolución por características demográficas y tipo de uso de TIC (2006-2023).*



Fuente: Adaptado de "Los mayores españoles continúan reduciendo su brecha digital", por A. B. Castillo Belmonte, J. Pérez Diaz, y D. Ramiro, 2023, *Envejecimiento en Red*. https://envejecimientoenred.csic.es/58857-2/

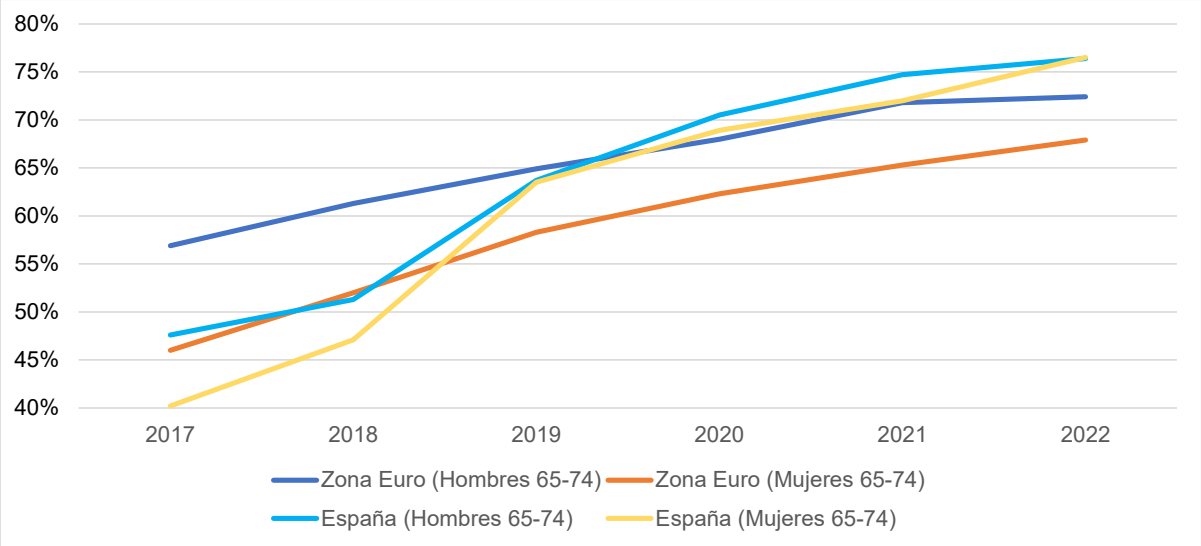
Este aumento en el uso de tecnologías entre las personas mayores puede atribuirse principalmente a tres factores interrelacionados (Envejecimiento en Red. CSIC, 2023):

- En primer lugar, la incorporación progresiva de nuevas generaciones a este grupo etario, que ya contaban con **experiencia previa** en el uso de Internet y tecnologías digitales.
- En segundo lugar, las notables **mejoras en la infraestructura digital**, incluyendo una mayor cobertura de redes, conexiones más estables y accesibles, y dispositivos cada vez más intuitivos y adaptados a las necesidades de esta población.
- Finalmente, un **acelerado** proceso de aprendizaje impulsado por la pandemia de la **COVID-19**, que obligó a muchas personas mayores a adoptar herramientas tecnológicas para mantener la comunicación social, acceder a servicios básicos y realizar actividades cotidianas desde sus hogares.

Aun así, a pesar de los esfuerzos del gobierno español por reducir la brecha digital y alcanzar los objetivos digitales de la Unión Europea, todavía persisten desafíos importantes. Uno de los objetivos clave es lograr **que el 80% de la población posea competencias digitales básicas**; sin embargo, según Eurostat, la población de entre 65 y 75 años en España aún está lejos de este indicador. En 2021, solo el 32,83% de las personas de 65 a 74 años contaba con un nivel elevado de competencias digitales, cifra que se reduce al 8% en personas mayores de 75 años. Además, se observan desigualdades de género y nivel educativo, con una brecha de 13 puntos porcentuales entre hombres y mujeres y una diferencia sustancial

entre quienes poseen mayor o menor nivel educativo (Eurostat, 2021). No obstante, Pérez et al. (2024, p.47) indican que la brecha de género en el **uso de internet** finaliza el año 2022 "cuando las mujeres superan muy ligeramente en porcentaje a los hombres (76,4% vs. 76,5%)". Además, en España, el grupo de 65 a 74 años usa Internet más que sus vecinos europeos.

Figura 2. *Uso de internet (últimos tres meses) por sexo.*



Fuente: Adaptado de "Los mayores españoles continúan reduciendo su brecha digital", por A. B. Castillo Belmonte, J. Pérez Diaz, y D. Ramiro, 2023, *Envejecimiento en Red*. https://envejecimientoenred.csic.es/58857-2/

En este contexto, resulta fundamental no solo promover el acceso a la tecnología, sino también garantizar que este acceso se traduzca en un uso seguro y autónomo. En una sociedad cada vez más digitalizada, fomentar la inclusión digital de los colectivos en situación de vulnerabilidad cobra especial relevancia. Las personas mayores, en particular, no solo enfrentan barreras de acceso y aprendizaje, sino que también son más susceptibles a riesgos asociados al entorno digital, como la ciberdelincuencia.

Además, la digitalización no debe entenderse como un proceso sin alternativas (Agencia Española de Protección de Datos, 2024). La apuesta por los medios digitales para la prestación de servicios no puede implicar la desaparición de opciones no digitales, especialmente cuando estas son claves para garantizar la no discriminación, la capacidad de obrar y la autonomía de colectivos vulnerables como las personas mayores. Una digitalización mal implementada, basada únicamente en plataformas digitales, puede generar exclusión por falta de acceso a dispositivos, conocimientos técnicos o confianza, lo que obliga a muchas personas mayores a depender de terceros, comprometiendo su privacidad y autonomía.

La estrategia España Digital 2026 impulsa el uso de tecnologías avanzadas, pero debe respetar el Reglamento General de Protección de Datos (RGPD), evitando que esta transformación excluya a quienes no pueden adaptarse con la misma rapidez. Las administraciones y empresas tienen la obligación de ofrecer alternativas accesibles no digitalizadas, sin trasladar la responsabilidad de adaptación a los ciudadanos. Solo así puede garantizarse que la digitalización sea realmente inclusiva, eficaz y adecuada para todas las personas.

Por ello, la reducción de la brecha digital no debe entenderse únicamente como una cuestión de equidad, sino también como una condición necesaria para proteger los derechos de las personas mayores en el entorno digital. En consonancia con esta visión, la ciberseguridad se ha convertido en una preocupación prioritaria tanto a nivel nacional como internacional. Los desafíos derivados de la transformación digital exigen una ciudadanía resiliente, capaz de adaptarse a los cambios tecnológicos sin quedar expuesta a nuevas formas de vulnerabilidad (Torres Vargas, 2023). En este marco, el Gobierno de España ha intensificado sus esfuerzos mediante políticas públicas orientadas a reforzar la resiliencia digital y a reducir los riesgos asociados a las amenazas cibernéticas, con especial atención a los colectivos más frágiles (Borredá & González Herrero, 2024).

4.2. Ciberdelincuencia: concepto, tipologías y retos en el entorno digital

En el Informe sobre Cibercriminalidad en España (2023) se define la cibercriminalidad como:

> El conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo (Muniesa et al., 2023).

Por otro lado, la **concienciación sobre la ciberseguridad** (del inglés *cibersecurity awareness*) se refiere a la familiaridad de un individuo con temas relacionados con la seguridad en línea, como las últimas amenazas de seguridad, las mejores prácticas en ciberseguridad y los riesgos asociados con comportamientos peligrosos, como hacer clic en enlaces maliciosos, descargar archivos infectados, interactuar con desconocidos en línea o compartir información personal, entre otros (Buja et al., 2024).

A rasgos generales, existen dos tipos de amenazas diferenciadas en el ámbito del ciberespacio. Por un lado, los **ciberataques**, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos; los ataques de ransomware (secuestro de datos) o la denegación de servicio, entre otros. Por otro lado, el **uso del ciberespacio para realizar actividades ilícitas**, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización.

En la era digital, los ciberataques representan una amenaza constante para toda la sociedad, y aunque las personas mayores no son el grupo más afectado en términos absolutos, sí constituyen un colectivo especialmente vulnerable. Aunque otros grupos de edad utilizan más la tecnología y, en términos porcentuales, acumulan un mayor número de víctimas, las personas mayores siguen siendo un objetivo frecuente de los ciberdelincuentes. Esto se debe a que, en muchos casos, cuentan con menos experiencia en el uso de la tecnología y tienden a confiar más en correos electrónicos y mensajes no solicitados, lo que aumenta su nivel de riesgo.

El Ministerio del Interior ha establecido la siguiente tipología de delitos (ver Tabla 1), basada en el Convenio de Budapest de 2001 y ampliada según las necesidades generadas por los constantes avances tecnológicos, que utiliza en sus informes anuales sobre el estado de la cibercriminalidad en el país.

Tabla 1. Módulo de consulta de cibercriminalidad

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	Descubrimiento/Relevación de secretos
		Descubrimiento y relevación de secretos e informaciones relativas a la defensa nacional
		Acceso ilegal a sistemas informáticos
		Interceptación trasmisiones no públicas de datos informáticos
		Facilitación de dispositivos, programas o claves para acceder ilegalmente a datos o sistemas informáticos
		Sexting
		Otros relativos al mercado/consumidores
Interferencia en los datos y en el sistema	Arts. 263 a 267. Daños y daños informáticos	Daños
		Facilitación de dispositivos, programas o claves para cometer ataques informáticos
		Ataques a datos o programas informáticos
		Ataques a sistemas informáticos
Falsificación informática	Arts. 386 al 403.	Falsificación de moneda, sellos y efectos timbrados
		Falsificación/tráfico tarjetas de crédito y débito/cheques viaje
		Falsificación/tráfico de DNI/Pasaporte
		Otras falsificaciones documentos
		Fabricación/tenencia de útiles para falsificar
		Usurpación de estado civil
		Usurpación de funciones públicas
		Intrusismo
Fraude informático	Arts. CP 248 a 251.	Estafa bancaria (hasta 2021)
		Estafas con tarjeta de crédito, débito y cheques de viaje (248.2.c CP)
		Otras estafas
		Estafa de inversores
		Estafas informáticas (arts. 248.2.a.b CP)
Delitos sexuales	Arts. CP 178 a 189.	Agresión sexual
		Agresión sexual con penetración
		Abuso sexual (hasta 07/10/2022)
		Abuso sexual con penetración (hasta 07/10/2022)
		Delito de contacto mediante tecnología con menor de 16 años con fines sexuales (grooming)

		Acoso sexual
		Exhibicionismo
		Provocación sexual
		Corrupción de menores/con discapacidad/diversidad funcional
		Delitos relativos a la prostitución
		Pornografía de menores
Contra la propiedad industrial/intelectual	Arts. 270 a 277 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	Delitos contra la propiedad intelectual
		Delitos contra la propiedad industrial
		Acceso fraudulento a servicios de radiodifusión/TV/otros
		Delito de espionaje industrial y secreto profesional (278 a 280 CP)
Contra el honor	Arts. 205 a 210 del Código Penal.	Calumnias
		Injurias
		Injurias y calumnias a funcionario público, autoridad o agente de la autoridad (205 y 215 CP)
Amenazas y coacciones	Arts. 169 a 173 del C. Penal.	Amenazas
		Amenazas a grupo étnico, cultural o religioso
		Coacciones
		Extorsión
		Trato degradante
		Acoso laboral y funcionarial
		Acoso contra la libertad de las personas
		Perfiles falsos con fines de acoso (hostigamiento/humillación)

Fuente: Adaptado de “Informe sobre la cibercriminalidad en España”, por P. Muniesa Tomás, D. Herrera Sánchez, J. Guerrero Olmos, F. Martínez Moreno, M. Rubio García, V. Gil Pérez, A. M. Santiago Orozco, M. A. Gómez Martín, 2023, *Ministerio del Interior. Gobierno de España.*

Dentro del fraude informático, que como se mostrará más adelante con datos, es inequívocamente la forma de cibercrimen más cometida, destacan los siguientes delitos por su incidencia e impacto, por lo que deben ser tenidos en especial consideración al diseñar los programas de acompañamiento:

- **El timo del familiar necesitado**:

Este fraude consiste en recibir una llamada o mensaje de texto de un supuesto familiar cercano (como un hijo o un nieto) que dice estar en una emergencia y necesita dinero urgente. Las personas estafadoras suelen utilizar artimañas para que la historia suene creíble, como alegar que el familiar ha perdido su teléfono. La víctima se siente presionada a actuar rápidamente y transferir dinero sin pensar demasiado.

- **El fraude del técnico informático**:

En este timo, el delincuente se hace pasar por un técnico informático que contacta a la víctima para informarle de problemas detectados en su dispositivo. El supuesto técnico ofrece solucionar el problema de forma remota, pero para ello solicita acceso al equipo o información personal sensible. Una vez obtenida la autorización, instala malware o roba datos bancarios, pudiendo incluso vaciar las cuentas de la víctima.

- **Phishing y sitios web fraudulentos**:

Los ciberdelincuentes envían un correo electrónico o mensaje de texto que parece provenir de una entidad confiable, como un banco o la Agencia Tributaria. El mensaje incluye un enlace para "actualizar" o "verificar" datos personales. Si la víctima hace clic en el enlace, es redirigida a un sitio web falso que se asemeja a una página legítima, donde entrega sus datos, los cuales luego son utilizados para cometer fraudes.

- **Ciberestafas en redes sociales**:

Los estafadores crean perfiles falsos en redes sociales para engañar a las personas, haciéndose pasar por conocidos o instituciones confiables. A través de mensajes privados, intentan robar dinero u obtener información personal. Estos fraudes incluyen solicitudes de dinero urgentes o engaños como clics en enlaces fraudulentos.

- **Las estafas románticas**:

Este fraude se basa en la creación de perfiles falsos en plataformas de citas o redes sociales. Los delincuentes, que se presentan como personas atractivas y encantadoras, inician una relación sentimental con la víctima. Una vez ganada su confianza, utilizan excusas para solicitar dinero o información personal que luego es utilizada para su beneficio.

- **Timos de inversión**:

En este timo, los ciberdelincuentes se presentan como asesores financieros o empresas que ofrecen una oportunidad de inversión "segura" y con altos rendimientos. Presionan a las víctimas para que inviertan rápidamente, sin tiempo para investigar. Al final, la "inversión" resulta ser una estafa, y la víctima pierde su dinero sin recibir ninguna rentabilidad.

4.3. Incidencia de la ciberdelincuencia: datos y estadísticas

El empleo de términos como “delincuencia informática”, “cibercriminalidad”, “delitos informáticos”, etc., se ha convertido en una constate en nuestra sociedad actual. El nacimiento y la rápida difusión de las redes informáticas están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento en España. Es por todo ello que se necesita medir y contabilizar todos estos parámetros para controlar y tener unos datos precisos.

En este sentido, según el Sistema Estadístico de Criminalidad (SEC), la cibercriminalidad ha ido creciendo de manera incremental año tras año, como se demuestra con el aumento del número de hechos conocidos y su peso proporcional en la delincuencia en general (subiendo casi 10 puntos porcentuales en un período de 4 años).

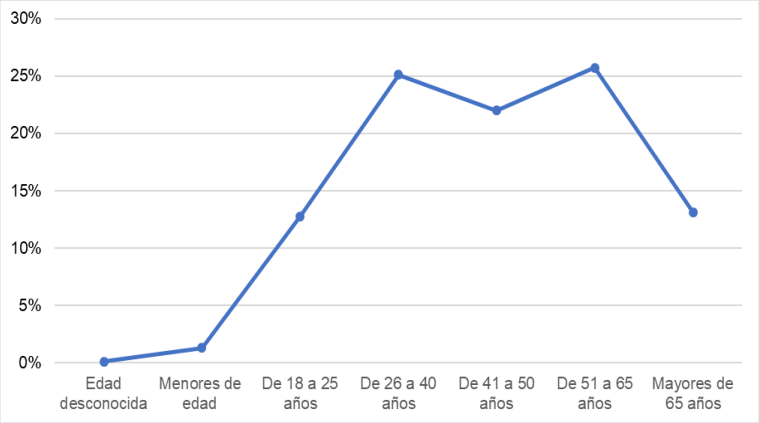
Tabla 2. *Porcentaje de la cibercriminalidad sobre el total de infracciones penales*

2019	2020	2021	2022	2023
9,9%	16,3%	15,6%	16,1%	19,2%

Fuente: Adaptado de “Informe sobre la cibercriminalidad en España”, por P. Muniesa Tomás, D. Herrera Sánchez, J. Guerrero Olmos, F. Martínez Moreno, M. Rubio García, V. Gil Pérez, A. M. Santiago Orozco, M. A. Gómez Martín, 2023, *Ministerio del Interior. Gobierno de España.*

En 2023, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 354.610 casos, es decir, un 18,9% más que en el año 2022; de las que un 49,3% pertenecen al sexo masculino y un 50,7% al sexo femenino. La mayoría de las víctimas de ciberdelincuencia se sitúa entre 26 a 40 años en ambos sexos, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y falsificación informática.

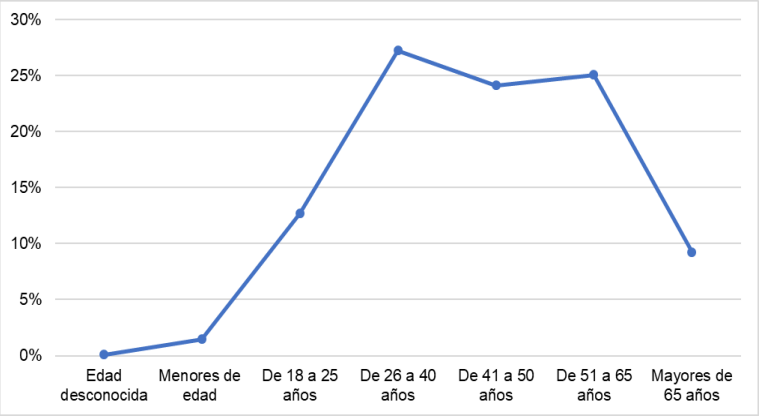
Figura 3. *Víctimas de cibercrímenes por grupo de edad (hombres).*



Grupo de edad	Víctimas
Edad desconocida	159
Menores de edad	2.238
De 18 a 25 años	22.286
De 26 a 40 años	43.843
De 41 a 50 años	38.428
De 51 a 65 años	44.921
Mayores de 65 años	22.895
Total	174.770

Fuente: Adaptado de "Informe sobre la cibercriminalidad en España", por P. Muniesa Tomás, D. Herrera Sánchez, J. Guerrero Olmos, F. Martínez Moreno, M. Rubio García, V. Gil Pérez, A. M. Santiago Orozco, M. A. Gómez Martín, 2023, *Ministerio del Interior. Gobierno de España.*

Figura 4. *Víctima de cibercrímenes por grupo de edad (mujeres).*



Grupo de edad	Víctimas
Edad desconocida	160
Menores de edad	2.651
De 18 a 25 años	22.841
De 26 a 40 años	48.973
De 41 a 50 años	43.382
De 51 a 65 años	45.049
Mayores de 65 años	16.650
Total	179.906

Fuente: Fuente: Adaptado de "Informe sobre la cibercriminalidad en España", por P. Muniesa Tomás, D. Herrera Sánchez, J. Guerrero Olmos, F. Martínez Moreno, M. Rubio García, V. Gil Pérez, A. M. Santiago Orozco, M. A. Gómez Martín, 2023, *Ministerio del Interior. Gobierno de España.*

Uno de los documentos más relevantes en cuanto al análisis de la cibercriminalidad a nivel nacional es el **Informe sobre la Cibercriminalidad en España**, reporte oficial elaborado por el **Ministerio del Interior** que ofrece un análisis detallado sobre los delitos cometidos a través de medios informáticos en el país. Este informe se publica **anualmente** y recopila datos de todas las **fuerzas y cuerpos de seguridad** del Estado (Policía Nacional, Guardia Civil, cuerpos policiales autonómicos y locales), así como de la colaboración internacional.

Dichos informes recogen, entre otras cosas, la incidencia de los cibercrímenes en cada año, diferenciando entre los tipos de delitos. En el informe más reciente al que se ha tenido acceso (2023), el número de casos total fue 472.125, dividido en:

- Fraude informático: 427.448
- Amenazas y coacciones: 17.472
- Falsificación informática: 15.137
- Acceso e interceptación ilícita: 7.367
- Contra el honor: 1.174
- Delitos sexuales: 1.804
- Interferencia en los datos y en el sistema: 1.659
- Contra la propiedad industrial/intelectual: 64
- Delitos contra la salud pública: 0

Aunque no se ha logrado hallar la incidencia específica de cada tipo de delito por grupo de edad, es de entrada destacable la inequívoca predominancia del fraude informático, que representa por sí solo un 90% del total de los casos del 2023. Es, pues, razonable pensar que los delitos que afectan a las personas mayores pertenecen también principalmente a este ámbito.

Según un estudio de 65YMÁS (2024) sobre ciberseguridad basado en una encuesta a 3.210 personas mayores, el 84% de los encuestados manifestaba temer caer en estafas en línea. Aunque solo el 21,8% admitía haber sido víctima de este tipo de fraudes, el porcentaje aumentaba al 28,2% en el grupo de 80 a 89 años.

Asimismo, la exploración cualitativa del contenido de los programas de atención y formación a las personas mayores que han desarrollado entidades financieras (La Caixa, BBVA, entre otras) y empresas de telecomunicaciones (como Orange y Telefónica) refuerza esta conclusión. Así, la gran mayoría de cursos hacen referencia al fraude informático en sus diferentes formas, y no cubren en profundidad otro tipo de delitos.

La importancia estadística del fraude informático tiene consecuencias más allá de indicarnos el tipo de delitos a los que se enfrentan las personas mayores. Como se detallará más adelante, haber sido víctima de un fraude, ya sea presencial o informático, viene asociado a una serie de estereotipos y percepciones negativas, como que la víctima es estúpida o irresponsable. Esto aplica tanto a la sociedad en general como a las propias víctimas, que tienden a sentirse avergonzadas o culpables y ocultan el crimen a sus familias y entorno cercano, especialmente porque temen que se asocie el delito a unas menores capacidades debido a su edad. Esto lleva, como varios autores han apuntado en las últimas décadas (Mason & Benson, 1996; Rebovich & Layne, 2000; Schoepfer & Piquero, 2009; Titus et al., 1995), a que el fraude sea un delito muy poco reportado en comparación a otros crímenes. Se estima que la falta de denuncias es aún más significativa en el caso del fraude informático (Smith, 2007).

4.4. Más allá del daño visible: el impacto integral de la victimización en el cibercrimen

4.4.1. Huella integral de la victimización

El cibercrimen no se reduce al robo digital o a la pérdida monetaria; constituye una forma de agresión que puede desencadenar consecuencias profundas en diversos ámbitos de la vida de la víctima. Estas repercusiones abarcan lo económico, lo psicológico, lo relacional, lo profesional y hasta lo identitario, generando un conjunto complejamente entrelazado de daños que superan el mero costo financiero.

En primer lugar, el **impacto económico** suele percibirse como la consecuencia más tangible del cibercrimen: pérdidas directas de dinero, robos bancarios, fraudes con tarjetas o compras online fraudulentas. Según el informe Economic Impact of Cybercrime – No Slowing Down del CSIS, se estima que el cibercrimen cuesta globalmente unos 600 mil millones de dólares al año, casi un 1 % del PIB mundial. Sin embargo, este dato es solo la punta del iceberg, porque también hay un conjunto de costes indirectos que muchas veces no se cuantifican: gastos legales, recuperación forense de datos, adquisición de nuevas defensas digitales, pérdida de productividad por el tiempo invertido en la resolución del incidente, entre otros. En algunos casos, la victimización cibernética incluso puede afectar el historial financiero del individuo: si alguien usa la identidad de la víctima para contraer deudas, esto puede dejar registros negativos que persistan a largo plazo. Tanto las actuaciones de la administración pública como de los bancos, e incluso de la comunidad académica, han tendido a centrarse en las repercusiones económicas de los crímenes, obviando las consecuencias mentales y psicológicas de estos, que pueden llegar a ser devastadores en función de la gravedad y alcance del crimen y del perfil de la persona.

La victimización digital comporta un **impacto psicológico y emocional** profundo que, en numerosos casos, iguala o supera el asociado al delito tradicional. La literatura reciente documenta ansiedad, miedo, insomnio, depresión, vergüenza y rumiación, así como síntomas somáticos relacionados con el estrés (Randa & Reyns, 2020; Morales & Salas, 2020). En fraudes interpersonales (por ejemplo, romance scams) se observan culpa y estigmatización autoimpuesta, que dificultan la denuncia y prolongan el malestar (Whitty, 2018; Drew, 2024).

Aplicaciones teóricas como la de las “suposiciones fracturadas” ayudan a explicar cómo el ataque quiebra esquemas básicos de seguridad y control, provocando una crisis cognitivo-afectiva que se traduce en hipervigilancia y retraimiento digital (Hengstler et al., 2020). Investigaciones recientes confirman que la victimización cibernética se asocia a afectación emocional significativa, con diferencias según tipologías (p. ej., sextorsión, suplantación,

intrusiones) y factores personales y circunstanciales (Borwell, 2025; Cross, 2025; Tavakoli, 2024). En identidad robada, además del perjuicio económico, son frecuentes la irritabilidad, la desconfianza generalizada y la sensación de vulnerabilidad, con manifestaciones físicas (insomnio, fatiga) que agravan el cuadro (Irvin-Erickson, 2024; Randa & Reyns, 2020).

A este respecto, **hay que entender que la victimización**, entendida como el proceso mediante el cual una persona se percibe a sí misma como víctima de un crimen o maltrato, es una realidad eminentemente subjetiva, que se ve mediada por las creencias y habilidades de la víctima. El efecto y el impacto de la victimización varía según el crimen, pero también por las características individuales de la persona, incluyendo edad, género e ingresos (Button et al., 2014; Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Las mujeres, por ejemplo, son más propensas a sufrir más o peores efectos psicológicos que los hombres, al menos en crímenes financieros "presenciales". Shapland y Hall (2007) también comentan que las circunstancias domésticas y vitales de la persona tienen un papel en la manera como se produce la victimización.

La falta de atención al **impacto emocional del crimen** tiene que ver con la percepción social de que los cibercrímenes tienden a ser de bajo impacto y a no generar víctimas (Button et al., 2014). Así, la población general suele tener la idea de que los cibercrímenes son básicamente casos de uso fraudulento de tarjetas de crédito, en los que las víctimas son compensadas por sus pérdidas por parte de las instituciones financieras. Alternativamente, en los casos más graves, suelen pensar que el robo o fraude ha sido cometido en contra de grandes empresas o personas ricas, que en cualquier caso pueden permitirse hacer frente a las repercusiones. Sin embargo, estas percepciones suponen una idea muy equivocada de la realidad de las víctimas de los ataques de la ciberdelincuencia.

De esta manera, al margen del impacto económico del crimen, es indudable que la victimización supone una **carga emocional y psicológica**. Satchell (2023) identifica un total de 31 consecuencias a partir de la revisión de 21 artículos académicos: sentimiento de molestia, susto, incredulidad, llanto, vergüenza, fatiga, falta de sueño, pensamientos intrusivos, sentirse vulnerable, inseguridad, ira, molestia, irritación, trastorno de estrés postraumático, miedo a ser víctima más delitos, miedo a salir/agorafobia, miedo a quedarse solo/a, concentración deteriorada, ansiedad, depresión, autoestima reducida, pérdida de confianza/desconfianza, pérdida de seguridad, vergüenza, escepticismo, recuerdos retrospectivos, estrés, ataques de pánico, autoculpa, conmoción y cambios de comportamiento.

En el caso de las víctimas de delitos de fraude o robo, como es el caso de muchas personas mayores, son predominantes la culpabilidad, la vergüenza y el hecho de sentirse "estúpido/a".

Además, es habitual que estas manifiesten sentimientos de frustración hacia los bancos a los que se dirigen tras el delito, o hacia la aseguradora contactada, en caso de que contaran con una póliza que les cubriera ante el delito sufrido. Lo mismo sucede con la administración pública, en estos casos principalmente la policía nacional, pero puede haber otras agencias implicadas, donde la respuesta no es lo suficientemente efectiva o satisfactoria para las víctimas. Esto se conoce como **victimización secundaria**, que ocurre cuando la persona que ya ha sido víctima de un hecho traumático se enfrenta a una revictimización por parte de la sociedad, instituciones o incluso seres cercanos.

Aparte de la culpabilidad y la vergüenza, las víctimas de fraudes a menudo reportan una disminución significativa en su **autoestima** y **confianza**. La sensación de haber sido engañadas por una institución en la que confiaban previamente, como un banco o una aseguradora, puede hacer que se cuestionen su capacidad para tomar decisiones, lo que lleva a una **desconfianza generalizada**. Esta pérdida de confianza puede extenderse a otros aspectos de sus vidas, como sus relaciones personales y su capacidad para gestionar sus finanzas. Los efectos a largo plazo también pueden incluir **ansiedad** y **depresión**, condiciones que pueden agravarse si la víctima no recibe el apoyo adecuado (Havers et al., 2024). Las personas mayores, en particular, pueden ser más propensas a experimentar **estrés postraumático** debido a las malas experiencias con el sistema de apoyo, lo que puede tener repercusiones duraderas en su bienestar emocional (Satchell, 2023).

El **estrés** generado por ser víctima de un fraude también puede desencadenar reacciones fisiológicas, como problemas digestivos, dolores de cabeza y tensión muscular. Estos síntomas, que a menudo no son reconocidos como consecuencia del trauma psicológico, contribuyen a un **círculo vicioso de malestar físico y emocional**. Las personas mayores, debido a sus posibles problemas de salud preexistentes, pueden ser más susceptibles a estos efectos físicos, lo que afecta negativamente su calidad de vida. La falta de sueño y la fatiga, por ejemplo, son comunes entre las víctimas de fraude, quienes pasan noches inquietas pensando en el fraude o preocupándose por las consecuencias de haber sido engañadas (Havers et al., 2014).

Button et al. (2014) y Cross y Button (2017) comentan que el hecho de que existan múltiples agencias u organizaciones, tanto de carácter público como privado, que participan en la atención a las víctimas en caso de fraude contribuye a la falta de una respuesta efectiva a las necesidades de la población. Es habitual que se produzca **el efecto "merry-go-round**"; donde los diferentes organismos (bancos, cuerpos policiales, servicios de atención ciudadana, etc.) **eludan responsabilidad y van redirigiendo a la persona de un servicio a otro, sin que esta reciba una respuesta adecuada.**

Este impacto psicológico y emocional se proyecta en la **esfera social y relacional**, alimentando el aislamiento, la reducción de la huella digital y la desconfianza hacia plataformas y servicios. La evidencia muestra que el miedo al cibercrimen puede desalentar la participación en entornos digitales, con costes sociales (menos acceso a oportunidades, redes y servicios) y efectos desiguales en grupos con menos competencias digitales (Oksanen et al., 2022). En ciertos delitos con fuerte dimensión interpersonal (p. ej., sextorsión), se añaden dinámicas de estigma y victimización secundaria, especialmente en adolescentes y jóvenes, donde se reportan incrementos de casos y la utilización de técnicas de ingeniería social cada vez más sofisticadas, a veces potenciadas con IA (EU Parliament/EPRS, 2024; IWF, 2024). Esta desconfianza no solo afecta a "extraños" o a las plataformas: puede tensar vínculos familiares o de pareja, sobre todo si se comparten dispositivos o contraseñas, y si aflora el reproche ("¿cómo te ha podido pasar?"), que dificulta la búsqueda de apoyo y la denuncia.

En este sentido, múltiples estudios apuntan que los cibercrímenes causan cambios en el comportamiento de las víctimas, incluyendo evitar la banca en línea, evadir llamadas de personas no identificadas y aumentar la seguridad del hogar (Bailey et al., 2020; Qin & Yan, 2018; Tripathi et al., 2019). De manera general, estos cambios son hacia comportamientos de evitación, un fenómeno observado en contextos socioculturales tan diversos como Estados Unidos (Reisig et al., 2017) o China (Qin & Yan, 2018).

No obstante, el **impacto social y relacional** de la ciberdelincuencia constituye una esfera autónoma de vulnerabilidad que altera los modos de relación, pertenencia y participación comunitaria en entornos digitales. Diversos estudios muestran que el miedo al cibercrimen erosiona la confianza interpersonal y social, reduciendo la disposición a interactuar o compartir información en línea, lo que limita el acceso a redes, servicios y oportunidades (Oksanen et al., 2022). Este impacto se traduce también en cambios conductuales orientados a la evitación, como restringir el uso de la banca electrónica, evitar llamadas de desconocidos o reforzar la seguridad doméstica (Bailey et al., 2020; Qin & Yan, 2018; Tripathi et al., 2019). Dichas conductas de autoprotección, observadas en contextos tan diversos como Estado Unidos o China (Reisig et al., 2017; Qin & Yan, 2018), evidencian una reorganización social basada en la desconfianza y la reducción de la huella digital.

Al mismo tiempo, la ciberdelincuencia produce tensiones en los vínculos más próximos. En los delitos con una marcada dimensión interpersonal (como la sextorsión o la difusión no consentida de imágenes), estas fracturas de confianza se amplifican mediante `procesos de estigmatización y victimización secundaria, especialmente entre adolescentes y jóvenes, en un contexto donde proliferan las técnicas de manipulación emocional y de ingeniería social

potenciadas por IA (EU Parliament/EPRS, 2024; IWF, 2024). En conjunto, este impacto relacional no se limita a la pérdida de seguridad individual: transforma la arquitectura de la confianza social y condicional la capacidad colectiva para construir entornos digitales seguros, empáticos y cohesionados.

En el **terreno identitario y de la autoestima**, episodios como la suplantación de identidad, la filtración de datos sensibles o la difusión no consentida de contenidos íntimos erosionan el "yo digital" y precipitan estrategias defensivas (cierre de cuentas, cambio de alias, desaparición temporal de redes) que, si bien protectoras, empobrecen la agencia digital de la persona. La investigación internacional constata que la sextorsión se vincula a depresión, ansiedad, vergüenza e hipervigilancia, con afectación de la autoimagen y del sentido de control sobre la propia narrativa online (Tavakoli, 2024; Henry et al., 2024). Estas trayectorias se agravan en colectivos vulnerables (p. ej., menores, personas con discapacidad o minorías sexuales) que pueden sufrir mayor exposición y menor acceso a recursos de afrontamiento y reparación (Irvin-Erickson, 2025; Henry et al., 2024).

Sin embargo, en una sociedad cada vez más digitalizada como la actual, el resultado de dichas conductas es la disminución de la autonomía de las personas mayores y, consecuentemente, una mayor dependencia de núcleo familiar, si lo tienen; o el desamparo ante la creciente digitalización de la sociedad, si no lo tienen. Hay que recordar que el acceso y uso de los medios digitales se está convirtiendo en una condición inevitable para el ejercicio de la ciudadanía en plenas facultades y las conductas evitativas suponen la desconexión de la vida pública en muchos aspectos.

Al margen de estos mecanismos de afrontamiento, algunos estudios apuntan a consecuencias psicológicas más graves, como son manifestaciones psicosomáticas de su malestar. Así, Jansen y Leukfeldt (2018) comentan como uno de los participantes en su estudio reportó tener un trauma y haber pasado noches sin dormir: "no es por el dinero, es más bien por mi estupidez". Así, el participante se culpaba a sí mismo por el fraude. Curiosamente, el estudio mencionado sí hace referencia a cibercrimen, en concreto a casos de phishing, lo que sugiere que los efectos psicológicos más nocivos del crimen no están limitados a casos "presenciales" en los que haya habido uso de fuerza y/o forcejeo para cometer el acto.

Otros autores (Whitty & Buchanan, 2016) apuntan que cierto tipo de delitos pueden ser más devastadores que otros. Por ejemplo, una estafa romántica puede suponer un doble golpe, ya que la víctima ha de hacer frente no solo a la pérdida económica, sino también a la pérdida de la relación, pudiendo pasar por un periodo de duelo.

Las **consecuencias legales** del cibercrimen forman parte del impacto global que experimenta la víctima, aunque suelen pasar más desapercibidas que las pérdidas económicas o el daño emocional. La persona afectada se ve obligada a recorrer un camino jurídico complejo que comienza con la denuncia y continúa con la recopilación de pruebas, la espera de respuestas institucionales y, en muchos casos, la frustración ante procesos largos, costosos y con resultados inciertos. Un estudio desarrollado por el Australian Institute of Criminology (2024) mostró que, aunque los efectos legales directos son menos frecuentes que los económicos o psicológicos, representan una carga significativa dentro del conjunto del daño total sufrido por las víctimas, evidenciando que un pequeño porcentaje de ellas concentra la mayor parte del perjuicio.

La dificultad para identificar al agresor, su posible residencia en otro país o su insolvencia económica reducen las posibilidades de obtener justicia o reparación efectiva. Como señalan Borwell, Jansen y Stol (2021), el carácter transnacional del delito y la falta de armonización entre los marcos jurídicos nacionales afectan directamente la capacidad de las víctimas para reclamar responsabilidades o recibir compensación. De hecho, la cooperación internacional sigue siendo limitada a pesar de los esfuerzos impulsados por tratados como el Convenio de Budapest sobre Ciberdelincuencia (United Nations Office on Drugs and Crime [UNODC], 2001), lo que retrasa investigaciones y dificulta la ejecución de sentencias.

Cuando la víctima es una persona mayor, menor de edad o pertenece a un colectivo vulnerable, las barreras se multiplican: la falta de asesoramiento especializado, el miedo a denunciar, la revictimización durante el proceso y la desconfianza en las instituciones. En el caso de jóvenes, Griffith (2023) subraya que los delitos digitales como el ciberacoso, el hacking o la difusión de imágenes íntimas requieren un entorno legal más adaptado y sensible, ya que las víctimas suelen enfrentarse a la estigmatización y ausencia de vías de reparación efectivas.

A lo largo de los procedimientos judiciales pueden prolongar el malestar: la exposición pública, la reiteración de testimonios o la obligación de participar en peritajes y trámites legales añaden estrés y desgaste emocional. Aunque las vías legales ofrecen la posibilidad de indemnización o reparación, para muchas víctimas el proceso se convierte, como advierte Rasiwan (2025), en una segunda forma de victimización, al tener que revivir los hechos y sostener una carga jurídica y emocional difícil de asumir sin apoyo especializado.

En síntesis, el impacto del cibercrimen es **multidimensional, acumulativo e interdependiente**: el daño económico alimenta el malestar emocional; el miedo y el estigma constriñen la participación social; la erosión identitaria empobrece la agencia digital; y las exigencias de continuidad de negocio pueden posponer la reparación psicosocial. De ahí que

las respuestas más eficaces sean integrales: restauración financiera y técnica; acompañamiento psicológico basado en evidencia; reducción del estigma y mejora de la accesibilidad a canales de denuncia; y políticas organizativas que integren seguridad, gobernanza de IA y protección centrada en la persona. Solo así se atiende no solo al delito, sino al sufrimiento, y a los derechos, de las víctimas.

4.4.2. Mecanismos de afrontamiento

Un factor para tener especialmente en consideración son los mecanismos de afrontamiento de las víctimas, que pueden influir tanto de forma positiva como negativa en su proceso de recuperación. Lazarus y Folkman (1984) hacen una distinción entre **estrategias de afrontamiento centradas en el problema, y estrategias de afrontamiento centradas en la emoción**. Las primeras se centran en resolver una situación adversa, atacando directamente la causa del problema o amenaza, mientras que las segundas intentan gestionar las emociones asociadas con la situación, sin tomar medidas directas para solucionar el problema.

Según Lai, Li y Hsieh (2012), existen dos tipos de afrontamiento centrado en el problema dentro del contexto de los sistemas de información:

1. El **afrontamiento tecnológico** implica el uso de tecnologías para prevenir futuros fraudes o protegerse de ellos. Un ejemplo de esta categoría es la instalación o actualización de un software antivirus para proteger los dispositivos de ataques de programa malicioso (*malware*) La víctima utiliza herramientas tecnológicas para defenderse de futuros incidentes de cibercrimen.
2. El **afrontamiento emocional**, que se refiere al comportamiento que una persona realiza sin usar tecnología, como verificar el saldo de una cuenta en busca de posibles inconsistencias. Un ejemplo es la acción de verificar regularmente el saldo de una cuenta bancaria o las transacciones realizadas, con el fin de detectar irregularidades o inconsistencias que puedan indicar un fraude. Este tipo de afrontamiento es más directo y no depende de la tecnología, sino de comportamientos que pueden resultar en una mayor vigilancia de las actividades financieras personales.

Las estrategias centradas en el problema son especialmente útiles cuando la persona cree que puede controlar o modificar la situación. En estos casos, las víctimas de fraude cibernético pueden sentir que tienen control sobre el riesgo y que sus acciones pueden mitigar la amenaza futura. Sin embargo, estos mecanismos de afrontamiento pueden ser insuficientes si no se cuenta con la formación o las herramientas adecuadas para

implementarlos, lo que podría llevar a las víctimas a sentirse desbordadas por la situación y a recurrir a otros mecanismos.

Satchell (2023) realizó un estudio en el Reino Unido con una muestra de 100 personas de entre 65 y 89 años (2/3 siendo mujeres) en el que analizaba los comportamientos de personas mayores que habían sido víctimas de crimen (en este caso, crimen en general; no cibercrimen en específico) para diseñar una escala de comportamiento de "búsqueda de seguridad" (Patient Reported Safety-Seeking Behaviour Measure). A pesar de las posibles limitaciones del estudio, como el hecho de que se entrevistaran únicamente personas con un perfil clínico, resulta interesante poder valorar los ítems que define para esta escala, ya que nos indican comportamientos que son asumidos por víctimas mayores.

Tabla 3. *Ítems de la Escala de Comportamientos de Búsqueda de Seguridad.*

Comprobación	En este contexto, se refiere a la verificación excesiva del entorno externo (Strauss et al., 2020). Las personas comprueban repetidamente cuando no están seguras de que el daño potencial haya sido eliminado o corregido, incluso cuando son conscientes de que esto no es racional (Rachman, 2002).
Búsqueda de validación/ confianza	Se define como la acción repetida de buscar información de seguridad de otras personas sobre un tema de preocupación, a pesar de que ya se haya recibido dicha información (Parrish & Radomsky, 2010).
Rumiado	Se define como pensar repetidamente sobre situaciones pasadas o futuras, con exageraciones de los problemas percibidos, tratando de sentir control (Douglas et al., 1998; Nolen-Hoeksema, 2003). Esto se incluyó como un comportamiento de seguridad tanto cognitivo como conductual (Rachman & Hodgeson, 1980).
Evitación	Se define como intentos constantes y persistentes de evitar estímulos asociados con factores temidos, como factores externos (por ejemplo, personas o lugares) e internos (por ejemplo, recuerdos) (Perrotta, 2019). Esto se ha informado previamente en víctimas mayores (Triganti et al., 2019; Reiss et al., 2017) y trabajadores en contextos vulnerables (Dumore, Ehlers & Clark, 2001).
Rituales	Los rituales fueron incluidos en mi estudio de doctorado observando víctimas mayores que informaron preparaciones antes de salir de casa (Sachat et al., 2023). Un término más amplio fue utilizado para abordar tanto prácticas religiosas (Yaden et al., 2020) como prácticas no religiosas, como supersticiones (Poonam & Triganti, 2023).
Hipervigilancia	Se define como un aumento en la atención para asignar recursos atencionales al entorno con el fin de detectar amenazas (Bar-Haim et al., 2007).
Hacer las cosas de manera diferente	Esto fue recomendado por un miembro de un estudio del NIHR-BRC for Public and Patient Involvement (PPI) que informó que había comenzado a llevar su bolsa/o en un lugar diferente.

Fuente: Adaptado de "Older Victims of Community Crime: Psychological Impact and Coping", por J. Satchell, 2023, *University College London*.

Todos estos componentes son perfectamente transferibles y aplicables en el ámbito exclusivo de la tecnología. A pesar del impacto inicialmente positivo de estos mecanismos, son prácticas que, a la larga, contribuyen a mantener a las personas en un estado de victimización, impiden su recuperación y las vuelven dependientes de su entorno social y familiar (Satchell, 2023).

Por otro lado, las estrategias centradas en la emoción buscan modificar los sentimientos o emociones no deseadas hacia un problema o amenaza, tales como el estrés, la ira, el miedo, la tristeza o la impotencia, sin tomar acción directa contra la causa. Entre los ejemplos de estas estrategias se incluyen técnicas cognitivas como la evasión, el distanciamiento emocional y la atención selectiva, así como estrategias conductuales como la meditación, buscar apoyo emocional o consumir alcohol (Lazarus & Folkman, 1984). Aunque no alteran la realidad objetiva, estas estrategias ayudan a las personas a manejar sus emociones y reducir el malestar emocional (Green et al., 2010), lo que también es esencial para un afrontamiento efectivo (Lazarus & Folkman, 1984). No obstante, estas estrategias pueden generar una visión distorsionada de la realidad (Liang & Xue, 2009).

El afrontamiento centrado en la emoción tiende a ser más frecuente cuando se percibe que no hay nada que hacer frente a una situación, mientras que el centrado en el problema es más probable cuando se considera que la situación puede ser modificada o controlada (Lazarus & Folkman, 1984). Según Liang y Xue (2009), las personas racionales suelen preferir el afrontamiento centrado en el problema porque poseen el conocimiento y las habilidades necesarias para abordarlo. Sin embargo, si no encuentran una solución efectiva o recurren a una medida inadecuada (como un antivirus incapaz de detectar nuevas variantes de malware), se verán forzadas a utilizar una estrategia centrada en la emoción para mantener un nivel adecuado de bienestar psicológico. Estas estrategias no son mutuamente excluyentes; de hecho, pueden complementarse. Aunque la estrategia centrada en el problema suele ser preferida, pues se percibe como más significativa tomar medidas frente a una amenaza que cambiar la interpretación de la situación (Liang & Xue, 2009), las estrategias centradas en la emoción siguen siendo muy relevantes para un afrontamiento adecuado.

La literatura también indica que los efectos psicológicos del crimen son potencialmente mitigados por una **red de apoyo social,** que ha sido identificada como uno de los factores determinantes para un afrontamiento positivo y sano ante la victimización (Frieze et al., 1987). En este sentido, Reisig et al. (2017) llegan a la conclusión de que los síntomas de depresión tras un crimen fueron más leves en aquellas personas mayores que tienen una fuerte

vinculación o conexión con su cónyuge o con hijos/as adultos/as. No obstante, conviene señalar que las mismas redes familiares y sociales que pueden favorecer la recuperación emocional también pueden actuar como un factor de riesgo. En algunos casos, las reacciones de incomprensión, juicio o minimización por parte del entorno cercano pueden intensificar el sentimiento de vergüenza y aislamiento de la víctima, dificultando la búsqueda de apoyo y la superación de la experiencia traumática. De ahí la necesidad de trabajar la dimensión emocional y relacional de la prevención, creando espacios donde puedan compartir experiencias sin juicio ni culpa.

Asimismo, Jansen y Leukfeldt (2018) ponen el foco en la importancia de hablar sobre la experiencia del crimen, lo que puede tener un efecto terapéutico en la víctima. A este respecto, los autores apuntan una serie de recomendaciones y consideraciones a ser aplicadas por los bancos, policía y otras posibles organizaciones que atienden a las víctimas, que se pueden resumir en dos enfoques generales:

- Adoptar una actitud de apoyo, mostrando empatía y comprensión y evitando juzgar o culpar a la víctima.
- Dar actualizaciones constantes sobre el caso de cada persona, contribuyendo a que las víctimas se sientan escuchadas, reconocidas, a la vez que protegidas y cuidadas.

Por otro lado, la relevancia de las relaciones sociales en la reducción del impacto negativo de los cibercrímenes choca con la aparente desestimación de la población general respecto a la ciberdelincuencia, **que es percibido como algo muchas veces inofensivo**. Así pues, se hace evidente la necesidad de incidir en mayor medida en la población en general, **no solo en labores de prevención, sino también en la concienciación sobre los delitos, su incidencia real y sus varios impactos.**

En el caso de las personas mayores, las estrategias de afrontamiento tienden a ser menos efectivas y, en muchos casos, contribuyen a una mayor victimización o previenen la recuperación (Kemp & Erades Pérez, 2023; Satchell, 2023). Esto puede ocurrir debido a una combinación de factores, como la falta de conocimientos tecnológicos, el aislamiento social, o incluso la desconfianza en las instituciones. Muchas personas mayores, después de haber sido víctimas de fraude, **recurren a la evitación, evitando el uso de servicios en línea o desactivando sus cuentas bancarias en línea. Aunque estas estrategias pueden proporcionar un alivio inmediato, a largo plazo pueden limitar su capacidad para interactuar con el mundo digital de manera segura y efectiva.**

Además, las personas mayores pueden ser más propensas a utilizar estrategias centradas en la emoción debido a su mayor vulnerabilidad emocional. Esto puede

llevar a que se distancien de las instituciones o a que se vuelvan más desconfiadas, lo que dificulta aún más su recuperación (Liang & Xue, 2009; Burton et al., 2024).

Ante este panorama, se hace urgente un doble llamamiento (Martínez Souto, 2022). Por un lado, a la comunidad investigadora, para que dirija su mirada hacia estos nuevos fenómenos delictivos que aún permanecen insuficientemente explorados. Por otro, a la sociedad en general, para fomentar una mayor sensibilización frente al sufrimiento de las víctimas y promover una justicia más empática y humana. Solo así podremos hacer frente al proceso de deshumanización que, alimentado por la indiferencia y el egoísmo, amenaza con alejarnos de los valores fundamentales de una convivencia justa y solidaria.

4.5. Conclusiones

La ciberdelincuencia se ha consolidado en España como un fenómeno estructural y en crecimiento que exige una respuesta integral basada en la prevención, la atención a víctimas y la coordinación institucional. En 2023 representó cerca del 19% de las infracciones penales, lo que refuerza la necesidad de métricas sólidas y políticas que compatibilicen digitalización y seguridad ciudadana. El **fraude informático**, que supone en torno al 90% de los casos, centra el principal foco de intervención: estafas de ingeniería social, *phishing*, timos románticos o falsos técnicos. Ante ello, la prevención debe priorizar estos guiones delictivos mediante formación práctica, protocolos de actuación claros y acompañamiento accesible.

Las **personas mayores** constituyen un grupo particularmente vulnerable por la brecha de competencias digitales, la confianza interpersonal y la dependencia creciente de servicios en línea. Estas vulnerabilidades se ven agravadas por el **subregistro de fraudes** y por una respuesta institucional percibida como fragmentada o poco empática. Además de las pérdidas económicas, las consecuencias psicológicas (vergüenza, ansiedad o aislamiento) pueden ser igualmente severas. Por ello, la prevención debe orientarse al empoderamiento, no al miedo, aprovechando las fortalezas y experiencias vitales de las personas mayores.

Una **estrategia preventiva eficaz** y que promueve el **empoderamiento** se sustenta en tres pilares: (1) la formación básica en hábitos seguros, (2) la sensibilización mediante ejemplos y simulaciones, y (3) la existencia de herramientas accesibles de protección y denuncia, tanto digitales como presenciales. La **coordinación interinstitucional** (entre banca, cuerpos de seguridad y servicios de atención) requiere protocolos comunes y canales únicos que eviten la revictimización, garantizando además **alternativas no digitales** para una inclusión plena.

Finalmente, la **evaluación continua** debe considerar no solo la incidencia delictiva, sino también el impacto psicológico y los cambios conductuales de las víctimas. En conjunto, precisa una estrategia sostenida que priorice el fraude informático, sitúe a la víctima en el

centro y asegure que la innovación tecnológica refuerce la autonomía y la confianza social, sin generar nuevas formas de exclusión.

5. Abordaje del cibercrimen en personas mayores: prevención, formación y atención

La ciberdelincuencia se ha consolidado como un fenómeno estructural en España y Europa, con predominio del fraude informático y un impacto creciente en la vida cotidiana, lo que obliga a articular respuestas que combinen alfabetización digital, acompañamiento a víctimas, así como una mejora sustantiva de la coordinación institucional para evitar circuitos de derivación ineficaces y la revictimización secundaria.

El colectivo de personas mayores afronta una vulnerabilidad específica por la convergencia de brechas de competencias, estigma, barreras de acceso y diseños tecnológicos poco inclusivos, junto con patrones de confianza y dependencia de canales digitales para trámites esenciales, circunstancia que incrementa el riesgo de exposición y dificulta la recuperación si no se facilitan apoyos adecuados y opciones no digitales equivalentes en los servicios públicos y privados.

El presente informe propone un marco de abordaje del cibercrimen en personas mayores, desplegado en bloques interdependientes. El bloque inicial analiza críticamente el tratamiento vigente de la ciberdelincuencia en el colectivo sénior, identificando fortalezas y áreas de mejora. El bloque subsiguiente desarrolla y operacionaliza instrumentos pedagógicos para la prevención, la detección y el cuidado conductual, combinando alfabetización digital con apoyos de acompañamiento centrados en la persona.

1. Un primer bloque de **segmentación de la población objetivo** para definir el tipo de intervención y delimitar la teoría alrededor de la formación hacía personas mayores, así como los tipos de ciberdelitos más comunes entre esta población.
2. Un segundo bloque de **marco legislativo y políticas públicas** para situar el abordaje en la intersección entre derechos, protección de datos, estrategias digitales y ciberseguridad, garantizando el principio de no exclusión y la disponibilidad de canales analógicos y accesibles en los servicios esenciales;
3. Un tercer bloque sobre el **cambio de paradigma en el trabajo de prevención para trabajar un modelo integral de prevención, detección temprana y recuperación emocional en ciberseguridad** para las personas mayores, con especial atención a la gestión emocional y al temor a juicios sobre la capacidad.
4. Un cuarto bloque desarrolla **factores de riesgo y protección** integrando dimensiones personales (cognitivas, emocionales y de autoeficacia), contextuales y estructurales (brecha digital, accesibilidad, calidad del apoyo tecnológico recibido) y socioculturales (aislamiento, género, clase social y trayectorias formativas y laborales), con el objetivo

de orientar medidas de mitigación que conviertan el afrontamiento en aprendizaje seguro y no en evitación o dependencia.

5. El quinto bloque describe los **canales de atención**, analizando el rol de fuerzas de seguridad, entidades financieras y administraciones, e introduciendo el diseño de una "ventanilla de referencia" y protocolos interoperables que aseguren detección, acompañamiento empático, contención emocional, asesoramiento financiero-jurídico y reencauzamiento seguro a la vida digital, evitando la fragmentación de recursos y el "merry-go-round" de derivaciones.

Posteriormente, el documento se centra en el diseño y la operativización de acciones formativas que impulsen el empoderamiento de las personas mayores en prevención, detección y acompañamiento, integrando el desarrollo de competencias técnicas en nuevas tecnologías con un cuidado y apoyo integral ante situaciones de riesgo o de posible cibervictimización.

6. El sexto bloque aborda **la prevención y la formación con metodologías prácticas** y accesibles: simulaciones de guiones de fraude más prevalentes, ejercicios de capacitación digital, actividades de gestión del bienestar emocional, y programas de empoderamiento que promuevan independencia frente a apoyos que generan dependencia, todo ello con materiales adaptados para quienes utilizan menos medios digitales.
7. El séptimo bloque **se centra en comunicación y desestigmatización** para aumentar la denuncia y la búsqueda de ayuda, con mensajes que visibilicen el daño psicológico, normalicen la petición de apoyo y ofrezcan instrucciones claras de actuación ante incidentes, reforzando la confianza en los circuitos institucionales y comunitarios.

Este marco reorganiza las prioridades poniendo en primer término el valor añadido del estudio: **desplazar el foco del delito y su coste económico hacia la experiencia integral de la víctima mayor, incorporando diversidad e interseccionalidad, co-diseño con las personas mayores, atención empática** y opciones no digitales equivalentes que garanticen autonomía y dignidad en todo el itinerario de prevención, detección y recuperación.

Sobre esta base, se concreta el diseño de una guía pedagógica aplicada que traduzca los hallazgos en metodologías prácticas, simulaciones de guiones de fraude, protocolos de verificación y materiales en lectura fácil, integrando, junto a las competencias técnicas, pautas de contención emocional, validación sin culpa y rutas claras de ayuda para reducir la evitación y la victimización secundaria. La guía se acompaña de contenidos visuales para la identificación inmediata de agentes de protección (señalética, pictogramas de pasos críticos, etc.) ubicados en equipamientos y centros de personas mayores para activar conductas clave

sin imponer cargas digitales. El conjunto se ancla en una gobernanza y coordinación multi-actor con responsabilidades claras, intercambio de información relevante y tiempos de respuesta medibles. Por ello, se debe ir complementando el papel de los principales responsables en garantizar los derechos de las personas mayores (entidades bancarias, fuerzas de seguridad, administraciones y comunidad) en planes de ciberseguridad con enfoque social y mecanismos de seguimiento que eviten derivaciones circulares y fortalezcan la resiliencia y la autonomía en la era digital de este colectivo.

5.1. Segmentación de la población objetivo

Aunque la revisión de artículos académicos ha señalado que las personas mayores son más susceptibles a los ciberataques, “es importante alejarse de concepciones estereotipadas y edadistas que las presentan como un grupo homogéneo con escasas habilidades en alfabetización digital” (Morrison et al., 2023, p.437). Al igual que otros grupos etarios, la población mayor presenta una **diversidad** significativa en cuanto a sus competencias, conocimientos y comportamientos en el entorno digital.

Esta heterogeneidad cobra todavía más relevancia en un contexto demográfico en transformación. Las proyecciones de población[2] del Instituto Nacional de Estadística (INE, 2024) reflejan un crecimiento significativo de la población mayor de 65 años, que en 2024 representaba el 20,4% del total de la población, es decir, más de 9,5 millones, y se prevé que en 2041 alcance el 27,9% de una población que estará por encima de los 52 millones de habitantes, es decir, unos 14,5 millones de personas mayores. Esta tendencia resalta la importancia de adaptar estrategias de prevención de ciberdelincuencia específicamente para este grupo, considerando tanto su diversidad como su posible vulnerabilidad ante amenazas digitales en constante evolución.

Dentro del colectivo de personas mayores, resulta clave diferenciar entre dos perfiles; teniendo en cuenta en todo momento que no se trata de grupos homogéneos en cuanto a competencias digitales y exposición a riesgos en línea.

En primer lugar, las **personas de 65 a 74 años** (4.773.628 en 2024). Debido a la presencia cada vez más habitual de las nuevas tecnologías, las competencias digitales de las personas mayores de entre estas edades son más elevadas, y están más acostumbradas a disponer de dispositivos móviles, uso del internet, etc. y, por tanto, hay que diferenciarlos del colectivo de edad más elevado. El informe de Somos Digital (2022) indica que el 76,4% de las personas

[2] Las proyecciones de población muestran la evolución que seguiría la población de España en el caso de mantenerse las tendencias demográficas actuales. No constituyen una predicción, en el sentido de que no tienen como objetivo determinar cuál es la evolución más probable (INE, 2024).

entre 65 y 74 años utilizaron internet en los últimos tres meses de 2022. Este porcentaje ha ido en aumento en los últimos años, reflejando una mayor familiaridad con las tecnologías digitales en este grupo de edad.

Por otro lado, las **personas de 74 o más años** (4.705.382 en 2024). Menos habituadas a las nuevas tecnologías y, por tanto, a su uso, no son las principales víctimas estadísticamente hablando, pero son todavía más vulnerables a ser víctimas de ciberdelincuencia por el impacto generado en su calidad de vida. En contraste con el grupo anterior, solo el 35,9% de las personas de 75 años o más utilizaron internet en el mismo período. Esta menor adopción tecnológica sugiere una mayor vulnerabilidad frente a la ciberdelincuencia, ya que la falta de competencias digitales puede dificultar la identificación de amenazas en línea.

Comprender la diversidad interna del colectivo de personas mayores en los dos grupos mencionados, permite diseñar estrategias de prevención más ajustadas y efectivas frente a la ciberdelincuencia atendiendo a las necesidades específicas de cada grupo. Sin embargo, **estas estrategias deben enmarcarse en un contexto normativo sólido que garantice la protección de los derechos digitales y la atención integral a las víctimas**. El desarrollo legislativo en materia de cibercrimen constituye, por tanto, un elemento clave para articular respuestas coherentes entre los ámbitos de la seguridad, la justicia y la inclusión digital. A continuación, se presenta el marco legislativo que regula la ciberdelincuencia y las principales normativas que inciden en la protección de las personas mayores en el entorno digital.

5.2. Marco legislativo y políticas actuales frente al cibercrimen en la población mayor

Aunque los y las ciberdelincuentes suelen enfocarse en personas jóvenes y adultas debido a su mayor actividad en línea, **han encontrado en las personas mayores un objetivo propicio debido a su menor familiaridad con las tecnologías**. Un informe publicado en 2011 por el Instituto Australiano de Criminología (Australian Institute of Criminology) apunta que, pese a que las personas mayores no son el grupo demográfico más afectado ni en términos relativos ni absolutos, el cibercrimen en sus diferentes formas es el delito que más se comete contra el colectivo (Carcach et al., 2011).

Además de las pérdidas económicas, el **impacto** de estos delitos en la **calidad de vida** de las personas mayores es significativo, generando desconfianza, aislamiento social y ansiedad. La falta de competencias digitales y la vergüenza de admitir haber sido víctima de fraude dificultan la denuncia de estos delitos, lo que perpetúa la problemática (Havers et al., 2024).

5.2.1. Contexto europeo y marco de actuación internacional

Según el **Informe EUROPOL 2023**, las principales tendencias en ciberamenazas incluyen:

- Incremento del uso de **ransomware**, con extorsión a las víctimas mediante los datos obtenidos.
- Expansión del **phishing** y otros métodos de ingeniería social.
- Aprovechamiento del teletrabajo y de servicios como VPN, cifrado extremo a extremo o criptomonedas ("infraestructura gris").
- Crecimiento de las **campañas de desinformación**, especialmente en contextos de tensión geopolítica (Consejo de Seguridad Nacional, 2023).

La **digitalización acelerada** durante la pandemia de COVID-19 amplificó estas amenazas, incrementando la exposición al riesgo. Las instituciones europeas prevén que la tendencia siga creciendo: se estima que **en 2024 habrá más de 22.300 millones de dispositivos conectados a la Internet de las Cosas (IoT)**, lo que aumentará exponencialmente la superficie de ataque.

En respuesta, la **Unión Europea** ha establecido un **marco diplomático conjunto** frente a actividades cibernéticas maliciosas ("caja de herramientas de la diplomacia cibernética", 2017) y un **régimen de medidas restrictivas** contra ciberataques (2019).

Asimismo, se han impulsado iniciativas estructurales para fortalecer la **resiliencia europea frente a la cibercriminalidad**, entre las que destacan:

- La **Identidad Digital Europea**, para mejorar la seguridad y el control sobre los datos personales.
- La **Brújula Digital para la Década Digital de la UE**, articulada en torno a cuatro ejes estratégicos.

Figura 5. *Ejes de la Brújula Digital para la Década Digital de la UE.*

Fuente: Elaboración propia a partir de Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

5.2.2. Políticas nacionales de prevención y capacitación

España ha desplegado en los últimos años un conjunto de **estrategias nacionales de ciberseguridad y competencias digitales** orientadas a fortalecer la protección ciudadana en el entorno digital y reducir la brecha existente entre distintos grupos sociales. Entre ellas destaca el **Plan Nacional de Competencias Digitales (PNCD)**, aprobado en 2021 y enmarcado en la **Agenda Digital 2026** y en el **Plan de Recuperación, Transformación y Resiliencia (PRTR)**. Este plan constituye uno de los ejes de la política digital española y tiene como objetivo garantizar que la ciudadanía adquiera las habilidades digitales necesarias para participar plenamente en la sociedad y en la economía digital, con una atención específica a los colectivos más vulnerables, entre ellos las personas mayores (Ministerio de Economía, Comercio y Empresa, 2021).

El PNCD se articula en torno a **cinco líneas de actuación principales**:

1. **Competencias digitales básicas para la ciudadanía**, orientadas a asegurar un mínimo de alfabetización digital funcional en toda la población.
2. **Competencias digitales avanzadas para el empleo**, destinadas a mejorar la empleabilidad y la adaptación de los trabajadores al nuevo entorno laboral digital.
3. **Competencias digitales en educación**, integrando la transformación digital en el sistema educativo y la formación del profesorado.
4. **Competencias digitales para las Administraciones Públicas**, fomentando servicios más eficientes, accesibles y seguros.
5. **Especialistas TIC**, con el fin de aumentar el número de profesionales en ciberseguridad, inteligencia artificial y tecnologías emergentes.

El **componente 19 del PRTR** refuerza este marco al incluir la "**competencia digital de la ciudadanía**" como palanca clave para la transformación social y económica, destinando fondos europeos del Mecanismo de Recuperación y Resiliencia (MRR) a programas de capacitación digital inclusiva. En este contexto, las personas mayores han sido identificadas como un grupo prioritario, con iniciativas específicas impulsadas por el **Ministerio de Asuntos Económicos y Transformación Digital**, el **Instituto Nacional de Ciberseguridad (INCIBE)** y la **Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA)**.

Entre los programas más relevantes dirigidos a las personas mayores se encuentran:

- **"Experiencia Senior" (INCIBE)**, centrado en la sensibilización sobre ciberseguridad mediante talleres, materiales didácticos y campañas divulgativas adaptadas al lenguaje y las rutinas digitales de las personas mayores.
- **"Generación D"**, lanzado en 2023, que busca promover la adquisición de competencias digitales básicas a través de una red de centros presenciales y un portal interactivo, incluyendo módulos de ciberseguridad, prevención de fraudes y gestión segura de la identidad digital.
- **"Plan España Digital 2026"**, que fija el objetivo de que el 80% de la población adquiera competencias digitales básicas, integrando a los colectivos mayores en los itinerarios de aprendizaje a lo largo de la vida.
- **"Plan de Acción de la Estrategia Nacional de Ciberseguridad 2019–2025"**, que contempla la protección de la ciudadanía y de los colectivos vulnerables como prioridad estratégica, impulsando la cooperación entre Administraciones, sector privado y sociedad civil.

Además, el **Instituto de Mayores y Servicios Sociales (IMSERSO)** colabora en diversas iniciativas de inclusión digital y envejecimiento activo mediante convenios con el **INCIBE**, comunidades autónomas y entidades del tercer sector. Estas alianzas promueven la realización de cursos de ciberseguridad, guías de buenas prácticas, materiales divulgativos accesibles y campañas específicas para evitar fraudes en línea, especialmente en el ámbito bancario y de la administración electrónica.

En el ámbito autonómico, varias comunidades han desarrollado **planes de competencias digitales para la ciudadanía** que complementan el marco estatal. Por ejemplo, el **Plan de Competencias Digitales de Cataluña (2023–2025)** y el **Programa Andalucía Vuela** incluyen actuaciones dirigidas específicamente a la población sénior, combinando formación digital, sensibilización sobre fraudes y acompañamiento personalizado en gestiones electrónicas.

Sin embargo, a pesar del amplio despliegue institucional, **persisten importantes desafíos**. Por un lado, muchas de las acciones formativas no incorporan una **perspectiva adaptativa**, es decir, no se ajustan al ritmo de aprendizaje, a las motivaciones ni a las condiciones cognitivas o emocionales propias de las personas mayores. Por otro lado, las iniciativas suelen centrarse en la **transmisión de conocimientos técnicos**, sin abordar los **factores psicosociales y relacionales** que condicionan la adopción tecnológica y la confianza digital.

La **Estrategia Nacional de Ciberseguridad (ENCS)**, aprobada por el Consejo de Seguridad Nacional en 2019, identifica expresamente la necesidad de desarrollar una cultura sólida de ciberseguridad basada en la **formación, la sensibilización y la corresponsabilidad ciudadana**. Este enfoque reconoce que la seguridad en el entorno digital no puede depender exclusivamente de las medidas tecnológicas o punitivas, sino que debe apoyarse en la **educación y la participación activa** de la población.

En definitiva, las políticas nacionales han avanzado hacia la construcción de un ecosistema de **prevención, capacitación y sensibilización** en materia de ciberseguridad, pero todavía es necesario integrar plenamente la **dimensión intergeneracional** y adaptar las estrategias al **contexto vital de las personas mayores**. Ello implica fortalecer la colaboración entre Administraciones, entidades sociales y empresas tecnológicas, generar entornos de aprendizaje accesibles y sostenibles, y reconocer el papel activo de las personas mayores como **agentes de cambio y promotores de una ciudadanía digital segura e inclusiva**.

5.2.3. Marco autonómico

Junto al marco estatal, varias comunidades autónomas han desarrollado en los últimos años **estrategias y organismos propios de ciberseguridad** que refuerzan la capacidad territorial de prevención, detección y respuesta frente al cibercrimen. Aunque la competencia penal en materia de ciberdelitos corresponde al Estado, conforme al art. 149.1.29 de la Constitución Española y la jurisprudencia del Tribunal Constitucional, estos marcos autonómicos resultan esenciales para articular políticas públicas de proximidad, mejorar la coordinación interinstitucional y promover la protección ciudadana ante las amenazas digitales.

En este sentido, **Cataluña** fue pionera con la aprobación de la *Ley 15/2017*[3]*, de la Agencia de Ciberseguridad de Cataluña* (con su **CATALONIA-CERT** como equipo de respuesta a incidentes), que establece un organismo público especializado en la protección y gestión de incidentes en el entorno digital, complementado por el *Decreto 76/2020*[4]*, de Administración*

[3] Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña. https://www.boe.es/eli/es-ct/l/2017/07/25/15
[4] Decret 76/2020, de 4 d'agost, d'Administració digital. https://portaljuridic.gencat.cat/eli/es-ct/d/2020/08/04/76

Digital. Por su parte, el **País Vasco** ha avanzado con la *Ley 7/2023*[5], de 29 de junio, de creación de la *Agencia Vasca de Ciberseguridad (Cyberzaintza*), que integra actuaciones de prevención y respuesta. La **Comunidad de Madrid** ha seguido una línea similar con la *Ley 14/2023*[6], que crea la *Agencia de Ciberseguridad de la Comunidad de Madrid*, centrada en el apoyo a administraciones locales, operadores esenciales y en la cultura digital de la ciudadanía.

Otras comunidades han optado por marcos estratégicos y centros técnicos de referencia. **Andalucía** cuenta con la *Estrategia Andaluza de Ciberseguridad 2022-2025* y con el *Centro de Ciberseguridad de Andalucía (ADA)*, que refuerza la colaboración público-privada. La **Comunitat Valenciana**, a través del *CSIRT-CV* (Centro de Seguridad TIC de la Comunitat Valenciana), opera desde 2007 como centro de respuesta ante incidentes y ofrece servicios de sensibilización y apoyo a ciudadanía, empresas y administraciones. De forma análoga, **Galicia** ha consolidado su estructura de ciberseguridad mediante el CSIFRT.gal, gestionado por la *Agencia de Modernización Tecnológica (Amtega*), y el *Decreto 73/2014*[7]*,* que regula la seguridad de la información en la Administración gallega. A continuación, se muestra el despliegue de las diferentes estrategias que tiene cada Comunidad Autónoma.

Tabla 4. *Resumen de la legislación sobre cibercrimen en las comunidades autónomas de España*

Comunidad	**Estrategia y/o ley de agencia**	**CSIRT / SOC**[8]
Andalucía	Estrategia Andaluza 2022-2025	Centro de Ciberseguridad de Andalucía (CIAN)
Aragón	Estrategia en despliegue	Centro de Ciberseguridad de Aragón (CCA) (evolución de AST.CERT)
Asturias	Iniciativas y línea estratégica	SOC/servicios de seguridad en la Admón.
Illes Balears	Política y organización TIC	Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions
Canarias	—	CSIRT-CAN (centro autonómico)
Cantabria	Agenda Digital con foco en ciber	C3 – Centro de Ciberseguridad de Cantabria
Castilla-La Mancha	Portal y plan de impulso	SOC/servicios y portal público
Castilla y León	Estrategia propia	SOC Junta de CyL

[5] Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad. https://www.boe.es/eli/es-pv/l/2023/06/29/7
[6] Ley 14/2023, de 20 de diciembre, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid. https://www.boe.es/eli/es-md/l/2023/12/20/14
[7] Decreto 73/2014, de 12 de junio, por el que se crean y regulan los órganos colegiados con competencias en materia de seguridad de la información y gobierno electrónico de la Administración general y del sector público autonómico de Galicia. https://www.xunta.gal/dog/Publicados/2014/20140630/AnuncioG0244-230614-0003_es.html
[8] Acrónimo de Centro de Operaciones de Ciberseguridad

Cataluña	Ley 15/2017	CATALONIA-CERT (Agència de Ciberseguretat)
Comunitat Valenciana	Política y normativa sectorial	CSIRT-CV (desde 2007)
Extremadura	Estrategia Digital 2027	SOC + plataforma CIBEREXT
Galicia	Decretos orgánicos de seguridad	CSIRT.gal (Amtega)
La Rioja	Programas de capacitación	— (formación/ThinkTIC)
Comunidad de Madrid	Plan estratégico propio y Ley 14/2023	CSIRT/servicios asociados a la Agencia
Región de Murcia	—	CSIRT-CARM (miembro de CSIRT.es)
Navarra	Plan de digitalización EELL	Navarra Cybersecurity Center (NavCC)
País Vasco	Ley 7/2023	Agencia Vasca de Ciberseguridad (Cyberzaintza)

Fuente: Elaboración propia

En conjunto, estas iniciativas autonómicas fortalecen el sistema nacional de ciberseguridad y contribuyen a la construcción de un ecosistema digital más seguro, resiliente y coordinado, alineado con las directrices europeas y los objetivos del Plan Nacional de Competencias Digitales y de la Agencia España Digital 2026.

5.2.4. Limitaciones de las estrategias actuales

Aunque en los últimos años España ha avanzado de manera significativa en el desarrollo de políticas de alfabetización y ciberseguridad, persisten **limitaciones estructurales y metodológicas** que reducen la eficacia de las estrategias frente a la ciberdelincuencia en personas mayores.

En primer lugar, las intervenciones públicas se han diseñado tradicionalmente bajo un enfoque **tecnocéntrico**. Es decir, centrado en la adquisición de habilidades instrumentales o técnicas (uso de dispositivos, contraseñas seguras, navegación en línea, sin integrar suficientemente la **dimensión emocional, social y cognitiva** del aprendizaje en la vejez. Este sesgo ha llevado a tratar a las personas mayores como un grupo homogéneo y pasivo, cuando en realidad existe una gran diversidad en términos de edad, formación, entorno socioeconómico, género, experiencias digitales previas y niveles de autonomía (Kemp & Erades Pérez, 2023).

Este enfoque unidimensional tiende a **invisibilizar el rol de las personas mayores**, relegándolas a un papel de receptoras de información, más que de coproductoras de soluciones. La evidencia muestra que los programas que fomentan la participación, por ejemplo, mediante el aprendizaje intergeneracional, el acompañamiento entre pares o las metodologías basadas en la experiencia, generan mayores niveles de confianza, retención del conocimiento y sostenibilidad de los aprendizajes (Button & Cross, 2017).

En segundo lugar, las estrategias vigentes suelen concentrarse en la **prevención técnica del delito** y en la **minimización de pérdidas económicas**, dejando en un segundo plano los **impactos emocionales, relacionales y reputacionales** asociados a la cibervictimización. Este vacío resulta especialmente problemático en el caso de las personas mayores, ya que las consecuencias psicológicas (vergüenza, culpa, pérdida de confianza o miedo a volver a conectarse) pueden ser tan graves o incluso más duraderas que las pérdidas financieras (Havers et al., 2024).

Otra limitación importante es la **fragmentación institucional** y la **escasa coordinación intersectorial** entre los diferentes organismos que intervienen en el ámbito de la ciberseguridad y la protección de personas mayores. A nivel estatal, el INCIBE, el Ministerio del Interior, el Ministerio de Derechos Sociales y las comunidades autónomas desarrollan programas complementarios, pero sin una estrategia unificada ni protocolos comunes de atención a las víctimas. Ello provoca **duplicidades, vacíos competenciales y disparidad territorial** en la implementación de medidas. Las entidades del tercer sector, que frecuentemente ofrecen acompañamiento y formación digital en el territorio, no siempre están integradas en los circuitos oficiales de prevención ni en los mecanismos de derivación y atención posterior al fraude.

A ello se suma una **falta de evaluación sistemática** del impacto de las políticas implementadas. Si bien existen indicadores de ejecución (número de talleres, personas formadas, materiales distribuidos), pocos programas realizan un seguimiento cualitativo o longitudinal de los cambios en el comportamiento, la autopercepción de seguridad o la reducción efectiva de la victimización digital. Este déficit evaluativo impide generar evidencia robusta que oriente la mejora continua de las intervenciones.

También se observa una **desigualdad territorial** significativa: los programas de ciberseguridad y alfabetización digital suelen concentrarse en áreas urbanas, con una oferta mucho más limitada en zonas rurales o municipios pequeños, donde el acceso a la conectividad, los recursos formativos y la asistencia técnica es menor. Esta brecha territorial

refuerza la **exclusión digital estructural** de muchas personas mayores, que ya enfrentan limitaciones por edad, renta o discapacidad.

En términos comunicativos, muchas campañas de prevención recurren a mensajes **alarmistas o paternalistas**, que refuerzan estereotipos edadistas ("las personas mayores no saben usar Internet", "son más crédulas") en lugar de promover una narrativa de **empoderamiento digital**. Este enfoque, además de limitar la eficacia de las campañas, puede aumentar la resistencia al aprendizaje y el sentimiento de inseguridad. En contraste, los programas basados en una comunicación respetuosa, participativa y adaptada culturalmente muestran mejores resultados de compromiso y autoconfianza.

Desde un punto de vista jurídico y operativo, otro obstáculo reside en la **complejidad del proceso de denuncia**. Las personas mayores que sufren un fraude digital a menudo desconocen cómo y dónde denunciar, temen ser culpabilizadas o no confían en una resolución favorable. El sistema de denuncia electrónica no siempre es accesible ni adaptado a las limitaciones tecnológicas o cognitivas del colectivo. Esta situación contribuye a una **alta infradenuncia**, estimada en torno al 70% de los casos (Ministerio del Interior, 2023), lo que limita la respuesta institucional y la visibilidad del problema.

Finalmente, las políticas actuales tienden a **subestimar el papel del entorno relacional** (familias, amistades, redes comunitarias) en la prevención y detección temprana de fraudes. Sin la implicación de estas redes de apoyo, las estrategias individuales de autoprotección resultan insuficientes. Incluir la perspectiva comunitaria en los programas de prevención permitiría fortalecer la **resiliencia digital colectiva** y reducir la carga emocional de las víctimas.

En síntesis, las limitaciones de las estrategias actuales pueden agruparse en cinco dimensiones principales:

1. **Conceptual**: enfoque tecnocéntrico que no considera las dimensiones emocionales y sociales.
2. **Metodológica**: falta de adaptación pedagógica y de participación activa de las personas mayores.
3. **Institucional**: fragmentación y falta de coordinación intersectorial.
4. **Evaluativa**: carencia de seguimiento y medición del impacto real.
5. **Cultural y territorial**: sesgos edadistas, desigualdad de acceso y brecha rural-digital.

Superar estas limitaciones implica avanzar hacia una **estrategia nacional integral**, basada en la evidencia, con una visión inclusiva y centrada en la persona. Esto supone promover la

participación de las personas mayores en la co-creación de políticas, fortalecer la cooperación entre administraciones y tercer sector, adaptar los materiales y metodologías formativas a sus realidades diversas, y construir un sistema de atención accesible y empático que reconozca tanto los daños económicos como los psicológicos derivados de la cibervictimización.

5.3. Bienestar digital sin estigmas: prevenir, detectar y acompañar

En la era contemporánea de acelerada digitalización, el **acompañamiento integral** a personas mayores víctimas de cibercrimen emerge como un campo teórico-práctico esencial que trasciende la mera prevención técnica para abordar las **profundas transformaciones conductuales, emocionales y relacionales** que generan estos delitos digitales (Erades Pérez et al., 2022). La creciente victimización de las personas mayores en el ciberespacio no solo requiere respuestas reactivas centradas en la recuperación económica, sino **un cambio de paradigma que sitúe en el centro la detección temprana de signos de alerta, la comprensión del impacto psicosocial y el acompañamiento especializado que facilite la recuperación integral y prevenga la cronicidad del daño** (Del Pozo Manzano, 2024). Este enfoque cobra especial relevancia cuando se considera que el 84,6% de las personas mayores ha sido objetivo de al menos un tipo de fraude digital, mientras que solo el 15,2% lo ha denunciado, evidenciando un subregistro masivo que perpetúa la invisibilidad del problema y la revictimización (Kemp & Erades Pérez, 2023).

Desde INCIBE a través de la Oficina de Seguridad del Internauta (OSI) en colaboración con la Policía Nacional se ha creado una guía[9] con el objetivo de divulgar y concienciar en ciberseguridad a los más mayores. En ella se detalla el paso a paso para configurar correctamente los dispositivos, incluyendo opciones concretas para cada sistema operativo. También contiene información sobre cómo crear contraseñas robustas y cómo configurar la doble verificación. Además, se explica cómo acceder a Internet y navegar de forma segura. Adicionalmente, incorpora pistas para identificar y evitar los fraudes más utilizados por los ciberdelincuentes, así como información sobre cómo identificar noticias falsas. Finalmente, la guía ofrece información para configurar de manera segura los perfiles de redes sociales y mensajería instantánea, un checklist de seguridad, varios recursos para ampliar información sobre todo lo tratado a lo largo de la guía y un apartado de 'Denuncia', para todos aquellos que lo necesiten.

No obstante, las estrategias de prevención y capacitación, aun siendo imprescindibles para reducir la exposición al riesgo, resultan insuficientes si no se complementan con mecanismos

[9]Disponible en: https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf

eficaces de detección temprana, atención y acompañamiento integral. La prevención se ocupa de fortalecer las competencias digitales y la conciencia del riesgo, pero la creciente sofisticación de los fraudes digitales y la vulnerabilidad emocional de las víctimas exigen ampliar el foco hacia modelos de intervención centrados en la persona, capaces de abordar el impacto psicológico, relacional y social derivado del delito. En este sentido, la ciberseguridad social debe entenderse como un continuum que va desde la alfabetización preventiva hasta la recuperación y resiliencia postvictimización, integrando herramientas de apoyo técnico, orientación emocional y empoderamiento ciudadano. Esta transición hacia un enfoque integral marca un cambio de paradigma necesario para proteger no solo los datos, sino también el bienestar y la dignidad de las personas mayores en el entorno digital.

5.3.1. Indicadores conductuales y emocionales de la cibervictimización

La **detección temprana** de cambios conductuales requiere una **sistematización de indicadores observables** que permitan a profesionales, familiares y redes comunitarias identificar situaciones de riesgo antes de que se produzca daño irreversible (Álvarez et al., 2024). Los **indicadores conductuales de cibervictimización en personas mayores** incluyen **cambios en hábitos cotidianos** que podrían indicar pérdida de dinero, como modificaciones no explicadas en patrones de gasto, comentarios sobre dificultades económicas repentinas, evitación de conversaciones sobre finanzas o tecnología, y aparición de documentos bancarios sospechosos o beneficiarios inusuales en estados de cuenta (Centro de Inteligencia Digital Alicante, 2022). A nivel emocional, las señales incluyen **incremento de la ansiedad** al usar dispositivos digitales**, reticencia repentina** a realizar trámites en línea que antes manejaban con normalidad**, expresiones de culpa o vergüenza** no relacionadas con eventos concretos, y cambios en el patrón de interacciones familiares que pueden indicar miedo al juicio o rechazo (Morrison et al., 2021).

El **impacto emocional trasciende la pérdida económica** para incluir **vergüenza, autoculpa, pérdida de confianza** en las propias capacidades y, en casos severos, **depresión y aislamiento social** que pueden persistir mucho más allá de la resolución del incidente (Segal et al., 2021). Un estudio reciente realizado en Chile (ClaroVTR & Criteria, 2024), revelan que más de la mitad de los adultos mayores ha sido víctima de estafas digitales, con los fraudes de suplantación de identidad, intento de robo de dinero y plagio de tarjetas como las modalidades más frecuentes. Sin embargo, la naturaleza anónima y global de los ciberdelitos dificulta la identificación de perpetradores, mientras que el aislamiento social y la falta de apoyo especializado en línea impiden un adecuado acompañamiento a las víctimas (Caravaca-Llamas & Girona-Berná, 2021).

5.3.2. Modelos de construcción de significado y recuperación post-trauma

Park (2010) establece que cuanto más percibe un individuo una situación como injusta, más angustiado estará, y que la recuperación no se producirá hasta que haya encontrado una explicación que ofrezca resolución o consuelo ("significado") mediante procesos que pueden implicar cambiar su perspectiva sobre la situación para que se ajuste a sus creencias ("asimilación") o cambiar sus creencias para que se ajusten a la situación ("adaptación") (Frankl, 1946; Joseph & Linley, 2006). Algunos ejemplos de construcción de significado en víctimas mayores incluyen expresar compasión hacia el agresor o considerar cómo la situación podría haber sido peor, estrategias que pueden ser funcionales cuando facilitan la aceptación sin comprometer la seguridad futura, pero que resultan problemáticas cuando derivan en autoinculpación excesiva o minimización del daño sufrido (Janoff-Bulman, 1989).

El modelo cognitivo propone que las interpretaciones negativas pueden conducir a trastornos psicológicos duraderos cuando la persona no puede encontrar una explicación significativa o se adapta en exceso a la amenaza, como víctimas mayores que piensan que el mundo se ha vuelto más peligroso, desarrollando así creencias negativas sobre la peligrosidad del mundo y sentimientos de incompetencia que sustentan el trastorno de estrés postraumático (Ehlers & Clark, 2000). La depresión se sustenta en la desesperanza sobre el mundo y sentimientos de indignidad, mientras que la ansiedad deriva de la sobreestimación de amenazas, llevando a estrategias de afrontamiento inútiles que ofrecen alivio a corto plazo, pero refuerzan trastornos a largo plazo, como la evitación sistemática de entornos digitales (Beck et al., 1979; Clark & Beck, 2010; Salkovskis, 1996).

5.3.3. Factores psicosociales y de vulnerabilidad diferencial

Las investigaciones sobre vulnerabilidad digital en adultos mayores han identificado factores cognitivos y emocionales específicos que aumentan la exposición al riesgo de cibervictimización, aunque no existe evidencia concluyente de que sean proporcionalmente más víctimas que otros grupos (Aperador, 2024). Entre los principales factores se encuentra **el deterioro cognitivo** (aun cuando sea leve) y una reducción de la memoria episódica, que junto con la disminución en la velocidad de procesamiento de información y en la capacidad de resolver problemas, limita significativamente la detección de señales de engaño (Brashier & Schacter, 2020). Un segundo factor se relaciona con la salud mental y el potencial aislamiento social, **donde la depresión y la soledad constituyen factores de riesgo críticos**, haciendo que los adultos mayores con síntomas depresivos o con redes sociales o familiares de apoyo limitadas tengan hasta tres veces más probabilidad de ser víctimas de fraudes (Papí-Gálvez & La-Parra-Casado, 2022).

Los rasgos de personalidad y de confianza, específicamente la credulidad (tendencia a creer sin evidencia suficiente), se encuentran frecuentemente en personas mayores con alta necesidad de pertenencia o con niveles elevados de amabilidad, características que las hacen más propensas a confiar en mensajes o interacciones fraudulentas (Valera-Ordaz et al., 2022). Esta vulnerabilidad se amplifica por el hecho de que las personas mayores tienden a depositar su confianza no en el medio de comunicación, sino en quienes les hacen llegar la información, convirtiendo plataformas como WhatsApp en vectores especialmente efectivos para la difusión de desinformación y fraudes (Amoedo-Casais et al., 2021). La competencia digital limitada, o en muchas ocasiones su ausencia, se convierte en un factor clave que amplifica los efectos nocivos de estos fenómenos, especialmente considerando que las personas mayores consumen mucha información y están interesados y preocupados por los asuntos informativos (Brashier & Schacter, 2020).

5.3.4. Dinámicas familiares y redes de apoyo social

El papel de las redes familiares y comunitarias presenta una dualidad compleja que debe ser cuidadosamente gestionada en el proceso de acompañamiento, ya que pueden actuar tanto como factores protectores como de riesgo adicional (Segal et al., 2021). Por un lado, el apoyo familiar es de gran importancia para las personas mayores en la toma de decisiones de consumo digital, como ilustra el testimonio de Lea, de 91 años: "A menudo, cuando quiero comprar algo, me alegro mucho si tengo a uno de mis hijos conmigo. Porque pueden aconsejarme y decirme qué es bueno y qué no, simplemente porque saben más". Esta dependencia puede incrementarse con la pérdida de cónyuge o el declive de funciones físicas y cognitivas, convirtiendo el apoyo familiar en un recurso esencial para la navegación segura del entorno digital (Segal et al., 2021).

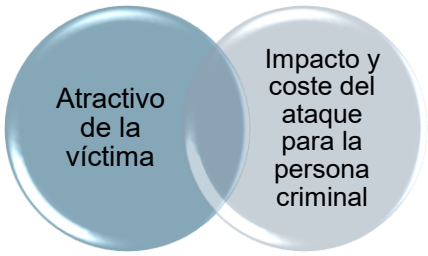
Sin embargo, las personas mayores que encuentran reacciones negativas de miembros familiares pueden experimentar autoculpa intensificada, pérdida de confianza, falta de energía e indefensión, frecuentemente relacionadas con el "edadismo auto-impuesto" donde adoptan e internalizan estereotipos negativos relacionados con la edad (Levy, 2001; Minichiello et al., 2000). Las víctimas expresan sentimientos de vergüenza y miedo a reacciones familiares negativas del tipo "culpar a la víctima" (Wallace & Roberson, 2007), subrayando la importancia de educar tanto a personas mayores como a sus familiares sobre edadismo, edadismo auto-impuesto y culpabilización de víctimas para interrumpir estos ciclos disfuncionales. Esta educación debe ayudar tanto a personas mayores como a familiares a comprender y aceptar las causas del fraude, las dificultades enfrentadas durante estos eventos, las posibles reacciones emocionales y el impacto de las reacciones familiares en el proceso de recuperación (Segal et al., 2021).

5.4. Factores de riesgo y protección de una persona mayor a un cibercrimen

Existen variables extrínsecas e intrínsecas a las personas que están relacionadas con su grado de vulnerabilidad a la hora de convertirse en víctimas de un ciberataque (BBVA, 2023).

Las **variables extrínsecas** son totalmente ajenas a la persona y, como su propio nombre indica, no se pueden controlar. Estas son, por un lado, **el atractivo de la víctima**, es decir, si posee algún activo (por ejemplo, de tipo financiero, reputacional o informativo) que puede resultar de interés a las personas cibercriminales. Por otro lado, el **impacto y coste** que implica el ataque para la persona criminal, y que será lo que determina su atractivo.

Figura 6. *Variables extrínsecas en las personas víctimas de un ciberataque.*



Fuente: Elaboración propia.

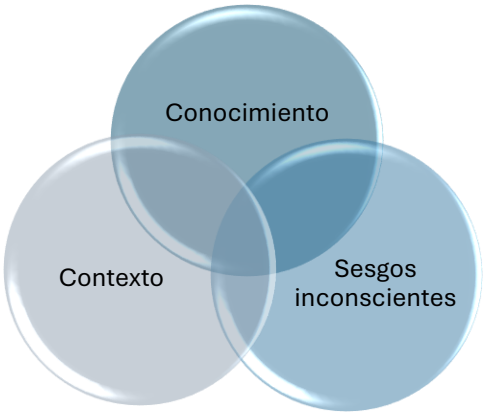
Por otro lado, existen las **variables intrínsecas**, que son aquellas que sí están relacionadas con la persona y se pueden tratar de controlar. Estas son las siguientes:

- El **conocimiento**: Es evidente que tener "skills" técnicas tiene un impacto en la seguridad personal y que, cuanto más conocimiento posea la víctima sobre ciberseguridad, más elaboradas y concienzudas serán sus conductas. Sin embargo, es importante destacar que no por tener conocimientos de este tipo, se consigue ser inmune a los ciberataques.
- El **contexto**: Hay múltiples elementos contextuales como el estrés, la fatiga o el aburrimiento, que minan la capacidad de atención en los elementos que van apareciendo en el entorno digital. Un buen ejemplo es la época de confinamiento, en la que la mayoría de la gente tuvo que lidiar con sentimientos y situaciones a las que no estaban acostumbradas y, muy probablemente, se prestó menor atención a los posibles riesgos.
- Los **sesgos inconscientes**: Otro factor que puede tratar de controlar y que influye en nuestra vulnerabilidad es la existencia de sesgos cognitivos, es decir, ciertos esquemas mentales o formas de procesar la realidad.

- **Responsabilidad delegada**: Se produce cuando se tiende a pensar que la protección no depende de uno mismo y, por tanto, se delega en otros el ser cuidadoso.
- **Sobreconfianza al percibir riesgos**: Muchas veces no se valora lo suficiente la probabilidad de que suceda un ataque. Se infravaloran las consecuencias negativas que conlleva una conducta arriesgada.
- **Preferencia por lo más fácil**: Es un pensamiento habitual en las personas, que tienden a minimizar los esfuerzos. Por ejemplo, cuando se tiene la misma contraseña para múltiples webs.
- **Seguir las normas sociales**: También es habitual, por ejemplo, al compartir con amigos y familiares las contraseñas personales.
- **La conexión continua**: Estar conectados permanentemente, que ha hecho que las personas se vuelvan mucho más dependientes, sobre todo en el contexto actual.
- **Sobreexposición a los estímulos del entorno digital**: La exposición a contenidos, como por ejemplo las ventanas emergentes con publicidad, es muy alta y hace que las personas, acostumbradas, los acepten sin prestar atención.

Además de estas variables intrínsecas, existen **características demográficas**, como el género, la edad o la pertenencia a determinados grupos culturales, que, en ocasiones, también pueden contribuir en cierta medida a hacer más vulnerables a las personas frente a los ciberataques.

Figura 7. *Variables intrínsecas en las personas víctimas de un ciberataque.*



Fuente: Elaboración propia.

A partir de aquí, entran en juego diversos factores que, según el entramado vital de cada persona, pueden actuar como elementos de riesgo o de protección.

5.4.1. Factores personales

- **Factores psicológicos y cognitivos**

Con la edad, es habitual que aparezcan **alteraciones como la disminución de la atención, problemas de memoria o una confianza excesiva**, que pueden aumentar la vulnerabilidad ante engaños y fraudes digitales. Estas características dificultan la capacidad para identificar señales de alerta en situaciones sospechosas, especialmente en entornos digitales donde las decisiones deben tomarse de forma rápida y bajo presión.

- **Percepción de responsabilidad en la seguridad**

El nivel de responsabilidad que una persona percibe en relación con su propia seguridad digital es un factor clave. Algunas personas usuarias delegan esta responsabilidad en otras debido al estrés o la ansiedad. No obstante, empoderar a las personas mayores a través de la educación y la formación en ciberseguridad tiene un impacto positivo en su autonomía y en la reducción del riesgo de victimización.

- **El estrés como factor de vulnerabilidad**

La literatura científica sobre ciberseguridad subraya cada vez con mayor énfasis el papel del estrés digital en la experiencia de las personas usuarias (Mawson et al., 2022; Dhir et al., 2021). El entorno en línea se caracteriza por la complejidad técnica de los sistemas, la imprevisibilidad de los eventos en tiempo real y la exigencia de tomar decisiones rápidas bajo presión, factores que pueden generar una sensación sostenida de alerta y fatiga cognitiva.

En el caso de las personas mayores, estas condiciones se ven agravadas por el ritmo acelerado de los cambios tecnológicos y por la percepción de menor autoeficacia digital, es decir, la creencia de no poseer las competencias necesarias para protegerse o desenvolverse con seguridad en el entorno digital (Bandura, 1997; Marston et al., 2020). La exposición continua a nuevos dispositivos, plataformas o actualizaciones, sumada a la aparición constante de nuevas modalidades de fraude, puede provocar ansiedad, inseguridad e incluso evitación del uso de la tecnología (Leist, 2013; Chen & Chan, 2014).

Este estrés se manifiesta, además, en la dificultad para procesar información ambigua o sospechosa, como correos, llamadas o mensajes fraudulentos, que requieren evaluar la veracidad de los contenidos en un tiempo limitado. Las personas mayores, al carecer en

muchos casos de marcos de referencia previos sobre estas dinámicas, tienden a experimentar una sobrecarga cognitiva que aumenta el riesgo de error y la vulnerabilidad ante el engaño (Mitzner et al., 2019).

Asimismo, la falta de confianza en las propias habilidades tecnológicas puede derivar en prácticas contraproducentes, como anotar contraseñas en lugares visibles, compartir datos personales con terceros o no activar medidas de protección básicas. Este fenómeno, identificado como “estrés por inseguridad tecnológica” (Vaportzis et al., 2017), se asocia con sentimientos de indefensión, frustración y pérdida de control sobre el propio entorno digital.

En conjunto, la literatura evidencia que el estrés digital no solo incrementa el riesgo de victimización, sino que también erosiona la autonomía y la participación digital activa de las personas mayores, contribuyendo a reproducir la brecha digital y el aislamiento social. Por ello, abordar la ciberseguridad desde una perspectiva psicosocial implica reducir los factores de estrés asociados al uso de la tecnología, fortaleciendo la autoconfianza, la comprensión de los riesgos y la capacidad crítica ante la información digital. La literatura (Nobles, 2022; Méndez, 2024) sobre ciberseguridad destaca cada vez más el papel del estrés en la experiencia de las personas usuarias. En este ámbito convergen múltiples factores que hacen que las operaciones en el ciberespacio sean altamente estresantes: la complejidad de los sistemas, la imprevisibilidad de los eventos en tiempo real y la necesidad de tomar decisiones constantes bajo presión.

Las personas mayores experimentan con frecuencia **estrés y sobrecarga cognitiva** al interactuar en entornos digitales porque deben **valorar continuamente posibles riesgos** (como distinguir entre mensajes legítimos y fraudulentos) en un contexto que perciben incierto. Esta tensión se agrava por la **velocidad de los cambios tecnológicos** y la aparición constante de **nuevas estrategias de engaño** por parte de los ciberdelincuentes, que erosionan la sensación de control y generan **inseguridad, ansiedad y miedo a cometer errores**. A ello se suma la **brecha de autoconfianza tecnológica**: muchas personas mayores dudan de sus propias competencias digitales, lo que incrementa el estrés y las lleva, paradójicamente, a adoptar **hábitos poco seguros** (como apuntar contraseñas o no actualizar dispositivos) o incluso a **evitar el uso** de determinadas herramientas para reducir la ansiedad que les produce.

- **La falta de información y formación: alfabetización digital y ansiedad tecnológica**

El aumento del uso de internet por parte de personas mayores se ha visto acompañado por un incremento en los casos de cibervictimización. El estudio de Morrison et al. (2021) identifica cuestiones importantes en este ámbito aún poco exploradas. Destaca el impacto del estrés, **exacerbado por la falta de información y formación específica en ciberseguridad para este grupo.** Muchas personas mayores reportan sentirse ansiosas, temerosas o abrumadas al gestionar su seguridad digital, lo que las lleva a adoptar estrategias de riesgo.

La falta de competencias digitales y el acceso limitado a recursos educativos adaptados aumentan la vulnerabilidad ante amenazas en línea. A pesar de los avances en la investigación del papel de las emociones en la ciberseguridad, aún se requieren instrumentos metodológicos más precisos para comprender la relación entre el estrés y el comportamiento en este grupo poblacional.

Asimismo, la escasez de estudios fuera del entorno laboral es preocupante. Mientras que la seguridad organizacional ha abordado el tecnoestrés en empleados, existe un vacío en el conocimiento sobre cómo viven estos procesos las personas mayores, quienes cuentan con menor alfabetización digital y menos apoyo tecnológico. El estudio de Morrison et al. (2021) también resalta la importancia de la confianza y la percepción de autoeficacia en la adopción de medidas de seguridad. Sin una formación adecuada, resulta difícil desarrollar un “círculo virtuoso” de aprendizaje y empoderamiento.

En este sentido, iniciativas como CyberGuardians, que capacitan a personas mayores como embajadoras en ciberseguridad dentro de sus comunidades, son prometedoras para reducir la brecha digital y mejorar la percepción de control.

Finalmente, la investigación sugiere que es esencial facilitar el acceso a recursos de formación accesibles y adaptados, para fomentar estrategias de afrontamiento eficaces. Cada vez más estudios exploran cómo hacer que la ciberseguridad sea más comprensible y menos intimidante, pero sigue siendo urgente desarrollar enfoques inclusivos que permitan a las personas mayores sentirse seguras y confiadas en un entorno digital en constante cambio.

- **Alfabetización digital**: Se refiere a la capacidad de una persona para interactuar de forma funcional con la tecnología. Es esencial para aplicar los conocimientos de seguridad digital.

- **Ansiedad tecnológica**: Las personas mayores presentan niveles significativamente más altos de tecnofobia[10]. **La ansiedad no afecta el rendimiento en sí, sino el tiempo que se tarda en decidir cómo ejecutar una tarea.** Diversos estudios han demostrado que, en contextos laborales con cambios tecnológicos frecuentes, **la experiencia previa reduce la ansiedad ante la tecnología, tanto en jóvenes como en mayores.**

En esta línea, E1 propone reforzar los **espacios de envejecimiento activo** como plataformas de prevención comunitaria, formando a personas mayores líderes y voluntarias como agentes multiplicadores de buenas prácticas en ciberseguridad.

> *"Nuevos tipos de metodología y participaciones que tengan esta visión más innovadora más disruptiva, más cambiante, para que esto nos permita, pues también reflexionar en torno la figura del papel profesional, desarrollar nuevas maneras de intervenir y poder acercar a diferentes colectivos y diferentes metodologías a espacios de envejecimiento activo" (E1, 36:15)*

Asimismo, sugiere implementar talleres breves en formato cápsula y dinámicas de co-creación de mensajes visuales —por ejemplo, memes o mensajes de WhatsApp— diseñados por las propias personas mayores, de manera que los contenidos resulten comprensibles y culturalmente cercanos.

> *"Se pueden generar sesiones de co-creación con las personas mayores para hacer estas imágenes, igual con las cosas que a ellos les gustan. Con los tipos de dibujos o de animales que les gustan normalmente compartir o les parecen monos, para que les llegue, porque a veces muchas cosas lo vemos desde nuestro prisma, que para nosotros lo bonito, lo que está chulo es lo que nosotros tenemos en nuestro imaginario, pero igual hay otro, otras personas que lo que les gustan son otros tipos de imágenes, entonces, trabajar esto también igual desde la creatividad, pues puede ser interesante, de eso que decía, juntar disciplinas desde el movimiento" (51:39)*

Por otra parte, diversas informantes proponen usar instrucciones paso a paso o visuales y analogías cotidianas (p. ej., "llave = contraseña") para que las personas practiquen a su ritmo y comprendan mejor los conceptos.

> *"El tema de dar pasos escritos yo es algo que no hacía antes, y que me he dado cuenta de que para ellos es súper necesario, o sea, paso 1, paso 2, estas cosas sobre el papel que ellos puedan practicar, o sea, que ellos lleguen a casa y digan, vale, yo tengo aquí mi hojita que me pone todos los pasitos que tengo que hacer para esto, y entonces ahora voy a practicar esto" (E5, 25:44).*

> *"En el en el caso del vocabulario, siempre va acompañado de la definición básica de ejemplos de hacer paralelismos, ¿qué es una carpeta en el ordenador? Pues (…) ¿Te acuerdas de la carpeta de cuando ibas al cole? (…) al final tiene que ser algo familiar y que lo puedan relacionar" (E2, 16:16).*

[10] La tecnofobia es el miedo, rechazo o ansiedad hacia el uso de nuevas tecnologías, especialmente cuando implican cambios en los hábitos o entornos de trabajo.

"(…) oye, cuando te vas de casa ¿a que cierras la puerta con llave y te aseguras de que está cerrado?, pues lo mismo ¿vale?, es decir, al final la contraseña es una entrada a tu vida (…) y, más que asegurarte, se trata de aplicar el sentido común" (E5, 31:04).

5.4.2. Factores contextuales / estructurales

- **Brecha digital y limitaciones tecnológicas**

Muchas personas mayores enfrentan dificultades en el uso de dispositivos electrónicos, en la navegación por internet y en la comprensión de mecanismos de seguridad digital. Reducir la brecha digital no solo es esencial para garantizar sus derechos en una sociedad cada vez más conectada, sino también para fortalecer su autonomía y prevenir riesgos asociados al entorno digital. Es fundamental implementar estrategias de educación digital accesibles, adaptadas a sus necesidades, que promuevan el aprendizaje continuo, el acceso a tecnologías seguras y el desarrollo de habilidades para desenvolverse con confianza.

Desde una perspectiva interseccional, cuanto más baja es la posición social de una persona, más marcada es la segregación de género, lo que refuerza los roles tradicionales en relación con el uso de las tecnologías. La gestión de la sociabilidad digital no depende solo del género, sino que también está jerarquizada según el capital cultural de cada individuo. Así, una mujer mayor en un entorno social desfavorecido tiene menos oportunidades de acceder a formación digital básica que le permita romper con su contexto de origen y superar estereotipos vinculados a su clase, género y edad.

Aunque la edad, el género y la clase social suelen funcionar como ejes de dominación, también es necesario considerar el potencial emancipador de las tecnologías cuando se abordan desde un enfoque inclusivo y comunitario.

- **Dificultad en la denuncia**

Diversas barreras como el **miedo, la vergüenza o el desconocimiento de los procedimientos** pueden impedir que las víctimas mayores reporten los delitos cibernéticos. Si bien los adultos jóvenes suelen experimentar más incidentes digitales, los delitos sufridos por personas mayores tienden a ser más graves, repetitivos y con mayores consecuencias económicas. Esta vulnerabilidad se ve agravada por una menor conciencia sobre las estafas digitales y el desconocimiento de las vías existentes para denunciar.

Uno de los principales obstáculos es **la falta de familiaridad con los procesos legales y tecnológicos para reportar un ciberdelito.** Muchas personas mayores no saben cómo ni dónde acudir, lo que facilita la impunidad de los agresores. El miedo a ser juzgados o

considerados incapaces, especialmente si el fraude implica un engaño emocional, también puede hacer que las víctimas oculten lo ocurrido.

Diversas barreras como el **miedo, la vergüenza o el desconocimiento de los procedimientos** pueden impedir que las víctimas mayores reporten los delitos cibernéticos. Si bien los adultos jóvenes suelen experimentar más incidentes digitales, los delitos sufridos por personas mayores tienden a ser más graves, repetitivos y con mayores consecuencias económicas. Esta vulnerabilidad se ve agravada por una menor conciencia sobre las estafas digitales y el desconocimiento de las vías existentes para denunciar.

Otro factor es la **desconfianza en las instituciones** y en la efectividad de los mecanismos de denuncia. Algunas personas mayores perciben que el proceso será demasiado complicado o que sus casos no serán tomados en serio. Además, la dificultad para recuperar el dinero perdido en fraudes internacionales aumenta la percepción de inutilidad de denunciar.

Datos como los de la Encuesta de Criminalidad 2019/20 (CSEW) en Inglaterra y Gales revelan que los hombres mayores tienen mayor probabilidad de ser víctimas recurrentes, posiblemente por asumir más riesgos en línea. Sin embargo, la falta de redes de apoyo y el aislamiento son factores clave que, independientemente del género, pueden impedir que se busque ayuda o se denuncie, perpetuando el ciclo de victimización.

E2 advierte que, tras un episodio de estafa, algunas familias reaccionan restringiendo el acceso digital de la persona mayor —por ejemplo, sustituyendo su teléfono por uno sin Internet— con la intención de protegerla. Esta respuesta, aunque bienintencionada, refuerza la dependencia y el miedo tecnológico. La recuperación pasa por un acompañamiento gradual que devuelva autonomía y confianza, incorporando espacios donde la víctima pueda compartir su experiencia sin juicio.

> *"los hijos a veces quieren ayudar, pero con la ayuda provocan más miedo, que como no quieren que les pase nada a sus padres… Entonces les dicen, no toques esto, no toques lo otro. Entonces había gente que decía no hago compras por Internet porque mi hijo me dice que no lo haga, que me van a estafar" (E2, 30:43).*

- **Disponibilidad y calidad del apoyo tecnológico**

El apoyo que reciben las personas mayores en el uso de tecnologías digitales es un factor determinante para su inclusión y seguridad en línea. No obstante, este apoyo no siempre es adecuado y puede influir directamente en su nivel de vulnerabilidad.

Morrison et al. (2023) identifican dos tipos de apoyo:

1. **Apoyo que fomenta la independencia**: se basa en enseñar a la persona mayor cómo realizar una tarea, promoviendo el aprendizaje y la autonomía digital.
2. **Apoyo que fomenta la dependencia**: quien brinda ayuda realiza directamente la tarea sin explicar el proceso, generando una relación de dependencia que impide el desarrollo de competencias propias y perpetúa un enfoque paternalista en ciberseguridad.

Este segundo tipo de apoyo, aunque bienintencionado, puede aumentar la vulnerabilidad a largo plazo al limitar el empoderamiento digital. A pesar de su relevancia, la literatura que analiza el impacto del apoyo social en la ciberseguridad de las personas mayores es aún escasa, lo que representa una línea de investigación pendiente.

- **Infraestructura tecnológica y accesibilidad**

Muchas plataformas digitales no están diseñadas teniendo en cuenta las necesidades de las personas mayores. Interfaces poco intuitivas, textos pequeños, jerarquías de navegación confusas y falta de instrucciones claras dificultan la interacción segura con servicios digitales. La ausencia de estándares de accesibilidad digital específicos para personas mayores puede aumentar su frustración y desconfianza, y en consecuencia, su exposición a errores o fraudes. Diseñar entornos digitales inclusivos, accesibles y amigables es una condición estructural indispensable para una verdadera equidad en ciberseguridad.

5.4.3. Factores socioculturales

- **Aislamiento social**

La falta de redes de apoyo puede hacer que las personas mayores sean más propensas a confiar en mensajes fraudulentos o solicitudes engañosas. **El aislamiento y la soledad también se relacionan con un mayor riesgo de deterioro cognitivo y emocional**, lo que impacta directamente en la capacidad de reconocer situaciones de riesgo en entornos digitales. Se ha demostrado que el aislamiento social está asociado con **dificultades en la toma de decisiones y una mayor susceptibilidad al fraude**, ya que las personas mayores pueden tender a confiar más en desconocidos en espacios virtuales debido a la escasez de interacciones sociales en el mundo físico.

Este aislamiento se considera un factor de riesgo crítico porque limita la posibilidad de validar con otras personas —familiares, amistades o profesionales— la autenticidad de correos, mensajes o llamadas sospechosas. A su vez, la sensación de soledad puede llevar a buscar

más contacto o compañía en el entorno digital, lo que incrementa el nivel de exposición a potenciales amenazas y estafas.

- **Interseccionalidad**

Las variables como el género, la clase social y la edad no actúan de forma aislada, sino que se entrecruzan y refuerzan mutuamente, generando diferentes niveles de vulnerabilidad digital y distintas formas de afrontar los riesgos en ciberseguridad.

- **Género**: Las mujeres mayores, por ejemplo, pueden haber tenido menos oportunidades previas de exposición y formación digital debido a roles de género tradicionales, lo que condiciona su nivel de alfabetización digital actual.
- **Clase social y acceso**: La situación económica determina el acceso a tecnologías de calidad, la posibilidad de renovar dispositivos y contar con asesoramiento técnico, elementos todos ellos fundamentales para una experiencia digital segura.
- **Edad**: La edad condiciona tanto la autopercepción de competencia como la manera en que se busca (o no) ayuda ante una situación sospechosa.

Esta intersección de factores contribuye a amplificar desigualdades preexistentes y crea escenarios donde algunas personas mayores están significativamente más expuestas que otras a la ciberdelincuencia, no por su edad en sí, sino por su posición social, su red de apoyo, y su trayectoria formativa y laboral previa.

- **Posición financiera**

La situación económica de una persona mayor tiene un impacto directo en su seguridad digital. Investigaciones previas han mostrado cómo la brecha digital afecta el acceso a tecnología actualizada, a internet de calidad, y a dispositivos seguros. Además, la desigualdad en la calidad de los dispositivos empleados también condiciona las posibilidades de aplicar medidas de seguridad digital efectivas, ya que sistemas antiguos o con menor soporte técnico pueden ser más vulnerables a ataques. Una menor capacidad económica también limita el acceso a servicios de soporte técnico o formación especializada, perpetuando la vulnerabilidad digital.

La situación económica de las personas mayores constituye un determinante estructural de su seguridad digital. Diversas investigaciones han evidenciado que la brecha digital no depende únicamente de factores generacionales o cognitivos, sino también de condicionantes socioeconómicos que afectan al acceso, uso y aprovechamiento de las tecnologías (Van Dijk, 2020; Helsper, 2021). Las limitaciones económicas restringen la

posibilidad de disponer de dispositivos actualizados, conexiones de calidad y servicios de soporte técnico, lo que repercute directamente en la capacidad de prevenir incidentes de seguridad y de recuperarse tras ellos.

Las personas mayores con ingresos limitados suelen mantener durante años el mismo equipo o teléfono móvil, muchas veces con sistemas operativos obsoletos o sin actualizaciones de seguridad. Estos dispositivos, al carecer de soporte técnico, se convierten en vectores de riesgo más fáciles de explotar por los ciberdelincuentes (Reisdorf & Rhinesmith, 2020). Del mismo modo, el acceso a planes de conexión más económicos puede implicar una menor estabilidad o velocidad de red, dificultando la implementación de herramientas de protección como antivirus, actualizaciones automáticas o sistemas de doble autenticación.

A ello se suma la carencia de recursos para contratar asistencia técnica o formación especializada. Las personas mayores con menor renta suelen depender de familiares o conocidos para resolver incidencias digitales, lo que puede aumentar su exposición al fraude y la pérdida de privacidad. Este fenómeno, identificado en la literatura como vulnerabilidad digital económica (Eynon & Geniets, 2016), describe cómo la desigualdad de ingresos se traduce en desigualdad en la capacidad de protegerse en el entorno digital.

La dimensión económica también influye en la percepción subjetiva de la seguridad, ya que las personas mayores con menos recursos tienden a desarrollar menor confianza en la tecnología y a priorizar el uso funcional básico (por ejemplo, banca o trámites administrativos), en detrimento del aprendizaje sobre ciberseguridad (Marston & Samuels, 2019). Esta relación entre precariedad material y falta de autoconfianza tecnológica genera un círculo vicioso: la inseguridad económica refuerza la inseguridad digital, y viceversa.

Por último, las desigualdades territoriales amplifican la brecha socioeconómica. En zonas rurales o de menor densidad poblacional, donde viven muchas personas mayores con pensiones reducidas, las infraestructuras digitales suelen ser más deficientes y el acceso a servicios de acompañamiento o reparación técnica, limitado. De este modo, la vulnerabilidad económica no solo se expresa en el nivel individual, sino también en la infraestructura social y territorial de la ciberseguridad, configurando un escenario en el que la exclusión económica y digital se retroalimentan (Friemel, 2016).

En conjunto, estas evidencias subrayan la necesidad de incorporar la variable socioeconómica en las políticas de alfabetización y protección digital, garantizando que los programas públicos incluyan el acceso a dispositivos seguros, conectividad estable y formación accesible y gratuita. Sin estas condiciones materiales mínimas, las estrategias de

ciberseguridad seguirán reproduciendo las desigualdades preexistentes, dejando fuera precisamente a quienes más necesitan protección.

5.5. Canales para la atención a las víctimas del cibercrimen

La atención a las personas mayores víctimas de cibercrimen constituye uno de los principales desafíos institucionales y sociales en el marco de la seguridad digital contemporánea. Este reto se manifiesta tanto en la detección temprana de los casos como en la calidad, accesibilidad y coordinación de los canales disponibles para su atención. En la actualidad, los principales actores implicados en la respuesta a la cibervictimización en España son las fuerzas y cuerpos de seguridad del Estado, las entidades financieras, las administraciones públicas y, en menor medida, el tercer sector. Sin embargo, la fragmentación de recursos, la escasa especialización en el trato con personas mayores y la falta de integración entre los servicios de atención limitan la eficacia de la respuesta (Gómez-Jara, 2023; Kemp & Erades Pérez, 2023).

Las fuerzas policiales desempeñan un papel fundamental en la **recepción de denuncias y la investigación de delitos cibernéticos**. La **Policía Nacional** cuenta con la *Brigada Central de Investigación Tecnológica (BIT)*, y la **Guardia Civil** con el *Grupo de Delitos Telemáticos (GDT)*, ambos con amplia experiencia en la persecución del cibercrimen y en la cooperación internacional. Sin embargo, las **rutas de acceso a la denuncia** no siempre son adecuadas para las personas mayores.

Por un lado, los canales telemáticos (formularios web, denuncias electrónicas o plataformas de cita previa) suelen resultar **inaccesibles para quienes carecen de competencias digitales básicas** o no disponen de dispositivos adecuados (Ministerio del Interior, 2023). Por otro, la atención presencial en comisarías o cuarteles no siempre está adaptada a las necesidades cognitivas, comunicativas o emocionales del colectivo sénior.

En este sentido, los **cuerpos policiales de proximidad**, como la Guardia Urbana o las Policías Locales, han comenzado a desempeñar un papel clave en la **detección temprana y la sensibilización comunitaria**, dado su contacto cotidiano con el vecindario y su conocimiento del territorio. Algunos municipios han implementado **programas de prevención y acompañamiento** orientados a personas mayores, como charlas de sensibilización o campañas informativas en centros cívicos, si bien la cobertura sigue siendo desigual entre territorios.

El sistema financiero es un **actor estratégico** en la detección y atención de víctimas, dado que una parte significativa de los ciberdelitos que afectan a personas mayores están

vinculados a **fraudes bancarios, phishing o suplantación de identidad**. Los bancos y cajas han reforzado sus **protocolos de seguridad y canales de atención al cliente**, implementando sistemas de alerta y validación en operaciones sospechosas.

No obstante, las medidas de prevención técnica contrastan con la **insuficiencia de mecanismos de acompañamiento humano**. La **reducción del número de oficinas físicas**, la **automatización de los servicios** y la **externalización de la atención al cliente** han generado una brecha de accesibilidad para muchas personas mayores (Banco de España, 2023). La atención telefónica o digital, basada en menús automatizados, resulta especialmente frustrante para quienes tienen dificultades auditivas o cognitivas, mientras que la pérdida del contacto personal reduce la posibilidad de detectar cambios de comportamiento que podrían alertar sobre situaciones de fraude.

Algunas entidades han comenzado a desarrollar **programas de inclusión financiera sénior**, como el *Protocolo Estratégico para Reforzar la Inclusión Financiera de las Personas Mayores* (2022), firmado por el Gobierno y las asociaciones bancarias, que contempla medidas para simplificar la comunicación, reforzar la atención presencial y mejorar la educación financiera y digital. Sin embargo, la implementación es desigual y su impacto real todavía limitado (Ayuso, 2025).

Las **administraciones públicas**, tanto locales como autonómicas y estatales, desempeñan un rol esencial en la **prevención y sensibilización** frente al cibercrimen, aunque su implicación en la **detección y atención directa de las víctimas** sigue siendo insuficiente. Los programas de alfabetización digital —como los impulsados por el *Plan Nacional de Competencias Digitales* o las iniciativas de los *Puntos de Inclusión Digital*— han contribuido a mejorar la capacitación tecnológica básica, pero **no están diseñados para identificar ni acompañar a víctimas de ciberdelitos**.

A menudo, los servicios de ciberseguridad y los de atención social o sanitaria operan de forma **paralela y sin canales de derivación efectivos**. La falta de coordinación impide detectar situaciones de vulnerabilidad digital asociadas a otros indicadores de riesgo social (soledad, deterioro cognitivo, abuso económico). La atención institucional se centra con frecuencia en la dimensión técnica o legal (denuncia, bloqueo de cuentas, restauración de datos, dejando en segundo plano los **efectos emocionales y relacionales** que la cibervictimización produce (Del Pozo Manzano, 2024).

Algunos gobiernos autonómicos y locales comienzan a promover **ventanillas únicas de atención digital**, que combinan asesoramiento técnico, formación básica y acompañamiento emocional, integradas en la red de servicios sociales o de atención ciudadana. Estas

iniciativas, todavía incipientes, apuntan hacia un modelo de **atención integral y cercana** que puede servir de referencia para futuras políticas públicas.

Las **organizaciones del tercer sector** (fundaciones, asociaciones de mayores, entidades de voluntariado) cumplen un papel complementario fundamental, actuando como **puente entre la ciudadanía y las instituciones**. Su proximidad territorial, su experiencia en acompañamiento social y su capacidad de generar confianza resultan claves para detectar casos de victimización que no llegan a los canales formales.

Entidades como la Fundación Pilares, Cruz Roja o la Fundación Mayores UDP han desarrollado **programas de educación digital y apoyo emocional** para personas mayores, en algunos casos en colaboración con el INCIBE o con las administraciones locales. Estos programas contribuyen a reducir la brecha de confianza y a fomentar el **autorreconocimiento de la victimización**, un paso previo indispensable para acceder a la justicia o la reparación (Havers et al., 2024).

Pese a ello, el tercer sector enfrenta **limitaciones de financiación y de cobertura**, y sus acciones carecen aún de un marco de coordinación estable con los servicios públicos. La ausencia de **protocolos comunes de derivación y seguimiento** impide consolidar un sistema de atención integral que combine prevención, acompañamiento y reparación.

Ante esta situación, resulta necesario promover canales accesibles, empáticos y coordinados entre actores, que consideren la diversidad del colectivo mayor y fomenten su participación activa en el diseño de soluciones.

Tabla 5. *Canales estatales de denuncia e información de ciberdelitos*

Canal	Tipo de organismo	A quién atiende	Contacto / Web
INCIBE	Estatal (Ministerio para la Transformación Digital y de la Función Pública)	Ciudadanía, menores, pymes, profesionales y autónomos	017 (todos los días, 9–21h) https://www.incibe.es
Oficina de Seguridad del Internauta (OSI)	Estatal	Ciudadanía (casos leves y moderados)	https://www.osi.es
INCIBE-CERT	Estatal (CERT nacional para ciudadanos y pymes)	Empresas, profesionales, pymes y ciudadanía	incidencias@incibe-cert.es
CCN-CERT (Centro Criptológico Nacional)	Estatal (adscrito al CNI)	Administraciones públicas y empresas estratégicas	https://www.ccn-cert.cni.es
Policía Nacional – Brigada de Investigación Tecnológica (BIT)	Estatal	Denuncias por ciberdelitos (estafas, hackeo, suplantación, sextorsión…)	https://www.policia.es/_es/colabora_internet.php
Guardia Civil – Grupo de Delitos Telemáticos (GDT)	Estatal	Denuncias y avisos sobre ciberdelitos en todo el país	https://www.gdt.guardiacivil.es
Agencia Española de Protección de Datos (AEPD)	Estatal	Denuncias por vulneración de datos personales, suplantación o difusión de contenidos sin consentimiento	https://www.aepd.es
Canal Prioritario AEPD	Estatal	Retirada urgente de contenido sexual o íntimo difundido sin permiso	https://www.aepd.es/canalprioritario

Fuente: Elaboración propia.

Tabla 6. *Canales autonómicos sobre ciberdelincuencia*

Comunidad Autónoma	Canal / Organismo	A quién atiende	Web / Contacto
Catalunya	CATALONIA-CERT (Agència de Ciberseguretat de Catalunya)	Administración pública catalana, empresas, ciudadanía	https://ciberseguretat.gencat.cat cert@gencat.cat
Comunidad de Madrid	Madrid Digital – Centro de Ciberseguridad de la Comunidad de Madrid	Administración autonómica, servicios públicos y empresas colaboradoras	https://madrid.org/ciberseguridad
País Vasco	Basque CyberSecurity Centre (BCSC)	Ciudadanía, empresas y administraciones	https://www.ciberseguridad.eus
Galicia	Ciber.gal (Nodo galego de ciberseguridade)	Empresas, ciudadanía y sector público	https://www.ciber.gal
Andalucía	Centro de Ciberseguridad de Andalucía (Digital Agency of Andalucía)	Administración y empresas andaluzas	https://www.juntadeandalucia.es/agenciadigital
Comunitat Valenciana	CSIRT-CV (Computer Security Incident Response Team)	Ciudadanía, empresas y administración	https://www.csirtcv.gva.es
Castilla-La Mancha	Centro de Ciberseguridad de Castilla-La Mancha (CCCM)	Administración, empresas y ciudadanía	https://ciberseguridad.castillalamancha.es
Castilla y León	Centro de Ciberseguridad de Castilla y León	Administración autonómica y entidades locales	https://ciberseguridad.jcyl.es
Extremadura	CIBEREX (Centro Extremeño de Ciberseguridad)	Ciudadanía y sector público	https://www.ciberex.es
Canarias	Centro de Ciberseguridad de Canarias (CICAN)	Administración autonómica y ciudadanía	https://www.cican.es
Illes Balears	CSIRT-IB	Administración autonómica y empresas colaboradoras	https://www.caib.es/sites/csirtib
Navarra	Centro de Ciberseguridad de Navarra (Nasertic-Gobierno de Navarra)	Administración y sector público	https://www.nasertic.es/ciberseguridad
Aragón	Centro de Ciberseguridad de Aragón (Aragon Digital)	Administración y pymes	https://www.aragon.es/-/ciberseguridad

Cantabria	Dirección General de Transformación Digital – Gobierno de Cantabria	Administración y ciudadanía	https://www.cantabria.es/web/transformacion-digital
Murcia	Centro de Ciberseguridad de la Región de Murcia (CSIRT-RM)	Administración y pymes	https://www.carm.es/web/pagina?IDCONTENIDO=64238&IDTIPO=240
Asturias	Asturias CERT (en desarrollo, dependiente del SEPEPA / D. G. de Estrategia Digital)	En fase de implementación	—
La Rioja	Centro Riojano de Ciberseguridad (CRCS)	Ciudadanía, administración y empresas	https://www.larioja.org/crcs

Fuente: Elaboración propia.

5.6. Acompañamiento de las víctimas mayores de un cibercrimen: Transformando la prevención técnica en acompañamiento integral para personas mayores

Esta aproximación descansa en la convergencia de varios marcos conceptuales complementarios que trascienden las aproximaciones tradicionales de la victimología clásica para incorporar las particularidades del ciberespacio y sus efectos diferenciales en poblaciones vulnerables (Caravaca-Llamas & Girona-Berná, 2021). Los modelos de construcción de significado de Park (2010) explican cómo las víctimas interpretan el trauma y reconstruyen **su sentido de seguridad mediante procesos de asimilación** (cambiar su perspectiva sobre la situación) **o adaptación** (cambiar sus creencias para que se ajusten a la realidad). En personas mayores víctimas de cibercrimen, estos procesos se complican por **la intersección de factores como la vergüenza, el estigma edadista, la pérdida de confianza en la tecnología y el miedo al juicio familiar o social** (Aperador & Pascual, 2024). Los enfoques de victimología que abordan las dinámicas específicas de la cibervictimización revelan diferencias sustanciales con otras formas de victimización por sus características de invisibilidad, persistencia digital de las evidencias y pérdida de control sobre los procesos de revelación (Miró-Llinares, 2013).

Las teorías del cambio conductual identifican patrones de adaptación y afrontamiento específicos que emergen tras experiencias de cibervictimización, incluyendo estrategias de evitación tecnológica que pueden resultar contraproducentes a largo plazo al limitar la participación digital y aumentar la dependencia de terceros (Jansen & Leukfeldt, 2018). Los modelos de acompañamiento psicosocial informados por el trauma priorizan **la validación, la contención y el empoderamiento como elementos centrales de la recuperación,**

reconociendo que el proceso de sanación trasciende la resolución del incidente específico para incluir la restauración de la confianza, la autonomía y la capacidad de participación social (Beck et al., 2019). Esta perspectiva resulta especialmente relevante cuando se considera que los servicios psicológicos deben ser accesibles, apropiados y receptivos a las comunidades locales, incluyendo trabajo continuo para mejorar conocimiento, curiosidad y respeto por diversidades culturales (D'Ardenne et al., 2005).

Los modelos cognitivos proponen que las interpretaciones negativas pueden conducir a trastornos psicológicos duraderos si la persona no logra encontrar una explicación significativa o se adapta en exceso a la amenaza, como ocurre con víctimas mayores que concluyen que "el mundo digital se ha vuelto demasiado peligroso" y desarrollan estrategias de evitación que les privan de los beneficios de la inclusión digital (Ehlers & Clark, 2000; Beck et al., 1979). El trastorno de estrés postraumático, la depresión y la ansiedad que pueden derivarse de la cibervictimización tienen raíces en creencias negativas sobre la peligrosidad del mundo, sentimientos de incompetencia y sobreestimación de amenazas que, sin acompañamiento adecuado, se traducen en conductas disfuncionales como el aislamiento digital, la dependencia excesiva de terceros o la hipervigilancia que paraliza la interacción tecnológica (Clark & Beck, 2010; Salkovskis, 1996).

La comprensión profunda de las dinámicas específicas de la cibervictimización en personas mayores requiere reconocer que estas difieren sustancialmente de otras formas de victimización por sus características de invisibilidad, persistencia digital de las evidencias y pérdida de control sobre los procesos de revelación (Miró-Llinares, 2013). **Los ciberdelincuentes explotan vulnerabilidades psicológicas específicas de este colectivo: menor familiaridad con herramientas digitales, mayor confianza en figuras de autoridad, tendencia a la discreción sobre temas financieros y, paradójicamente, mayor propensión a ayudar a otros, que los estafadores manipulan mediante técnicas sofisticadas de ingeniería social que simulan emergencias familiares o solicitudes benéficas** (Kemp & Erades Pérez, 2023). Estos ataques **específicamente diseñados para personas mayores aprovechan inseguridades tecnológicas y una mayor disposición a confiar en autoridades, incorporando vectores mixtos como teléfonos fijos y computadoras o SMS y sitios web fraudulentos que aumentan la complejidad de detección y respuesta** (Kemp & Erades Pérez, 2023).

El acompañamiento integral especializado debe fundamentarse en principios de atención informada por el trauma que reconozcan la complejidad del impacto psicosocial y eviten aproximaciones culpabilizadoras o paternalistas que reproduzcan dinámicas edadistas (Jansen & Leukfeldt, 2018).

Los enfoques recomendados por Jansen y Leukfeldt (2018) enfatizan la importancia terapéutica de hablar sobre la experiencia del crimen, resumiendo las consideraciones para bancos, policía y organizaciones de atención a víctimas en dos enfoques generales fundamentales: adoptar una actitud de apoyo, mostrando empatía y comprensión mientras se evita juzgar o culpar a la víctima; y proporcionar actualizaciones constantes sobre cada caso, contribuyendo a que las víctimas se sientan escuchadas, reconocidas, protegidas y cuidadas. Este marco de actuación debe complementarse con competencias específicas en detección de signos de vulnerabilidad, comunicación empática libre de estigma, manejo de la vergüenza y la autoculpa, y coordinación efectiva con recursos especializados que eviten la fragmentación de la atención (Caravaca-Llamas & Girona-Berná, 2021).

El diseño de programas de acompañamiento debe incorporar la comprensión de que las intervenciones con personas mayores víctimas de fraude no pueden centrarse únicamente en la recuperación de fondos, sino también en bienestar y conexiones sociales, incluyendo orientación que ayude a lidiar con las reacciones emocionales que habitualmente siguen al fraude (Kemp & Erades Pérez, 2023).

De acuerdo con E1, los proyectos más sostenibles son aquellos que articulan redes comunitarias de apoyo, actuando como "antenas" que detecten señales de riesgo y deriven casos a recursos especializados. Este enfoque comunitario fortalece la confianza institucional y convierte la prevención digital en una herramienta de cohesión social y bienestar colectivo.

> *"Incluso poder generar talleres creativos con estas personas de cómo lo podemos comunicar, cómo podemos intervenir, el espacio, de qué forma podemos hacerlo, llegar más a nuestro barrio, a nuestra tienda de confianza, a nuestra farmacia, a los bares donde vamos, etc. Es decir, como poder generar también grupos de activismo en los propios espacios para que intervengan de alguna manera y sean ellos también los que puedan transmitir esta información" (E1, 45:42)*

Las mejores prácticas de servicios de apoyo a víctimas de fraude documentadas internacionalmente subrayan la importancia de **respuestas multidisciplinarias** que combinen asesoramiento legal, soporte técnico para recuperar seguridad digital, apoyo psicológico para manejar el impacto emocional y educación para **prevenir** futuros incidentes (Cross et al., 2017). Sin embargo, estos servicios especializados no están ampliamente disponibles en países europeos como España, donde la respuesta corresponde principalmente a fuerzas policiales e instituciones financieras, y donde víctimas de fraude expresan frecuentemente insatisfacción con la atención recibida, haciendo evidente la necesidad de explorar cómo mejorar las respuestas a fraudes desde la perspectiva de las víctimas (Button & Cross, 2017; Kemp & Erades Pérez, 2023).

La capacitación de profesionales que trabajan con personas mayores emerge como elemento crítico para mejorar la calidad de la respuesta institucional y comunitaria, **requiriendo formación específica en competencias relacionales, detección de signos de vulnerabilidad, comunicación empática libre de estigma, manejo de la vergüenza y la autoculpa, y coordinación efectiva con recursos especializados** (Caravaca-Llamas & Girona-Berná, 2021). Esta formación debe incluir técnicas de escucha activa, lenguaje libre de reproches, guiones claros de primera acogida, protocoles de derivación responsable y manejo de la revictimización secundaria, así como estrategias para fortalecer la confianza institucional en cada interacción (Jansen & Leukfeldt, 2018). Los profesionales requieren también competencias específicas para manejar la interseccionalidad de factores que condicionan la vulnerabilidad, incluyendo género, clase social, nivel educativo y estado civil, que influyen tanto en los riesgos de victimización como en los procesos de recuperación (Segal et al., 2021).

Las acciones formativas cocreadas, adaptadas y orientadas a generar una guía en espacios compartidos son pertinentes y beneficiosas porque alinean la prevención técnica con el acompañamiento psicoemocional y la coordinación institucional, mejorando la adherencia, reduciendo la vergüenza y acelerando la búsqueda de ayuda en personas mayores ante incidentes digitales (Kemp & Erades Pérez, 2023; Segal, Doron, & Mor, 2021). Este enfoque integra principios de atención informada y evita prácticas culpabilizadoras o paternalistas, lo que resulta crucial para **un colectivo que a menudo sufre subregistro por miedo al juicio y estigma asociado a la edad y a la competencia digital percibida** (Jansen & Leukfeldt, 2018; Levy, 2001).

La cocreación incorpora la voz de las personas mayores en la definición de objetivos, contenidos y formatos, aumentando pertenencia, relevancia percibida y eficacia de las intervenciones, tal como reflejan experiencias de inclusión digital que ajustan materiales a necesidades reales del territorio (Morrison et al. 2021; Centro de Inteligencia Digital Alicante, 2022). La evidencia sectorial en protocolos de intervención subraya, además, que la personalización y la documentación del estado emocional, barreras cognitivas y necesidades específicas son condiciones de calidad para evitar revictimización y adecuar la respuesta a cada usuaria, criterios que la cocreación facilita al diseñar materiales y circuitos con quienes los usarán (Beck et al., 2019; D'Ardenne et al., 2005). La participación activa en espacios compartidos (equipamientos y centros para personas mayores) habilita la detección temprana y la primera atención sin exigir denuncia formal, con guiones claros y derivación responsable, algo que los dispositivos no cocreados suelen pasar por alto al priorizar canales exclusivamente digitales (Jansen & Leukfeldt, 2018; Caravaca-Llamas & Girona-Berná, 2021).

Las acciones formativas para trabajar con las personas mayores se centran en ejercicios de validación emocional, manejo de vergüenza y autoculpa, y mensajes antiestigma que normalizan pedir ayuda y desplazan el foco de la culpa hacia el delito, coherentes con recomendaciones internacionales para bancos, policía y servicios de víctimas sobre empatía, no juicio y actualizaciones periódicas del caso (Jansen & Leukfeldt, 2018; Button & Cross, 2017). La pertinencia del enfoque aumenta en contextos de riesgo elevando la autoeficacia y el control percibido: al practicar guiones de fraude, verificación de fuentes y conservación de evidencias, **las personas mayores adquieren competencias operativas que se consolidan gracias al soporte emocional y a la claridad de los itinerarios de ayuda, mejorando el tiempo de reacción y la calidad de la denuncia** (Morrison et al., 2021; Cross, Richards, & Smith, 2017).

5.7. Del silencio a la acción: comunicación sin estigmas que visibiliza el daño, guía la ayuda y refuerza la confianza

Una comunicación clara, en lectura fácil y apoyada en materiales visuales transforma las advertencias abstractas en rutas de acción concretas que reducen la carga cognitiva, disminuyen la ansiedad y facilitan la detección temprana y el acompañamiento sin barreras técnicas ni estigma en personas mayores expuestas a incidentes digitales o dudas razonables de fraude (Morrison, Coventry, & Briggs, 2021; Beck et al., 2019). Cuando los mensajes visibilizan el daño psicológico, normalizan pedir ayuda y ofrecen instrucciones breves y memorables —por ejemplo, “cuelga, verifica y llama”—, aumentan significativamente la probabilidad de que la persona pida apoyo a tiempo y de que su entorno cercano identifique señales de riesgo y active conductas de protección, en coherencia con un enfoque informado por el trauma y libre de edadismo (Jansen & Leukfeldt, 2018; Segal et al., 2021).

La evidencia victimológica y de intervención muestra que la claridad comunicativa y la accesibilidad del soporte son determinantes del tiempo hasta la consulta, de la adherencia a las pautas de actuación y de la reducción del malestar emocional tras el incidente, por lo que las guías deben organizarse por capas temporales (“ahora” proteger, “hoy” avisar, “esta semana” restaurar) con tipografía grande, alto contraste, verbos de acción y ausencia de jerga técnica (Miró-Llinares, 2013; Morrison et al., 2021). La producción de materiales visuales tangibles y reutilizables permite seguir instrucciones en segundos incluso con fatiga o menor alfabetización digital, desplazando la carga desde la pericia individual hacia entornos que protegen por diseño (Centro de Inteligencia Digital Alicante, 2022; Button & Cross, 2017) . En este ecosistema, la línea 017 de ayuda en ciberseguridad y los puntos presenciales de confianza actúan como canales de baja barrera que convierten la primera consulta en un acto

sencillo y seguro, con promesa de confidencialidad y actualizaciones periódicas del caso para evitar incertidumbre y abandono (INCIBE, “Tu Ayuda en Ciberseguridad”).

Un diseño comunicativo anti-estigma, validante y culturalmente competente es esencial para disminuir el subregistro asociado a vergüenza y miedo al juicio, y para desplazar el foco de la culpa hacia el delito, coherente con las recomendaciones a bancos, policía y servicios de víctimas de escuchar sin juzgar y mantener informadas a las personas afectadas (Jansen & Leukfeldt, 2018; Beck et al., 2019). La cocreación de contenidos con personas mayores asegura pertinencia y aumenta la autoeficacia, mientras que el uso de testimonios y un video de sensibilización protagonizado por mayores activa el “efecto cascada” que rompe el silencio, reduce la evitación digital y mejora la intención de denuncia, alineando prevención técnica con bienestar psicosocial y apoyo comunitario (Segal et al., 2021; Kemp & Erades Pérez, 2023).

En conjunto, una comunicación clara, accesible y visual, reforzada por canales no digitales, señalética común y una ventanilla de referencia, es el eje operativo que convierte la prevención en acompañamiento efectivo, acelera la detección temprana y dignifica la recuperación, integrando capacidades individuales con entornos y circuitos de ayuda confiables, medibles y responsables (Miró-Llinares, 2013; Centro de Inteligencia Digital Alicante, 2022).

5.8. Conclusiones

Las personas mayores afrontan la cibervictimización en un entorno digital cada vez más complejo, donde el foco debe desplazarse del delito y su coste económico hacia la **experiencia de la víctima, su recuperación integral y el fortalecimiento de su autonomía digital**. Este cambio de perspectiva exige una respuesta sistémica que combine **prevención, detección, acompañamiento y gobernanza**, sustentada en métricas de impacto comparables y una evaluación continua orientada a la mejora.

La **prevención** debe centrarse en metodologías prácticas, accesibles y emocionalmente seguras: simulaciones de fraudes habituales, verificación de fuentes, higiene digital y aprendizaje entre pares. La evidencia muestra que los entornos formativos que reducen el alarmismo y promueven la confianza facilitan la adquisición de hábitos protectores y disminuyen la evitación digital.

En la **detección y el acompañamiento**, la llamada “primera milla” de atención debe garantizar escucha empática, contención emocional, orientación inmediata y derivación responsable. Ofrecer ayuda sin exigir denuncia reduce la revictimización, mitiga la vergüenza y mejora la adherencia a los circuitos de apoyo.

En materia de **comunicación pública**, se requiere un enfoque informado por el trauma y libre de edadismo, que valide emociones y normalice la búsqueda de apoyo. Los mensajes breves, visuales y accionables, junto con testimonios de “pares que cuidan a pares”, fortalecen la confianza institucional y fomentan la denuncia sin culpabilizar.

El **diseño seguro por defecto** constituye, además, una estrategia de prevención: interfaces legibles, navegación sencilla y retroalimentación clara disminuyen la carga cognitiva y la exposición al riesgo, desplazando la responsabilidad de la seguridad desde el usuario hacia sistemas tecnológicos que protegen por diseño.

Una **gobernanza multinivel** efectiva requiere roles nítidos, intercambio de información responsable y objetivos compartidos entre banca, cuerpos policiales, administraciones y comunidad. Los dispositivos comunitarios (casales, centros cívicos, asociaciones vecinales) deben actuar como antenas de alerta y puntos de primera acogida, dotados de guías, microherramientas y protocolos de atención coherentes.

Por último, la **evaluación de impacto** debe ir más allá de la satisfacción inmediata y considerar cambios reales en la conducta, el bienestar emocional, la confianza institucional y la autonomía digital. Medir estos indicadores de forma sostenida permitirá ajustar estrategias y consolidar aprendizajes duraderos.

En definitiva, avanzar hacia un **ecosistema de bienestar digital** implica cuidar tanto la seguridad tecnológica como la dimensión emocional del proceso, garantizando accesibilidad, acompañamiento humano y participación activa de las personas mayores. Desde esta base, el siguiente capítulo profundiza precisamente en este componente humano: **la sensibilización y el apoyo emocional frente a la cibervictimización**, entendidos como pilares del acompañamiento preventivo y postdelito. Abordar la dimensión emocional (miedo, vergüenza, desconfianza o pérdida de autoestima) resulta esencial para que las intervenciones técnicas se conviertan en procesos de **reparación, empoderamiento y resiliencia digital**.

6. Personas mayores y seguridad digital: enfoques de sensibilización y apoyo frente a la cibervictimización

En la era actual de expansión tecnológica, las personas se ven forzadas a **adaptarse de manera inmediata a cambios constantes y profundos** (Gheorgita, 2014). Este proceso de ajuste resulta especialmente desafiante para la población mayor, que no ha vivido experiencias previas comparables y, por tanto, puede desconocer sus propios límites o enfrentarse a mayores dificultades de adaptación. La ciberseguridad, entendida como una competencia ciudadana esencial, exige desarrollar **capacidades cognitivas, emocionales y sociales** para desenvolverse en entornos digitales seguros, lo que requiere metodologías educativas inclusivas y emocionalmente sostenibles.

En este contexto, el presente bloque articula un **ecosistema de herramientas y recursos** que conecta la formación preventiva en competencias digitales con un **acompañamiento accesible, empático y continuado** en la detección y gestión de incidentes. El propósito es superar el enfoque tecnocentrista y alarmista habitual, situando en el centro la **autonomía personal, la validación emocional y la continuidad de cuidados** centrados en la persona mayor y su bienestar digital.

El resultado esperado del estudio es la construcción de un **modelo de ciberseguridad integral**, el *OSICSAM* (Modelo de Concienciación sobre Ciberseguridad Organizacional, Social e Individual para Personas Mayores). Este modelo incorpora factores organizativos, sociales e individuales que inciden en la capacidad de las personas mayores para generar conciencia y comportamientos digitales seguros.

Dentro de este marco general, se desarrolla el **submodelo ISACM (Modelo de Concienciación sobre Ciberseguridad Individual)**, que identifica tres dimensiones clave, alineadas con los principios de la norma ISO/IEC 27002:

1. **Concienciación sobre la ciberseguridad:** grado de comprensión sobre la importancia de los controles y medidas de protección digital, y su influencia en la capacidad para reconocer y evitar fraudes.
2. **Capacidad de concienciación:** habilidad práctica y cognitiva para identificar situaciones de riesgo, interpretar señales de alerta y tomar decisiones informadas.
3. **Concienciación del riesgo:** análisis de la brecha entre la percepción subjetiva del riesgo y el nivel real de conocimiento y preparación.

El modelo ISACM proporciona una **base conceptual y operativa** para el diseño de programas de formación y acompañamiento que integren las dimensiones técnicas,

emocionales y sociales de la seguridad digital, fortaleciendo la **autonomía y la resiliencia digital** del colectivo mayor.

6.1. Principios pedagógicos: aprendizaje adulto y clima de confianza

El proceso formativo se inspira en los fundamentos de la **pedagogía social y la andragogía**, que adaptan la enseñanza a las características específicas del aprendizaje adulto (Gheorgita, 2014; Knowles, 1973). Según la evidencia y las entrevistas realizadas, el **factor determinante para la eficacia de las formaciones** es generar un **clima de confianza** desde el primer día.

Los principios pedagógicos se resumen en seis ejes:

1. Las personas adultas necesitan **comprender la utilidad** del aprendizaje y vincularlo a objetivos concretos de su vida cotidiana (Knowles, 1970,1973; Lindeman, 1989).
2. Requieren ser tratadas como **personas competentes y autónomas**, con capacidad de dirigir su propio proceso de aprendizaje (Knowles, 1973; Brookfield, 1986).
3. Sus **experiencias previas** deben aprovecharse como punto de partida, personalizando estrategias y favoreciendo la participación activa (Knowles, 1970,1973; Lindeman, 1989; Mezirow, 1991).
4. El conocimiento debe orientarse a la **resolución de problemas reales**, integrando las dimensiones personales y sociales del aprendizaje (Kolb, 1984).
5. La motivación del adulto es **intrínseca**, vinculada a la autorrealización, la utilidad práctica o el deseo de independencia digital (Knowles, 1973; Lindeman, 1926; Maslow, 1954).
6. La formación debe **reconocer la diversidad** del colectivo sénior, adaptándose a diferentes niveles de alfabetización, contextos culturales y situaciones vitales (Jarvis, 2012; Mezirow, 1991; Freire, 1970).

El diseño de los talleres se centra en metodologías participativas, experienciales y no paternalistas, privilegiando la práctica guiada y la ejemplificación cotidiana frente al tecnicismo y al discurso abstracto (Knowles, 1984, citado en Paloş et al., 2007, pp. 107-110).

La persona entrevistada E2 observa que muchas personas mayores **asocian la tecnología con peligro**, influenciadas por el bombardeo mediático de noticias sobre fraudes. Este temor fomenta la **evitación tecnológica** —la idea de que “si no uso el móvil, estoy más seguro”— y aumenta el aislamiento digital. La formación preventiva debe, por tanto, **combinar cautela y confianza**, promoviendo una relación más tranquila y curiosa con las herramientas digitales.

> *“[…] tienen mucho miedo a utilizar el teléfono móvil, a utilizar la tecnología, porque están constantemente bombardeados de mensajes, sobre todo en las noticias, pues me han robado*

mi cuenta en el banco… […] entonces al ver esas noticias lo que hacen es, pues entonces no utilizo el móvil […] y estaré más seguro, eso es lo que nos estamos encontrando mayoritariamente" (E2, 4:08).

6.2. Enfoques formativos: diversidad, intergeneracionalidad y dimensión emocional

El colectivo de personas mayores presenta una notable **diversidad de perfiles, capacidades y trayectorias vitales**, que exige que las acciones formativas sean flexibles, adaptables y personalizadas. Las formaciones deben atender desde personas activas y autónomas que buscan ampliar su participación digital hasta aquellas que precisan acompañamiento intensivo por motivos cognitivos, físicos o emocionales. Esta heterogeneidad obliga a diseñar propuestas **centradas en la persona**, que reconozcan los ritmos, motivaciones y necesidades de cada participante.

Superar la **visión tecnocentrista** es un requisito clave. La relación de muchas personas mayores con la tecnología está mediada por el miedo, la desconfianza o la frustración, sentimientos que suelen derivarse no de una falta de capacidad, sino de experiencias negativas previas o de discursos sociales que las infantilizan. Por ello, las formaciones deben integrar una **dimensión emocional y relacional**, trabajando la autoestima digital, desestigmatizando el error y ofreciendo entornos de aprendizaje seguros, amables y libres de juicios. No se trata solo de transmitir conocimientos técnicos (contraseñas, PIN o verificación de enlaces), sino de **acompañar procesos de confianza y reconocimiento de la propia competencia**.

Los expertos entrevistados confirman que el acompañamiento profesional y comunitario es esencial para **reducir la culpa y el aislamiento** tras una situación de fraude o intento de estafa. La persona entrevistada E1 subraya que, incluso cuando las personas mayores detectan un engaño, tienden a minimizarlo o evitar la denuncia por desconfianza institucional o miedo al juicio. En este sentido, los espacios grupales actúan también como **entornos de apoyo emocional**, donde compartir experiencias transforma la vergüenza individual en aprendizaje colectivo.

> *"Me parece interesante poder hacer grupos de ayuda mutua, etcétera. Pues también es interesante el acompañamiento a la víctima, incluso no de dar este recurso a la policía, ¿no? para cuando detecten a alguien que haya sido estafado, pues le lo puedan derivar a estos grupos que es verdad que este tipo de talleres funcionan muy bien" (E1, 45:42).*

En línea con esta idea, E3 destaca que los espacios grupales de formación o sensibilización también actúan como entornos de apoyo emocional y, además, cuando la formadora se muestra también vulnerable —"todos podemos ser víctimas"—, se genera validación, empatía y autoconfianza.

> *"Yo siempre empiezo poniéndome a mí como posible víctima, porque por desgracia, les digo, todos somos posibles víctimas de estos delitos. Por ser personas mayores, también son posibles víctimas, pero lo que intento es que no tengan miedo de, como soy mayor me va a pasar a mí. Le va a pasar a usted, como me puede pasar a mí, exactamente igual" (E3, 7:03).*

> *"Trabajo mucho con las experiencias de los asistentes, incluso las de sus amigos o familiares. Les hago participar, y les pregunto qué podemos hacer para evitar los engaños. A veces, alguien dice: '¿Cómo voy a dar mis datos?' y otro admite que, a pesar de todo, los ha dado. Aunque parezca ilógico, los estafadores nos manipulan para conseguir nuestros datos, como el DNI o el nombre" (E3, 07:03).*

El **aprendizaje entre iguales** emerge como una metodología eficaz. Escuchar a otras personas de edad similar que han vivido experiencias parecidas reduce la barrera emocional y facilita la comprensión de conceptos complejos. Tal como señala E5, el *mentoring* entre personas mayores refuerza la conexión emocional y mejora la asimilación de contenidos.

> *"Con ellos, funciona muy bien que, en la formación en algún momento, pueda explicarles cosas personas de su misma edad, muchísimo. Realmente hacer mentoring con gente de su edad, es algo que le suele funcionar superbién, muy, muy bien" (E5, 25:16).*

Asimismo, el **aprendizaje intergeneracional** constituye una oportunidad para reforzar vínculos y romper estereotipos edadistas. El intercambio con personas jóvenes, ya sea en contextos familiares o comunitarios, permite a los mayores acceder a nuevos conocimientos en un entorno de confianza, mientras los jóvenes desarrollan empatía y una visión más realista del envejecimiento. Las personas mayores, a menudo más desconfiadas respecto a los medios digitales, encuentran gran valor en la participación activa de familiares jóvenes (nietos, sobrinos), quienes comparten sus experiencias y conocimientos de manera natural. Esto refuerza la confianza y facilita la asociación de conceptos, haciendo el aprendizaje más vivencial.

Por otro lado, muchas personas repiten los mismos talleres, no solo para consolidar aprendizajes, sino porque encuentran en ellos un **espacio de socialización y bienestar**, que combate la soledad no deseada.

> *"Hay personas mayores que repiten la misma cápsula varias veces, incluso van por las bibliotecas buscando al formador en quien confían. Más que aprender, muchos vienen por compañía y me acuerdo de una señora que me decía, yo la repito muchas veces y cada vez que vengo me quedo con un concepto diferente y ya estoy feliz" (E2, 25:54).*

El éxito de estos enfoques depende también de **profesionales y referentes comunitarios capacitados**, capaces de identificar necesidades, acompañar desde la escucha activa y mediar ante situaciones de riesgo. Su papel es determinante tanto en la prevención como en el apoyo emocional y práctico tras un incidente digital. Según E2, el factor determinante para la eficacia de las formaciones es generar un clima de confianza desde el primer día.

> *"Los que trabajamos mucho con los formadores es crear un ambiente de confianza desde el inicio, al final no vamos a acabar un contenido, sí que tenemos, pues, una serie de contenido para dar, pero si no acabamos no pasa nada. Lo importante es que salgan de la sesión con una cosa aprendida y que se sientan seguros" (E2, 8:50)*

Finalmente, se propone diversificar los **formatos formativos** para aumentar la participación y la retención: cápsulas breves, talleres creativos, grupos de ayuda mutua o sesiones de cocreación pueden combinar contenidos técnicos con dinámicas participativas basadas en el humor, el teatro social o el vídeo. Dado que WhatsApp es uno de los canales más utilizados por este grupo etario, su uso para difundir mensajes breves de sensibilización también se considera una herramienta eficaz.

De forma transversal, las personas entrevistadas coinciden en varios aspectos clave:

- La **necesidad de visibilizar la diversidad** de las víctimas y adaptar las formaciones a distintos niveles de alfabetización digital.
- El **uso de lenguaje claro y ejemplos cotidianos** que traduzcan los tecnicismos y faciliten la comprensión.
- La **enseñanza orientada a la detección autónoma del fraude**, reconociendo las señales y sensaciones asociadas a un intento de estafa.
- La **importancia de mantener formatos presenciales y de proximidad**, que favorezcan el contacto humano, la confianza y la continuidad del aprendizaje.

En conjunto, estos enfoques formativos permiten convertir la prevención técnica en un proceso de **aprendizaje emocional y relacional**, donde la seguridad digital se construye desde la confianza, la empatía y la comunidad.

Es fundamental desarrollar iniciativas educativas dirigidas a la población mayor, especialmente en relación con sus necesidades sociosanitarias, con el objetivo de mejorar su calidad de vida.

Para garantizar el bienestar de las personas mayores, es esencial que todos los actores sociales sumen esfuerzos para facilitar su permanencia en el entorno familiar. En este contexto, las políticas sociales deben anticipar la implementación de programas integrales de educación para adultos, fomentando actitudes proactivas hacia el envejecimiento y promoviendo el acceso a cuidados médicos, psicológicos y sociales en el hogar. En la medida de lo posible, tanto los proveedores públicos como privados deben asumir la responsabilidad de atender estas necesidades (Gheorgita, 2014).

6.3. Formación, acompañamiento y comunicación para un bienestar digital

Este bloque plantea un puente explícito entre la formación en competencias digitales orientada a la prevención y la necesidad de reforzar el acompañamiento emocional cuando se detecta un posible fraude o abuso, integrando ambos planos en un mismo itinerario centrado en la persona mayor y su bienestar digital. La premisa es triple: por un lado, **consolidar hábitos y habilidades prácticas de seguridad** (verificación, protección de identidad, gestión de contraseñas y reconocimiento de guiones de estafa) sin recurrir al alarmismo que incrementa la ansiedad; por otro, **reconocer los sentimientos generados por el suceso y no caer en la victimización-revictimización**, y por último, garantizar que, ante la mínima sospecha o confirmación de incidente, **es conocida la primera línea de ayuda** accesible, empática y coordinada que ofrezca contención emocional, pautas claras de actuación y derivación efectiva sin revictimización secundaria.

El programa parte de una constatación creciente: las personas mayores se enfrentan a riesgos digitales que no solo amenazan su seguridad económica, sino también su bienestar emocional y su confianza en el entorno digital. Ante esta realidad, se propone un **itinerario integral de prevención, acompañamiento y empoderamiento** que combina tres herramientas complementarias: un **curso de formación**, un **workshop para profesionales** y un **díptico divulgativo**.

La propuesta se basa en una idea central: **prevenir el fraude digital no consiste solo en aprender a protegerse, sino también en saber pedir ayuda, comprender las emociones que genera una estafa y reconstruir la confianza en uno mismo y en las instituciones**. Así, la prevención deja de ser un fin en sí mismo y se convierte en la puerta de entrada a un bienestar digital pleno, que abarca tanto la dimensión técnica como la emocional y comunitaria.

- **Talleres de ciberdelincuencia para personas mayores**

El primer componente del programa son **talleres prácticos** de 1 h 30 min a 2 h de duración, dirigidos a grupos reducidos de personas mayores. Su objetivo es proporcionar un espacio cercano, participativo y libre de juicios donde aprender a reconocer las estafas digitales más comunes, identificar las emociones que intervienen en cada tipo de fraude y conocer los recursos de ayuda disponibles en caso de ser víctima.

A lo largo de los talleres[11] se abordan las modalidades de fraude más frecuentes (suplantaciones bancarias, estafas de soporte técnico, mensajes afectivos manipuladores…), explorando las **emociones que suelen acompañarlas**, como la urgencia, la confianza excesiva, la culpa o el miedo. Mediante ejemplos reales y dinámicas participativas, las personas participantes aprenden a **reconocer los patrones emocionales que los estafadores explotan**, de modo que puedan anticiparlos y reaccionar con serenidad.

El enfoque es **centrado en la persona y anti-edadista**, reconociendo que la vergüenza, la culpa o la confusión son reacciones comprensibles y que el fraude es un delito del que la víctima no es responsable. Los talleres promueven la **validación emocional**, la **normalización de la búsqueda de ayuda** y la conexión con una **primera línea de apoyo local**, sin olvidar las pautas de seguridad digital básicas.

Estas sesiones se han desarrollado en **espacios de confianza** (centros cívicos y equipamientos de personas mayores) y utilizan un lenguaje claro y materiales adaptados a distintos niveles de alfabetización digital. Incluye, además, el tríptico divulgativo (que se explica a continuación), como resumen del taller.

- **Tríptico divulgativo: comunicar sin miedo, acompañar con empatía**

El tercer elemento del programa es un **tríptico divulgativo** destinado a sensibilizar y ofrecer información clara, cercana y libre de tecnicismos a las personas mayores y su entorno. Su función es doble: **informar y desestigmatizar**.

El material recoge, de forma visual y comprensible, los **tres pilares de todo el itinerario formativo**:

1. **Reconocimiento del daño y validación emocional.**
2. **Normalización de la búsqueda de ayuda.**
3. **Instrucciones inmediatas y seguras** para actuar ante un posible fraude o sospecha.

Se pone a disposición de la ciudadanía y se distribuye en equipamientos de personas mayores y centros de barrio, donde profesionales o vecinos pueden ejercer como **"agentes antena"** para detectar y orientar posibles casos. De este modo, el tríptico extiende el alcance

[11] Ver anexo 3 para leer el dosier del formador

del programa a la comunidad, reforzando la red de apoyo informal y favoreciendo una cultura de acompañamiento respetuosa y libre de paternalismo.

Fuente: Elaboración propia para los talleres de Cataluña.

- **Workshop para profesionales de proximidad**

En paralelo al taller, el programa incorpora un **workshop aplicado para profesionales** [12]que trabajan en contacto directo con personas mayores: personal técnico de servicios sociales, dinamizadores de equipamientos, voluntariado, policía local o profesionales del ámbito comunitario.

Por ello, diseñar un workshop en espacios comunitarios, como centros de personas mayores, casales o entidades de base local, convierte dichos espacios en **entornos protectores** y de empoderamiento, no solo de transferencia de conocimiento técnico, sino de fortalecimiento de redes sociales, confianza digital, acompañamiento emocional y detección precoz de vulnerabilidades. En este sentido, la metodología participativa refuerza la dimensión relacional y de cuidado mutuo: no se trata solo de «enseñar a usar tecnología», sino de trabajar desde el acompañamiento, la escucha activa, la empatía y la acción colectiva.

Este taller replicable busca **dotar a estos agentes de competencias relacionales, comunicativas y de derivación**, de modo que puedan ejercer una primera acogida empática y libre de juicios ante situaciones de fraude digital.

Otra dimensión fundamental es la **co-creación de herramientas**. Cuando los participantes, tanto profesionales como voluntarios de espacios de personas mayores, colaboran en el diseño de fichas, checklists, scripts de acogida, circuitos de derivación, etc., se favorece la apropiación, la relevancia contextual, la sostenibilidad de la intervención y su transferencia al día a día. Esta estrategia está alineada con los principios de la Investigación-Acción Participativa (IAP) (Kemmis & McTaggart, 2000) que propone implicar a los sujetos del cambio en la producción activa de sus herramientas y de sus procesos de mejora.

La priorización de competencias mediante herramientas interactivas (por ejemplo, votación digital, uso de Wooclap u otros recursos) permite también la configuración democrática del taller: los participantes deciden qué problemas son más urgentes, qué competencias deben adquirirse antes, qué recursos son más relevantes para ellos. Esto no solo incrementa su motivación y compromiso, sino que configura el taller como un espacio de **co-decisión** y liderazgo compartido.

El workshop combina teoría y práctica a través de:

- **Protocolos y guiones de actuación** para la primera escucha, derivación responsable y coordinación con la “ventanilla de referencia”.

[12] Ver anexo 7 para el programa del workshop

- **Checklist de señales de vulnerabilidad**, pautas de lectura fácil y estrategias para reducir la revictimización secundaria.
- **Debriefing emocional**, para que las propias personas profesionales aprendan a gestionar el impacto emocional que estos casos pueden generarles.

En el worskshop se presenta un **Toolkit**[13] (tarjetas con pasos inmediatos, scripts de llamadas, guías locales de recursos y canales de consulta con expertos), que facilita la aplicación práctica y el aprendizaje continuado dentro de los equipos. El workshop se concibe como un espacio de **aprendizaje organizativo y cooperativo**, en el que cada detección alimenta la mejora de los contenidos y protocolos institucionales.

Un enfoque integral: de la prevención al empoderamiento

En conjunto, este diseño de workshop se justifica por varios motivos clave:

1. **Relevancia práctica**: En el contexto de la prevención de ciberdelincuencia para personas mayores, el taller ofrece un contenido que responde a una necesidad real, actual y de gran importancia social.
2. **Empoderamiento y autonomía**: Más allá de la educación técnica, se promueve que los participantes tomen un papel activo, co-diseñen herramientas, decidan prioridades y actúen en su entorno. Esto favorece la autonomía y reduce la percepción de vulnerabilidad.
3. **Contextualización comunitaria**: Utilizar los espacios de personas mayores y las dinámicas de red comunitaria amplifica el impacto del taller, al situar la formación en un contexto de confianza, cercanía y apoyo mutuo.
4. **Enfoque emocional y relacional**: Incorporar la dimensión emocional (miedo, vergüenza, implicación social) es clave para que las personas mayores se sientan comprendidas, acompañadas y seguras, lo cual facilita la adopción de prácticas de protección digital.
5. **Sostenibilidad y transferencia**: La co-creación de herramientas y la toma de decisiones conjunta favorecen que los resultados del taller no queden aislados, sino que se integren en los espacios de personas mayores, se adapten localmente y se sostengan con el tiempo.

La combinación de estos tres productos genera un **ecosistema coherente de intervención**:

- los **talleres** fortalecen las competencias digitales, la autonomía y la seguridad emocional de las personas mayores;

[13] Ver anexo 8.

- el **workshop** mejora la capacidad de respuesta y coordinación de los profesionales;
- y el **díptico** actúa como herramienta de sensibilización y refuerzo comunitario.

El conjunto responde a una misma lógica: **prevenir, acompañar y transformar la experiencia del fraude en aprendizaje y resiliencia digital.** Cada acción formativa o comunicativa busca reducir la culpabilidad, fomentar la denuncia y construir relaciones de confianza entre ciudadanía e instituciones.

Con este enfoque integral, el programa no solo mejora las capacidades digitales, sino que **teje redes de apoyo y bienestar emocional** en torno a la persona mayor, convirtiendo el cuidado digital en un valor compartido por toda la comunidad.

6.4. Evaluación

La **evaluación** en el contexto de los talleres y workshops desempeña un **papel fundamental en la mejora continua de los procesos formativos**. Este proceso no solo busca medir la satisfacción de los participantes, sino también generar un espacio de reflexión entre los facilitadores y los participantes, que permita ajustar la metodología, los contenidos y los enfoques pedagógicos a las necesidades emergentes. De este modo, la evaluación se convierte en una herramienta clave para garantizar la efectividad del aprendizaje y la consecución de los objetivos pedagógicos establecidos. En especial, en el ámbito de la educación para adultos, donde la autonomía y la participación activa son esenciales, la evaluación fomenta un aprendizaje significativo, transformador y centrado en la persona.

Una de las herramientas más utilizadas en este proceso de evaluación son las **encuestas de satisfacción**. Estas encuestas permiten captar tanto información cuantitativa como cualitativa sobre diversos aspectos del taller, tales como la claridad de los contenidos, la calidad de las actividades, el ambiente creado por los facilitadores, y la aplicabilidad de lo aprendido en la vida cotidiana de los participantes. Las preguntas cerradas proporcionan datos cuantificables que permiten comparar la satisfacción entre diferentes grupos y ediciones del taller, mientras que las preguntas abiertas recogen comentarios más detallados que pueden ofrecer información valiosa sobre las fortalezas y debilidades percibidas por los participantes. Esta doble vertiente de la evaluación permite obtener **una visión integral, personalizada y profunda** sobre lo que los participantes valoran más o lo que consideran que podría mejorarse, facilitando así una mejora constante en las formaciones.

Además de las encuestas de satisfacción, la **observación directa es otra herramienta clave en el proceso evaluativo**. A través de esta técnica, los facilitadores pueden observar, en tiempo real, las interacciones entre los participantes y los contenidos del taller. Esta

observación permite captar comportamientos, dinámicas de grupo y reacciones espontáneas que no siempre son evidentes a través de las encuestas. También ofrece una visión más profunda del nivel de compromiso de los participantes y de la efectividad de las actividades, especialmente en talleres que emplean metodologías experienciales y de participación activa. La observación directa permite a los facilitadores ajustar su enfoque pedagógico de manera inmediata, respondiendo a las necesidades emergentes de los participantes y mejorando la dinámica de aprendizaje en tiempo real. Por otro lado, en este caso, también hubo evaluadores externos[14] que fueron a los talleres e iban hablando con los facilitadores para ir ajustando los talleres.

Es importante destacar que la evaluación debe estar integrada a lo largo de todo el proceso formativo, no limitándose a un ejercicio aislado al final del taller. La evaluación continua permite realizar ajustes y enriquecer las dinámicas de aprendizaje, garantizando que los objetivos pedagógicos sean alcanzados de manera efectiva. Este enfoque también fomenta un ambiente de confianza y colaboración, fundamental en la educación de adultos, al permitir que los participantes se sientan valorados y que sus opiniones sean tomadas en cuenta. Como señalan teóricos como Knowles (1970) y Maslow (1954), la implicación activa de los participantes en el proceso evaluativo refuerza su motivación intrínseca, ya que sienten que sus necesidades y expectativas están siendo consideradas y que tienen un papel activo en su propio proceso de aprendizaje.

Las notas de las observaciones directas realizadas durante los talleres han ayudado a retocar aspectos y detalles de los talleres de cuestión técnica y teórico-práctico, como ajustar mejor los tiempos para cada dinámica y actividad, así como rebajar el nivel de tecnicismo de algunas partes del taller. **Estos insights han sido clave para ajustar y mejorar continuamente los enfoques pedagógicos para los siguientes talleres.**

Por otro lado, las encuestas de satisfacción muestran cómo el taller ha sido valorado de manera muy positiva tanto por los participantes como por las formadoras. En general, las personas participantes destacaron la claridad de los contenidos, la calidad de la dinamización y la utilidad práctica de los temas tratados. La mayoría de las respuestas fueron positivas, con un alto porcentaje (más del 75%) de valoraciones entre 3 y 4, lo que refleja una gran aceptación del formato, los contenidos y la metodología empleada. Los aspectos más valorados fueron la adecuación del espacio y los recursos técnicos, con una valoración destacada del 93% de respuestas positivas en cuanto a la adecuación del espacio y un 89% en los recursos técnicos, como los proyectores y los ordenadores. También se valoró

[14] Ver annexo 9

positivamente que los materiales y recursos didácticos fueron claros y útiles para el aprendizaje, con un 83,9% de respuestas positivas.

Sin embargo, también se han identificado áreas de mejora. La duración del taller recibió una valoración más baja, con el 62% de respuestas positivas, lo que sugiere que algunos participantes sintieron que no hubo tiempo suficiente para profundizar en los temas. De hecho, varios comentarios mencionaron la necesidad de más sesiones o de más tiempo para poder aprovechar mejor los contenidos. En cuanto a las actividades prácticas y dinámicas, aunque se valoraron de manera positiva, algunos participantes sugirieron incluir más ejemplos prácticos que se ajusten a la realidad de su día a día digital.

Por otro lado, las personas formadoras también dieron una valoración global bastante positiva, con una media de 3,3 sobre 4, destacando la claridad y coherencia de los objetivos del taller. Apreciaron la metodología utilizada y la posibilidad de que los asistentes participaran activamente, aunque señalaron que la duración fue insuficiente para cubrir todos los contenidos previstos. También mencionaron que algunos de los medios técnicos no fueron completamente adecuados, y sugirieron que los ejemplos de fraudes deberían ser más actualizados y basados en situaciones más cercanas a las experiencias cotidianas de los participantes. Además, mencionaron que las dinámicas como las de las papeletas con emociones fueron difíciles de realizar sin mesas, ya que los asistentes se encontraban sentados sin ese apoyo. En cuanto a la duración de las sesiones, también las consideraron demasiado breves.

En este sentido, los talleres de ciberdelincuencia han sido muy bien recibidos por las personas mayores, especialmente por su enfoque práctico y su claridad. Sin embargo, las áreas de mejora están relacionadas principalmente con la duración, que debe ser ampliada para cubrir adecuadamente todos los contenidos, y con la mejora en el uso de recursos técnicos y las condiciones de espacio. Las formadoras, al igual que los participantes, consideran que este tipo de talleres deben continuar y replicarse, pero con ajustes en el tiempo y los recursos para hacerlos aún más efectivos y accesibles. En total, el impacto real fue que 96 personas mayores recibieron este taller.

Tabla 7. *Relación de talleres y participantes*

Taller	Número de participantes	Lugar	Fecha
1	13	Casal Gent Gran Sant Genís	2 octubre 17:00 -19:00h
2	9	Casal de Gent Gran Penitents	13 octubre 11:15 -13:15h
3	10	Casal de Gent Gran de la Palmera	17 octubre 10:30 -12:30h
4	8	Casal de Gent Gran Bon Pastor	21 octubre 11:15-12:45h
5	9	Casal Gent Gran Baix Guinardó	21 octubre 17:00 - 19:00 h
6	9	Casal de Gent Gran Montmany	22 octubre 16:00 -18:00h
7	9	Casal Gent Gran Vall d'Hebron	23 octubre 10:00 - 12:00 h
8	10	Casal de Gent Gran Navas	24 octubre 10:00 -11:30h
9	9	Espai de Gent Gran La Violeta	29 octubre 16:30 -18:00h
10	10	Casal de Gent Gran Bascònia	30 octubre 10:30 -12:00h.
Total	96		

Fuente: Elaboración propia.

Por último, el workshop fue bien valorado por las personas participantes, destacándose especialmente la utilidad y claridad de los materiales del *toolkit* compartidos durante la jornada, que facilitaron la comprensión y aplicación de los contenidos trabajados. No obstante, las principales áreas de mejora se relacionan con el nivel de participación, ya que, pese a contar inicialmente con 16 personas inscritas, la asistencia final se redujo a 8. Este hecho apunta a la necesidad de reforzar las estrategias de convocatoria y seguimiento, con el fin de garantizar una mayor implicación y aprovechamiento de este tipo de espacios formativos.

6.5. Conclusiones

En conclusión, la necesidad inaplazable de implantar acciones formativas estables en los equipamientos y centros de personas mayores y en paralelo, de capacitar a sus profesionales para una primera acogida empática, coordinada y eficaz ante la detección de fraudes o abusos digitales, integrando prevención y acompañamiento en un mismo itinerario centrado en la persona mayor y su bienestar emocional y digital.

Estos talleres deben alejarse del alarmismo y apostar por la práctica segura con ejemplos reales, validando emociones como la vergüenza o el miedo y normalizando la petición de ayuda, al tiempo que ofrecen rutas claras de actuación con opciones presenciales y telefónicas para quienes no utilizan canales digitales. La presencia territorial y la confianza comunitaria de los equipamientos y centros de personas mayores los convierten en espacios privilegiados para la detección temprana, la desestigmatización y el aprendizaje entre iguales, incorporando testimonios y narrativas que desplacen la culpa hacia la resiliencia y refuercen la autonomía personal.

La formación específica de los equipos (escucha activa, lenguaje libre de reproches, guiones sencillos, derivación responsable y coordinación con una ventanilla de referencia) reduce la victimización secundaria, acorta tiempos de respuesta y mejora la experiencia de las personas usuarias. Además, cada caso atendido debe retroalimentar contenidos y protocolos mediante indicadores de uso (tiempo hasta la consulta, tasas de denuncia, confianza en instituciones y reducción del malestar emocional), consolidando un ciclo de mejora continua ajustado al riesgo real del territorio. En suma, invertir en talleres para la ciudadanía mayor y en el empoderamiento profesional de los equipamientos y centros de personas mayores no solo previene el daño y acelera la recuperación, sino que fortalece las redes de confianza y la inclusión efectiva, garantizando que pedir ayuda sea sencillo, seguro y socialmente.

La atención a las personas mayores víctimas de cibercrimen requiere un enfoque integral que combine la **intervención psicológica, el acompañamiento familiar-comunitario y la educación digital adaptada**. Tal como señalan Beck et al. (2019), los servicios psicológicos deben ser accesibles, culturalmente competentes y sensibles a las particularidades de cada paciente, incluyendo sus creencias religiosas o espirituales, que pueden influir en la vivencia del daño y las estrategias de afrontamiento (D'Ardenne et al., 2005). En este sentido, los y las profesionales que trabajan con personas mayores víctimas de fraude deberían incorporar herramientas de apoyo emocional y orientación terapéutica que faciliten la recuperación del bienestar y la reconstrucción de la confianza (Segal et al., 2019). Los estudios internacionales subrayan que las estafas basadas en la **suplantación de identidad** o en el uso de canales mixtos (teléfono, SMS, internet) son las más frecuentes entre las personas mayores, ya que los ciberdelincuentes aprovechan su menor familiaridad tecnológica y su tendencia a confiar en autoridades o instituciones reconocidas (Button et al., 2020). Sin embargo, la respuesta institucional en Europa sigue siendo fragmentaria: la atención recae principalmente en la policía o las entidades financieras, mientras que las víctimas manifiestan **insatisfacción con la falta de acompañamiento humano y psicológico** (Cross et al., 2018). Además, el papel de las **familias** resulta decisivo: un entorno familiar empático y colaborador puede reforzar la toma de decisiones seguras, mientras que las reacciones negativas o culpabilizadoras

agravan sentimientos de vergüenza, indefensión o “autoedadismo”, es decir, la interiorización de estereotipos negativos sobre la propia edad (Levy, 2001; Minichiello, Browne & Kendig, 2000). Para prevenir esta espiral de vulnerabilidad, es fundamental promover **procesos formativos inclusivos** que reconozcan las capacidades de las personas mayores, evitando enfoques paternalistas y favoreciendo una enseñanza paciente, progresiva y respetuosa (Lacalle, 2024). Solo mediante la combinación de **educación digital adaptada, apoyo familiar y comunitario informado y la atención psicológica sensible a la edad y la cultura**, será posible construir entornos digitales seguros y resilientes para la población mayor.

7. Síntesis y mirada hacía el futuro

Un eje de comunicación claro, empático y libre de estigma constituye la base para articular, en un mismo marco coherente, la prevención, la detección temprana y el acompañamiento frente a la ciberdelincuencia que afecta a las personas mayores. Cuando la comunicación se diseña desde una perspectiva de derechos, deja de centrarse en advertencias abstractas y se convierte en una herramienta práctica que orienta hacia rutas de acción sencillas, comprensibles y disponibles en los espacios cotidianos de las personas.

Desde esta lógica, la guía cocreada con personas que trabajan con personas mayores no es un producto informativo más, sino el **núcleo operativo de un ecosistema comunitario de protección**. Su función es activar a los equipamientos y centros de personas mayores como agentes “antena” y articular una **ventanilla de referencia clara y reconocible**, capaz de coordinar la ayuda sin derivaciones circulares ni pérdida de información. Entendida como un servicio público, la comunicación reduce la ansiedad, evita la culpabilización, normaliza la petición de ayuda y traduce en prácticas concretas las responsabilidades de los distintos actores implicados: banca, fuerzas de seguridad, administraciones públicas y recursos comunitarios.

La cocreación garantiza la pertinencia del lenguaje, el formato y los contenidos, y aporta un valor añadido decisivo: **convierte a las propias personas mayores en mensajeras de confianza**. Sus relatos y experiencias corrigen el sesgo paternalista, reducen la vergüenza asociada al fraude y activan un efecto cascada que favorece la verbalización de dudas o incidentes, facilitando la detección temprana y el acceso al apoyo. Abrir el diseño de la guía a grupos de mayores en equipamientos comunitarios permite validar casos reales, seleccionar ejemplos que resuenan y consensuar instrucciones claras, sin tecnicismos ni dependencia de aplicaciones digitales. El resultado es un material sintético, replicable y escalable, adaptable a distintos perfiles y útil tanto para la orientación individual como para la programación de actividades preventivas.

El diseño comunicativo de la guía se fundamenta en un enfoque informado por el trauma y explícitamente anti-edadista. Esto implica validar emociones como el miedo, la rabia o la vergüenza; afirmar de manera clara que el fraude es un delito del que la víctima no es responsable; y ofrecer instrucciones estructuradas por capas temporales —qué hacer ahora, hoy y esta semana— que ordenan la acción sin saturar de información. El uso de lenguaje llano, frases breves y verbos de acción, junto con una tipografía accesible, alto contraste y jerarquía visual, reduce la carga cognitiva y facilita la comprensión. La coexistencia de formatos analógicos y digitales garantiza el acceso universal.

El apartado de “cómo actuar” se refuerza mediante materiales insertados en los puntos de contacto cotidianos —cajeros, extractos bancarios, salas de espera o mostradores— con mensajes simples y accionables como “Si dudas: cuelga, verifica y llama a tu punto de confianza”. La señalética común identifica de forma visible a los agentes de protección y los canales de ayuda, mediante pictogramas consistentes. La guía incorpora además una ficha de conservación de evidencias y un decálogo básico de autoprotección digital, recordando prácticas clave como no compartir códigos ni contraseñas ni permitir accesos remotos no solicitados.

De forma complementaria, el **workshop de capacitación** está diseñado para dotar a profesionales de equipamientos de personas mayores, centros cívicos y recursos de proximidad de habilidades relacionales, guiones operativos y materiales estándar que los convierten en puntos de apoyo seguros, coordinados y eficaces. El enfoque, igualmente informado por el trauma y anti-edadista, refuerza la validación emocional, la comunicación sin culpa y la oferta de alternativas telefónicas y presenciales para quienes no utilizan canales digitales. La formación prioriza metodologías prácticas —role-plays, simulaciones y ejercicios de escucha activa— y un kit reutilizable de microherramientas que garantiza homogeneidad y claridad en la atención.

Los beneficios del workshop se manifiestan en varios niveles. A nivel individual y emocional, mejora la adherencia al circuito de ayuda, reduce el abandono de la denuncia y preserva la autonomía de la persona mayor, incrementando la consulta temprana y evitando la evitación digital tras el incidente. A nivel organizativo, la estandarización de mensajes, iconografía y teléfonos de referencia unifica la comunicación entre actores y refuerza la confianza ciudadana en el sistema, condición necesaria para aumentar la denuncia y la búsqueda de apoyo. Además, el uso de checklists breves de señales de riesgo y rutas de actuación por niveles facilita la detección temprana sin sobrecargar de información técnica.

La dimensión comunitaria del taller amplía su impacto al habilitar una red de agentes “antena” en el entorno cotidiano —farmacias, comercios, peluquerías y equipamientos de barrio— dotados de un kit mínimo de acogida y derivación responsable. Su función no es resolver situaciones complejas, sino identificar señales de alerta, validar el relato y activar los canales adecuados, ampliando la cobertura territorial sin medicalizar ni tecnificar innecesariamente el primer contacto. Para garantizar la sostenibilidad, el workshop incorpora espacios de debriefing emocional y pautas de autocuidado para los equipos, y adopta una metodología de “formar para formar” que convierte a referentes locales en multiplicadores del modelo.

La guía cocreada y el vídeo de sensibilización protagonizado por personas mayores se integran como materiales de trabajo en sesiones grupales y puntos de contacto cotidianos,

reforzando el efecto cascada de los testimonios y contribuyendo a reducir la infradenuncia. Su distribución se apoya en la ecología comunicativa local —casals, centros cívicos, farmacias, oficinas bancarias, radios locales y redes vecinales— y cada emisión incorpora un llamado a la acción claro y accesible: un teléfono gratuito, un punto presencial y el compromiso explícito de un trato empático y confidencial.

Todo ello se inscribe en una estrategia integral de inclusión digital comunitaria que reconoce una limitación estructural del contexto actual: mientras la respuesta institucional se ha centrado en proteger sistemas y organizaciones, las personas siguen siendo el eslabón más vulnerable. Frente a este vacío, el programa propone estructuras de proximidad capaces de advertir, orientar y acompañar cuando los datos o la seguridad digital de la ciudadanía se ven comprometidos, complementando la protección institucional con acompañamiento cotidiano. En este marco, organismos como el INCIBE constituyen un referente estratégico a escala nacional, cuya eficacia se amplifica cuando sus orientaciones se traducen en dispositivos autonómicos y municipales próximos a la vida diaria de las personas.

El modelo resultante es una **estructura distribuida, colaborativa y sostenible**, donde la ciberseguridad se convierte en una responsabilidad compartida entre administraciones, sociedad civil, entorno comunitario y las propias personas mayores. Esta coherencia evita contradicciones, reduce la fatiga informativa y refuerza la confianza institucional.

En síntesis, una guía cocreada, accesible y no digitalmente excluyente, reforzada por un vídeo de sensibilización y enraizada en la red comunitaria, transforma la comunicación en una auténtica intervención de salud pública. Reconoce el daño sin culpabilizar, enseña pasos accionables, identifica agentes de protección y ofrece un canal inmediato de ayuda con seguimiento. Al alinear diseño accesible, formatos diversos y gobernanza compartida, la comunicación deja de ser un medio para convertirse en la infraestructura que sostiene la prevención, acelera la detección y dignifica el acompañamiento, permitiendo pasar del miedo a la acción y del aislamiento a la confianza, fortaleciendo la autonomía y la resiliencia digital de las personas mayores.

8. Referencias bibliográficas

Agencia Española de Protección de Datos. (2024, 19 febrero). Digitalización sin alternativas: el riesgo de discriminar a las personas mayores. https://www.aepd.es/prensa-y-comunicacion/blog/digitalizacion-sin-alternativas-el-riesgo-de-discriminar-las-personas

Álvarez, N., García, J., & Romero, C. (2024). *Estafas virtuales en adultos mayores*. Universidad Católica de Cuyo.

Amoedo-Casais, A., Vara-Miguel, A., & Negredo, S. (2021). *Digital News Report España 2021*. Universidad de Navarra.

Aperador, M. (2024). *Ciberseguridad y criminología: Protección de personas vulnerables en el entorno digital*. LISA Institute.

Aperador, M., & Pascual, V. (2024). Cibervictimología: atención a víctimas de ciberdelitos. *Masterclass LISA Institute*.

Australian Institute of Criminology. (2024). *Developing a harm index for individual victims of cybercrime* (Trends & Issues in Crime and Criminal Justice, No. 706). https://www.aic.gov.au/sites/default/files/2025-02/ti706_developing_a_harm_index_for_individual_victims_of_cybercrime.pdf

Ayuso, S. (2025, 31 enero). Más del 40% de los europeos carece de habilidades digitales para gestiones 'online': "No ponen facilidades al ciudadano, sino barreras". *El País*. https://elpais.com/sociedad/2025-01-31/mas-del-40-de-los-europeos-carece-de-habilidades-digitales-para-gestiones-online-no-ponen-facilidades-al-ciudadano-sino-barreras.html

Azam, N. A., Buja, A. G., Sahri, N. M., Ahmad, R., Habidin, N. F., Latip, S. F. A., ... & Saat, S. (2025). A Light Review on Cyber Security Awareness Models for the Elderly. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *44*(1), 31-45.

Bailey, J., Taylor, L., Kingston, P., y Watts, G. (2020). *Older adults and "scams": Evidence from the Mass Observation Archive.* The Journal of Adult Protection, 23(1), 57-69. https://doi.org/10.1108/jap-07-2020-0030

BBVA. (2023, 4 octubre). ¿Qué elementos hacen vulnerable a una víctima ante un ciberataque? https://www.bbva.com/es/innovacion/en-la-mente-de-la-victima-de-un-ciberataque/

Beck, A. T., Rush, A. J., Shaw, B. F., & Emery, G. (1979). *Cognitive therapy of depression*. Guilford Press.

Beck, J. G., McNiff, J., Clapp, J. D., Olsen, S. A., Avery, M. L., & Hagewood, J. H. (2011). Exploring negative emotion in women experiencing intimate partner violence: Shame, guilt, and PTSD. *Behavior Therapy*, 42(4), 740-750.

Brashier, N. M., & Schacter, D. L. (2020). Aging in an era of fake news. *Current Directions in Psychological Science*, 29(4), 316-323.

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

Borredá, A., & González Herrero, E. (2024, 14 mayo). «Interior apuesta por crear una agencia de ciberseguridad que aúne a todos los actores». Red Seguridad. https://www.redseguridad.com/entrevistas/interior-apuesta-por-crear-una-agencia-de-ciberseguridad-que-aune-a-todos-los-actores_20240514.html

Borwell, J., Jansen, J., & Stol, W. (2021). *Comparing the victimisation impact of cybercrime and traditional crime: Literature review and future research directions. Journal of Digital Social Research, 3*(3), 1–21. https://doi.org/10.33621/jdsr.v3i3.66

Bourdeloie H. (2018). Tecnologías digitales y relaciones sociales de la edad, género y clase entre adultos mayores: Un enfoque interseccional. Comunicación y Género, 1(2), 147-160. https://doi.org/10.5209/CGEN.62672

Brookfield, S. D. (1986). *Understanding and facilitating adult learning*. Jossey-Bass.

Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2024). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration*, *8*(76), 511.

Bunbury, E., Pérez-Calle, R., & Osuna-Acedo, S. (2022). Las Competencias Digitales en personas mayores: de amenaza a oportunidad. *Vivat Academia*, *155*, 173–195. https://doi.org/10.15178/va.2022.155.e1383

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology*, *159*, 111678. https://doi.org/10.1016/j.exger.2021.111678

Button, M., Lewis, C., y Tapley, J. (2014). *Not a victimless crime: The impact of fraud on individual victims and their families.* Security Journal, 27(1), 36–54.

Button, M., y Cross, C. (2017). *Cyber frauds, scams and their victims.* Routledge, Taylor & Francis Group.

Caravaca-Llamas, C., & Girona-Berná, M. (2021). El Trabajo Social en la atención de las víctimas de los ciberdelitos en España. *TS nova: trabajo social y servicios sociales*, 17, 47-58.

Carcach, C., Graycar, A., y Muscat, G. (2011). *The victimization of older Australians.* Recuperado de http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi212.pdf

Centro de Inteligencia Digital Alicante. (2022). *Guía de actuación para una inclusión digital efectiva de las personas mayores*. Universidad Miguel Hernández.

CEREZO DOMÍNGUEZ, A. I.; GARCÍA CORNEJO, R. (2020). La ciberdelincuencia en España: un estudio basado en las estadísticas policiales, Revista Peruana de Ciencias Penales, 1(34), 91–106. https://doi.org/10.56176/rpcp.34.2022.3

ClaroVTR & Criteria. (2024). *Radiografía Digital de Personas Mayores: Senior Tech 2024*.

Clark, D. A., & Beck, A. T. (2010). *Cognitive therapy of anxiety disorders: Science and practice*. Guilford Press.

Cross, C., Richards, K., & Smith, R. G. (2017). *Responding to cybercrime: Current trends*. Australian Institute of Criminology.

D'Ardenne, P., Ruaro, L., Cestari, L., Fakhoury, W., & Priebe, S. (2005). Does interpreter-mediated CBT with traumatized refugee people work? A comparison of patient outcomes in East London. *Behavioural and Cognitive Psychotherapy*, 33(3), 293-301.

Del Pozo Manzano, P. (2024). *RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las estafas digitales*. Universidad Europea.

Dirección General de Coordinación y Estudios. (2023). Informe sobre la cibercriminalidad en España. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf

Ehlers, A., & Clark, D. M. (2000). A cognitive model of posttraumatic stress disorder. *Behaviour Research and Therapy*, 38(4), 319-345.

Envejecimiento en Red. CSIC. (2023, 20 diciembre). Los mayores españoles continúan reduciendo su brecha digital. Envejecimiento en Red. https://envejecimientoenred.csic.es/58857-2/

Erades Pérez, N., & Kemp, S. (2022). Uso de las TIC y cibervictimización de personas adultas mayores: un estudio exploratorio. *Revista Internacional de Estudios Migratorios*, 12(2), 156-178.

Erades Pérez, N., & Sitges Maciá, E. (2025). Perfil de conducta digital, ciberdelitos y cifra negra: análisis de una muestra española. Revista Española De Investigación Criminológica, 22(2), e887. https://doi.org/10.46381/reic.v22i2.887

European Commission. (2023). 2030 Digital Decade: Report on the state of the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

European Commission. (2023). 2030 Digital Decade Annex Spain: Report on the state of the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

Eurostat. (2021). Individuals' level of digital skills (from 2021 onwards). https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21__custom_11653438/default/bar?lang=en&page=time:2021

Federación Iberoamericana de Asociaciones de Derecho e Informática, & Peña Labrin, D. E. (2023). Rol de la prevención en la expansión de la ciberdelincuencia. Revista Iberoamericana de Derecho Informático. https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/view/3998/3473

Frankl, V. E. (1946). *Man's search for meaning*. Beacon Press.

Freire, P. (1970). *Pedagogy of the oppressed*. Herder and Herder.

Frieze, I.H., Hymer, S., & Greenberg, M.S. (1987). *Describing the crime victim: Psychological reactions to victimization.* Professional Psychology: Research and Practice, 18(4), 299.

Gale, J.-A., y Coupe, T. (2005). *The behavioural, emotional and psychological effects of street robbery on victims.* International Review of Victimology, 12(1), 1–22.

Gheorgita, N. (2014). New Educational Strategies regarding Quality of Life for Elderly People. https://www.sciencedirect.com/science/article/pii/S1877042814045819

Green, D.L., Choi, J.J., y Kane, M.N. (2010). *Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping.* Journal of Human Behavior in the Social Environment, 20(6), 732–743.

Griffith, C. E. (2023). *Understanding the cyber-victimisation of young people. Journal of Cybersecurity and Digital Crime, 1*(1), 1–14. https://doi.org/10.1016/j.teler.2023.100042

Hargittai, E., Piper, A. M., & Morris, M. R. (2019). From internet access to internet skills: Digital inequality among older adults. *Universal Access in the Information Society, 18*(4), 881-890. https://doi.org/10.1007/s10209-018-0617-5

Havers B, Tripathi K, Burton A, McManus S, Cooper C (2024) Cybercrime victimisation among older adults: A probability sample survey in England and Wales. PLoS ONE 19(12): e0314380. https://doi.org/10.1371/journal.pone.0314380

INCIBE. (2022). Guía de ciberseguridad: La ciberseguridad al alcance de todos. https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf

INE. (2024, 24 junio). Proyecciones de población. Años 2024-2074 [Comunicado de prensa]. https://www.ine.es/dyngs/Prensa/PROP20242074.htm

Janoff-Bulman, R. (1989). Assumptive worlds and the stress of traumatic events: Applications of the schema construct. *Social Cognition*, 7(2), 113-136.

Jansen, J., y Leukfeldt, R. (2018). *Coping with cybercrime victimization: An exploratory study into impact and change.* Journal of Qualitative Criminal Justice and Criminology, 6(2), 205-228.

Jarvis, P. (2012). *Adult education and lifelong learning: Theory and practice* (4th ed.). Routledge.

Joseph, S., & Linley, P. A. (2006). Growth following adversity: Theoretical perspectives and implications for clinical practice. *Clinical Psychology Review*, 26(8), 1041-1053.

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

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.

Kuong, M.A. & Chaparro, J.J. (2025). Competencias digitales e inclusión tecnológica en adultos mayores: una revisión sistemática. *Revista InveCom*, *5*(2). https://doi.org/10.5281/zenodo.13851765

Knowles, M. S. (1970). *The modern practice of adult education: Andragogy versus pedagogy*. Association Press.

Knowles, M. S. (1973). *The adult learner: A neglected species*. Gulf Publishing.

Lai, F., Li, D., y Hsieh, C.-T. (2012). *Fighting identity theft: The coping perspective.* Decision Support Systems, 52(2), 353–363.

Lamet, W., y Wittebrood, K. (2009). *Never the same again: The consequences of crime for victims.* The Hague: Sociaal Cultureel Planbureau.

Lazarus, R.S., y Folkman, S. (1984). *Stress, appraisal, and coping.* New York: Springer Publishing Company.

Levy, B. R. (2001). Eradication of ageism requires addressing the enemy within. *The Gerontologist*, 41(5), 578-579.

Liang, H., y Xue, Y. (2009). *Avoidance of information technology threats: A theoretical perspective.* MIS Quarterly, 33(1), 71–90.

Martinez Souto, N. (2022, 11 mayo). Problema de culpabilidad en víctimas de ciberdelitos. Pintos & Salgado Abogados. https://pintos-salgado.com/problema-de-culpabilidad-en-victimas-de-ciberdelitos/

Maslow, A. H. (1954). *Motivation and personality*. Harper & Row.

Mason, K., y Benson, M. (1996). The effect of social support on fraud victims' reporting behaviour: A research note. *Justice Quarterly*, 13(3), 511–524. https://doi.org/10.1080/07418829600093071

Méndez, R. M. (2024). Perfilación criminal de los ciberdelincuentes: Análisis sobre motivaciones y rasgos de los hackers.

Mezirow, J. (1991). *Transformative dimensions of adult learning*. Jossey-Bass.

Minichiello, V., Browne, J., & Kendig, H. (2000). Perceptions and consequences of ageism: Views of older people. *Ageing & Society*, 20(3), 253-278.

Ministerio del Interior. (2023, 8 febrero). Grande-Marlaska presenta la campaña de Interior contra la ciberdelincuencia [Comunicado de prensa]. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2023/080223-grande-marlaska-campana-ciberdelincuencia.aspx

Ministerio de Economía, Comercio y Empresa. (2021). Plan Nacional de Competencias Digitales. https://portal.mineco.gob.es/recursosarticulo/mineco/ministerio/ficheros/210127_plan_nacional_de_competencias_digitales.pdf

Ministerio para la Transformación Digital y de la Función Pública. (2025, 6 mayo). El Gobierno aprueba un refuerzo de las capacidades de España en ciberseguridad y ciberdefensa con 1.157 millones de euros [Comunicado de prensa]. https://digital.gob.es/comunicacion/sala-de-prensa/comunicacion_ministro/2025/05/2025-05-06.html

Miró-Llinares, F. (2013). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. *Revista de Derecho Penal y Criminología*, 3(10), 145-189.

Morrison, B. A., Nicholson, J., Coventry, L., & Briggs, P. (2023, September). Recognising diversity in older adults' cybersecurity needs. In Proceedings of the 2023 ACM Conference on Information Technology for Social Good (pp. 437-445).

Morrison, B., Coventry, L., & Briggs, P. (2021). How do Older Adults feel about engaging with Cyber-Security?. *Human behavior and emerging technologies*, 3(5), 1033-1049.

Munanga, A. (2023). Protecting Older Adults From Cybercriminals: The Role of Health Care Providers. *Journal of Gerontological Nursing*, *49*(7), 3-4.

Muniesa Tomás, P, Herrera Sánchez, D., Guerrero Olmos, J., Martínez Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A. M., Gómez Martín, M. A. (2023). *Informe sobre la cibercriminalidad en España*. Dirección General de Coordinación y Estudios. Secretaria de Estado de Seguridad.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, *13*(1), 49-72.

Office for National Statistics. (2025). *Crime in England and Wales: year ending December 2024*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2024

OMS. (2021, 18 marzo). El edadismo es un problema mundial [Comunicado de prensa]. https://www.who.int/es/news/item/18-03-2021-ageism-is-a-global-challenge-un

Observatorio Nacional de Tecnología y Sociedad (ONTSI). (2024). *Competencias digitales de la población española 2024*. Ministerio para la Transformación Digital y de la Función Pública. https://www.ontsi.es

Papí-Gálvez, N., & La-Parra-Casado, D. (2022). Digital literacy and fake news consumption: The case of older adults in Spain during COVID-19. *Media and Communication*, 10(2), 120-130.

Park, C. L. (2010). Making sense of the meaning literature: An integrative review of meaning making and its effects on adjustment to stressful life events. *Psychological Bulletin*, 136(2), 257-301.

Pérez Díaz, J., Castillo Belmonte, A. B., Aceituno Nieto, P., & Ramiro Fariñas, D. (2024). Un perfil de las personas mayores en España, 2024. Indicadores estadísticos básicos (Informe nº 33, 50 págs.). Informes Envejecimiento en red. https://envejecimientoenred.csic.es/wp-content/uploads/2024/12/enred-indicadoresbasicos2024.pdf

Pino Juste, M. R., Soto Carballo, J. G., & Rodríguez López, B. (2015). Las personas mayores y las TIC: Un compromiso para reducir la brecha digital (Sociedad Iberoamericana de Pedagogía Social, Ed.). https://gredos.usal.es/bitstream/handle/10366/140160/38449-120337-1-PB.pdf?sequence=1&isAllowed=y

Qin, N., y Yan, E. (2018). *Common crime and domestic violence victimization of older Chinese in urban China: The prevalence and its impact on mental health and constrained behavior.* Journal of Interpersonal Violence, 33(6), 889-914. https://doi.org/10.1177/0886260517698825

Rasiwan, I. (2025). *Cybercrime victim protection: Legal challenges for the victim. LAJU: Journal of Law & Justice,* 2(1), 45–58. https://journal.ppipbr.com/index.php/laju/article/download/560/512/208

Rebovich, D., y Layne, J. (2000). The national public survey on white collar crime. Morgantown: National White Collar Crime Centre. Disponible en: https://www.ncjrs.gov/pdffiles1/Digitization/181968NCJRS.pdf

Reisig, M. D., Holtfreter, K., y Turanovic, J. J. (2017). *Criminal victimization, depressive symptoms, and behavioral avoidance coping in late adulthood: The conditioning role of strong familial ties.* Journal of Adult Development, 25, 13-24. https://doi.org/10.1007/s10804-017-9270-0

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to Psychological and Popular Opinion, There Is No Compelling Evidence That Older Adults Are Disproportionately Victimized by Consumer Fraud. *Perspectives on psychological science : a journal of the Association for Psychological Science*, *9*(4), 427–442. https://doi.org/10.1177/1745691614535935

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Salkovskis, P. M. (1996). The cognitive approach to anxiety: Threat beliefs, safety-seeking behavior, and the special case of health anxiety and obsessions. In P. M. Salkovskis (Ed.), *Frontiers of cognitive therapy* (pp. 48-74). Guilford Press.

Satchell, J. (2023). *Older victims of community crime: Psychological impact and coping* (Tesis doctoral, UCL (University College London)).

Segal, M., Doron, I., y Mor, S. (2021). *Consumer fraud: Older people's perceptions and experiences. Journal of Aging & Social Policy*, 33(1), 1-21.

Sitges-Maciá, E., Erades-Pérez, N., & Bonete-López, B. (2022). Digitalización y cibervictimización en personas adultas mayores: Estrategias de prevención e intervención. *Revista de Investigación en Ciberseguridad*, 15(3), 45-67.

65YMÁS. (2024, 17 de enero). *El 73% de los mayores tiene miedo a caer en una estafa online*. https://www.65ymas.com/ciberseguridad/mayores-miedo-caer-estafas-online-encuesta-ciberseguridad_55612_102.html (consultado el 20 de marzo de 2024).

Shapland, J., y Hall, M. (2007). *What do we know about the effects of crime on victims?* International Review of Victimology, 14(2), 175–217.

Schoepfer, A., y Piquero, N. (2009). Studying the correlates of fraud victimisation and reporting. *Journal of Criminal Justice*, 37, 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Smith, R. G. (2007). Consumer scams in Australia. *Trends and Issues in Crime and Criminal Justice*, no. 331. Canberra: Australian Institute of Criminology. Disponible en: http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi331.pdf

Solórzano Jiménez, E., & Monge Montoya, L. D. (2022). *Propuesta de un marco de trabajo para mejorar la seguridad en Internet para personas en edad laboral madura y personas adultas mayores de la asociación gerontológica costarricense que cuentan con alfabetización digital* (Doctoral dissertation, Universidad Cenfotec).

Somos Digital. (2022). “Aumentan un 4,2% los ciudadanos de 65 a 74 años que usan internet; la brecha digital sigue reduciéndose". En somos-digital.org. https://somos-digital.org/wp-content/uploads/2023/09/Uso_de_internet-_personas_mayores-.pdf

Titus, R., Heinzelman, F. y Boyle, J. (1995) Victimisation of persons by fraud. Crime and Delinquency 41(1): 54–72.

Torres Vargas, G. A. (2023). La resiliencia como parte de la transformación digital.

Tripathi, K., Robertson, S., y Cooper, C. (2019). *A brief report on older people’s experience of cybercrime victimization in Mumbai, India.* Journal of Elder Abuse & Neglect, 31(4-5), 437-447. https://doi.org/10.1080/08946566.2019.1674231

Valera-Ordaz, L., Codina, L., & Pedraza-Jiménez, R. (2022). Desinformación y personas mayores: Competencias, estrategias y vulnerabilidades informacionales. *Profesional de la Información*, 31(2), e310208.

Vandecar-Burdin, T., & Akpinar-Elci, M. (2023). A qualitative exploration of dual vulnerability: cybersecurity and social isolation risks for Alzheimer’s caregivers during the COVID-19 pandemic. Criminal Justice Studies, 36(3), 292–310. https://doi.org/10.1080/1478601X.2023.2254100

Wallace, H., & Roberson, C. (2007). *Principles of criminal law* (4th ed.). Allyn & Bacon.

Whitty, M.T. & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims-both financial and non-financial. Criminology and Criminal Justice, 16(2), 176–194.

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. En *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE ’14)* (pp. 1-10). Association for Computing Machinery. https://doi.org/10.1145/2601248.2601268

9. Anexo

Anexo 1. Lista de abreviaturas

CERT: Equipo de Respuesta ante Emergencias Informáticas

CP: Código Penal

CSIC: Consejo Superior de Investigaciones Científicas

EUROPOL: Oficina Europea de Policía

FATEC: Federació d'Associacions de Gent Gran de Catalunya

FPT: Fundación Pere Tarrés

INCIBE: Instituto Nacional de Ciberseguridad

INE: Instituto Nacional de Estadística

OSI: Oficina de Seguridad del Internauta

PESC: Política Exterior y de Seguridad Común

SEC: Sistema Estadístico de Cibercriminalidad

TIC: Tecnologías de la Información y la Comunicación

Anexo 2. Listado de personas entrevistadas

Tabla 8. *Relación de personas entrevistadas*

Código	Cargo[15]	Fecha de la entrevista
E1	Coordinador de proyectos del ámbito de personas mayores de Acción Social de una fundación sin ánimo de lucro	23/04/25
E2	Responsable de Acción Digital de una fundación sin ánimo de lucro	28/04/25
E3	Miembro de la Unidad de Formación de un cuerpo de seguridad municipal.	20/05/25
E4	Ex responsable de formación de una entidad sin ánimo de lucro especializada en la emancipación digital de las personas mayores.	03/06/25
E5	Investigador de una Universidad española	04/06/25
E6	Especialista en ciberseguridad en un proyecto de divulgación sobre ciberseguridad.	08/09/25
E7	Criminóloga especializada en Ciberseguridad y CEO de una APP de ciberseguridad.	23/09/25
E8	Investigadora especialista en ciberseguridad de una Universidad española.	09/10/25
E9	Director técnico de una empresa sobre ciberseguridad	22/10/25
E10	Investigador especialista en ciberseguridad de una Universidad española.	27/10/25
E11	Investigador especialista en ciberseguridad de una Universidad española.	28/10/25

Fuente: Elaboración propia.

[15] Con el fin de garantizar el anonimato y la confidencialidad de las personas participantes en las entrevistas, se han omitido las referencias a las entidades a las que pertenecen.

Anexo 3. Dosier del facilitador

Marco teórico

Comprender y reconocer las estrategias de manipulación emocional en el entorno digital

Introducción

La ciberdelincuencia no solo utiliza técnicas tecnológicas avanzadas, sino que también explota profundamente las emociones humanas. Los delincuentes digitales conocen con detalle cómo funcionan las emociones y cómo pueden ser instrumentalizadas para generar confianza, provocar miedo o crear ilusiones. De este modo, manipulan psicológicamente a sus víctimas para alcanzar sus objetivos. Comprender esta dimensión emocional es clave para prevenir engaños digitales y empoderar a las personas en su navegación cotidiana por el entorno digital.

Las emociones forman parte de la vida… y también del mundo digital.

Todas las emociones humanas son **naturales y necesarias** para la vida. Son respuestas adaptativas que nos ayudan a comprender nuestro entorno, tomar decisiones y establecer vínculos. Ahora bien, en el entorno digital, estas emociones pueden ser explotadas de manera intencionada por personas con objetivos fraudulentos.

En este taller, exploraremos cómo los ciberdelincuentes utilizan las emociones como "ganchos emocionales" para manipularnos. No se trata de una cuestión de ingenuidad, sino de manipulación psicológica basada en mecanismos emocionales profundos.

Los ganchos emocionales más habituales en la ciberdelincuencia.

a) Confianza

Los mensajes que parecen provenir de una fuente conocida (familiares, bancos, servicios públicos) activan nuestra confianza automática. Esta confianza, en el mundo analógico, es clave para las relaciones sociales. En el entorno digital, sin embargo, puede ser explotada si no verificamos las fuentes.

La confianza es la seguridad que permite a una persona abrirse y mostrarse vulnerable ante otra, con la esperanza de que será respetada y no juzgada..

Ejemplos:

- SMS o correos supuestamente del banco solicitando datos personales.
- Peticiones de ayuda económica por parte de "familiares" a través de WhatsApp.

b) Miedo y urgencia

El miedo es una emoción intensa ante una amenaza, real o percibida. Los delincuentes digitales la combinan con otro mecanismo poderoso: la urgencia. Esto reduce el tiempo de reacción crítica y favorece la respuesta impulsiva.

El miedo es la respuesta emocional ante la percepción de un peligro.
La urgencia es la sensación de que hay que actuar de inmediato, sin reflexión.

Ejemplos:

- Mensajes que anuncian multas pendientes con consecuencias legales.
- Ofertas que "caducan en 10 minutos".
- Simulación de situaciones de emergencia ("tu hija ha tenido un accidente").

c) Vergüenza y culpabilidad

Cuando una persona cae en un engaño, a menudo siente **culpabilidad** por "haberse dejado engañar" y **vergüenza** ante los demás. Estas emociones pueden inhibir la denuncia o la búsqueda de ayuda.

La culpabilidad es la sensación de haber causado un daño o un error.
La vergüenza es la emoción asociada al miedo a ser juzgado por los demás.

Impacto:

- Inhibición de la denúncia.
- Aislamiento emocional.
- Falta de recuperación psicológica.

d) Ilusión y esperanza

Muchos fraudes aprovechan el deseo de una vida mejor o la esperanza en acontecimientos positivos. Esto se manifiesta en estafas románticas, promesas de premios, herencias o inversiones irreales.

La ilusión es la emoción ante la esperanza de un futuro deseado.

Ejemplos:

- Citas románticas que acaban solicitando dinero.
- Comunicaciones sobre falsas loterías o herencias de un familiar desconocido.

e) Otras emociones o sentimientos que suelen estar presentes en los engaños digitales.

- **Preocupación**: se explota cuando la víctima se muestra inquieta por la salud, la economía o la familia.
- **Soledad**: las personas que viven solas pueden ser más vulnerables a establecer vínculos con desconocidos.
- **Desesperación**: una situación vital límite puede hacer que la persona acepte ofertas que no valoraría en otras circunstancias.

- **Duda**: la incertidumbre y la falta de conocimiento tecnológico favorecen que una persona no sepa cómo actuar o a quién recurrir.

Comprender las vulnerabilidades sin culpabilizar. Desmontar estigmas con una perspectiva crítica.

Introducción

En el imaginario colectivo, a menudo se asocia la vulnerabilidad de las personas mayores en el ámbito digital con una supuesta ingenuidad o pérdida de capacidades. Esta mirada estigmatizadora, además de ser injusta, es contraproducente: genera culpa, vergüenza e inhibe la denuncia. Para prevenir los fraudes digitales y empoderar a las personas mayores, es necesario abordar el problema desde una perspectiva sistémica, emocional y pedagógica.

Este taller propone **desmontar los estigmas** y comprender por qué las personas mayores pueden estar más expuestas a la ciberdelincuencia**, no por quienes son, sino por las circunstancias que las rodean**, las cuales pueden ser aprovechadas por los ciberdelincuentes.

No es una cuestión de ingenuidad, sino de vulnerabilidad.

Los ciberdelincuentes no buscan personas “ingenuas”, sino contextos en los que la **vulnerabilidad** (emocional, económica, tecnológica o relacional) puede ser explotada. Estas vulnerabilidades pueden afectar a cualquier persona, independientemente de la edad, pero en el caso de las personas mayores, a menudo convergen diversos factores.

Factores que pueden aumentar la exposición a la ciberdelincuencia en la vejez.

a) Más capacidad económica

Muchas personas mayores disponen de recursos económicos acumulados, como pensiones, ahorros o propiedades. Esto puede hacer que sean objetivo de fraudes relacionados con inversiones, herencias, premios o ventas falsas.

Clave: No es una cuestión de riqueza extrema, sino de disponer de recursos líquidos o patrimoniales que pueden atraer a los estafadores.

b) Confianza generacional

Las generaciones que crecieron en contextos sociales marcados por la proximidad y la confianza interpersonal a menudo tienen una predisposición a confiar en los demás, especialmente cuando los mensajes parecen provenir de autoridades o instituciones reconocidas.

Clave: Esta confianza no es ningún defecto, sino un valor que puede ser manipulado si no se adapta a los nuevos códigos de verificación digital.

c) Brecha digital y menor familiaridad con la tecnología.

La aceleración constante de los cambios tecnológicos puede dificultar la comprensión o la identificación de fraudes digitales. No se trata de una incapacidad, sino de una desventaja formativa e informacional que puede revertirse con un acompañamiento adecuado.

Clave: Los ciberdelincuentes aprovechan la confusión o el desconocimiento tecnológico para hacer pasar acciones fraudulentas por gestiones normales.

d) Tiempo libre y soledad

Algunas personas mayores disponen de más tiempo libre o viven situaciones de soledad, especialmente emocional. Estas condiciones pueden aumentar la exposición a estafas como las románticas, conversaciones prolongadas en línea con fines manipuladores u oportunidades falsas de inversión o ayuda.

Clave: Las estafas románticas no buscan amor, sino dependencia emocional y económica.

e) Miedo a perder la autonomía y a ser juzgadas.

Después de sufrir un engaño, algunas personas mayores pueden evitar hablar de ello por **miedo a ser juzgadas** o porque temen que se las considere “incapaces” o con deterioro cognitivo. Este miedo también puede estar vinculado al temor a perder derechos o autonomía.

Clave: La **culpa** y la **vergüenza** son obstáculos que es necesario visibilizar y desactivar para favorecer la ayuda y la denuncia. La víctima no es culpable.

Ser víctima de un fraude digital **no es culpa de la persona afectada**. Los ciberdelincuentes son especialistas en manipulación emocional y tecnológica. Señalar o ridiculizar a las víctimas solo agrava las consecuencias y favorece el silencio.

El engaño a través de les emociones

Introducción

Los fraudes digitales no solo se basan en la ingeniería informática, sino, sobre todo, en la **ingeniería emocional**. Los ciberdelincuentes conocen en profundidad las emociones humanas y diseñan estafas que apelan a sentimientos como el miedo, la urgencia, la ilusión o la preocupación. Este módulo explora los **tipos de estafa más habituales**, destacando la **emoción clave que intentan activar** y ofreciendo pautas claras para detectar y evitar estas situaciones.

Casos prácticos de estafa emocional.

Cada caso incluye una descripción del mecanismo, las emociones que busca activar y los indicadores para detectarlo. El objetivo es ofrecer herramientas de detección precoz y de autoprotección desde una perspectiva empoderadora y sin culpabilización.

Estafas de phishing o smishing

Formato habitual: Correos electrónicos o mensajes SMS con enlaces fraudulentos.

Fuentes supuestas: Bancos, Hacienda, Seguridad Social, Correos, empresas de suministros.
Finalidad: Robar datos personales, bancarios o acceder a los dispositivos.

Emociones explotadas:

- **Miedo:** «Te bloquearemos la cuenta», «has recibido una multa».
- **Urgencia:** «La tarjeta caduca hoy», «responde en 24 horas».

Indicadores de detección:

- URL extraña o mal redactada.
- Faltas de ortografía o expresiones forzadas.
- Saludos genéricos («Estimado cliente»).
- Presión para actuar con rapidez.
- Solicitud de datos que normalmente no se piden por mensaje.
- Mensaje inesperado (no esperabas ningún paquete ni ninguna comunicación oficial).
- **Atención:** la URL puede parecer correcta, pero el enlace real es falso.

Estafa del “hijo en apuros”

Formato habitual: Mensaje de WhatsApp (o SMS) suplantando a un hijo, hija o nieto, solicitando ayuda urgente (normalmente dinero).

Emociones explotadas:

- **Preocupación:** «Estoy en un problema grave».
- **Urgencia:** «Necesito que hagas una transferencia ahora mismo».

Indicadores de detección:

- El número no es el habitual, pero pide ser reconocido como familiar.
- Historia excesivamente dramática y con prisas.
- Forma de expresarse que no coincide con la manera habitual del supuesto familiar.
- **Clave**: verificar siempre por otra vía antes de realizar cualquier acción.

Estafas sentimentales o románticas

Formato habitual: Conexión a través de redes sociales (Facebook, aplicaciones de citas) con un perfil atractivo y amable que inicia una relación emocional.

Emociones explotadas:

- **Ilusión:** «Alguien se ha fijado en mí».
- **Soledad:** se crea un vínculo emocional.
- **Esperanza:** «Podemos tener una vida juntos, solo hay que superar un obstáculo».

Indicadores de detección:

- Historias demasiado perfectas, perfiles muy atractivos o exagerados.
- Declaraciones de amor rápidas o desproporcionadas.
- Excusas para no encontrarse presencialmente.
- Peticiones de dinero para emergencias («tengo que ir a verte, pero no puedo pagar el vuelo», «mi hijo está enfermo y no tengo seguro»).
- Dudas o incoherencias cuando se solicitan detalles concretos.

Falsos soportes técnicos o estafas de “servicio técnico”.

Formato habitual: Llamadas telefónicas, ventanas emergentes o visitas a domicilio. El estafador afirma detectar un problema grave en tu ordenador o conexión y ofrece ayuda (a cambio de acceso remoto o dinero).

Emociones explotadas:

- **Miedo:** «Tu ordenador está infectado».
- **Desesperación:** «Puedes perder todos tus datos».
- **Confianza:** se hacen pasar por Microsoft, Google o técnicos de compañías conocidas.

Indicadores de detección:

- Llamadas no solicitadas.
- Afirmaciones muy alarmantes sin pruebas.
- Presión para encender el ordenador, compartir pantalla o instalar programas.
- Solicitud de datos bancarios o pagos inmediatos.
- **Clave:** ninguna empresa tecnológica te llamará sin una solicitud previa. Ante la duda, cuelga y consulta con alguien de confianza.

Pautas de ciberseguridad, gestión emocional y canales de denuncia.

Pautas generales de ciberseguridad.

Cómo protegerse en el día a día digital.

Este bloque ofrece **recomendaciones prácticas** y fácilmente aplicables para minimizar los riesgos digitales. No se trata de convertirse en una persona experta en informática, sino de desarrollar **hábitos digitales saludables y seguros**, adaptados a las circunstancias personales de cada persona.

La regla de oro: Para, piensa y verifica

Antes de hacer clic o compartir información, es necesario detenerse un momento.

- **Para:** no actuar de manera impulsiva.
- **Piensa:** ¿tiene sentido este mensaje?, ¿conozco a la persona o a la entidad?
- **Verifica:** busca fuentes oficiales o llama al banco, empresa o institución que supuestamente lo ha enviado.

Esta regla nos ayuda a ganar tiempo para activar el pensamiento crítico.

Contraseñas fuertes y diferentes

Una buena contraseña es clave para proteger la identidad digital.

- Combina letras (mayúsculas y minúsculas), números y símbolos.
- No debería ser tu nombre, fecha de nacimiento ni “123456”.
- Evita repetir la misma contraseña en todos los servicios.
- Si es necesario, escríbelas en un lugar seguro (nunca visibles cerca del ordenador).

Actualizaciones del programario

Mantener el dispositivo actualizado **corrige errores y vulnerabilidades**.

- Las actualizaciones automáticas son recomendables.
- Tanto el móvil como el ordenador reciben mejoras de seguridad periódicas.

¡Cuidado con la información que compartimos!

No publicar datos personales en las redes sociales (dirección, vacaciones, compras).

- Las personas con malas intenciones pueden hacer un mal uso de esta información.
- Es importante configurar la privacidad de los perfiles digitales.

No abrir enlaces ni archivos sospechosos

Si no esperas el mensaje o no conoces a quien lo envía, **es mejor eliminarlo.**

- Muchos fraudes comienzan con un simple clic.
- **Ante la duda, no actuar.**

Redes Wi-Fi públicas

Evitar realizar trámites bancarios o compras online desde una Wi-Fi pública.

- **Importante**: sabemos que no todo el mundo tiene internet en casa. Si se utiliza una Wi-Fi pública, evitar introducir datos sensibles.

Cerrar la sesión en ordenadores compartidos

En bibliotecas, centros cívicos o locutorios, hay **que cerrar siempre la sesión del correo, banco o redes sociales antes de marcharse**.

- También es recomendable **borrar el historial de navegación**.

Canal de avisos oficiales de la Generalitat de Catalunya WhatsApp de ciberseguridad de la Generalitat:

https://www.whatsapp.com/channel/0029Vane15j77qVO9dIJ8L1j

- Ofrece información actualizada sobre fraudes y alertas.
- Es un recurso gratuito y fácil de usar.

La gestión emocional ante un engaño digital.

Cómo cuidarse emocionalmente si hemos sido víctimas.

Los engaños digitales no solo tienen consecuencias materiales, sino también **emocionales.** Vergüenza, tristeza, rabia o culpa son reacciones normales y legítimas. Este espacio invita a reconocer y normalizar estas emociones.

Es normal sentirse mal.

Caer en un engaño puede hacernos sentir **avergonzados, frustrados, enfadados o tristes.**

- Es importante remarcar: **no es culpa tuya.**
- Los estafadores utilizan técnicas profesionales de manipulación.

Hablarlo ayuda

El silencio favorece el sufrimiento. Compartir lo que ha ocurrido:

- Con personas de confianza (familia, amistades, referentes sociales).
- Con profesionales (bancos, cuerpos policiales, servicios sociales o jurídicos).

Expresar las emociones alivia y facilita encontrar soluciones.

Cómo reaccionar si sospechas o eres víctima

- **NO** responder al mensaje ni continuar la conversación.
- **NO** enviar dinero ni facilitar datos personales.
- Mantener la calma: respirar, alejarse del dispositivo, evitar reacciones impulsivas.
- Cortar la comunicación: bloquear el número o el correo.
- **Pedir ayuda:** no te lo guardes para ti. Compartir es protegerse.

Donde y como denunciar

Canales oficiales para recibir ayuda y denunciar una estafa.

Este bloque es breve y práctico. Se recomienda entregar una hoja impresa con esta información para facilitar su retención y consulta posterior.

Cuerpos policiales

- Llamada al 112 en casos urgentes o si la estafa está ocurriendo en ese momento.
- Denuncia presencial en cualquier comisaría.

Entidad bancaria

- Contactar inmediatamente con el banco si se han realizado transferencias o se han compartido datos bancarios.
- Pueden bloquear movimientos e iniciar investigaciones.

CERT

- Punto de referencia para la ciberseguridad
- Ofrecen:
    - Canal de contacto para incidencias.
    - Guia de buenas prácticas.
    - Alertas actualitzadas.

Recomanación final: ante la duda, **es mejor actuar** que quedarse con la inquietud. Nunca es tarde para pedir ayuda.

Desarrollo del taller

Datos del taller

Duración: 1 hora 45 minutos (ajustable entre 1h 30min y 2h)

Objetivo General: Sensibilizar a las personas mayores sobre los riesgos de la ciberdelincuencia, poniendo énfasis en la gestión emocional ante estas amenazas y proporcionando herramientas prácticas para protegerse, fomentando al mismo tiempo la confianza y la capacidad de pedir ayuda.

Participantes máximos: 12 personas

Material necesario: Proyector, ordenador, conexión a internet (si es posible, para mostrar ejemplos), pizarra o papel/cartulina y rotuladores.

Secuencia formativa:

- Parte 1. Bienvenida y desmontando mitos: las emociones en el mundo digital – 20 minutos.
- Parte 2. Reconociendo el engaño emocional y las estafas más comunes – 45 minutos.
- Parte 3. Herramientas para la protección y la resiliencia emocional – 40 minutos.
- Parte 4. Resolución de dudas e ideas clave de recuerdo – 15 minutos.

Parte 1. Bienvenida y desmontando mitos: las emociones en el mundo digital

- **Bienvenida y creación de un espacio de confianza (5 minutos)**: dar la bienvenida y presentar el taller como un espacio seguro para aprender y compartir. **Pregunta abierta**: «¿Por qué estáis aquí?, ¿qué nos mueve a utilizar internet o el móvil?, ¿y qué miedos o inquietudes nos generan?» (Fomentar la participación sin juzgar, únicamente para recoger impresiones).
- **Las emociones como "gancho" de la ciberdelincuencia (15 minutos)**: explicar que todas las emociones (alegría, tristeza, miedo, confianza, ilusión, rabia, etc.) forman parte de la vida y del ser humano, y también están presentes en el mundo digital. **Punto clave**: los ciberdelincuentes conocen muy bien nuestras emociones y las utilizan como "ganchos" para manipularnos. No se trata de ingenuidad, sino de manipulación psicológica.

Las personas participantes deberán adivinar la definición de las siguientes emociones:

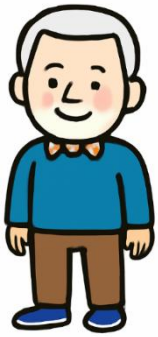
- **Confianza**: seguridad que permite a una persona abrirse y mostrar su vulnerabilidad ante otra, con la certeza de que será escuchada, respetada y no juzgada.
- **Miedo**: respuesta interna ante la percepción de una amenaza o peligro, real o imaginado.
- **Urgencia**: sensación intensa de que algo debe resolverse de manera inmediata.
- **Culpabilidad**: sensación interna de responsabilidad por haber hecho (o dejado de hacer) algo que ha causado un daño o perjuicio, real o percibido.
- **Ilusión**: emoción positiva que surge ante la esperanza de que ocurra algo bueno.
- **Preocupación**: emoción que aparece cuando anticipamos que algo puede ir mal o generar consecuencias negativas.

- **Soledad**: estado de quien es (o se siente) solo, vive solo o casi solo. Es la percepción de desconexión emocional o ausencia de vínculos significativos con otras personas.
- **Desesperación**: emoción profunda que surge cuando sentimos que hemos perdido toda esperanza y no vemos salida ante una situación difícil.
- **Duda**: emoción o estado mental que aparece cuando no estamos seguros de qué pensar, sentir o hacer. Suele surgir ante la incertidumbre, la falta de información o el miedo a equivocarse.

Parte 2. Reconociendo el engaño emocional y las estafas más comunes

(10 minutos) Se comenzará preguntando a las personas participantes: «¿Por qué pensáis que podéis ser objetivo de ciberestafas?». La intención de la pregunta es desmontar los mitos relacionados con la edad. A partir de esta cuestión, se explicarán los cinco puntos anteriores. A continuación, se presentarán los dos avatares que nos acompañarán en la actividad siguiente.

Paquita tiene 79 años y ha vivido toda su vida en el mismo barrio [o pueblo], un lugar que conoce como la palma de su mano. Le gusta mantenerse activa y conectada con su comunidad. Disfruta de paseos diarios por el barrio, siempre a un ritmo tranquilo. Los cafés con sus amigas son momentos esenciales para ella; se convierten en pequeños encuentros para charlar, compartir recuerdos y disfrutar de las pequeñas cosas de la vida. Es una mujer que aprecia los detalles sencillos, como una buena conversación o una sonrisa. Sus amigas la ven como una fuente de sabiduría, alguien a quien pueden acudir para recibir consejos amables pero profundos. A pesar de ser una persona tranquila, Paquita siente una gran pasión por la amistad y la escucha activa, ofreciendo apoyo emocional a quien lo necesita. Es independiente y disfruta de su propia compañía, pero nunca duda en pasar tiempo con sus seres queridos. En los últimos años ha participado en algunos cursos de alfabetización digital en el centro cívico del barrio y, aunque no lo domina del todo, se defiende bastante bien. Aun así, ha visto cómo algunos amigos suyos, que saben mucho más que ella, han sido víctimas de engaños por internet. Estas experiencias la han hecho estar más alerta, pero también le han dejado claro que no es suficiente con saber un poco: cualquiera puede caer.



Antoni/o tiene 74 años y también ha vivido toda su vida en el mismo barrio [o pueblo]. Es un hombre que encuentra alegría en las pequeñas cosas, como pasear por el parque o disfrutar de un día soleado. Por las tardes, quizá lo encuentres sentado con sus amigos, compartiendo alguna historia o simplemente disfrutando de una buena conversación. Es un hombre simpático, de carácter afable y con una gran pasión por las plantas. Cuidar su huerto comunitario es una de sus actividades preferidas; no solo lo hace por afición, sino también como una forma de enriquecer su vida y establecer conexiones con los demás. Aunque es un hombre más reservado, su presencia transmite calidez y bondad. Siempre tiene un consejo generoso que ofrecer y nunca pierde la oportunidad de hacer un pequeño gesto amable hacia los demás. A Antoni también le gusta la soledad en momentos concretos, pero su actitud abierta hace que todo el mundo se sienta cómodo a su alrededor. Últimamente, sin embargo, se siente un poco preocupado. Sus nietos le han explicado que hay muchas personas mayores que reciben engaños por teléfono o por internet, y le han dicho que tenga cuidado. Aunque intenta mantenerse tranquilo, a veces le da miedo no darse cuenta si alguien quiere aprovecharse de él.

Una vez explicados los personajes, se repartirán diferentes carteles con emociones para que las personas participantes levanten la emoción o emociones que les despierta cada estafa. En la pantalla se proyectarán distintas estafas (10 minutos por estafa) y se leerán en voz alta. Tras la lectura de la primera estafa, se preguntará a las personas participantes qué emoción sienten al leerla.

A partir de aquí, la persona tallerista hará hincapié en la importancia de identificar estas emociones para prevenir y no caer en engaños. A continuación, ofrecerá algunos consejos sobre cómo detectar cada estafa y aportará ejemplos concretos de este tipo de fraude.

Los ejemplos de estafas se vincularán con los avatares presentados: ¿cómo se adaptaría este tipo de estafa al perfil del avatar?, ¿con qué elementos de su biografía o perfil conecta? De este modo, se relacionarán las estafas con situaciones que resultan familiares y “cotidianas” para las personas mayores participantes en el taller.

Por ejemplo: Paquita es más sociable, por lo que puede tener más posibilidades de caer en una estafa relacional o romántica; Antoni tiene hijos y nietos y dispone de menos competencias digitales que Paquita; existe la posibilidad de la estafa de “hijos en apuros”.

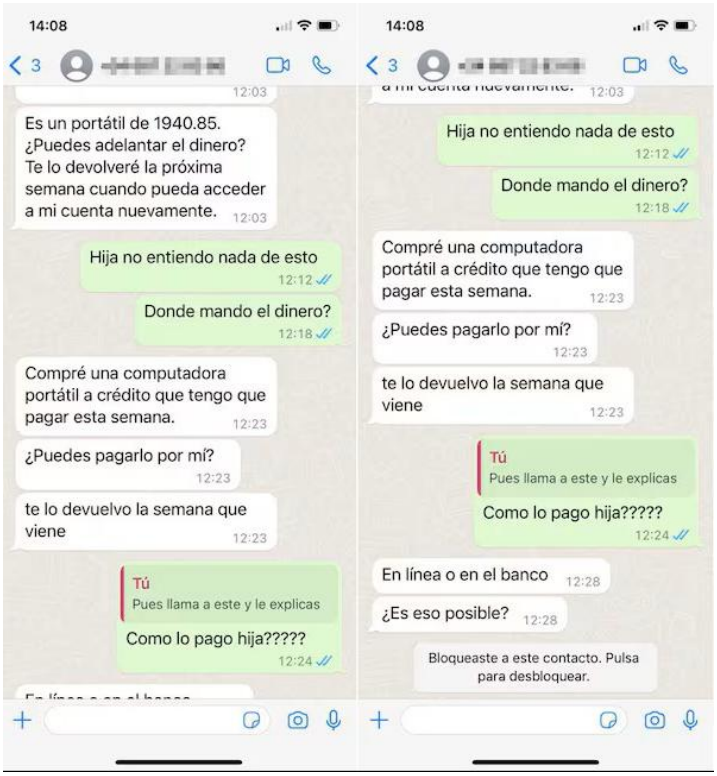
Una vez trabajadas todas las estafas, se realizará una conclusión final sobre cómo deberían actuar si reciben una llamada.

Phishing/Smishing (correos o mensajes falsos)

Se hacen pasar por bancos, administraciones públicas (Hacienda, Seguridad Social), Correos o empresas de suministros.
Emociones clave: Miedo (si no haces clic, tendrás problemas o una multa).Urgencia (tu tarjeta caduca, la cuenta está bloqueada).
Cómo detectarlo: URL extraña o mal redactada. Faltas de ortografía. Saludos genéricos. Solicitud urgente de datos. No esperabas ningún paquete. El número no te resulta conocido. Mensaje demasiado genérico.En ocasiones, la URL parece correcta, pero el enlace real es falso.

Estafa del "hijo en apuros"

Un mensaje (a menudo por WhatsApp) de un supuesto familiar que necesita dinero de manera urgente.
Emociones clave: Preocupación. Urgencia.
Cómo detectarlo: No contacta desde el número habitual. La historia es excesivamente dramática. Presión para realizar la transferencia con rapidez. La forma de expresarse del “hijo” resulta extraña o no coincide con la habitual. Verificar siempre por otra vía antes de actuar.



Estafas sentimentales/románticas:

Alguien se interesa por ti en línea y, después de ganarse tu confianza, pide dinero para una supuesta emergencia.
Emociones clave: Ilusión. Soledad. Esperanza.
Cómo detectarlo: Historias demasiado perfectas. Declaraciones de amor rápidas o desproporcionadas. Excusas para no encontrarse en persona. Peticiones de dinero. Falta de detalles o incoherencias en el relato.

Falsos soportes técnicos:

Llamadas o ventanas emergentes que afirman que tienes un virus y te piden acceder a tu ordenador o realizar un pago. [No siempre es virtual: también puede tratarse de una estafa "puerta a puerta" o telefónica]
Emociones clave: miedo, desesperación, confianza.
Cómo detectarlo: Ninguna empresa como Microsoft o Google te llamará sin que tú lo hayas solicitado. Ante la duda, cierra todo y contacta con alguien de confianza.

Conclusión. Cómo reaccionar si te sientes atacado o engañado:

NO responder: bloquear el número y borrar el correo.
NO enviar dinero ni datos personales.
Mantener la calma: respirar y no tomar decisiones precipitadas.
Cortar la comunicación.
Pedir ayuda: no te quedes solo/a con esto.

Parte 3. Herramientas para la protección y la resiliencia emocional

En esta parte se presentará a las personas participantes, de manera cercana y dinámica, un tríptico con la información más relevante sobre ciberseguridad desde el punto de vista emocional y con información sobre dónde denunciar. (5–10 minutos).

Pautas generales de ciberseguridad

- **La regla de oro: "Para, Piensa y Verifica"**: antes de hacer cualquier clic, parar, pensar si es lógico y verificar con una fuente oficial (llamando al banco, buscando la web oficial, etc.).
- **Crear contraseñas fuertes**: explicar de forma sencilla qué es una contraseña robusta y por qué es importante tener contraseñas diferentes.
- **Realizar actualizaciones de software**: la importancia de mantener el móvil/ordenador actualizado para protegerse de vulnerabilidades.
- **Cuidado con la información que compartimos**: no publicar datos personales, vacaciones, etc., en redes sociales.
- **No abrir enlaces ni archivos sospechosos**: si no se está seguro, es mejor eliminarlo.
- **Evitar redes Wi-Fi públicas para operaciones sensibles**: banco, compras, etc. [IMPORTANTE: tener en cuenta la vulnerabilidad; hay gente que no tiene internet en casa].
- **Cerrar la sesión si se utilizan ordenadores públicos** (biblioteca, centros cívicos, locutorios, etc.).
- **Consultar el WhatsApp de la Generalitat de Cataluña que avisa de estafas**:https://www.whatsapp.com/channel/0029Vane15j77qVO9dIJ8L1j

La gestión emocional delante el engaño

Normalizar los sentimientos: es NORMAL sentirse avergonzado, frustrado, enfadado o triste si se es víctima de un engaño. No es culpa tuya. (15 minutos)

La importancia de hablarlo:

- **Con la familia o amistades de confianza**: compartir lo ocurrido alivia la carga emocional y puede ayudar a encontrar soluciones.
- **Con profesionales**: banco, cuerpos policiales, servicios sociales.

Cómo reaccionar si te sientes atacado o engañado:

- **NO responder**: bloquear el número y borrar el correo.
- **NO enviar** dinero ni datos personales.
- **Mantener la calma**: respirar y no tomar decisiones precipitadas.
- **Cortar la comunicación**.
- **Pedir ayuda**: no te quedes solo/a con esto.

Dónde y cómo denunciar:

- **Cuerpos policiales**: acudir a comisaría o llamar al 112 (en casos urgentes o si está ocurriendo en ese momento).
- **Banco**: si ha habido movimientos de dinero.
- **Agencia de Ciberseguridad de Cataluña (CERT de Cataluña)**: punto de contacto para incidencias de ciberseguridad.

Parte 4. Resolución de dudas y claves de recuerdo

- **Espacio de preguntas y dudas (15–20 minutos):**
  - Abrir el turno de palabra para que las personas participantes hagan preguntas.
  - Responder de forma clara y sencilla, fomentando la participación.
- **Recapitulación y mensajes clave para llevarse a casa (5 minutos):**
  - **La tecnología es una herramienta útil**: no debemos tener miedo a utilizarla, sino aprender a hacerlo de forma segura.
  - **La resiliencia**: cada experiencia, incluso las negativas, nos ayuda a aprender y a fortalecer nuestra seguridad y bienestar emocional.
  - **Recordatorio**: no estás solo/a. Pedir ayuda es la mejor protección.

Anexo 4. Modelo de cartel de los talleres

Anexo 5. Modelo del díptico


¿Cómo prevenir?
Contraseñas
Fuertes y seguras
Actualizaciones
Del software de los dispositivos
Protección
De la información personal
Redes
Evita enlaces sospechosos
Dispositivos
Cierra la sesión en ordenadores públicos
Conexión
Utiliza redes seguras
Información
Mantente informado/a
No tengas miedo a preguntar
Apóyate en tu entorno y comunidad
¿Cómo reaccionar?
¿Te sientes presionado/a?
¿Tienes sensación de urgencia?
¿Te transmite seguridad?
¿La situación te angustia?
PARA
PIENSA
VERIFICA
5 PEDIR AYUDA
4 CORTAR LA COMUNICACIÓN
3 MANTENER LA CALMA
2 NO COMPARTIR DATOS
1 IDENTIFICAR EMOCIONES
¿Cómo denunciar?
UNA VEZ ESTAFADO/DA...
NO TE SIENTAS CULPABLE
Nos puede pasar a todas...
¿ES URGENTE?
SÍ → Llamar al 112
NO → Ir a comisaría
¿EXISTE MOVIMIENTO DE DINERO?
SÍ → Contactar con tu entidad bancaria
NO → Contactar con CATALONIA-CERT o INCIBE
Acceder a recursos e información

Anexo 6. Materiales para la realización del taller

Confianza

Miedo

Urgencia

Culpabilidad

Ilusión

Preocupación

Soledad

Desesperación

Duda

Anexo 7. Programa workshop

Workshop online

Ciberseguridad para gente mayor

Inscripción aquí

1 DE DICIEMBRE

11 - 13H

"Promover la seguridad digital de las personas mayores es también cuidar su bienestar y su autonomía."

Con motivo del **Día Mundial de la Ciberseguridad,** que se celebra el 30 de noviembre, hemos organizado un workshop dirigido a profesionales y agentes vinculados a la atención de las personas mayores.

¿Qué encontrarás?

- Aprende a detectar, acompañar y proteger.
- Activa tu centro como radar de barrio.
- La ciberseguridad también se construye en comunidad.

¡Súmate al workshop y ayúdanos a construir respuestas frente a la ciberdelincuencia en personas mayores!

Contacto

Equipo de Consultoría y Estudios. Fundación Pere Tarrés.
cguardiet@peretarres.org 934 101 602 Ext. 3593

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

Anexo 8. Toolkit

CHECKLIST DE SEÑALES DE VULNERABILIDAD

INDICADORES DE VULNERABILIDAD DIGITAL:

Dificultades digitales básicas

- [ ] Le cuesta mucho saber si un mensaje es real o falso.
- [ ] No sabe qué hacer cuando recibe un SMS; correo o llamada extraña.
- [ ] Tiene miedo de utilizar el teléfono móvil o el ordenador.

Comportamientos de riesgo

- [ ] Hace clic en cualquier enlace sin pensar.
- [ ] Da información personal con facilidad.
- [ ] Acepta ayuda de desconocidos para "hacer gestiones".

Señales emocionales

- [ ] Se pone nervioso/a cuan recibe mensajes o llamadas.
- [ ] Tiene vergüenza de decir que no entiende alguna cosa.
- [ ] Está asustado/da y dice "me pueden engañar".

Situaciones que preocupan

- [ ] Ha recibido muchos mensajes sospechosos últimamente.
- [ ] Ha perdido dinero o no sabe explicar algún pago.
- [ ] Tiene movimientos extraños en la cuenta o tarjeta.

Riesgo inmediato

- [ ] Ha dado la contraseña, códigos o fotos del DNI.
- [ ] Ha realizado un pago o transferencia que no tocaba.
- [ ] Ha instalado una aplicación que no reconoce.

COMO USARLO:

- [x] 1 o 2 señales: Atención suave → dar consejos y revisar dudas.
- [x] 3 o 4 señales: Vulnerabilidad clara → activación de circuito preventivo.
- [x] Cualquier señal de riesgo inmediata: Acción urgente. Llamar a la policía.

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

CIRCUITOS

CIRCUITO 1 → **Cuando recibe un mensaje sospechoso (no ha hecho nada)**

LA PERSONA RECIBE UN MENSAJE EXTRAÑO
↓
EXPLICAR EL CASO AL/LA PROFESIONAL
↓
EL/LA PROFESIONAL ESCUCHA Y TRANQUILIZA
↓
REVISA EL MENSAJE CON LA PERSONA
(WhatsApp / SMS / Correo / Llamada)
↓
ES UNA ESTAFA? ——► **NO**
|
SÍ
↓
ACCIÓN:
- Bloquear el número/correo
- Borrar el mensaje
- No contestar
↓
EXPLICAR CÓMO DETECTAR FUTURAS ESTAFAS
↓
ACOMPAÑAMIENTO BREVE
"Si tienes dudas, tráemelo antes de hacer nada."
↓
FIN DEL CIRCUITO

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

CIRCUITO 2 → **Ha contestado, pero NO ha dado datos**

LA PERSONA HA RESPONDIDO A UN MENSAJE
↓
ESTÁ PREOCUPADA Y LO EXPLICA
↓
EL/LA PROFESIONAL CALMA:
"Estás a tiempo de pararlo."
↓
REVISAR QUÉ HA HECHO:
- ¿Hizo clic?
- ¿Abrió algún enlace?
-¿Escribió alguna respuesta?
↓
ACCIÓN:
- Bloquear el contacto
- Cambiar contraseñas básicas
- Revisar Apps estrañas
↓
ACOMPAÑAMIENTO:
"Ven mañana para asegurarnos de que todo está bien."
↓
DERIVACIÓN SI HACE FALTA:
- Dinamizador/a TIC
- Familiares o persona de confianza
↓
FIN DEL CIRCUITO

GOBIERNO DE ESPAÑA MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

CIRCUITO 3 → **Ha dado datos, códigos o dinero**

LA PERSONA HA DADO DATOS / CÓDIGOS / DINERO
↓
LA PERSONA ESTÁ ANGUSTIADA O AVERGONZADA
↓
EL/LA PROFESIONAL TRANQUILIZA:
"No es culpa tuya. Lo arreglaremos paso a paso."
↓
PREGUNTAR QUÉ HA ENTREGADO EXACTAMENTE:
- Datos personales?
- Contraseñas?
- Tarjeta bancaria?
- Códigos por SMS?
- Transferencias?
↓
ACCIONES URGENTES:

SI HAY DATOS DEL BANCO:
→ Orientarla para que llame al banco o vaya a la sucursal para bloquear tarjeta/cuenta.

SI HAY CONTRASEÑAS:
→ Cambiar contraseñas inmediatamente.
→ Activar la verificación en dos pasos.

SI HA PERDIDO DINERO:
→ Recoger información
→ Orientar hacia la denuncia (Policía). Indicarle que no borre mensajes ni ninguna evidencia.

↓
ACOMPAÑAMIENTO ACTIVO:
"Te ayudo a hacer la llamada o a preparar la denuncia."
↓
SEGUIMIENTO:
Revisar en los días siguientes si todo continúa seguro.
↓
FIN DEL CIRCUITO

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

CIRCUITO 4 → Cuando el riesgo no es claro (situación difusa)

MENSAJE / LLAMADA / SITUACIÓN AMBIGUA

↓

EL/LA PROFESIONAL ESCUCHA Y OBSERVA

↓

FORMULAR 3 PREGUNTAS CLAVE:

1. ¿Te pedían dinero?
2. ¿Te pedían datos?
3. ¿Te hicieron sentir prisa?

↓

SI ALGUNA ES "SÍ" → TRATAR COMO RIESGO MEDIO/ALTO

↓

SI TODO ES "NO" → probablemente no es estafa

↓

ACCIÓN:

- Explicar precauciones
- Recomendar no responder
- Revisar futuros mensajes

↓

FIN DEL CIRCUITO

CIRCUITO 5 → Acompañamiento emocional (transversal a todos)

PERSONA ASUSTADA / AVERGONZADA

↓

EL/LA PROFESIONAL ACOGE:

"Es normal sentirse así."

"No estás solo/a."

↓

NORMALIZAR:

"A mucha gente le pasa."

↓

MARCAR CONTROL:

"Lo revisaremos juntos/as y lo podemos arreglar."

↓

ACOMPAÑAMIENTO:

Ofrecer ayuda para llamar, revisar, denunciar.

↓

SEGUIMIENTO SUAVE:

"Si te sientes mal, ven y lo hablamos."

↓

FIN DEL CIRCUITO

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

SCRIPT DE PRIMERA ACOGIDA

SI LA PERSONA MAYOR EXPRESA DUDAS O SOSPECHA DE ESTAFA

OBJETIVO

Escuchar, validar, reducir la angustia y obtener información básica para valorar el riesgo.

1 ACOGIDA Y VALIDACIÓN

"Entiendo que esto te preocupa. Gracias por explicármelo. Aquí estás en un espacio seguro y veremos juntos qué ha pasado."

2 PREGUNTA ABIERTA PARA SITUAR EL CASO

"¿Me puedes contar qué ha pasado paso a paso? ¿Cuándo lo recibiste y qué te hizo sospechar?"

3 RECOGIDA MÍNIMA DE INFORMACIÓN (SIN HACER SENTIR INTERROGADA A LA PERSONA)

¿Qué canal fue? (teléfono, SMS, WhatsApp, correo, redes...)
¿Qué pedían? (datos, dinero, clics, contraseña...)
¿Sabes si llegaste a hacer clic/enviar algo?

4 TRANQUILIZAR Y NORMALIZAR

"Cada vez hay más casos como este. No es tu culpa: estos fraudes están hechos expresamente para engañar y son muy convincentes."

5 PRIMER CONSEJO DE SEGURIDAD

"Lo más importante ahora mismo es no responder y no hacer clic en nada más."

6 DERIVACIÓN O SEGUIMIENTO

"Si te parece, revisemos juntos qué puedes hacer ahora mismo para protegerte, y si es necesario te ayudo a contactar con los servicios de apoyo correspondientes."

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

SCRIPT PARA PERSONAS MAYORES
QUE NO ESTÁN SEGURAS DE SI HAN SIDO VÍCTIMAS

OBJETIVO

Resolver dudas sin hacer que la persona se sienta ignorante.

"Es muy buena idea consultarlo. A veces no es fácil distinguir si es una estafa o no, y preguntar es la mejor manera de prevenir."

"¿Me explicarías qué recibiste o qué te pidieron? Así podré orientarte sobre si existe un riesgo real."

SI PARECE UNA ESTAFA:

"Entiendo la confusión: estas estafas están diseñadas para parecer reales. Te propongo dar el paso X (bloquear, denunciar, revisar movimientos...). Te acompaño en ello."

SI NO PARECE UNA ESTAFA:

"Por lo que me explicas, no parece un caso de riesgo, pero has hecho muy bien en preguntar. Siempre es una buena práctica comprobarlo."

SCRIPT CUANDO LA PERSONA ESTÁ
MUY ANGUSTIADA O AVERGONZADA

OBJETIVO

Reducir el impacto emocional, evitar la culpa y ofrecer apoyo.

"Es normal que te sientas así. Estas situaciones pueden generar mucha angustia, pero no estás solo/a. Estamos aquí para ayudarte."

"A cualquiera le puede pasar. Además, estas estafas están pensadas para presionar y confundir. Lo importante ahora es qué hacemos a partir de este momento, y te acompañaré en el proceso."

"Si te parece, respiramos un momento juntos/as y lo revisamos con calma."

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

SCRIPT DE DETECCIÓN PROACTIVA
(CUANDO EL/LA PROFESIONAL VE INDICIOS)

OBJETIVO

Abrir conversación sin señalar ni juzgar.

"Estamos viendo muchos casos de llamadas y mensajes sospechosos estos días. ¿Has recibido algo raro últimamente?"

"A veces parece que es del banco o de Correos, pero puede ser una estafa. Si alguna vez tienes dudas, nos lo puedes comentar sin ningún problema."

"Hace poco hemos ayudado a otras personas a las que les pasó algo parecido, así que si necesitas revisar algo, lo hacemos juntos/as."

SCRIPT CUANDO LA PERSONA ADMITE
QUE HA DADO DATOS O DINERO

OBJETIVO

No culpabilizar, recoger información clave y activar medidas.

"Gracias por contármelo y por confiar en mí. Es más habitual de lo que parece, y has hecho muy bien en decirlo."

"Para poder ayudarte, ¿puedo preguntarte qué llegaste a compartir o enviar? (datos personales, datos bancarios, códigos, dinero, contraseñas…)"

"Con lo que me explicas, lo más recomendable es hacer estos pasos: … Si quieres, los hacemos juntos/as."

"Es importante que no te culpes. Lo que importa es que hemos reaccionado a tiempo."

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

SCRIPT PARA REFORZAR EMPODERAMIENTO Y PREVENCIÓN AL FINAL DE LA CONVERSACIÓN

OBJETIVO

Reforzar el empoderamiento, consolidar pautas de prevención y promover la consulta antes de actuar.

"Recuerda que no tienes que hacer nada que no tenga sentido o que te presione. Tienes derecho a parar la conversación, colgar o pedir ayuda."

"Lo más importante es que, si tienes cualquier duda, antes de iniciar cualquier trámite nos lo consultes. Esa es la mejor protección."

"Si quieres, puedo darte algunos consejos prácticos para que no te vuelva a pasar y para que te sientas más seguro/a."

GOBIERNO DE ESPAÑA MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL
FUNDACIÓ PERE TARRÉS

PARA

PÁRATE. RESPIRA. NO HAGAS CLIC.

PIENSA

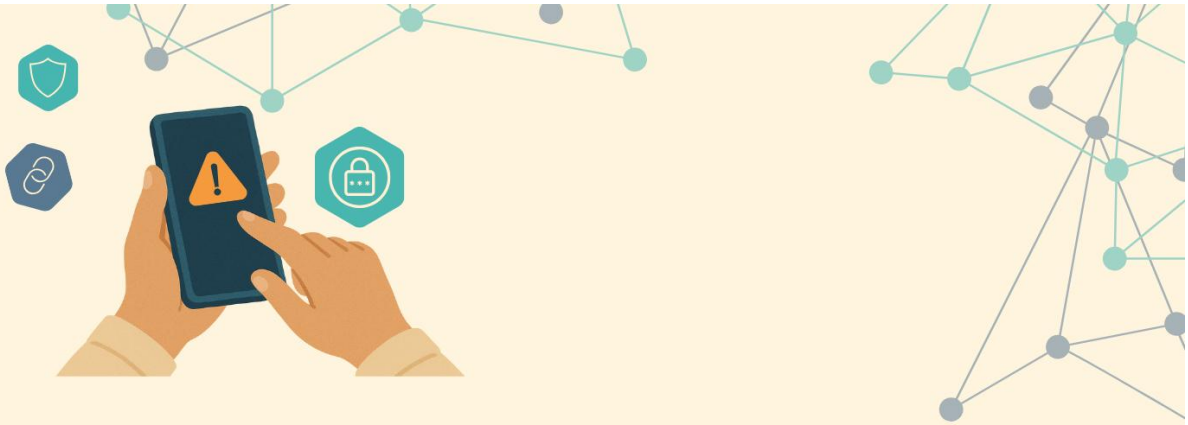
¿ESTA PERSONA TE PIDE DINERO O INFORMACIÓN?

VERIFICA

ENSEÑA EL MENSAJE A ALGUIEN ANTES DE HACER NADA

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS



PARA

AYUDA A LA PERSONA A FRENAR EL IMPULSO DE ACTUAR SIN PENSAR.

PIENSA

HACEROS JUNTOS 3 PREGUNTAS:

- **¿PIDE DATOS?**
- **¿PIDE DINERO?**
- **¿TIENES SENSACIÓN DE PRISA O MIEDO?**

VERIFICA

COMPROBAD JUNTOS LA INFORMACIÓN ANTES DE RESPONDER.

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

FUNDACIÓ PERE TARRÉS

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

PARA
NO HAGAS CLIC. NO RESPONDAS. NO PAGUES.

SI TE LLEGA UN MENSAJE EXTRAÑO, PARA.

LAS ESTAFAS SIEMPRE QUIEREN QUE HAGAS LAS COSAS RÁPIDO.

TIENES DERECHO A TOMARTE TU TIEMPO.

RECORDATORIO CLAVE:

“CUANDO TIENES PRISA, ES MÁS FÁCIL QUE TE ENGAÑEN.”

GOBIERNO DE ESPAÑA · MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

FUNDACIÓ PERE TARRÉS

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD: OTROS FINES DE INTERÉS SOCIAL

PIENSA

¿QUÉ ME PIDEN? ¿POR QUÉ TANTA PRISA?

¿TE PIDEN DINERO?

¿TE PIDEN DATOS O CONTRASEÑAS?

¿TE HACEN SENTIR MIEDO, PRISA O CULPA?

¿TE DICEN QUE “SI NO LO HACES AHORA, HABRÁ PROBLEMAS”?

SI ALGUNA RESPUESTA ES “SÍ”:

ES MUY PROBABLE QUE SEA UNA ESTAFA.

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030
POR SOLIDARIDAD: OTROS FINES DE INTERÉS SOCIAL

FUNDACIÓ PERE TARRÉS

VERIFICA

PREGUNTA A ALGUIEN DE CONFIANZA. NOS LO PUEDES ENSEÑAR.

ENSEÑA EL MENSAJE A ALGUIEN DEL CASAL, BIBLIOTECA O CENTRO.

LLAMA TÚ MISMO AL BANCO, A CORREOS O A QUIÉN SEA.

BUSCA EL TELÉFONO REAL (NO EL DEL MENSAJE).

SI TIENES DUDAS: MEJOR NO HACER NADA ANTES DE VERIFICAR.

RECORDATORIO CLAVE:
"ENSEÑAR UN MENSAJE A ALGUIEN ES LA MEJOR PROTECCIÓN."

Anexo 9. Comentarios de los evaluadores externos

Casal	Dia	Hora	Direcció	Observacions
Casal Gent Gran Sant Genís	2 octubre	17:00 – 19:00 h	Carrer de Naïm, Horta- Guinardó, 08035 Barcelona	*Es van repartir + tríptics dels que tocaven. Es faran + còpies.*
Casal de Gent Gran Penitents	13 octubre	11:15-13:15h	Pg. de la Vall d'Hebron, 76-78, Gracia, 08023 Barcelona	*Tot ok*
Casal de Gent Gran de la Palmera	17 octubre	10:30-12:30h	Carrer d'Olesa, 41, Sant Andreu, 08027 Barcelona	*Tot ok*
Casal de Gent Gran Bon Pastor	21 octubre	11:45-13:45h	Carrer d'Ardèvol, 25, Sant Andreu, 08030 Barcelona	*Per una errada per part del CGG de convocatoria, el taller inicia 30 min + tard. Els talleristes recuperaran aquest temps de les hores de "programació".*
Casal Gent Gran Baix Guinardó	21 octubre	17:00 – 19:00 h	Carrer de la Marina, 380, 08025 Barcelona	*La millora que proposen és que el taller tingui més duració, ja sigui allargant el taller el mateix dia o fent dues sessions.*
Casal de Gent Gran Montmany	22 octubre	16:00-18:00h	Carrer de Montmany, 45, Gràcia, 08012 Barcelona	*Va anar molt bé, tant pel que fa a l'organització com per la sessió. Les usuàries van sortir molt contentes i van comentar-me que havia superat les seves expectatives*
Casal Gent Gran Vall d'Hebron	23 octubre	10:00 – 12:00 h	Carrer de l'Arquitecte Moragas, 5, Horta-Guinardó, 08035 Barcelona	*"El taller va agradar molt i es van quedar amb ganes de poder fer sessions al llarg del trimestre."*
Casal de Gent Gran Navas	24 octubre	10:00-12:00 h	Carrer de Capella, 14, Sant Andreu, 08041 Barcelona	

Espai de Gent Gran La Violeta	29 octubre	16:30-18:00h (horari definitiu 16.00 a 18.30)	Carrer de Maspons, 6, Gràcia, 08012 Barcelona	*Dinamització demana començar 30 min abans (ho demana el dia 21/10/2025). Els talleristes donen l'ok)*
Casal de Gent Gran Bascònia	30 octubre	10:30-12:30h.	Carrer de Bascònia, 42, Sant Andreu, 08030 Barcelona	*"El taller al nostre casal ha anat molt bé i ha agradat molt a totes les persones participants.* *Hem trobat que l'activitat s'ha desenvolupat segons el previst i que els objectius plantejats s'han complert amb èxit.* *En general, tot ha estat molt satisfactori, tant pel contingut com per la dinamització. No tenim cap suggeriment concret de millora, però sí que animem a continuar organitzant activitats d'aquest tipus, ja que aporten molt valor a la comunitat i fomenten la participació i el vincle entre les persones.Gràcies de nou per la vostra dedicació i per compartir aquest projecte amb nosaltres.*

7

FUNDACIÓ
PERE TARRÉS

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL