OCC

OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

MINISTERIO DEL INTERIOR

ESPAÑA

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2024

GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS

5ª edición, 2025

Contenidos: Ministerio del Interior. Dirección General de Coordinación y Estudios

Edición: Ministerio del Interior. Secretaría General Técnica

Catálogo de Publicaciones de la Administración General del Estado (CPAGE)

https://cpage.mpr.gob.es/

NIPO: 126-20-021-2

ÍNDICE

1. INTRODUCCIÓN 5

1.1 El Informe sobre la Cibercriminalidad y el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior 6

1.2 Estructura de este Informe sobre la Cibercriminalidad en España 7

1.3 Contexto internacional 7

1.4 Evolución en la respuesta estratégica contra el cibercrimen 10

1.5 Tendencias y respuestas ante la cibercriminalidad 12

2. INCIDENTES DE CIBERSEGURIDAD. Oficina de Coordinación de Ciberseguridad (OCC) . 17

2.1 Incidentes gestionados con afectación en operadores críticos de nivel ALTO, MUY ALTO o CRÍTICO 18

2.2 Incidentes gestionados por Sector Estratégico con afectación en operadores críticos de nivel ALTO, MUY ALTO o CRÍTICO 20

2.3 Incidentes remitidos a ENISA a través de la autoridad española según la Directiva NIS (Network and Information Systems) 22

3. DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD 26

4. CIBERATAQUES: Comparativa entre diferentes fuentes 49

5. ANEXO: Metadata 57

>> Datos estadísticos de criminalidad 57

>> Datos de la OCC 59

1

INTRODUCCIÓN

1. INTRODUCCIÓN

La lucha contra la **ciberdelincuencia**, como fenómeno de naturaleza compleja y alcance global, exige un enfoque multidisciplinar que permita articular respuestas eficaces frente a sus múltiples manifestaciones. Como punto de partida, resulta imprescindible comprender y visualizar con claridad la realidad criminal a la que hay que enfrentarse. Este conocimiento no puede limitarse únicamente al análisis de datos estadísticos; debe ampliarse hacia otras dimensiones clave que permitan contextualizar y entender en profundidad el fenómeno de la ciberdelincuencia. En este sentido, la elaboración periódica de informes especializados constituye una herramienta fundamental para dimensionar objetivamente esta realidad, identificar sus aspectos más relevantes y alertar sobre los riesgos —tanto actuales como potenciales— que plantea.

La publicación de este **Informe sobre la Cibercriminalidad en España**, correspondiente al **ejercicio 2024**, responde precisamente a ese propósito de contextualización general, siendo una evolución del anterior informe sobre la cibercriminalidad en España. Su objetivo es ofrecer un acercamiento a la visión global de la delincuencia cibernética registrada durante dicho año en España que sirva como herramienta útil de apoyo a todos los actores implicados en su prevención y respuesta.

Los datos que conforman este informe proceden del **Sistema Estadístico de Criminalidad (SEC)** y de los incidentes registrados por la **Oficina de Coordinación de Ciberseguridad (OCC)**, en función de sus respectivas competencias.

Por un lado, se incluyen las cifras aportadas por los distintos cuerpos policiales con presencia en el territorio nacional —Policía Nacional, Guardia Civil, Ertzaintza, Mossos d'Esquadra, Policía Foral de Navarra y cuerpos de Policía Local que colaboran con el SEC[1]—, tanto en lo relativo a hechos conocidos y victimizaciones como a detenciones e investigaciones. Por otro, se presentan datos propios de la OCC, los cuales incluyen los incidentes gestionados por la OCC en base a las notificaciones obligatorias conforme la normativa vigente de seguridad de las redes y sistemas de información. Finalmente, se incluye también información de los datos monitorizados y obtenidos de diversas fuentes que, como Observatorio de Cibercriminalidad del Ministerio del Interior, tienen como finalidad el análisis de tendencias cibercriminales que favorezcan el diseño de planes preventivos y la respuesta ante estos.

[1] En el anexo sobre metadata, además, se detalla la procedencia específica de la información suministrada por cada cuerpo policial.

1.1 El Informe sobre la Cibercriminalidad y el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior

Con el propósito de fortalecer las capacidades institucionales del Ministerio del Interior en la detección, prevención y persecución de la ciberdelincuencia, y de impulsar una respuesta operativa y técnica eficaz que garantice la protección de los derechos fundamentales y la seguridad ciudadana, en marzo de 2021 se aprobó el Plan Estratégico contra la Cibercriminalidad.

Este plan, diseñado por la Secretaría de Estado de Seguridad, se articula en torno a varios ejes prioritarios: la prevención como principio rector; la cooperación entre las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y los operadores jurídicos; el refuerzo de capacidades técnicas y humanas para responder a las distintas tipologías delictivas; la colaboración activa con la industria y los actores clave del ámbito de la ciberseguridad, tanto del sector público como del privado; y el respeto absoluto a la libertad, la privacidad y los derechos fundamentales.

Desde estos principios rectores, el plan establece una estrategia integral orientada a alcanzar los siguientes objetivos específicos:

- Promover la cultura de prevención de la cibercriminalidad entre la ciudadanía y la empresa.
- Impulsar la formación y la especialización de los miembros de las FCSE en materia de ciberseguridad y cibercriminalidad.
- Proteger los sistemas de información y telecomunicaciones utilizados por el Ministerio del Interior.
- Incrementar y mejorar el uso y disposición de las herramientas tecnológicas e implementar el ámbito de la I+D+i.
- Gestionar adecuadamente la información disponible en el ciberespacio.
- Promover un marco legal e institucional que dé solución a los desafíos que surjan relacionados con la ciberseguridad y la cibercriminalidad.
- Impulsar la coordinación a nivel nacional e internacional y favorecer la colaboración entre el sector público y privado.

Para alcanzar estos fines, el plan contempla un total de 49 líneas de acción, estructuradas en torno a seis ejes estratégicos: cultura de prevención de la cibercriminalidad, potenciación de capacidades, generación de ciberinteligencia, coordinación nacional y cooperación internacional, desarrollo de un marco normativo actualizado, y colaboración público-privada.

Este informe contribuye al cumplimiento de la **Línea de Acción 3.6**, enmarcada en el **Eje Estratégico III**: Generación de Ciberinteligencia. Dicha línea plantea como objetivo «**incrementar las capacidades actuales de obtención, tratamiento y análisis estratégico de información en el Ministerio del Interior**», con el propósito de evaluar las herramientas disponibles e implantar aquellas que permitan un tratamiento más eficaz de la inteligencia estratégica, elemento clave para anticipar y prevenir amenazas. Se presta especial atención al papel del SEC como fuente esencial en este proceso.

1.2 Estructura de este Informe sobre la Cibercriminalidad en España

El presente informe cuenta con un primer apartado como introducción al mismo. En este se realiza un recorrido que incluye su motivación, contexto situacional en que se encuentra España y el entorno internacional en materia cibernética, y analizando las tendencias, desafíos y respuestas actuales.

Los apartados segundo y tercero ofrecen un análisis sobre los distintos datos obtenidos de la OCC y el SEC. Esta información se presenta desglosada en distintos apartados —como hechos conocidos, distribución territorial, perfil de las víctimas, detenciones practicadas, incidentes clasificados por Comunidad Autónoma, o por sector estratégico, entre otros—, lo que permite ofrecer una visión estructurada de la realidad de la cibercriminalidad en nuestro país.

La clasificación de las conductas delictivas sigue los criterios establecidos por el Convenio de Budapest, a los que se han añadido, como en ocasiones anteriores, debido a su volumen e impacto, las siguientes infracciones penales:

a) delitos contra el honor;
b) amenazas y coacciones.

1.3 Contexto internacional

España no es un ente aislado en esta lucha contra la cibercriminalidad, por lo que siempre ha tenido un papel muy activo en el ámbito internacional para una mejor protección de los intereses de la nación y los ciudadanos en el entorno digital. Esto puede verse reflejado en el **Índice Global de Ciberseguridad elaborado por la Unión Internacional de Telecomunicaciones (UIT),** organismo

especializado de la ONU[2], que sitúa a España en los puestos más altos de la clasificación mundial en términos de ciberseguridad.

Un aspecto que merece especial atención es el crecimiento sostenido y cada vez más sofisticado de la ciberdelincuencia que afecta tanto a España como a los países de nuestro entorno. Según el informe **EU-SOCTA 2025**[3] de Europol, la inteligencia artificial se ha convertido en un catalizador clave de esta amenaza, al facilitar ataques más complejos, automatizados y difíciles de detectar. A ello se añade el aumento de dispositivos conectados a internet, principalmente los sistemas denominados Internet de las Cosas (IoT), lo que aumenta la superficie de exposición.

En este contexto, la ciberdelincuencia no solo representa una amenaza creciente para infraestructuras críticas, gobiernos y empresas, sino también para la ciudadanía, que se ve cada vez más expuesta a fraudes en línea, suplantaciones de identidad y ataques dirigidos, no solo dentro del ámbito nacional, si no que este tipo de actividades delictivas no reconocen fronteras. Esta realidad exige una respuesta integral, coordinada y tecnológicamente avanzada por parte de los Estados y del conjunto de la sociedad.

Es importante tener en cuenta que, en su esfuerzo por consolidar un entorno digital seguro, resiliente y comprometido con los derechos fundamentales, la Unión Europea ha desplegado un conjunto de medidas estratégicas orientadas a reforzar la capacidad de los Estados miembros frente a la ciberdelincuencia. Entre ellas destacan la **Estrategia de Ciberseguridad de la UE**[4], el **Reglamento de Ciberresiliencia**[5], el **Reglamento de Cibersolidaridad**[6] y la creación de la **Unidad Cibernética Conjunta**. Todos ellos concebidos para mejorar la prevención, detección y respuesta ante amenazas digitales, así como para fomentar la cooperación público-privada y la inversión en tecnologías avanzadas. En este contexto, la **Identidad Digital Europea**[7] emerge como un pilar clave para fortalecer la confianza en el ecosistema digital. A través de ella se prevé la creación de una **cartera digital europea**[8], que permitirá a los ciudadanos y empresas identificarse electrónicamente y acceder a servicios públicos y privados en toda la Unión, tanto en línea como fuera de línea, con pleno control sobre sus datos personales,

---

[2] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf
[3] https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
[4] https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-strategy
[5] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:4797302
[6] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202500038
[7] https://digital-strategy.ec.europa.eu/es/policies/eudi-regulation
[8] https://digital-strategy.ec.europa.eu/es/factpages/european-digital-identity-wallet

facilitando transacciones digitales más seguras que ayudarán a reducir el fraude de identidad, uno de los vectores de ataque más comunes de la ciberdelincuencia.

Cabe destacar la hoja de ruta marcada por la Unión Europea para liderar la transformación digital. Esta se materializa en la conocida **Brújula Digital 2030**[9,10], representando el compromiso de Europa por garantizar que su ciudadanía, empresas e instituciones estén adecuadamente preparadas para afrontar los retos y aprovechar las ventajas de esta era digital. Todo ello basándose en cuatro grandes ejes:

- Capacidades digitales para la ciudadanía.
- Infraestructuras digitales seguras y sostenibles.
- Transformación digital de las empresas.
- Digitalización de los servicios públicos.

A todo lo anterior, hay que añadir la **lucha contra la cibercriminalidad**, de la que se encargan las distintas Fuerzas y Cuerpos de Seguridad dentro del ámbito europeo con herramientas como:

EC3 (Centro Europeo de Ciberdelincuencia), integrado en Europol y que representa el brazo operativo contra el cibercrimen a nivel policial, además de ser el organismo responsable del informe **IOCTA**[11], en el que se evalúan, de forma anual, todas las amenazas cibernéticas más relevantes en Europa.

EUCTF (Grupo de Trabajo sobre Ciberdelincuencia de la UE) que, bajo el paraguas de Europol, concretamente en coordinación con el EC3, actúa como foro clave para el intercambio de información, buenas prácticas y coordinación de investigaciones conjuntas.

Además, se señalan otras herramientas que, aunque no actúan directamente sobre la cibercriminalidad, ayudan a analizar el entorno cibernético, entendiendo cuales son las tendencias y los posibles desarrollos tecnológicos que se van realizando:

ENISA (Agencia de la Unión Europea para la Ciberseguridad), que actúa como centro neurálgico de la política de ciberseguridad en Europa, con el objetivo de reforzar la resiliencia digital de los Estados miembros. ENISA desempeña un papel clave en la implementación de la mencionada Brújula Digital 2030.

[9] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es
[10] https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0118
[11] https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

CERT-EU (Equipo de Respuesta ante Emergencias Informáticas de la Unión Europea), que protege las redes y sistemas de las instituciones, agencias y otros organismos de la Unión Europea. Así mismo, gestiona, analiza, recopila y comparte información sobre amenazas, vulnerabilidad e incidentes relacionados con infraestructuras TIC.

En el amplio espectro de organismos conformados tanto por los Estados miembros, como asociados (Islandia, Noruega y Suiza), que abarca la lucha contra la ciberdelincuencia en nuestro entorno, se integran grupos de trabajo conjuntos en los que se identifican, discuten y priorizan aquellos desafíos y acciones necesarias para combatirla, destacando particularmente el **J-CAT** (fuerza operativa internacional permanente creada para combatir el cibercrimen de forma coordinada y transfronteriza), ubicado en el Centro Europeo contra la Cibercriminalidad (EC) de **EUROPOL.** Es también crucial en el esfuerzo común que supone la lucha contra la cibercriminalidad, la coordinación y colaboración con otras agencias europeas e internacionales, como **EUROJUST**[12], que facilita cooperación judicial a nivel europeo ayudando a las autoridades a combatir el crimen organizado y el terrorismo más allá de las fronteras nacionales; o como **INTERPOL**[13], que coordina operaciones policiales, alianzas multisectoriales y ofrece plataformas protegidas para el intercambio de información, además de realizar análisis e impartir formación, con miras a reducir las ciberamenazas, entre otros.

1.4 Evolución en la respuesta estratégica contra el cibercrimen

A medida que las tecnologías de la información y la comunicación (TIC) evolucionan con rapidez, también cambian las formas en que se accede a la información y hay que relacionarse con ella. Esta transformación ha comenzado a difuminar los límites entre lo físico y lo digital, otorgando a la ciberseguridad un papel estratégico que va más allá de los aspectos puramente técnicos. España, consciente de esta transformación, ha ido adaptando su enfoque mediante la aprobación de la **Estrategia Nacional de Ciberseguridad de 2019**[14] y, posteriormente, de la **Estrategia de Seguridad Nacional de 2021**[15]**,** entre otras. Este trayecto no solo ha procurado fortalecer las capacidades defensivas del país frente a las amenazas a la ciberseguridad, sino que ha incorporado nuevos

[12] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_es
[13] https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL2
[14] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347
[15] https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20Accesible_1.pdf

desafíos, como la **desinformación**, que amenazan la cohesión social y la estabilidad democrática.

La **Estrategia Nacional de Ciberseguridad 2019** marcó un hito al reconocer el ciberespacio como un dominio estratégico que requiere protección integral. En ella se establecieron líneas de acción orientadas a la protección de infraestructuras críticas, el refuerzo de capacidades nacionales y la cooperación internacional. Sin embargo, ya entonces se vislumbraba la necesidad de abordar fenómenos emergentes como la manipulación informativa y las campañas de influencia digital.

Esta preocupación se consolidó en la **Estrategia de Seguridad Nacional de 2021**, que amplió el enfoque de la ciberseguridad hacia una visión más holística. En un contexto marcado por eventos que tienden a la polarización social y el auge de las amenazas híbridas, la estrategia identificó la **desinformación como un vector de ataque no convencional**, capaz de erosionar la confianza pública, manipular procesos democráticos y debilitar la respuesta institucional. Así, la ciberseguridad dejó de ser solo una cuestión de protección tecnológica para convertirse en una herramienta integral para la defensa de la democracia.

Este enfoque se ve reforzado por la **Directiva NIS2**[16], en cuya trasposición está participando la OCC en la actualidad y que amplía el alcance de las obligaciones de ciberseguridad a nuevos sectores y entidades, promoviendo una mayor armonización normativa entre los Estados miembros. Aunque su núcleo sigue siendo la protección de redes y sistemas de información, esta directiva se inscribe en una visión más amplia de **resiliencia digital**, la cual se combina con la lucha contra la desinformación y las amenazas híbridas, las cuales están ocupando un lugar cada vez más relevante.

En este sentido, la convergencia entre las estrategias nacionales y europeas refleja una evolución profunda: el uso seguro del ciberespacio no implica solamente blindar infraestructuras, sino que se proyecta también como un **escudo frente a la manipulación informativa**, un garante de la integridad institucional y un pilar de la soberanía digital.

Así, el camino que comenzó con la Estrategia Nacional de Ciberseguridad de 2019 y se articuló con la Estrategia de Seguridad Nacional de 2021, confluye en una **visión europea compartida**, donde la ciberresiliencia se complementa con la defensa frente a la desinformación, como dos esfuerzos indispensables con un mismo objetivo: la protección del espacio público digital como bien común. En

[16] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un nivel común elevado de ciberseguridad en toda la Unión. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

este ámbito, el Ministerio del Interior, a través de la OCC, participa activamente en la **Comisión Permanente contra la Desinformación, creada por la Orden PCM/1030/2020, de 30 de octubre**[17], en el marco del procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Esta participación refuerza el compromiso del Estado con la protección del espacio informativo y la defensa de la integridad democrática frente a campañas de manipulación.

Como se ha señalado en el apartado 1.1., además de la Estrategia Nacional de Ciberseguridad, se cuenta con el Plan Estratégico contra la Cibercriminalidad de 2021, el cual está siendo revisado en la actualidad y que, como se ha dicho, fue concebido con el objetivo de potenciar las capacidades del Ministerio del Interior para la detección, prevención, protección, respuesta y persecución de la cibercriminalidad.

Igualmente, es relevante mencionar el **Real Decreto 207/2024**[18], de 27 de febrero, que desarrolla la estructura orgánica básica de este Ministerio del Interior. En este real decreto, además de las funciones que ya venía ejerciendo la OCC, como la de ser el órgano a través del cual la Secretaría de Estado de Seguridad ejerce como autoridad competente para los operadores de servicios esenciales designados operadores críticos, o la de ejercer como canal específico de comunicación entre los centros de respuesta a incidentes informáticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad; se han añadido la creación de un **Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior** de apoyo y coordinación a la Policía Judicial (CSIRT-MIR-PJ) y el **Observatorio de Cibercriminalidad del Ministerio del Interior**.

El **Plan Estratégico Nacional de Prevención y lucha contra la Radicalización Violenta**[19], es otra de las herramientas con las que se cuenta, cuyo objetivo principal es establecer un marco efectivo de prevención, conocimiento de los procesos y tratamiento de los extremismos violentos, en el cual señala el ámbito del ciberespacio como una amenaza para el adoctrinamiento, la propaganda y la formación de terroristas para alcanzar sus fines.

1.5 Tendencias y respuestas ante la cibercriminalidad

A partir de la información recopilada por Europol -organismo en el que participa activamente España- se elabora el informe **IOCTA** (*Internet Organinsed Crime Threat Assesment*), que analiza las amenazas y tendencias emergentes en el

[17] https://www.boe.es/eli/es/o/2020/10/30/pcm1030/dof/spa/pdf
[18] https://www.boe.es/buscar/pdf/2024/BOE-A-2024-3793-consolidado.pdf
[19] https://www.boe.es/boe/dias/2022/07/28/pdfs/BOE-A-2022-12626.pdf

ámbito del cibercrimen en Europa, y del que se extraen, en su documento del año 2024, las siguientes conclusiones referentes a la evolución de la cibercriminalidad en la UE:

- Se prevé que el **uso creciente de la Inteligencia Artificial** por parte de los ciberdelincuentes podría aumentar la generación de contenido fraudulento, más sofisticado, para automatizar ataques y manipular víctimas en múltiples idiomas.
- El **uso de plataformas con cifrado de extremo a extremo** (E2EE) y tecnologías descentralizadas, como *blockchain* y redes P2P, seguirá siendo aprovechado por actores maliciosos para ocultar sus actividades. La expansión de los principios de la Web3 dificulta la supervisión y el control por parte de las autoridades, al tiempo que facilita transacciones anónimas fuera del alcance legal. Este entorno técnico plantea importantes retos para el acceso legítimo a las comunicaciones delictivas.
- Se anticipa la **aparición de nuevas formas de RaaS (Ransomware como servicio)**, cuya supervivencia dependerá de la sofisticación de los grupos criminales que las operan. Ante la complejidad inherente a la cooperación judicial internacional -marcada por diferencias legislativas, jurisdiccionales y procedimentales entre países-, las Fuerzas y Cuerpos de Seguridad seguirán adoptando estrategias de disrupción y desmantelamiento de servicios ilícitos, buscando erosionar su actividad y frenar su proliferación.
- La lucha contra el fraude se verá reforzada por nuevas normativas, como son **la Directiva de Servicios de Pago 3[20] (PSD3) y el Reglamento de Servicios de Pago[21] (PSR),** impulsados por la Comisión Europea, y que anticipan un nuevo marco de cooperación entre entidades financieras, promoviendo el intercambio de información para combatir este fraude en línea y reforzando los derechos de los consumidores frente a estafas por suplantación de identidad.

En paralelo, la puesta en marcha de la versión 4.0 del estándar técnico PCI DSS[22] en marzo de 2025 introduce exigencias más estrictas para los comercios digitales. Entre ellas, destaca el control reforzado sobre los *scripts* en las páginas de pago, una medida clave para prevenir ataques de *skimming* y proteger los datos de los usuarios en tiempo real.

[20] https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_23_3543/IP_23_3543_ES.pdf
[21] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366
[22] PCI DSS (Payment Card Industry Data Security Standard)

- Para garantizar la seguridad del entorno digital europeo, se desarrolla **el Reglamento de Servicios Digitales[23] (DSA)**, en vigor desde febrero de 2024, el cual establece un marco normativo robusto que obliga a las plataformas a mejorar sus prácticas de **verificación de usuarios**, prohíbe la publicidad dirigida basada en criterios sensibles y exige medidas de mitigación frente a riesgos como la **desinformación**, la violencia digital y el daño a menores. Este reglamento representa un paso decisivo hacia una Internet más segura, transparente y respetuosa con los derechos fundamentales.
- Frente a la **creciente sofisticación del cibercrimen**, el Ministerio del Interior, las Fuerzas y Cuerpos de Seguridad y el resto de las instituciones competentes en ciberseguridad, están adoptando un enfoque preventivo que busca abordar las causas profundas de la delincuencia digital. Factores como la falta de concienciación de los usuarios, los incentivos económicos que obtienen los ciberdelincuentes y las condiciones socioeconómicas tanto de la víctima como de los actores son elementos clave que, al ser comprendidos y abordados, permiten reducir de forma sostenible la criminalidad en línea.

Este enfoque no solo mitiga riesgos inmediatos, sino que también fomenta una cultura de ciberseguridad más sólida y resiliente. En particular, se ha identificado que muchos ciberdelincuentes son jóvenes con habilidades técnicas avanzadas, pero escasa conciencia de las consecuencias legales de sus actos. Redirigir ese talento hacia fines legítimos representa una oportunidad tanto para la sociedad como para los propios individuos.

En este contexto, la **Prevención del Delito Cibernético** está ganando protagonismo en la Unión Europea como complemento esencial a las medidas de investigación. Desde 2023, Europol respalda la red **InterCOP**, una alianza internacional de cuerpos policiales que, junto con actores públicos y privados, desarrolla campañas preventivas y comparte buenas prácticas. Esta colaboración multisectorial es clave para construir un ciberespacio más seguro, inclusivo y resiliente.

En otro ámbito, fuera del Ministerio del Interior, pero con repercusión en las actuaciones de dicho ministerio, se publica la **Orden TDF/149/2025[24], la cual refuerza la prohibición de las llamadas comerciales sin consentimiento previo** (ya establecido en la Ley 11/2022, General de Telecomunicaciones) y obliga a los operadores a bloquear llamadas y SMS de números no asignados o que simulen ser números españoles. Con esta orden se establecen medidas para combatir las

[23] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2065
[24] https://www.boe.es/eli/es/o/2025/02/12/tdf149/dof/spa/pdf

estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos.

Además del empleo de la inteligencia artificial para el desarrollo de mejores ataques de tipo *ransomware*, esta también es una de las principales amenazas hoy en día para las Fuerzas y Cuerpos de Seguridad, debido a que está siendo utilizada por actores maliciosos para ejecutar campañas de ingeniería social hiperrealistas, crear identidades falsas mediante *deepfakes* o automatizar su ejecución, o incluso detectar vulnerabilidades explotables con mayor rapidez. Esta evolución tecnológica ha ampliado de forma significativa la escala y el impacto de los ataques en el espectro digital.

A ello se suma la expansión imparable del ecosistema digital. Se estima que en 2025 habrá más de 32.000 millones de dispositivos conectados a internet, los IoT, en todo el mundo, lo que incrementa exponencialmente la superficie de exposición a ciberataques.

Por último, en la lucha contra los riesgos derivados de la **desinformación**, ya desde 2018 se viene advirtiendo en el Plan de Acción contra la desinformación de la Comisión Europea[25], la importancia de su impacto negativo sobre la sociedad en todos sus ámbitos. Esta actividad tiene fuertes implicaciones para la ciberseguridad, como ha reconocido **ENISA**[26]. Esta amenaza a la seguridad nacional se manifiesta en diferentes puntos, que van desde la pérdida de confianza por parte de la ciudadanía en las instituciones hasta el debilitamiento de la cohesión interna de los Estados, pasando por la creciente polarización social o las posibles repercusiones que todo ello acarrea para la seguridad pública. La propia Comisión Europea califica esta amenaza como una de sus principales preocupaciones para los próximos años[27]. Para hacer frente en España a esta realidad, el pasado mes de marzo se publicó la **Orden PJC/248/2025**[28], sobre el Acuerdo del Consejo de Seguridad Nacional para la elaboración de la **Estrategia Nacional contra las Campañas de Desinformación**, lo que permitirá a la Comisión Permanente de Desinformación desarrollar dicha Estrategia y fortalecer de esta forma la lucha contra la desinformación.

[25] https://www.eeas.europa.eu/node/54866_en
[26] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
[27] https://www.weforum.org/stories/2024/01/ursula-von-der-leyen-full-speech-davos/
[28] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151

2

INCIDENTES DE CIBERSEGURIDAD

OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD (OCC)

2. INCIDENTES DE CIBERSEGURIDAD. Oficina de Coordinación de Ciberseguridad (OCC)

La OCC constituye el órgano de referencia del Ministerio del Interior en materia de ciberseguridad, cuyas funciones están reguladas por el Real Decreto 207/2024, de 27 de febrero, que desarrolla la estructura orgánica básica de este. Integrada en la Dirección General de Coordinación y Estudios, la OCC actúa como punto nacional de contacto para la coordinación operativa en el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo dispuesto por la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

Asimismo, la OCC ejerce como **canal específico de comunicación** entre los **CSIRT nacionales de referencia,** el del Instituto Nacional de Ciberseguridad (INCIBE-CERT), el del Centro Criptológico Nacional (CCN-CERT), el del Mando Conjunto del Ciberespacio (ESPDEF-CERT) y la Secretaría de Estado de Seguridad, y se configura como el Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior de apoyo a la Policía Judicial (CSIRT-MIR-PJ). En el ejercicio de esta función, proporciona soporte técnico y coordina a las unidades de investigación de ciberdelincuencia de las Fuerzas y Cuerpos de Seguridad del Estado, en los supuestos que así se determinen.

Además, en virtud del **Real Decreto-ley 12/2018, de 7 de septiembre, sobre la seguridad de las redes y sistemas de información**[29], la OCC asume las funciones atribuidas a la Secretaría de Estado de Seguridad como autoridad competente en esta materia para los **operadores de servicios esenciales** que, a su vez, sean designados como **operadores críticos**. En consecuencia, es el organismo encargado de recibir todas las **notificaciones obligatorias de incidentes** conforme a dicho Real Decreto-ley y a la Instrucción Nacional de Notificación y Gestión de Ciberincidentes incluida en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información[30].

La OCC, el INCIBE, el CCN y el Mando Conjunto del Ciberespacio son cuatro entidades clave en el ecosistema de ciberseguridad en España, cada una con funciones específicas pero complementarias. La OCC, dependiente del Ministerio del Interior, coordina las políticas de ciberseguridad en el ámbito de la seguridad pública y la protección de los operadores de servicios esenciales que, a su vez, sean designados como operadores críticos.

[29] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf
[30] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

El CCN, adscrito al Centro Nacional de Inteligencia, se encarga de la ciberseguridad en el ámbito de las administraciones públicas y la protección de información clasificada.

Por su parte, el INCIBE, bajo el Ministerio para la Transformación Digital, se enfoca en la ciberseguridad de ciudadanos, empresas y operadores estratégicos del sector privado, operando el INCIBE-CERT en colaboración con la OCC para gestionar incidentes que afecten a operadores de servicios esenciales.

El ESPDEF-CERT del Mando Conjunto del Ciberespacio contribuye a la vigilancia de redes y sistemas militares, respuesta ante emergencias informáticas y cooperación con organismos civiles y militares en materia de ciberseguridad para la defensa de España.

Estas cuatro entidades colaboran estrechamente para garantizar una respuesta coordinada ante amenazas cibernéticas, alineadas con la Estrategia de Seguridad Nacional.

2.1 Incidentes gestionados con afectación en operadores críticos de nivel ALTO, MUY ALTO o CRÍTICO

En relación con la Instrucción Nacional de Notificación y Gestión de Ciberincidentes antes referenciada, la OCC gestionó y notificó un total de **ciento sesenta (160) incidentes de ciberseguridad en España** durante el año 2024, todos ellos clasificados con niveles de peligrosidad e impacto alto, muy alto o crítico.

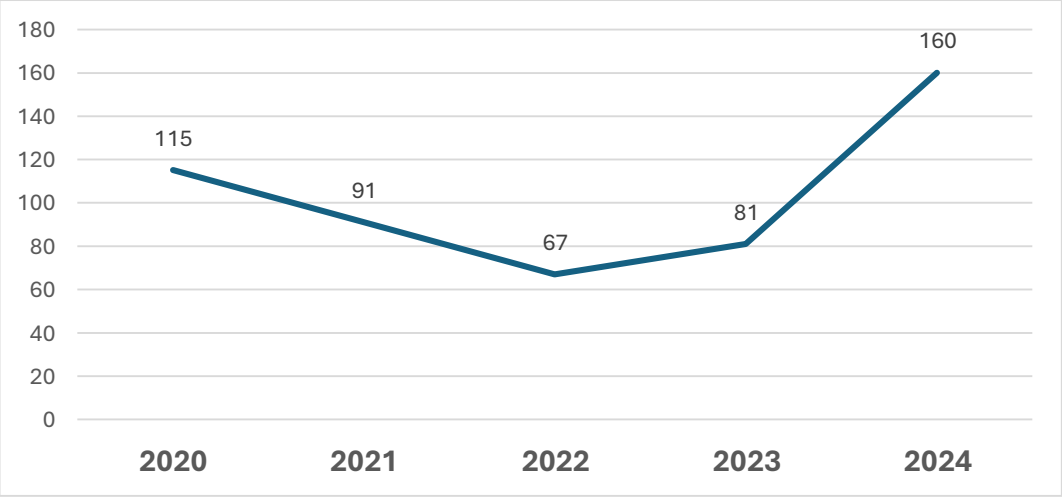


Ilustración 1. Incidentes operadores de servicios esenciales (OSE) gestionados por OCC, peligrosidad o impacto alto o superior. Fuente: OCC

Este valor supone un aumento del 97,53% con respecto al año 2023.

Tipo de incidente	2020	2021	2022	2023	2024
Compromiso de la información	21	19	26	22	62
Contenido abusivo	0	0	0	0	0
Contenido dañino	36	32	11	4	7
Disponibilidad	8	5	6	28	65
Fraude	29	18	15	11	12
Intento de intrusión	0	0	1	0	2
Intrusión	1	10	7	10	8
Obtención de información	1	0	0	0	0
Otros	1	3	0	2	3
Vulnerabilidad	18	4	1	4	1
	115	**91**	**67**	**81**	**160**

Tabla 1. Incidentes OSE gestionados por OCC, según tipología. Fuente: OCC

Del análisis de los incidentes registrados durante el año 2024, clasificados según su tipología, se desprende que los incidentes relacionados con la Disponibilidad fueron los más frecuentes, representando aproximadamente el 40,63 % del total. En segundo lugar, se situaron los incidentes tipificados como Compromiso de la información, con una proporción del 38,75 % sobre el total.

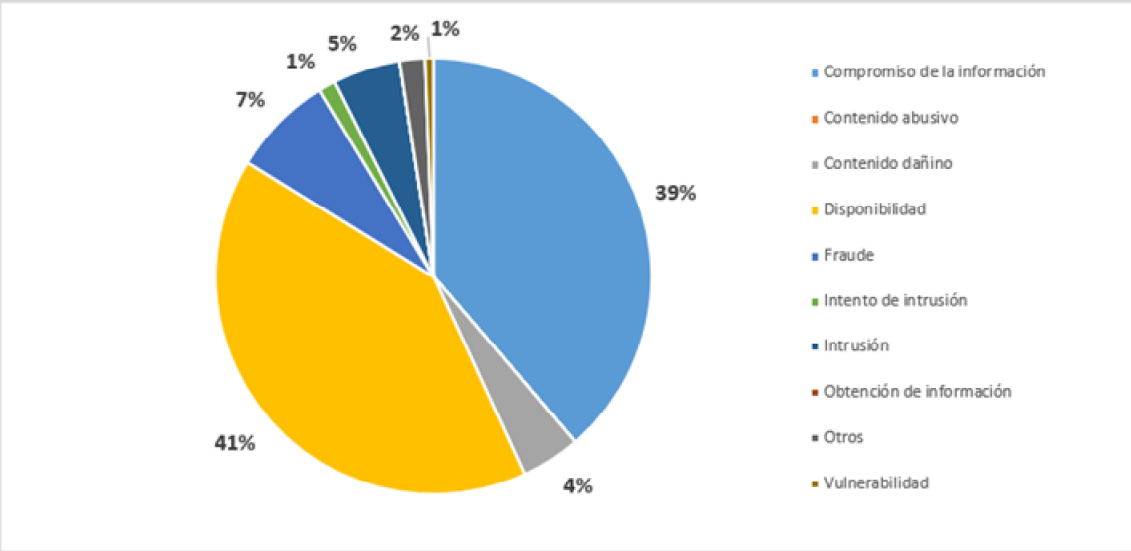


Ilustración 2. Porcentajes de incidentes OSE gestionados por OCC en 2024, según tipología. Fuente: OCC

Por otro lado, con respecto a los incidentes relativos al fraude, cabe destacar que durante el año 2024 han continuado proliferando campañas de suplantación de identidad de clientes o proveedores, tanto por vía telefónica como a través del correo electrónico, registrándose un total **7,5 % del total de incidentes** en los distintos ámbitos del sector público y privado.

2.2 Incidentes gestionados por Sector Estratégico con afectación en operadores críticos de nivel ALTO, MUY ALTO o CRÍTICO

Entre los incidentes gestionados que afectaron a operadores de servicios esenciales y que fueron clasificados con niveles de peligrosidad o impacto alto, muy alto o crítico.

Sector estratégico	**2020**	**2021**	**2022**	**2023**	**2024**
Administración	4	7	4	2	2
Agua	5	4	3	2	12
Alimentación	11	0	0	0	0
Energía	13	5	11	7	23
Espacio	0	0	0	2	0
General	0	0	0	0	0
Industria nuclear	24	5	1	3	3

Industria química	10	7	8	3	10
Instalaciones de investigación	0	0	0	0	0
No aplica	0	0	0	0	0
Salud	2	0	2	2	2
Sistema tributario y financiero	20	23	12	18	28
TIC	13	20	11	17	19
Transporte	12	17	11	23	60
Varios	1	3	4	2	1
	115	**91**	**67**	**81**	**160**

Tabla 2. Número de incidentes OSE gestionados por OCC, por sector. Fuente: OCC

Los sectores más afectados fueron el de Transporte, que concentró el 37,5 % del total, seguido del Sistema Financiero y Tributario con un 17,5 %, y el sector de la Energía, con un 14,38 %.

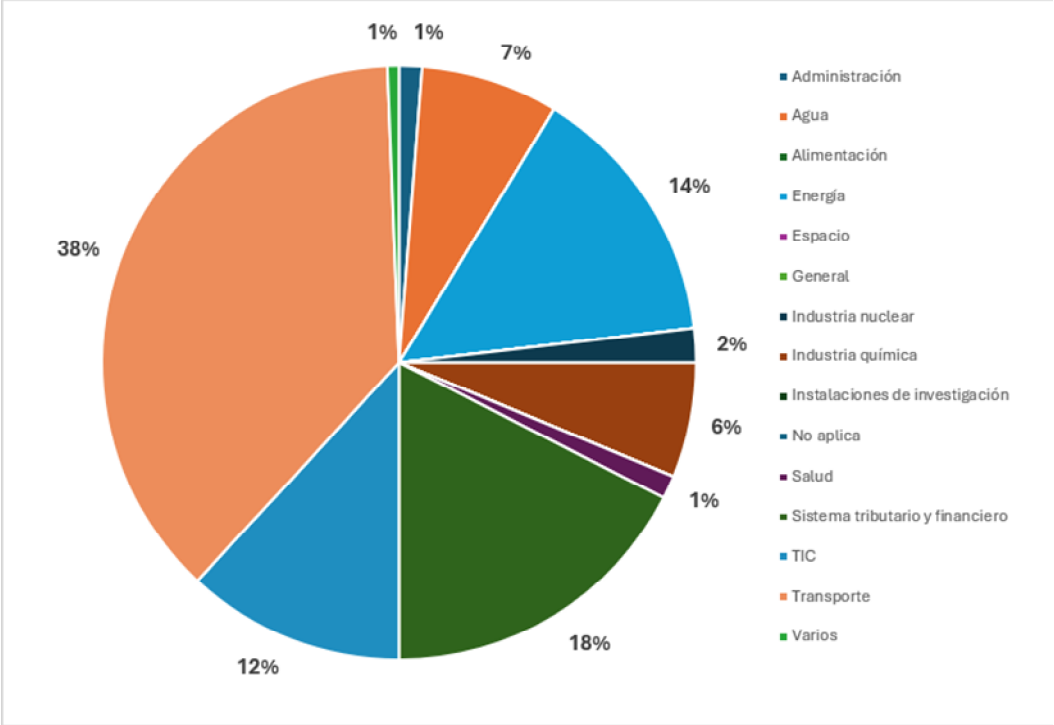


Ilustración 3. Porcentajes incidentes OSE gestionados por OCC en 2024, según sector. Fuente: OCC

2.3 Incidentes remitidos a ENISA a través de la autoridad española según la Directiva NIS (Network and Information Systems)

Durante el año 2024, a través de la OCC, se notificaron un total de **treinta y un (31) incidentes de ciberseguridad** a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), a través del punto de contacto nacional, representado por el Departamento de Seguridad Nacional (DSN), en cumplimiento de lo establecido en el artículo 27 del Real Decreto-ley 12/2018, legislación que supone la trasposición de la Directiva europea NIS.

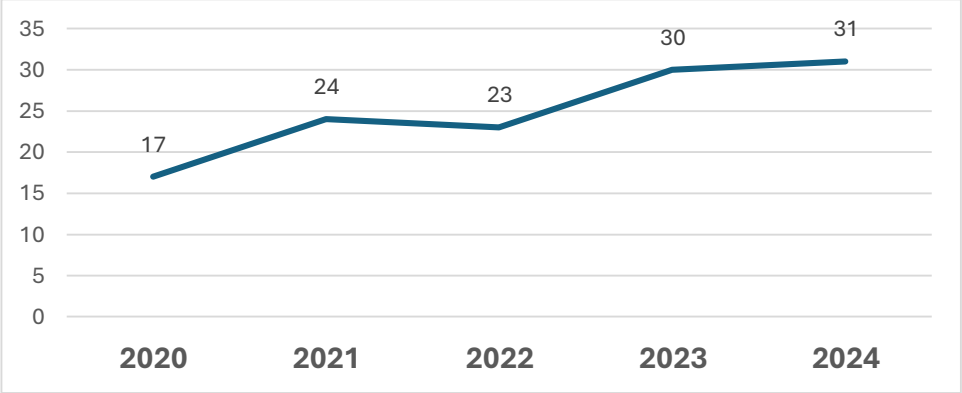


Ilustración 4. Incidentes reportados a ENISA por años. Fuente: OCC

Esta cifra supuso un incremento del 3,3 % respecto al año anterior.

Tipo de incidente	2020	2021	2022	2023	2024
Compromiso de la Información	6	4	11	4	9
Contenido abusivo	0	0	0	0	0
Contenido dañino	2	7	1	1	1
Disponibilidad	3	3	5	15	13
Fraude	5	4	0	3	4
Intento de Intrusión	0	0	1	0	0
Intrusión	0	4	5	6	3
Obtención de información	0	0	0	0	0
Otros	1	2	0	0	1
Vulnerabilidad	0	0	0	1	0
	17	**24**	**23**	**30**	**31**

Tabla 3. Incidentes remitidos a ENISA por años, según tipología. Fuente: OCC

En cuanto a la tipología de los incidentes comunicados, los más relevantes volvieron a estar relacionados con la Disponibilidad, que representaron el 42 % del total. A continuación, se situaron los incidentes de Compromiso de la información con un 29 %, seguido por los de fraude con un 13 %.

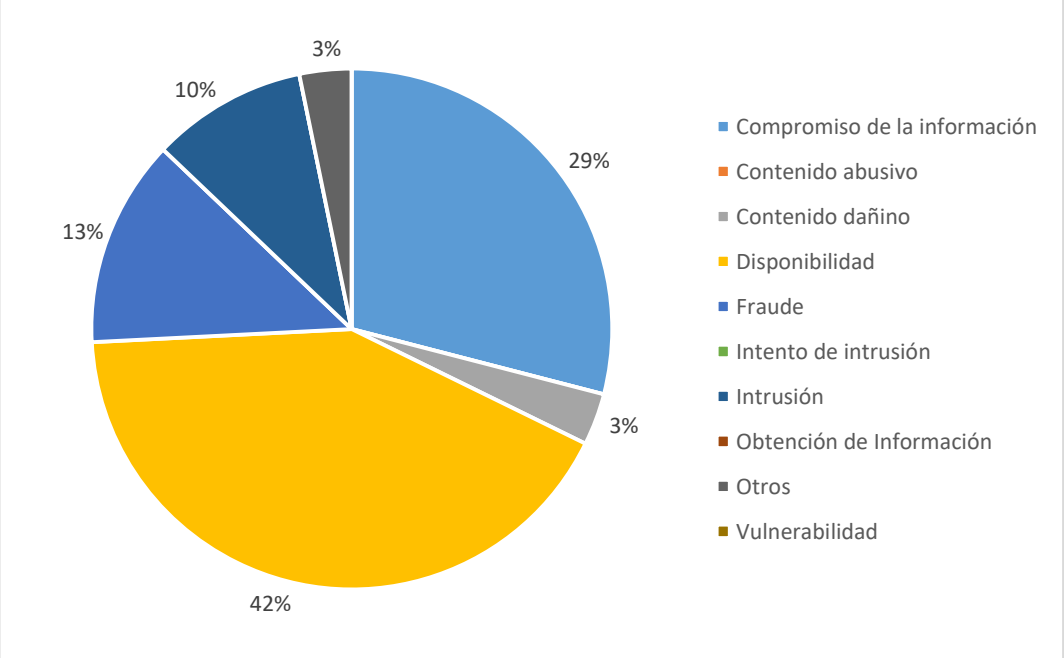


Ilustración 5. Porcentajes incidentes remitidos a ENISA en 2024, según tipología. Fuente: OCC

La distribución de los incidentes por sector estratégico muestra como el sector transporte asume más del 40 % de los incidentes, muy por encima de los dos siguientes sectores más afectados, Energía y TIC, con un porcentaje de 16,1 % cada uno.

Sector estratégico	2020	2021	2022	2023	2024
Administración	0	1	1	0	0
Agua	1	2	0	1	1
Alimentación	0	0	0	0	0
Energía	3	2	5	2	5
Espacio	0	0	0	1	0
Industria nuclear	0	0	0	0	0
Industria química	3	2	0	1	0
Instalaciones de investigación	0	0	0	0	0
Salud	0	0	0	2	2
Sistema tributario y financiero	5	4	4	4	4
TIC	3	7	9	8	5
Transporte	2	6	4	10	13
Varios	0	0	0	1	1
	17	**24**	**23**	**30**	**31**

Tabla 4. Incidentes remitidos a ENISA, distribución por sector estratégico. Fuente: OCC

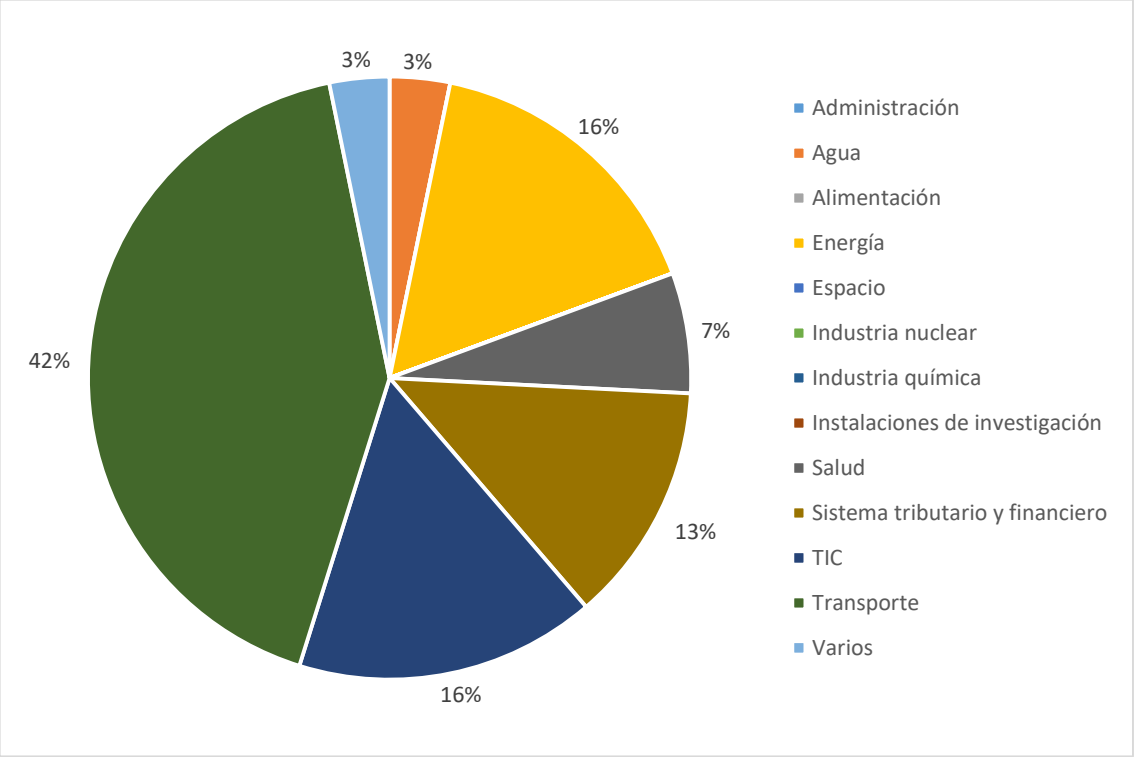


Ilustración 6. Porcentajes incidentes remitidos a ENISA en 2024, distribución por sector estratégico. Fuente: OCC

3

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

3. DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

El Sistema Estadístico de Criminalidad (SEC) comenzó a operar en enero de 2008, sustituyendo al anterior Programa Estadístico de Criminalidad (PES), con el propósito de mejorar la calidad y precisión en la recopilación y análisis de datos sobre criminalidad en España. Esta evolución permitió avances metodológicos y técnicos que incrementaron la fiabilidad de los informes generados por el Ministerio del Interior.

Posteriormente, el Real Decreto 400/2012, de 17 de febrero, desarrolló la estructura orgánica básica del Ministerio del Interior, asignando al entonces Gabinete de Coordinación y Estudios (actualmente Dirección General de Coordinación y Estudios) las funciones en materia de estadística criminal.

Un año después, el 31 de enero de 2013, la Secretaría de Estado de Seguridad dictó la Instrucción 1/2013 sobre la Estadística Nacional de Criminalidad, cuyo objetivo era «*dictar las directrices básicas para el desarrollo y gestión de la Estadística Nacional de Criminalidad, determinando los elementos que la componen —especialmente el Sistema Estadístico de Criminalidad—, definiendo los actores que interactúan en la misma y fijando las responsabilidades de cada uno de ellos*». Con esta instrucción, se establecieron criterios claros para la gestión de los datos estadísticos en materia de criminalidad.

Esta responsabilidad se ha mantenido incluso tras la publicación del Real Decreto 734/2020, de 4 de agosto, que reafirmaba la estructura organizativa del Ministerio y consolidó la continuidad del análisis estadístico en seguridad y criminalidad.

La Instrucción 1/2013 sobre la Estadística Nacional de Criminalidad ha contribuido a fortalecer el sistema de recopilación y análisis de datos sobre criminalidad en España, a través de la base de datos que registra las actuaciones policiales y responsables. Esta base de datos es alimentada por toda la información aportada por las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil), otras Fuerzas y Cuerpos de Seguridad dependientes de las Comunidades Autónomas (Ertzaintza, Mossos d'Esquadra y Policía Foral de Navarra), así como por aquellos cuerpos de Policía Local que facilitan datos a las Fuerzas y Cuerpos de Seguridad del Estado y, en definitiva, al SEC.

A continuación, se detallará concretamente aquella información consignada en el SEC sobre cibercriminalidad en España.

Datos globales

En relación con la **evolución de hechos conocidos por categorías delictivas**, se recoge el total de hechos delictivos registrados por las Fuerzas y Cuerpos de Seguridad durante la serie histórica 2020-2024. (La información de cada cuerpo se detalla en el apartado correspondiente a Anexo: Metadata).

La clasificación utilizada en este análisis sigue los criterios establecidos en el **Convenio sobre Ciberdelincuencia** aprobado por el Comité de ministros del Consejo de Europa el 8 de noviembre de 2001 y propuesto para su firma el 23 de noviembre[31] del mismo año (también conocido como Convenio de Budapest) y otras infracciones penales reguladas en la legislación nacional. Asimismo, además de las categorías específicamente identificadas como ciberdelincuencia, deben incluirse dentro de este fenómeno y computarse en el SEC todos aquellos delitos cuya comisión haya requerido el uso de tecnologías de la información y la comunicación (TIC).

Adicionalmente, junto a los delitos contemplados en el citado convenio, se han incorporado una serie de tipologías penales que, por su relevancia, merecen una especial consideración:

- Delitos contra el honor.
- Amenazas y coacciones.

En el período comprendido entre 2020 a 2023, se constató un aumento progresivo de los delitos informáticos, si bien en 2024 puede observarse un descenso, al haberse conocido un total de **464.801** delitos de esta tipología, lo que supone **una disminución del 1,6 % con respecto a 2023**. De esta cifra, el 88,8% corresponde a fraudes informáticos (estafas), y el 4,2 % a falsificación informática (que aglutina delitos como la usurpación de estado civil, falsificación/tráfico de tarjetas bancarias y otras falsificaciones documentales entre otros).

[31] https://rm.coe.int/1680081561

HECHOS CONOCIDOS	2020	2021	2022	2023	2024
ACCESO E INTERCEPTACIÓN ILÍCITA	4.653	5.342	5.578	7.367	9.773
AMENAZAS Y COACCIONES	14.066	17.319	15.982	17.472	17.738
CONTRA EL HONOR	1.550	1.426	1.191	1.174	1.128
CONTRA PROPIEDAD INDUST./INTELEC.	125	137	114	117	227
DELITOS SEXUALES(*)	1.783	1.628	1.646	1.804	1.676
FALSIFICACIÓN INFORMÁTICA	6.289	10.476	12.569	15.137	19.492
FRAUDE INFORMÁTICO	257.907	267.011	335.995	427.448	412.850
INTERFERENCIA DATOS Y EN SISTEMA	1.590	2.138	1.662	1.741	1.917
Total HECHOS CONOCIDOS	**287.963**	**305.477**	**374.737**	**472.260**	**464.801**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Tabla 5. Número de hechos conocidos. Fuente SEC.

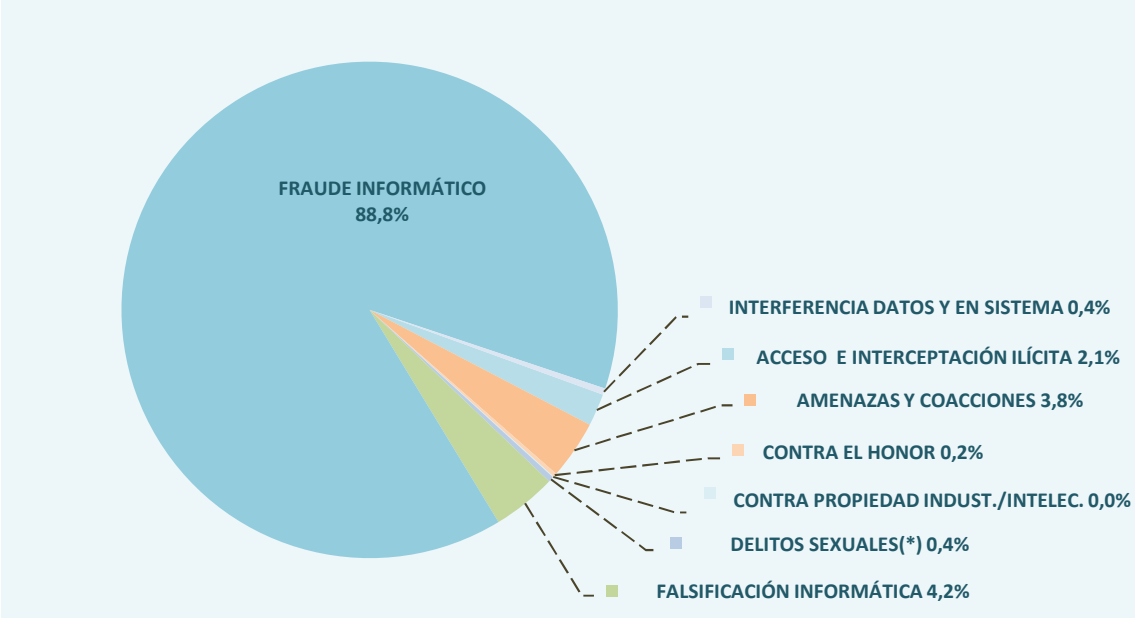


Ilustración 7. Porcentajes hechos conocidos. Fuente: SEC

Hasta la fecha, el análisis de los datos registrados en el ámbito de la cibercriminalidad evidencia un crecimiento sostenido de este fenómeno. Su impacto, en comparación con el total de hechos de la delincuencia en general, ha mostrado su tendencia al alza. No obstante, en 2024 se ha alcanzado la cifra del 18,9 %, lo que supone una recesión en esta evolución.

2019	9,9%
2020	16,3%
2021	15,6%
2022	16,1%
2023	19,2%
2024	18,9%

Tabla 6. Porcentaje que representa la Cibercriminalidad sobre el total de infracciones penales. Fuente: SEC

Las gráficas sobre la evolución global de hechos conocidos, esclarecidos y detenciones/investigados, presentan de manera visual la dinámica de la criminalidad registrada por las Fuerzas y Cuerpos de Seguridad a lo largo del período 2020-2024.

En cuanto al porcentaje de hechos esclarecidos en 2024, este representa aproximadamente el 13,8 % del total de hechos conocidos, evidenciando un leve ascenso con respecto al año anterior. Asimismo, el número de detenidos e investigados ha alcanzado la cifra de 19.322, lo que supone un incremento del 14% en comparación con 2023, cuando se contabilizaron 17.225 detenidos e investigados.

Ilustración 8. Evolución global de hechos conocidos, esclarecidos y detenciones/investigados. Fuente: SEC

Tras observar el desglose mensual de los datos, se resalta que, en 2024, **enero** fue el mes con **mayor incidencia**.

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	731	635	647	787	852	737	630	589	628	1.741	1.010	786	**9.773**
AMENAZAS Y COACCIONES	1.569	1.468	1.471	1.464	1.571	1.445	1.476	1.533	1.423	1.596	1.459	1.263	**17.738**
CONTRA EL HONOR	91	103	95	96	85	78	95	82	103	105	112	83	**1.128**
CONTRA PROPIEDAD INDUST./INTELEC.	15	26	25	32	23	24	20	10	11	15	15	11	**227**
DELITOS SEXUALES	140	138	189	140	132	144	101	93	128	153	184	134	**1.676**
FALSIFICACIÓN INFORMÁTICA	1.601	1.409	1.495	1.891	2.281	2.016	1.650	1.397	1.534	1.580	1.472	1.166	**19.492**
FRAUDE INFORMÁTICO	44.252	34.990	31.458	34.054	33.980	31.832	33.991	30.504	33.012	36.285	35.438	33.054	**412.850**
INTERFERENCIA DATOS Y EN SISTEMA	186	159	144	147	202	180	168	110	113	161	196	151	**1.917**
Total HECHOS CONOCIDOS	**48.585**	**38.928**	**35.524**	**38.611**	**39.126**	**36.456**	**38.131**	**34.318**	**36.952**	**41.636**	**39.886**	**36.648**	**464.801**

Tabla 7. Distribución mensual de hechos conocidos. Año 2024. Fuente: SEC

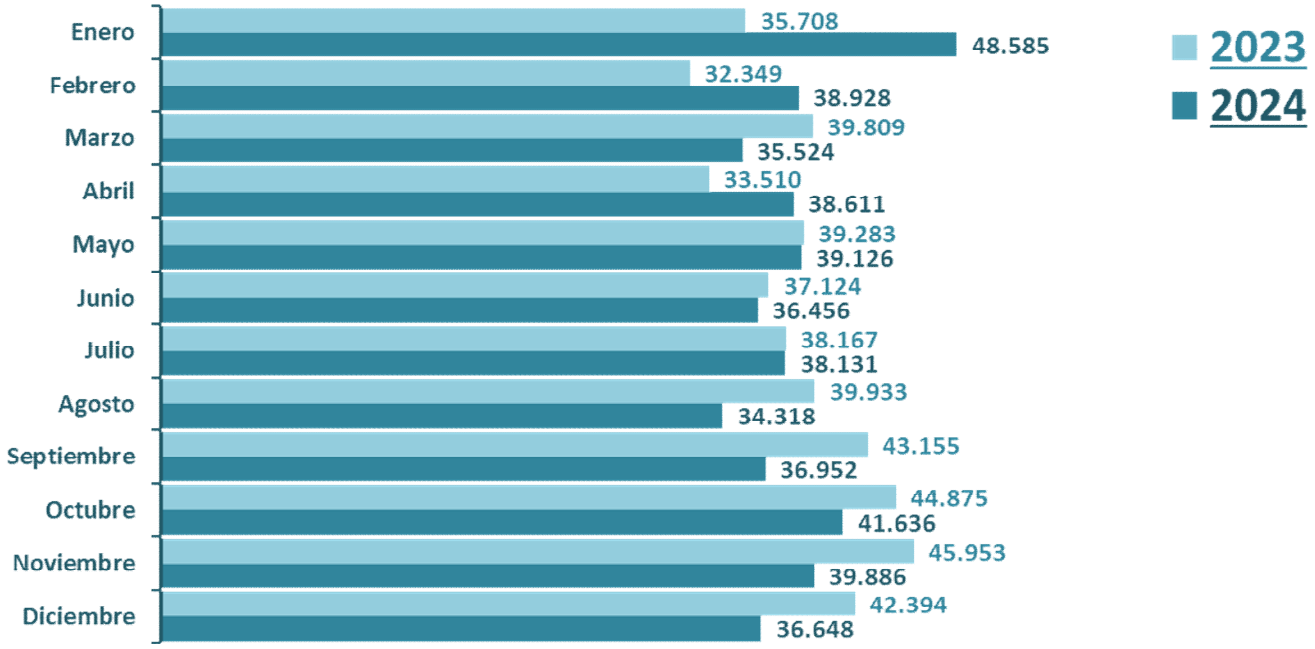


Ilustración 9. Comparativa mensual entre 2023 y 2024. Fuente SEC.

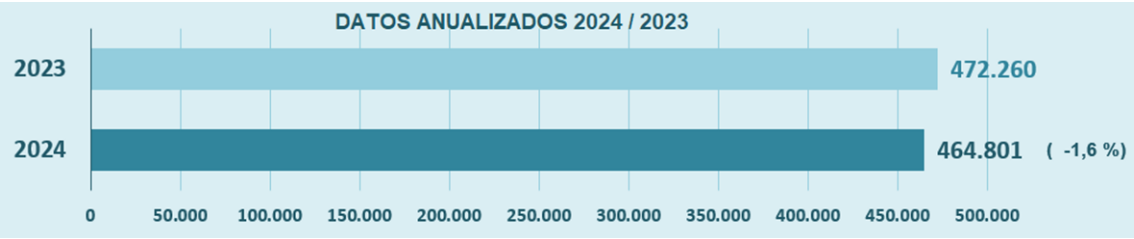


Ilustración 10. Comparativa anual 2023 y 2024. Fuente: SEC

La **representación territorial de los hechos denunciados de cibercriminalidad** revela que, a lo largo de 2024, Andalucía, Cataluña y Madrid se encuentran entre las Comunidades Autónomas con mayor concentración de

infracciones penales en este ámbito. A nivel provincial, destacan Madrid, Barcelona y Valencia como las zonas con mayor incidencia.

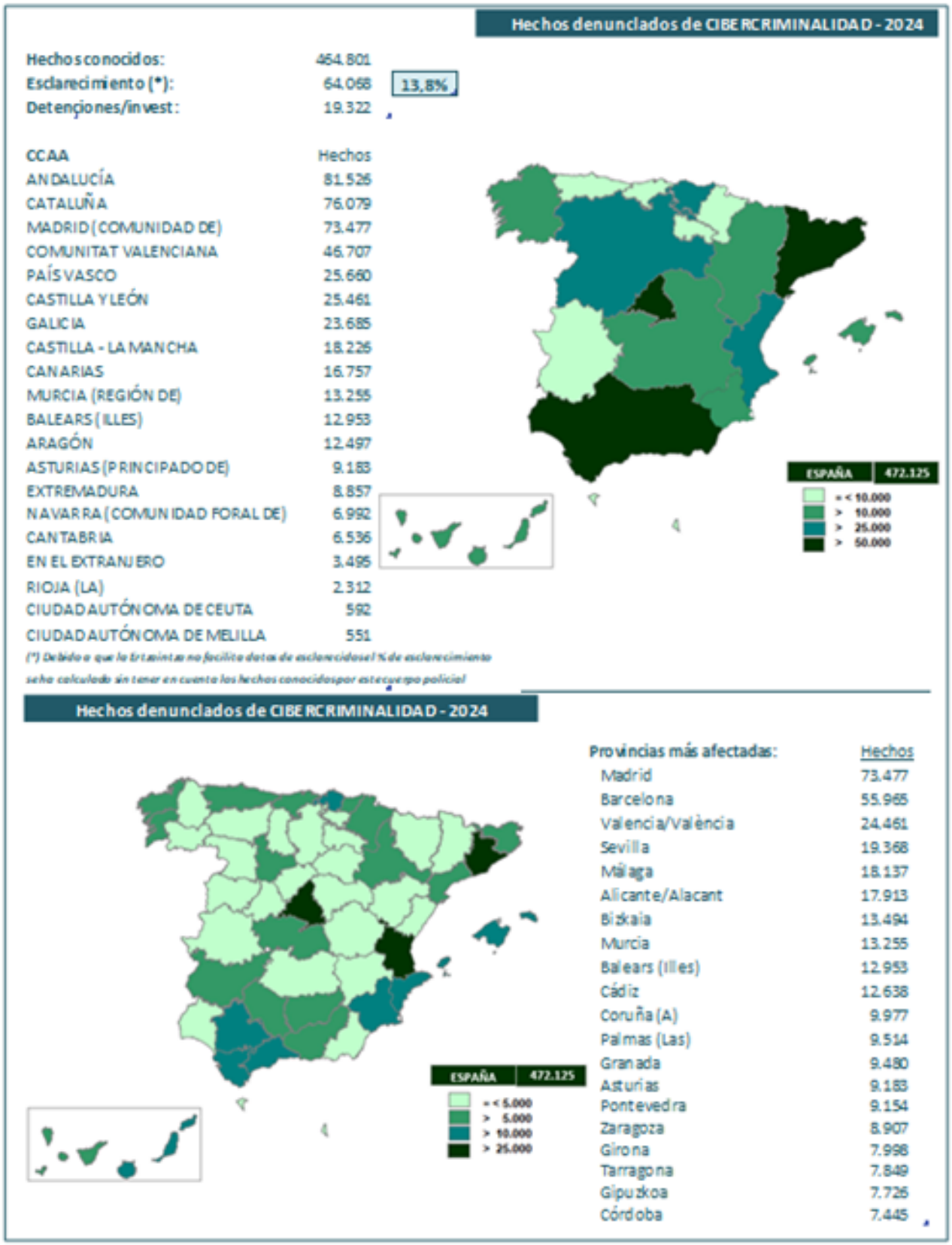


Ilustración 11. Distribución territorial de hechos denunciados de cibercriminalidad.

Los datos relativos a **victimizaciones registradas según grupo penal y sexo** sirven para definir las características y el perfil de las víctimas de los delitos informáticos en España. Este apartado recoge información proporcionada de todos los cuerpos policiales.

En 2024, las **victimizaciones** registradas por las Fuerzas y Cuerpos de Seguridad alcanzan un total de 350.795, lo que representa una **disminución del 1,08 %** respecto a 2023. De este total, un 51,2 % corresponde al sexo masculino y un 48,8 % al sexo femenino. La **mayoría de las víctimas** de ciberdelincuencia se encuentran **entre 26 y 40 años** en ambos sexos y son principalmente objeto de fraude informático.

VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	4.359	4.650	2	9.011
AMENAZAS Y COACCIONES	11.532	6.403	9	17.944
CONTRA EL HONOR	569	597	2	1.168
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	49	33	0	82
DELITOS SEXUALES	385	889	6	1.280
FALSIFICACIÓN INFORMÁTICA	7.785	7.059	3	14.847
FRAUDE INFORMÁTICO	154.072	150.601	73	304.746
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	888	787	5	1.680
Total VICTIMIZACIONES	**179.639**	**171.019**	**100**	**350.758**

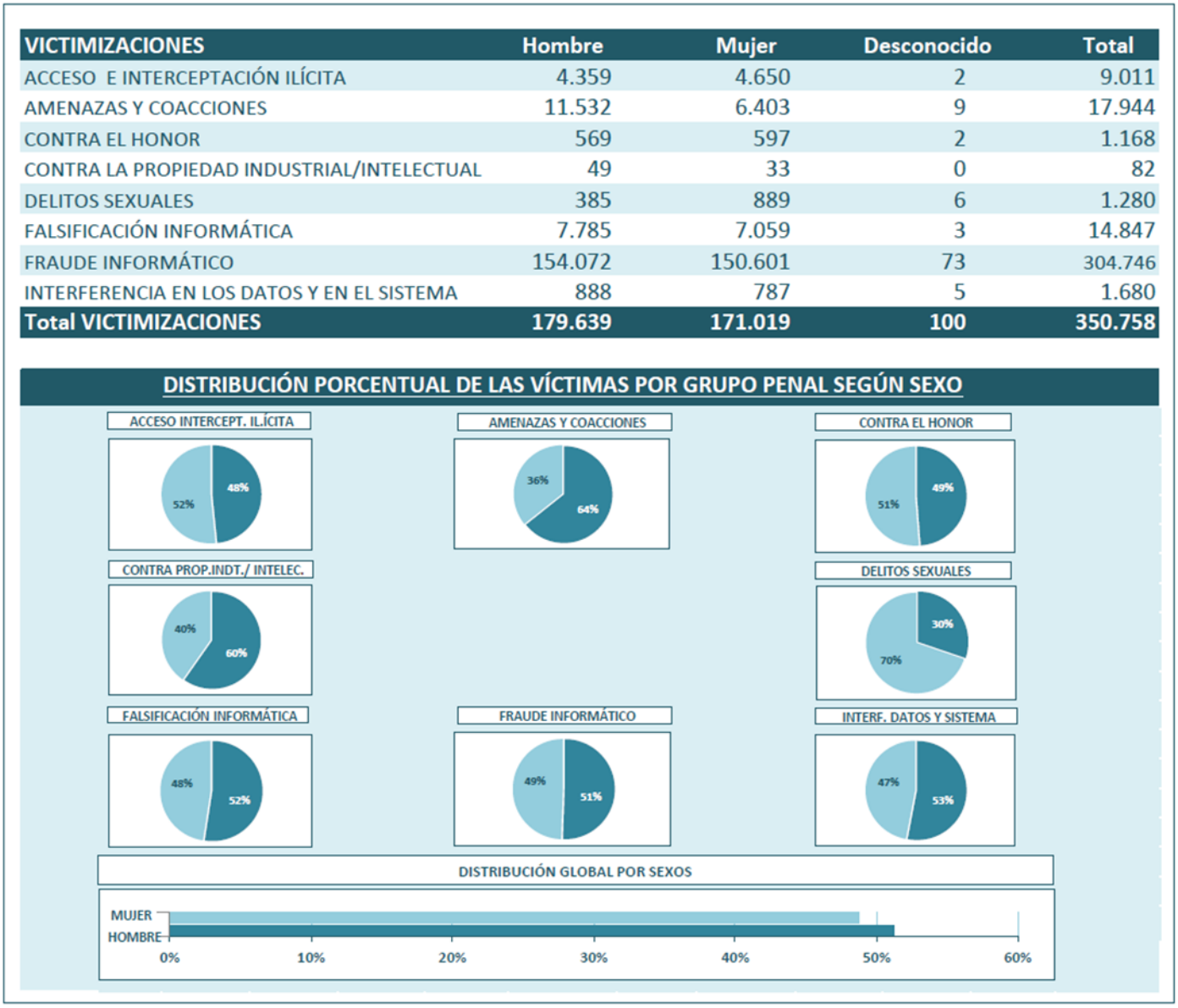
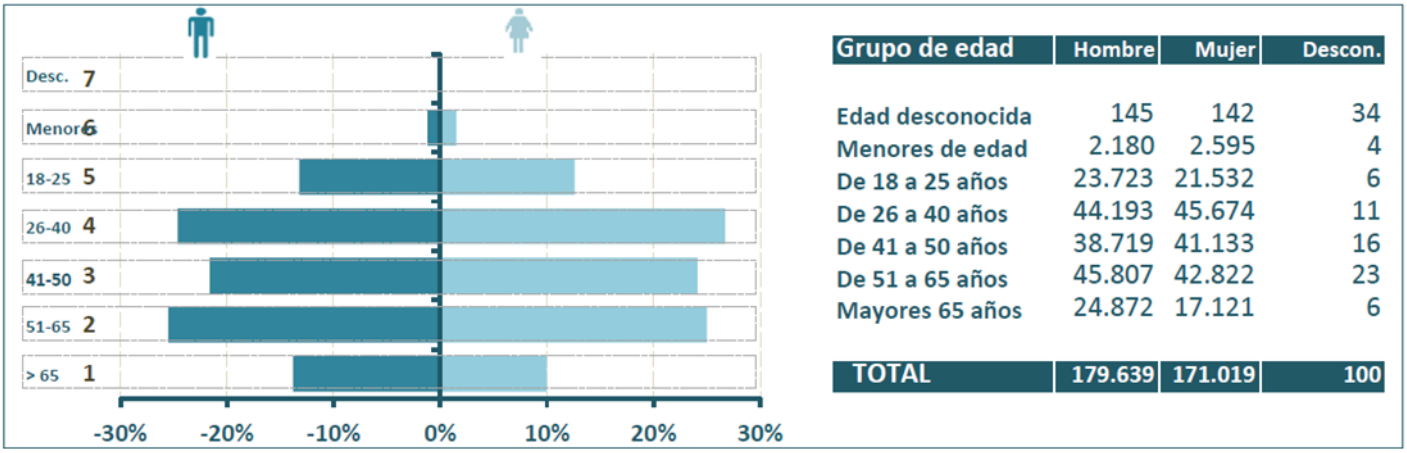


Ilustración 12. Victimizaciones registradas según grupo penal y sexo.



Grupo de edad	Hombre	Mujer	Descon.
Edad desconocida	145	142	34
Menores de edad	2.180	2.595	4
De 18 a 25 años	23.723	21.532	6
De 26 a 40 años	44.193	45.674	11
De 41 a 50 años	38.719	41.133	16
De 51 a 65 años	45.807	42.822	23
Mayores 65 años	24.872	17.121	6
TOTAL	179.639	171.019	100

Ilustración 13. Victimizaciones según grupo de edad y sexo. Fuente: SEC

En relación con **las victimizaciones por tipología penal y sexo,** observando los datos puede afirmarse que entre los principales hechos conocidos contra víctimas de ambos sexos destacan **las estafas relacionadas con tarjetas de crédito o débito y cheques de viaje.**

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS TARJ CRÉD, DÉBITO Y CHEQUES VIAJE	72.985	75.285	22	148.292
OTRAS ESTAFAS	48.487	43.134	34	91.655
ESTAFA BANCARIA	19.653	20.007	0	39.660
ESTAFAS INFORMÁTICAS	12.429	11.905	17	24.351
USURPACIÓN DE ESTADO CIVIL	7.417	6.844	2	14.263
AMENAZAS	6.377	3.994	7	10.378
EXTORSIÓN	3.772	516	1	4.289
ACCESO ILEGAL SISTEMAS INFORMÁTICOS	1.751	2.129	1	3.881
DESCUBRIMIENTO/REVELACIÓN SECRETOS	1.720	2.044	1	3.765
RESTO	5.048	5.161	15	10.224
Total VICTIMIZACIONES	**179.639**	**171.019**	**100**	**350.758**

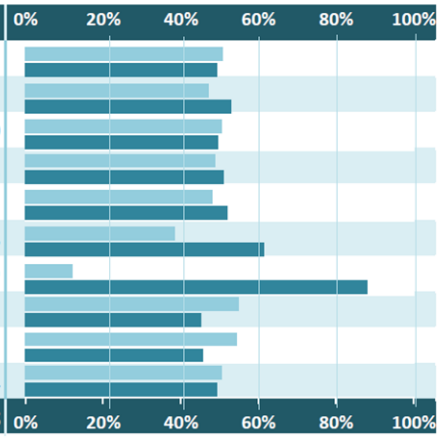


Tabla 8. Victimizaciones por tipología penal y sexo. Fuente: SEC

En cuanto a **la nacionalidad de las víctimas**, el 14,4 % son de nacionalidad extranjera, mientras que el 85,6 % restante corresponde a personas nacionalidad española. Dentro de las víctimas extranjeras, destacan las originarias de Marruecos (1,4 %), Colombia (1,3 %) y Rumanía (1 %), que presentan los valores más elevados.

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	300.223	85,6%
2.- EXTRANJEROS	50.535	14,4%
2.1.- UNIÓN EUROPEA	12.171	3,5%
RUMANÍA	3.424	1,0%
ITALIA	2.827	0,8%
FRANCIA	1.212	0,3%
BULGARIA	773	0,2%
ALEMANIA	978	0,3%
Resto	2.957	0,8%
2.2.- AMÉRICA	22.053	6,3%
COLOMBIA	4.672	1,3%
VENEZUELA	2.995	0,9%
ECUADOR	1.909	0,5%
Resto	12.477	3,6%
2.3.- ÁFRICA	8.921	2,5%
MARRUECOS	4.912	1,4%
SENEGAL	1.062	0,3%
Resto	2.947	0,8%
2.4.- ASIA	3.030	0,9%
CHINA POPULAR	982	0,3%
PAQUISTÁN	697	0,2%
Resto	1.351	0,4%
2.5.- RESTO PAÍSES	4.360	1,2%
UCRANIA	1.096	0,3%
REINO UNIDO	894	0,3%
Otros	2.370	0,7%
TOTAL	350.758	100%

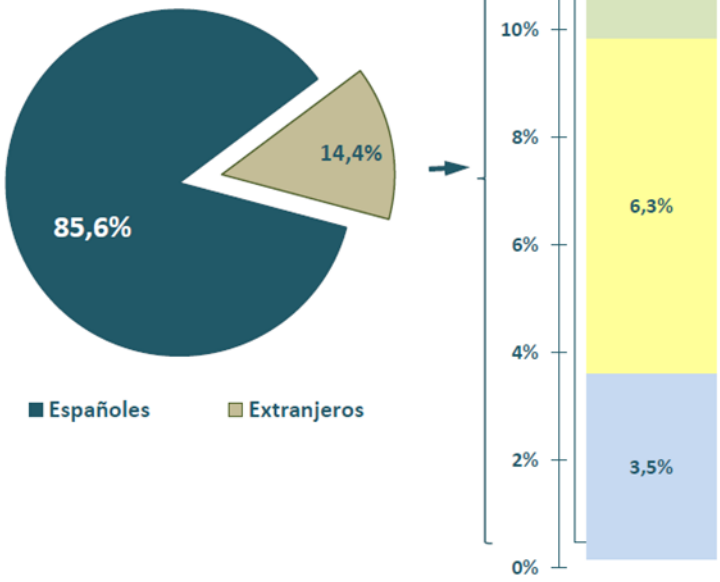


Ilustración 14. Nacionalidad de la víctima. Fuente: SEC

Tal como se presentó en el informe de 2023, el Informe sobre la Cibercriminalidad en España de 2024 incorpora datos que permiten analizar la relación entre los rangos de edad de las víctimas y la tipología penal de los delitos sufridos. Según los registros, el **fraude informático** es el delito con **mayor incidencia en todos los grupos de edad establecidos, salvo en el caso de menores de edad**. Dentro de este grupo penal destacan especialmente los segmentos de población entre los 18 y 25 años y el grupo mayores de 65 años, donde el número de victimizaciones es la mitad que el de resto de grupos de edad comprendidos entre los 26 y 65 años.

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	9	628	1.511	2.736	2.028	1.714	385
AMENAZAS Y COACCIONES	26	1.606	4.903	5.343	3.330	2.234	502
CONTRA EL HONOR	8	92	119	375	310	240	24
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	3	22	23	32	2
DELITOS SEXUALES	6	1.078	77	54	43	21	1
FALSIFICACIÓN INFORMÁTICA	20	182	1.729	4.669	3.632	3.586	1.029
FRAUDE INFORMÁTICO	248	1.175	36.783	76.232	70.029	80.321	39.958
INTERFERENCIA EN DATOS Y EN SISTEMA	4	18	136	447	473	504	98
Total VICTIMIZACIONES	**321**	**4.779**	**45.261**	**89.878**	**79.868**	**88.652**	**41.999**

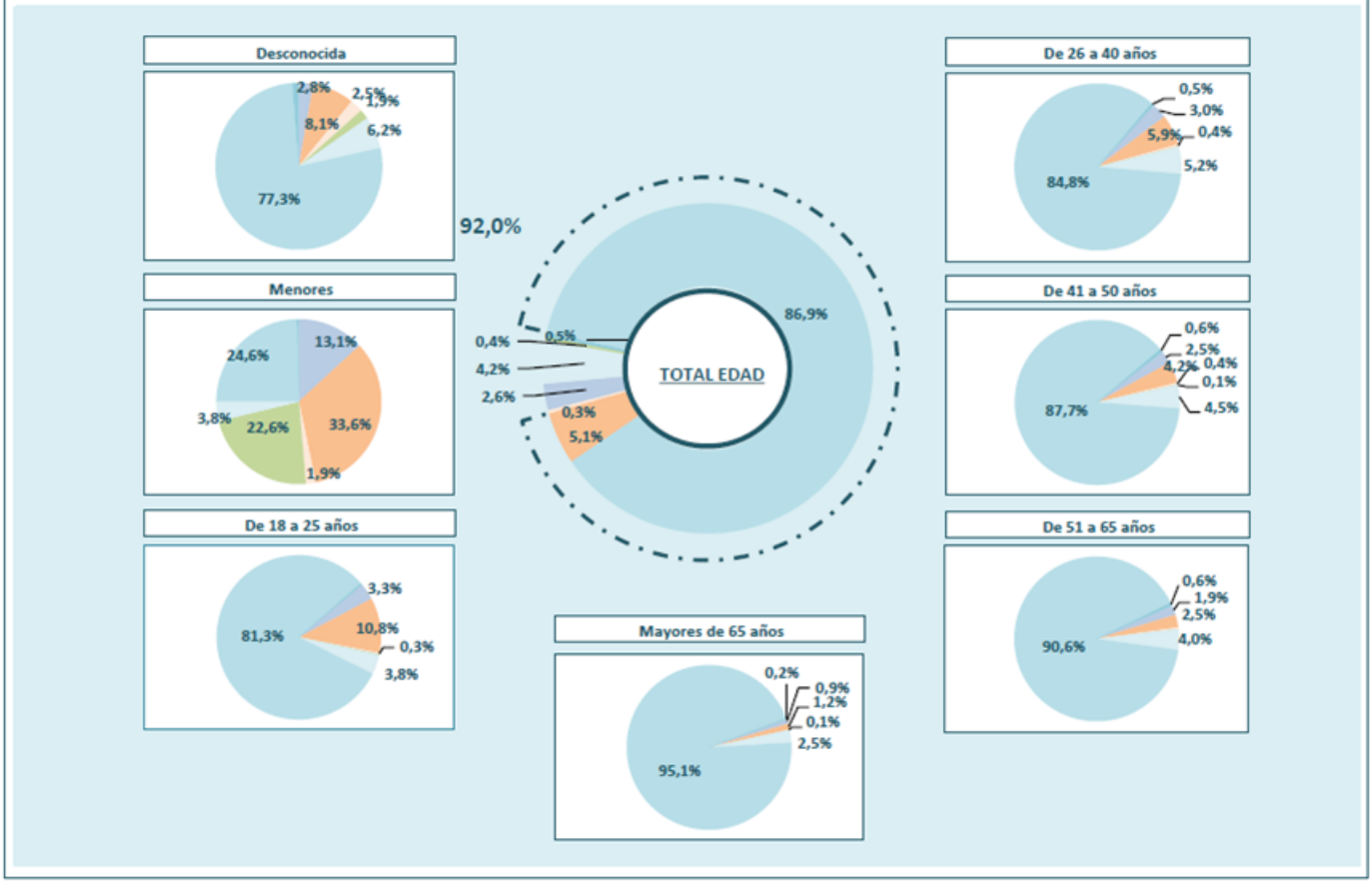
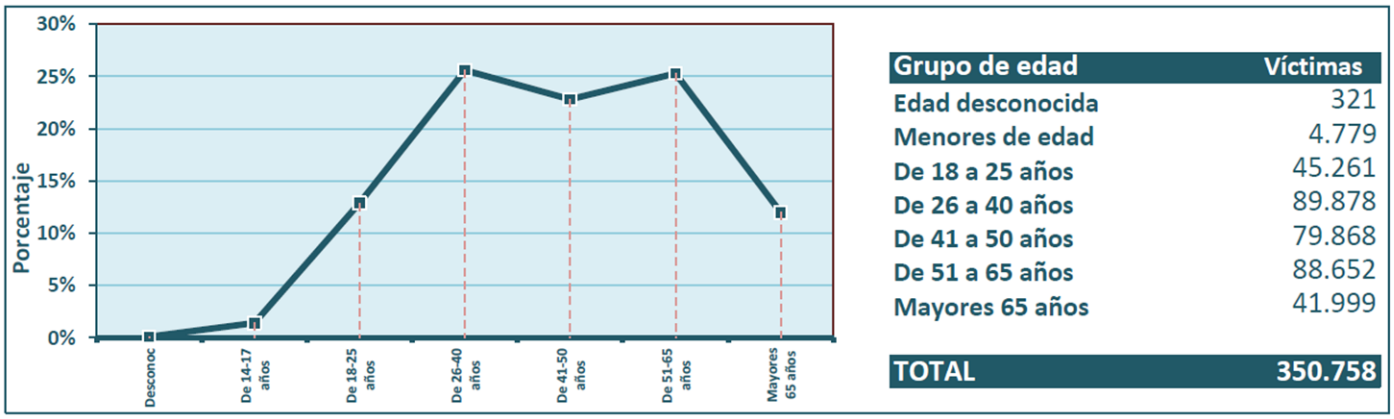


Ilustración 15. Victimizaciones registradas según grupo penal y edad. Fuente: SEC

El análisis de la información extraída del SEC revela que el comportamiento de las **víctimas menores de edad** no sigue el mismo patrón que el de las víctimas adultas. Este grupo presenta una mayor vulnerabilidad ante otro tipo de delitos, especialmente **amenazas, coacciones y delitos sexuales**.

En términos generales, el rango de edad donde existe un mayor volumen de víctimas está entre los 26 y 65 años, principalmente por el fraude informático, como se ha señalado anteriormente.



Grupo de edad	Víctimas
Edad desconocida	321
Menores de edad	4.779
De 18 a 25 años	45.261
De 26 a 40 años	89.878
De 41 a 50 años	79.868
De 51 a 65 años	88.652
Mayores 65 años	41.999
TOTAL	350.758

Ilustración 16. Edad de la víctima. Fuente: SEC

Asimismo, este estudio recoge datos detallados sobre **victimizaciones según el sexo**. La Ilustración 17 e Ilustración 18 presentan información relativa al sexo masculino, mientras que la Ilustración 19 e Ilustración 20 abordan la del sexo femenino. Ambos grupos comparten una característica común:

La **ciberdelincuencia de naturaleza sexual** tiene su mayor incidencia en menores de edad, con valores **particularmente elevados en el sexo femenino**. Además, se observa que, en el grupo de **mayores de 65 años**, **el fraude informático** destaca en términos porcentuales dentro del total de delitos de cibercriminalidad registrados para cada rango de edad.

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	4	231	816	1.320	910	877	201
AMENAZAS Y COACCIONES	10	885	3.758	3.294	1.842	1.395	348
CONTRA EL HONOR	6	23	43	190	152	137	18
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	0	14	12	22	1
DELITOS SEXUALES	1	335	21	11	12	5	0
FALSIFICACIÓN INFORMÁTICA	9	64	819	2.372	1.882	2.030	609
FRAUDE INFORMÁTICO	112	633	18.209	36.742	33.668	41.066	23.642
INTERFERENCIA EN DATOS Y EN SISTEMA	3	9	57	250	241	275	53
Total VICTIMIZACIONES	**145**	**2.180**	**23.723**	**44.193**	**38.719**	**45.807**	**24.872**

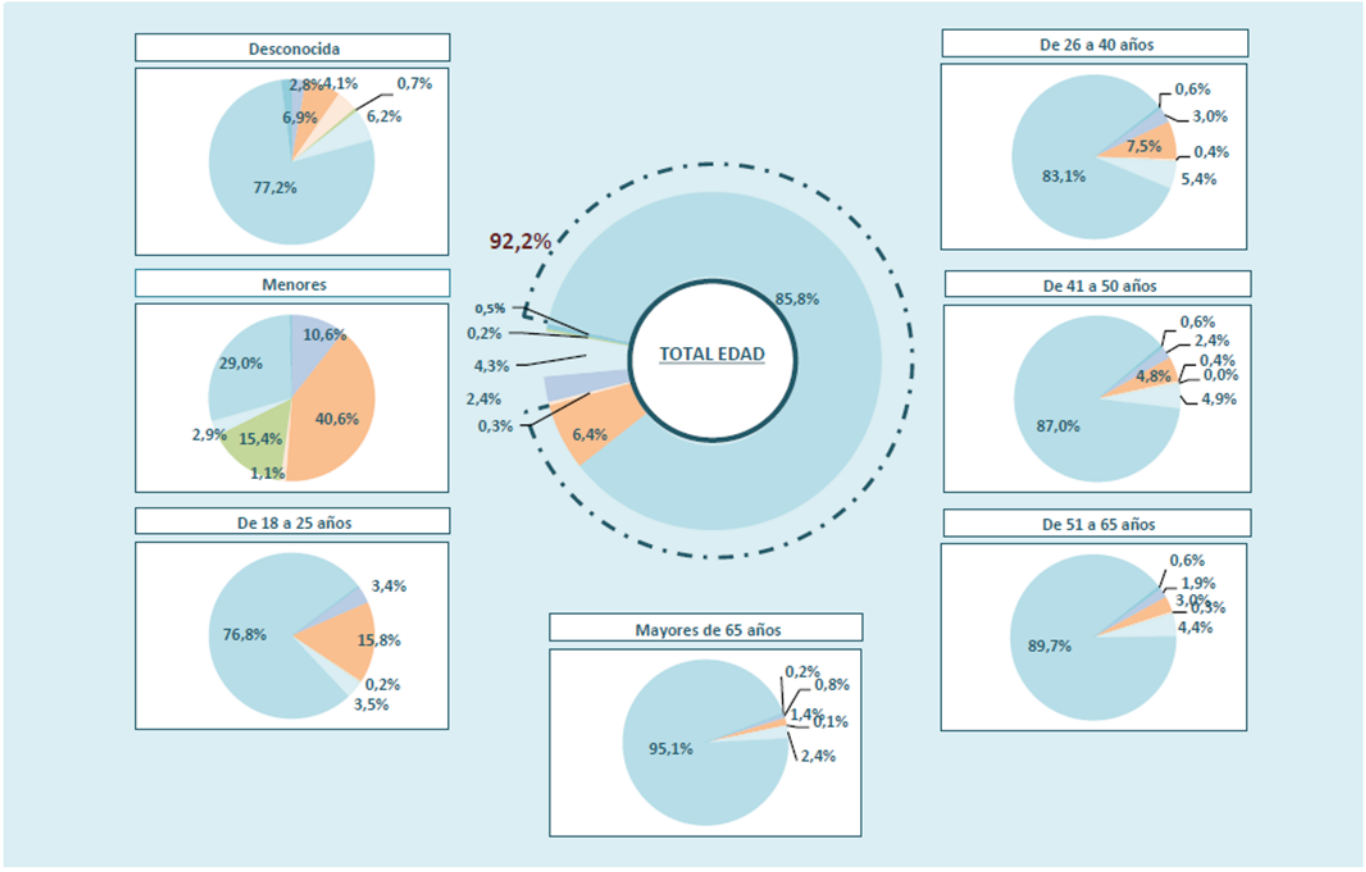
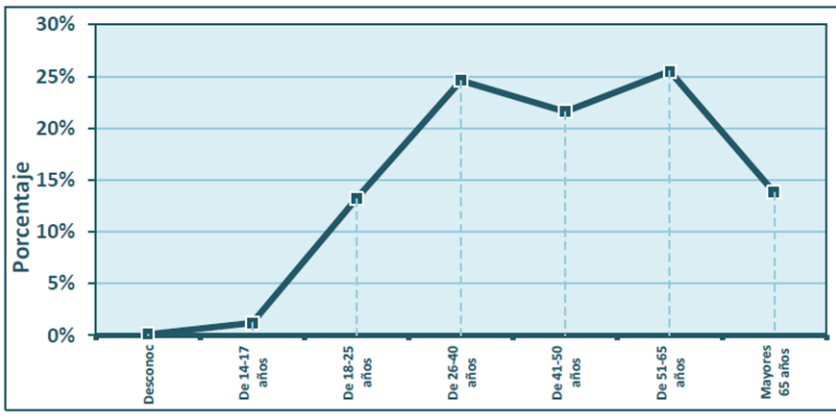


Ilustración 17. Victimizaciones registradas según grupo penal y edad. Sexo masculino. Fuente: SEC



Grupo de edad	Víctimas
Edad desconocida	145
Menores de edad	2.180
De 18 a 25 años	23.723
De 26 a 40 años	44.193
De 41 a 50 años	38.719
De 51 a 65 años	45.807
Mayores 65 años	24.872
TOTAL	**179.639**

Ilustración 18. Edad de las victimas masculinas. Fuente: SEC

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	5	396	695	1.415	1.118	837	184
AMENAZAS Y COACCIONES	13	721	1.144	2.048	1.486	838	153
CONTRA EL HONOR	2	69	76	183	158	103	6
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	3	8	11	10	1
DELITOS SEXUALES	2	740	56	43	31	16	1
FALSIFICACIÓN INFORMÁTICA	10	118	909	2.296	1.750	1.556	420
FRAUDE INFORMÁTICO	110	542	18.570	39.484	36.351	39.233	16.311
INTERFERENCIA EN DATOS Y EN SISTEMA	0	9	79	197	228	229	45
Total VICTIMIZACIONES	**142**	**2.595**	**21.532**	**45.674**	**41.133**	**42.822**	**17.121**

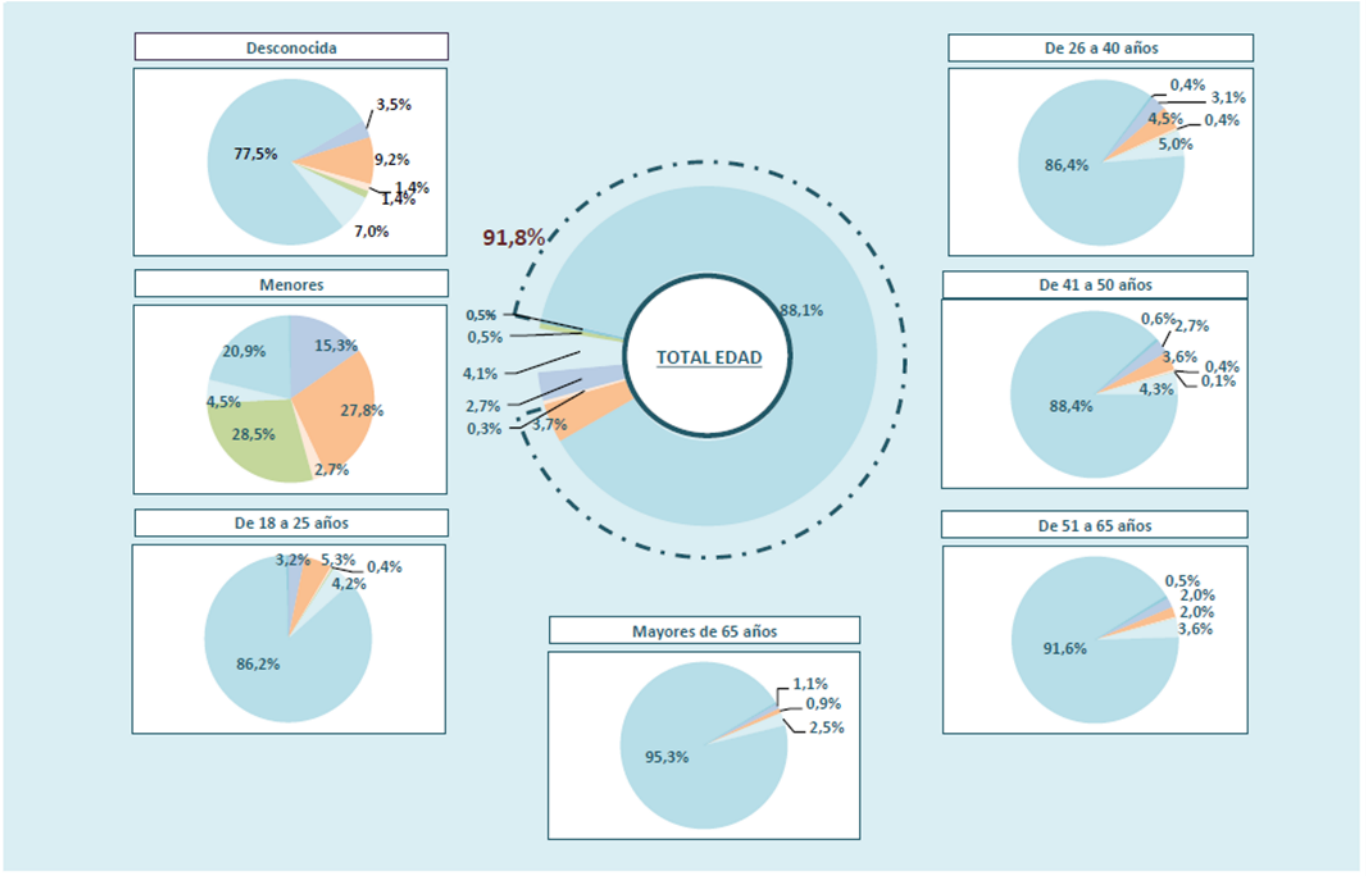
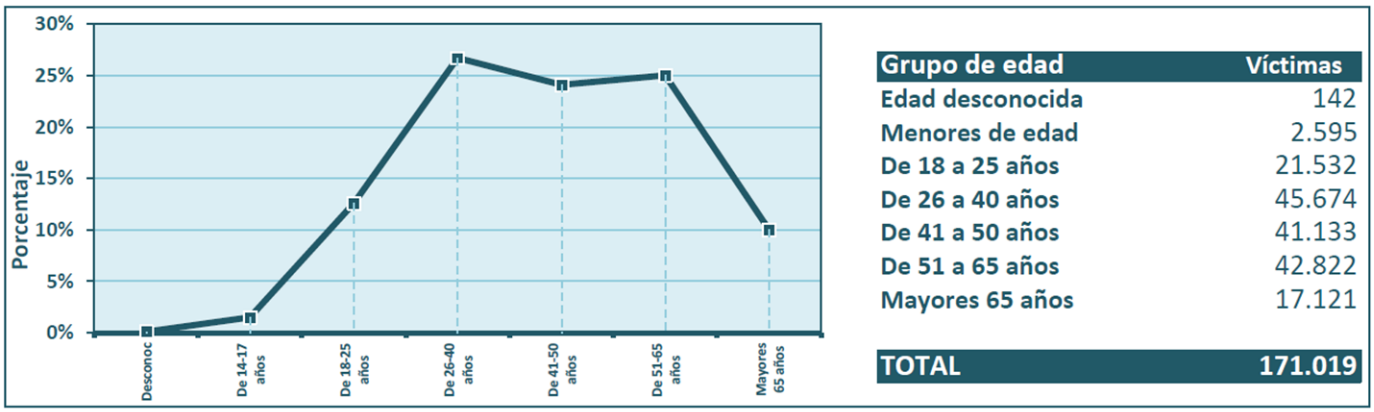


Ilustración 19. Victimizaciones registradas según grupo penal y edad. Sexo femenino. Fuente SEC



Grupo de edad	Víctimas
Edad desconocida	142
Menores de edad	2.595
De 18 a 25 años	21.532
De 26 a 40 años	45.674
De 41 a 50 años	41.133
De 51 a 65 años	42.822
Mayores 65 años	17.121
TOTAL	**171.019**

Ilustración 20. Edad de la víctima. Sexo femenino. Fuente: SEC

Relativo a información sobre **detenciones e investigados** según el tipo penal y sexo, del total de detenciones e investigaciones realizadas por las Fuerzas y Cuerpos de Seguridad, el número asciende a 19.322, siendo un 71,5 % de este total correspondiente al sexo masculino. Los principales motivos de estas intervenciones han sido por fraude informático, así como delitos de amenazas y coacciones, y delitos sexuales. Por otro lado, la mayoría de las detenciones e investigaciones de personas de sexo femenino se han llevado a cabo por delitos relacionados con fraude informático.

DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	396	123	519
AMENAZAS Y COACCIONES	1.790	569	2.359
CONTRA EL HONOR	68	33	101
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	113	31	144
DELITOS SEXUALES	770	27	797
FALSIFICACIÓN INFORMÁTICA	461	266	727
FRAUDE INFORMÁTICO	10.188	4.452	14.640
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	28	7	35
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**13.814**	**5.508**	**19.322**

ISTRIBUCIÓN PORCENTUAL DE LAS DETENCIONES/INVESTIGADOS POR GRUPO PENAL SEGÚN SEXO

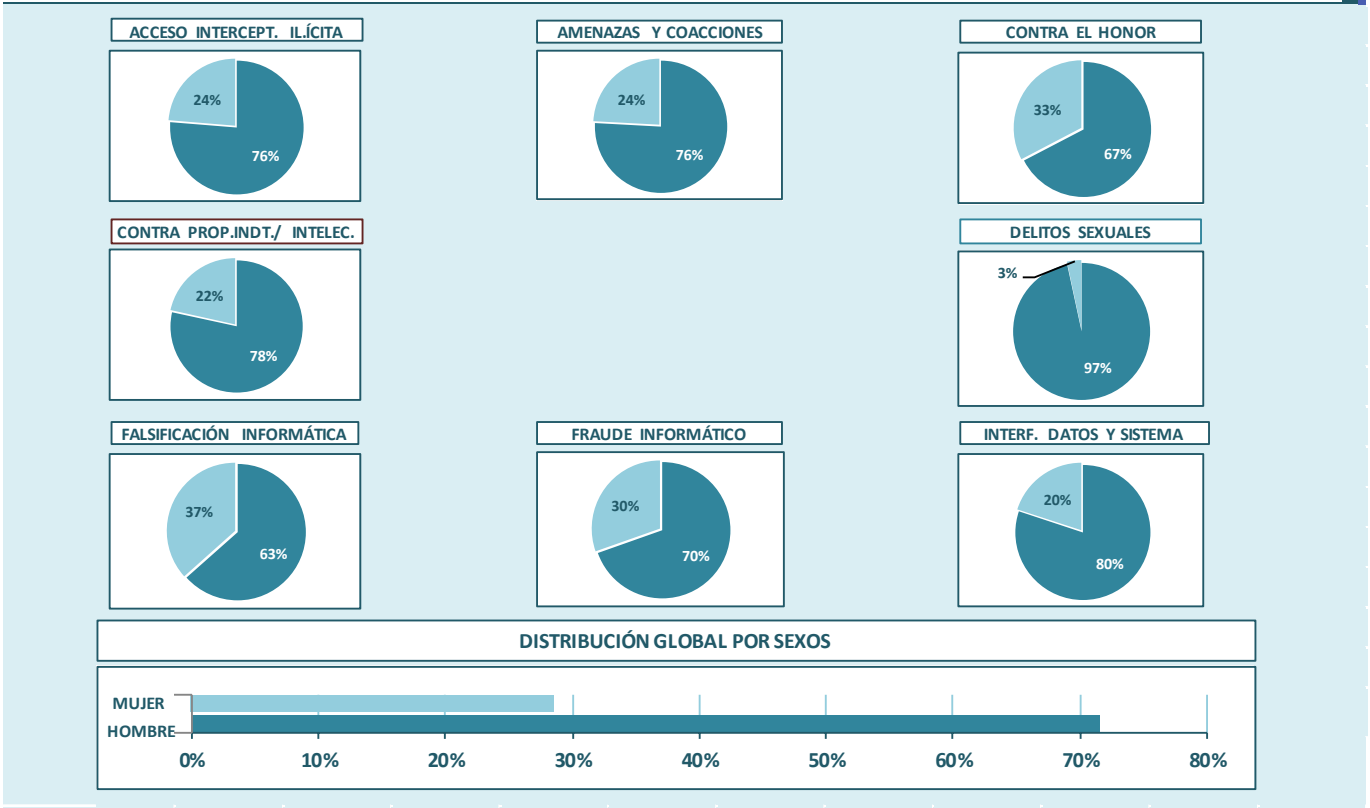
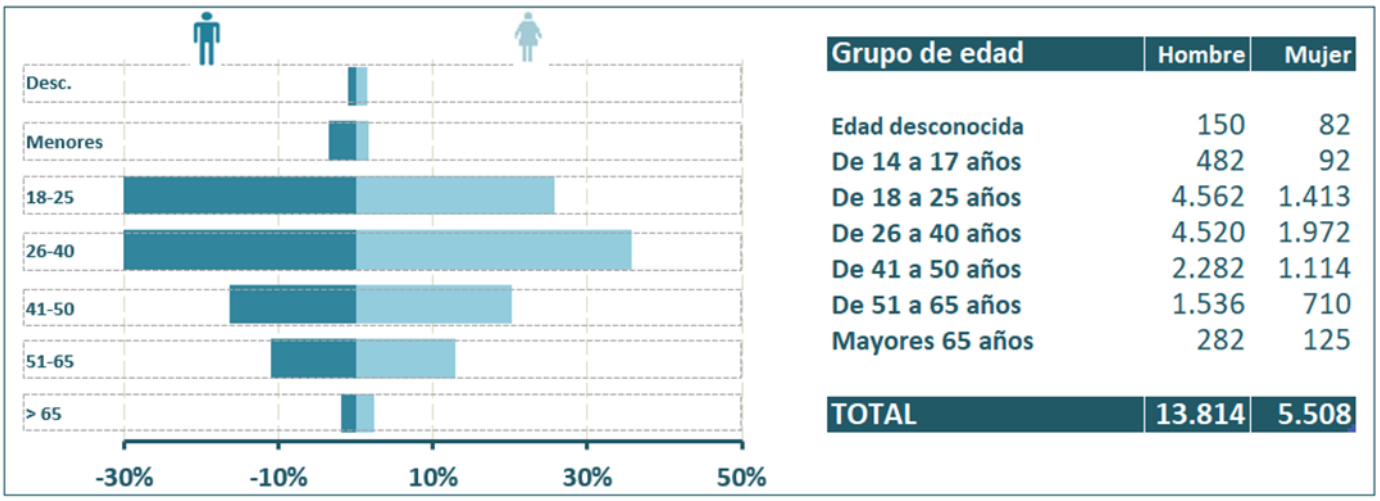


Ilustración 21. Detenciones/investigados registrados según grupo penal y sexo. Fuente: SEC



Grupo de edad	Hombre	Mujer
Edad desconocida	150	82
De 14 a 17 años	482	92
De 18 a 25 años	4.562	1.413
De 26 a 40 años	4.520	1.972
De 41 a 50 años	2.282	1.114
De 51 a 65 años	1.536	710
Mayores 65 años	282	125
TOTAL	13.814	5.508

Ilustración 22. Detenciones/investigados registrados según grupo edad y sexo. Fuente: SEC

Por lo que respecta a las diferentes infracciones penales (**detenciones/investigados por tipología penal y sexo**), los datos establecen que las causas por las que las personas de ambos sexos han sido objeto de detención/investigación han sido principalmente por el grupo denominado «otras estafas», que incluye entre otros, *phishing*, venta online fraudulenta u otras formas de engaño.

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	6.898	3.035	9.933
ESTAFAS TARJETA CRÉD, DÉBITO Y CHEQUES VIAJE	2.018	921	2.939
ESTAFAS INFORMÁTICAS	1.159	470	1.629
AMENAZAS	1.080	367	1.447
USURPACIÓN DE ESTADO CIVIL	409	247	656
PORNOGRAFÍA DE MENORES	424	18	442
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	231	71	302
EXTORSIÓN	274	83	357
COACCIONES	180	68	248
RESTO	1.141	228	1.369
Total VICTIMIZACIONES CIBERCRIMINALIDAD	**13.814**	**5.508**	**19.322**

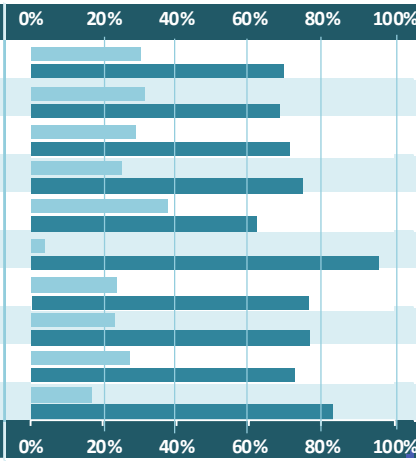


Tabla 9 Detenciones/investigados por tipología penal y sexo. Fuente: SEC

La mayoría de las personas detenidas o investigadas por ciberdelincuencia son de nacionalidad española, representando un 76,2 % del total. En cuanto a los detenidos e investigados de nacionalidad extranjera, los datos muestran que los casos más numerosos corresponden a ciudadanos originarios de Marruecos (3,6%), Colombia (2,5 %) y Rumanía (2 %).

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	14.724	76,2%
2.- EXTRANJEROS	4.598	23,8%
2.1.- UNIÓN EUROPEA	801	4,1%
RUMANÍA	382	2,0%
BULGARIA	53	0,3%
ITALIA	79	0,4%
FRANCIA	57	0,3%
PORTUGAL	59	0,3%
Resto	171	0,9%
2.2.- AMÉRICA	2.045	10,6%
COLOMBIA	485	2,5%
REP. DOMINICANA	300	1,6%
VENEZUELA	333	1,7%
Resto	927	4,8%
2.3.- ÁFRICA	1.235	6,4%
MARRUECOS	688	3,6%
NIGERIA	99	0,5%
Resto	448	2,3%
2.4.- ASIA	142	0,7%
BANGLADESH	16	0,1%
PAQUISTÁN	36	0,2%
Resto	90	0,5%
2.5.- RESTO PAÍSES	375	1,9%
UCRANIA	85	0,4%
RUSIA	55	0,3%
Otros	235	1,2%
TOTAL	19.322	100%

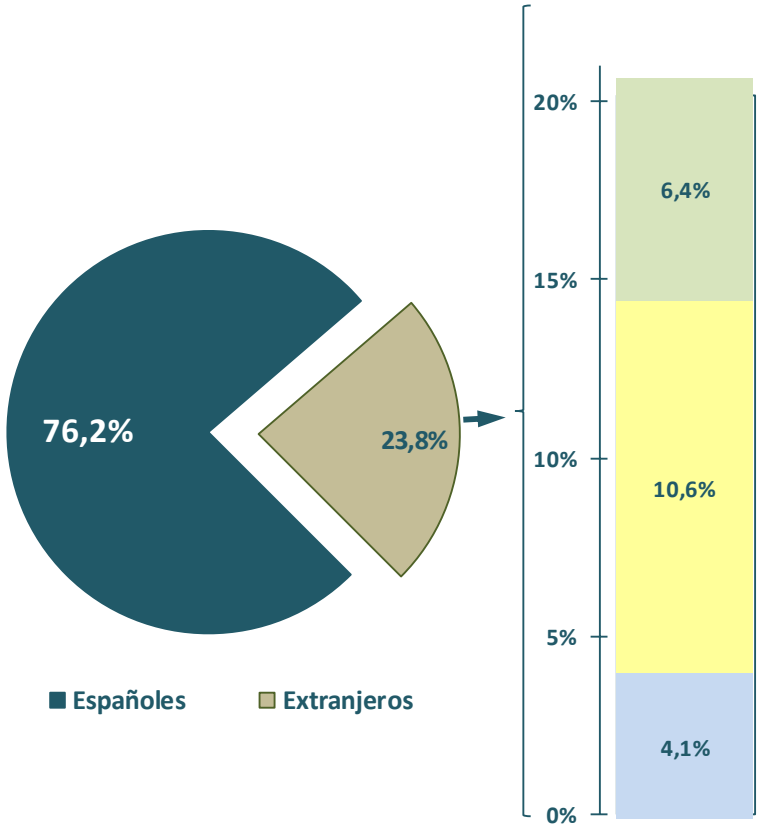


Ilustración 23. Nacionalidad de las detenciones/investigados. Fuente: SEC

Al analizar la información según los rangos de edad sobre detenciones/investigados según grupo de edad y sexo, se observa que el mayor número de responsables de ciberdelincuencia se concentra en el grupo de edad comprendido entre **los 26 y 40 años**.

Rango de edad de los detenidos/investigados							
GRUPO PENAL	**Descon.**	**14-17**	**18-25**	**26-40**	**41-50**	**51-65**	**> 65**
ACCESO E INTERCEPTACIÓN ILÍCITA	1	143	103	147	72	45	8
AMENAZAS Y COACCIONES	13	150	475	862	515	302	42
CONTRA EL HONOR	0	7	11	34	23	21	5
CONTRA PROPIEDAD INDUST./INTELEC.	1	1	6	41	50	38	7
DELITOS SEXUALES	3	116	177	191	143	129	38
FALSIFICACIÓN INFORMÁTICA	7	10	139	283	165	109	14
FRAUDE INFORMÁTICO	207	145	5049	4927	2.422	1.597	293
INTERFERENCIA EN DATOS Y EN SISTEMA	0	2	15	7	6	5	0
Total DETENCIONES/INVESTIGADOS	**232**	**574**	**5.975**	**6.492**	**3.396**	**2.246**	**407**

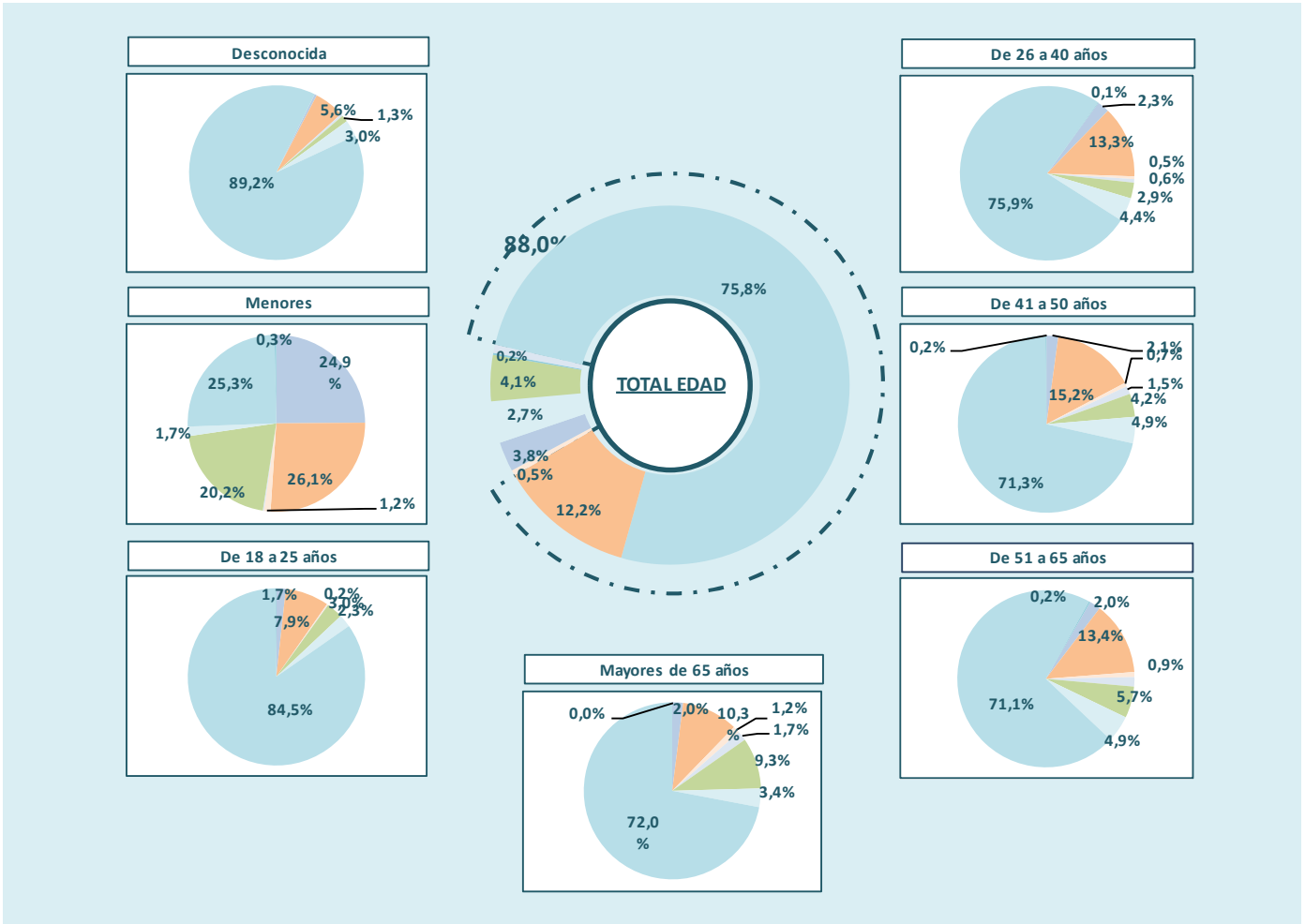
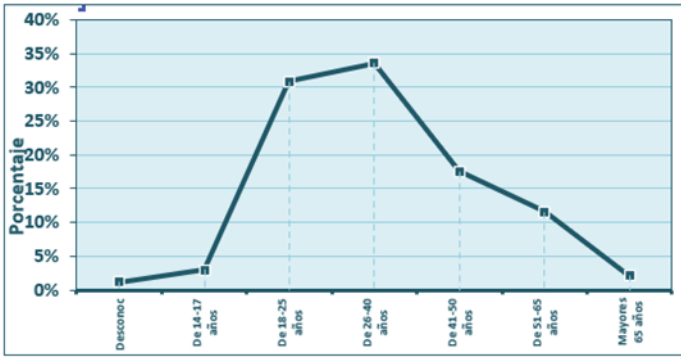


Ilustración 24. Detenciones/investigados registrados según grupo penal y edad. Fuente: SEC



Grupo de edad	Det./Inv.
Edad desconocida	232
De 14 a 17 años	574
De 18 a 25 años	5.975
De 26 a 40 años	6.492
De 41 a 50 años	3.396
De 51 a 65 años	2.246
Mayores 65 años	407
TOTAL	19.322

Ilustración 25. Edad de las personas detenidas/investigadas. Fuente: SEC

Rango de edad de los detenidos/investigados							
GRUPO PENAL	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	123	85	104	50	27	6
AMENAZAS Y COACCIONES	8	114	360	667	379	228	34
CONTRA EL HONOR	0	5	5	25	17	13	3
CONTRA PROPIEDAD INDUST./INTELEC.	0	1	5	32	39	29	7
DELITOS SEXUALES	3	111	174	184	136	124	38
FALSIFICACIÓN INFORMÁTICA	1	5	105	179	98	66	7
FRAUDE INFORMÁTICO	137	121	3.814	3.325	1.559	1.045	187
INTERFERENCIA EN DATOS Y EN SISTEMA	0	2	14	4	4	4	0
Total DETENCIONES/INVESTIGADOS	**150**	**482**	**4.562**	**4.520**	**2.282**	**1.536**	**282**

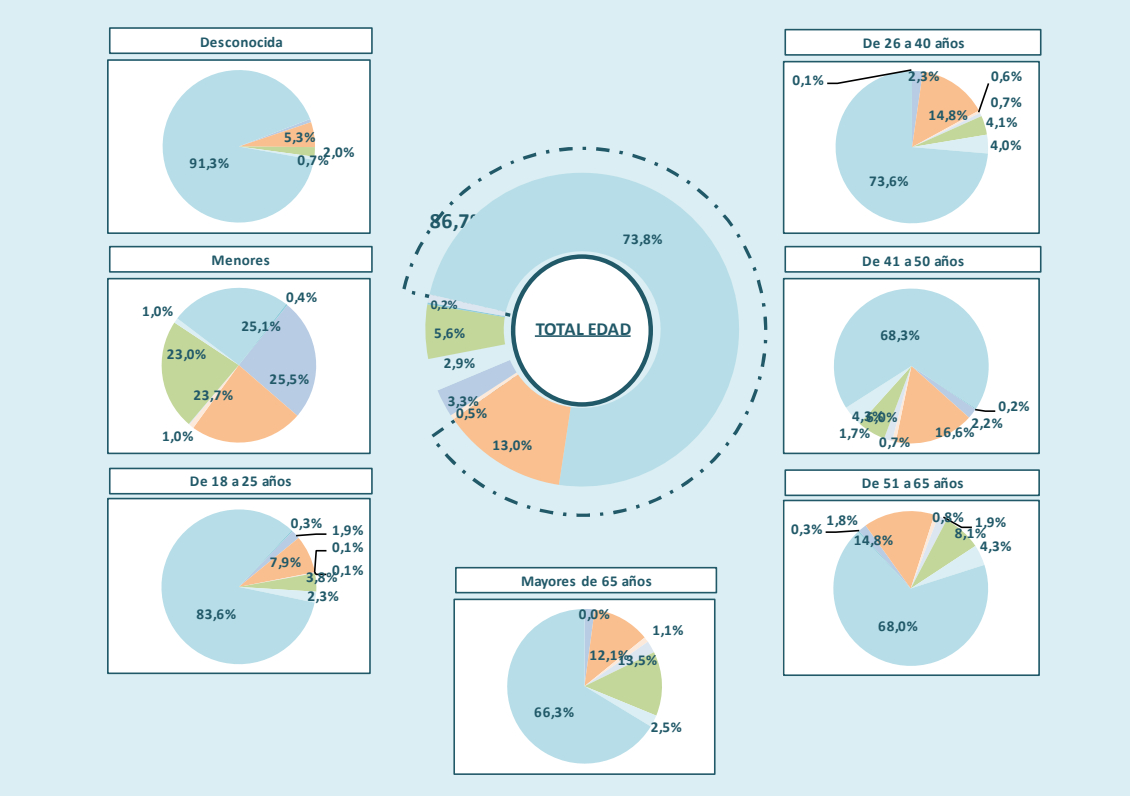
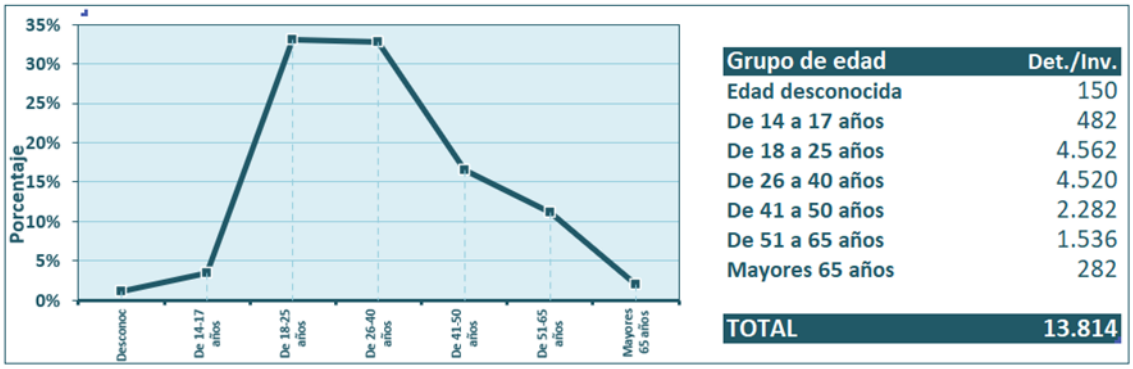


Ilustración 26. Detenciones/investigados registrados según grupo penal y edad. Sexo masculino. Fuente: SEC



Grupo de edad	Det./Inv.
Edad desconocida	150
De 14 a 17 años	482
De 18 a 25 años	4.562
De 26 a 40 años	4.520
De 41 a 50 años	2.282
De 51 a 65 años	1.536
Mayores 65 años	282
TOTAL	13.814

Ilustración 27. Edad de las personas detenidas/investigadas. Sexo masculino. Fuente:SEC

GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	20	18	43	22	18	2
AMENAZAS Y COACCIONES	5	36	115	195	136	74	8
CONTRA EL HONOR	0	2	6	9	6	8	2
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	9	11	9	0
DELITOS SEXUALES	0	5	3	7	7	5	0
FALSIFICACIÓN INFORMÁTICA	6	5	34	104	67	43	7
FRAUDE INFORMÁTICO	70	24	1.235	1.602	863	552	106
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	1	3	2	1	0
Total DETENCIONES/INVESTIGADOS	**82**	**92**	**1.413**	**1.972**	**1.114**	**710**	**125**

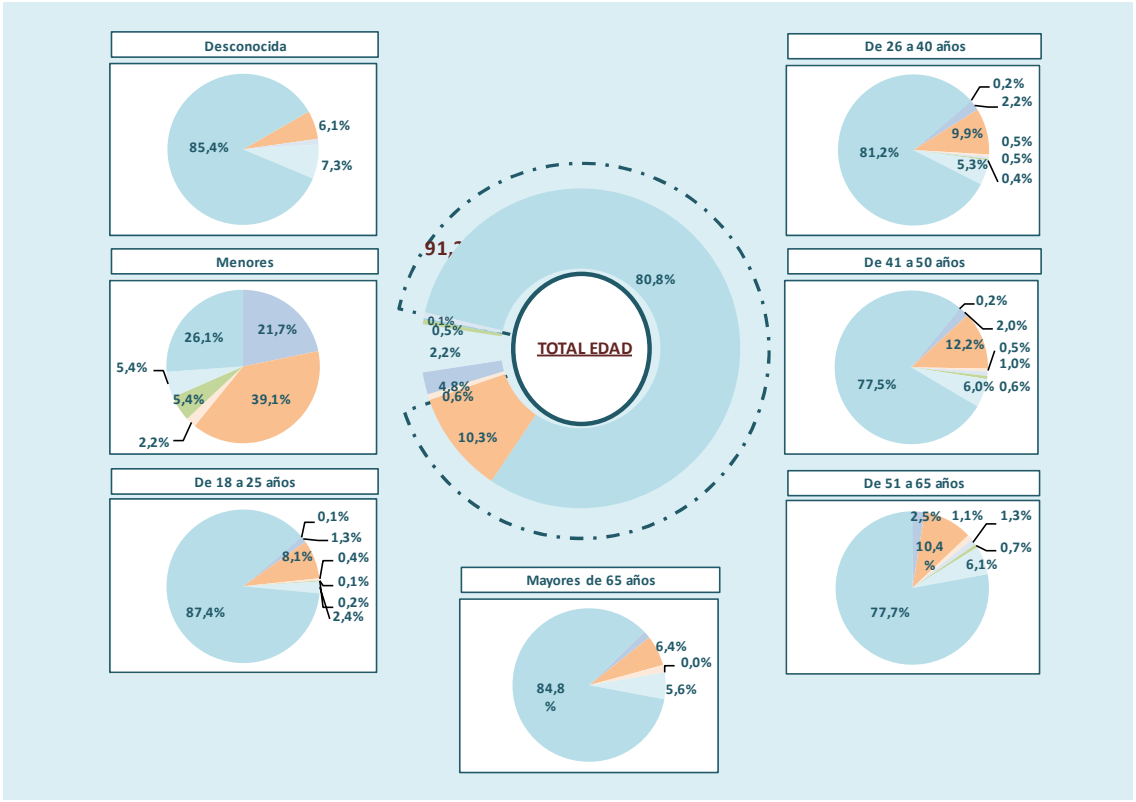
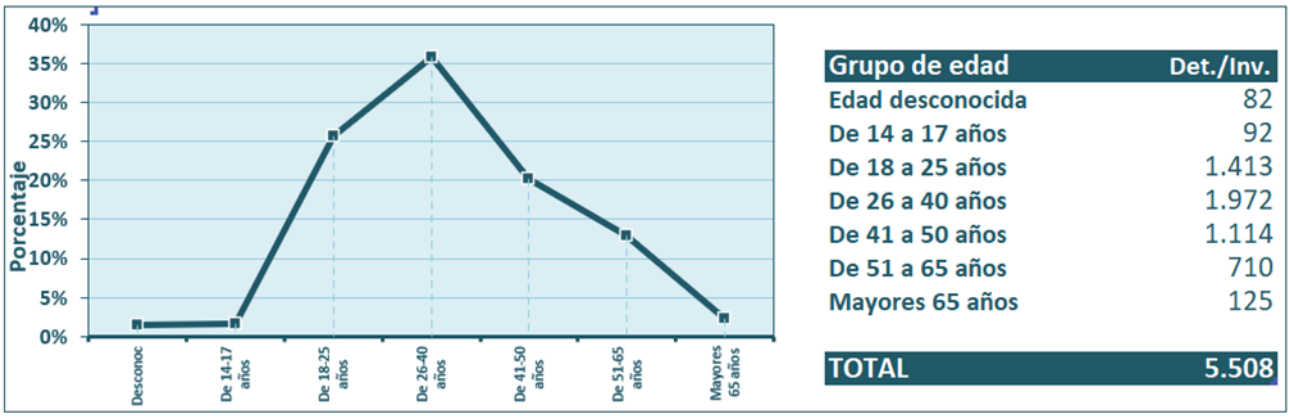


Ilustración 28. Detenciones/investigados registrados según grupo penal y edad. Sexo femenino. Fuente: SEC



Grupo de edad	Det./Inv.
Edad desconocida	82
De 14 a 17 años	92
De 18 a 25 años	1.413
De 26 a 40 años	1.972
De 41 a 50 años	1.114
De 51 a 65 años	710
Mayores 65 años	125
TOTAL	5.508

Ilustración 29. Edad de las personas detenidas/investigadas. Sexo femenino. Fuente: SEC

4

CIBERATAQUES

COMPARATIVA ENTRE DIFERENTES FUENTES

4. CIBERATAQUES: Comparativa entre diferentes fuentes

Desde su puesta en marcha en enero de 2008, **el SEC ha evolucionado significativamente**. A lo largo de los años, la incorporación progresiva de nuevos organismos dedicados a la monitorización, recopilación y análisis de datos vinculados a la ciberdelincuencia ha permitido un avance sustancial en la captación de información. Esta evolución ha marcado un salto cuantitativo en la capacidad de analizar datos desde diversas perspectivas, enriqueciendo el conocimiento que servirá de soporte para fortalecer los mecanismos en la lucha contra los delitos en el ámbito digital.

Uno de los organismos públicos más relevantes en esta obtención de distintos tipos de datos relacionados con la ciberdelincuencia es la **OCC,** creada en el año 2014 y que, desde la puesta en marcha de su **Observatorio de la Cibercriminalidad,** adopta una metodología más amplia en la obtención y análisis de los datos de cibercriminalidad, poniendo el foco, principalmente, en aquellos tipos delincuenciales que atentan contra las redes y los sistemas de información.

El SEC centraliza la recopilación, procesamiento y análisis de numerosos **datos aportados por los diferentes Cuerpos de Seguridad**, incluyendo los relacionados con la cibercriminalidad. Esta última información, integra tanto aquellos delitos que se cometen haciendo uso de medios tecnológicos para su consecución o dificultar la investigación, así como aquellos cuyo fin es atentar contra los propios sistemas informáticos. Su finalidad consiste en generar estadísticas, basadas íntegramente en la actividad policial, que permitan evaluar las tendencias delictivas y así poder diseñar estrategias de prevención y respuesta. Por otro lado, la OCC monitoriza y detecta amenazas en el ámbito de la ciberseguridad y la cibercriminalidad recabando información de **múltiples fuentes**, con un **enfoque** más **estratégico** en la **lucha** contra las **amenazas digitales**.

Debido a las diferentes fuentes empleadas, la variación en los datos es evidente al comparar las cifras registradas por el **SEC** y la **OCC** respecto a ciertos **ciberataques**. En particular, el análisis de dos amenazas específicas como son el ***ransomware*** y los ***ataques de denegación de servicios (DDoS)*** pone de manifiesto diferencias significativas. Esta variación responde a los distintos orígenes, enfoques y metodologías de recopilación y análisis de información empleados por cada organismo, lo que influye directamente en la interpretación y alcance de los datos obtenidos.

Por lo que respecta al *Ransomware,* se puede definir como un tipo de *malware* que infecta una máquina cifrando la información que contiene o el acceso a la misma, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente, la víctima recibe, posteriormente, algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que le permita recuperar los archivos bloqueados, y suele ir precedido de un robo de información.

A escala internacional, la información recopilada a través de fuentes abiertas, indica que los ataques de tipo *ransomware* continúan aumentando, registrándose desde el año 2022, un crecimiento de casi el 90 % en este tipo de ciberincidentes.

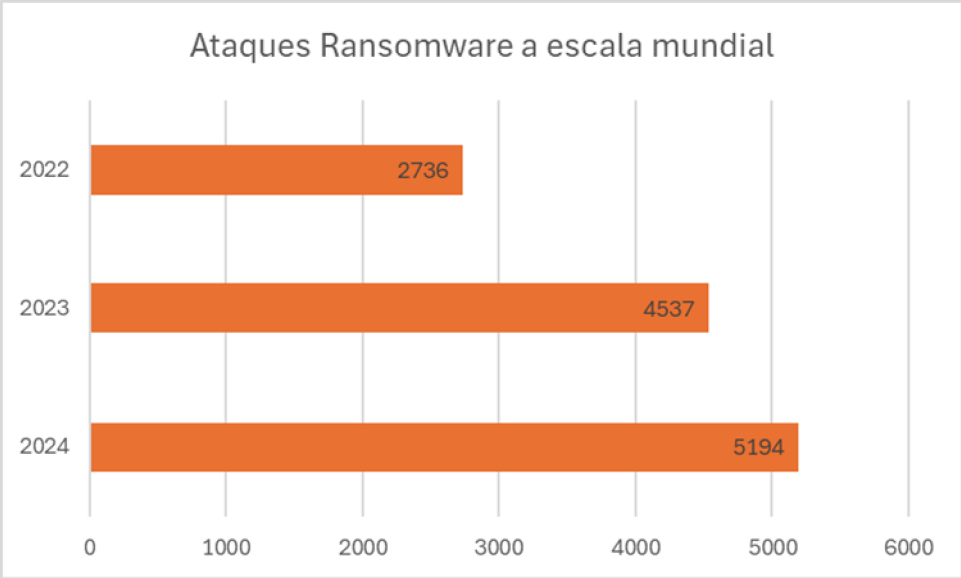


Ilustración 30. Ransomware a nivel mundial por años. Fuente: OCC

Dentro del entorno nacional, en la siguiente tabla puede observarse el número de ataques de *ransomware* recopilados tanto por la SEC como por la OCC:

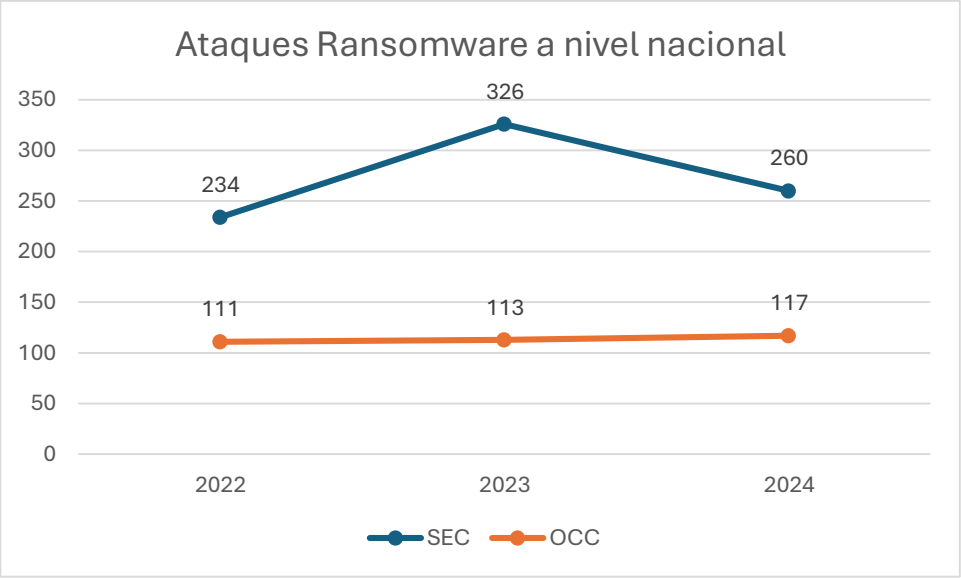


Ilustración 31. Ransomware a nivel nacional por años. Fuente OCC y SEC

Se puede comprobar que a nivel nacional el crecimiento del *ransomware,* independientemente de en cuál de las dos fuentes nos fijemos, no aumenta de la misma forma que en el resto del contexto internacional. El aumento máximo, en el ámbito nacional del 2022 al 2024, se observa que alcanza en torno a un 11% (en el caso de los datos de la SEC) frente al 89,9 % a escala internacional en el mismo periodo. Ambos datos parecen indicar que un crecimiento a escala mundial más acusado que en España, que sufre una tendencia al alza algo más leve. En esta línea, España ha pasado de padecer aproximadamente el 4 % de los ataques *ransomware* mundiales a un 2,25 %.

Por otro lado, los sectores más afectados a nivel global fueron la industria manufacturera y el sector sanitario, representando el 14 % y el 9 % de los ataques respectivamente. Mientras que, en la esfera nacional, el sector que más ataques recibió volvió a ser el de información y comunicaciones (12,82 %), seguido de las actividades profesionales, científicas y técnicas (11,97 %) y el comercio (11,97 %), que pasaron de ser el tercer y quinto sector más afectados en 2023, respectivamente, a los segundos en 2024.

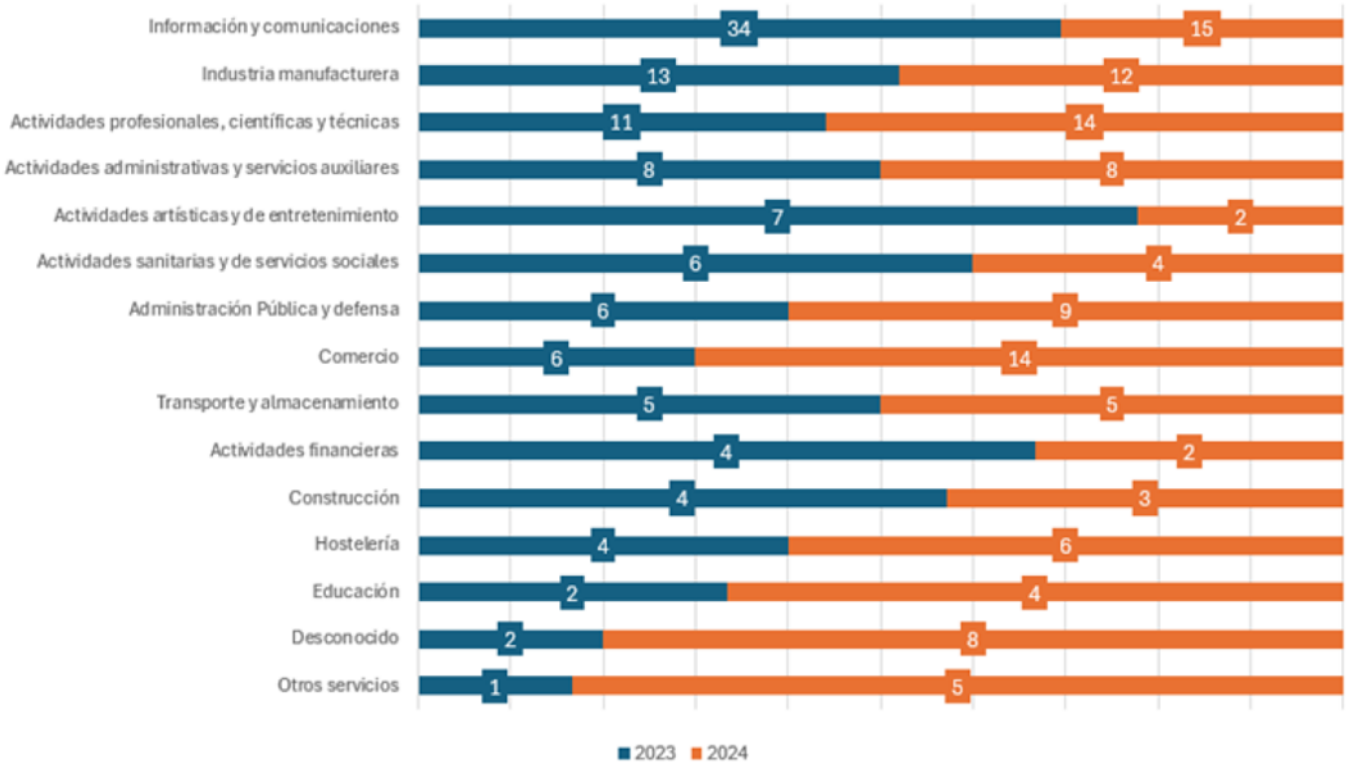


Ilustración 32. Gráfica nº de ataques ransomware de los sectores más afectados a nivel nacional en 2023 y 2024. Fuente: OCC

En el marco de los incidentes comunicados a la OCC por parte de los operadores de servicios esenciales, el *ransomware* ha demostrado una capacidad creciente para afectar a los mismos, comprometer datos sensibles y exigir rescates económicos cada vez más elevados.

Durante el último año, este tipo de amenaza ha evolucionado no solo en sofisticación técnica, sino también en sus modelos de extorsión, combinando el cifrado de datos con la filtración y publicación de información confidencial. Se prevé que el *ransomware* continúe su evolución hacia formas más dirigidas y automatizadas, aprovechando la inteligencia artificial para identificar vulnerabilidades con mayor precisión y seleccionar objetivos de alto valor. Además, se anticipa un aumento en las campañas de *ransomware* como servicio (RaaS), lo que facilitará el acceso a estas herramientas a actores menos especializados, ampliando así el espectro de amenazas.

Por otro lado, los *DDoS* son ataques que tienen como objetivo degradar o anular la calidad de un servicio; por ejemplo, una página web corporativa, hasta dejarla en un estado no funcional. Para conseguirlo los ciberdelincuentes saturan los recursos del sistema que aloja el servicio a interrumpir, enviándoles una avalancha de peticiones que no son capaces de atender.

Dentro del análisis de este tipo de ciberataques encontramos un volumen mucho más significativo que en el caso del *ransomware* dentro del marco de actuación de la OCC, no así dentro de los datos de la SEC. Cabe reseñar en este punto que prácticamente la totalidad de los *DDoS* recogidos por parte de la OCC están directamente relacionados con actores hacktivistas, los cuales justifican sus actuaciones con un fin ideológico y por tanto necesitan dar la mayor difusión posible de sus acciones. En ocasiones estos ataques son realizados por actores extranjeros y no llegan a causar graves interrupciones en los sistemas, lo que puede hacer que los afectados piensen que no merece la pena denunciarlo.

Destacan las campañas de ataques atribuidas al actor prorruso NoName057(16), que afectaron a diferentes entidades y a numerosos operadores de servicios esenciales pertenecientes a diversos sectores estratégicos. Estas acciones se enmarcan en el actual contexto geopolítico, que ha motivado un incremento en este tipo de amenazas.

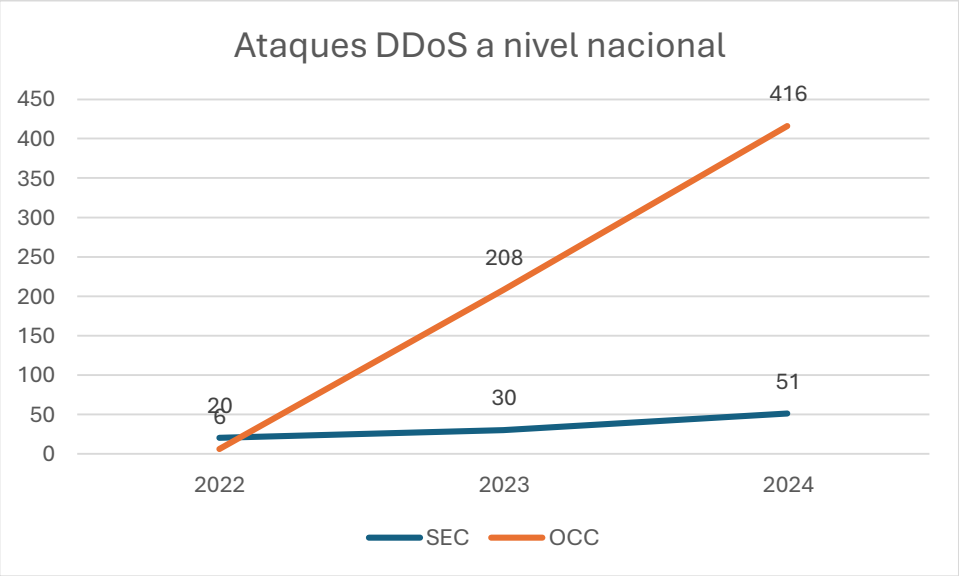


Ilustración 33. Evolución de DDoS a nivel nacional. Fuente: OCC y SEC

Se ha registrado que los sectores más atacados por los grupos hacktivistas durante los últimos años han sido el de Transporte y la Administración Pública. Esta actuación es lógica ya que su objetivo es destacar su actividad entre la ciudadanía, que su mensaje se haga oír en el mayor espectro posible y deslegitimar a las instituciones y organismos nacionales como respuesta a las políticas que desarrollan.

Por otro lado, con respecto a los incidentes relativos al fraude, continúan proliferando campañas de suplantación de identidad de clientes o proveedores, tanto por vía telefónica como a través del correo electrónico. Estas campañas, cada vez más sofisticadas, han incluido técnicas de *phishing* dirigidas y ataques de fraude al CEO *(Business Email Compromise, BEC)* en los que los atacantes se hacen pasar por altos cargos de una organización para inducir a empleados a realizar transferencias económicas o compartir información confidencial.

El *phishing,* en sus múltiples variantes (*spear phishing, smishing, vishing*), continúa siendo una de las principales puertas de entrada para este tipo de fraudes, aprovechando la ingeniería social y la urgencia emocional para comprometer a las víctimas. Por su parte, el fraude al CEO ha evolucionado hacia escenarios más personalizados, con un uso creciente de inteligencia artificial para imitar patrones de comunicación y generar mensajes altamente creíbles.

Finalmente, como se señaló en el apartado 1.4, se ha publicado la Orden TDF/149/2025, la cual refuerza la prohibición de las llamadas comerciales sin consentimiento previo, esta orden está directamente relacionada con los ataques de suplantación de identidad identificados como *spoofing*. Con esta medida se pretende frenar este tipo de actividad que ha ido creciendo durante los últimos años.

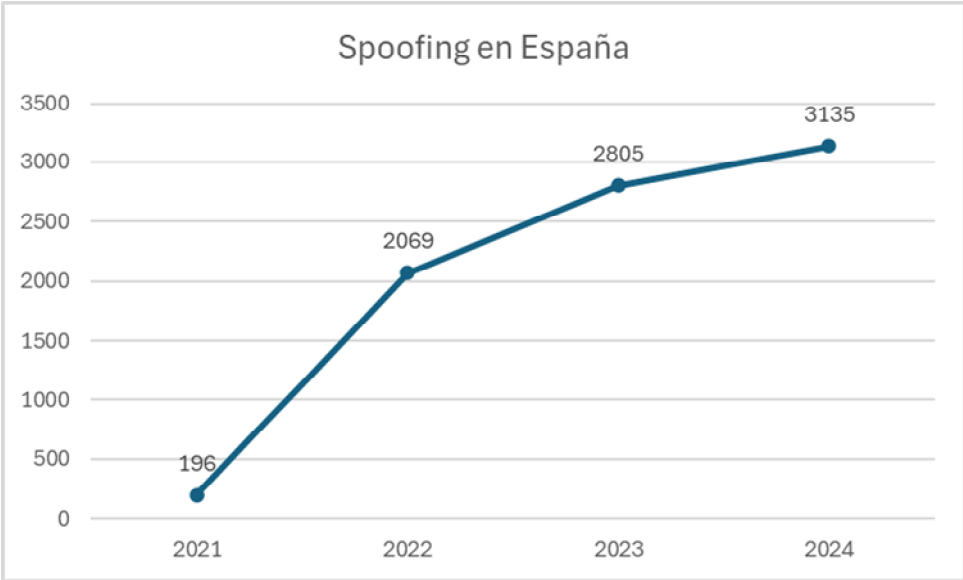


Ilustración 34. Evolución de spoofing en España. Datos del SEC

Atendiendo a la ilustración superior y con la nueva entrada en vigor de la Orden TDF/149/2025 antes mencionada, podrá valorarse en un futuro a medio plazo la eficacia real de las medidas implantadas en la lucha contra el engaño digital.

Las diferencias observadas entre los datos estadísticos de actividad policial y los obtenidos a través de fuentes abiertas pueden explicarse en base a diversos factores, entre los cuales destacan la cifra oculta de delitos (incidentes que no son denunciados ni registrados por desconocimiento, temor a represalias o cualquier otra causa), la rápida y constante evolución de las técnicas de ataque en el ámbito de la cibercriminalidad, o la alta variabilidad en las metodologías de recopilación de datos en el caso de las fuentes abiertas, no necesariamente de carácter estadístico.

Así, no se trata de cuadrar ambas cifras, sino de complementarlas para obtener una visión más amplia de este fenómeno complejo y una mayor capacidad de planificación de las estrategias de prevención y respuesta; ya que la mejora constante en la recolección y análisis de información se hace imprescindible para comprender su alcance real.

En línea con lo anterior, las Fuerzas y Cuerpos de Seguridad, como actores clave en la recopilación de información reflejada en el informe estadístico sobre la criminalidad, mantienen un esfuerzo y compromiso constantes para garantizar la **unificación de criterios** y el fortalecimiento de la **coordinación**. Esto resulta especialmente crítico en el ámbito de la cibercriminalidad, donde la objetividad en la representación de los datos es fundamental para una interpretación precisa y una respuesta eficaz ante las amenazas digitales. Razón por la que se trabaja de manera sostenida para la mejora continua de ciertos aspectos esenciales, como:

- **Fortalecimiento de la comunicación** entre las Fuerzas y Cuerpos de Seguridad y los expertos en ciberseguridad para mejorar la detección y clasificación de los delitos.
- **Promoción de mecanismos de denuncia más accesibles**.
- **Establecimiento de un protocolo de registro unificado**, que permita consolidar los datos del SEC, ofreciendo una visión más precisa del fenómeno de la ciberdelincuencia en España.
- **Formación constante** por parte de las personas encargadas de categorizar delitos tecnológicos, que permitirá aumentar la eficacia en la distinción y clasificación de las diferentes tipologías delictivas en el ámbito de la ciberseguridad.

5

ANEXO

METADATA

5. ANEXO: Metadata

Los datos utilizados por el SEC en el presente informe han utilizado la metodología y fuentes de datos que a continuación se relacionan:

>> Datos estadísticos de criminalidad

Origen de los datos

Los datos han sido obtenidos del SEC. Para su cómputo se tienen en cuenta los hechos de los que han tenido conocimiento los siguientes Cuerpos policiales: Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Mossos d'Esquadra y las Policías Locales que facilitan datos al SEC. La Ertzaintza aporta datos de hechos conocidos y detenciones e investigados, no así de hechos esclarecidos.

Definición y cómputo estadístico de Cibercriminalidad

Se detallan las conductas ilícitas registradas en el SEC, siguiendo la clasificación adoptada por el Convenio sobre Cibercriminalidad o Convenio de Budapest.

No obstante, además de las conductas que introduce el Convenio de Budapest, nuestra realidad criminal denota que existen otras categorías distintas que conviene reseñar. Así, cuando los medios empleados en su comisión sean las tecnologías de información y comunicación (TIC), pueden considerarse dentro de los delitos tecnológicos las siguientes tipologías delictivas:

- Delitos contra el honor.
- Amenazas y coacciones.

La explotación estadística se hace basándose en la localización del hecho, es decir, el territorio donde se produce, independientemente de la unidad policial que lo conozca y de la fecha de instrucción de las diligencias policiales.

Concepto de hechos conocidos, esclarecidos, detenciones/investigados y victimizaciones

Por hechos conocidos se entiende el conjunto de infracciones penales que han sido conocidas por las distintas Fuerzas y Cuerpos de Seguridad, bien por medio de denuncia interpuesta o por actuación policial realizada *motu proprio* (labor preventiva o de investigación).

Los hechos esclarecidos se clasifican como tales cuando en el hecho se da alguna de estas circunstancias:

• Detención del autor *in fraganti*.

• Identificación plena del autor, o alguno de los autores, sin necesidad de que esté detenido, aunque se encuentre en situación de libertad provisional, huido o fallecido.

• Cuando exista una confesión verificada, pruebas sólidas o cuando haya una combinación de ambos elementos.

• Cuando la investigación revele que, en realidad, no hubo infracción.

Hay que significar, que como se ha apuntado anteriormente, sólo hay datos de hechos esclarecidos de Cuerpo Nacional de Policía, Guardia Civil, Mossos d' Esquadra, Policía Foral de Navarra y cuerpos de Policía Local que facilitan datos al SEC. Es por ello, que, al no poseerse datos de la Ertzaintza, los datos de hechos esclarecidos del País Vasco están infrarrepresentados.

El porcentaje de esclarecimiento se obtiene dividiendo el total de hechos esclarecidos entre el total de hechos conocidos y multiplicando el resultado por 100.

Se considera que una persona física o jurídica está investigada a causa de la atribución de participación en un hecho penal, sin adoptar medidas restrictivas de libertad para esa persona investigada. La detención va más allá, realizando todo el proceso que lleva a la lectura de derechos de la persona física, privándole de libertad y poniéndolo a disposición judicial, por la atribución de la comisión de una infracción penal.

El concepto de victimización viene referido al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal. Se diferencia del concepto de víctima, ya que éste se refiere a personas individuales.

En una denuncia pueden darse varios hechos conjuntamente, e incluso pueden existir varias víctimas o perjudicados, siendo las victimizaciones el término que engloba a los diferentes hechos que afectan a una determinada víctima.

Los contrastes entre victimización y víctima se pueden ejemplificar con el siguiente supuesto: una persona presenta una denuncia y manifiesta que, en un determinado período de tiempo, ha sido objeto de tres hechos de malos tratos en el ámbito familiar y un delito de amenazas. Además, en esta misma denuncia manifiesta que su hijo de tres años también ha sido objeto de malos tratos en una ocasión.

• Total denuncias: 1

- Total víctimas: 2
- Total victimizaciones: 5 (3 hechos de malos tratos al denunciante + 1 delito de amenazas al denunciante + 1 hecho de malos tratos al niño).

>> Datos de la OCC

Dentro de la OCC se establecen diferentes fuentes de información complementarias. Se monitoriza y detecta amenazas en el ámbito de la ciberseguridad y la cibercriminalidad recabando información de **múltiples fuentes**, con un **enfoque** más **estratégico** en la **lucha** contra las **amenazas digitales**.

Cabe destacar que la OCC incorpora **información procedente de diversas fuentes**, entre las que se incluyen:

- Información procedente de las **unidades especializadas** de delitos tecnológicos de las Fuerzas y Cuerpos de Seguridad.
- Datos provenientes de notificaciones de operadores de servicios esenciales a través de **centros de respuesta a incidentes de seguridad (CSIRT) nacionales de referencia**. En virtud del Real Decreto-ley 12/2018, de 7 de septiembre, sobre la seguridad de las redes y sistemas de información, la OCC asume las funciones atribuidas a la Secretaría de Estado de Seguridad como autoridad competente en esta materia para los **operadores de servicios esenciales** que, a su vez, sean designados como **operadores críticos**. En consecuencia, es el organismo encargado de recibir todas las **notificaciones obligatorias de incidentes** conforme a dicho Real Decreto-ley y a la Guía Nacional de Notificación y Gestión de Ciberincidentes.
- **Informes** sobre tendencias de ciberataques basados en documentos **públicos** y **privados** que contienen redes de monitorización permanentes desde las que observan actividades delictivas sin necesidad de denuncias formales.
- **Monitorización propia** para identificar y analizar distintos actores entre los diferentes ecosistemas que conforman la ciberdelincuencia global. Entre ellos se encuentran **grupos hacktivistas**, **ciberyihadistas** y **organizaciones especializadas en la distribución de *ransomware***, entre otros. Aunque cada uno opera con motivaciones y objetivos específicos, sus acciones, pese a sus diferencias, desembocan en un mismo propósito: la ejecución de ataques contra sistemas de información. Este enfoque permite una comprensión profunda de sus tácticas y estrategias, facilitando la anticipación y mitigación de amenazas en el ámbito de la ciberseguridad.

Es pertinente destacar que, con los datos obtenidos de la monitorización de ciberataques a través de fuentes abiertas, aunque valiosa para identificar patrones generales y amenazas emergentes fruto de la diversidad de fuentes empleadas en la obtención de información y motivada por sus distintas finalidades, no se deben llevar a cabo conclusiones absolutas sobre los datos recopilados. La interpretación de las cifras relacionadas con la cibercriminalidad, especialmente en el ámbito de los ataques a sistemas de información, está condicionada por múltiples variables que influyen en su análisis y comprensión, por lo que no deben emplearse los datos con una finalidad académica, excepto los relacionados con la cibercriminalidad en el ámbito de los operadores de servicios esenciales.

GOBIERNO
DE ESPAÑA
MINISTERIO
DEL INTERIOR
SECRETARÍA DE ESTADO
DE SEGURIDAD
DIRECCIÓN GENERAL
DE COORDINACIÓN
Y ESTUDIOS

OCC