TRABAJO FIN DE GRADO – GRADO EN CRIMINOLOGÍA

RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior

Autora del TFG:

Paula Del Pozo Manzano

Tutora del TFG:

Dra. Susana Berrocal Díaz

UNIVERSIDAD EUROPEA DE VALENCIA

2024/2025

Paula Del Pozo Manzano

RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior

UNIVERSIDAD EUROPEA

Facultad de Ciencias Sociales

Grado en Criminología

Tutora: Dra. Susana Berrocal Díaz

Valencia, a 31 de mayo de 2025.

"La protección de los vulnerables no es un acto de compasión, sino de justicia".

Michelle Bachelet.

DEDICATORIA

A todas las personas mayores, que nos han cuidado y guiado con paciencia, amor y entrega.

A quienes, con años vividos y caminos recorridos, siguen enfrentando los desafíos de un mundo cada vez más digitalizado.

A quienes, pese a la brecha tecnológica, no dejan de adaptarse, aprender y resistir.

A quienes necesitan ser acompañados, protegidos y comprendidos.

Que estas páginas sean un pequeño gesto de gratitud, una contribución a una sociedad más justa, más empática y verdaderamente adaptada para todos.

AGRADECIMIENTOS

A mis padres, por creer en mí incluso cuando yo dudaba, por acompañarme en cada meta y por darme la fuerza, la confianza y el amor que han hecho posible este camino. Gracias por ser mi impulso y enseñarme lo que significa el esfuerzo, la paciencia y la dedicación.

A mi hermana, Elena, por ayudarme a traducir mis ideas en algo bonito y lleno de sentido, con su creatividad desbordante y su apoyo constante.

A Patricia, por apoyarme y animarme en cada paso de este proceso. Gracias por sostenerme y recordarme, una y otra vez, que sí podía lograrlo.

A Jimena, por compartir conmigo este recorrido de aprendizaje y pasión por la Criminología. Gracias por tu apoyo incondicional.

A mi profesora, Susana, por guiarme en el camino de la Criminología y enseñarme su verdadero sentido. Gracias por transmitir con tanto cariño, compromiso y pasión.

Este trabajo también es vuestro.

Resumen

La población senior, entendida como aquellos individuos mayores de 65 años, se enfrenta a una emergente sofisticación de las amenazas cibernéticas, en el que proliferan nuevas técnicas dificultan la identificación de las señales de alerta.

La escasa familiaridad con el entorno tecnológico, junto a la alta confianza interpersonal que presenta este grupo poblacional, hace que, desde una perspectiva criminológica, se conviertan en un colectivo especialmente vulnerable y en consecuencia en un objetivo prioritario para los ciberdelincuentes.

En este contexto, y con la intención de emplear como herramienta preventiva el control social, se plantea, tras el análisis de teorías criminológicas aplicables como la Teoría del Control Social de Hirschi o la Teoría de las Actividades Rutinarias de Cohen y Felson, un programa de prevención de estafas digitales denominado “RED SENIOR SEGURA”.

Esta propuesta está diseñada con el objetivo de proporcionar, desde una perspectiva adaptada a sus necesidades, materiales accesibles y fomentar una participación activa del público objetivo. En suma, su finalidad es promover un desarrollo y conocimiento de elementos clave para reforzar, empoderar y potenciar la autonomía digital de la población senior.

Se apuesta así por una prevención empática y de educación digital, como forma de reducir las oportunidades delictivas de los ciberdelincuentes y aumentar las buenas prácticas de seguridad digital en las actividades cotidianas de la población senior.

Palabras-clave: población senior, estafas digitales, control social, educación digital, prevención.

Abstract

The senior population, understood as individuals over 65 years of age, is facing an emerging sophistication of cyber threats, in which new techniques proliferate, making it difficult to identify warning signs. The lack of familiarity with the technological environment, together with the high interpersonal trust that this population group provides, makes them, — from a criminological perspective — a particularly vulnerable group and therefore a priority target for cybercriminals.

In this context, and with the intention of using social control as a preventive tool, we propose, after the analysis of applicable criminological theories such as Hirschi's Social Control Theory or Cohen and Felson's Theory of Routine Activities, a program for the prevention of digital scams called “RED SENIOR SEGURA” (SAFE SENIOR NETWORK).

This proposal is designed with the objective of providing, from a tailored perspective, accessible materials and encouraging an active participation of the target audience. In short, its purpose is to promote the development and knowledge of key elements to strengthen, empower and enhance the digital autonomy of the senior population.

It is thus committed to empathetic prevention and digital education, as a way to reduce criminal opportunities for cybercriminals and increase good digital security practices in the daily activities of the senior population.

Keywords: senior population, digital scams, social control, digital education, prevention.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE SIGLAS Y ABREVIATURAS

Sigla	Inglés	Español
DNI	*National Identity Document*	Documento Nacional de Identidad
INCIBE	*National Cybersecurity Institute*	Instituto Nacional de Ciberseguridad
INE	*National Statistics Institute*	Instituto Nacional de Estadística
ISI	*Introduction, Self-protection, Interaction*	Introducción, Autoprotección, Interacción
OSINT	*Open Source Intelligence*	Inteligencia de Fuentes Abiertas
PMS	*Senior Security Plan*	Plan Mayor de Seguridad
SMS	*Short Message Service*	Mensajes de texto
TIC	*Information and Communication Technologies*	Tecnologías de la Información y la Comunicación

1. INTRODUCCIÓN

1.1. Problema de investigación

En la actualidad, el desarrollo del entorno digital está avanzando de forma realmente acelerada, generando un escenario nuevo propicio para la comisión de nuevos fenómenos delictivos, en particular debido al desconocimiento generalizado de este medio por parte de la población. En este contexto, todos los ciudadanos pueden considerarse víctimas potenciales de los fenómenos delictivos en el ámbito cibernético, no obstante, uno de los más comunes y preocupantes –y que constituye el objeto de este Trabajo de Fin de Grado– son las estafas digitales.

De acuerdo con los datos publicados por el Ministerio de Interior en su portal oficial, registran que los hechos conocidos de infracciones penales relacionadas con la cibercriminalidad a nivel nacional, alcanzaron en 2023 un total de 33.261 casos de estafas informáticas y 44.612 casos de estafas bancarias. Asimismo, se estima que para el año 2024 los ciberdelitos han experimentado un aumento de un 26%, siendo esto reflejo de una tendencia sostenida al alza de este entorno criminológico.

En relación con estos datos, la Organización de Consumidores y Usuarios (OCU) ha alertado que hay un aumento alarmante del 166% en las consultas y reclamaciones relacionadas con estafas digitales en este último periodo mencionado, principalmente referidas a la obtención de datos bancarios y realización de cargos fraudulentos, generalmente mediante técnicas de suplantación de identidad (OCU, 2025).

En esta línea, resulta fundamental prestar especial atención a la vulnerabilidad intrínseca de la población senior, siendo estos los mayores de 65 años, quienes presentan un mayor riesgo de victimización. Esta vulnerabilidad, se relaciona con la menor familiarización y competencia con el uso de herramientas para desenvolverse en el entorno digital en comparación con otros grupos poblacionales, incrementando significativamente su victimización al tener una mayor exposición a la cibercriminalidad.

Dicha situación, en conjunto con el continuo desarrollo de las tecnologías de la información y comunicación, ha propiciado un crecimiento notable en los delitos cibernéticos, en particular de las estafas digitales, cuya consumación resulta más probable cuando las víctimas carecen de habilidades digitales suficientes.

En términos cuantitativos, el Ministerio de Interior estima que las victimizaciones por cibercriminalidad en mayores de 65 años sobre estafas digitales en 2023 alcanzaban una cifra de 2.486, duplicando así el año anterior, 2022, cuya cifra era de 1.276. A partir de esta tendencia ascendente, se estima que las cifras correspondientes al año 2024 hayan seguido reflejando un aumento sostenido, reforzando la necesidad de abordar esta problemática con carácter urgente y desde un enfoque multidisciplinar.

Desde una perspectiva criminológica y en lo que se refiere a este Trabajo de Fin de Grado, se plantea la necesidad de elaborar un método de control social en el cual se forme y se facilite a este grupo poblacional de nuevas herramientas y conocimientos que les ayude en su día a día a no convertirse en víctimas de las estafas digitales.

Por otro lado, con base al autor Linares (2013) y en lo relativo a la victimización por la cibercriminalidad social, se destaca la importancia de la Teoría de las Actividades Cotidianas en el ciberespacio como marco explicativo para comprender el riesgo de victimización digital. Esta teoría, originaria de los autores Cohen y Felson (1979) ha sido adaptada por este autor para exponer cómo las rutinas tecnológicas de los usuarios incrementan la exposición a consultas delictivas, ejemplo de esto es la ausencia de mecanismos de protección o la interacción social que conlleva a la introducción de información personal. En este sentido, se considera clave los elementos que forman el acrónimo ISI (*Introduction, Self-protection, Interaction*) los cuales hacen que los autores de estos delitos cibernéticos puedan identificar qué actividades cotidianas realiza un individuo y si puede convertirse en un objetivo adecuado para llevar a cabo el ciberdelito (P. 16).

Desde esta perspectiva, esta teoría es relevante para analizar la situación de la población senior, dado que su menor conocimiento de este entorno y la falta de medidas de autoprotección los sitúan como un colectivo de alta vulnerabilidad frente a esta criminalidad emergente.

1.2. Pregunta de investigación

En el marco de los desafíos que plantea la criminalidad cibernética para los colectivos más vulnerables, especialmente la población senior, resulta pertinente formular una pregunta de investigación que oriente el desarrollo del presente Trabajo de Fin de Grado. De este modo, se pretende que el enfoque de dicha investigación sea hacia una problemática concreta y actual, analizando el contexto social y los mecanismos de protección de las estafas digitales, vinculadas a la protección de la población senior en el entorno digital.

Por ello, este proyecto se centrará en la pregunta de investigación siguiente: **¿Cómo el control social puede servir como herramienta de prevención contra las estafas para población senior en el ámbito cibernético?**

En base a la pregunta expuesta, se ha considerado fundamental analizar en profundidad los mecanismos existentes de control social aplicables al entorno digital y la capacidad de estos para reducir la vulnerabilidad de la población senior frente a las estafas en este entorno tan complejo y que está en continuo desarrollo. Esta creciente digitalización de la sociedad ha generado nuevos riesgos para este grupo de personas, quienes, debido a la brecha digital con la cual hay una desigualdad de conocimiento de las tecnologías, ha provocado en consecuencia un desconocimiento de las amenazas cibernéticas y la confianza en fuentes que no son fiables ni verificadas, haciendo que estos sean un foco sencillo de comisión de engaños digitales.

Dado que la protección del grupo de población senior en este entorno digital es una prioridad para prevenir las estafas en este ámbito, esta investigación se orienta hacia el estudio del control social, ya sea formal o informal, como estrategia para mitigar el impacto negativo, para, posteriormente, proponer un programa de prevención por medio del control social que pueda enseñar a las personas en tercera edad a identificar esas amenazadas de estafas, entre otros aspectos. En suma, se quiere ayudar a fortalecer la seguridad digital de las personas mayores y reducir su riesgo a exponerse a estas amenazas.

1.3. Objetivos

1.3.1. Objetivo general

Como objetivo general de este Trabajo de Fin de Grado, primeramente, se plantea analizar la influencia del control social como medida de prevención de las estafas digitales en la población senior, siendo estos aquellos mayores de 65 años, considerando su vulnerabilidad intrínseca, la cual se ve más presente en el entorno digital.

Para ello, se busca desarrollar un estudio desde una perspectiva criminológica que permita evaluar cómo es el papel control social en la protección de la población senior y en la prevención de las estafas digitales.

1.3.2. Objetivos específicos

Como objetivos específicos se plantean los siguientes:

- Identificar los mecanismos de control social formal e informal existentes para la prevención de estafas digitales en la población senior.
- Evaluar el marco jurídico vigente en materia de protección de la vulnerabilidad de este colectivo frente a las estafas en el entorno digital.
- Identificar las teorías criminológicas aplicables a la prevención de estafas y al control social.
- Analizar los factores de riesgo asociados a la vulnerabilidad de la población senior en materia de estafas digitales.
- Realizar una propuesta de prevención de control social que forme, capacite y conciencie a la población senior en la identificación de estafas digitales.

1.4. Justificación: La relevancia, la originalidad y la contribución científica al conocimiento académico

El presente Trabajo de Fin de Grado se justifica por la necesidad emergente de abordar, desde un enfoque académico y aplicado con perspectiva criminológica, los riesgos que plantea la acelerada digitalización para la sociedad, especialmente para la población senior, considerado un colectivo de especial vulnerabilidad. Esta viene agravada por el hecho de que las tecnologías digitales se han convertido en un medio imprescindible para el acceso a servicios públicos, financieros, sociales, sanitarios e incluso para la comunicación cotidiana, lo que sitúa a este grupo ante barreras de acceso, protección y comprensión dentro del entorno digital, incrementando su exposición de forma significativa a fenómenos delictivos con las estafas digitales.

La relevancia social de esta propuesta radica en visibilizar una problemática que es frecuentemente subestimada, pues la cibervictimización de la población senior en ocasiones queda ignorado, pero la realidad es que cada vez están más presentes en este entorno, y que no cuentan con las herramientas y conocimientos necesarios para protegerse y desenvolverse de forma segura. Frente a esta situación, se plasma la importancia de realizar un riguroso análisis criminológico que permita comprender esta problemática desde una perspectiva integral, con el fin de plantear dinámicas y herramientas para reducir la vulnerabilidad y exposición al riesgo, desde el control social.

En cuanto a la originalidad de la temática del presente trabajo, tras analizar el contexto social y jurídicos, así como los mecanismos de protección de este colectivo ante las

estafas digitales, se constata la escasez de propuestas centradas en el control social como método de prevención. Por ello, se ha considerado oportuno realizar una propuesta de prevención de control social que tiene como objetivo dotar a la población senior de conocimientos y herramientas desde una perspectiva práctica en su vida de tal manera que comprendan y apliquen medidas de autoprotección en su contacto con la tecnología.

Finalmente, en términos de contribución e impacto en el diseño de políticas preventivas, este proyecto pretende cubrir un vacío existente, desde una perspectiva criminológica, concretamente en lo referido a las estafas digitales sufridas por la población senior. Asimismo, se pretende que la propuesta plasmada de prevención basada en control social pueda, en un futuro, tener una aplicación práctica. Por esta razón, ha sido desarrollada con un enfoque aplicado, orientado a su implementación y seguimiento real, con el objetivo de demostrar la necesidad y utilidad de formar, concienciar y empoderar a la población senior.

En suma, este Trabajo Final de Grado aspira no solo a aportar conocimientos académicos, sino también a servir como base para futuras líneas de investigación y para el diseño de políticas públicas centradas en la prevención e inclusión digital de la población senior, teniendo en cuenta su especial vulnerabilidad.

2. FUNDAMENTACIÓN TEÓRICA

2.1. Revisión de la literatura científica: Marco teórico

2.1.1. El Control Social

El control social constituye uno de los elementos fundamentales de la Criminología, junto al delito, víctima y victimario. Estos cuatro pilares conforman el núcleo de estudio de esta disciplina, la cual busca comprender la conducta delictiva y las respuestas sociales frente a ella. Particularmente, el control social puede ser tanto formal como informal. Mediante ellos la sociedad regula el comportamiento delictivo y trata de mantener el orden y la cohesión.

El control social, es un pilar básico de la Criminología. Sin su presencia, resulta imposible comprender la dinámica del delito, los factores de riesgo y las formas de prevención del mismo.

2.1.1.1. Concepción

Históricamente, los conceptos de desviación y delincuencia comienzan a formar parte de la sociología a través de la Escuela de Chicago, cuyo departamento se fundó en 1892; a pesar del pensamiento eminentemente científico que se tenía en este ámbito. La gran aportación que los sociólogos hacen a la Criminología es concluir que esta se centra en el hecho de que la delincuencia es fruto de combinación de elementos, evidenciando que se debía a una falta o a una deficiencia efectiva de controles sociales morales, familiares o ambientales, entre otros.

Posteriormente, a finales de los años sesenta, se originaron las primeras teorías del control, con la implicación directa de Travis Hirschi (*Causes of Delinquency*, 1969) dando pie a investigaciones empíricas y evidenciando la necesidad del control social. A partir de entonces, es cuando se comienza a evidenciar la necesidad de estudios e investigaciones versadas sobre el control y la prevención social en la criminología (Fernández, 2017, P. 172).

Existe gran variedad de definiciones del concepto “control social”, una de ellas es la propuesta por De la Cruz Ochoa (2001) quien considera que es la “capacidad de la sociedad para regularse a sí misma de acuerdo a principios y valores aceptados mayoritariamente” (P. 04).

Por otro lado, Avilés (2010) refiere que el control social se define como aquellos mecanismos, procedimientos o muros de contención que tiene la sociedad para alinear la conducta de los miembros de ella, así como para promover y garantizar un comportamiento de los ciudadanos adecuado a los modelos y normas comunitarias (P. 06).

En suma, la implantación del control social es necesaria una vez que sale a la luz un desajuste entre la sociedad y el comportamiento del individuo, de tal manera que dicha implantación lleva consigo unos controles tanto coactivos como persuasivos para regular, orientar y disuadir la realización de conductas no deseadas o que no se adecuan a las normas sociales de una sociedad.

2.1.1.2. Tipología

Diversos autores plasman que el control social, estudiado por la Criminología, puede ser de carácter formal o informal, teniendo cada uno su propio ámbito de aplicación y sus respectivos agentes encargados de actuar en la prevención.

En lo que respecta al *control social formal,* y según lo dispuesto por Olmo (2021), se entiende como aquel ejercido por el Estado, el cual asume funciones públicas destinadas a definir, detectar, individualizar, controlar y, cuando sea necesario, suprimir aquellas conductas prohibidas. En el caso de España, el control social formal se manifiesta, por ejemplo, a través de las Fuerzas y Cuerpos de Seguridad del Estado, el sistema judicial —mediante la aplicación del Código Penal español y otras normativas— y el sistema penitenciario (P. 14).

En suma, este tipo de control social es institucionalizado, pues proviene de organismos estatales, se basa en normas legales donde se tipifican las conductas prohibidas, lo cual genera sanciones de carácter formal y se caracteriza por su enfoque objetivo, ya que no depende de las relaciones personales sino de las reglas establecidas (Masó, 2023).

Por otro lado, en lo referido al *control social informal*, como señala Vargas, (2024), sus agentes se centran en condicionar al individuo desde la infancia con las normas sociales. Este proceso comienza en los núcleos primarios de la infancia, como la familia, y continúa en el entorno académico y laboral, hasta que el individuo acepta las normas y modelos de conducta aprendidos (P. 11).

En resumen, los agentes informales son (Fernández, 201, Pp. 174-177):

La familia, siendo fundamental que los progenitores estén presentes durante el crecimiento de los hijos, mostrándoles medidas de control, adecuándose al grado de madurez que presenten.

La escuela, la cual influye notoriamente en el desarrollo personal del individuo, donde adquirirá conocimientos y patrones de conducta, así como las primeras interacciones en grupos externos al núcleo familiar. Por ello, es esencial el comportamiento del resto de los integrantes del grupo que conforme el individuo.

El entorno laboral, que sucede al ámbito escolar y tiene una gran influencia en el individuo, en la etapa final de la adolescencia y comienzo de la madurez. En este entorno se seguirán recibiendo influencias sobre las actitudes, valores y principios morales socialmente aceptados

Los medios de comunicación de masas, que funcionan como sistema de comunicación masiva de modelos de conducta, dónde aportan valores y pueden ser utilizados como adoctrinamiento. Muchos autores consideran que es un método realmente influyente sobre las conductas socialmente aceptadas.

En esta línea, Fernández (2018) menciona unos elementos clave del individuo que le vincula con la sociedad para disuadir de la realización de conductas delictivas, lo cual se consigue con la combinación de ambos controles sociales, siendo (P. 178): el apego, gracias al cual las personas no delinquen cuando aceptan las normas sociales y jurídicas adecuadas; el compromiso, siendo el sentimiento de unidad con la sociedad, lo cual hace que el individuo se comporte de manera social y moral; la participación, pues si el individuo se centra en actividades sociales, se alejará de las conductas delictivas; y, por último, las creencias, lo cual es positivo cuando el individuo acepta y comparte valores y principios que se vinculen con un comportamiento socialmente aceptable.

2.1.2. La Constitución Española de 1978 y la situación jurídica de la población senior

La Constitución Española de 1978 establece los principios fundamentales para la protección de todos los ciudadanos. Estos principios pueden extrapolarse a la hora de hacer referencia a aquello que se debe proteger en relación a la población senior, de tal manera que se garantice su dignidad y el deber de las instituciones públicas de velar por su protección integral, priorizando su bienestar e integridad.

En lo relativo a la población senior, reconoce su dignidad y el deber de las instituciones públicas de garantizar su bienestar y seguridad.

En el contexto actual de creciente digitalización y de mayor exposición a riesgos cibernéticos por parte de este grupo poblacional, surge la necesidad de analizar el marco jurídico en materia de protección de su vulnerabilidad intrínseca. Esta vulnerabilidad, entendida no solamente como consecuencia de víctimas de delitos digitales, sino como una condición de estos individuos —derivada de su proceso natural de envejecimiento, lo cual trae consigo posibles limitaciones en diversos ámbitos cotidianos—. El avance tecnológico de los últimos años ha intensificado esta situación, pues, lo que ha hecho acrecentar la brecha digital preexistente entre la población senior y otros grupos generacionales. Por todo ello, se considera imprescindible evaluar si las garantías constitucionales y legales cumplen con esta protección para cubrir adecuadamente las necesidades y riesgos.

2.1.2.1. Artículo 50 de la Constitución Española

El artículo 50 de la Constitución Española refiere que los poderes públicos tendrán que garantizar, con pensiones adecuadas y actualizadas de forma periódica, la suficiencia económica a los ciudadanos durante la tercera edad, reconociendo así un derecho económico y su protección integral.

Además de esto, el artículo exige que, sin perjuicio de las obligaciones familiares, los poderes públicos tendrán que promover su bienestar con un sistema de servicios sociales que pueda atender las necesidades de salud, vivienda, ocio y cultura que pudieran generarse. Mediante esto, se refuerza la corresponsabilidad del Estado en la protección de la población senior, evidenciando que no sólo dependen de su entorno familiar para tener una vida digna y autónoma.

En síntesis, este precepto sirve como base constitucional para el desarrollo de políticas dirigidas a la población senior teniendo en cuenta sus vulnerabilidades elaborando una intervención estatal eficaz y apropiada. No obstante, esta redacción puede resultar genérica, dando lugar a interpretaciones dispares, por lo que se plantea una concreción normativa que permita su aplicación en los contextos actuales como es la creciente digitalización y aparición de nuevos riesgos derivados de la brecha digital.

2.1.2.2. Derechos específicos

En lo que respecta a los derechos específicos de la población senior, pueden identificarse diversos reconocimientos, tanto en la Constitución Española como en normativa sectorial relativa a la dependencia, igualdad y los derechos digitales, entre otras.

Por un lado, en lo que respecta a la Constitución Española, se extrae el derecho a la seguridad jurídica y la protección contra la arbitrariedad de los poderes públicos del artículo 9.3, así como la defensa de los consumidores y usuarios, velando por su salud, intereses económicos y seguridad, recogido en el artículo 51, siendo esto relevante ante la situación de vulnerabilidad que presenta el colectivo senior debido a la brecha digital.

Asimismo, se debe hacer referencia al derecho a la dignidad del artículo 10.1 y a los derechos inviolables inherentes a la persona, siendo pilares fundamentales del orden político y de la paz social. Así como al derecho al trato respetuoso, de tal manera que no se lleven a cabo conductas discriminatorias (artículo 14) en este ámbito por razón de edad de este colectivo en lo relativo a acceso de servicios tecnológicos y financieros.

En lo referido al derecho a la información y educación digital, el artículo 20 y 27 reconocen respectivamente el derecho a recibir información veraz por los medios de difusión y el derecho a la educación, lo cual resulta extrapolable a la necesidad de la formación digital a esta población como medida de prevención frente a estafas, suplantación de identidad y otros riesgos del mundo digital.

Por otro lado, la Ley General para la Defensa de los Consumidores y Usuarios establece en sus artículos 8 y siguientes el derecho a la protección frente a prácticas comerciales engañosas y contratos abusivos, lo cual resulta de especial importancia en el entorno cibernético, pues son muchos los casos de los individuos de avanzada edad que son víctimas de estafas llevadas a cabo con medios digitales debido a la carencia de conocimiento para identificar los riesgos en este entorno.

Desde la perspectiva de asegurar el derecho a la atención digna y a la voluntad de las personas que forman parte del colectivo senior en situación de dependencia, quedan protegidos por la Ley de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia la cual pretende garantizar una vida autónoma con el apoyo adecuado, fomentando su independencia en la vida diaria.

En la línea del acceso y seguridad en el uso de medios tecnológicos, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico que vela por estos aspectos, a lo que se suma la Carta de Derechos Digitales (2021) como parte de un Plan de Recuperación, Transformación y Resiliencia, que reconoce el derecho a la educación digital y a un uso accesible y adaptado a los servicios tecnológicos de todos los ciudadanos, especialmente para colectivos vulnerables.

Desde la perspectiva del Código Penal (1995), se contempla indirectamente la protección de los derechos de la población senior por medio de la tipificación y sanción de conductas que se llevan a cabo con el beneficio de la especial vulnerabilidad o confianza, facilitando la comisión de ciertos delitos —como ocurre en muchos ciberdelitos—, aspecto el cual influye en la determinación de la pena aplicable.

Un ejemplo de ello es el artículo 22, que recoge las circunstancias agravantes, entre ellas el abuso de confianza en su apartado 6, aplicable a situaciones en las que los delincuentes se aprovechan de la confianza depositada por este colectivo en sus actividades diarias, facilitando que las estafas se consuman como desean.

Además de estas normas que incluyen de forma implícita a la población senior, existen otras específicas creadas para su protección, como la Ley de Atención y Protección a las Personas Mayores, que se centra en garantizar un sistema regulado que vele por la protección y atención necesaria para este colectivo, todo ello con la cooperación de las Administraciones Públicas, en concreto, del Departamento de la Comunidad Autónoma de Andalucía. Otro ejemplo existente es la Ley de Asistencia y Protección al Anciano del Departamento del Principado de Asturias, que engloba los derechos del mencionado grupo poblacional, creando una figura denominada “Letrado Defensor” encargada de llevar a cabo las acciones públicas necesarias con el fin de defenderlos, siempre que se requiera su intervención.

No obstante, a pesar de existir normativa específica, se ha de señalar que las leyes que protegen de forma directa a este colectivo son aún escasas, así como presentan una deficiente actualización a las necesidades actuales y riesgos emergentes. Resulta necesario un desarrollo legislativo más amplio y concreto en materias como los ciberdelitos, donde el colectivo senior se ha convertido en un objetivo por el desconocimiento tecnológico, la falta de herramientas derivado de la brecha digital y la creciente sofisticación de los mecanismos de engaño, todo ello potenciado con los avances de los sistemas de inteligencia artificial.

2.1.3. La población senior como colectivo vulnerable: el caso de las estafas

La población senior representa un colectivo de especial vulnerabilidad, condición que se ve acentuada en la vertiente digital, particularmente en lo relativo a las estafas. Factores como la brecha digital, la confianza y la dificultad para reconocer y detectar las amenazas de estas conductas fraudulentas, así como el conocimiento sobre conductas de protección les convierte en recurrentes víctimas de este fenómeno delictivo.

2.1.3.1. Las estafas

Las estafas, tipificadas en el ordenamiento jurídico español, constituyen un tipo de fraude de carácter económico que puede presentarse de muchas formas, ya sea en el ámbito financiero, en línea, telefónicas, en ventas y servicios, por medio de suplantación de identidad o mediante engaños de índole emocional o sentimental.

Generalmente, los estafadores tienden a aprovecharse de la confianza, ignorancia o urgencia de las víctimas para manipularlas. Con el auge reciente de la tecnología, las estafas han evolucionado y ahora incluyen diversas tácticas avanzadas dentro del ámbito digital.

2.1.3.1.1. Concepto

El delito de estafa en el ordenamiento jurídico español se encuentra tipificado en el Código Penal de 1995, en el Título XIII sobre los Delitos contra el patrimonio y contra el orden socioeconómico, dentro del Capítulo VI “De las defraudaciones·”; en su Sección 1º “De las estafas”, disponiendo este tipo penal desde el artículo 248 hasta el artículo 251 bis de este Código.

Se entiende como delito de estafa, conforme al artículo 248 del Código Penal, a aquel acto realizado con ánimo de lucro que tiene como fin utilizar el engaño bastante para conseguir error en otro, de tal manera que se le induzca a realizar un acto de disposición en perjuicio propio o ajeno.

Asimismo, serán castigados como reos de estafa a una pena de prisión de seis meses a tres años, teniendo en cuenta el importe defraudado y el quebranto económico que se haya causado al perjudicado, además de la relación entre el autor y la víctima, cómo los medios que se hayan utilizado para la comisión, pudiendo valorarse también otras circunstancias relevantes para valorar la gravedad de la infracción cometida.

En atención a la Sentencia del Tribunal Supremo 1474/2025 de fecha del 2 de abril de 2025, donde se definen los elementos esenciales del delito de estafa, se engloban los siguientes: el engaño bastante, el cual induzca a error a la víctima; el error provocado, a través del cual la víctima actúa con la creencia falsa generada por el engaño; un acto de disposición patrimonial, debido a que la acción de la víctima afecta a su patrimonio; un perjuicio económico, siendo este el resultado de la acción que la víctima lleva a cabo; y, por último, la intención del autor de tener un beneficio económico, esto es, el ánimo de lucro.

2.1.3.1.2. Manifestaciones en el entorno digital

Las posibles manifestaciones de las estafas en el mundo digital son diversas. A ello debemos sumar la progresiva evolución que provoca una mayor dificultad para su identificación y prevención. Los tipos más usuales de estafas digitales son: el *phishing*, el *vishing* y el *smishing*.

Rodríguez (2024) expone que el *phishing* se lleva a cabo a través de correos electrónicos fraudulentos que tienen el objetivo de simular que provienen de entidades legítimas de habitual uso de los ciudadanos, como son las entidades bancarias, administraciones públicas o tiendas frecuentadas diariamente para obtener datos personales induciendo a error a la víctima para proporcionarlos en un enlace falso. Estos datos pueden ser: contraseñas, datos personales o número de tarjetas de crédito (P. 26).

Asimismo, esta técnica puede ser realizada en varias maneras (P. 26-28): corrompiendo el sistema de nombres de dominio, haciendo que al introducir la dirección de la web que se desea consultar el servicios se convierta en la dirección en un servicios diferente al original, creando una página falsa hospedado en otro servidor bajo el control del estafador; creación de direcciones falsas que hacen que el individuo no pueda identificarlo, creyendo que está en la web seguridad del banco; por último, la utilización de formularios en emails donde por error se rellenas los datos personales haciendo que sea realmente eficaz la utilización de datos personales.

Un ejemplo típico de esta técnica sería un correo electrónico de la supuesta Tesorería General de la Seguridad Social indicando que hay un reembolso disponible, en el cual se introducen los datos bancarios y personales requeridos para poder recibirlo.

Por otro lado, Debnath et al. (2025) definen el término *vishing* como aquel método que se lleva a cabo por medio de realización de llamadas telefónicas en las que el estafador se

hace pasar por trabajadores de bancos, de entidades públicas, por familiares o incluso por autoridades del Estado. El objetivo de este método es aprovecharse de la aparente urgencia de la situación para obtener los datos deseados o dinero rápidamente (P. 279).

Ejemplo de ello es una llamada en la que se hacen pasar por una entidad bancaria mencionando que es urgente facilitar datos personales para evitar un intento de robo por un supuesto estafador, de tal manera que se da acceso a la cuenta bancaria al verdadero estafador que está detrás de la llamada telefónica.

Finalmente, patria de las modalidades más recurrentes es la denominada *smishing,* los autores Kamau & Kaburu (2022) explican que esta se basa en el envío de mensajes de texto, por teléfono móvil, donde facilitan enlaces web a páginas fraudulentas o se indican una serie de instrucciones para llevar a cabo una llamada telefónica al número del estafador. Este método también tiende a aprovechar la aparente urgencia que general en las comunicaciones, expresando que se ha de realizar las indicaciones rápidamente por algún tipo de riesgo (P. 10).

Generalmente esta técnica suele abordar temas sobre pago de multas, servicios bancarios o asuntos familiares. Un ejemplo común es un mensaje por parte de correos que explican que tienen un paquete que no puede ser entregado y que se ha de pinchar en el enlace proporcionado y rellenar los datos necesarios para recuperarlo.

Estas tipologías, aunque son distintas en su ejecución, tienen patrones comunes que ayudan a identificar posibles amenazas de estafas digitales. Estos suelen girar en torno a la urgencia, mensajes inesperados o sumisión a un supuesto riesgo si no se lleva a cabo las indicaciones recibidas.

2.1.3.2. Vulnerabilidad específica de la población senior

La población senior, considerada como tal a la población de 65 años o más, representa un colectivo de especial vulnerabilidad, más aún frente a las posibles amenazas delictivas en su día a día. No obstante, esta se ve acentuada en el entorno digital y no sólo se limita a lo físico o cognitivo, sino también a perspectivas jurídicas, sociales y psicológicas.

En el contexto digital, esta fragilidad intrínseca de este colectivo se ve aumentada debido a su escasa familiarización tecnológica haciendo que la integración en este ámbito no sea equitativa ni adaptada a sus necesidades.

En este sentido, Vilches (2024) señala que el ordenamiento penal en España reconoce esta situación de vulnerabilidad de la población senior, considerando esto como un agravante en la calificación jurídica de ciertos delitos, como ocurre en el de estafa. Por otro lado, desde el punto de vista criminológico y victimológico, esta situación convierte a este colectivo en objetivo prioritario para los ciberdelincuentes, evidenciando la urgencia de proporcionarles apropiados mecanismos de protección adaptados a sus características las exigencias de su situación de fragilidad (P. 94-96).

2.1.3.2.1. Factores de riesgo

Entre los principales factores de riesgo que influyen en la victimización de la población senior, se pueden destacar los siguientes.

Primeramente, el más determinante es la brecha digital. Como expone Noriega (2022) esta representa un factor determinante en la consumación de una estafa a través de medios informáticos, debido a que el escaso contacto con herramientas digitales y la falta de conocimientos técnicos hace que se dificulte la identificación de las amenazas digitales y se acentúe la situación de vulnerabilidad

Otro factor relevante y naturalmente asociado al envejecimiento es el deterioro cognitivo, que puede afectar a la toma de decisiones, así como a la memoria operativa y a la comprensión de la magnitud y consecuencias de compartir datos de carácter personal en el entorno digital (Arteaga et al., 2024, P. 05).

Por otro lado, también influye significativamente la alta confianza interpersonal que este grupo poblacional otorga a las figuras de autoridad o entidades que aparentan ser legítimas que se ponen en contacto con ellos. Como mencionan los autores Francia & Pilar (2019), este factor hace que sean más propensos a introducir datos derivados de técnicas de estafas digitales como el *phishing* o el *vishing* por razón del abuso de confianza que conocen los estafadores al no cuestionar la autenticidad del mensaje o llamada recibido (P. 116).

Por último, desde la perspectiva de la teoría de las actividades rutinarias, se considera esto un factor de riesgo, como expone Llinares (2013), los patrones de comportamiento predecibles por los estafadores en el entorno digital, los cuales pueden ser detectados fácilmente para llevar a cabo la planificación de la conducta, de tal manera que, tener una educación digital sobre las prácticas adecuadas es esencial en la prevención (P. 12-15). Además, esta teoría trae consigo la relevancia de la ausencia de “guardianes capaces” esto es,

que además de estos patrones, si en el entorno no hay personas que asesoren o aconsejen —actuando como factor de profesión—, se incrementa exponencialmente la exposición al riesgo (P. 16).

No obstante, todos estos factores de riesgo son susceptibles de mejora mediante una apropiada estimulación cognitiva, así como el acceso a herramientas y contenidos que conciencien e informen sobre los riesgos y manifestaciones de estas estafas digitales. Todo ello, es posible a través de programas y campañas formativas de prevención, destinadas de forma específica y adaptada a las necesidades de este grupo poblacional, de tal forma que el impacto de estos factores de riesgo experimente una reducción significativa.

2.1.3.2.2. Impacto psicológico y social

El impacto que supone sufrir una estafa digital siendo parte de la población senior va más allá del perjuicio que acarrea la pérdida económica ocasionada. Las consecuencias psicológicas resultan, en ocasiones, ser especialmente impactantes, generando sentimientos de culpa, desconfianza, ansiedad e incluso vergüenza, pues han sido sometidos a una situación de urgencia en la que han resultado ser engañados (Botero et al. 2009).

Ante esta realidad, resulta imprescindible ofrecer a este colectivo la atención y el apoyo necesarios, de tal manera que su experiencia de victimización no derive en una respuesta negativa y evasiva hacia el uso de los medios tecnológicos. Por el contrario, es fundamental que se les proporcione herramientas y conocimientos útiles para desenvolverse en este entorno con mayor seguridad. Con esto, podrán comprender que cualquiera puede ser víctima de estafa digital y que no están solos, por lo que no deben sentirse culpables ni avergonzados por haber sido engañados.

Desde la perspectiva social y en línea Colorado (2006), es de vital importancia reducir el impacto social que produce un proceso de victimización, ya que cada caso genera un problema social de fondo (P. 148). De manera extrapolable a las estafas digitales en la población senior, sufrir esta experiencia en ellos produce un impacto social negativo, llevándolos a un aislamiento voluntario del entorno digital por miedo a ser nuevamente engañados. Esto supone una desconexión a servicios esenciales, privándoles de acceso a las gestiones bancarias, servicios públicos o comunicación entre familiares siendo una barrera añadida.

En esta línea, se debe considerar como consecuencia adicional la posible victimización secundaria o revictimización, entendida como un nuevo daño hacia el individuo que ha sido víctima previamente, ocasionada por una inadecuada atención por parte de los operadores del sistema penal, instituciones médicas o trabajadores sociales. Esta forma de victimización genera en la víctima una reviviscencia del miedo y la culpa que experimentó cuando ocurrieron los hechos (Marchiori, 2017, P. 665).

Esta experiencia se considera realmente negativa en el colectivo senior, puesto que genera una desconfianza institucional, personal e incluso familiar, lo cual desincentiva la denuncia de los hechos ocurridos y la petición de ayuda. Como consecuencia, se fomenta la situación de abandono y retraimiento, además de una desconexión y desconocimiento digital, aumentando el riesgo de sufrir nuevas victimizaciones y dificultando la reparación del daño sufrido.

2.1.4. Teorías Criminológicas aplicables al control social y a la prevención de estafas

En el estudio de la Criminología, diversas han sido las teorías formuladas para explicar la delincuencia y la relación con el control social. En este caso en específico, se busca abordar el fenómeno de las estafas y poder apreciar, así como es de esencial analizar cómo los mecanismos de control pueden prevenir e influir en cómo los delincuentes justifican facilitan sus acciones delictivas.

Dentro de este marco, se plasman algunas teorías que resultan relevantes por la perspectiva que ofrecen sobre la comprensión de los factores que facilitan la comisión de delitos, en este caso se abordarán las estafas, así como los medios de control social que pueden servir para reducir su comisión.

2.1.4.1. Teoría Del Control Social de Hirschi

Esta teoría sostiene que las personas se abstienen de llevar a cabo conductas delictivas no por miedo al castigo, sino porque tienen lazos fuertes sociales que hace que los mantengan dentro de las normas sociales que se deben respetar.

Este autor considera que la desviación se lleva a cabo cuando los vínculos sociales que deberían disuadir a la persona de las conductas delictivas se vuelven débiles o inexistentes. Por ello, propone los cuatro elementos básicos del control social (Hirschi 2003, P. 08-17):

Por un lado, el *apego*, como conexión emocional con amigos, familiares o figuras de autoridad, el cual cuanto más fuerte sea, menor será la probabilidad de que la persona realice una conducta desviada.

Otro elemento es el *compromiso*, este hace referencia al grado en que una persona ha invertido en su trabajo, formación o educación, y cuanto mayor es este, mayor éxito social se podrá desarrollar generando menor probabilidad de llevar a cabo conductas desviadas.

Por otro lado, está el *involucramiento*, siendo aquella participación en actividades convencionales, como son la escuela, el centro de trabajo, actividades sociales o deportes, lo cual hace que se tenga menos tiempo para dedicar a actos delictivos.

Por último, la *creencia*, la cual hace referencia a la aceptación de valores sociales y normas, con lo cual, si una persona cree en que las leyes sostienen una moralidad, es menos probable que opte por no respetar las normas.

A través de esta teoría, Hirschi quería explicar que el delito no es causado por factores externos como la falta de recursos económicos o presión social, si no por falta de estos elementos que fortalecen unos vínculos sociales que alejan a las personas de las conductas delictivas.

En conclusión, se ha escogido esta teoría por ser aplicable en la prevención de las estafas, por medio del control social, debido a que desde esta teoría se busca fortalecer los lazos sociales de tal manera que se reduzcan las posibilidades de cometer delitos. En este caso, para prevenir que las personas se conviertan en estafadores, es fundamental potenciar esos elementos claves de control social, como la educación, promoción de valores éticos o el refuerzo de las conductas morales y sociales.

2.1.4.2. Teoría De La Neutralización de Sykes y Matza

Esta teoría se centra en sostener que los delincuentes no rechazan como tal las normas sociales, sino que desarrollan una serie de justificaciones para los actos ilícitos que llevan a cabo con el fin de aliviar la culpa generada y poder mantener la imagen de ellos mismos como individuos moralmente aceptables y correctos.

Para ello que se utilizan las llamadas “técnicas de neutralización” de tal manera que con estas racionalizan su comportamiento y minimizan la posible desaprobación social, siendo técnicas tales como (Sykes & Matza, 2008, P. 163-170):

Negación de la responsabilidad, mediante esta técnica, el delincuente no se define a sí mismo como responsable de una conducta desviada, en ocasiones considerando que los actos son fruto de un accidente sin intencionalidad alguna. En ocasiones, también se recurre a considerar que las acciones venían derivadas de unas fuerzas ajenas que eran incontrolables que le han impulsado a llevar a cabo una conducta desviada, como, por ejemplo, la falta de afecto en la infancia o de recursos económicos.

Negación del daño, esta técnica genera diversidad de interpretaciones por parte del delincuente, pues dependerá de este lo que considere como daño. Normalmente, con esta técnica el delincuente pretende justificar que a pesar de haber contradicho la ley no ha provocado ningún daño de valor, haciendo así que el juicio que realiza sobre él sea positivo, como, por ejemplo, considerar que un acto de vandalismo no es más que una “travesura” que ha generado unos daños sobre unos bienes y no sobre una vida humana.

Negación de la víctima, mediante esta técnica el delincuente busca evitar la indignación moral consigo mismo, considerando que la víctima en sí no lo era por las características del hecho cometido, debido a ello, el delincuente debía generar una forma justa de retribución o castigo, es decir, transforma a la víctima en una persona que merece sufrir un daño. Por ejemplo, una estafa a una persona de alta capacidad económica o a una persona que parecía comportarse de forma engañosa.

Condena a quien condena, con ella el delincuente traslada el foco de atención de sus actos desviados al comportamiento de aquellos que desaprueban su conducta, y esto es, los que en la sociedad se encargan de velar por la ley y hacerla cumplir. Por ejemplo, pueden considerar que todos los policías son corruptos o que los jueces condenan de manera arbitraria y no adecuada.

Apelación a lealtades superiores, esta última técnica neutraliza la conducta desviada argumentando que su conducta viene provocada por un probiótico más grande o por una causa que considera más relevante que seguir las normas sociales, y,

por lo tanto, generando en sí mismo autoaceptación moral, como por ejemplo hacerlo por el bien de la familia, siendo algo que está por encima de cumplir la ley.

Esta teoría es aplicable al control social y a la prevención de estafas porque los estafadores pueden usar las justificaciones a su conducta, de tal manera que conocerlas por parte de las autoridades y de la sociedad puede beneficiar en la identificación de comportamientos delictivos y en el desarrollo de estrategias para contrarrestar y controlar esta conducta, promoviendo una cultura de responsabilidad social.

2.1.4.3. Teoría De Las Oportunidades Delictivas de Clarke y Felson

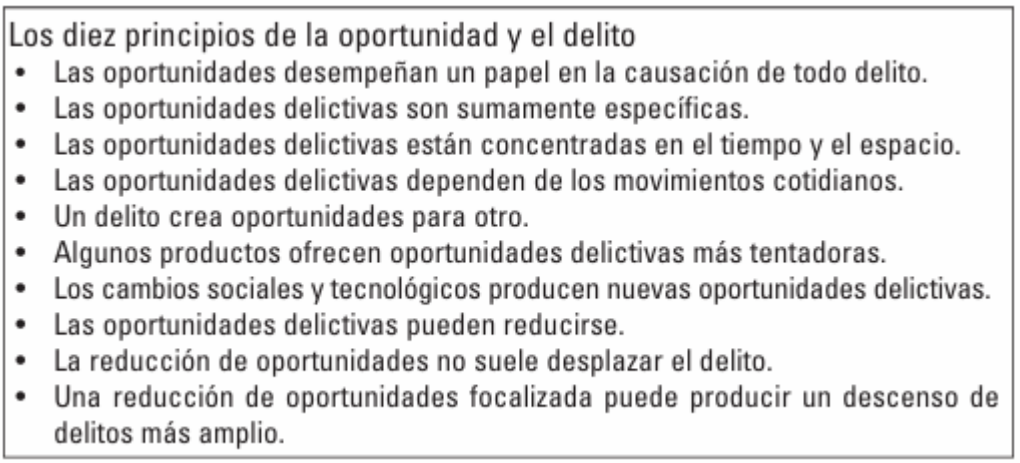
Como determinan los autores Felson & Clarke (2008) "la ocasión hace al ladrón", y esta afirmación es clave para poder comprender por qué esto es una forma de poder prevenir el delito. Tal y como es sabido por estudios criminológicos, el comportamiento individual es producto de una interacción entre la persona y el entorno, poniendo de manifiesto que los trabajos de criminólogos ambientales muestran la relevancia del escenario que rodea al individuo para crear una situación de oportunidad delictiva, siendo una condición necesaria para que el delito suceda (P. 194).

De esta teoría se extrae el llamado *patrón delictivo,* entendiendo como un componente central de la Criminología ambiental para analizar cómo es que se mueve en el tiempo y espacio los sujetos y los elementos que se involucran en un delito, lo cual también es compartido con la Teoría de las Actividades Rutinarias de Cohen y Felson[1]. Ante esto, se puede apreciar como ciertos delitos son más probables que se lleven a cabo cuando los elementos apreciados en este patrón concurren pudiendo prever la comisión de los mismos (P. 199-200).

No obstante, esta teoría no solo se basa en este patrón mencionado, si no que interrelacionan esto con los principios de oportunidad y delito, mostrando que las oportunidades del entorno desempeñan un papel clave en la causación de todos los delitos. En otras palabras, esta teoría se centra en que, de acuerdo a las características del entorno y la situación en concreto, se podrá facilitar o inhibir la conducta delictiva, lo cual dependerá de la disponibilidad de los objetivos adecuados, de la ausencia o presencia de guardianes capaces y la motivación de un sujeto a realizar una conducta desviada (P. 203).

[1] Véase apartado 2.1.4.4.

Figura 01. - *Los diez principios de la oportunidad y el delito.*



Nota. Adaptado de *La ocasión hace al ladrón. Teoría práctica para la prevención del delito,* de Felson & Clarke (2008), P. 203.

Esta teoría puede aplicarse al fenómeno delictivo de las estafas debido a que estas ocurren en un entorno que facilita que los delincuentes actúen, normalmente debido a que el perfil de víctima que se escoge hace que sea más accesible por algún tipo de vulnerabilidad, como puede ser el caso de adultos mayores que no están facilitados con la tecnología, personas que buscan soluciones rápidas por una necesidad económica y les lleva a confiar demasiado o incluso por una falta de protección o regulación de controles bancarios o de autoridades que eviten esta conducta.

2.1.4.4. Teoría De Las Actividades Rutinarias de Cohen y Felson

La presente teoría, también conocida como Teoría de las Actividades Cotidianas, es utilizada en el campo criminológico debido a que resulta de gran utilidad para analizar la victimización al favorecer la identificación de factores de riesgo que propician la probabilidad de victimización de un individuo. Estos factores determinan la victimización, esencialmente en cuanto a la interacción entre la víctima y el delito (Llinares, 2013, P. 07).

Debido a esta repetición rutinaria de ciertos comportamientos de un individuo que puede provocar que se convierta en víctima. En este sentido, la teoría de Cohen y Felson introduce el concepto de “guardián capaz”, quien, con su mera presencia, disminuye el riesgo de que se lleve a cabo un delito. Por el contrario, su ausencia potencia que esta actividad rutinaria desemboque en una situación potencial delictiva, pues el autor ve en ella una oportunidad de poder llevar a cabo una conducta delictiva (Llinares, 2013, P. 15).

Por ello, estos guardianes son elementos esenciales en la prevención situacional de un delito. En este caso se quiere hacer referencia a las estafas, pues el delincuente podrá apreciar una oportunidad criminal que genera un entorno próspero para cometer el delito. Ejemplo claro de ello es el ciberespacio, con sus características complejas e innovadoras en coincidencia con ciertos perfiles de personas, pueden crear un entorno propicio de vulnerabilidad y conseguir que se favorezca la realización de las estafas.

Para esta teoría, se considera clave estudiar los posibles factores de riesgo de los individuos para poder plantear una estrategia de prevención y protección de ellos y evitar que el delincuente aprecie una situación motivante para la comisión de un delito, como las estafas.

2.1.4.5. Teoría Del Aprendizaje Social de Bandura

Esta teoría, tal y como expone Villagómez-Cabezas et al. (2023), sostiene que las personas aprenden comportamientos por medio de la observación de los demás y repitiéndolos, sin depender de un refuerzo directo que proponían los conductistas.

Puesto que se centra en el aprendizaje por observación o modelado, se requiere un proceso de ello, y Bandura señala que son cuatro los pasos: la atención; la retención; la reproducción; y, la motivación. En otras palabras, aprenden por medio de las propias experiencias, observando a los demás.

Además de esto, se trata el término “refuerzo vicario” siendo este el que se refiere a que las personas también aprenden por ver cómo los demás son recompensadas o castigadas por el comportamiento que realizan, entendiendo así cual deben o no imitar.

Finalmente, una vez el individuo interioriza la conducta, se genera la “autoeficacia” esto es que la persona elabora la creencia de que lo correcto es persistir en la conducta aprendida por ser adecuada social y moralmente.

En conclusión, esta guarda relación con las estafas debido a que gracias a esta teoría de control social se puede conseguir educar con ejemplos reales, mostrando casos de víctimas de estafas para que las personas aprendan de sus experiencias sin caer en el engaño que crean los delincuentes. Además, en base a esta teoría, se podrían reforzar modelos de comportamiento responsable, para verificar la información y denunciar los fraudes lo antes posible, tomando precauciones.

2.1.5. El control social como estrategia preventiva de las estafas en la población senior

El control social —entendido como el conjunto de mecanismos, formales e informales, que orientan el comportamiento de los individuos en la sociedad— desempeña un papel fundamental en lo relativo a la prevención de hechos delictivos. En la línea de las estafas digitales, tiene gran implicación en la prevención de las mismas que ocurren a la población senior cada vez con más asiduidad, debido a la sofisticación de los mecanismos de amenaza y utilización de nuevas herramientas cibernéticas.

Este grupo poblacional, debido a su vulnerabilidad intrínseca derivada de su posible deterioro cognitivo, su grado de confianza o su falta de familiaridad con las tecnologías, hacen que sean unas víctimas potenciales para los estafadores, quienes encuentran en estas condiciones una oportunidad perfecta para perpetrar las estafas.

Por ello, el control social facilita herramientas fundamentales para potenciar la prevención, que junto con el acompañamiento y concienciación de la población senior, es posible reducir notoriamente este tipo de amenazas delictivas en el mundo digital.

2.1.5.1. El control social informal: participación comunitaria

En lo que respecta a la manifestación del control social informal en España, este suele apreciarse mediante participación comunitaria, siendo esencial en la prevención delictiva y cohesión social. Son diversas las iniciativas y proyectos que se han desarrollado e implementado involucrando directamente a la población, no obstante, son escasos los que involucran específicamente la prevención de fenómenos delictivos en el entorno cibernético.

No obstante, ejemplo de iniciativas específicas enfocadas a la prevención de estafas en el mundo digital a la población senior son los talleres de prevención del fraude digital que elabora Cruz Roja (2023), dónde abordan temas de protección de datos personales y cómo identificar los patrones usuales de una amenaza de fraude digital, con el objetivo de sensibilizar sobre el riesgo que supone el desconocimiento sobre las nuevas tecnologías y formas delictivas.

Asimismo, el Ayuntamiento de Albacete (2022) ha creado la campaña “Por tu seguridad, no piques” presentado por la Concejalía de Seguridad Ciudadana, con el que se busca ofrecer información a los ciudadanos para protegerse contra las estafas y fraudes digitales. Aunque enfocado a individuos de cualquier edad, inciden en la necesidad de

concienciar a la población senior debido a la rápida evolución de los nuevos métodos delictivos en el mundo digital.

Por otro lado, existen gran cantidad de iniciativas destinadas al desarrollo de herramientas y conocimientos ante situaciones de vulnerabilidad, si bien es cierto son escasas las que se enfocan en la prevención específica de las estafas digitales.

Otro ejemplo es el promovido por la Asociación de la Prensa de Málaga (2025) en colaboración con Fundación "La Caixa". Nos referimos a una serie de talleres de alfabetización mediática dónde enseñan a la población senior a manejar herramientas del entorno digital y a identificar las amenazas de bulos y estafas cibernéticas. Este proyecto ha sido de gran influencia para este colectivo poblacional debido a que se busca fomentar la autonomía y la confianza con unos hábitos de rutina digital adecuados para su protección.

2.1.5.2. El control social formal: programas de prevención

En lo referente a los mecanismos de control social formal existentes en España, este viene implementado por las Fuerzas y Cuerpos de Seguridad del Estado —Cuerpo Nacional de Policía y la Guardia Civil—, las instituciones públicas y servicios sociales, así como la legislación y regulación —Código Penal de 1995—. Mediante estos, se desarrollan campañas formativas y preventivas y se establecen marcos legales para perseguir los fenómenos delictivos.

Por un lado, es relevante mencionar el Plan de Acción Integral de Madrid sobre el Envejecimiento el cual fue adoptado durante la Segunda Asamblea Mundial sobre Envejecimiento. Este estableció una estrategia a nivel global para abordar los desafíos y oportunidades que ocasionará en envejecimiento poblacional en el siglo XXI, todo ello con el fin de garantizar que la población senior pueda desenvolverse en el mundo actual con seguridad y dignidad (Naciones Unidas, 2002). Aunque en el desarrollo de este plan específicamente no se hacía alusión al mundo digital, abrió un camino apropiado para fomentar el bienestar de esta población y creación de un entorno favorable.

Aunque son realmente escasos los planes y programas enfocados a la prevención de la ciberdelincuencia, en concreto, las estafas, más aún es aquellos dirigidos a la población senior como potenciales víctimas de estos. Entre esta reducida cantidad, se encuentra el Plan Mayor de Seguridad (PMS) el cual es una iniciativa del Cuerpo Nacional de Policía de España, la cual tiene como fin prevenir y mejorar la seguridad de la población senior por razón de ser un

colectivo vulnerable, y, aunque la temática no verse específicamente sobre la ciberdelincuencia, sí que está adaptado y su público objetivo es especialmente este grupo poblacional (Ministerio de Interior, s.f.).

Los objetivos principales de prevención y desarrollo de la seguridad de este plan se llevan a cabo por medio de charlas informativas que se impartirán en centro de mayores y asociaciones, así como por medio de la colaboración institucional a través de convenios con administraciones y entidades públicas y privadas, así como por medio de atención personalizada a los individuos que hayan sido víctimas, facilitándoles los canales de denuncia y seguimiento.

2.1.6. Propuesta desde una perspectiva criminológica: "RED SENIOR SEGURA"

A continuación, se presenta una propuesta de elaboración propia de un programa de control social para la prevención de estafas digitales en la población senior, llamado "RED SENIOR SEGURA".

Este programa ha sido diseñado como parte del presente Trabajo de Fin de Grado, con el objetivo de poder ofrecer una intervención preventiva que aborde la emergente problemática de las estafas en el entorno digital relacionadas con la población senior como colectivo vulnerable desde la perspectiva integral que permite la Criminología.

A lo largo del contenido trabajo, se desarrollan diversos apartados estructurales, como la introducción y relevancia del programa, los objetivos planteados, el público objetivo al que va dirigido, los recursos necesarios para la implementación, así como la planificación, duración y el sistema de aplicación y seguimiento.

Por otro lado, el núcleo central del programa se compone de una serie de módulos, organizados en dos bloques principales. El primero, está dirigido a criminólogos, siendo estos los que recibirán la información especializada para ponerla en conocimiento del público objetivo. El segundo, está adaptado a la población senior, con un diseño específico de contenidos accesibles y un vocabulario cuidadosamente adaptado a sus necesidades visuales y a su lenguaje, facilitando así la comprensión del material, fomentando su seguridad, confianza y autonomía en el entorno digital.

La razón de ser de esta doble estructuración radica en la necesidad de adaptar el enfoque y lenguaje del contenido, garantizando que los profesionales que impartan los

contenidos cuenten con las herramientas necesarias y que el mensaje llegue adecuadamente a la población senior.

2.1.6.1. Introducción y relevancia

La población senior —entendiendo como tal a las personas mayores de 65 años— representan un colectivo realmente afectado por la transformación digital emergente. Aunque la tecnología ha traído grandes beneficios en la actualidad, también genera nuevos retos, riesgos y amenazas, como son las estafas digitales y la sofisticación de los mecanismos para cometerlas.

En esta misma línea, este grupo poblacional, debido a factores cognitivos y emocionales, entre otros, se encuentran en una situación de especial vulnerabilidad, más aún ante las nuevas manifestaciones delictivas en el mundo digital.

Además de la vulnerabilidad intrínseca que presentan, esta se ve agravada por la brecha digital, la cual ha causado en la población senior una desigualdad en el acceso, comprensión y uso de las tecnologías, siendo un factor de riesgo esencial en la creación de una situación de alto riesgo. Esto se debe a la falta de formación digital, convirtiendo a estos individuos en un blanco fácil para los ciberdelincuentes, los cuales usan técnicas de engaño que progresivamente pasan más desapercibidas, siendo difíciles de detectar.

Ante esta situación y tras analizar los escasos mecanismos de prevención existentes en España, se ha considerado urgente y necesaria la creación de nuevas estrategias preventivas específicas, centradas en el desarrollo de técnicas y conocimientos que empoderen al colectivo, todo ello desde la perspectiva de la criminología.

En esta línea, se propone desde una perspectiva de control social, dónde la protección digital se considera un derecho vinculado a la autonomía, dignidad y seguridad de la población senior, otorgándoles —desde un enfoque cercano y adaptado— una nueva forma de protección y acompañamiento ante las posibles amenazas de estafas digitales.

2.1.6.2. Objetivos

El objetivo general es el diseño de un programa de prevención enfocado en el control social que reduzca la vulnerabilidad de la población senior frente a las estafas digitales, promoviendo la concienciación y proporcionándoles herramientas necesarias para fomentar su autonomía y seguridad en el entorno digital.

Los objetivos específicos son:

- Capacitar a los criminólogos con el contenido necesario para poder impartir el programa eficazmente.
- Promover la relevancia del control social como red comunitaria de apoyo, prevención de riesgos digitales y herramienta para la educación digital.
- Concienciar a la población senior sobre los riesgos asociados a las interacciones en el entorno digital.
- Informar sobre los métodos habituales de los estafadores por medio de la tecnología.
- Proporcionar conocimientos clave sobre el uso adecuado de las tecnologías en la vida diaria de la población senior.
- Fomentar la autonomía de la población senior, haciendo que puedan identificar por ellos mismos las amenazas de estafas y cómo reaccionar ante ellas.
- Proporcionar contenido y recursos comprensibles para este colectivo caracterizado por su especial vulnerabilidad.

2.1.6.3. Público objetivo

El público objetivo al que se destinarán las sesiones de este programa de prevención serán las personas de tercera edad, esto es, aquellas que tienen 65 años o más. Este grupo poblacional presenta unas características y necesidades específicas que requieren de una atención especializada y concreta para garantizar su calidad de vida, bienestar y protección, debido a su vulnerabilidad.

Esta vulnerabilidad, se ve agravada cuando se trata del entorno digital, debido a que la gran mayoría no ha crecido en ese entorno y pueden carecer de información necesaria para protegerse, en este caso, de las amenazas de estafas en este ámbito.

Puesto que las personas de la tercera edad suelen presentar dificultades en el uso de la tecnología, los convierte en un foco fácil para los ciberdelincuentes, es por ello por lo que se ha querido enfocar en este público objetivo para facilitar, desde una perspectiva educativa y práctica, las herramientas necesarias de concienciación, asesoramiento e identificación para fortalecer su autonomía y reducir su vulnerabilidad.

2.1.6.4. Recursos

Para la implementación de este programa, se emplearán esencialmente una serie de trípticos explicativos elaborados específicamente para esta propuesta, destinados a favorecer la comprensión y acceso a la información por parte del público objetivo.

El propósito de este recurso es plasmar y ofrecer unas pautas claras y prácticas que ayuden a identificar y denunciar las posibles amenazas de estafas en el entorno digital. Estos, estarán redactados en un lenguaje sencillo, accesible y de forma visual, con ejemplos concretos y reales que se pueden dar en el día a día. De este modo, se pretende que los usuarios puedan reconocer de una forma rápida las señales de alerta y poder actuar de la forma más segura posible.

Los títulos que tendrán los trípticos elaborados[2] serán:

- ¿Cómo protegerte en el mundo digital? Guía básica.
- Señales de alerta para detectar una estafa digital.
- Estafas digitales: lo que nunca debes compartir.
- Pasos a seguir si has caído en una estafa digital.

Para este programa, se ha considerado especialmente beneficioso se elabore un material exclusivo para el público objetivo para el que está destinado, puesto que el fin es fomentar su autonomía en relación al contacto que tienen con las tecnologías en su vida diaria. Con este material esencialmente educativo, se quiere empoderar a este grupo vulnerable, otorgándoles las herramientas necesarias para poder interactuar con los medios tecnológicos de la forma más segura posible y en confianza. En suma, si se les traslada una información clara y comprensible, se conseguirá reducir el riesgo de ser víctimas de fraudes y se fomentará la independencia.

Asimismo, se han plasmado los contenidos teóricos adaptados de los módulos destinados a la población senior en unos pósteres, facilitando así el acceso rápido y permanente siempre que se necesite. El contenido teórico que se recogerá estos pósteres será el impartido en las sesiones que conforman el proceso educativo del programa[3].

Además, se utilizarán como recurso una serie de charlas formativas dirigidas al mismo público objetivo. En ellas, se proporcionarán contenidos adaptados, de forma que los

[2] Véase apartado 7. Anexos.
[3] Este recurso queda plasmado en el apartado 7. Anexos.

asistentes puedan comprender los conceptos con facilidad. Por este motivo, los módulos han sido elaborados desde dos perspectivas: la del formador y la del asistente.

Durante las charlas, se fomentará la participación activa, la resolución de dudas en tiempo real y la creación de un espacio de confianza en el que los asistentes se sientan cómodos compartiendo sus inquietudes. Asimismo, se incluirán actividades de carácter práctico, simulaciones y ejemplos reales para identificar las estafas de forma autónoma y segura.

Este recurso, no sólo tiene un propósito informativo, sino también preventivo y empoderador, ofreciendo la autoestima digital de la población senior, ayudándoles a sentir mayor seguridad en sus interacciones diarias con el mundo digital. Con todo ello, también se velará por el apoyo mutuo y creación de redes para que compartan entre ellos los aprendizajes fuera del ámbito de las charlas, en su día a día.

2.1.6.5. Planificación y duración

Los módulos desarrollados a continuación están diseñados para ser impartidos en 5 sesiones, las cuales tendrán una duración de 90 minutos, con un descanso de 20 minutos a mitad de cada sesión.

En cada una de las sesiones se impartirán dos módulos, exceptuando la última de ellas dónde exclusivamente se harán casos prácticos y resolución de dudas que puedan surgir.

2.1.6.6. Módulos

El programa RED SENIOR SEGURA se estructura en dos bloques diferenciados de contenido. El primero, está dirigido a los profesionales encargados de impartir los contenidos, siendo estos los criminólogos. El segundo bloque está enfocado en el público objetivo: la población senior. Ambos bloques han sido diseñados con un enfoque adaptado a las características de cada uno, garantizando la correcta implementación del programa.

2.1.6.6.1. Contenido para los criminólogos

A continuación, se presentan los módulos que conforman el bloque formativo para el desarrollo del programa de prevención. Estos módulos han sido elaborados con el propósito de proporcionar a los criminólogos la base teórica y práctica necesaria desde una perspectiva profesional, que les permita comprender la problemática de las estafas digitales y, posteriormente, transmitir esta información adecuadamente al público objetivo.

2.1.6.6.1.1. Módulo 01: Introducción al mundo digital

El mundo digital es aquel conjunto de dispositivos, tecnologías y mecanismos conectados a internet con los cuales interactuamos diariamente, ejemplo de estos son los teléfonos móviles, los ordenadores, las tabletas, etcétera. Estos dispositivos, nos dan acceso a las redes sociales, las plataformas de mensajería y pago o los servicios electrónicos, entre otros muchos. En este sentido, se considera apropiado mostrar el tríptico explicativo titulado "¿Cómo protegerte del mundo digital? Guía básica".

En términos generales, el mundo digital presenta tanto beneficios como riesgos. En lo relativo a los beneficios, el más significativo es la inmediatez del acceso a la información y en la comunicación, gracias a ello, es posible el contacto con familiares y amistades, realizar gestiones bancarias, sanitarias, administrativas o efectuar compras cotidianas en cualquier momento. Asimismo, destacan la facilidad de acceso a la educación y al aprendizaje desde cualquier lugar de forma gratuita o de bajo costo, la automatización de procesos haciendo que ciertos procesos laborales o personales sean más eficientes, así como el contenido recreativo al que se puede acceder al instante desde diversidad de plataformas.

No obstante, este entorno tiene significativos riesgos y amenazas, lo cual a medida que la tecnología avanza, se vuelven más sofisticadas y difíciles de identificar y prevenir. Entre estos riesgos, se encuentra la vulneración de la privacidad y la seguridad, pues la exposición de datos de carácter personal es común cuando no se protege de manera adecuada. Esta situación puede derivar en estafas y fraudes digitales, suplantación de identidad, acceso a información de carácter personal y manipulación psicológica.

Además, se deben considerar otros fenómenos como el ciberacoso y la violencia digital, pudiendo apreciarse discursos de odio y abuso en este entorno que afectan de forma transversal a múltiples colectivos. Igualmente, es común la desinformación y la desigualdad digital, pues no todas las personas tienen el mismo acceso a la tecnología o la misma capacidad para hacer uso de ella, fomentando la brecha digital.

Desde la Criminología, resulta fundamental comprender que la familiarización limitada con el mundo digital —como es el caso del público senior al que se dirigirán— incrementa el riesgo a la exposición de las amenazas de este entorno. La falta de competencias digitales en este entorno aumenta la exposición para convertirse en víctimas de algún fenómeno de ciberdelincuencia, así como limitar la capacidad de reacción frente a las amenazas.

Por ello, se debe enfatizar durante este módulo la importancia de comprender la peligrosidad de este entorno, y todo hacerlo entender desde una perspectiva lejos del miedo y en torno al empoderamiento y la sensibilidad, de forma clara y eliminando las barreras tecnológicas que presenta este colectivo, promoviendo la comprensión y la seguridad en el uso cotidiano de las tecnologías.

2.1.6.6.1.2. Módulo 02: La población senior como colectivo vulnerable

La población senior —entendido como la población mayor de 65 años— muestra una vulnerabilidad intrínseca en todos los sentidos derivada de los cambios fisiológicos, cognitivos y sociales que experimenta el ser humano a medida que va cumpliendo años. Esto, no sólo les hace más propensos a sufrir daños emocionales o físicos, sino que también requiere una atención especializada y de unas políticas públicas adaptadas a su situación, de tal manera que les proporcionen su derecho a una vida digna y protegida.

En el contexto de las estafas digitales, dicha vulnerabilidad está presente debido a una combinación de diversos factores. Estos son la brecha digital, ya que este colectivo no ha tenido una exposición continuada a los medios tecnológicos. A esto se añade el aislamiento social, lo cual minimiza las redes de apoyo, y una cultura de confianza interpersonal que es mayor que la que se da en las generaciones más jóvenes.

Desde el punto de vista criminológico, la vulnerabilidad implica una menor capacidad para anticipar, resistir o recuperarse de una situación de victimización. En cuanto al entorno digital, esta limitación está agravada por la brecha digital, siendo este un fenómeno que manifiesta la desigualdad del acceso, utilización y entendimiento de las tecnologías de la información y de la comunicación (TIC).

En este sentido, se habla de potenciales víctimas que carecen de los conocimientos necesarios para identificar los usuales mecanismos delictivos del entorno digital y que, en ocasiones pueden no contar con las redes de apoyo que les asesoren apropiadamente. Esto genera una situación propicia para los delincuentes a la hora de llevar a cabo manipulaciones emocionales con técnicas que les inducen al miedo, como amenazas de pérdida de pensiones, o a la compasión, suplantando familiares o personas de confianza.

Esta situación derivada de la brecha digital no tiene únicamente implicaciones tecnológicas, sino que también psicológicas y sentimentales para ese grupo poblacional, pues

puede sentir miedo o desconfianza con los medios digitales de uso habitual, así como vergüenza a pedir ayuda o admitir que no comprende o que ha sido víctima de un ciberdelito.

Por todo ello, es fundamental que el criminólogo conozca y comprenda los factores de riesgos de la población senior, para que pueda intervenir formativamente con un enfoque pedagógico y adaptado, trasladando un contenido visual y sencillo de tal forma que puedan comprender por qué son un colectivo vulnerable y cómo pueden mitigar los riesgos a través del conocimiento.

2.1.6.6.1.3. Módulo 03: Las estafas digitales

Las estafas digitales, recogidas en el Código Penal español —particularmente dentro de los delitos contra el patrimonio y orden socioeconómico, en los artículos 248 y siguientes—, es uno de los fenómenos delictivos más extendido en el entorno cibernético y tiende a darse en situaciones propicias para ello, siendo fundamental las características de la víctima a la que se dirige la acción.

Los ciberdelincuentes utilizan la suplantación de identidad, el anonimato y la ingeniería social, entre otras, como herramientas eficaces que utilizarán para llevar a cabo las conductas delictivas o hacia los perfiles más vulnerables, aprovechando la menor familiarización digital y la tendencia a confiar en fuentes que aparentemente puedan parecer reales e inofensivas.

En esta línea, es fundamental que el criminólogo conozca las tipologías más frecuentes de estafas digitales dirigidas a la población senior, así como el procedimiento que se realiza, con el fin de poder analizar un mecanismo de identificación y prevención. Estas principales modalidades son:

> El *phishing*, el cual se lleva a cabo a través de correos electrónicos fraudulentos que buscan simular provenir de entidades que son legítimas y de habitual uso de los ciudadanos, como son los bancos, las administraciones públicas o tiendas que se frecuentan habitualmente por las personas. El objetivo de esta técnica es inducir a error a la víctima para que se introduzca en el enlace falso y rellene los datos personales y bancarios.
>
> Un ejemplo de esto sería un correo electrónico de la Seguridad Social indicando que hay un reembolso disponible y que se deben introducir datos personales y bancarios para poder recibirlo.

El *vishing*, este método se centra en la realización de llamadas telefónicas en las cuales el estafador se hace pasar por personal lícito, como son trabajadores de bancos, entidades públicas como ayuntamientos, fuerzas y cuerpos de seguridad del Estado e incluso por familiares. Con esta técnica se aprovechan de la urgencia de la falsa situación con el fin de obtener rápidamente información bancaria o personal, así como dinero si es posible.

Un ejemplo sería una llamada ficticia del banco en la cual avisan de la urgencia de facilitar información bancaria para evitar un supuesto intento de robo de la cuenta por un estafador.

El *smishing*, esta modalidad se basa en el envío de mensajes de texto (SMS) con enlaces a páginas fraudulentas o bien indican una serie de instrucciones que indican contactar con el número del estafador. Esta técnica también tiende a aprovecharse de la urgencia de las comunicaciones, expresando que se debe tramitar con rapidez las indicaciones por motivos de multas, bancarios o temas familiares.

Un ejemplo sería un mensaje de texto de parte de correos alegando que un paquete no ha podido ser entregado y que se deben rellenar unos datos para poder solucionarlo o un mensaje de texto de la Dirección General de Tráfico dónde se dice que hay una multa por exceso de velocidad que hay que pagar y que para ello se deben proporcionar datos personales.

Todas estas tipologías suelen ser comunes en diversos patrones, los cuales pueden ayudar a identificar una amenaza, como son la urgencia, premios inesperados, amenazas, errores ortográficos, remitentes sospechosos, etcétera. Esta repetición de esquemas ayuda a la población senior a desarrollar patrones de alerta cognitiva e identificar la posible amenaza de estafa digital.

2.1.6.6.1.4. Módulo 04: Proceso de identificación de amenaza de estafa

En el proceso de identificación de amenazas de estafas son varios los elementos clave que se deben conocer para reconocer cuando se está ante una señal de alerta que potencialmente puede acabar en una consecución de estafa.

Para la correcta exposición de este módulo, se debe mostrar a los asistentes el tríptico explicativo denominado “Señales de alerta para detectar una estafa digital.”, a partir de este

material, los criminólogos tendrán que transmitir claramente estos indicadores de forma comprensiva, visual y clara, haciendo referencia a ejemplos reales que consoliden el aprendizaje.

Los indicios más comunes para detectar una posible amenaza de estafa digital son, en primer lugar, la urgencia o presión temporal. Generalmente buscan transmitir que se trata de una situación en la que hay que actuar rápidamente y proporcionar los datos personales o bancarios inmediatamente, lo que impide a la víctima poder evaluar la situación con claridad.

Suelen incluir comentarios como "¡*Contesta ya o perderás tu oportunidad!*", "*Si no pagas de inmediato, la multa se duplicará"* o "*Si no introduces tus datos con la mayor brevedad, no podrás recuperar tu paquete"* basados siempre en un lenguaje alarmista y de urgencia extrema.

En segundo lugar, se tiende a solicitar datos de carácter personal o bancarios, como son contraseñas, cuentas bancarias, números de tarjeta o DNIs. Se debe enfatizar que ninguna entidad legítima pedirá información sensible por correos electrónicos, mensajes de texto (SMS) o llamadas telefónicas, es por esto por lo que nunca se deben facilitar esta información por este medio.

En tercer lugar, estos mensajes generalmente son inesperados o sospechosos, este tipo de comunicaciones suelen estar no previstas por la víctima, de tal manera que es una buena señal para desconfiar, sobre todo si proviene de una entidad con la que no se había contactado previamente. En estos mensajes, pueden hacerse pasar desde por familiares, instituciones, hasta empresas de contacto habitual. Algunos ejemplos de cómo pueden ser estos mensajes son:

- Suplantación de familiares: los estafadores se hacen pasar por familiares para inducir al error abusando de la preocupación. Es por esto por lo que se recomienda llamar primero a tu familiar al número de teléfono para asegurarte. Estos mensajes pueden ser de este estilo: "*Hola abuela, este es mi nuevo número. ¿Me puedes enviar dinero? Es urgente.*"; "*Hola mamá, se me ha roto el móvil. Necesito que me des dinero urgentemente*".
- Aviso de paquete no solicitado: lo cual lo recomendable es ignorar el mensaje, pues si algo pasa con el paquete, la empresa de mensajería lo hará saber de una manera fiable.

Un ejemplo de mensaje es: "*Su paquete está retenido. Pulse aquí para pagar y recibirlo"*.

- Notificación de multa falsa: con lo que pretenden simular un requerimiento para generar miedo, pero la realidad es que las multas nunca se avisan por mensaje de texto, por lo que, si se tienen dudas, se debería preguntar en la oficina oficial o a alguien de confianza. Como, por ejemplo: "*Usted tiene una multa pendiente. Pague aquí para evitar problemas*."
- Premios inesperados: los cuales suelen recibirse, aunque no se haya participado ni se esperara, este es una señal notoria de una posible estafa, pues nadie regala premios sin motivo. Un ejemplo sería: "*¡Enhorabuena! Ha ganado un premio. Para recibirlo, pulse aquí y ponga sus datos.*".

En suma, ante todos estos escenarios, es clave promover la denominada desconfianza preventiva, es decir, fomentar una actitud basada en la prudencia y la comprobación antes de dar cualquier tipo de dato confidencial. Esto se consigue desarrollando en el público objetivo un pensamiento crítico digital, de tal manera que se les invite a cuestionar lo que recibe y comprobar la veracidad de sus mensajes y llamadas telefónicas que pueden recibir en su vida diaria.

2.1.6.6.1.5. Módulo 05: Pasos a seguir en caso de ser víctima de estafa

Una vez se está inmerso en una estafa digital y eres víctima de este fenómeno delictivo, la respuesta a esta debe ser inmediata, a la vez que prudente y comprensiva. Es esencial analizar la situación con claridad, con medidas eficaces para reducir el perjuicio que pudiera ocasionar. Por ello, es indispensable que el criminólogo conozca los protocolos de actuación para poder transmitirlos con claridad y seguridad a la población senior.

A lo largo de este módulo, se deberá de utilizar el tríptico explicativo titulado "Pasos a seguir si has caído en una estafa digital", dónde se aprecia de manera esquemática y sencilla los pasos fundamentales que deben seguirse.

A continuación, se detallan las pautas a seguir en caso de ser víctima de una estafa digital, siendo los pasos fundamentales:

1. Mantener la calma y cortar el contacto con el estafador. No se deben responder más mensajes, llamadas ni seguir indicaciones del estafador, con el fin de evitar prolongar el daño que se pudiera ocasionar.
2. En el caso de que se hayan dado datos bancarios, es conveniente llamar al banco para poner en conocimiento la situación y que ellos actúen de manera inmediata y apropiada. Es probable que recomienden realizar un cambio en las claves, anulen tarjetas o bloqueen los posibles movimientos sospechosos para evitar al máximo el perjuicio económico.
3. Se recomienda denunciar a las autoridades e informar de lo sucedido para que tomen medidas legales oportunas contra los estafadores. Es importante facilitarles todo tipo de información útil para identificar al autor o autores, como capturas de pantalla, número desde el que se recibió la llamada o mensajes y correos implicados.

   Los números de contacto son: el de la Policía Nacional es el 091; el de la Guardia Civil es 062; y el de la Ayuda al Entorno Digital del Instituto Nacional de Ciberseguridad (INCIBE) es 017.
4. Por último, es positivo hablar con un familiar o allegado, para recibir apoyo emocional y confirmar que se han tomado las medidas adecuadas contra el estafador y de seguridad.

Durante la exposición de este módulo, debe ponerse énfasis en la importancia de que los criminólogos aborden la dimensión emocional, esto es, el sentimiento de vergüenza, miedo al juicio familiar o culpabilidad. Desde el punto de vista criminológico, los profesionales deben actuar con empatía y sensibilidad, trasladando al público objetivo el mensaje de que "a cualquiera le puede pasar" y que lo más importante es velar por la denuncia de estos sucesos delictivos y la prevención con herramientas de empoderamiento, dejando de lado la estigmatización.

En suma, el mensaje que debe aportar el criminólogo es que la denuncia y muestra en conocimiento es símbolo de protección y empoderamiento, incidiendo en que la prevención es una herramienta de autonomía digital y dignidad.

2.1.6.6.1.6. Módulo 06: Prácticas de seguridad digital

Este módulo se centra en las prácticas adecuadas enfocadas a la seguridad digital pues, una vez se ha puesto en conocimiento los términos básicos y los riesgos que supone, es esencial la educación en ciberseguridad como herramienta preventiva. Para la explicación de este módulo, es conveniente mostrar el tríptico explicativo denominado "Estafas digitales: lo que nunca debes compartir."

En términos generales, no se debe compartir, por ningún medio — como mensajes de texto (SMS), llamadas telefónicas o correos electrónicos— bajo ningún concepto ningún tipo de contraseña, clave o código de cuentas personales, cuentas bancarias o tarjetas de crédito o débito. Tampoco es conveniente compartir fotos de las tarjetas bancarias ni personales cuya información pueda ser utilizada fraudulentamente.

Asimismo, tampoco deben ser compartidos los datos personales confidenciales, como son el DNI, dirección física o números de teléfono, pues con estos datos se puede facilitar la suplantación de identidad, entre otros.

En esta línea, además de no compartir los datos mencionados, se consideran buenas prácticas que fomentan la seguridad digital no hacer clic en enlaces de origen desconocido o abrir archivos adjuntos en conversaciones con interlocutores que no se sabe con certeza quienes son. Además, tampoco se recomienda el acceso a redes Wi-Fi públicas que requieren un registro con datos personales.

Por último, es esencial activar la doble verificación en dos pasos, si fuera posible, para las cuentas personales, así como crear contraseñas seguras. Esto último se consigue haciendo una combinación larga, con distintas letras, números y símbolos, dejando de lado las fechas o números personales y los nombres fáciles de conocer —por ejemplo, esto sería una contraseña adecuada: "*3T8a29oau_39qFsc**"; y esto sería una contraseña insegura: "*Ana1972*"—.

Además, siempre se ha de verificar quién está detrás de cada mensaje, pudiendo hacerse fácilmente realizando una llamada de teléfono a la persona o entidad que supuestamente contacta antes de facilitar ningún tipo de información confidencial.

En conclusión, se deben instaurar pequeños hábitos sencillos de gran eficacia para velar por la seguridad digital, todo ello en el enfoque de fomentar la autonomía del uso cotidiano de las tecnologías.

2.1.6.6.1.7. Módulo 07: Taller interactivo con simulaciones

Este módulo resulta eminentemente práctico, dónde se plantean una serie de supuestos con su correspondiente resolución, los cuales los criminólogos deben exponer y orientar con el objetivo de que la población senior comprenda e interiorice el contenido de los módulos previamente trabajados.

A) CASO 01: Suplantación de un familiar.

Situación: Ana recibe un mensaje de WhatsApp de un número desconocido, el mensaje dice "*Hola abuela, he cambiado de número y necesito tu ayuda. ¿Me puedes hacer una transferencia urgente? Perdí mi cartera y no puedo pagar una multa, si espero me van a subir la cantidad, por favor abuela*."

Preguntas a los participantes: ¿Qué haríais al recibir este mensaje? ¿Creéis que hay motivos para sospechar?

Resolución: Esta situación da lugar a duda, se identifica como señal de estafa la urgencia y la petición de dinero de manera inmediata. Lo más apropiado es comprobar que la persona por la que se está haciendo pasar es en realidad esta. Para ello, se ha de realizar una llamada al número verdadero guardado en la agenda y consultarlo o consultar a otro familiar para solicitar su ayuda.

Preguntas a los participantes: En el caso de realizar el pago, ¿qué pasos deberían seguirse?

Resolución: Primero contactar con una persona de confianza para que supiera la situación y ayudase a gestionarla lo más rápido posible, seguidamente, se ha de llamar al banco para poner en conociendo la situación y que bloqueasen o cancelasen los movimientos bancarios y las tarjetas. Finalmente, llamaría a la Policía Nacional o acudiría a una comisaría de policía para denunciar los hechos.

B) CASO 02: El paquete retenido.

Situación: Jesús recibe un mensaje de texto (SMS) que dice "*Su paquete se encuentra retenido. Por favor, pulse aquí lo antes posible para pagar las tasas de entrega y recuperarlo"*.

Pregunta a los participantes: ¿Qué se debería hacer en este caso?

Resolución: Es un mensaje que pone de manifiesto la señal de alerta de estafa por la urgencia del mensaje. Lo más prudente es eliminar el mensaje y no intercambiar ningún tipo de información, pues es probable que sea un enlace de un estafador.

Pregunta a los participantes: El problema surge en que Jesús ha pedido un paquete que está esperando, por lo que duda y decide pinchar en el enlace porque cree que es el paquete de verdad. Finalmente, resulta en una estafa y le extraen 4.000 euros de la cuenta bancaria, ¿qué se debería hacer a continuación?

Resolución: Primero contactar con una persona de confianza para que supiera la situación y ayudase a gestionarla lo más rápido posible, seguidamente, se ha de llamar al banco para poner en conociendo la situación y que bloqueasen o cancelasen los movimientos bancarios y las tarjetas. Finalmente, llamaría a la Policía Nacional o acudiría a una comisaría de policía para denunciar los hechos.

C) CASO 03: Una multa urgente.

Situación: Carmen recibe una llamada de una supuesta trabajadora de la Dirección General de Tráfico. En esta llamada, le informan de que tiene una multa sin pagar y le indica que, si no lo hace en ese momento, se duplicará el importe de la misma. Le comenta que para realizarlos basta con tener los datos de la tarjeta bancaria para realizar el pago en ese instante.

Pregunta a los participantes: ¿Qué se debería hacer en esta situación? ¿Creéis que pagan las multas de esta manera?

Resolución: Las multas nunca se cobrarán ni se pondrán en conocimiento a través de una llamada telefónica, y mucho menos se pedirán los datos bancarios por ese medio. En ese instante, es recomendable terminar la llamada y no dar ningún tipo de datos, seguidamente se ha de bloquear el número de teléfono. Tras esto, si duda de si tienes alguna multa, puedes contactar directamente con la institución o ir a una oficina a preguntar directamente.

D) CASO 04: El premio inesperado.

Situación: Roberto recibe un correo electrónico por tercera vez en la semana, dónde le indican "*¡Enhorabuena, has ganado un premio valorado en 1.500 euros con el que podrás comprar cualquier objeto de nuestra web! Rellene este formulario con los datos de cuenta bancaria y personales y le transferiremos la cantidad ganada. Date prisa o perderás este premio"* Ante esto, Roberto duda y prefiere no hacer caso, pues él no ha participado en ningún concurso.

Pregunta a los participantes: ¿Hay algo que os haga sospechar que es una estafa? ¿Cómo gestionaríais esta situación?

Resolución: Nunca se debe confiar en un premio que no ha sido solicitado pues nadie regala nada sin ningún motivo. Además, nunca se deben compartir datos bancarios ni personales por ese medio, por lo que es evidente que se está ante una posible estafa digital. Lo más prudente es eliminar el mensaje y bloquear el remitente.

Pregunta a los participantes: En el caso de que Roberto hubiera pinchado el enlace y rellenado los datos, estaría su cuenta bancaria en peligro de sufrir un perjuicio económico ¿cómo se debería afrontar la situación?

Resolución: Primero contactar con una persona de confianza para que supiera la situación y ayudase a gestionarla lo más rápido posible, seguidamente, se ha de llamar al banco para poner en conociendo la situación y que bloqueasen o cancelasen los movimientos bancarios y las tarjetas. Finalmente, llamaría a la Policía Nacional o acudiría a una comisaría de policía para denunciar los hechos.

E) CASO 05: Juego de roles.

En esta dinámica, se busca posicionar a los asistentes en una situación de amenaza de estafa digital, donde un criminólogo se hará pasar por un estafador para que el público practique en el proceso de identificación y reacción ante esta situación, de tal manera que se pongan en práctica las herramientas expuestas.

Esta actividad debe ser realizada en un ambiente de confianza y comprensión, dónde el error no sea motivo de vergüenza sino de aprendizaje, reforzando la seguridad emocional de los participantes y destacando los aciertos que tengan durante el desarrollo del taller práctico. El criminólogo que esté impartiendo deberá fomentar la participación activa para que se lleve a cabo un aprendizaje de la forma más consolidada posible.

2.1.6.6.2. Contenido para el público objetivo

A continuación, se presentan los módulos que conforman el bloque formativo destinado a la población senior en cuanto al apropiado desarrollo del programa de prevención. Estos módulos han sido elaborados con el propósito de proporcionar al público objetivo un contenido esquemático y comprensible sobre los temas que recibirán por parte de los profesionales en las sesiones.

La finalidad de estos es que puedan consultar el material cuando lo deseen y puedan encontrar la información de la manera más accesible y clara posible. Asimismo, tendrán acceso a los trípticos explicativos diseñados específicamente para reforzar su aprendizaje y teniendo en cuenta sus capacidades cognitivas.

2.1.6.6.2.1. Módulo 01: Empezando con el mundo digital

Hoy en día se vive rodeado de medios tecnológicos, como son los teléfonos, ordenadores, tabletas, entre otros. Estos permiten que interactuemos y nos comuniquemos con familiares, ver noticias, hacer compras, pedir citas o consultar el banco, entre otras muchas posibilidades. Esto es lo que se llama mundo digital, y tiene tanto ventajas como riesgos:

- Aspectos buenos: la comunicación con familiares y personas de confianza, comodidad para el acceso a información y facilidad de acceder a servicios.
- Aspectos peligrosos: el riesgo de estafas, robo de información personal o engaños si no tenemos cuidado.

Por ello, es aconsejable aprender poco a poco las maneras de actuar y navegar por internet de forma segura, de tal manera que podamos protegernos ante las posibles amenazas de estafas. Para comprender mejor este contenido, es aconsejable consultar el tríptico explicativo titulado "¿Cómo protegerte del mundo digital? Guía básica".

2.1.6.6.2.2. Módulo 02: ¿Por qué debéis protegeros?

El riesgo de convertirnos en víctima de una estafa digital será mayor o menor según el conocimiento que se tenga sobre las tecnologías. A menor costumbre de utilización de los medios tecnológicos, a más fácil será cometer un error y caer en la trampa de un estafador.

Por esto, es recomendable conocer bien cómo funcionan estos objetos tecnológicos, así como tener apoyo y no confiar tan fácilmente en los desconocidos. Además, se recomienda dejar de lado el miedo a preguntar si algo no se entiende, nadie nace sabiendo y es bueno comentarlo con alguien de confianza para orientarte en cómo es mejor que se realicen ciertas acciones relacionadas con el uso del internet y la tecnología.

2.1.6.6.2.3. Módulo 03: Cuidado con los engaños en internet

Las estafas digitales son aquellas que afectarán directamente a tu cuenta bancaria, causando un perjuicio económico en aquellos que han sido víctimas.

Para poder identificarlas, es importante conocer de qué maneras se pueden realizar, teniendo en cuenta que los delincuentes, generalmente, actúan escondiendo quiénes son y utilizando datos de los demás para hacerse pasar por ellos. Estas posibilidades son:

- Las estafas que se llevan a cabo a través de correos electrónicos, que buscan hacerse pasar por entidades o servicios que se conocen, como pueden ser los bancos o las tiendas que se frecuentan de forma habitual. Suelen intentar que se entre en un enlace falso y rellenar datos personales, como, por ejemplo, un mensaje sobre un cobro pendiente de la Seguridad Social.
- Las estafas que se llevan a cabo a través de llamadas telefónicas, donde el estafador se hace pasar por una persona que parece ser real. Un ejemplo es una llamada ficticia del banco, dónde piden una serie de datos para solucionar un problema que no existe en realidad.
- Las estafas que se llevan a cabo con mensajes de texto (SMS), los cuales envían enlaces que llevan a rellenar datos personales, como por ejemplo para el pago de multas o enviar dinero a familiares que en realidad no lo son.

En conclusión, si algún mensaje o llamada no se esperaba o se duda, es recomendable borrar el mensaje o colgar el teléfono, si es algo importante, lo harán saber de una forma distinta.

2.1.6.6.2.4. Módulo 04: ¿Cómo reconocer una estafa digital?

Este módulo es muy importante, pues la prevención de las estafas se consigue gracias a la identificación de señales de alerta. Ejemplo de estas son:

- La urgencia o rapidez para realizar lo que te piden, con mensajes como *¡Contesta ya o perderás la oportunidad!* o "*Si no pagas de inmediato, la multa se duplicará"*.

- La petición de datos personales, como DNI o dirección, así como datos relacionados con la cuenta bancaria.
- Mensajes sospechosos o que no se esperaban.
- En ocasiones, para parecer reales pueden hacerse pasar por familiares pidiendo ayuda de alguna manera para conseguir un ingreso de dinero. Por ejemplo, con un mensaje como: "*Hola abuela, soy tu nieto. Envíame dinero por favor, es importante, luego te lo explico.*"
- Otras formas son, el envío de un mensaje que hable sobre un paquete que no puede llegar a la dirección de la vivienda o también la notificación de premios inesperados o multas desconocidas.

Sobre estas señales, lo más importante es consultar con alguien de confianza antes de responder. Estos contenidos se aprecian de una forma más clara en el tríptico explicativo denominado "Señales de alerta para detectar una estafa digital." el cual se recomienda consultar para terminar de comprender el contenido del módulo.

2.1.6.6.2.5. Módulo 05: ¿Qué hacer si te intentan estafar o ya lo han hecho?

En el caso de creer que eres víctima de una estafa, deberíamos seguir unos sencillos pasos, los cuales están en el tríptico explicativo titulado "Pasos a seguir si has caído en una estafa digital", siendo los siguientes:

1. Mantener la calma y no contestar más al estafador.
2. Llamar a tu banco para bloquear tarjetas o movimientos.
3. Denunciar lo ocurrido, siendo números de teléfono importantes los siguientes:
    - Policía Nacional: 091.
    - Guardia Civil: 062.
    - Ayuda Ciberseguridad (INCIBE): 017.
4. Contar lo ocurrido a alguien de confianza, como un familiar, para que de su apoyo y ayude a comprobar que está todo bien.

Ante todo, en ningún momento deberías sentirte culpable, pues cualquiera puede ser víctima de una estafa digital.

2.1.6.6.2.6. Módulo 06: Consejos para estar seguro en internet

En cuanto a los consejos que se deben seguir para estar protegidos de los riesgos de sufrir una estafa en internet, se tiene que saber que no se deben compartir nunca los siguientes datos:

- Por ningún medio, como mensajes de texto (SMS), llamadas telefónicas o correos electrónicos, contraseñas, códigos de cuentas bancarias o tarjetas de crédito o débito.
- Fotos de las tarjetas bancarias ni personales, pues esa información puede utilizarse también.
- Datos personales, como son el DNI, dirección física o números de teléfono, pues con estos datos se pueden hacer pasar por nosotros con facilidad.

En cuanto los comportamientos adecuados, se recomienda:

- No meterse en enlaces de origen desconocido o abrir archivos enviados por conversaciones con quien no se sabe quiénes son.
- Crear contraseñas difíciles de descifrar, haciendo una combinación larga, con distintas letras, números y símbolos, dejando de lado las fechas o números personales y los nombres fáciles de conocer —por ejemplo, esto sería una contraseña adecuada: "*3T8a29oau_39qFsc**"; y esto sería una contraseña insegura: "*Ana1972*"—.
- Comprobar quién está detrás de cada mensaje, realizando una llamada de teléfono a la persona o entidad con la que se cree que se está hablando.

Todos estos puntos se encuentran de una forma más clara y visual en el tríptico explicativo denominado "Estafas digitales: lo que nunca debes compartir."

2.1.6.6.2.7. Módulo 07: Taller práctico con ejemplos reales

En este taller, se van a explicar una serie de situaciones reales que practicaremos juntos como identificar los engaños y reaccionar bien. Estos son los casos que veremos:

A) CASO 01: Nieto pidiendo dinero.

Ana recibe un mensaje de un número desconocido que dice "*Hola abuela, he cambiado de número y necesito tu ayuda. ¿Me puedes hacer una transferencia urgente? Perdí mi cartera y no puedo pagar una multa, si espero me van a subir la cantidad, por favor abuela*."

Preguntas: ¿Qué haríais al recibir este mensaje? ¿Creéis que hay motivos para sospechar? En el caso de realizar el pago, ¿qué pasos deberían seguirse?

B) CASO 02: Mensaje de falso paquete.

Jesús recibe un mensaje de texto (SMS) que dice "*Su paquete se encuentra retenido. Por favor, pulse aquí lo antes posible para pagar las tasas de entrega y recuperarlo"*.

Pregunta: ¿Qué se debería hacer en este caso?

El problema surge en que Jesús ha pedido un paquete que está esperando, por lo que duda y decide pinchar en el enlace porque cree que es el paquete de verdad. Finalmente, resulta en una estafa y le extraen 4.000 euros de la cuenta bancaria, ¿qué se debería hacer a continuación?

C) CASO 03: Llamada con una multa falsa.

Carmen recibe una llamada de una trabajadora de la Dirección General de Tráfico. En esta llamada, le informan que tiene una multa sin pagar y le indica que, si no lo hace en ese momento, tendrá que pagar más. Le explican que es tan fácil como que le de los datos de la tarjeta bancaria para realizar el pago en ese instante.

Pregunta: ¿Qué se debería hacer en esta situación? ¿Creéis que pagan las multas de esta manera?

D) CASO 04: Correo con un premio que no pidió.

Roberto recibe un correo electrónico por tercera vez en la semana, dónde le indican "*¡Enhorabuena, has ganado un premio valorado en 1.500 euros con el que podrás comprar cualquier objeto de nuestra web! Rellene este formulario con los datos de cuenta bancaria y personales y le transferiremos la cantidad ganada. Date prisa o perderás este premio"* Ante esto, Roberto duda y prefiere no hacer caso, pues él no ha participado en ningún concurso.

Pregunta: ¿Hay algo que os haga sospechar que es una estafa? ¿Cómo gestionaríais esta situación?

En el caso de que Roberto hubiera pinchado el enlace y rellenado los datos, estaría su cuenta bancaria en peligro ¿qué debería hacer?

2.1.6.6.3. Aplicación y seguimiento

En términos generales, en lo que respecta a la aplicación y seguimiento, este programa se implementará por medio de charlas educativas y distribución de trípticos informativos, de tal manera que se pueda dotar al público objetivo de herramientas prácticas y visuales para prevenir las estafas digitales.

Para la aplicación, es conveniente por un lado que las charlas sean de forma presencial, impartiendo sesiones didácticas por personal Graduado en Criminología, usando un lenguaje claro y con ejemplos lo más reales posibles. Estas, se realizarán en espacios comunitarios, residencias de ancianos, asociaciones u otras instituciones afines que cuenten con este público objetivo.

Por otro lado, se distribuirán entre los participantes acceso a trípticos explicativos con información clave y visual sobre la identificación y prevención de los fraudes digitales, para que puedan consultarlos siempre que lo necesiten.

Las charlas, siendo un elemento básico de la aplicación, requerirán que tengan un enfoque práctico para poder apreciar cómo es que se han integrado los conocimientos, así como puesta en práctica del uso de los trípticos elaborados. Además, se debe fomentar un espacio de consulta y de resolución de dudas, de tal manera que puedan interactuar y reforzar el aprendizaje.

Desde la perspectiva del seguimiento y evaluación, sería conveniente poder tener una retroalimentación institucional, es decir, obtener feedback desde los centros, asociaciones o instituciones en las que se han desarrollado las sesiones, pudiendo obtener información de periodos posteriores acerca de la efectividad y utilidad de los contenidos impartidos, así como del material facilitado.

Además, sería de gran interés realizar un monitoreo a mediano plazo, considerándose el periodo apropiado 1 año tras impartir las sesiones del programa al completo, realizando de nuevo visitas a los mismos lugares donde se impartieron las sesiones, con el objetivo de apreciar, de forma directa por parte del personal cualificado que desempeña las charlas cómo son los avances y la influencia de la aplicación del programa, pudiendo así reforzar contenidos y resolver nuevas dudas sobre la temática.

Asimismo, es conveniente analizar la percepción de los participantes sobre la utilidad y los métodos didácticos empleados, identificando si se ha logrado una comprensión óptima para interiorizar estrategias de prevención para su vida diaria.

Por último, dado que las estafas digitales están en continua evolución por razón del entorno cibernético, se han de revisar y actualizar periódicamente los contenidos que engloban el programa, así como los materiales informativos para poder estar de acuerdo con su vigencia y manifestación en dicho entorno.

2.2. Formulación de hipótesis: Resultados esperados

La hipótesis del presente Trabajo de Fin de Grado consiste en analizar la pregunta propuesta anteriormente: ¿Cómo el control social puede servir como herramienta de prevención contra las estafas para población senior en el ámbito cibernético?[4]

Partiendo de esta premisa, se plantea que el control social, desempeña un factor de protección fundamental ante la cibervictimización de la población senior, pues mediante este, se puede conseguir reforzar comportamientos de seguridad e información sobre el riesgo del mundo digital en lo referido a las estafas.

En consonancia con esta hipótesis, se esperan los siguientes resultados:

La identificación de una relación directa entre la vulnerabilidad de la población senior y los riesgos en el entorno, debido a su limitado contacto con las tecnologías de la información y la comunicación, de modo que son propensos a convertirse en víctimas de las estafas digitales.

La evidencia de la influencia del control social en la prevención de estafas digitales, todo ello mediante el aprendizaje experiencial, el acceso a información clara y adaptada, así como el apoyo intergeneracional para el uso cotidiano de las tecnologías.

La manifiesta escasa elaboración e implementación de programas en materia de control social como forma de prevención de las estafas digitales siendo víctimas la población senior, pese al potencial preventivo que presenta.

La elaboración de una propuesta de programa de prevención de las estafas digitales en este grupo poblacional en el marco del control social. Esta propuesta se

[4] Véase apartado 1.2.

fundamenta en la educación digital básica, el desarrollo de espacios de interacción entre las generaciones de tal manera que se apoyen y el refuerzo del papel de la familia y la comunidad como agentes protectores y de ayuda ante una estafa digital o una amenaza de ella.

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Metodología

El presente Trabajo de Fin de Grado, titulado "RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior", se ha desarrollado a través de una investigación por un método cualitativo recopilando información para evaluar y analizar datos no numéricos.

En la elaboración del presente marco teórico se ha empleado una metodología basada en la revisión bibliográfica, la cual se trata de recopilar y analizar una amplia cantidad de información relacionada con la temática escogida. Entre los materiales utilizados se incluyen manuales, informes, artículos o revistas científicas de áreas como Sociología, Psicología, Criminología, entre otras.

A partir de esa información, se ha diseñado un programa de control social de prevención de estafas digitales, con sus correspondientes módulos y método de aplicación y seguimiento.

Con el fin de garantizar la fiabilidad y adecuación de la información obtenida, se han utilizado fuentes contrastadas que contienen los recursos necesarios para poder elaborar un análisis completo. Para ello, se han usado plataformas académicas como Google Scholar, Dialnet o Scielo, además de manuales y libros, lo cual todo queda plasmado debidamente mediante las normas APA 7ª ed. en las referencias bibliográficas[5].

Además, se ha llevado a cabo un análisis de la legislación vigente en materia de estafas, como es el Código Penal, así como de normativas relacionadas con la protección integral a las personas que forman parte del grupo de población senior.

[5] Véase apartado 6.

Asimismo, se han revisado las páginas webs oficiales del Ministerio de Interior de España con el propósito de consultar los diversos programas existentes en materia de protección de personas en tercera edad como víctimas de posibles fenómenos delictivos.

Por último, con el objetivo de desarrollar una serie de trípticos explicativos con el contenido teórico de los módulos planteados del programa denominado "RED SENIOR SEGURA", se han usado programas de diseño gráfico como Illustrator, que requieren el uso de una tableta gráfica, con el fin de poder elaborarlos de una manera adecuada y obtener un resultado óptimo y deseado.

3.2. Consideraciones éticas

El presente Trabajo de Fin de Grado se ha desarrollado respetando los principios éticos fundamentales que deben regir tanto la actividad académica como cualquier propuesta de intervención social criminológica. En primer lugar, en lo que al entorno académico se refiere, se ha garantizado el respeto a la propiedad intelectual, los derechos de autor, los derechos humanos y el compromiso con la veracidad de la información plasmada en conformidad con la objetividad del análisis de las fuentes utilizadas.

Por otra parte, dado que en este proyecto se propone un programa de prevención basado en el control social dirigido a un colectivo vulnerable como es la población senior, se ha puesto especial atención a la protección de su dignidad, autonomía e integridad.

La propuesta del programa denominado "RED SEGURA SENIOR" ha sido diseñada desde una perspectiva inclusiva, orientada a proporcionar herramientas y conocimientos prácticos con el objetivo de empoderar a este colectivo y fortalecer su autonomía frente a las estafas digitales. En esta línea, se busca fomentar la participación activa, respetando sus capacidades y velando por una promoción de bienestar tanto digital como social.

Asimismo, se ha garantizado que todos los materiales –tanto los contenidos teóricos de las charlas formativas como los trípticos explicativos– respeten la accesibilidad cognitiva, comunicativa y tecnológica del público objetivo, utilizando un lenguaje claro, no discriminatorio y adaptado a sus necesidades, todo ello plasmado con un formato esquemático y visual que facilite al máximo la comprensión.

Estas consideraciones éticas van en consonancia con la Agenda 2023 de las Naciones Unidas, en cuanto a los Objetivos de Desarrollo Sostenible[6], en concreto los siguientes:

[6] También conocidos como ODS.

En primer lugar, el número 3 “Salud y bienestar”, pues es lo que precisamente se busca mediante la prevención de estafas digitales y la reducción de los perjuicios psicológicos que pudieran causar estas en este colectivo vulnerable.

En segundo lugar, el número 4 “Educación de calidad”, ya que a través de la implementación del programa elaborado se busca favorecer el conocimiento sobre el entorno digital y la autonomía de la población senior.

En tercer lugar, el número 10 “Reducción de las Desigualdades”, debido a que se busca facilitar el acceso equitativo a información y herramientas para desenvolverse en el mundo cibernético, cerrando lo máximo posible la brecha tecnológica que afecta a este grupo poblacional en cuanto a las estafas digitales.

En cuarto lugar, el número 16 “Paz, Justicia e Instituciones Sólidas”, este objetivo se relaciona con la promoción de entornos digitales que sean seguros, colaborando con las instituciones para proteger los derechos fundamentales que pueden verse afectados con el entorno digital de las personas que forman parte de este grupo poblacional.

Por último, el número 17 “Alianza para Lograr los Objetivos”, es fundamental para poder implementar estrategias de prevención eficaces y sostenibles en el tiempo como es la propuesta presentada. Todo ello en línea con la cooperación entre profesionales, entidades sociales y la población en su conjunto.

En suma, todo el procedimiento de elaboración del presente Trabajo de Fin de Grado ha sido guiado por un firme compromiso ético, asegurando la protección de la población senior y el respeto por los riesgos implícitos de su característica vulnerabilidad.

4. ANÁLISIS DE LOS RESULTADOS

Los resultados obtenidos tras el desarrollo del presente Trabajo de Fin de Grado y los que se esperan obtener tras la posible implementación del programa de prevención de control social elaborado, permitirían constatar, en primer lugar, en lo que respecta a la pregunta de investigación, que efectivamente el control social conforma un factor de prevención realmente influyente ante los fenómenos delictivos. En consecuencia, también para aquellos que ocurren en el entorno cibernético, concretamente las estafas digitales, constatando la necesidad de una apropiada educación digital para la población senior. De esta forma, se

consigue un control cercano que contribuya a conocer los riesgos y reforzar conductas seguras en el entorno digital y los medios tecnológicos cotidianos.

En cuanto a la hipótesis de la vinculación de la vulnerabilidad de la población senior con la delincuencia en el entorno digital, derivando en ello una propensión a sufrir estafas en este mundo; se confirma esta correlación en virtud de elementos como la brecha digital, el desconocimiento de los medios tecnológicos y la predisposición a confiar en situaciones aparentemente legítimas. Todo ello, así como el estudio de los factores de riesgo y de protección que se ha realizado durante el transcurso del Grado en Criminología, nos lleva a pensar que con toda probabilidad se confirmaría la hipótesis relativa a la fragilidad tecnológica, como factor de riesgo, y que esta será clave en términos de victimización en este grupo poblacional.

Por otro lado, en lo relativo a la hipótesis de la efectividad del control social en la prevención de estafas digitales, los resultados apuntan que la participación comunitaria, el apoyo entre generaciones y la transmisión de conocimientos clave sobre las conductas de autoprotección digital, constituyen factores de prevención altamente eficaces. Estas dinámicas pretenden favorecer a que la población senior tenga mayor concienciación frente a las señales de alerta de estafas digitales, promoviendo que cuestionen las situaciones sospechosas y eviten la comunicación de información personal en medios electrónicos lo cual se espera que sea uno de los resultados más positivos de la implementación del programa propuesto.

Asimismo, en lo que respecta a los recursos y la elaboración de programas en el contexto actual, tras realizar un exhaustivo análisis, se comprueba que no existen específicamente planes preventivos sobre control social en materia de estafas digitales en las que la víctima es un individuo senior. Las iniciativas identificadas resultan ser puntuales y realmente generales, sin estar enfocadas de forma concreta y adaptada a este grupo poblacional. Ante esto, se pone de manifiesto la urgente necesidad de desarrollar programas preventivos que integren el enfoque de la vulnerabilidad intrínseca de este colectivo, considerando sus características emocionales, cognitivas y tecnológicas, más aún ante la emergente sofisticación de las herramientas para consumar las estafas cibernéticas.

Finalmente, en respuesta de esta necesidad y conforme a la última hipótesis planteada, se ha conseguido diseñar un programa de intervención, denominado “RED SENIOR SEGURA”. Este, está basado en la educación digital y la elaboración tanto de contenidos

como de recursos adaptados a la población senior, con el objetivo de concienciar y educar en materia de identificación de estafas digitales, prevención y forma de actuar en caso de ser víctima. Este programa refuerza el potencial del control social, así como la necesidad de un programa adaptado a sus necesidades, características cognitivas y su limitado contacto con el entorno digital, fomentando una herramienta preventiva realmente efectiva.

5. CONCLUSIONES

5.1. Amplitud y limitaciones de la investigación

El presente Trabajo de Fin de Grado, ha permitido desarrollar un análisis eminentemente criminológico centrado en las características de la población senior en lo relativo al entorno digital. Este colectivo, atendiendo a su limitado y reciente contacto con la tecnología, junto a otros factores, ha desencadenado una situación de riesgo haciendo que sean un potencial objetivo para la comisión de estafas en el mundo digital. A partir de esta valoración, se ha planteado así, en base a esta teoría, la propuesta interventiva de prevención "RED SENIOR SEGURA".

La amplitud de este trabajo, concretamente del análisis realizado sobre contenidos criminológicos, la normativa vigente en materia de protección de derechos, el impacto de las estafas en este grupo poblacional y del programa elaborado, ha permitido ofrecer una visión de empatía y adaptación, como principios generales. Esto ha permitido apreciar qué factores de riesgo son los más frecuentes, así como la importancia de la brecha digital como potenciador de la vulnerabilidad y la necesidad de herramientas accesibles para fomentar el adecuado contacto con las tecnologías, por medio de buenas prácticas de uso de las mismas.

En esta línea, se ha buscado conseguir un impacto en el futuro, una proyección real, con la intención de que todo lo realizado pueda utilizarse, dado que ha sido elaborado para el uso práctico.

Sin embargo, también se han identificado limitaciones, entre ellas la imposibilidad de una apreciación de los resultados derivados de la aplicación del programa, puesto que, por falta de tiempo y la complejidad de los trámites necesarios para la puesta en marcha, no ha sido posible realizar un estudio de la efectividad de esta propuesta, sino que solamente se han podido estimar los posibles resultados esperados.

Asimismo, en lo relativo a los datos e información, ha sido limitante haber tenido acceso a escasa información en el ámbito académico o en páginas de instituciones oficiales, datos cualitativos o cuantitativos en cuanto a la victimización de la población senior. Esta carencia es aún mayor en cuanto a las estafas digitales, lo cual limita la elaboración de un análisis estadístico en aras de desarrollar políticas de prevención o de actuación, es por ello que esta manifiesta falta de validación empírica supone una falta de conocimiento de la realidad.

5.2. Futuras líneas de investigación

Tras el trabajo realizado, surgen potenciales líneas de investigación de utilidad para profundizar y enriquecer el abordaje de la cibervictimización de la población senior. En este sentido, la principal proyección es la implementación futura del programa "RED SENIOR SEGURA" en colaboración con organismos públicos españoles, con el objetivo de reforzar así el compromiso ético y preventivo por medio de técnicas de control social, como uno de los pilares esenciales de la Criminología, reduciendo así el impacto de las estafas digitales. En esta línea, se permitiría que el programa tuviera no sólo una visión teórica, sino también práctica, pudiendo explotar el objetivo con el que se diseñó, el cual es servir como herramienta útil, transformadora y empoderadora de la autonomía de la población senior. En este sentido, creemos que el mejor punto de partida son los Ayuntamientos debido, en primer lugar, a la cercanía con el ciudadano y, en segundo lugar, al hecho de que tienen competencias para poder implementar en sus municipios, de forma autonómica, programas como "RED SENIOR SEGURA", lo cual podría ayudar en la implantación a corto o a medio plazo.

En paralelo, resulta esencial registrar exhaustivamente las necesidades, percepciones y/o experiencias de este grupo poblacional respecto del uso de las tecnologías, pudiendo incidir y ajustar las actuaciones en sus necesidades y en aquellos factores de riesgo más relevantes, más aún ante la constante evolución tecnológica.

Por otro lado, también se considera de interés realizar una comparativa de iniciativas y programas existentes en esta temática en el entorno internacional, de tal forma que los organismos públicos españoles se puedan enriquecer de los diseños de políticas y proyectos para considerarlo en futuras propuestas a nivel nacional.

Si bien el presente trabajo figura desde la perspectiva de la población senior, se considera importante ampliar la investigación hacia otros colectivos vulnerables, como son

los menores de edad, valorando sus elementos de riesgo, de tal manera que se desarrollen propuestas teniendo en cuenta las necesidades de cada grupo poblacional, consiguiendo así unas políticas de prevención justas y eficaces.

Finalmente, y en aras de tratar el emergente auge de la Inteligencia Artificial y las nuevas tecnologías, se propone analizar qué factores, tanto de protección como de riesgo, pueden emanar de estos sistemas, evaluando así cómo es su implicación a la hora de diseñar entornos más seguros y adaptados para todos, o bien, situaciones vectores de riesgo propicias para consumar delitos cibernéticos.

6. REFERENCIAS BIBLIOGRÁFICAS

Doctrina

Arteaga, F. M. A., Ortíz, M. F. R., Casillas, C. A. M., Ávila, C. A. M., Pérez, A. J. Z., Guzmán, D. A. Z., & Álvarez, N. Y. C. (2024). Estimulación Cognitiva: clave para el bienestar y la mejora cognitiva en adultos mayores. *JÓVENES EN LA CIENCIA*, *28*, 1-6.

Avilés, D. A. (2010). Control Social y Prevención delictiva. Una introducción al tema desde el análisis de los medios de comunicación social. *Contribuciones a las Ciencias Sociales*, *5*.

Colorado, F. D. (2006). Una mirada desde las víctimas: el surgimiento de la victimología. Ensayo. *Umbral científico*, (9), 141-159.

Botero, C. G., Coronel, E., & Pérez, C. A. (2009). Revisión teórica del concepto de victimización secundaria. *Liberabit*, *15*(1), 49-58.

Debnath, B., Kar, N., Biswas, P., Das, N., & Das, A. (2025). A comprehensive assessment on phishing, smishing and vishing. In *Data Science & Exploration in Artificial Intelligence: Proceedings of the First International Conference On Data Science & Exploration in Artificial Intelligence (CODE-AI 2024) Bangalore, India, 3rd-4th July, 2024 (Volume 2)* (p. 274). CRC Press.

De la Cruz Ochoa, R (2001) "Control Social y Derecho Penal", en Revista Cubana de Derecho, No. 17:4.

Felson, M., & Clarke, R. V. (2008). La ocasión hace al ladrón. Teoría práctica para la prevención del delito.

Fernández, E. V. (2017). El control y la prevención del delito como objeto de la criminología. *Miscelánea Comillas. Revista de Ciencias Humanas y Sociales*, *75*(146), 171-194.

Francia, M., & Pilar, M. (2019). Los malos tratos en la tercera edad en España. La invisibilidad como factor de vulnerabilidad. *Trayectorias Humanas Trascontinentales*, (5).

Hirschi, T. (2003). Una teoría del control de la delincuencia. *Capítulo criminológico*, *31*(4).

Kamau, J., & Kaburu, D. (2022). A review of smishing attaks mitigation strategies. *International Journal of Computer and Information Technology (2279-0764)*, *11*(1).

Llinares, F. M. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista española de investigación criminológica*, *11*, 1-35.

Masó, M. M. (2023). Comentario a "La creación de la Escuela de Criminología Crítica de Barcelona. La institucionalización académica de una nueva mirada sobre el control social y punitivo (1980-2022)" de Guthmann y Rivera Beiras. *Nueva Crítica Penal*, *5*(10), 49-54.

Marchiori, H. (2017). Dificultades en el acceso a la justicia de víctimas ancianos-adultos mayores. *Revista De La Facultad De Derecho De México*, *67*(269), 639–673.

Noriega, L. E. P. (2022). Procedimientos en la investigación judicial de estafas a través de medios cibernéticos o informáticos.

Olmo, P. O. (2021). Introducción a los estudios históricos sobre el control del delito. *Millars: Espai i Història*, (51), 9.

Rodríguez, L. Á. L. (2024). La tipificación del phishing, smishing y vishing como defraudación en base a la concepción del bien jurídica seguridad informática.

Sykes, G. M. C., & Matza, D. (2008). Técnicas de neutralización: una teoría de la delincuencia. *Caderno CRH*, *21*, 163-170.

Vargas, C. S. S. (2024). Encuesta web sobre percepción control social informal en el delito de contrabando documentado: Un primer acercamiento a su medición y análisis.

Vilches, N. S. M. (2024). La vulnerabilidad victimal de los ancianos y su protección en el código penal: valoración y perspectivas de futuro. *Revista de Victimología/Journal of Victimology*, (18), 91-132.

Villagómez-Cabezas, A. V., Bonilla-Andrango, L. J., Bonilla-González, G. P. & Torres-García, T. D. (2023). El aprendizaje social de Albert Bandura como estrategia de educación para la ciudadanía. *Polo del Conocimiento,* 8(5), 1286-1307.

Jurisprudencia

Sentencia del Tribunal Supremo, Sala de lo Penal (2025). Sentencia n.º 1474/2025, de 2 de abril de 2025. ECLI:ES:TS:2025:1474. CENDOJ https://www.poderjudicial.es/

Legislación

Constitución Española [CE]. Boletín Oficial del Estado, núm. 311, de 29 de diciembre de 1978. Entrada en vigor el 29 de diciembre de 1978.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal [CP]. Boletín Oficial del Estado, núm. 281, de 24 de noviembre de 1995. Entrada en vigor el 24 de mayo de 1996.

Ley 7/1991, de Asistencia y Protección al Anciano. Boletín Oficial del Estado, núm. 88, de 19 de abril de 1991. Entrada en vigor el 9 de mayo de 1991.

Ley 6/1999, de 7 de julio, de Atención y Protección a las Personas Mayores. Boletín Oficial del Estado, núm. 87, de 29 de julio de 1999. Entrada en vigor el 20 de julio de 1999.

Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico [LSSI-CE]. Boletín Oficial del Estado, núm. 166, de 17 de julio de 2002. Entrada en vigor el 12 de octubre de 2002.

Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia. Boletín Oficial del Estado, núm. 299, de 15 de diciembre de 2006. Entrada en vigor el 1 de enero de 2007.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Boletín Oficial del Estado, núm. 287, de 30 de noviembre de 2007. Entrada en vigor el 1 de diciembre de 2007.

Páginas web

Asociación de la Prensa de Málaga (2025, 7 de mayo). *Prensa sin Edad promueve la alfabetización mediática en cuatro municipios*. Asociación de la Prensa de Málaga. https://aprensamalaga.com/actividades/prensa-sin-edad/prensa-sin-edad-promueve-la-alfabetizacion-mediatica-en-cuatro-municipios-20250507123312.html

Ayuntamiento de Albacete (2022, 14 de noviembre). *El Ayuntamiento lanza la campaña 'Por tu seguridad, no piques' contra los fraudes y las estafas digitales*. Ayuntamiento de Albacete.https://www.albacete.es/es/noticias/ayuntamiento-lanza-campana-tu-seguridad-no-piques-contra-fraudes-estafas-digitales

Cruz Roja (2023, 14 de noviembre). *Unos talleres para evitar el fraude digital*. Cuz Roja. https://www2.cruzroja.es/web/ahora/-/unos-talleres-para-evitar-el-fraude-digital

Gobierno de España (2021). *Carta de Derechos Digitales. Plan de Recuperación, Transformación y Resiliencia.* Gobierno de España. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Ministerio del Interior (2023). *Hechos conocidos de infracciones penales relacionadas con la cibercriminalidad por comunidades autónomas, tipología penal y periodo.* https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

Ministerio del Interior (2023). *Victimizaciones por causa de cibercriminalidad por provincias, tipología penal, periodo, grupo y edad.* https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

Ministerio del Interior (2022). *Victimizaciones por causa de cibercriminalidad por provincias, tipología penal, periodo, grupo y edad.* https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

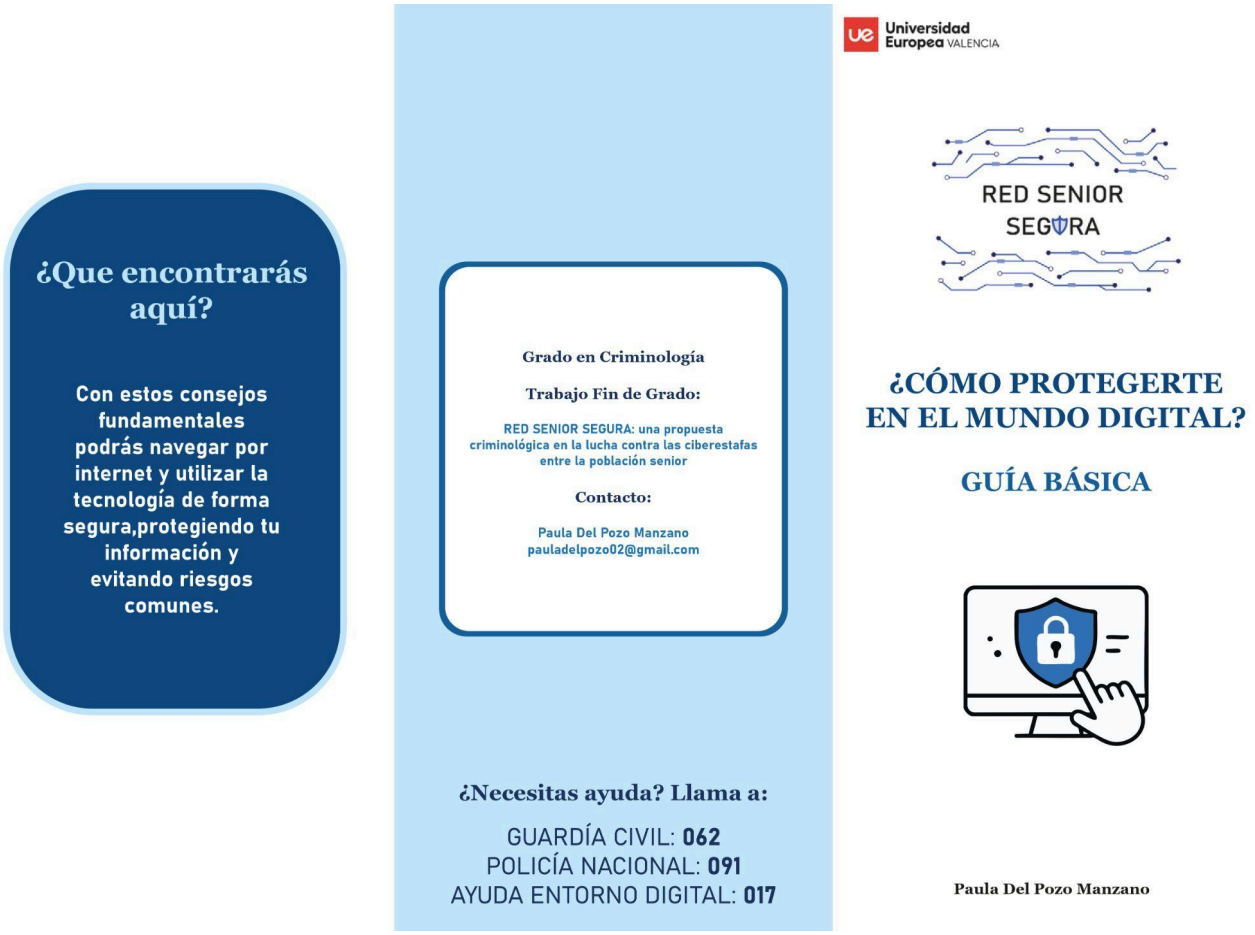
Ministerio de Interior. (s.f.). Plan Mayor de Seguridad. Gobierno de España. https://www.policia.es/_es/colabora_participacion_planmayor.php

Naciones Unidas (2002, abril). *Declaración Política y Plan de Acción Internacional de Madrid sobre el Envejecimiento*. Naciones Unidas. https://social.un.org/ageing-working-group/documents/mipaa-sp.pdf

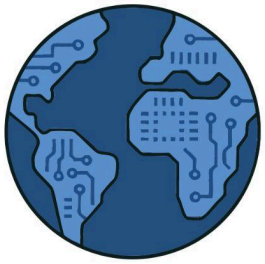
Organización de Consumidores y Usuarios (OCU) (2025, 1 abril). *Las consultas y reclamaciones por phishing tramitadas por OCU aumentaron un 166% en 2024.* https://www.ocu.org/organizacion/prensa/notas-de-prensa/2025/phishing010425

7. ANEXOS

7.1. Anexo 01 - Trípticos explicativos



¿QUÉ ES EL MUNDO DIGITAL?



Es todo aquello que hacemos a través de dispositivos electrónicos, como móviles, tablets u ordenadores. Incluye el uso de redes sociales y páginas webs.

CONSEJOS BÁSICOS DE SEGURIDAD:

1. **Mantén tus contraseñas en secreto.**

   No las compartas con nadie. Si lo haces, que sea de confianza y de una forma segura, como entregándoles un papel por escrito.

2. **Usa contraseñas seguras.**

   Que sean difíciles de adivinar, con números y símbolos.

3. **No compartas información personal.**

   Nunca des tu dirección, teléfono o datos del banco por teléfono, mensajes o por correo.

4. **Pide a alguien de confianza que revise si tus dispositivos están actualizados.**

   De esta manera tendrás todo con la última actualización de seguridad.

5. **Desconfía de enlaces y archivos que recibas.**

   No abras enlaces ni descargues archivos de personas desconocidas o que no esperabas.

¡RECUERDA!

Lo más importante es desconfiar de aquellos que nos solicitan información personal. Aunque te digan que es urgente o necesario, no hagas caso ni des tus datos.

Si realmente se trata de algo importante, las instituciones oficiales te informarán por los canales habituales y nunca te pedirán datos personales por mensajes o llamadas inesperadas.

¿Que encontrarás aquí?

Aprende a reconocer las señales más frecuentes de las estafas digitales para protegerte y sabe cuando desconfiar, evitando ser engañado.

Grado en Criminología

Trabajo Fin de Grado:

RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior

Contacto:

Paula Del Pozo Manzano
pauladelpozo02@gmail.com

¿Necesitas ayuda? Llama a:

GUARDÍA CIVIL: **062**
POLICÍA NACIONAL: **091**
AYUDA ENTORNO DIGITAL: **017**

Universidad Europea VALENCIA

RED SENIOR SEGURA

SEÑALES DE ALERTA PARA DETECTAR UNA ESTAFA DIGITAL

Paula Del Pozo Manzano

¡ATENCIÓN!

ESTAS SON SEÑALES DE ALERTA:

1. Te piden que lo hagas rápido:

- Te llaman o te envían mensajes diciendo que tienes que decidirte rápido por cualquier motivo o que perderás algo importante.
- Ejemplo: ¡Contesta ya o perderás tu oportunidad!

2. Te piden datos personales o bancarios:

- Nunca des tu número de cuenta del banco, contraseñas, DNI o datos personales por teléfono o por internet.
- Recuerda: los bancos NUNCA piden datos personales por mensajes o llamadas.

3. Mensajes inesperados:

- Desconfía si el mensaje no lo esperabas o de alguien que no reconoces.
- Pueden hacerse pasar por familiares o empresas para engañarte.

- ¿Cómo suelen ser estos mensajes?

A) Supuesto familiar:

"Hola abuela, este es mi nuevo número. ¿Me puedes enviar dinero? Es urgente."

"Hola mamá, se me ha roto el móvil. Necesito que me des dinero urgentemente".

No envíes dinero sin llamar primero a tu familiar al número de siempre.

B) Paquete que no esperabas:

"Su paquete está retenido. Pulse aquí para pagar y recibirlo".

Ignora el mensaje, si algo pasa con tu paquete, te lo harán saber.

C) Multa inesperada:

"Usted tiene una multa pendiente. Pague aquí para evitar problemas."

Las multas nunca se avisan por mensaje. Si tienes dudas, pregunta en la oficina oficial o llama a un familiar.

D) Premio aunque no hayas participado:

"¡Enhorabuena! Ha ganado un premio. Para recibirlo, pulse aquí y ponga sus datos."

Nadie regala premios sin motivo. No des tus datos y borra el mensaje.

¡RECUERDA!

- **Si tienes dudas:** Antes de hacer nada, pregunta a un familiar o a alguien de confianza.
- **También puedes llamar a tu banco** antes de responder.
- **No tengas miedo a preguntar,** no estás solo/a.
- **Es mejor esperar y comprobar,** nada es tan urgente como te lo hacen ver.

¿Que encontrarás aquí?

Descubre qué datos personales y bancarios nunca debes compartir en internet ni con desconocidos para mantener tu seguridad y evitar ser víctima de una estafa digital.

Grado en Criminología

Trabajo Fin de Grado:

RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior

Contacto:

Paula Del Pozo Manzano
pauladelpozo02@gmail.com

¿Necesitas ayuda? Llama a:

GUARDÍA CIVIL: **062**
POLICÍA NACIONAL: **091**
AYUDA ENTORNO DIGITAL: **017**

Universidad Europea VALENCIA

RED SENIOR SEGURA

ESTAFAS DIGITALES:

LO QUE NUNCA DEBES COMPARTIR

Paula Del Pozo Manzano

NUNCA COMPARTAS:

- Tus **contraseñas o códigos** de cuentas o tarjetas.
- Números de **tarjeta de crédito o débito.**

- Fotos de tus **tarjetas.**
- Fotos **privadas o familiares.**

- Datos personales como **DNI, dirección o teléfono** por mensaje o correo desconocido.

"¿Podrías mandarme tus datos personales?"

¿POR QUÉ?

Estos datos son muy valiosos para los estafadores.

Si los consiguen, pueden:

Robar tu dinero.

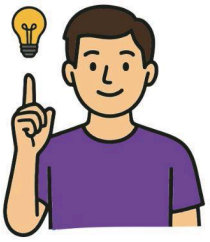
Hacerse pasar por ti.

Engañar a otras personas usando tu nombre.

¡CONSEJO IMPORTANTE!

Si alguien te pide estos datos y **no sabes quién es, ¡no lo des!**

Si **crees que conoces a la persona** detrás del mensaje, **llámala por teléfono para comprobarlo** antes de compartir cualquier información.



¿Que encontrarás aquí?

Si crees que has sido víctima de una estafa digital, aquí encontrarás los pasos a seguir para protegerte, recuperar tu seguridad y recibir ayuda.

Grado en Criminología

Trabajo Fin de Grado:

RED SENIOR SEGURA: una propuesta criminológica en la lucha contra las ciberestafas entre la población senior

Contacto:

Paula Del Pozo Manzano
pauladelpozo02@gmail.com

¿Necesitas ayuda? Llama a:

GUARDÍA CIVIL: **062**
POLICÍA NACIONAL: **091**
AYUDA ENTORNO DIGITAL: **017**

Universidad Europea VALENCIA

RED SENIOR SEGURA

PASOS A SEGUIR SI HAS CAÍDO EN UNA ESTAFA DIGITAL

Paula Del Pozo Manzano

¿QUÉ HACER SI CREES QUE TE HAN ESTAFADO?

PASO 1. **Mantén la calma** ☑

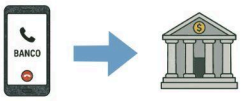
- No respondas más mensajes ni sigas las indicaciones del estafador.
- No te pongas en contacto con el estafador.

PASO 2. **No te sientas culpable ni te avergüences** ☑

- A cualquiera le puede pasar.
- No es tú culpa, los estafadores son muy hábiles.

PASO 3. **Llama a tu banco** ☑

- Avisa a tu banco si diste datos bancarios, ellos te van a ayudar a gestionar la situación.



PASO 4. **Contacta con la policía** ☑

- Informar lo sucedido, te ayudarán con todo.

PASO 5. **Habla con alguien de confianza o con un familiar** ☑

- Comenta lo que ha pasado, juntos es más fácil buscar una solución.
- No tengas miedo a pedir ayuda, todos podemos equivocarnos.

¡RECUERDA!

DEBES PEDIR AYUDA A:

- Algún familiar o alguien de confianza.
- Con el banco.
- Si puedes, acude a una comisaría de policía, mejor si vas acompañado/a.

7.2. Anexo 02 - Módulos adaptados a la población senior

Universidad Europea VALENCIA

RED SENIOR SEGURA

Paula Del Pozo Manzano
Trabajo Fin de Grado
Grado en Criminología

MÓDULO 1. Empezando con el mundo digital

Hoy en día se vive **rodeado de medios tecnológicos**, como son los teléfonos, ordenadores, tabletas, entre otros. Estos permiten que interactuemos y nos comuniquemos con familiares, ver noticias, hacer compras, pedir citas o consultar el banco, entre otras muchas posibilidades.

- **Aspectos buenos:** la comunicación con familiares y personas de confianza, comodidad para el acceso a información y facilidad de acceder a servicios.
- **Aspectos peligrosos:** el riesgo de estafas, robo de información personal o engaños si no tenemos cuidado.

Por ello, es aconsejable **aprender** poco a poco las **maneras de actuar** y **navegar por internet de forma segura**, de tal manera que podamos protegernos ante las posibles amenazas de estafas.

Para comprender mejor este contenido, es aconsejable consultar el tríptico explicativo titulado **"¿Cómo protegerte del mundo digital? Guía básica"**.

MÓDULO 2. ¿Por qué debéis protegeros?

El riesgo de convertirnos en víctima de una estafa digital será mayor o menor según el **conocimiento que se tenga sobre las tecnologías**. A **menor costumbre** de utilización de los medios tecnológicos, a **más fácil será cometer un error** y **caer en la trampa** de un estafador.

Por esto, es recomendable **conocer bien cómo funcionan estos objetos tecnológicos**, así como **tener apoyo** y **no confiar tan fácilmente** en los desconocidos.

Además, se recomienda dejar de lado el miedo a **preguntar si algo no se entiende**, nadie nace sabiendo y es **bueno comentarlo con alguien de confianza** para orientarte en cómo es mejor que se realicen ciertas acciones relacionadas con el uso del internet y la tecnología.

MÓDULO 3. Cuidado con los engaños en internet

Las estafas digitales son aquellas que **afectarán directamente a tu cuenta bancaria**, causando un perjuicio económico en aquellos que han sido víctimas.
Para poder identificarlas, es importante **conocer de qué maneras se pueden realizar**, teniendo en cuenta que los delincuentes, generalmente, actúan escondiendo quién son y utilizando datos de los demás para hacerse pasar por ellos. Estas posibilidades son:

- **A través de correos electrónicos**, buscando hacerse pasar por entidades o servicios que se conocen, como los bancos o las tiendas que se frecuentan de forma habitual.
  - Suelen intentar que se entre en un enlace falso y rellenar datos personales, como por ejemplo, un mensaje sobre un cobro pendiente de la Seguridad Social.
- **A través de llamadas telefónicas**, donde el estafador se hace pasar por una persona que parece ser real.
  - Un ejemplo es una llamada ficticia del banco, dónde piden una serie de datos para solucionar un problema que no existe en realidad.
- **Con mensajes de texto (SMS)**, los cuales envían enlaces que llevan a rellenar datos personales.
  - Por ejemplo para el pago de multas o enviar dinero a familiares que en realidad no lo son.

En conclusión, **si algún mensaje o llamada no se esperaba o se duda**, es recomendable **borrar el mensaje o colgar el teléfono**, si es algo importante, lo harán saber de una forma distinta.

Universidad Europea VALENCIA

RED SENIOR SEGURA

Paula Del Pozo Manzano
Trabajo Fin de Grado
Grado en Criminología

MÓDULO 4. ¿Cómo reconocer una estafa digital?

Este módulo es muy importante, pues la **prevención de las estafas** se consigue gracias a la **identificación de señales de alerta.** Ejemplo de estas son:

- La **urgencia o rapidez** para realizar lo que te piden, con mensajes como:

¡Contesta ya o perderás la oportunidad!

"Si no pagas de inmediato, la multa se duplicará".

- La **petición de datos personales**, como DNI o dirección, así como datos relacionados con la cuenta bancaria.
- **Mensajes sospechosos o que no se esperaban**
- En ocasiones, para parecer reales **pueden hacerse pasar por familiares** pidiendo ayuda de alguna manera para conseguir un ingreso de dinero. Por ejemplo con un mensaje como:

"Hola abuela, soy tu nieto. Envíame dinero por favor, es importante, luego te lo explico."

- Otras formas son, el **envío de un mensaje que hable sobre un paquete** que no puede llegar a la dirección de la vivienda o también la **notificación de premios inesperados o multas desconocidas**.

Estos contenidos se aprecian de una forma más clara en el tríptico explicativo denominado **"Señales de alerta para detectar una estafa digital.".** Recuerda, puedes **consultar con alguien de confianza** antes de responder.

MÓDULO 5. ¿Qué hacer si te intentan estafar o ya lo han hecho?

En el caso de creer que eres víctima de una estafa, deberíamos seguir unos sencillos pasos, los cuales están en el tríptico explicativo titulado **"Pasos a seguir si has caído en una estafa digital"**, siendo los siguientes:

1. Mantener la **calma** y **no contestar** más al estafador.
2. **Llamar a tu banco** para bloquear tarjetas o movimientos.
3. **Denunciar** lo ocurrido.
4. **Contar lo ocurrido a alguien de confianza**, como un familiar, para que de su apoyo y ayude a comprobar que está todo bien.

Ante todo, en **ningún momento deberías sentirte culpable**, pues cualquiera puede ser víctima de una estafa digital.

MÓDULO 6. Consejos para estar seguro en internet

En cuanto a los consejos que se deben seguir para **estar protegidos de los riesgos** de sufrir una estafa en internet, se tiene que saber que **no se deben compartir nunca** los siguientes datos:

- Por ningún medio, como mensajes de texto (SMS), llamadas telefónicas o correos electrónicos, contraseñas, **códigos de cuentas bancarias o tarjetas de crédito o débito.**
- **Fotos de las tarjetas bancarias ni personales**, pues esa información puede utilizarse también.
- **Datos personales**, como son el DNI, dirección física o números de teléfono, pues con estos datos se pueden hacer pasar por nosotros con facilidad.

En cuanto los **comportamientos adecuados**, se recomienda:

- **No meterse en enlaces d**e origen desconocido **o abrir archivos** enviados por conversaciones con quienes **no se sabe quienes son.**
- Crear **contraseñas difíciles de descifrar**, con distintas letras, números y símbolos. Sin fechas, números personales o nombres —por ejemplo es adecuado: 3T8a29oau_39qFsc*—.
- Comprobar **quién está detrás de cada mensaje**, realizando una llamada de teléfono a la persona o entidad con la que se cree que se está hablando.

Todos estos puntos se encuentran de una forma más clara y visual en el tríptico explicativo denominado **"Estafas digitales: lo que nunca debes compartir."**