PROYECTO FIN DE GRADO

LA EVOLUCIÓN DE LA CIBERDELINCUENCIA EN ESPAÑA RETOS Y TENDENCIAS ACTUALES

Autora: Alejandra Soriano Silva

Tutor: Prof. Mario Muñoz Anguita

GRADO EN CRIMINOLOGÍA

FACULTAD DE LAS CIENCIAS SOCIALES Y DE LA COMUNICACIÓN

UNIVERSIDAD EUROPEA

DEDICATORIA

A mis padres, por ser la base sólida sobre la que he construido cada uno de mis pasos.
A mi madre, por su amor infinito, por su entrega constante y por enseñarme que la fuerza más poderosa es la que se ejerce con cariño. Gracias por estar siempre, incluso cuando no hacía falta decir nada.
A mi padre, por su paciencia, su constancia y sus palabras que, aunque pocas, siempre llegan en el momento justo. Por mostrarme que la sabiduría no está en saberlo todo, sino en saber estar.

A mi hermana, mi compañera de vida, mi espejo, mi amiga. Gracias por tu apoyo incondicional, tus ánimos en los días de cansancio, tus bromas que me han sacado sonrisas y tu forma única de estar cerca incluso cuando estamos lejos.

A mi familia, por ser red, refugio y raíz. Cada gesto, cada palabra de aliento, cada celebración compartida han hecho que este camino fuera más llevadero y lleno de sentido.

Y cómo no, a mis perros, que con sus miradas, su compañía silenciosa y su alegría incondicional me han dado paz en los momentos de ansiedad, calma en los días de presión y amor sin juicio en cada jornada. Gracias por estar ahí, simplemente siendo, acompañando mis madrugadas de estudio y mis descansos robados. A vosotros, que no habláis con palabras pero decís tanto.

Este trabajo es para todos vosotros. Porque detrás de cada página escrita hay un pedacito de lo que me habéis dado.

RESUMEN

La revolución digital ha cambiado radicalmente no sólo la forma en que las personas y las empresas interactúan, sino también cómo se cometen los delitos, surgiendo así una nueva categoría conocida como cibercrímenes. Este término abarca una amplia gama de actividades ilícitas que explotan los sistemas tecnológicos, incluyendo el robo de identidad, el fraude financiero, los ataques de ransomware y el ciberacoso. Estos delitos a menudo traspasan fronteras, lo que dificulta su detección, investigación y enjuiciamiento. A medida que los cibercriminales se vuelven más sofisticados, estos crímenes evolucionan paralelamente con los avances tecnológicos, presentando retos crecientes tanto para los delincuentes como para las autoridades.

Este trabajo tiene como objetivo analizar la evolución de los cibercrímenes actuales, identificando las principales tendencias y examinando cómo los criminales adaptan sus tácticas a las nuevas tecnologías. Además, se investigarán los perfiles de los cibercriminales, explorando sus motivaciones, antecedentes y técnicas. También se examinará el impacto en las víctimas, particularmente en cuanto a las secuelas psicológicas y económicas que experimentan. Una parte importante del estudio se centrará en cómo las fuerzas de seguridad están abordando estos retos, las herramientas y técnicas que emplean y su efectividad. Por último, se explorará el papel de las campañas de concienciación pública y la importancia de las estrategias de prevención, proponiendo mejoras para enfrentar este problema creciente.

Justificación: A medida que el mundo avanza hacia una mayor digitalización, los cibercrímenes se convierten en una amenaza constante para individuos, empresas e incluso gobiernos. Es fundamental comprender la naturaleza cambiante de estos delitos, las debilidades que explotan y las medidas necesarias para prevenirlos y combatirlos de manera eficaz. Este estudio busca aportar soluciones prácticas y una mayor comprensión del problema.

Palabras clave

Cibercrimen, Evolución tecnológica, Prevención y seguridad.

ABSTRACT

The digital revolution has not only reshaped how individuals and businesses operate but has also transformed the landscape of criminal activity, leading to the rise of cybercrimes. Cybercrime refers to a wide array of illegal actions that exploit technological systems, including but not limited to identity theft, financial fraud, ransomware attacks, and cyberstalking. These crimes often cross borders, making it difficult for law enforcement agencies to detect, investigate, and prosecute offenders. As cybercrime becomes increasingly sophisticated, it evolves alongside technological advancements, presenting growing challenges for both perpetrators and the authorities trying to stop them.

This thesis aims to examine the evolution of the actual cybercrime, identifying key trends and analyzing how criminals are adapting their tactics to new technologies. Furthermore, it will delve into the profiles of cybercriminals, exploring their motivations, backgrounds, and techniques. The impact on victims, particularly the psychological and financial damage, will also be analyzed. A significant portion of the research will focus on how law enforcement agencies are addressing these challenges, the tools and techniques they use, and how effective they are. Finally, the study will explore the role of public awareness campaigns and the importance of prevention strategies, suggesting improvements for tackling this growing problem.

Justification: As the world continues to embrace digitalization, cybercrime becomes an ever-present threat to individuals, corporations, and even governments. It is crucial to understand the evolving nature of these crimes, the weaknesses they exploit, and the necessary measures to prevent and combat them effectively. This research seeks to contribute to this understanding by offering practical insights and solutions.

Key Words

Cybercrime, Technological evolution, Law enforcement strategies.

ÍNDICE

ÍNDICE DE TABLAS O FIGURAS

ÍNDICE DE SIGLAS Y ABREVIATURAS

SIGLA	INGLÉS	ESPAÑOL
CaaS	Crime as Service	Crimen como Servicio
IoT	Internet of Things	Internet de las cosas
IA	Artificial Intelligence	Inteligencia artificial
NIS2	Network and Information Security	Directiva de Seguridad de Redes e Información
GDPR	General Data Protection Regulation	Reglamento General de Protección de Datos
FBI	Federal Bureau of Investigation	Buró Federal de Investigación
Europol	European Union Agency for Law Enforcement Cooperation	Agencia de la unión Europea para la Investigación
Interpol	International Criminal Police Organization	Organización Internacional de Policía Criminal
CFAA	Computer Fraud and Abuse Act	Ley de Fraude y Abuso Informático
UN	United Nations	Naciones Unidas
VPN	Virtual Private Network	Red Privada Virtual
SMB	Server Message Block	Bloque de Mensajes del Servidor
TOR	The Onion Router	El Enrutador de Cebolla
CNI	National Intelligence Center	Centro Nacional de Inteligencia
TFG	Final Degree Project	Trabajo de Fin de Grado
CISA	Cibersecurtiy and Infrastructure Security Agency	Agencia de Ciberseguridad y Seguridad de Infraestructura
ODS	Sustainable Development Goal	Objetivos de Desarrollo Sostenible

1. INTRODUCCIÓN

En los últimos años, el avance vertiginoso de las tecnologías de la información y la comunicación ha transformado profundamente las dinámicas sociales, económicas y delictivas en España. La digitalización ha mejorado numerosos aspectos de la vida cotidiana, pero también ha abierto la puerta a nuevas formas de criminalidad: los cibercrímenes. Estos delitos, caracterizados por su comisión a través de medios digitales, han experimentado un notable crecimiento tanto en complejidad como en frecuencia, generando una amenaza real para la seguridad ciudadana y la estabilidad institucional (Wall, 2021; Holt & Bossler, 2020).

Según el Ministerio del Interior (2024), los delitos informáticos han pasado de representar una porción marginal del total de delitos registrados en el país, a ocupar posiciones destacadas en las estadísticas criminales. En 2023, se reportaron más de 25.000 ciberincidentes, lo que evidencia una tendencia ascendente preocupante y sostenida en el tiempo. Este incremento no solo se traduce en pérdidas económicas significativas especialmente en los sectores financiero y empresarial, sino también en un aumento de las afectaciones psicológicas y sociales entre las víctimas, quienes suelen sentirse desprotegidas ante la dificultad de rastreo y control que caracteriza este tipo de criminalidad digital (González-Caballero & Romero-Ruiz, 2023; Ministerio del Interior, 2024).

Uno de los principales retos que enfrentan las instituciones españolas es la constante evolución de los métodos utilizados por los ciberdelincuentes. Estos actores, muchas veces organizados en redes transnacionales, aprovechan las brechas tecnológicas, la falta de educación digital de la población y las limitaciones normativas para desarrollar ataques cada vez más sofisticados. Ejemplos recientes incluyen campañas masivas de phishing dirigidas a la ciudadanía, ataques de ransomware a hospitales públicos, o la explotación de vulnerabilidades en infraestructuras críticas (INCIBE, 2023; CCN-CERT, 2023).

La facilidad con la que pueden operar desde fuera del territorio nacional, combinada con el anonimato que permiten herramientas como las criptomonedas o las redes cifradas (Tor, VPN), complica enormemente su identificación y posterior persecución penal (Rodríguez-Serrano, 2022; Brenner, 2019).

En este contexto, España ha avanzado en el diseño de estrategias de ciberseguridad, tanto desde el ámbito gubernamental como desde el sector privado. No obstante, persisten desafíos importantes en la coordinación entre organismos, en la actualización legislativa frente a nuevas formas de ciberdelincuencia, y en la concienciación de la ciudadanía. La entrada en vigor de normativas como la Directiva NIS2 a nivel europeo, y su transposición al ordenamiento jurídico español, marcan avances significativos, pero aún insuficientes para responder de forma efectiva a la naturaleza cambiante y multifactorial del cibercrimen (Parlamento Europeo y Consejo de la UE, 2022; Maras, 2020).

Además, el entorno digital no distingue entre usuarios altamente cualificados y personas vulnerables. Tanto ciudadanos particulares como empresas y organismos públicos pueden convertirse en víctimas de estos delitos, lo que plantea una problemática transversal que requiere de un abordaje igualmente amplio y multidisciplinar. La falta de cultura en ciberseguridad, especialmente en segmentos de población como personas mayores o colectivos con bajo acceso a formación digital, aumenta el riesgo de victimización (Martínez-Ferrer & Marín-López, 2021; Newman, 2018).

Por tanto, resulta urgente analizar en profundidad la evolución del cibercrimen en España, identificar los factores que lo alimentan, y evaluar la eficacia de las estrategias actuales de prevención y control. Solo a partir de un diagnóstico riguroso será posible proponer mejoras en la respuesta institucional, fomentar la educación digital desde edades tempranas y promover una cultura de seguridad que permita mitigar los efectos de estos delitos en una sociedad cada vez más conectada (Europol, 2023; INCIBE, 2023).

Figura 1

Auge del cibercrimen, amenazas y consecuencias en las víctimas

Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico muestra el incremento del cibercrimen, sus principales amenazas y sus efectos en las víctimas

1.1 Problema de investigación

La transformación digital que ha experimentado España en la última década ha redefinido no solo la forma en que se comunican, informan y desarrollan sus actividades cotidianas los ciudadanos, sino también las modalidades de acción delictiva. Esta evolución, profundamente marcada por la expansión de las tecnologías de la información y la comunicación, ha dado lugar a un escenario en el que la criminalidad tradicional convive —e incluso se ve superada— por formas emergentes de delito en ento

rnos digitales. La ciberdelincuencia se manifiesta así como un fenómeno en ascenso, con un grado de sofisticación y mutabilidad que desafía las capacidades de respuesta del Estado y del marco normativo vigente (Wall, 2021; Maras, 2020).

Según datos del Ministerio del Interior (2023), en 2023 se registraron más de 25.000 ciberincidentes, una cifra que evidencia no solo una tendencia al alza, sino también un cambio estructural en el panorama delictivo nacional. Esta cifra refleja un aumento del 17,5 % en las infracciones penales relacionadas con el ámbito digital, frente al 2,4 % registrado en 2011, lo que sitúa al cibercrimen como una de las principales amenazas para la seguridad ciudadana y la estabilidad institucional (Ministerio del Interior, 2023). Más allá del volumen, lo preocupante es el grado de especialización de las amenazas: los ciberdelitos actuales no solo buscan el beneficio económico, sino que en muchos casos persiguen el sabotaje de infraestructuras críticas, la suplantación de identidades, la alteración de procesos democráticos o el deterioro de la reputación institucional (CCN-CERT, 2023).

El dinamismo del entorno tecnológico ha favorecido que los ciberdelincuentes actúen con una capacidad de adaptación que sobrepasa los ritmos de la respuesta legal y operativa. Gracias al anonimato que proporcionan herramientas como la red Tor, las VPN, las criptomonedas y el uso de servidores descentralizados, estos actores pueden operar desde cualquier parte del mundo, lo que complica su localización, identificación y enjuiciamiento (Rodríguez-Serrano, 2022; Brenner, 2019). Además, la disponibilidad de kits delictivos accesibles en la dark web, el modelo Crime-as-a-Service y la progresiva profesionalización del delito digital han reducido la barrera de entrada al cibercrimen, extendiendo su alcance a usuarios sin grandes conocimientos técnicos pero con capacidad de causar graves daños.

No se trata de un problema que afecte únicamente a las grandes corporaciones o instituciones públicas. Cada vez más ciudadanos, pymes, administraciones locales, centros educativos y hospitales son víctimas de este tipo de delitos. Las consecuencias no se limitan a pérdidas económicas, sino que incluyen también impactos psicológicos, crisis de confianza en el uso de tecnologías, afectación reputacional e interrupción de servicios esenciales. La transversalidad del fenómeno hace necesario un enfoque multidisciplinar y preventivo, que supere la visión meramente reactiva y se apoye en herramientas criminológicas, tecnológicas, educativas y legales (Holt & Bossler, 2020).

La presente investigación busca no solo identificar sus principales tipologías y factores estructurales, sino también examinar en profundidad las respuestas ofrecidas por el Estado, el sector privado y la sociedad civil. Esta labor se articula desde una perspectiva criminológica aplicada, capaz de generar propuestas fundamentadas que mejoren la prevención, detección y persecución del delito digital en un entorno social cada vez más interconectado (Europol, 2023).

1.2. Pregunta de investigación

Teniendo en cuenta el crecimiento exponencial de los delitos informáticos en España, y considerando los múltiples factores tecnológicos, sociales y normativos que inciden en su expansión, esta investigación se plantea la siguiente pregunta central:

¿Cuáles son los factores determinantes en la evolución del cibercrimen en España durante la última década y qué estrategias pueden implementarse para mejorar su prevención y control desde una perspectiva criminológica?

Esta pregunta busca no solo identificar las causas estructurales y coyunturales que propician el auge del cibercrimen en el contexto español, sino también evaluar críticamente la eficacia de las medidas adoptadas por el Estado, el sector privado y la sociedad civil. La intención es generar

conocimiento que permita no solo describir el fenómeno, sino también orientar acciones concretas para mitigarlo, con especial énfasis en la prevención, la cooperación institucional y la educación digital.

1.3. Objetivos

1.3.1 Objetivo General

Analizar la evolución de la ciberdelincuencia en España durante la última década, identificando sus principales tipologías, tendencias delictivas y factores determinantes, así como evaluar la eficacia de las estrategias de prevención y control implementadas, con el fin de proponer mejoras que fortalezcan la capacidad de respuesta del país frente a estas amenazas emergentes.

1.3.2 Objetivos Específicos

OE1: Identificar las principales tipologías de ciberdelincuencia registradas en España entre 2013 y 2023, y analizar su evolución en términos de frecuencia, complejidad y ámbito de afectación.

OE2: Identificar los principales factores de riesgo que han propiciado el incremento de los delitos informáticos en el país.

OE3: Evaluar críticamente las estrategias de prevención, detección y respuesta frente a la ciberdelincuencia implementadas por los sectores público y privado, identificando sus principales fortalezas y debilidades.

1.4. Justificación

La elección del cibercrimen como objeto de estudio responde a una necesidad urgente de adecuar el análisis criminológico a las nuevas formas de amenaza que plantea el entorno digital. Lejos de ser una moda académica, el estudio del delito en el ciberespacio constituye hoy un campo prioritario para las ciencias sociales aplicadas, especialmente para la Criminología, que debe adaptarse con rapidez a un contexto donde las lógicas tradicionales del delito —espacialidad, visibilidad, trazabilidad— han sido radicalmente transformadas (Wall, 2021).

Desde el plano académico, esta investigación se justifica por la escasa producción existente en el ámbito de la Criminología aplicada al entorno digital en España. Mientras que los enfoques legales, técnicos y policiales han avanzado de manera significativa, todavía existe un déficit de estudios que analicen la ciberdelincuencia desde una perspectiva interdisciplinar, integrando variables como la motivación delictiva, la percepción de las víctimas, el papel de la estructura social o la eficacia de las políticas públicas (Rodríguez-Serrano, 2022). Este trabajo pretende contribuir a esa línea emergente, generando conocimiento útil tanto para la comunidad académica como para los actores institucionales.

Desde una perspectiva institucional, la pertinencia de esta investigación se refuerza por el impacto creciente de los delitos informáticos en el funcionamiento de los servicios públicos y privados. La paralización del SEPE en 2021, el ataque al Hospital Clínic de Barcelona en 2023 o los bloqueos a plataformas bancarias mediante ransomware muestran que las consecuencias del

cibercrimen no son abstractas, sino profundamente disruptivas para la ciudadanía (CCN-CERT, 2023; INCIBE, 2023). Identificar los fallos del sistema de prevención y respuesta, y formular recomendaciones basadas en evidencia, es una necesidad prioritaria en un contexto donde la digitalización no se detendrá.

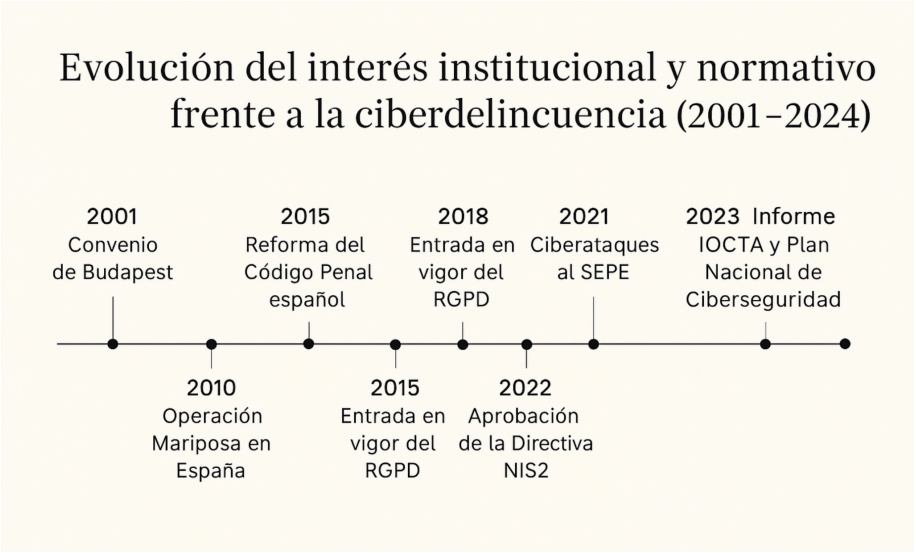
Desde el plano normativo y político, la ciberdelincuencia constituye un reto transversal para los sistemas democráticos. No solo vulnera derechos fundamentales como la intimidad, la seguridad o la protección de datos personales, sino que también pone en entredicho la capacidad de los Estados para garantizar el orden jurídico en entornos desmaterializados. A pesar de la existencia de marcos como la Convención de Budapest, el RGPD o la Directiva NIS2, su implementación efectiva sigue enfrentando importantes obstáculos, especialmente cuando los delitos se cometen desde jurisdicciones que no cooperan internacionalmente (Parlamento Europeo y Consejo de la UE, 2022; Consejo de Europa, 2001).

Además, esta investigación responde a los principios del Objetivo de Desarrollo Sostenible (ODS) 16, que promueve la consolidación de instituciones sólidas y el acceso equitativo a la justicia. En la medida en que el cibercrimen genera exclusión digital, desigualdad de protección y nuevas formas de violencia estructural, su análisis desde una óptica crítica se convierte en un imperativo ético y político (Naciones Unidas, 2015).

Desde una motivación personal y profesional, este TFG representa un compromiso con la construcción de una Criminología crítica, digitalmente alfabetizada y socialmente comprometida. El objetivo no es solo describir el problema, sino contribuir activamente a su comprensión y resolución, ofreciendo herramientas conceptuales y prácticas para que la sociedad española afronte con mayor eficacia los desafíos que plantea el delito en la era digital.

Figura 2

Línea temporal de la evolución normativa e institucional frente al cibercrimen (2001–2024)



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico muestra eventos clave en la respuesta legal e institucional al cibercrimen en España y la UE.

2. FUNDAMENTACIÓN TEÓRICA

2.1 Formulación de hipótesis: Resultados esperados

En el marco del presente Trabajo de Fin de Grado, se plantean un conjunto de hipótesis que permiten orientar el análisis y la interpretación de los resultados obtenidos. Estas hipótesis están formuladas a partir del problema de investigación y en correspondencia directa con los objetivos específicos del estudio. Su función es ofrecer una base teórica que pueda ser contrastada mediante el análisis cualitativo de casos reales y el apoyo en fuentes cuantitativas secundarias.

Las hipótesis propuestas buscan no solo describir la realidad de la ciberdelincuencia en España durante la última década, sino también explicar sus causas estructurales, evaluar la efectividad de las políticas implementadas y anticipar posibles líneas de mejora. A continuación, se exponen las hipótesis que guían esta investigación:

H1: La ciberdelincuencia en España ha experimentado una transición desde delitos individuales de bajo impacto hacia formas más complejas, organizadas y orientadas a sectores estratégicos como el financiero, el sanitario o las infraestructuras críticas.

H2: Factores como el aumento del acceso a internet, la falta de formación en ciberseguridad, la adopción masiva de nuevas tecnologías sin regulación suficiente y la escasa cultura de protección digital han contribuido de forma significativa a la expansión de la ciberdelincuencia en España.

H3: Las políticas y programas actuales presentan deficiencias en cuanto a cooperación internacional, actualización legislativa y formación especializada, lo que limita su eficacia frente a una amenaza en constante evolución.

2.2. Definición de cibercrimen y tipologías

La ciberdelincuencia constituye una de las formas más disruptivas y en constante evolución de la criminalidad contemporánea. Su rasgo distintivo es el uso de tecnologías de la información y la comunicación (TIC) como medio, herramienta o fin en la comisión del delito. A diferencia de la delincuencia tradicional, los ciberdelitos no requieren proximidad física entre agresor y víctima, ni una ubicación específica para su ejecución, lo que dificulta su identificación, rastreo y persecución (Wall, 2021). Esta deslocalización geográfica, combinada con el anonimato y la baja percepción de riesgo, ha convertido al entorno digital en un espacio propicio para la expansión delictiva.

Desde una perspectiva criminológica, se entiende por ciberdelincuencia toda conducta ilícita que se desarrolla total o parcialmente en el ciberespacio y que vulnera derechos individuales o colectivos, provocando daños patrimoniales, psicológicos, reputacionales o institucionales (Navarro-Torres, 2022). Esta definición permite abarcar no sólo los delitos “nativos digitales” (aquellos que no podrían existir fuera de un entorno informático), sino también los delitos tradicionales que han migrado o mutado al ecosistema virtual.

El enfoque académico distingue entre ciberdelitos propiamente dichos, que tienen como objetivo directo un sistema informático o una red (por ejemplo, el acceso no autorizado o el sabotaje digital), y delitos cometidos mediante las TIC, como la estafa, el acoso o la distribución de material ilícito, donde la tecnología actúa como instrumento facilitador (Brenner, 2019). Esta clasificación

funcional resulta especialmente útil para diseñar estrategias diferenciadas de prevención, intervención y respuesta legal.

En el contexto español, esta distinción también es relevante en términos legales, ya que el Código Penal contempla conductas como el acceso ilícito a sistemas, el daño informático o el fraude informático como delitos específicos, pero sanciona otras conductas tradicionales que, adaptadas al mundo digital, presentan un impacto más amplio y difícil de controlar (Ministerio del Interior, 2024).

La ciberdelincuencia se manifiesta en múltiples formas, y su tipología sigue ampliándose conforme se desarrollan nuevas herramientas tecnológicas. A continuación se presentan las principales categorías actualmente reconocidas:

Los fraudes digitales y delitos patrimoniales; Engloba prácticas como el *phishing*, la suplantación de identidad, la manipulación de plataformas de compraventa y el robo de credenciales bancarias. Estos delitos persiguen principalmente el lucro económico y se han convertido en la tipología más habitual en las denuncias registradas en España (Newman, 2018). La facilidad con la que pueden ejecutarse y el bajo riesgo percibido por los agresores explican su enorme proliferación.

Ataques contra infraestructuras críticas; Este tipo de delito implica acciones dirigidas a redes, sistemas o servicios esenciales, como hospitales, aeropuertos, bancos o centrales eléctricas. El uso de ransomware para paralizar servicios y extorsionar económicamente es una modalidad cada vez más frecuente. Estos ataques tienen un alto impacto social y pueden generar caos en la población, como ocurrió con “WannaCry” en 2017 (Europol, 2023).

Delitos contra la privacidad y la protección de datos; Incluyen el espionaje digital, el robo de datos personales, la captación ilícita de imágenes y la filtración de bases de datos sensibles. Estos delitos vulneran derechos fundamentales y están regulados por normativas como el Reglamento General de Protección de Datos (RGPD), cuya aplicación efectiva aún presenta importantes desafíos, especialmente ante ataques transfronterizos (Maras, 2020).

Violencia digital y ciberacoso; Abarca conductas como el *ciberbullying*, la sextorsión, el hostigamiento en redes, la difusión de contenido íntimo no consentido o el *doxing* (publicación maliciosa de datos personales). Estas formas de ciberdelincuencia afectan principalmente a mujeres, menores y colectivos vulnerables, generando consecuencias psicológicas graves y prolongadas en el tiempo (Holt & Bossler, 2020).

Ciberdelincuencia organizada; Se refiere a redes criminales estructuradas que actúan en el entorno digital para desarrollar actividades ilícitas como la venta de datos robados, la creación de *malware*, la distribución de pornografía infantil o el blanqueo de capitales. Estas organizaciones suelen operar desde la *dark web*, donde ofrecen sus servicios mediante el modelo “Crime-as-a-Service” (Brenner, 2019). Esta profesionalización del delito dificulta la labor policial y plantea nuevos retos en materia de cooperación internacional.

La naturaleza cambiante de la ciberdelincuencia exige un enfoque de análisis que combine elementos técnicos, jurídicos y sociales. No se trata simplemente de nuevas formas de cometer viejos delitos, sino de una transformación profunda de la lógica criminal, que aprovecha las debilidades estructurales del entorno digital, la falta de regulación unificada y el rezago institucional frente a la innovación tecnológica.

Una diferenciación clave para el análisis criminológico del fenómeno es la que distingue entre ciberdelitos propiamente dichos y delitos convencionales digitalizados. Los primeros son aquellos cuya existencia depende del entorno digital; es decir, no podrían cometerse sin una infraestructura tecnológica (como el acceso ilícito a sistemas, el sabotaje informático o la creación de malware) (Wall, 2007; Brenner, 2010). Estos constituyen lo que se ha denominado delincuencia no convencional, en tanto que rompen con las formas tradicionales de criminalidad y requieren una respuesta específica desde el ámbito legal y técnico.

En cambio, los delitos convencionales digitalizados son aquellos que ya existían en el mundo físico, pero que han encontrado en el entorno digital un nuevo canal de ejecución, expansión o amplificación (Holt & Bossler, 2015). Tal es el caso del fraude, el acoso o la extorsión, cuyas modalidades online han multiplicado su alcance y reducido el coste de oportunidad para los agresores.

Esta distinción es relevante no solo desde una perspectiva jurídica, sino también desde el análisis criminológico, ya que implica motivaciones, perfiles y patrones de conducta distintos, así como medidas de prevención diferenciadas.

En consecuencia, comprender la tipología de la ciberdelincuencia no solo permite identificar los mecanismos de acción de los agresores, sino también diseñar políticas públicas más eficaces, adaptar los marcos normativos y fomentar una cultura de ciberseguridad que proteja a los usuarios del entorno digital.

2.3. Evolución histórica de los cibercrímenes

El desarrollo de la ciberdelincuencia ha seguido una trayectoria paralela al avance de la tecnología digital, adaptándose con rapidez a los cambios en los modos de vida, las comunicaciones y las infraestructuras socioeconómicas. A diferencia de otras formas delictivas, la criminalidad digital se caracteriza por una capacidad excepcional de transformación, escalabilidad y anonimato, lo que ha permitido su expansión global con gran facilidad. Comprender su evolución histórica resulta esencial para analizar no sólo sus manifestaciones actuales, sino también los retos que plantea a medio y largo plazo para los sistemas de seguridad y justicia.

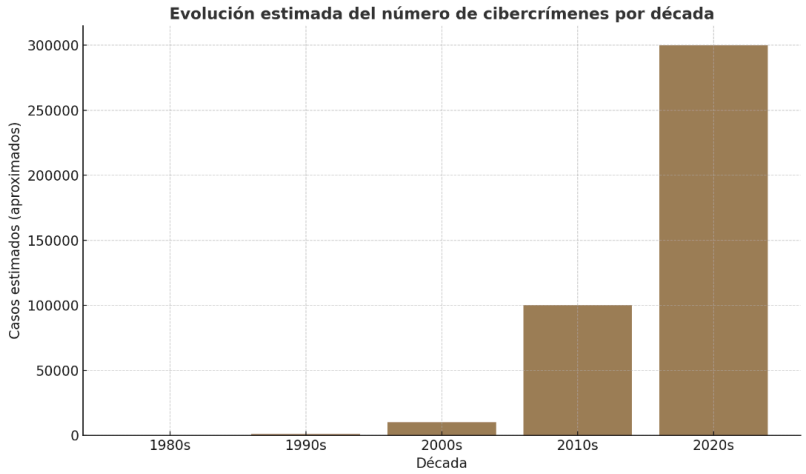
Los primeros indicios de ciberdelincuencia se remontan a la década de 1980, en una etapa aún incipiente del uso civil de la informática. Durante este periodo, los delitos informáticos se limitaban a acciones relativamente rudimentarias, como la creación de virus simples y fraudes informáticos en sistemas bancarios cerrados. Uno de los casos emblemáticos fue el virus “Elk Cloner” (1982), que afectaba a ordenadores Apple II a través de disquetes infectados, considerado por muchos como el primer *malware* de propagación masiva (Brenner, 2019). Poco después, el gusano de Morris (1988), liberado accidentalmente en “ARPANET”, mostró por primera vez el potencial disruptivo de un código autónomo capaz de paralizar sistemas conectados entre sí (Newman, 2018).

En la década de 1990, la masificación de Internet transformó el ecosistema digital y abrió nuevas posibilidades para la delincuencia. Surgieron delitos como el *phishing*, los primeros fraudes por correo electrónico, y el uso de troyanos para acceder a información bancaria. Uno de los eventos más notorios fue el gusano “ILOVEYOU” (2000), que causó daños por valor de miles de millones de dólares al propagarse a través del correo electrónico, aprovechando técnicas de ingeniería social

(Wall, 2021). Este ataque marcó un antes y un después en la percepción de los riesgos asociados al uso de la red.

Figura 3

Evolución estimada del número de cibercriminales por década



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico representa el crecimiento estimado de cibercriminales desde los años 80 hasta la década de 2020.

A partir de los años 2000, con la popularización del comercio electrónico y las redes sociales, la ciberdelincuencia adquirió una nueva dimensión. La aparición de *software* malicioso más sofisticado, como los *keyloggers* y los *rootkits*, permitió a los delincuentes obtener credenciales, acceder a sistemas protegidos y operar con altos niveles de ocultamiento y baja trazabilidad. Asimismo, comenzaron a surgir los primeros servicios ilegales ofrecidos en la *darkweb*, y con ellos las bases del modelo Crime-as-a-Service, donde herramientas delictivas podían adquirirse o alquilarse por cualquier usuario con conocimientos mínimos (Navarro-Torres, 2022).

La década de 2010 consolidó la profesionalización del delito cibernético. El *ransomware* se posicionó como una de las amenazas más lucrativas y frecuentes, destacando casos como “WannaCry” (2017), que afectó a más de 200.000 equipos en todo el mundo, incluidas infraestructuras hospitalarias y redes de transporte (Europol, 2023). Al mismo tiempo, los delitos contra la privacidad, como las filtraciones masivas de datos (ej. Yahoo (2013-2014)), evidenciaron la vulnerabilidad de incluso las grandes corporaciones tecnológicas.

En paralelo, los ciberdelitos adquirieron una dimensión geopolítica. Ataques atribuidos a actores estatales o grupos patrocinados por gobiernos comenzaron a utilizar el ciberespacio como terreno de confrontación. El caso de “NotPetya” (2017), que afectó principalmente a Ucrania pero se propagó a nivel internacional, fue calificado por expertos como un acto de ciberguerra encubierta, más

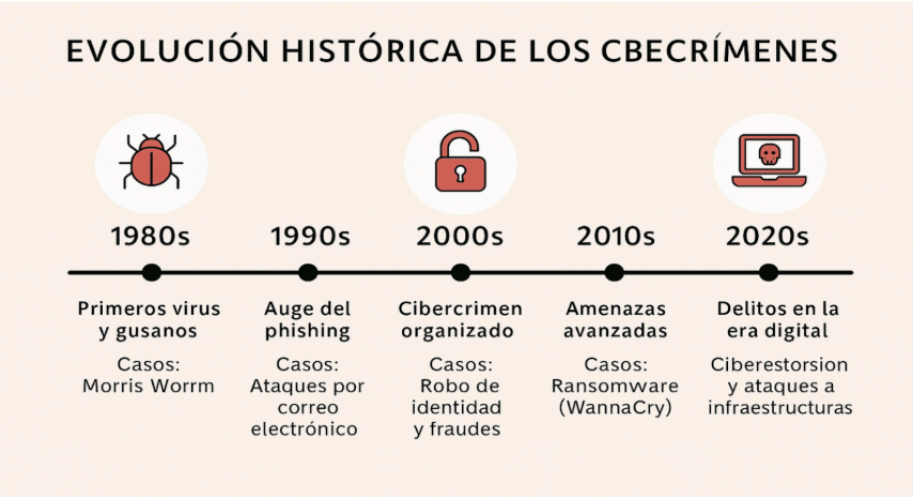
orientado a causar daño que a obtener beneficios económicos (Buchanan, 2020). Estas acciones revelaron una tendencia preocupante: el uso del ciberespacio como herramienta de desestabilización política.

En la actualidad, la ciberdelincuencia se encuentra en un punto de inflexión. La adopción acelerada de tecnologías emergentes ha ampliado exponencialmente las superficies de exposición digital. Los ataques son cada vez más personalizados, automatizados y dirigidos a objetivos estratégicos. Además, la combinación de técnicas como los *deepfakes*, el *phishing* de voz (*vishing*) y la suplantación de identidad biométrica está generando nuevas modalidades delictivas difíciles de detectar con métodos tradicionales (Holt & Bossler, 2020).

A medida que se diversifican los escenarios tecnológicos, la ciberdelincuencia deja de ser una amenaza meramente técnica para convertirse en un desafío estructural con implicaciones sociales, económicas y políticas. Su evolución no ha sido lineal, sino adaptativa, moldeándose a cada nuevo avance tecnológico, lo que obliga a las instituciones a anticiparse a las amenazas emergentes y revisar permanentemente sus modelos de prevención y respuesta.

Figura 4

Evolución histórica de los cibercriminales por décadas (1980s-2020s)



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico resume la progresión del cibercrimen, desde virus iniciales hasta ataques complejos a infraestructuras

2.4. Legislación nacional e internacional sobre cibercrimen

La creciente sofisticación de la ciberdelincuencia y su carácter transnacional han evidenciado la necesidad de establecer marcos legales coherentes, adaptativos y eficaces tanto a nivel nacional como internacional. A diferencia de otras formas de criminalidad, los delitos informáticos suelen implicar jurisdicciones múltiples, barreras tecnológicas, y sujetos anónimos o difíciles de localizar, lo que exige una regulación jurídica especializada y mecanismos sólidos de cooperación entre Estados. No obstante, a pesar de los esfuerzos normativos desarrollados en las últimas décadas, todavía

persisten importantes brechas legales, asimetrías entre países y limitaciones operativas que dificultan una respuesta penal integral frente a esta amenaza.

Ámbito internacional: hacia una cooperación jurídica universal

El principal instrumento jurídico de alcance global en materia de ciberdelincuencia es la Convención de Budapest sobre Ciberdelincuencia (2001), promovida por el Consejo de Europa y ratificada por más de 65 países, incluido España. Esta convención constituye el primer tratado internacional específicamente orientado a regular los delitos informáticos y establecer procedimientos comunes de cooperación penal internacional (Consejo de Europa, 2022). Su estructura normativa abarca cuatro grandes áreas: infracciones penales, procedimientos de investigación, cooperación internacional y principios de derecho penal. A pesar de su relevancia, su efectividad se ve limitada por la negativa de ciertos actores geopolíticos clave como Rusia o China a adherirse al tratado, lo que obstaculiza la persecución eficaz de delitos cometidos desde esas jurisdicciones (Maras, 2020).

En los últimos años, las Naciones Unidas han impulsado propuestas para la creación de una nueva convención global sobre cibercrimen, lo que refleja la urgencia de adaptar los marcos normativos a los delitos digitales emergentes y ampliar la cobertura jurídica más allá del ámbito europeo (Buchanan, 2020).

Ámbito europeo: protección de datos, ciberseguridad y resiliencia digital

En el contexto de la Unión Europea, el desarrollo normativo ha sido especialmente activo, con una serie de directivas y reglamentos que buscan armonizar la legislación de los Estados miembros. Destaca la reciente Directiva NIS2 (2022), que sustituye a su predecesora de 2016 y amplía las obligaciones de seguridad digital para operadores esenciales y empresas tecnológicas, reforzando los requisitos de ciberresiliencia, notificación de incidentes y supervisión estatal (Parlamento Europeo, 2022).

Además, el Reglamento General de Protección de Datos (RGPD), en vigor desde 2018, establece un marco común para la gestión, tratamiento y protección de datos personales en el ámbito digital. Si bien no regula de forma directa los delitos informáticos, su aplicación tiene un impacto significativo en la prevención de prácticas delictivas como el robo de identidad, la captación ilícita de datos o las filtraciones masivas (Maras, 2020).

La UE también ha impulsado la creación de agencias especializadas, como Europol y su Centro Europeo de Ciberdelincuencia (EC3), que actúan como nodos de coordinación y análisis para investigaciones transnacionales, fortaleciendo la cooperación entre cuerpos policiales y judiciales.

Ámbito nacional: regulación penal y desafíos institucionales

En el caso de España, la ciberdelincuencia se encuentra regulada principalmente en el Código Penal, reformado en 2015 para incorporar tipos penales específicos relativos a delitos informáticos. Entre las figuras destacadas se encuentran el acceso ilícito a sistemas, la interceptación de comunicaciones, la manipulación de datos, la suplantación de identidad, la distribución de *malware* y el fraude informático (Ministerio de Justicia, 2015). Estas tipificaciones se alinean con los estándares de la Convención de Budapest, lo que facilita la cooperación internacional en la materia.

Asimismo, la Ley Orgánica 4/2015, de Protección de la Seguridad Ciudadana, contempla sanciones para conductas como la difusión no autorizada de imágenes en redes sociales, la alteración de datos digitales con fines delictivos o la suplantación de identidad en entornos virtuales.

A nivel operativo, el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), junto con el INCIBE y las unidades especializadas de la Guardia Civil y el Cuerpo Nacional de Policía, constituyen los pilares del sistema español de ciberseguridad. No obstante, diversos informes señalan que persisten carencias en materia de recursos humanos especializados, formación continua, actualización tecnológica y capacidad de respuesta ante ataques complejos (CCN-CERT, 2023).

Desafíos legales y necesidades de armonización

A pesar del notable avance normativo, tanto en España como a nivel internacional, el marco legal vigente presenta ciertos límites frente a una amenaza que se transforma a mayor velocidad que las leyes. La fragmentación legislativa, las dificultades para establecer jurisdicción en entornos transnacionales, y la falta de instrumentos ágiles de extradición son obstáculos recurrentes en la persecución del delito digital (Wall, 2021).

Asimismo, el vertiginoso crecimiento de tecnologías emergentes como la inteligencia artificial, la biometría, las criptomonedas o el Internet de las Cosas exige una actualización constante del marco normativo para anticipar escenarios delictivos y garantizar una protección efectiva de los derechos fundamentales en el entorno digital.

En este contexto, se hace cada vez más evidente la necesidad de avanzar hacia una mayor armonización internacional, combinando esfuerzos legislativos con cooperación policial y judicial, inversión en ciberinteligencia y el fortalecimiento de capacidades técnicas a todos los niveles.

2.5. Factores que favorecen la expansión del cibercrimen

La ciberdelincuencia ha logrado expandirse de forma vertiginosa en las últimas décadas, impulsada no solo por el avance tecnológico, sino también por un conjunto de factores estructurales que configuran un entorno propicio para su proliferación. Esta expansión no se debe únicamente a la sofisticación de los medios empleados por los agresores, sino a un ecosistema digital que facilita la impunidad, reduce los riesgos percibidos y multiplica las oportunidades delictivas.

Uno de los elementos clave es la posibilidad de operar desde el anonimato, potenciada por herramientas como las redes privadas virtuales (VPN), la red Tor o las criptomonedas. Estas tecnologías dificultan la trazabilidad de las acciones delictivas, lo que no solo complica la labor investigadora, sino que también disminuye la percepción del riesgo entre los ciberdelincuentes. Esta condición, ampliamente reconocida en la literatura como uno de los motores estructurales del cibercrimen, contribuye a la repetición, profesionalización e incluso comercialización del delito (Wall, 2021; Navarro-Torres, 2022).

Además, la creciente interconexión de dispositivos mediante el Internet de las Cosas (IoT) ha multiplicado los vectores de ataque posibles. Muchos de estos dispositivos, como cámaras inteligentes, sistemas industriales o electrodomésticos conectados, carecen de protocolos de seguridad robustos, lo que los convierte en puntos vulnerables fácilmente explotables por actores maliciosos (Holt & Bossler, 2020).

A ello se suma la democratización del cibercrimen: actualmente, cualquier usuario con acceso a internet puede adquirir herramientas delictivas listas para usar, como kits de phishing o programas de ransomware. Esta accesibilidad ha diluido la frontera entre expertos y usuarios comunes, ampliando el espectro de agresores potenciales y facilitando delitos complejos sin conocimientos avanzados (Brenner, 2019).

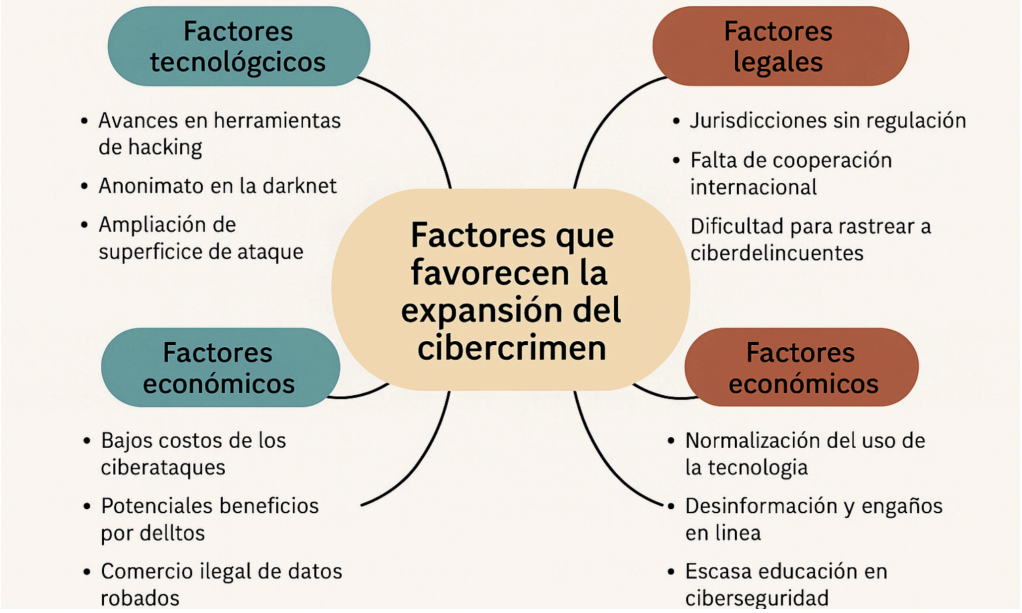
Por otra parte, la fragmentación normativa internacional permite que muchos ciberdelincuentes operen desde jurisdicciones laxas o sin acuerdos de cooperación judicial, lo que dificulta enormemente su localización, persecución y sanción efectiva. Este fenómeno ha dado lugar a la existencia de verdaderos "refugios digitales" que obstaculizan la acción penal (Maras, 2020).

Finalmente, la escasa cultura preventiva en ciberseguridad sigue siendo un problema extendido. El desconocimiento sobre los riesgos digitales, la falta de formación especializada y la ausencia de hábitos seguros en el uso de tecnologías aumentan la exposición tanto de particulares como de organizaciones. Aunque existen soluciones técnicas avanzadas, gran parte de los incidentes tienen su origen en el error humano, lo que subraya la necesidad de políticas educativas sostenidas y transversales (Newman, 2018).

En conjunto, estos factores configuran un entorno donde la ciberdelincuencia no solo se expande, sino que se consolida como un fenómeno complejo, transnacional y en constante mutación. Afrontarlo exige una respuesta integral que combine prevención, cooperación internacional, innovación tecnológica y alfabetización digital desde una perspectiva criminológica crítica.

Figura 5

Factores que favorecen la expansión del cibercrimen



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico sintetiza los factores tecnológicos, legales, económicos y sociales que impulsan el crecimiento del cibercrimen.

2.6. Perfil de los cibercriminales

La figura del ciberdelincuente ha evolucionado notablemente desde las primeras manifestaciones del delito informático hasta la actualidad, reflejando los cambios en el entorno tecnológico y en las dinámicas delictivas. Lejos de responder a un perfil único, quienes cometen delitos en el ciberespacio conforman un grupo extremadamente diverso, tanto en términos de motivación como de nivel técnico, estructura organizativa y grado de peligrosidad. Esta heterogeneidad obliga a analizar la ciberdelincuencia como un fenómeno plural, donde conviven desde actores individuales sin formación especializada hasta redes criminales altamente estructuradas, e incluso operadores patrocinados por Estados.

En los primeros años del fenómeno, los delincuentes informáticos eran frecuentemente individuos jóvenes, autodidactas, motivados por el reto intelectual, la curiosidad o el deseo de reconocimiento en comunidades virtuales. Estos primeros *hackers,* aunque responsables de daños importantes, rara vez actuaban con fines lucrativos. Sin embargo, con el paso del tiempo, y especialmente a partir de la década de 2000, la irrupción de modelos de negocio ilícitos en internet dio paso a una creciente profesionalización del delito digital. Hoy, muchos ciberdelincuentes actúan movidos por una lógica económica clara, estructurando sus actividades como auténticas empresas del crimen, con división de tareas, jerarquías internas y recursos técnicos avanzados (Navarro-Torres, 2022).

Dentro de este panorama, uno de los perfiles más frecuentes es el del agresor individual o en pequeños grupos, que opera desde entornos domésticos y comete delitos como fraudes por *phishing*, estafas en redes sociales o distribución de *malware* de bajo nivel. Estos delincuentes, aunque menos sofisticados, resultan especialmente peligrosos por el volumen de víctimas potenciales a las que pueden acceder gracias a la automatización de sus herramientas. En el otro extremo, encontramos estructuras delictivas complejas que operan en la dark web y se dedican a actividades como el tráfico de datos personales, el desarrollo de *ransomware,* la extorsión digital y la venta de servicios criminales en modalidad “Crime-as-a-Service” (Brenner, 2019). Estas organizaciones utilizan tecnologías de cifrado, servidores ocultos y redes de bots para dificultar su rastreo y mantener la impunidad de sus miembros.

Otra categoría relevante es la de los delincuentes con conocimientos técnicos intermedios que actúan de forma oportunista. Este perfil es especialmente común entre personas que utilizan *software* ya disponible en la red para ejecutar acciones delictivas sin comprender del todo su funcionamiento. Este fenómeno ha crecido gracias a la proliferación de tutoriales, herramientas listas para usar y foros donde se difunden métodos y recursos para cometer delitos informáticos. La accesibilidad del cibercrimen ha hecho que este tipo de delincuencia ya no esté reservada a expertos, sino abierta a una comunidad más amplia de usuarios con motivaciones diversas (Newman, 2018).

Cabe destacar también la existencia de actores patrocinados por Estados o vinculados a intereses ideológicos o geopolíticos, cuyo perfil responde a objetivos estratégicos más amplios que el mero beneficio económico. Estos ciberdelincuentes, muchas veces integrados en estructuras estatales o paramilitares, participan en operaciones de espionaje, sabotaje o desinformación, y su actuación suele orientarse al debilitamiento de instituciones públicas, la manipulación de procesos electorales o el ataque a infraestructuras críticas. Su nivel de sofisticación técnica es notablemente superior al promedio, y sus acciones se encuadran en lo que algunos autores han definido como “ciberguerra” o “ciberterrorismo” (Buchanan, 2020).

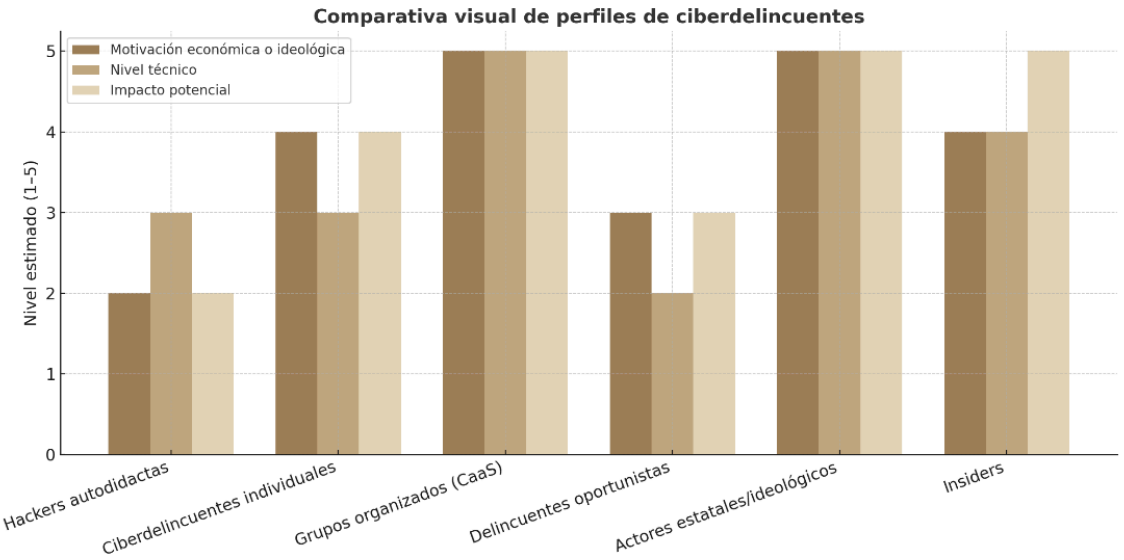
Por último, no debe ignorarse el papel de los llamados *insiders* o amenazas internas. Se trata de personas con acceso legítimo a sistemas informáticos como empleados, técnicos o contratistas que utilizan su posición para robar información, manipular datos o facilitar accesos a terceros. Este perfil, aunque menos visible, representa uno de los mayores riesgos para la seguridad digital, ya que combina conocimiento del sistema con acceso privilegiado, lo que complica su detección y permite acciones de gran impacto (Holt & Bossler, 2020).

En suma, el perfil del ciberdelincuente actual es poliédrico, dinámico y difícil de tipificar de forma cerrada. Comprender las distintas tipologías existentes, así como sus motivaciones y formas de operar, resulta esencial para diseñar estrategias de prevención y persecución efectivas. La ciberdelincuencia no responde a un único patrón, sino a una red cambiante de actores que actúan desde múltiples niveles de complejidad, con intereses que van desde lo económico hasta lo político, y con un grado de adaptabilidad que desafía los marcos tradicionales del control penal.

Esta diversidad de perfiles se resume gráficamente en la comparativa que se muestra a continuación, donde se representan tres variables clave: la motivación económica o ideológica del ciberdelincuente, su nivel técnico y el impacto potencial de sus acciones. A través de una escala cualitativa del 1 al 5, el gráfico permite visualizar cómo ciertos perfiles —como los actores estatales o los insiders— presentan niveles más elevados en las tres dimensiones, mientras que otros —como los hackers autodidactas o los delincuentes oportunistas— muestran menor sofisticación técnica, aunque no por ello resultan menos peligrosos en términos de número de víctimas o volumen de ataques. Esta representación facilita una comprensión integral del fenómeno y refuerza la necesidad de estrategias diferenciadas de prevención y control adaptadas a cada tipo de agente.

Figura 6

Comparativa visual de perfiles de ciberdelincuentes según nivel técnico, motivación e impacto



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico compara diferentes perfiles de ciberdelincuentes según su motivación, nivel técnico y potencial de impacto.

2.7. Impacto del cibercrimen en las víctimas

El cibercrimen no solo representa una amenaza para la seguridad digital de los Estados o de las empresas, sino que también genera consecuencias profundas y duraderas en las personas que lo sufren. A diferencia de otras formas de criminalidad, su impacto trasciende lo puramente económico o material y alcanza esferas como la salud mental, la integridad emocional, la confianza en la tecnología y, en muchos casos, el tejido mismo de las relaciones sociales y profesionales de las víctimas. Esta dimensión humana del delito digital es a menudo menos visible, pero no por ello menos devastadora.

Uno de los efectos más significativos del cibercrimen es el daño psicológico. Las víctimas de ciberdelitos, especialmente aquellos relacionados con el ciberacoso, la sextorsión o el *doxing*, suelen experimentar ansiedad, depresión, trastornos del sueño, sensación de persecución o miedo a utilizar medios digitales. El sentimiento de vulnerabilidad que provoca la intromisión no consentida en la intimidad, unido a la incertidumbre sobre el uso futuro de los datos expuestos, genera una angustia persistente que puede prolongarse mucho después de haber sufrido el ataque (Holt & Bossler, 2020). En casos extremos, como el acoso sistemático en redes sociales o la exposición pública de imágenes íntimas, el impacto emocional puede derivar en aislamiento social, abandono laboral o incluso ideaciones suicidas, especialmente entre adolescentes y jóvenes.

En el ámbito económico, los efectos del cibercrimen también son relevantes. Muchas víctimas sufren pérdidas directas a través de fraudes bancarios, suplantación de identidad o compras no autorizadas, enfrentándose luego a largos y complejos procedimientos legales para recuperar sus fondos o limpiar su historial crediticio. En los casos de *ransomware*, las empresas y particulares se ven obligados a pagar elevadas sumas de dinero para recuperar el acceso a sus datos, y no siempre con garantías de éxito. Las consecuencias financieras pueden extenderse incluso a las víctimas indirectas, como los clientes de empresas afectadas por filtraciones de datos o los ciudadanos cuyas instituciones públicas han sido atacadas (Europol, 2023).

Otro efecto importante es la pérdida de confianza en la tecnología. Muchas víctimas, tras sufrir un ataque, desarrollan desconfianza hacia plataformas digitales, redes sociales o servicios online. Esto puede traducirse en una reducción del uso de herramientas tecnológicas, en un mayor aislamiento digital o en una renuncia al aprovechamiento de las ventajas que ofrece la sociedad de la información. Esta desconfianza afecta también a la percepción de seguridad institucional, especialmente cuando las víctimas sienten que no han recibido una respuesta adecuada por parte de las autoridades o que su denuncia ha sido ignorada, archivada o nunca resuelta (Maras, 2020).

Desde un punto de vista legal y procedimental, las víctimas del cibercrimen suelen enfrentarse a un sistema lento, fragmentado y poco preparado para dar respuesta a sus necesidades específicas. La dificultad para identificar a los agresores, especialmente cuando operan desde el extranjero o emplean técnicas de anonimato sofisticadas, limita en muchos casos las posibilidades de obtener justicia. Además, la falta de personal especializado, la escasez de unidades forenses digitales y la ausencia de protocolos claros en la atención a la víctima dificultan la reparación del daño y fomentan un sentimiento de abandono institucional (Wall, 2021).

En el plano social, el cibercrimen puede afectar gravemente la reputación de las personas. La difusión de contenidos íntimos, la manipulación de perfiles en redes sociales, la publicación de datos privados o la suplantación de identidad pueden tener consecuencias irreversibles, tanto en el ámbito personal como profesional. En determinados contextos, como el laboral o el académico, estas acciones

pueden derivar en despidos, pérdida de oportunidades o discriminación. La huella digital que deja el delito puede mantenerse indefinidamente, dificultando la recuperación emocional y la reintegración de la víctima en la vida cotidiana (Newman, 2018).

Finalmente, conviene señalar que el impacto del cibercrimen se amplifica en contextos de desigualdad, falta de recursos o baja alfabetización digital. Colectivos vulnerables como personas mayores, menores de edad, mujeres o personas con discapacidad son especialmente susceptibles de ser víctimas, ya que suelen tener menos herramientas para identificar amenazas, proteger su información o responder eficazmente ante una situación de riesgo. Esta desigualdad digital se convierte así en un factor de victimización secundaria que perpetúa los efectos del delito y agrava las consecuencias sociales.

En definitiva, el cibercrimen no puede analizarse únicamente desde la perspectiva del daño técnico o económico. Sus efectos sobre las víctimas requieren una atención integral que combine apoyo psicológico, protección jurídica, reparación económica y acompañamiento social. Para ello, es necesario avanzar hacia un modelo de intervención centrado en la víctima, que reconozca la complejidad del impacto delictivo en el entorno digital y promueva mecanismos de atención específicos, ágiles y empáticos.

A continuación, se resume gráficamente el impacto que tienen los principales tipos de ciberdelitos sobre las víctimas, diferenciando sus consecuencias económicas, psicológicas y sociales.

Figura 7

Impacto del cibercrimen en las víctimas: económico, psicológico y social

Nota. Elaboración propia mediante Canva, Madrid, 2025. La tabla muestra los principales tipos de cibercrimen y sus efectos sobre las víctimas en tres dimensiones clave.

2.8. Medidas de prevención y estrategias de mitigación

La creciente sofisticación de la ciberdelincuencia y su capacidad de adaptación a nuevas tecnologías requieren una respuesta igualmente dinámica, multidisciplinar y coordinada. La prevención y mitigación del cibercrimen no puede depender únicamente de medidas técnicas, sino que debe abordarse desde un enfoque integral que combine educación digital, actualización legislativa, cooperación internacional, refuerzo institucional y concienciación social. En este sentido, las estrategias deben orientarse no solo a reducir las oportunidades delictivas, sino también a empoderar a los usuarios y reforzar la resiliencia de los sistemas frente a posibles ataques.

A continuación, se presentan las principales líneas de actuación que constituyen el eje de una política de prevención eficaz frente a la ciberdelincuencia:

Fortalecimiento de la ciberseguridad técnica; Una de las medidas más urgentes es la implementación de protocolos robustos de protección en infraestructuras digitales críticas y sistemas de información sensibles. Esto incluye el cifrado de datos, el uso de autenticación multifactor, la segmentación de redes, la detección de intrusiones en tiempo real y la actualización permanente de *software* y parches de seguridad. Estas acciones permiten minimizar la exposición a amenazas y dificultar el acceso de los ciberdelincuentes a entornos vulnerables (Holt & Bossler, 2020).

Educación digital y cultura preventiva; La concienciación del usuario es uno de los pilares fundamentales de la prevención. La mayoría de los ataques exitosos ocurren debido a errores humanos evitables, como el uso de contraseñas débiles, la descarga de archivos maliciosos o la respuesta a correos fraudulentos. Por ello, es esencial implementar programas educativos dirigidos a toda la población, desde escolares hasta personas mayores, que enseñan buenas prácticas en el uso seguro de la tecnología, fomenten el pensamiento crítico y promuevan la responsabilidad digital (Newman, 2018).

Normativas actualizadas y cooperación internacional; La lucha contra el cibercrimen exige marcos legales actualizados que respondan con agilidad a las nuevas formas delictivas. Es necesario armonizar la legislación entre países, fortalecer los tratados internacionales como la Convención de Budapest, y agilizar los mecanismos de cooperación judicial y extradición. La ciberdelincuencia no entiende de fronteras, por lo que la respuesta tampoco puede ser exclusivamente nacional (Maras, 2020).

Fomento de la colaboración público-privada; Dado que gran parte de la infraestructura digital se encuentra en manos privadas, es imprescindible establecer canales de cooperación entre el sector público y el privado. Esto implica compartir información sobre amenazas, coordinar respuestas ante incidentes y establecer estándares comunes de seguridad. La creación de centros de respuesta a incidentes (CSIRT), como el del INCIBE en España, es un ejemplo de esta sinergia positiva (CCN-CERT, 2023).

Uso de tecnologías predictivas e inteligencia artificial; La inteligencia artificial y el análisis de datos pueden ser herramientas poderosas para anticipar amenazas, detectar comportamientos anómalos en la red y responder proactivamente a posibles ataques. La aplicación de algoritmos de aprendizaje automático permite identificar patrones de actividad sospechosa en tiempo real,

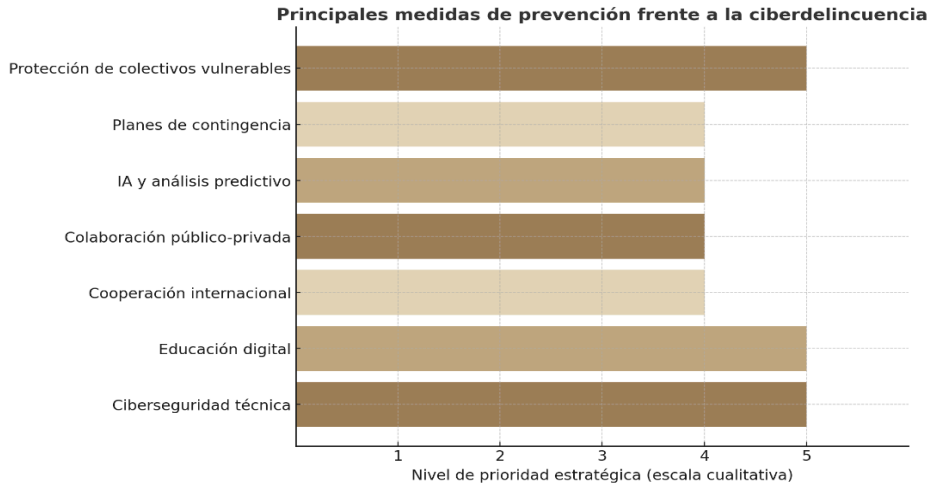
mejorando la capacidad de detección temprana y reduciendo el tiempo de reacción ante incidentes críticos (Europol, 2023).

Respaldo, recuperación de datos y planes de contingencia; Ante ataques inevitables, es fundamental contar con sistemas de respaldo automatizado, copias de seguridad externas, y protocolos de recuperación rápida. La existencia de planes de contingencia y simulacros periódicos reduce el impacto de los ataques y mejora la capacidad de las organizaciones para continuar operando de manera segura y eficiente.

Protección específica para colectivos vulnerables; Es necesario diseñar estrategias de protección adaptadas a colectivos especialmente expuestos, como menores, personas mayores, víctimas de violencia de género o personas con escasa alfabetización digital. Esto incluye campañas de sensibilización específicas, asistencia jurídica y psicológica, y canales de denuncia accesibles y seguros.

Figura 8

Principales medidas de prevención frente a la ciberdelincuencia



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico representa una priorización cualitativa de estrategias preventivas frente al cibercrimen.

En conjunto, estas medidas deben formar parte de una estrategia nacional de ciberseguridad coherente, proactiva y centrada en la prevención. La formación de ciudadanos críticos, la actualización normativa y la colaboración entre actores públicos y privados no solo reducen el riesgo de victimización, sino que fortalecen la confianza en el entorno digital y contribuyen a la construcción de una sociedad más segura, resiliente e informada.

2.9.Perspectivas futuras y nuevos retos

El futuro de la ciberdelincuencia se proyecta como un escenario de alta complejidad, marcado por la aceleración tecnológica, el aumento de la interdependencia digital y la aparición de nuevos vectores de riesgo. A medida que la sociedad se digitaliza y las tecnologías emergentes se integran en todos los ámbitos de la vida cotidiana desde el hogar hasta las infraestructuras críticas, la superficie de

exposición a amenazas digitales se amplía, y con ella, el margen de acción de los ciberdelincuentes. Esta evolución constante plantea el desafío de anticiparse al delito, en lugar de limitarse a reaccionar ante sus consecuencias.

Uno de los retos más significativos es el uso de inteligencia artificial (IA) como herramienta tanto de defensa como de ataque. Mientras que los sistemas de ciberseguridad están incorporando algoritmos de aprendizaje automático para detectar amenazas en tiempo real, los ciberdelincuentes también están utilizando la IA para automatizar ataques, perfeccionar técnicas de suplantación (como el *phishing* o el *vishing*) y crear contenidos falsos altamente persuasivos. Los *deepfakes*, por ejemplo, han comenzado a utilizarse para fraudes financieros, chantajes y manipulación informativa, y se espera que su uso malicioso se intensifique en los próximos años (Wall, 2021).

El crecimiento del Internet de las Cosas (IoT) representa otro foco de vulnerabilidad. La conexión masiva de dispositivos domésticos, industriales y sanitarios ha generado una red compleja y en gran parte insegura, ya que muchos de estos sistemas carecen de estándares de protección adecuados. La posibilidad de que un simple dispositivo inteligente mal configurado se convierta en una puerta de entrada para un ciberataque masivo es una realidad cada vez más tangible. Además, se prevé que el número de dispositivos conectados supere los 75 mil millones en 2030, lo que complica aún más la gestión de riesgos en entornos heterogéneos (Europol, 2023).

En el plano geopolítico, la expansión del ciberterrorismo y la ciberguerra constituye una amenaza creciente. Estados y actores no estatales están empleando herramientas digitales para desestabilizar sistemas democráticos, interferir en procesos electorales, atacar infraestructuras críticas y manipular la opinión pública. Los ciberataques dirigidos contra servicios de salud, transporte o energía no solo buscan interrumpir su funcionamiento, sino también sembrar el caos y la desconfianza en la ciudadanía. El caso del *malware* “NotPetya”, atribuido a un actor estatal, mostró cómo un ataque encubierto bajo apariencia de *ransomware* puede causar daños económicos globales y dejar en evidencia la fragilidad de los sistemas digitales (Buchanan, 2020).

Otro desafío prioritario es la regulación de las nuevas tecnologías y la armonización normativa a nivel global. Mientras la innovación avanza de forma exponencial, la legislación tiende a ir por detrás, lo que deja vacíos legales que son rápidamente explotados por los ciberdelincuentes. A pesar de esfuerzos como la Directiva NIS2 en la Unión Europea o la Convención de Budapest, aún existe una notable fragmentación jurídica y dificultades para establecer mecanismos de cooperación internacional eficaces. La existencia de “refugios digitales” en países con legislaciones laxas o sin acuerdos de extradición dificulta considerablemente la lucha contra el delito transnacional (Maras, 2020).

El fenómeno del Crime-as-a-Service (CaaS) continuará en expansión. Esta modalidad convierte la ciberdelincuencia en un mercado abierto donde herramientas delictivas se venden, alquilan o distribuyen por encargo en plataformas clandestinas. Se estima que la facilidad de acceso a malware personalizado, redes de *bots* o servicios de *ransomware* contribuye no solo al aumento del número de atacantes, sino también a la diversificación y sofisticación de los delitos cometidos (Brenner, 2019).

Por otra parte, la privacidad y la protección de datos personales se verán sometidas a presiones crecientes debido a la generalización del uso de tecnologías biométricas, reconocimiento facial, *big data* y vigilancia algorítmica. Las empresas y gobiernos recopilan cantidades ingentes de

información personal, muchas veces sin el consentimiento informado de los usuarios o sin garantías suficientes sobre su tratamiento. La posibilidad de abusos, fugas o manipulación de datos plantea no sólo un riesgo técnico, sino un desafío ético de gran envergadura.

Ante estos escenarios, será necesario repensar las estrategias de ciberseguridad desde una perspectiva proactiva, anticipatoria y multidimensional. No se trata únicamente de desarrollar barreras técnicas más sólidas, sino de fomentar una cultura digital crítica, fortalecer la cooperación global, promover la transparencia algorítmica y garantizar que los derechos fundamentales no se vean erosionados en la era digital. La formación de profesionales especializados, la inversión en tecnologías de detección avanzada y la creación de marcos éticos claros serán elementos esenciales para enfrentar los retos que se avecinan.

En definitiva, el futuro de la ciberdelincuencia no es una amenaza estática, sino un proceso en evolución que exigirá respuestas constantes, innovadoras y colectivas. Solo mediante la combinación de prevención, regulación, educación y cooperación será posible garantizar un entorno digital seguro, justo y resiliente.

2.10. Casos emblemáticos de cibercrimen

El análisis de casos reales de ciberdelincuencia resulta fundamental para comprender la evolución de este fenómeno, las vulnerabilidades explotadas por los agresores, y las consecuencias que los delitos digitales pueden tener a nivel social, económico y político. A continuación, se presentan algunos de los ciberataques más emblemáticos tanto a escala internacional como en el contexto español.

2.10.1. Casos internacionales

WannaCry (2017): El ransomware global que paralizó infraestructuras sanitarias y corporativas

En mayo de 2017, el *ransomware* WannaCry afectó a más de 200.000 dispositivos en más de 150 países, explotando una vulnerabilidad en sistemas Windows. Este *malware* bloqueaba el acceso a archivos y exigía un rescate en criptomonedas. Entre los sectores más afectados se encontraron hospitales del Reino Unido, servicios de transporte y empresas como Telefónica en España. El ataque puso de manifiesto la fragilidad de muchas infraestructuras críticas frente a amenazas digitales globales (Europol, 2023).

Colonial Pipeline (2021): El ataque que afectó al suministro energético de EE.UU

El grupo de ciberdelincuentes DarkSide ejecutó un ciberataque mediante *ransomware* contra el oleoducto Colonial Pipeline, clave para el suministro de combustible en la costa este de Estados Unidos. La empresa se vio obligada a suspender sus operaciones durante varios días, generando escasez de combustible y subidas de precios. Este ataque motivó la declaración de emergencia nacional por parte del gobierno de EE.UU. y marcó un antes y un después en la consideración del cibercrimen como amenaza de seguridad nacional (Buchanan, 2020).

REvil (2021): El modelo Ransomware-as-a-Service en su máxima expresión

El grupo REvil se especializó en alquilar su software malicioso a terceros a través de la dark web, consolidando el modelo Ransomware-as-a-Service (RaaS). En 2021, lanzaron un ataque contra

la empresa de TI Kaseya, afectando a más de 1.500 empresas en todo el mundo. El impacto económico y logístico fue tal que requirió la intervención coordinada de Europol, FBI y diversas agencias de ciberseguridad. Este caso mostró el grado de organización empresarial que ha adquirido la ciberdelincuencia moderna (Navarro-Torres, 2022).

Yahoo (2013-2014): La mayor filtración de datos personales registrada

Durante dos años consecutivos, la compañía Yahoo sufrió brechas de seguridad que expusieron datos personales de más de 3.000 millones de cuentas de usuario. La información comprometida incluía nombres, correos electrónicos, contraseñas y preguntas de seguridad. El escándalo tuvo consecuencias legales y financieras para la empresa, y evidenció la importancia de implementar políticas de protección de datos robustas y auditables (Maras, 2020).

2.10.2. Casos nacionales (España)

Telefónica (2017): Impacto directo de WannaCry en España

Uno de los efectos más notorios de "WannaCry" se produjo en España, donde Telefónica fue una de las primeras grandes empresas en verse afectada. El ataque forzó el cierre preventivo de sistemas y obligó a cientos de empleados a desconectarse de la red corporativa. Este incidente impulsó al Gobierno español a reforzar su estrategia nacional de ciberseguridad y a activar los protocolos del Instituto Nacional de Ciberseguridad (INCIBE).

SEPE (2021): Paralización del Servicio Público de Empleo Estatal

En marzo de 2021, el SEPE fue víctima de un ataque de *ransomware* que inhabilitó temporalmente sus sistemas informáticos en plena pandemia. Este incidente provocó retrasos en la gestión de citas, pagos y trámites de desempleo, afectando a miles de ciudadanos. El ataque evidenció la vulnerabilidad de las administraciones públicas españolas frente a ciberamenazas y la necesidad de invertir en sistemas de contingencia (CCN-CERT, 2023).

Hospital Clínic de Barcelona (2023): Ciberataque a infraestructuras sanitarias

En marzo de 2023, el Hospital Clínic de Barcelona sufrió un ciberataque masivo que afectó a sus sistemas clínicos, quirúrgicos y de urgencias. Los atacantes exigieron un rescate millonario, lo que fue rechazado por las autoridades sanitarias. Este caso alertó sobre la creciente exposición del sector sanitario a ataques digitales, especialmente críticos por su impacto directo en la salud de los pacientes y la operatividad de servicios vitales (INCIBE, 2023).

Caso "Mariposa Botnet" (2009): Uno de los primeros casos de ciberdelincuencia organizada desde España

Tres ciudadanos españoles fueron detenidos por controlar una red de bots que infectó más de 13 millones de ordenadores a nivel mundial. Esta botnet fue utilizada para robar datos bancarios,

cometer fraudes financieros y distribuir *malware*. El caso representó un hito en la lucha contra la ciberdelincuencia internacional coordinada desde territorio español (Guardia Civil, 2010).

Estos casos reflejan la diversidad de objetivos, estrategias y consecuencias asociadas a los ciberataques, así como la urgencia de desarrollar políticas de prevención adaptadas a los retos del entorno digital. Analizar sus causas, respuestas institucionales y repercusiones sociales permite identificar debilidades y oportunidades de mejora en el sistema de ciberseguridad tanto en España como a nivel global.

3. METODOLOGÍA

3.1. Enfoque metodológico

La presente investigación adopta un enfoque cualitativo, centrado en el análisis documental, jurídico y de casos reales, con el objetivo de comprender la evolución, tipologías y desafíos del fenómeno de la ciberdelincuencia en España. Este enfoque se apoya en fuentes cuantitativas secundarias como estadísticas oficiales, pero no aplica técnicas propias de la investigación cuantitativa, por lo que no se considera una metodología mixta en sentido estricto.

Las herramientas metodológicas empleadas en el estudio han sido las siguientes:

1. Revisión de literatura especializada, que ha permitido construir el marco teórico y contextualizar el fenómeno. Esta revisión se ha desarrollado a partir de fuentes académicas primarias y secundarias, seleccionadas por su actualidad, rigor científico y relevancia temática, procedentes de bases de datos como Scopus, Google Scholar, Dialnet y el catálogo de la Biblioteca de la Universidad Europea.

2. Análisis documental, basado en informes técnicos, memorias institucionales y estadísticas publicadas por organismos nacionales e internacionales como el Ministerio del Interior, el Instituto Nacional de Estadística (INE), el Instituto Nacional de Ciberseguridad (INCIBE), Europol y ENISA. Este análisis ha sido clave para detectar patrones delictivos, identificar tendencias emergentes y valorar la evolución del cibercrimen en la última década.

3. Estudio de casos reales, seleccionados de forma intencionada por su relevancia representativa en el contexto español y europeo. Estos casos han permitido ilustrar situaciones concretas de ciberdelincuencia, analizar fallos de seguridad, respuestas institucionales y efectos sobre las víctimas, aportando profundidad interpretativa al estudio.

4. Análisis jurídico, a través de la interpretación de normas, tratados y directivas relevantes, como el Código Penal español (reforma de 2015), la Convención de Budapest, la Directiva NIS2 y el Reglamento General de Protección de Datos (RGPD). Esta herramienta ha permitido evaluar la adecuación y eficacia del marco normativo frente a los retos actuales de la criminalidad digital.

5. Representación visual de resultados, mediante la elaboración de figuras, esquemas y gráficos informativos diseñados con el software Canva, con el fin de sintetizar y comunicar de forma clara los hallazgos principales del trabajo.

Este enfoque metodológico permite desarrollar un análisis riguroso, crítico e integral del objeto de estudio, abordando sus múltiples dimensiones criminológica, legal, tecnológica y social, en coherencia con los objetivos planteados.

3.2. Diseño y estrategia de investigación

El diseño adoptado es de tipo no experimental, descriptivo y explicativo, basado en el análisis de información secundaria. La investigación no implica intervención directa sobre los sujetos ni recolección de datos primarios, sino que se fundamenta en la observación, selección y análisis de contenidos ya publicados.

La estrategia metodológica combina dos niveles de análisis complementarios:

•Un análisis transversal, centrado en la situación actual de la ciberdelincuencia en España, a través de la revisión de estadísticas recientes, informes institucionales y casos actuales.

•Un análisis longitudinal, que permite examinar la evolución del fenómeno a lo largo de la última década (2013–2023), identificando cambios estructurales, nuevas tipologías delictivas y transformaciones en los perfiles de los ciberdelincuentes.

Además, se ha desarrollado un análisis cualitativo de casos emblemáticos, cuya selección responde a criterios de relevancia temática, impacto mediático y valor ilustrativo. Estos casos constituyen unidades de análisis que permiten profundizar en la comprensión del fenómeno y evaluar críticamente las respuestas institucionales.

Por último, el análisis jurídico-normativo se ha integrado como eje interpretativo, permitiendo contrastar el marco legal vigente con las realidades empíricas y doctrinales del cibercrimen. Esta dimensión normativa es esencial para identificar vacíos legislativos, evaluar la adaptación de las leyes al contexto digital y proponer recomendaciones de mejora.

Este diseño responde a la necesidad de abordar un fenómeno complejo, dinámico y multifactorial, a través de una estrategia investigadora flexible, crítica e interdisciplinar.

3.3. Revisión bibliográfica (fuentes académicas y organismos oficiales)

La revisión bibliográfica ha sido un componente clave para establecer los fundamentos teóricos y empíricos del estudio. Se ha llevado a cabo una revisión de literatura especializada, priorizando la calidad, actualidad y pertinencia de las fuentes.

En el ámbito académico, se han consultado libros, artículos científicos, tesis doctorales y trabajos de investigación relacionados con la criminología digital, la ciberseguridad, el derecho penal tecnológico y la sociología del delito. Autores como David Wall, Susan Brenner, Michael Maras, Holt y Bossler han sido referentes fundamentales en la construcción del marco teórico.

En el ámbito institucional, se han analizado informes y estudios técnicos publicados por organismos como el Ministerio del Interior, INE, INCIBE, CCN-CERT, Europol, INTERPOL y

ENISA. Estas fuentes aportan datos estadísticos, diagnósticos de amenazas y recomendaciones estratégicas de alto valor empírico.

Asimismo, se ha incorporado el análisis de marcos jurídicos relevantes, como el Código Penal español, la Convención de Budapest, la Directiva NIS2 y el RGPD, con el fin de contextualizar legalmente el objeto de estudio.

La selección de fuentes ha seguido criterios rigurosos de fiabilidad, autoridad científica, actualidad y pertinencia temática. Se han descartado contenidos no verificados o duplicados, y se ha utilizado como soporte documental bases de datos como Scopus, Google Scholar, Dialnet y el catálogo de la Biblioteca de la Universidad Europea.

Esta revisión ha permitido identificar vacíos en el conocimiento, contrastar enfoques doctrinales y fundamentar los objetivos e hipótesis con base en evidencias contrastadas y verificables

3.4. Análisis de casos reales de cibercrimen *(ransomware, phishing,* fraude digital, etc.)

El análisis de casos reales constituye una parte esencial del componente cualitativo de esta investigación, ya que permite ilustrar, con ejemplos concretos, la diversidad de formas que adopta la ciberdelincuencia, así como sus consecuencias a nivel individual, institucional y social. A través de la observación de hechos verificados, se busca comprender cómo operan los ciberdelincuentes, qué vulnerabilidades aprovechan, cómo responden las autoridades y qué impacto generan en las víctimas.

Para ello, se ha seleccionado una muestra intencionada de casos emblemáticos, tanto de ámbito nacional como internacional, recogidos en el marco teórico de este trabajo. Entre ellos se encuentran ataques como “WannaCry” (2017), el ciberataque al Hospital Clínic de Barcelona (2023), el incidente contra el SEPE (2021) o el caso del grupo REvil, especializado en *ransomware*. Estos eventos han sido documentados a través de fuentes oficiales, informes técnicos, prensa especializada y literatura académica, garantizando la veracidad y relevancia de los datos analizados.

Cada caso ha sido estudiado a partir de varios criterios: el tipo de delito cometido (*ransomware, phishing*, fraude financiero, sabotaje informático, filtración de datos, etc.), el perfil de los agresores, los objetivos del ataque, las herramientas tecnológicas utilizadas, las consecuencias generadas y la respuesta institucional o empresarial ante el incidente. Esta metodología ha permitido establecer patrones de conducta comunes, así como detectar vulnerabilidades recurrentes en los sistemas de ciberseguridad.

El análisis de casos reales no solo ofrece una perspectiva concreta del fenómeno, sino que también contribuye al desarrollo de una visión crítica respecto a las estrategias de prevención y mitigación actualmente vigentes. Asimismo, permite contextualizar las cifras estadísticas y vincular los datos cuantitativos con situaciones reales que afectan directamente a ciudadanos, empresas y administraciones públicas.

Esta aproximación cualitativa enriquece la investigación al aportar profundidad interpretativa, facilitar la triangulación metodológica con los datos estadísticos y apoyar el contraste empírico de las hipótesis planteadas.

Para el análisis cualitativo, se seleccionaron seis casos emblemáticos de cibercrimen ocurridos entre 2017 y 2023, tanto en el contexto internacional como nacional. Los criterios de selección fueron:

•Relevancia mediática y jurídica.
•Diversidad tipológica (ransomware, phishing, filtración de datos, etc.).
•Impacto social, institucional o económico.
•Accesibilidad a fuentes verificadas y contrastables.

Los casos fueron analizados mediante un enfoque descriptivo-interpretativo, orientado a identificar patrones comunes, brechas de seguridad explotadas, y consecuencias institucionales o ciudadanas. Se priorizó la fiabilidad de la información, recurriendo a fuentes oficiales y reportes de ciberseguridad ampliamente reconocidos.

A continuación, se presenta una tabla que resume los casos reales de ciberdelincuencia analizados en esta investigación, seleccionados por su impacto, relevancia institucional y grado de sofisticación técnica. Se incluyen tanto casos nacionales como internacionales, lo que permite una visión más completa del fenómeno.

Figura 9

Casos reales representativos de ciberdelincuencia internacional

ANÁLISIS DE CASOS REALES DE CIBERCRIMEN

CASO	AÑO	PAÍS	TIPO DE CIBERDELLITO	AFECTADOS	FUENTE
Operación Mariposa	2010	España	Malware	Más de 13 millonen	BBC News
Sony Pictures hackeo	2014	Estados Unido	Ransomware	Empleacioss y clientes	The Washinggton
Estafa electoral en EEUU	2016	Estados Unido	Phishing	Votantes	Cybercrime Magazine
Robo en City Banco	2018	México	Fraude financieros	Instituciones financieras	Reuters
Filtración de datos en Facebook	2021	Estados Unido	Data breacn	Más de 53Q millon usuarios	El País
COFIDES sextorsiön	2022	España	Sextorsión	Estudiantes universitarios	ABC

Nota. Elaboración propia mediante Canva, Madrid, 2025. La tabla recoge distintos casos reales de cibercrimen clasificados por año, país, modalidad delictiva, víctimas y fuente de información.

3.5. Análisis estadístico de datos sobre incidencia del cibercrimen en España

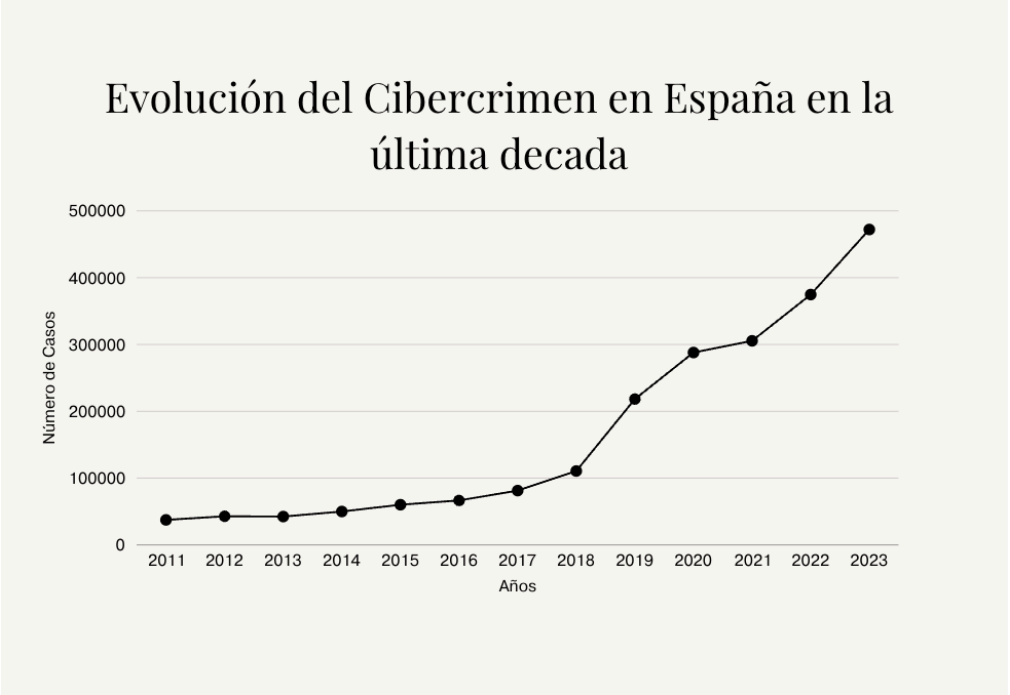
El componente cuantitativo de esta investigación se basa en el análisis de datos estadísticos relativos a la evolución, tipología y prevalencia de los ciberdelitos registrados en España durante la última década. Esta dimensión permite medir la magnitud del fenómeno, identificar tendencias delictivas y evaluar el impacto real del cibercrimen sobre la sociedad española desde una perspectiva empírica y verificable.

Para ello, se han recopilado datos procedentes de fuentes oficiales como el Ministerio del Interior, a través del Balance de Criminalidad y sus informes anuales sobre cibercriminalidad, el

Instituto Nacional de Estadística (INE), el Observatorio Español de Delitos Informáticos (OEDI), el Centro Criptológico Nacional (CCN-CERT) y el Instituto Nacional de Ciberseguridad (INCIBE). Estas entidades ofrecen información detallada sobre la evolución anual de los delitos informáticos, desagregada por tipo penal, comunidad autónoma, número de denuncias, tasa de resolución y perfil de las víctimas y agresores.

Figura 10

Evolución del cibercrimen en España entre 2011 y 2023



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico muestra el incremento anual del número de delitos informáticos registrados en España en la última década

El análisis se ha centrado en variables clave como el incremento porcentual de los delitos de fraude informático, el crecimiento de las denuncias por suplantación de identidad, la distribución geográfica de los ciberdelitos y el impacto de fenómenos globales como la pandemia de COVID-19 en la actividad delictiva digital. También se han considerado informes de Europol e INTERPOL, con el fin de situar los datos españoles en el contexto europeo y observar si las tendencias nacionales coinciden con las del resto del continente.

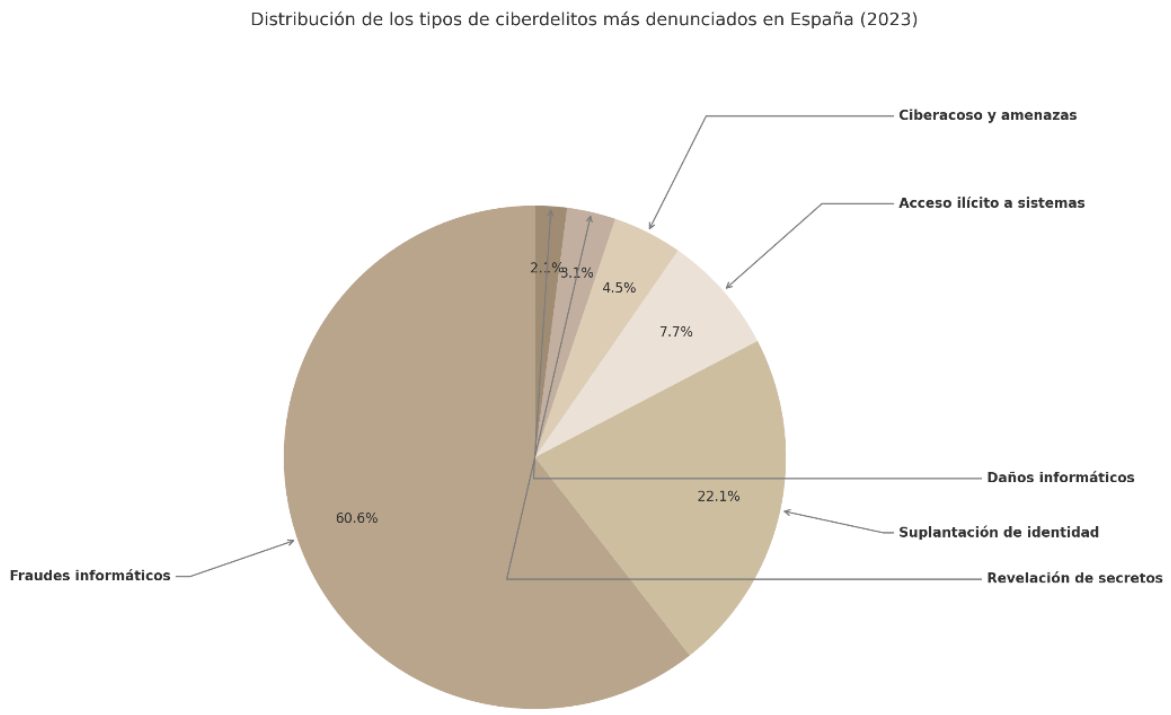
Los datos recopilados han sido procesados y representados en forma de tablas y gráficos explicativos, lo que facilita su interpretación y contribuye a la identificación de patrones delictivos relevantes. Este análisis cuantitativo permite, además, establecer correlaciones entre el aumento de determinadas tipologías de ciberdelitos y factores de riesgo como la expansión del comercio electrónico, el teletrabajo, la digitalización de servicios públicos o la falta de concienciación en ciberseguridad por parte de la ciudadanía.

En cuanto al componente cuantitativo, se recopilaron datos estadísticos de fuentes públicas como el Ministerio del Interior (Balance de Criminalidad 2023 y 2024), el INE, INCIBE y Eurostat. Estos datos fueron utilizados para observar la evolución temporal del cibercrimen en España entre 2013 y 2023, centrándose en variables como el número de denuncias, tipos de delitos más frecuentes, sectores más afectados y nivel de resolución judicial. El análisis se centró en la identificación de tendencias, cambios porcentuales y correlaciones básicas, sin aplicar técnicas estadísticas inferenciales complejas, dado el carácter exploratorio del estudio.

Este apartado ofrece una base sólida para contrastar las hipótesis del trabajo y para respaldar las conclusiones con evidencia empírica. Asimismo, contribuye a fundamentar propuestas de mejora en la prevención, persecución y respuesta institucional frente al cibercrimen en España, adaptadas a las necesidades reales detectadas mediante el análisis de datos.

Figura 11

Distribución de los tipo de ciberdelitos más denunciados en España (2023)



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico muestra los porcentajes de ciberdelitos más frecuentes registrados en España según datos de 2023.

3.6. Consideraciones éticas

Este trabajo ha sido elaborado respetando los principios éticos fundamentales que guían la investigación en el ámbito de las ciencias sociales y jurídicas. Aunque no se ha requerido la participación directa de personas, ya que el estudio se basa en fuentes secundarias y documentales, se ha manejado información relativa a delitos reales, víctimas y datos institucionales, lo que exige un tratamiento responsable y respetuoso.

En primer lugar, se ha velado por la confidencialidad y el anonimato de las personas implicadas en los casos analizados. Todos los datos han sido extraídos de fuentes oficiales, académicas y periodísticas verificadas, y se ha evitado cualquier uso de información que pudiera identificar o revictimizar a afectados por ciberdelitos. El enfoque ha sido estrictamente analítico, sin juicios morales ni descripciones morbosas.

Asimismo, se ha respetado el principio de propiedad intelectual, aplicando el sistema de citación APA 7 en todo el trabajo para garantizar la trazabilidad de las fuentes utilizadas y reconocer el aporte de los autores consultados. No se ha recurrido a contenidos anónimos, no contrastados o provenientes de medios poco fiables.

Desde una perspectiva más amplia, esta investigación se compromete con el principio de responsabilidad social, promoviendo un uso ético del conocimiento y orientando sus resultados hacia la mejora de las políticas públicas, la protección de los derechos digitales y la concienciación sobre los riesgos asociados a la delincuencia en el ciberespacio. En este sentido, el trabajo contribuye de forma directa al cumplimiento del Objetivo de Desarrollo Sostenible (ODS) 16 de la Agenda 2030 de Naciones Unidas, que promueve la paz, la justicia y la construcción de instituciones sólidas, transparentes y responsables, así como la reducción de la violencia y la criminalidad en todas sus formas, incluyendo aquellas que se manifiestan en entornos digitales.

Por último, se ha mantenido el compromiso con los principios de veracidad, objetividad y rigor científico, evitando sesgos intencionados o manipulaciones interpretativas. El análisis se ha desarrollado con base en datos contrastados, marcos teóricos consolidados y fuentes fiables, contribuyendo así a una comprensión ética y responsable del fenómeno de la ciberdelincuencia en el contexto español.

3.7. Limitaciones del estudio

Como toda investigación académica, este estudio reconoce ciertas limitaciones derivadas del alcance y la naturaleza del propio Trabajo de Fin de Grado, las cuales no invalidan sus resultados, pero sí marcan el marco desde el cual deben ser interpretados. En este sentido, las limitaciones aquí expuestas responden más a decisiones metodológicas conscientes que a deficiencias del proceso investigador.

En primer lugar, el trabajo se ha centrado en el análisis de fuentes secundarias, sin incluir entrevistas, encuestas o trabajo de campo directo. Esta elección responde tanto a criterios éticos como a la viabilidad del proyecto, y no pretende suplir estudios de campo, sino complementarlos desde una perspectiva documental, interpretativa y estadística. Aun así, se reconoce que la incorporación de voces expertas o testimonios directos podría haber enriquecido aún más el análisis, especialmente en lo relativo al impacto subjetivo de los ciberdelitos o la percepción institucional sobre su gestión.

Por otro lado, aunque se ha hecho un esfuerzo riguroso por recopilar y comparar datos estadísticos oficiales (proporcionados por el Ministerio del Interior, el INE, INCIBE o Europol), cabe señalar que algunas fuentes presentan limitaciones de acceso, actualización o desagregación, lo que ha obligado a complementar la información con informes complementarios y análisis de contexto. Este reto es común en el estudio de la ciberdelincuencia, ya que se trata de un fenómeno dinámico, transversal y en parte invisible debido al infraregistro.

También debe considerarse que el análisis de casos reales se ha limitado a una selección representativa, pero no exhaustiva. La intención no ha sido generalizar a partir de estos casos, sino ilustrar aspectos clave del fenómeno a través de ejemplos significativos que ayuden a contextualizar los datos y enriquecer la comprensión teórica.

Por último, es importante destacar que esta investigación se sitúa en un campo de conocimiento altamente cambiante, donde los avances tecnológicos, las nuevas tipologías delictivas y las reformas normativas evolucionan con rapidez. Por ello, se reconoce la necesidad de mantener una revisión constante del marco conceptual y empírico, algo que podrá abordarse en futuras líneas de investigación con mayor profundidad y alcance.

En resumen, estas limitaciones no restan validez a los hallazgos obtenidos, sino que definen con honestidad el marco desde el que se ha abordado el estudio, asegurando la transparencia, el rigor y la coherencia metodológica del proyecto.

3.8. Contraste de hipótesis

El contraste de hipótesis constituye una fase fundamental dentro del proceso metodológico, ya que permite verificar si las proposiciones teóricas formuladas encuentran respaldo en los datos empíricos y en el análisis documental desarrollado. Esta etapa refuerza la validez del trabajo, al permitir el tránsito de una formulación hipotética inicial hacia unas conclusiones contrastadas y sólidamente argumentadas.

La primera hipótesis plantea que “la ciberdelincuencia en España ha experimentado una transición desde delitos individuales de bajo impacto hacia formas más complejas, organizadas y orientadas a sectores estratégicos como el financiero, el sanitario o las infraestructuras críticas”. Esta afirmación encuentra respaldo en informes como los del Ministerio del Interior (2023), el Observatorio Español de Delitos Informáticos (OEDI) y el CCN-CERT (2023), que reflejan un incremento notable de ciberataques dirigidos a entidades institucionales, financieras y sanitarias, destacando especialmente el uso de ransomware y suplantación de identidad a gran escala. Casos como el ataque al SEPE en 2021 o al Hospital Clínic de Barcelona en 2023 constituyen ejemplos ilustrativos de esta transformación. Además, autores como Holt y Bossler (2020) sostienen que esta evolución responde a una progresiva profesionalización del delito digital, que ha pasado de ser una actividad individual a una forma de crimen organizado transnacional.

La segunda hipótesis sostiene que “factores como el aumento del acceso a internet, la falta de formación en ciberseguridad, la adopción masiva de nuevas tecnologías sin regulación suficiente y la escasa cultura de protección digital han contribuido de forma significativa a la expansión de la ciberdelincuencia en España”. Esta proposición se ve confirmada por la literatura especializada, que identifica una clara correlación entre la digitalización acelerada de la sociedad y la multiplicación de vulnerabilidades. Autores como Maras (2020) y Wall (2021) advierten que la insuficiente

concienciación ciudadana y empresarial respecto a los riesgos digitales facilita delitos como el phishing, la interceptación de datos personales y el fraude electrónico. El Informe IOCTA de Europol (2023) subraya que esta tendencia se intensificó durante la pandemia de COVID-19, cuando muchas instituciones y empresas adoptaron entornos digitales sin contar con una infraestructura de seguridad adecuada.

La tercera hipótesis afirma que "las políticas y programas actuales presentan deficiencias en cuanto a cooperación internacional, actualización legislativa y formación especializada, lo que limita su eficacia frente a una amenaza en constante evolución". Esta hipótesis se confirma de forma parcial. Si bien España ha implementado avances importantes en el ámbito normativo como la reforma del Código Penal en 2015 y su adhesión a la Directiva NIS2 y a la Convención de Budapest, persisten importantes retos operativos. Diversos informes del INCIBE (2023) y del CCN-CERT alertan sobre la falta de recursos humanos especializados, la dispersión institucional y la limitada agilidad en los mecanismos de cooperación judicial internacional, especialmente ante delitos cometidos por redes transnacionales altamente tecnificadas, como REvil o LockBit (Navarro-Torres, 2022).

En conjunto, el contraste de hipótesis corrobora de forma coherente y argumentada la validez de los planteamientos iniciales. La triangulación entre análisis documental, datos estadísticos y casos reales ha permitido confirmar las hipótesis con distintos niveles de intensidad, aportando una base empírica sólida sobre la que se sustentan las conclusiones y propuestas de mejora que se desarrollarán en los bloques finales del presente trabajo.

4. ANÁLISIS DE RESULTADOS

4.1. Análisis de los principales hallazgos

El análisis de los datos recopilados, tanto desde el enfoque cuantitativo como cualitativo, ha permitido identificar una serie de hallazgos clave que confirman y matizan las hipótesis formuladas en esta investigación. En primer lugar, los datos estadísticos oficiales evidencian un crecimiento sostenido de la ciberdelincuencia en España durante la última década, con un aumento particularmente significativo en los delitos de fraude informático, suplantación de identidad y ataques mediante *ransomware*. Este incremento ha sido paralelo a la expansión de la digitalización en todos los sectores de la sociedad, lo que refuerza la hipótesis de que los delitos han evolucionado hacia formas más complejas y de mayor impacto, especialmente dirigidas a infraestructuras críticas y servicios estratégicos (Ministerio del Interior, 2023; CCN-CERT, 2023).

Desde una perspectiva cualitativa, el análisis de casos reales como los ataques sufridos por el SEPE o el Hospital Clínic de Barcelona confirma la sofisticación creciente de los ciberataques, así como la especial vulnerabilidad de organismos públicos y entidades del ámbito sanitario. Estos casos ilustran con claridad cómo la ciberdelincuencia ha superado el ámbito de lo individual para convertirse en una amenaza sistémica con capacidad de generar disrupciones a gran escala (INCIBE, 2023).

Otro hallazgo relevante es la identificación de múltiples factores que favorecen la expansión del cibercrimen, entre los que destacan la insuficiente formación en ciberseguridad, el bajo nivel de concienciación de los usuarios, la rápida adopción de tecnologías sin acompañamiento regulatorio adecuado y la facilidad de acceso a herramientas delictivas en la dark web. Estas condiciones han sido

ampliamente documentadas por autores como Wall (2021) y Maras (2020), y se ven reforzadas por el marco teórico presentado en este trabajo.

Asimismo, los datos muestran que, si bien existen esfuerzos institucionales relevantes para prevenir y mitigar el impacto del cibercrimen como la reforma del Código Penal de 2015, el desarrollo del Plan Nacional de Ciberseguridad o la implementación de la Directiva NIS2, todavía persisten importantes debilidades en términos de cooperación internacional, actualización legislativa efectiva y dotación de recursos especializados. Esto confirma parcialmente la tercera hipótesis, en la medida en que las estrategias actuales presentan avances formales, pero limitaciones operativas y estructurales que afectan su eficacia (INCIBE, 2023; Navarro-Torres, 2022).

En síntesis, los principales hallazgos de esta investigación apuntan a una tendencia de profesionalización y complejidad del cibercrimen en España, impulsada por factores estructurales y tecnológicos, y enfrentada a una respuesta institucional que, si bien ha mejorado, todavía requiere adaptarse a un entorno digital en constante transformación.

4.2. Patrones y tendencias identificadas

El análisis de los datos disponibles, tanto estadísticos como documentales, ha permitido identificar una serie de patrones y tendencias significativas en relación con la evolución de la ciberdelincuencia en España durante el periodo comprendido entre 2013 y 2023. Estos patrones no solo aportan una visión dinámica del fenómeno, sino que también permiten anticipar posibles escenarios futuros y señalar puntos críticos en la prevención y gestión del delito digital.

Uno de los primeros patrones observados es la tendencia sostenida al alza en la incidencia de ciberdelitos a nivel nacional. Según los informes del Ministerio del Interior (2023) y del Observatorio Español de Delitos Informáticos (OEDI, 2022), el número de denuncias relacionadas con delitos informáticos ha aumentado de forma continua, con picos destacados durante los años 2020 y 2021, coincidiendo con la aceleración de la digitalización como consecuencia de la pandemia de COVID-19. Esta progresión evidencia no solo una mayor actividad delictiva, sino también una posible mejora en los mecanismos de detección y denuncia, aunque aún limitada.

En cuanto a las tipologías predominantes, se consolida el dominio del fraude informático, seguido por la suplantación de identidad y los delitos de acceso ilícito a sistemas. Esta regularidad se mantiene en prácticamente todas las comunidades autónomas, lo que indica un patrón de afectación generalizado, independientemente del contexto territorial o del grado de desarrollo digital. Paralelamente, los delitos de ransomware y extorsión digital han mostrado un crecimiento notable en los últimos cinco años, especialmente en ataques dirigidos contra infraestructuras críticas y entidades del sector público (CCN-CERT, 2023; INCIBE, 2023).

Otro patrón destacable es el uso sistemático de ingeniería social como medio de acceso inicial a los sistemas o a la información de las víctimas. Prácticas como el phishing, el smishing o el vishing se repiten con frecuencia, adaptándose a las tendencias tecnológicas y contextuales del momento. Esto revela una evolución en las estrategias delictivas, que se vuelven cada vez más personalizadas, automatizadas y difíciles de detectar en fases tempranas (Maras, 2020).

En términos de víctimas, se observa una tendencia creciente hacia la diversificación de objetivos. Aunque en años anteriores el cibercrimen se centraba mayoritariamente en usuarios

particulares, en la actualidad se dirigen con mayor frecuencia ataques contra instituciones públicas, hospitales, empresas tecnológicas, y entidades financieras. Este desplazamiento en los objetivos sugiere una profesionalización del delito digital y una clara priorización del rendimiento económico por parte de los atacantes, tal como señala Wall (2021).

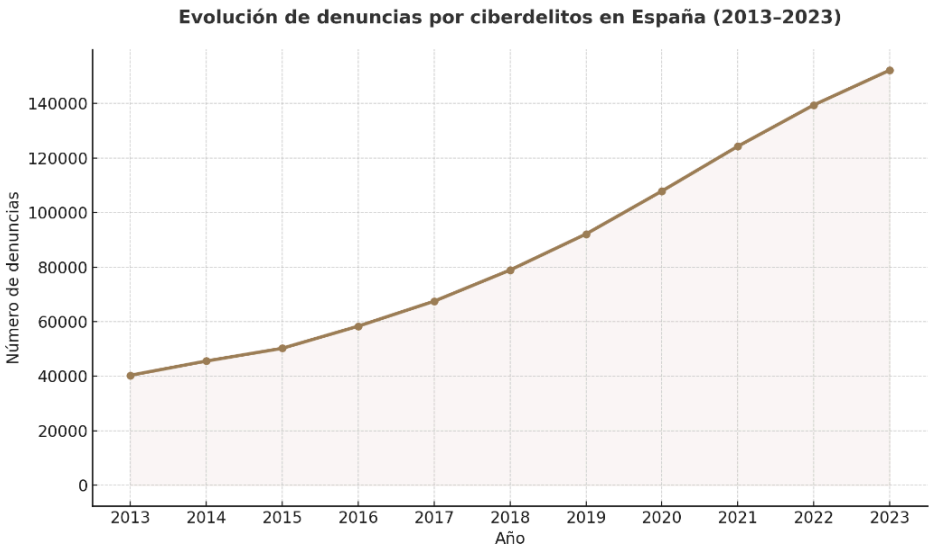
También se ha detectado un patrón de reutilización y mutación de herramientas delictivas. Muchas campañas de ciberataques replican malware ya existente con ligeras modificaciones que permiten eludir las medidas de detección convencionales. Este fenómeno, vinculado al modelo de negocio del Crime-as-a-Service (CaaS), pone de manifiesto una tendencia a la especialización del delito digital, en el que los atacantes se convierten en clientes de servicios ilegales ofertados en la dark web (Europol, 2023).

Por último, se aprecia una tendencia creciente a la internacionalización del ciberdelito. Gran parte de los ataques dirigidos a entidades españolas tienen su origen en servidores o redes ubicadas en terceros países, lo que dificulta la persecución penal y ralentiza las respuestas institucionales. Esta globalización del delito digital demanda una cooperación internacional más ágil, coordinada y eficaz, una necesidad ya expresada por organismos como INTERPOL y el Consejo de Europa.

En conjunto, los patrones y tendencias identificados confirman que la ciberdelincuencia no es un fenómeno aleatorio ni puntual, sino un problema estructurado, en expansión y con una clara evolución en sus métodos, objetivos y consecuencias. Estas regularidades deben ser tenidas en cuenta para el diseño de estrategias preventivas más eficaces y adaptativas.

Figura 12

Evolución de denuncias por ciberdelitos en España (2013–2023)



Nota. Elaboración propia mediante Canva, Madrid, 2025. El gráfico muestra el crecimiento anual en el número de denuncias por ciberdelitos en España durante la última década.

4.3. Comparación de legislación y respuestas gubernamentales

La evolución del cibercrimen en España ha obligado a las instituciones a adaptar su marco jurídico y sus estrategias de intervención para hacer frente a nuevas formas de delincuencia digital. En este contexto, es necesario analizar comparativamente las principales medidas legislativas y respuestas gubernamentales implementadas tanto a nivel nacional como internacional, con el fin de valorar su eficacia, coherencia y capacidad de adaptación ante un fenómeno en constante transformación.

Desde el plano legislativo, España ha realizado avances significativos en los últimos años. La reforma del Código Penal de 2015 introdujo nuevos tipos delictivos vinculados al uso fraudulento de tecnologías de la información, como el acceso ilícito a sistemas, la interceptación de comunicaciones electrónicas o la alteración de datos informáticos. Asimismo, se incorporaron disposiciones específicas sobre delitos de sexting, grooming y distribución de contenidos ilegales en línea, lo que supuso una ampliación del espectro normativo en relación con la criminalidad digital (Gobierno de España, 2015).

En paralelo, España ha adoptado la Directiva NIS2 (2022), de obligado cumplimiento en el marco de la Unión Europea, orientada a mejorar la ciberseguridad en operadores de servicios esenciales, plataformas digitales y entidades públicas. Esta directiva refuerza las obligaciones de reporte de incidentes, auditoría de sistemas y protección de infraestructuras críticas, así como la cooperación entre Estados miembros en materia de ciberseguridad (Parlamento Europeo y Consejo de la UE, 2022).

En cuanto a protección de datos, el Reglamento General de Protección de Datos (RGPD), aplicado desde 2018, ha marcado un hito en la regulación del tratamiento de información personal en el ámbito digital, imponiendo sanciones severas a quienes no garanticen la seguridad de los datos que gestionan. Esta norma europea ha sido incorporada al ordenamiento español mediante la Ley Orgánica 3/2018, de protección de datos personales y garantía de derechos digitales (Unión Europea, 2016).

No obstante, a pesar de estos avances normativos, existen diferencias notables entre la legislación española y la de otros países en cuanto a la agilidad de respuesta, la especialización judicial y la dotación de recursos técnicos. Por ejemplo, países como Estonia, Finlandia o los Países Bajos han desarrollado estrategias de ciberseguridad mucho más integradas y proactivas, que incluyen centros de respuesta a incidentes 24/7, unidades policiales altamente especializadas y plataformas de cooperación público-privada que permiten la detección temprana de amenazas (ENISA, 2023).

Además, mientras que en algunos países europeos existen tribunales especializados en delitos informáticos, en España los casos de ciberdelincuencia suelen tramitarse en juzgados ordinarios, lo que ralentiza los procedimientos y limita la capacidad del sistema judicial para abordar delitos con alta carga técnica. A esto se suma la dispersión competencial entre distintos organismos (Policía Nacional, Guardia Civil, INCIBE, CCN-CERT), lo que a menudo genera duplicidades, solapamientos y falta de coordinación efectiva (INCIBE, 2023).

A nivel internacional, la Convención de Budapest sobre Ciberdelincuencia (2001) sigue siendo el principal instrumento jurídico multilateral en esta materia. España es parte de este tratado, lo que facilita la cooperación judicial con otros países firmantes. Sin embargo, la ausencia de actores clave como Rusia o China en este marco limita su alcance, especialmente en lo relativo a la

persecución de ataques transnacionales y al rastreo de redes criminales globales (Consejo de Europa, 2001).

En definitiva, aunque el ordenamiento jurídico español ha avanzado en la incorporación del cibercrimen y la ciberseguridad en su legislación, aún se encuentra por detrás de otros modelos europeos más consolidados. Las respuestas gubernamentales, si bien bien orientadas en términos estratégicos, requieren mayor especialización técnica, inversión sostenida en ciberdefensa y una mejor articulación entre actores públicos y privados.

4.4. Impacto en las víctimas según datos recogidos

El impacto del cibercrimen sobre las víctimas va mucho más allá de la pérdida económica inmediata. Los datos analizados y la bibliografía especializada coinciden en señalar que los efectos de estos delitos se extienden a niveles psicológicos, sociales y, en ocasiones, institucionales, generando consecuencias profundas en los individuos y en la confianza colectiva en los entornos digitales.

Desde el punto de vista económico, los fraudes en línea, la suplantación de identidad y el ransomware generan importantes pérdidas tanto para ciudadanos como para empresas e instituciones. Según datos del Ministerio del Interior (2023), más del 85% de las denuncias por ciberdelito en España están relacionadas con delitos patrimoniales, lo que refleja la alta rentabilidad que estos crímenes suponen para los atacantes. En muchos casos, las víctimas particulares no logran recuperar el dinero perdido, y las empresas deben destinar recursos considerables a mitigar los daños, restaurar sus sistemas y proteger su reputación.

En el plano psicológico, los efectos son igualmente alarmantes. Las víctimas de ciberacoso, sextorsión o robo de datos personales manifiestan elevados niveles de ansiedad, miedo, impotencia y, en algunos casos, trastornos depresivos. El informe del INCIBE (2023) destaca que un porcentaje creciente de afectados especialmente entre menores y jóvenes experimenta síntomas de aislamiento social y deterioro de la autoestima como consecuencia de la exposición digital no consentida o la amenaza constante de chantaje. Este tipo de impacto tiende a ser invisible en los datos estadísticos, pero resulta clave en la comprensión integral del fenómeno.

A nivel social, uno de los efectos más frecuentes es la pérdida de confianza en los entornos digitales. Muchas víctimas de fraudes o accesos no autorizados a sus cuentas se muestran reacias a seguir realizando trámites o compras por internet, lo que limita su integración plena en la vida digital. Esta desconfianza afecta también a la percepción que la ciudadanía tiene sobre la capacidad del Estado y de las empresas para garantizar su seguridad online, generando una sensación de vulnerabilidad generalizada (Wall, 2021; Maras, 2020).

En el ámbito institucional, los ciberataques a hospitales, universidades, ayuntamientos o agencias de empleo han tenido consecuencias especialmente graves. El caso del SEPE en 2021, por ejemplo, interrumpió servicios esenciales a miles de ciudadanos, y el ataque al Hospital Clínic de Barcelona en 2023 obligó a suspender cirugías y consultas, afectando tanto al personal sanitario como a los pacientes. Estos eventos no solo tienen un coste económico alto, sino que también erosionan la credibilidad de las instituciones y generan alarma social.

Otro aspecto preocupante es el bajo índice de denuncias, especialmente en delitos como el ciberacoso, el chantaje o la sextorsión. Factores como la vergüenza, el miedo a la exposición pública o

la desconfianza en la eficacia del sistema judicial contribuyen a que muchas víctimas no informen de lo ocurrido, lo que dificulta su protección y la persecución del delito (Navarro-Torres, 2022).

En definitiva, el impacto del cibercrimen es multidimensional y afecta de forma desigual según el tipo de delito, la vulnerabilidad de la víctima y el contexto en el que se produce. Comprender estas dimensiones es fundamental para diseñar estrategias más humanas, integrales y eficaces de prevención, asistencia y reparación.

4.5. Análisis de eficacia de las medidas de prevención

La prevención del cibercrimen constituye uno de los grandes retos de la política criminal contemporánea. A lo largo de esta investigación se han identificado múltiples estrategias impulsadas tanto por el sector público como por el privado en España. Sin embargo, el análisis realizado pone de manifiesto que, si bien existen avances en la formulación de políticas y marcos regulatorios, su aplicación práctica presenta limitaciones importantes que condicionan su eficacia real.

En el plano institucional, organismos como el INCIBE, el Centro Criptológico Nacional (CCN-CERT) o el Ministerio del Interior han desarrollado campañas de concienciación, sistemas de alerta temprana, protocolos de actuación frente a incidentes y programas de formación para usuarios y profesionales. También se han implementado líneas de financiación pública para reforzar la ciberseguridad en pymes y administraciones locales. Estas acciones han tenido un impacto positivo en términos de visibilización del problema y de mejora progresiva en la detección de amenazas (INCIBE, 2023).

No obstante, estos esfuerzos presentan ciertos límites estructurales. Uno de los principales es la fragmentación entre organismos, lo que produce duplicidades de funciones, falta de coordinación interinstitucional y una respuesta reactiva más que preventiva. A ello se suma la escasez de profesionales especializados en ciberseguridad, tanto en el ámbito técnico como en el jurídico, lo que ralentiza la capacidad de respuesta ante amenazas complejas o ataques de gran escala (CCN-CERT, 2023).

Desde la perspectiva legislativa, aunque la reforma del Código Penal de 2015 y la implementación de directivas europeas como la NIS2 han supuesto avances normativos importantes, estos no siempre se traducen en una aplicación efectiva. En muchos casos, la falta de adaptación del poder judicial al contexto tecnológico dificulta la persecución penal del cibercrimen, especialmente cuando se trata de delitos transnacionales o de carácter técnico elevado (Wall, 2021; Navarro-Torres, 2022).

Las iniciativas privadas, por su parte, han comenzado a incorporar medidas de seguridad más robustas en sectores sensibles como la banca o el comercio electrónico, incluyendo autenticación multifactor, detección de fraude en tiempo real y protocolos de cifrado de datos. Sin embargo, muchas pequeñas y medianas empresas continúan sin implementar mecanismos básicos de ciberseguridad, ya sea por desconocimiento, falta de recursos o baja percepción del riesgo.

En cuanto a la educación digital, se ha detectado un déficit estructural en la formación del conjunto de la población, especialmente en colectivos vulnerables como personas mayores, jóvenes y trabajadores no especializados en tecnología. Las campañas de sensibilización impulsadas por el

Estado han sido útiles, pero intermitentes y poco integradas en el sistema educativo, lo que limita su sostenibilidad y alcance real (Maras, 2020; Europol, 2023).

Por todo lo anterior, puede afirmarse que las medidas de prevención actualmente en vigor han generado ciertos avances formales, pero presentan deficiencias sustanciales en términos de implementación, coordinación y eficacia. Este análisis confirma parcialmente la hipótesis 3 del estudio, y pone de manifiesto la necesidad de avanzar hacia un modelo de prevención más integral, transversal y proactivo, que combine tecnología, formación, legislación y cooperación internacional.

Figura 13

Evaluación de la eficacia de medidas de prevención frente al cibercrimen en España

Eficacia de las medidas de prevención frente al cibercrimen en España

Medida	Institución responsable	Nivel de eficacia	Obstáculos principales
Campañas de concienciación pública	INCIBE / Ministerio del Interior	Media	Baja continuidad e impacto desigual por segmentos
Directiva NIS2 (UE)	Unión Europea / Estados miembros	Alta	Falta de implementación total en todos los sectores
Reforma del Código Penal (2015)	Gobierno de España	Media	Desactualización frente a nuevas amenazas
Formación en ciberseguridad en empresas	Sector privado / INCIBE	Baja	Desigualdad de recursos entre empresas
Implementación de protocolos en sanidad pública	CCN-CERT / Consejerías de Salud	Baja	Falta de formación y presupuesto técnico

Nota. Elaboración propia mediante Canva, Madrid, 2025. La tabla compara distintas medidas de prevención en función de su eficacia, responsables institucionales y principales obstáculos.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Resumen de hallazgos

El desarrollo de esta investigación ha permitido alcanzar una visión global y estructurada de la evolución de la ciberdelincuencia en España, así como de sus principales manifestaciones, condicionantes y respuestas institucionales. A través de un análisis documental riguroso, el tratamiento de datos estadísticos actualizados y el estudio de casos representativos, se ha logrado construir una base empírica y teórica sólida que da respuesta a la pregunta de investigación formulada.

Uno de los hallazgos clave ha sido la reconfiguración del delito digital: se ha superado la etapa de acciones individuales esporádicas para dar paso a una estructura delictiva más compleja, profesionalizada y tecnológicamente avanzada. Este cambio ha venido acompañado por la aparición de modelos de negocio criminal como el ransomware-as-a-service y la venta de herramientas en la dark web, que han descentralizado y democratizado el acceso a recursos para delinquir en línea.

Otro resultado significativo es la identificación de factores estructurales que explican la vulnerabilidad del entorno digital, muchos de los cuales tienen carácter sistémico: la ausencia de una cultura preventiva sólida, la dispersión normativa, la falta de competencias digitales en la ciudadanía y la lentitud en la adaptación institucional a los cambios tecnológicos. Estos elementos, combinados, han contribuido a que el cibercrimen no solo se expanda, sino que también evolucione de forma acelerada y difícilmente predecible.

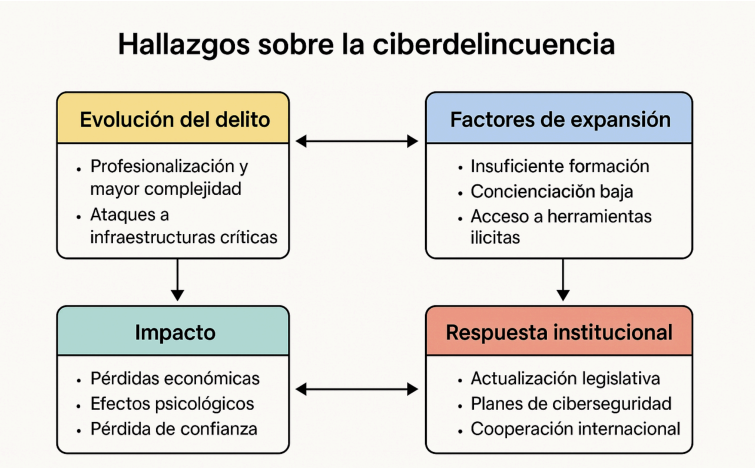
También se ha constatado que, aunque existen políticas y normativas diseñadas para hacer frente a esta problemática, su aplicación práctica enfrenta limitaciones que condicionan su impacto real. Las carencias en la especialización profesional, la falta de recursos humanos y la débil cooperación interinstitucional suponen obstáculos importantes para avanzar hacia una estrategia nacional de ciberseguridad verdaderamente eficaz y sostenible.

Por último, el estudio ha permitido visibilizar el impacto multidimensional del cibercrimen en las víctimas, una dimensión a menudo relegada en los análisis técnicos. Las consecuencias psicológicas, sociales y económicas que sufren los afectados tanto individuos como organizaciones reflejan la urgencia de abordar el fenómeno desde una perspectiva transversal, que combine prevención, atención y reparación.

En suma, los hallazgos obtenidos subrayan la necesidad de un enfoque integral en la lucha contra el cibercrimen, que trascienda la mera actualización normativa y promueva una verdadera transformación institucional, educativa y cultural frente a los riesgos del entorno digital contemporáneo.

Figura 14

Síntesis de hallazgos sobre la ciberdelincuencia: evolución, causas, impacto y respuesta



Nota. Elaboración propia mediante Canva, Madrid, 2025. El esquema resume los principales hallazgos del estudio en torno a la evolución del delito, los factores que lo impulsan, su impacto y las respuestas institucionales.

5.2. Amplitud y limitaciones de la investigación

El presente trabajo ha ofrecido una aproximación amplia, documentada y actualizada al fenómeno de la ciberdelincuencia en el contexto español, abordando su evolución, sus causas estructurales, su impacto sobre las víctimas y la eficacia de las medidas implementadas para su prevención y control. Desde un enfoque metodológico cualitativo pero con apoyo en fuentes cuantitativas secundarias, se han combinado fuentes académicas, datos oficiales y casos reales para construir un análisis sólido y coherente con los objetivos planteados.

Entre los principales logros del estudio destaca la capacidad para sintetizar una gran diversidad de fuentes nacionales e internacionales, así como identificar patrones y tendencias comunes en la forma en que se manifiesta el delito digital en España. Igualmente, el trabajo ha logrado relacionar de forma articulada los objetivos, hipótesis y resultados, ofreciendo una visión integral del problema desde una perspectiva criminológica contemporánea.

No obstante, como toda investigación de carácter académico y de alcance limitado, el presente estudio presenta ciertas limitaciones que conviene reconocer. En primer lugar, la ausencia de trabajo de campo (entrevistas, encuestas o testimonios directos de víctimas o profesionales del ámbito) ha restringido el acceso a una dimensión más cualitativa y experiencial del fenómeno. Si bien se ha compensado mediante el análisis de casos reales ampliamente documentados, esta decisión metodológica ha supuesto una renuncia a la profundización en el plano subjetivo.

Asimismo, el estudio ha estado condicionado por la disponibilidad y actualización de los datos estadísticos oficiales. Si bien se ha trabajado con informes recientes del Ministerio del Interior, el INCIBE o el OEDI, en algunos casos no ha sido posible acceder a series completas ni a datos desagregados por región, perfil de víctima o tipología específica, lo cual podría haber aportado un mayor nivel de detalle al análisis cuantitativo.

Otra limitación viene dada por la naturaleza dinámica del objeto de estudio. La ciberdelincuencia es un fenómeno en constante evolución, que se transforma al ritmo de los avances tecnológicos. Esto implica que algunas de las tipologías, técnicas o herramientas analizadas en el trabajo podrían quedar parcialmente obsoletas en un corto periodo de tiempo, lo que exige una actualización continua tanto de la legislación como de la investigación académica.

Finalmente, es importante señalar que, si bien se han examinado con detalle las políticas públicas y las estrategias institucionales vigentes, no se ha realizado una evaluación empírica directa sobre su implementación o impacto específico, lo cual podría constituir una línea de investigación futura.

En resumen, esta investigación ha logrado ofrecer una visión amplia, crítica y fundamentada sobre la ciberdelincuencia en España, sin perder de vista las restricciones propias de un trabajo académico de fin de grado. Estas limitaciones no invalidan los resultados obtenidos, sino que delimitan el marco desde el cual deben ser interpretados, y sirven como punto de partida para futuras investigaciones más específicas, empíricas y transversales.

5.3. Futuras líneas de Investigación

Este Trabajo de Fin de Grado se ha desarrollado con un enfoque exploratorio, utilizando metodologías cualitativas para comprender la evolución y las tendencias actuales del cibercrimen. Este enfoque ha permitido identificar patrones y desafíos emergentes en el ámbito de la ciberseguridad.

Con el objetivo de profundizar en este campo, planeo cursar el próximo año el Máster Universitario en Ciberseguridad en la Universidad Politécnica de Madrid. Este programa proporciona una formación avanzada en técnicas de ciberataque, ciberdefensa y gestión de la ciberseguridad, aspectos fundamentales para abordar las amenazas actuales en el entorno digital.

Durante el desarrollo del Trabajo de Fin de Máster, mi intención es adoptar una metodología cuantitativa que complemente y amplíe los hallazgos obtenidos en este TFG. Para ello, se diseñará un cuestionario estructurado dirigido a una muestra representativa de la población española, con el propósito de:

- Cuantificar la incidencia de diferentes tipos de cibercrímenes en distintos segmentos demográficos.

- Evaluar el nivel de conocimiento y percepción de los ciudadanos sobre las amenazas cibernéticas.

- Identificar las medidas de seguridad más comúnmente adoptadas y su eficacia percibida.

La elección de una muestra amplia y diversa permitirá obtener datos estadísticamente significativos, facilitando un análisis detallado de las variables en estudio. Esta aproximación cuantitativa proporcionará una visión más precisa y generalizable del impacto del cibercrimen en la sociedad española.

Al integrar los enfoques cualitativo y cuantitativo en estas investigaciones sucesivas, se espera contribuir de manera más sólida al entendimiento del fenómeno del cibercrimen y al desarrollo de estrategias efectivas para su prevención y mitigación en el contexto nacional.

5.4. Reflexión final sobre el papel de la Criminología en el cibercrimen

La ciberdelincuencia se ha consolidado como uno de los grandes desafíos de las sociedades contemporáneas. Su carácter transnacional, su constante mutación tecnológica y su capacidad para afectar a individuos, empresas e instituciones en múltiples niveles exigen una mirada renovada y multidisciplinar que supere los marcos tradicionales del análisis delictivo. En este contexto, la Criminología está llamada a desempeñar un papel clave, no solo en la comprensión del fenómeno, sino también en el diseño de respuestas eficaces, sostenibles y socialmente responsables.

La Criminología, como ciencia social aplicada, posee herramientas teóricas y metodológicas fundamentales para abordar el delito en el ciberespacio. Su capacidad para analizar las motivaciones, perfiles, contextos y efectos del comportamiento delictivo resulta esencial para interpretar no solo el "cómo" y el "qué", sino especialmente el "por qué" de las nuevas formas de criminalidad. Frente a visiones puramente técnicas o legales, la mirada criminológica permite situar el cibercrimen en su complejidad social, cultural y estructural.

Desde esta perspectiva, resulta imprescindible incorporar enfoques criminológicos en la prevención primaria, diseñando políticas públicas centradas en la educación digital, la concienciación ciudadana y la reducción de factores de riesgo. Asimismo, en la prevención secundaria, el análisis criminológico permite identificar patrones de conducta delictiva, mejorar los sistemas de alerta temprana y contribuir a la creación de perfiles más precisos de ciberdelincuentes. En el ámbito de la prevención terciaria, la Criminología también aporta herramientas para la rehabilitación, la justicia restaurativa y el apoyo a las víctimas, dimensiones todavía poco exploradas en el contexto digital.

Además, la investigación criminológica puede servir como puente entre disciplinas técnicas, jurídicas y sociales, favoreciendo un enfoque verdaderamente integral en la lucha contra la

ciberdelincuencia. Esta interdisciplinariedad es especialmente relevante en un entorno donde los ataques evolucionan con rapidez, las fronteras jurídicas son difusas y los daños trascienden lo económico, afectando también a la intimidad, la salud mental y la cohesión social.

Este Trabajo de Fin de Grado ha representado una primera aproximación a ese compromiso desde la Criminología con los desafíos emergentes actuales. Lejos de agotar el tema, ha pretendido abrir camino hacia nuevas preguntas y nuevas metodologías que permitan profundizar en el estudio del cibercrimen desde una perspectiva crítica, empírica y transformadora.

Como futura criminóloga, el compromiso es claro: contribuir al desarrollo de una Criminología digitalmente alfabetizada, éticamente comprometida y científicamente rigurosa, capaz de acompañar a la sociedad en su tránsito hacia un entorno digital más justo, seguro e inclusivo.

6. REFERENCIAS BIBLIOGRÁFICAS

Brenner, S. W. (2019). Cybercrime: Criminal threats from cyberspace (2nd ed.). Routledge.

Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

Centro Criptológico Nacional (CCN-CERT). (2023). Informe de ciberamenazas y tendencias 2022–2023. CCN-CERT. https://www.ccn-cert.cni.es

Comisión Europea. (2024). Estrategia de Ciberseguridad de la UE. Comisión Europea. https://digital-strategy.ec.europa.eu

Consejo de Europa. (2001). Convenio de Budapest sobre ciberdelincuencia. https://www.coe.int/en/web/cybercrime

Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA 2023). Europol. https://www.europol.europa.eu

Gobierno de España. (2015). Código Penal español (Reforma 2015). Boletín Oficial del Estado. https://www.boe.es

Gobierno de España. (2015). Ley Orgánica 4/2015, de Protección de la Seguridad Ciudadana. Boletín Oficial del Estado. https://www.boe.es

Guardia Civil. (2010). Informe Operación Mariposa. Ministerio del Interior.

Holt, T. J., & Bossler, A. M. (2020). Cybercrime and digital forensics: An introduction (2nd ed.). Routledge.

INCIBE. (2023). Ciberseguridad en España: Estado y desafíos. Instituto Nacional de Ciberseguridad. https://www.incibe.es

Instituto Nacional de Estadística (INE). (2023). Delitos informáticos: Datos estadísticos. INE. https://www.ine.es

Interpol. (2023). Cybercrime. INTERPOL. https://www.interpol.int/en/Crimes/Cybercrime

Maras, M. H. (2020). Cybercrime and information technology security. Jones & Bartlett Learning.

Ministerio del Interior. (2023). Balance de Criminalidad. Informe sobre delincuencia en España. Gobierno de España. https://www.interior.gob.es

Ministerio del Interior. (2023). Informe anual sobre criminalidad en España. Secretaría de Estado de Seguridad. https://www.interior.gob.es

Navarro-Torres, L. (2022). Ciberdelincuencia organizada y delitos emergentes en la red. Revista de Criminología y Seguridad Digital, 11(2), 45–63.

Newman, G. R. (2018). Handbook of cybercrime prevention. Springer.

Observatorio Español de Delitos Informáticos (OEDI). (2022). Informe anual sobre cibercriminalidad en España. OEDI. https://www.oedi.es

Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 (Directiva NIS2) sobre medidas para un elevado nivel común de ciberseguridad en la Unión. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu

REvil Ransomware Group. (2021). Análisis de actividades delictivas 2021. Informes técnicos consolidados a través de Europol y Kaspersky.

Unión Europea. (2016). Reglamento General de Protección de Datos (UE) 2016/679 (RGPD). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu

Wall, D. S. (2021). Crime and the Internet (2nd ed.). Routledge.

Yahoo. (2017). Data Breach Disclosure Report. Yahoo Inc. https://www.yahooinc.com

ANEXOS

Anexo 1. Cronología de eventos

Esta cronología recoge los principales hitos relacionados con el desarrollo del marco normativo, institucional y operativo en materia de ciberdelincuencia, tanto a nivel nacional como europeo, desde la aprobación del primer tratado internacional hasta los incidentes más recientes que han marcado la agenda de ciberseguridad en España.

AÑO	EVENTO	DESCRIPCIÓN
2001	Convenio de Budapest	Primer tratado internacional sobre ciberdelincuencia, promovido por el Consejo de Europa. España lo firma y ratifica como parte del marco de cooperación internacional.
2010	Operación Mariposa	Investigación española que permitió desmantelar una red internacional de fraude digital. Supuso un hito en la cooperación policial frente a amenazas cibernéticas
2015	Reforma del Código penal	Introducción de nuevos tipos penales relacionados con el uso indebido de tecnologías de la información. Se amplía el marco legal para perseguir delitos informáticos.
2018	Aplicación del Reglamento General de Protección de Datos	Norma europea que refuerza la protección de datos personales y establece obligaciones de seguridad para empresas e instituciones.
2021	Ciberataque al SEPE	Ataque con ransomware al Servicio Público de Empleo Estatal, que paralizó su actividad durante varios días. Destacó la vulnerabilidad de organismos públicos.
2022	Aprobación de la directiva NIS2	Nueva directiva europea para mejorar la ciberseguridad de infraestructuras críticas y servicios esenciales. Obliga a España a reforzar su marco regulatorio.
2023	Ciberataque al hospital Clínic de Barcelona	Uno de los ciberataques más graves en el ámbito sanitario español. Afectó a sistemas clínicos y obligó a cancelar cientos de operaciones y consultas.
2023	Plan Nacional de Seguridad	Publicación del plan estratégico para fortalecer la resiliencia del país ante amenazas cibernéticas. Define acciones concretas para la prevención y respuesta.

Fuente: Elaboración propia a partir de informes del CCN-CERT (2023), Ministerio del Interior (2023), Consejo de Europa (2001), y datos de prensa oficial (RTVE, La Moncloa, INCIBE)

Anexo 2. Instrumentos de análisis de casos reales de ciberdelincuencia

Con el objetivo de ilustrar de forma práctica la diversidad y complejidad de los delitos informáticos registrados en España durante la última década, se presenta a continuación una tabla resumen con una selección representativa de casos reales. Estos casos han sido elegidos por su relevancia mediática, impacto institucional, diversidad tipológica y valor analítico en el contexto del estudio.

Cada caso ha sido clasificado según su tipología delictiva, el año de ocurrencia, el país afectado (con foco en España), el número o tipo de víctimas, y la fuente informativa utilizada. Este instrumento permite observar cómo los ciberdelitos han evolucionado desde ataques individuales hasta acciones organizadas que afectan a sectores críticos como la sanidad, la administración pública o la banca digital.

El análisis de estos casos ha servido como base complementaria para contrastar las hipótesis de la investigación y reforzar los hallazgos cualitativos obtenidos a través de la revisión documental.

"Ficha de análisis criminológico de ciberataques emblemáticos (2013–2023)"

Caso	Año	Tipo de delito	Técnicas utilizadas	Respuesta institucional
Ataque al SEPE	2021	Ransomware	Cifrado de archivos, bloqueo de sistemas	Intervención del INCIBE, restauración de sistemas, alerta nacional
Hospital Clínic de Barcelona	2023	Ciberdelito contra infraestructuras críticas	Ransomware, ataque dirigido	Suspensión de cirugías, colaboración con Mossos d'Esquadra e INCIBE
Filtración de datos de Iberdrola	2022	Robo de datos	Acceso indebido, exfiltración de información	Investigación abierta y refuerzo de medidas de seguridad
Estafa por WhatsApp – suplantación de identidad	2020	Phishing / Ingeniería social	Falsos perfiles, enlaces maliciosos	Campaña de concienciación de la Policía Nacional
Ciberataque al Ayuntamiento de Jerez	2019	Secuestro de sistemas	Ransomware	Activación de planes de contingencia y denuncia a autoridades

Fuente: Elaboración propia a partir de datos recopilados en informes oficiales (CCN-CERT, INCIBE, Europol) y medios especializados (Kaspersky, ESET, La Vanguardia, El País).

Anexo 3. Estadísticas ampliadas de ciberdelincuencia en España (2013-2023)

El presente anexo recoge la evolución cuantitativa de los delitos informáticos registrados en España durante la última década. Estos datos permiten identificar patrones de crecimiento, cambios en las tipologías predominantes y momentos críticos vinculados a transformaciones tecnológicas o eventos coyunturales como la pandemia de COVID-19.

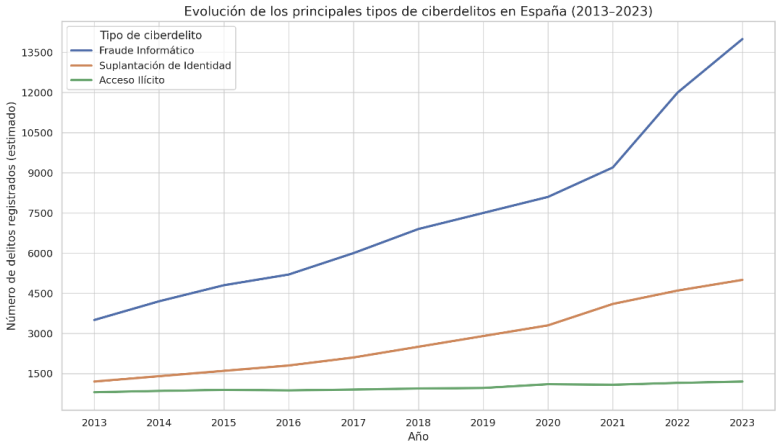
La tabla siguiente sintetiza la progresión anual de las denuncias por ciberdelito recogidas por el Ministerio del Interior, junto con observaciones relevantes que contextualizan los principales picos de incidencia.

Evolución anual del número de ciberdelitos registrados en España (2013–2023)

Año	Total de ciberdelitos registrados	Variación anual (%)	Observaciones relevantes
2013	20.534	—	Año base. Incremento inicial vinculado al uso masivo de smartphones y redes sociales.
2015	38.961	+89,7%	Reforma del Código Penal. Mejora en los mecanismos de denuncia.
2018	81.307	+108,6%	Crecimiento del comercio electrónico y banca online.
2020	218.302	+168,5%	Aceleración digital por pandemia. Aumento de fraudes online y ataques de ransomware.
2021	287.963	+31,9%	Consolidación del phishing y ataques a instituciones públicas.
2023	375.506	+30,4%	Máximo histórico. Alta sofisticación de delitos y diversificación de víctimas.

Fuente: Elaboración propia a partir de datos del Ministerio del Interior (2023) y el Instituto Nacional de Ciberseguridad (INCIBE, 2023).

Como puede observarse, el fraude informático ha sido el tipo de ciberdelito con mayor crecimiento sostenido durante el periodo analizado, reflejando una clara tendencia ascendente año tras año. Este incremento se acentuó especialmente a partir de 2020, coincidiendo con el auge del teletrabajo y el incremento del uso de plataformas digitales a raíz de la pandemia de COVID-19.



Por otro lado, los delitos de suplantación de identidad también han aumentado, aunque de forma más moderada, con picos en años concretos como 2021. En contraste, los accesos ilícitos a sistemas informáticos presentan una evolución más irregular y estable, sin un crecimiento tan pronunciado, pero con repuntes puntuales vinculados a brechas de seguridad en infraestructuras críticas. Esta evolución evidencia la necesidad de reforzar la ciberseguridad y la educación digital como ejes estratégicos de prevención.

Anexo 4. Marco Legal Comparado

El presente anexo ofrece una síntesis comparativa entre el marco legal español en materia de ciberdelincuencia y las normativas vigentes en otros contextos internacionales, con el fin de identificar fortalezas, debilidades y buenas prácticas que puedan servir de referencia para futuras reformas.

País / Región	Instrumentos legales clave	Fortalezas	Debilidades / Retos
España	- Código Penal (Reforma 2015) - Ley Orgánica 3/2018 (LOPDGDD) - Directiva NIS2 (UE)	- Tipificación clara de delitos informáticos - Protección de datos adaptada al RGPD	- Falta de tribunales especializados - Lenta cooperación internacional - Recursos limitados
Unión Europea	- Directiva NIS2 (2022) - Reglamento General de Protección de Datos (RGPD)	- Armonización normativa en ciberseguridad - Obligación de notificación de incidentes	- Desigual implementación por países miembros - Falta de sincronización judicial
Estados Unidos	- Computer Fraud and Abuse Act (CFAA) - USA PATRIOT Act	- Marco robusto de persecución federal - Agencias especializadas (FBI Cyber Division)	- Controversias sobre privacidad - Exceso de vigilancia gubernamental
Estonia	- Ley de Ciberseguridad (2018) - Estrategia Nacional de Ciberseguridad	- Modelo de referencia en digitalización y resiliencia - Respuesta ágil a incidentes	- Dependencia tecnológica elevada - Necesidad constante de actualización legislativa
Consejo de Europa	- Convenio de Budapest sobre Ciberdelincuencia (2001)	- Primer tratado internacional sobre el tema - Marco de cooperación judicial transnacional	- No ratificado por algunos países clave (China, Rusia)

Fuente: Elaboración propia a partir de datos legislativos del Código Penal español (Gobierno de España, 2015), el Reglamento General de Protección de Datos (Unión Europea, 2016), la Directiva NIS2 (Parlamento Europeo y Consejo de la Unión Europea, 2022), y la Convención de Budapest sobre ciberdelincuencia (Consejo de Europa, 2001).

El análisis comparado muestra que, si bien España ha avanzado en la incorporación de normativas europeas y en la tipificación de delitos informáticos, aún presenta retos en la especialización judicial, la coordinación interinstitucional y la cooperación internacional. En contraste, países como Estonia o EE.UU. han desarrollado sistemas más proactivos y centralizados. El Convenio de Budapest sigue siendo el marco multilateral de referencia, aunque su alcance se ve limitado por la falta de adhesión universal.