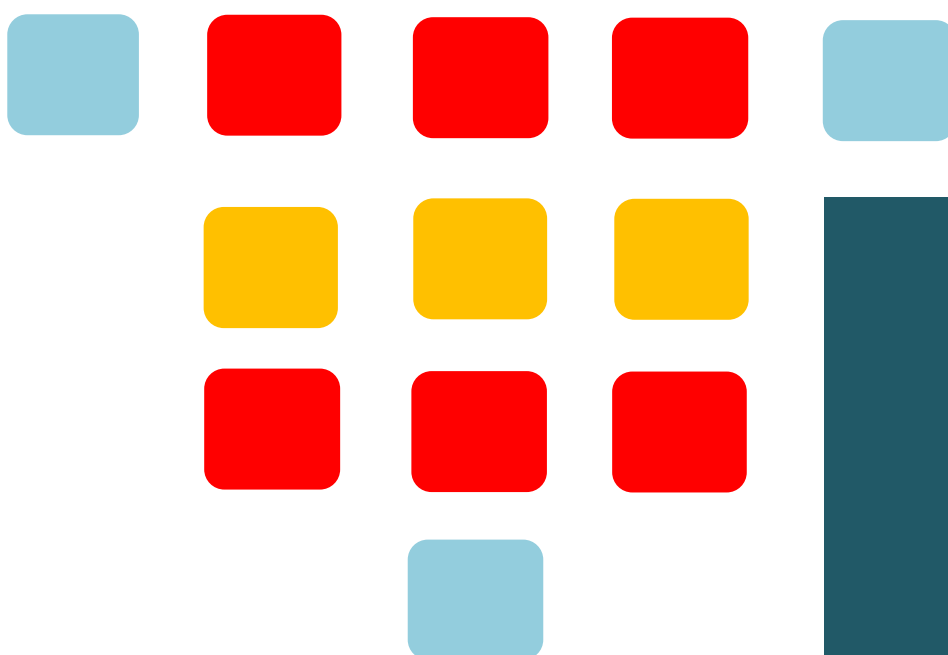


INFORME SOBRE LA CIBERCRIMINALIDAD EN

ESPAÑA





INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

AUTORES

DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS
SECRETARÍA DE ESTADO DE SEGURIDAD

PILAR MUNIESA TOMÁS
DAVID HERRERA SÁNCHEZ
JORGE GUERRERO OLMOS
FRANCISCO MARTÍNEZ MORENO
MARCOS RUBIO GARCÍA
VICTORIA GIL PÉREZ
ANA M^a SANTIAGO OROZCO
MIGUEL ÁNGEL GÓMEZ MARTÍN

Edita:



© De los textos: sus autores

© De la presente edición: Ministerio del Interior. Gobierno de España

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

0 INDICE

1. Introducción

4

2. Infraestructuras críticas y ciberseguridad

23

3. Datos estadísticos de cibercriminalidad

26

4. Metadata

40

2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1

INTRODUCCIÓN >>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1.-

INTRODUCCIÓN

La Cibercriminalidad como fenómeno complejo y global requiere un enfoque multidisciplinar para abordar cualquier planteamiento de respuesta contra la misma. Para ello, una primera aproximación impone el conocimiento y la visualización de la realidad criminal a la que nos enfrentamos. El conocimiento de esta realidad viene obligado a describir aspectos no solamente relacionados con los datos estadísticos, sino que implica también ahondar en otras temáticas de referencia que deben ser consignadas aquí para dimensionar y comprender adecuadamente el fenómeno de la ciberdelincuencia.

Con dicho polo de actuación, la publicación periódica de informes sobre esta materia, dimensionando su realidad objetiva, trata de poner de manifiesto los aspectos más relevantes de este fenómeno criminal, alertando sobre los peligros reales y potenciales, y convirtiéndose en un elemento facilitador e imprescindible para la concienciación frente a este fenómeno.

A tales fines responde la publicación de este *Informe sobre Cibercriminalidad*, correspondiente a la delincuencia informática registrada en el año 2022.

Los datos de este Informe son los correspondientes a la información estadística que computa la ciberdelincuencia conocida y registrada por las Fuerzas y Cuerpos de Seguridad. Se aúnan en este tipo de informe los **datos de los cuerpos policiales del territorio nacional** (Policía Nacional, Guardia Civil, Ertzaintza, Mossos d' Esquadra, Policía Foral de Navarra y Cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad), tanto en la vertiente de los hechos conocidos y las victimizaciones, como de las detenciones e investigados.

Los datos proceden del Sistema Estadístico de Criminalidad (SEC), y de los incidentes que registra la Oficina de Coordinación de Ciberseguridad (OCC), en función de su ámbito de actuación y competencias. Reseñar, que se detallan en el apartado de Metadata, la información que proporcionan cada Cuerpo policial.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior

Con el objetivo de mejorar las capacidades de los órganos del Ministerio para detectar, prevenir y perseguir la ciberdelincuencia y generar un nuevo impulso operativo y técnico eficaz que garantice la protección de los derechos y libertades y la seguridad ciudadana, **en marzo de 2021**¹ se aprobó el Plan Estratégico contra la Cibercriminalidad del Ministerio del Interior.

El plan estratégico diseñado por la Secretaría de Estado de Seguridad pone el foco en la prevención; en la cooperación entre las diferentes Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y los operadores jurídicos; en la dotación de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas; en la colaboración con la industria y los operadores relevantes en materia de ciberseguridad en el sector público y privado; y en el respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales.

Desde estos principios, el plan diseña una estrategia global para 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.
- 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 la consecución de estos objetivos, el plan contempla en cuarenta y nueve líneas de acción concretas que se articulan en torno a seis ejes estratégicos: cultura de prevención de la cibercriminalidad, potenciación de capacidades, generación de ciberinteligencia,

¹ <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2021/090321-cibercriminalidad.aspx>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

coordinación nacional y cooperación internacional, generación de un marco normativo adecuado y colaboración público-privada.

Este informe ayuda a dar cumplimiento a la **Línea de Acción 3.6** recogida dentro del **Eje Estratégico III** (Generación de Ciberinteligencia). Dicha línea de acción se formula como **“incrementar las capacidades actuales de obtención, tratamiento y análisis estratégico de información en el Ministerio del Interior”**, y sus resultados esperados son: *“evaluar las herramientas y capacidades disponibles, implantando aquellas que permitan un mejor tratamiento y análisis de la inteligencia estratégica como elemento fundamental en la prevención y anticipación de amenazas, con especial atención al Sistema Estadístico de Criminalidad (SEC)”*.

Estructura de este Informe sobre la cibercriminalidad en España

En el primer y segundo bloque del Informe se explican los datos procedentes de la Oficina de Coordinación de Ciberseguridad (OCC), así como los extraídos del Sistema Estadístico de Criminalidad (SEC), registrados por las Fuerzas y Cuerpos de Seguridad. Información que es desglosada en diferentes apartados (hechos conocidos, distribución territorial, perfil de las víctimas, detenciones efectuadas, incidentes por Comunidad Autónoma de referencia, por sector estratégico, etc.), lo que permite mostrar la realidad de la Cibercriminalidad en nuestro país.

Debe tenerse en cuenta que cuando dentro del presente Informe se facilitan datos de series históricas, se ven afectados por varios cambios legislativos producidos durante los últimos años. Uno de ellos fue la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en el año 2015. La otra fue la ratificación por España del *Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*, hecho en Estrasburgo, el 28 de enero de 2003 (entró en vigor 1 de abril de 2015).

La tipificación de las conductas sigue las mismas conceptualizaciones que emplea el Convenio de Budapest², a los que se le ha añadido por el volumen y la importancia de la cifra registrada, las siguientes infracciones penales: a) delitos contra el honor; b) amenazas y coacciones.

² https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Un aspecto que es necesario resaltar es el previsible aumento de la ciberdelincuencia. En palabras de las propias instituciones europeas³, *“Los ciberataques y la ciberdelincuencia están aumentando en toda Europa, y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro, ya que se espera que 22 300 millones de dispositivos en todo el mundo estén conectados a la internet de las cosas de aquí a 2024”*.

Es importante destacar como aspecto referencial el hecho de que en junio de 2017 la Unión Europea estableció un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas (la "caja de herramientas de la diplomacia cibernética"). El marco permite que la UE y sus estados miembros utilicen todas las medidas de la Política Exterior y de Seguridad Común (PESC), incluidas las medidas restrictivas si es necesario, para prevenir, desalentar, disuadir y responder a las actividades cibernéticas maliciosas que tienen como objetivo la integridad y la seguridad de la UE y sus estados miembros.⁴ El marco de la UE para medidas restrictivas contra los ciberataques que amenazan a la UE y sus estados miembros se estableció en mayo de 2019⁵.

Las propias instituciones europeas han puesto en marcha además de lo expuesto en el párrafo anterior una serie de medidas para promover una mayor resiliencia contra la cibercriminalidad, entre las que destacan:

*Identidad Digital Europea: permitirá a todos los europeos acceder a los servicios en línea sin tener que utilizar métodos de identificación privada ni compartir datos personales sin necesidad.

³ <https://www.consilium.europa.eu/es/policies/cybersecurity/>

⁴ <https://www.consilium.europa.eu/es/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/>

⁵ <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02019D0797-20201124&from=EN>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

*Brújula Digital⁶ para la Década Digital de la UE: que persigue los siguientes objetivos para 2030.⁷



Infografía n.º 1: Metas digitales para 2030 de la Unión Europea.

⁶ <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0118>

⁷ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

*Ciudadanía digital: derechos y principios para los europeos. Tal como puede verse en la siguiente infografía son los siguientes:

 <p>Prioridad a las personas</p> <p>Las tecnologías digitales deben proteger los derechos de las personas, sustentar la democracia y garantizar que todos los actores del sector digital actúen con responsabilidad y seguridad. La UE promueve estos valores en todo el mundo.</p>	 <p>Libertad de elección</p> <p>Las personas deberían poder desenvolverse en un entorno en línea justo, verse protegidas del contenido ilegal y pernicioso y estar capacitadas para interactuar con las tecnologías nuevas y evolutivas, como la inteligencia artificial.</p>	 <p>Seguridad y protección</p> <p>El entorno digital debe ser seguro y ofrecer protección. Todos los usuarios, desde los más pequeños hasta los más ancianos, deben estar empoderados y protegidos.</p>
 <p>Solidaridad e inclusión</p> <p>La tecnología debe unir, no dividir, a las personas. Todo el mundo debe tener acceso a internet, a las capacidades digitales, a los servicios públicos digitales y a unas condiciones de trabajo justas.</p>	 <p>Participación</p> <p>Los ciudadanos deben poder participar en el proceso democrático a todos los niveles y tener control sobre sus propios datos.</p>	 <p>Sostenibilidad</p> <p>Los dispositivos digitales deben favorecer la sostenibilidad y la transición ecológica. Los usuarios deben conocer el impacto medioambiental y el consumo de energía de sus dispositivos.</p>

Infografía nº 2: Derechos y principios digitales en la UE (Fuente Comisión Europea)⁸

Sumado a todo lo anterior, un aspecto destacado en la lucha contra la Cibercriminalidad, es la respuesta policial que se da dentro del ámbito europeo. Para ello, se disponen de una serie de herramientas dentro del seno de EUROPOL, tales como:

Grupo de trabajo sobre ciberdelincuencia de la Unión Europea (EUCTF): es una red basada en la confianza que se reúne dos veces al año en Europol y proporciona un foro para que los jefes de las unidades de ciberdelincuencia de la UE y los países asociados (Dinamarca, Islandia, Noruega y Suiza), junto con EUROPOL, CEPOL, EUROJUST y DG HOME identifiquen, discutan y prioricen los principales desafíos y acciones en la lucha contra el ciberdelito.⁹

⁸ <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles>

⁹ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Grupo de trabajo conjunto de acción contra el ciberdelito (J-CAT): Ubicado en el Centro Europeo de Ciberdelincuencia (EC3) de Europol, ayuda a combatir la ciberdelincuencia dentro y fuera de la UE.



Infografía nº 3: Participantes del J-CAT (Fuente EC3-EUROPOL)

SPACE (Secure Platform for Accredited Cybercrime Experts): Dentro de la Plataforma de Expertos de Europol (EPE). Creada para reunir a expertos en cibercrimen de todo el mundo. Se divide en dos partes: un área común visible y disponible para todos los usuarios de SPACE acreditados y una serie de subcomunidades cerradas, restringidas solo a miembros.¹⁰

Otro aspecto que va a tener un alto impacto en los niveles futuros de ciberseguridad, ha sido la aprobación de la Directiva NIS 2. Recientemente, el Centro Criptológico Nacional (CCN) publicó una nota de prensa en la que se decía lo siguiente sobre el particular¹¹:

“El Consejo y el Parlamento Europeo han llegado recientemente a un acuerdo sobre las medidas para garantizar un nivel común elevado de ciberseguridad en toda la Unión Europea, con el fin de mejorar la resiliencia y las capacidades de respuesta a incidentes tanto del sector público como del sector privado, así como del conjunto de la UE.

Esta nueva Directiva NIS 2 sustituirá a la Directiva actual sobre la seguridad de las redes y sistemas de información y sentará las bases para las medidas de gestión de riesgos

¹⁰ https://www.europol.europa.eu/cms/sites/default/files/documents/space_flyer-2019.pdf

¹¹ <https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11799-la-union-europea-refuerza-su-ciberseguridad-y-resiliencia-con-la-aprobacion-de-la-directiva-nis-2.html>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

de ciberseguridad y la obligación de notificación en los sectores que cubre (energía, transporte, sanidad e infraestructura digital).

El objetivo primordial es eliminar las diferencias entre los requisitos de ciberseguridad y de aplicación de las medidas entre los distintos Estados miembros. Para ello, se establecen normas mínimas para un marco regulador y mecanismos para una cooperación eficaz entre las autoridades de cada Estado miembro. Así, se establecerá la Red Europea de Organización de Enlace de Crisis Cibernéticas (EU-CYCLONe) para mejorar la coordinación en la gestión de incidentes de ciberseguridad a gran escala.”

Por último, es de destacar que la Comisión Europea¹² propuso dos iniciativas legislativas para actualizar las normas que rigen los servicios digitales en la UE: la Ley de Servicios Digitales (DSA) y la Ley de Mercados Digitales (DMA). La Comisión hizo las propuestas en diciembre de 2020 y el 25 de marzo de 2022 se alcanzó un acuerdo político sobre la Ley de Mercados Digitales, y el 23 de abril de 2022 sobre la Ley de Servicios Digitales.

Juntos forman un conjunto único de nuevas reglas que serán aplicables en toda la UE para crear un espacio digital más seguro y abierto.

La DSA y la DMA tienen dos objetivos principales:

-Crear un espacio digital más seguro en el que se protejan los derechos fundamentales de todos los usuarios de servicios digitales;

-Establecer condiciones equitativas para fomentar la innovación, el crecimiento y la competitividad, tanto en el Mercado Único Europeo como a nivel mundial.

Otro hecho sometido a controversia es la realización de un análisis del coste de lo que suponen las amenazas cibernéticas, pues en muchos casos son datos que no son de acceso público. No obstante, existen algunos entes privados que han realizado estudios tentativos sobre esta materia. Un ejemplo de ello es el “2022 Ponemon Cost of Insider Threats Global Report.”¹³ En dicho informe se encuestó a más de 1000 profesionales de las TIC en América del Norte, Europa, Medio Oriente, África y Asia-Pacífico. El informe revelaba que, en los últimos dos años, la frecuencia y los costos asociados con las amenazas internas han aumentado drásticamente en las tres categorías de amenazas internas, que incluyen: empleados/contratistas descuidados o negligentes, información privilegiada malintencionada o criminal y robo de credenciales. Asimismo, aporta otro dato a tener en cuenta: “el

¹² <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

¹³ <https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

56% de los incidentes de amenazas internas conocidos fueron el resultado de un empleado o contratista descuidado.”¹⁴

Las amenazas a la ciberseguridad son objeto de una atención preferencial de las políticas públicas, prueba de ello es la nueva Estrategia de Seguridad Nacional (ESN 2021), aprobada el pasado 28 de diciembre de 2021, mediante Real Decreto 1150/2021¹⁵. En la misma, se definen los dos tipos de amenazas existentes en el ciberespacio:

Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de ransomware (secuestro de datos) o la denegación de servicio, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización.

La importancia que se le otorga dentro de la nueva ESN 2021 a la ciberseguridad, es patente, ya que en la misma se cita textualmente que: *“En términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa”*. Para ello y dentro de la Línea de Acción 17, el ciberespacio que es considerado como uno de los espacios comunes globales junto al marítimo, aéreo y ultraterrestre, se promueve el avance en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

Otro aspecto que se destaca en la ESN 2021 es el relacionado con la desinformación. Esta actividad tiene fuertes implicaciones para la ciberseguridad, como ha reconocido la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), en su informe “THREAT LANDSCAPE 2021”¹⁶. La citada agencia, establece cuatro tipos de objetivos que persigue la desinformación, catalogando los medios con los que se lleva cada uno de ellos.

¹⁴ <https://www.globenewswire.com/news-release/2022/01/25/2372208/35374/en/Global-Cybersecurity-Study-Insider-Threats-Cost-Organizations-15-4-Million-Annually-up-34-Percent-from-2020.html#:~:text=Organizations%20impacted%20by%20insider%20threats,percent%20in%20just%20two%20years.>

¹⁵ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884

¹⁶ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@/download/fullReport>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Target	Means	Goal
People	Disinformation, misinformation, fake news	Reduce perceived honesty and trustworthiness of individuals
Enterprises	Market distortion, misinformation, disinformation, smear campaigns, fake news, propaganda	Affect brand reputation, financial solidity of the company, and the trustworthiness of the management.
Society	Disinformation, fake news	Inability to distinguish real and fake news, apathy, exhaustion in trying to find the truth, manipulating and misleading public-opinion
Any	Sharing of inaccurate information	Make money based on advertisement

Tabla nº 1.- Objetivos y medios con los que se lleva a cabo la desinformación (Fuente: Informe THREAT LANDSCAPE 2021-ENISA)

En relación con las principales tendencias de las amenazas relacionadas con la Cibercriminalidad, un organismo de referencia es EUROPOL. Dicho organismo a través de sus informes anuales (Internet Organised Crime Threat Assessment - IOCTA)¹⁷, analiza cuales son. En su informe del año 2021¹⁸, se extraen una serie de conclusiones:

- El ransomware se ha aprovechado de las vulnerabilidades del teletrabajo.
- El aumento de mercado online lleva aparejado un incremento de las actividades intrusivas informáticas, como phishing, robos de identidad, banca online, etc.
- Creciente venta de productos médicos falsificados, como consecuencia de la pandemia generada por la Covid-19.
- La Covid-19 ha provocado un mayor acceso de la población infantil a contenidos en línea, con los riesgos que ello conlleva.
- El comercio y la venta de datos privados, al amparo de accesos ilegales informáticos, es un mercado floreciente.

¹⁷https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

¹⁸ <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.-

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

En la introducción al Capítulo se detallan los aspectos más relevantes en esta materia, entre los que se incluyen datos sobre incidentes gestionados por el Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad.

Dentro de dicho apartado se muestran gráficos y datos según el tipo de incidente, así como los que están relacionados con las infraestructuras críticas y el sector estratégico afectado.

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

En enero de 2008 entraba en funcionamiento el Sistema Estadístico de Criminalidad (SEC), en sustitución del Programa Estadístico de Criminalidad (PES), que incorporaba mejoras tanto desde el punto de vista metodológico como técnico, que suponían mayores cuotas de los niveles de calidad de los procesos estadísticos que se realizan desde el Ministerio del Interior.

Como consecuencia del Real Decreto 400/2012, de 17 de febrero, por el que se desarrollaba la estructura orgánica básica del Ministerio del Interior, el entonces Gabinete de Coordinación y Estudios (actualmente Dirección General de Coordinación y Estudios) asumió las funciones en materia de estadística de criminalidad, que continuaron tras la publicación del Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

Fue el 31 de enero de 2013, cuando se dictó la Instrucción 1/2013, de la Secretaría de Estado de Seguridad, sobre la Estadística Nacional de Criminalidad, cuyo objeto es *“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”*.

Así pues, y según consta en esta Instrucción, a partir del Sistema Estadístico de Criminalidad (SEC) que se compone de la Base de Datos que registra las actuaciones policiales y responsables¹⁹, se llevará a cabo la explotación estadística de los datos que se

¹⁹ Actuaciones policiales y responsables: son dos operaciones estadísticas dadas de alta en el Inventario de Operaciones Estadísticas del INE

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

conozcan por las por las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil), las Fuerzas y Cuerpos de Seguridad dependientes de las Comunidades Autónomas (Ertzaintza, Mossos d' Esquadra y Policía Foral de Navarra), y también por aquellos Cuerpos de Policía Local que facilitan datos a las Fuerzas y Cuerpos de Seguridad del Estado, y en definitiva al SEC.

En este caso concreto que nos ocupa se detalla a continuación la información estadística consignada en el SEC sobre Cibercriminalidad en España.

Datos globales

El apartado 3.1 (Evolución de hechos conocidos por categorías delictivas), contabiliza el total de los hechos conocidos por las Fuerzas y Cuerpos de Seguridad durante la serie histórica 2018-2022 (la información que los Cuerpos facilitan se detalla en el apartado de metadata), siguiendo la clasificación adoptada por el Convenio sobre Cibercriminalidad o Convenio de Budapest y otras infracciones penales reguladas en nuestra legislación interna. Asimismo, junto a las categorías específicamente concretadas como ciberdelincuencia, se debe incluir dentro de este fenómeno y por lo tanto computar los registros disponibles en el SEC todos los delitos que para su comisión se hayan empleado las TIC. A los delitos contemplados en el convenio citado, se han añadido una serie de tipologías penales que por su importancia merece la pena destacar:

- Delitos contra el honor.
- Amenazas y coacciones.

En el periodo comprendido entre 2018 a 2022, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2022, se han conocido un total de 374.737 hechos, lo que supone un 22,7% más con respecto al año anterior. De esta cifra, el 89,7 % corresponde a fraudes informáticos (estafas) y el 4,3% a amenazas y coacciones.

Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos y su peso proporcional en la delincuencia en general. Se puede observar en la tabla nº 2, que se ha pasado de un 7,5% en el año 2018, a un 16,1% en el año 2022.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2018	7,5%
2019	9,9%
2020	16,3%
2021	15,6%
2022	16,1%

Tabla nº 2. % que representa la Cibercriminalidad sobre el total de infracciones penales. Fuente: Sistema Estadístico de Criminalidad (SEC)

Las gráficas del punto 3.2 (Evolución global de hechos conocidos, esclarecidos y detenciones/investigados) evidencian de manera esquemática los datos correspondientes a los hechos conocidos, esclarecidos y la cifra de las detenciones e investigaciones registradas por las Fuerzas y Cuerpos de Seguridad, en el periodo 2018 a 2022.

En relación al porcentaje de hechos esclarecidos, en el año 2022, éste supone el 14,6% del total de los hechos conocidos, lo que implica un descenso con respecto al año anterior, que alcanzó el porcentaje de esclarecimiento del 15,9%. Por otra parte, los detenidos e investigados han alcanzado la cifra de 15.097, lo que supone un aumento de un 9,4% con respecto al año 2021, en el que se registraron 13.801 detenidos e investigados.

En el apartado 3.3 y 3.4 se detallan datos por meses, observándose que durante el 2022, el mes de mayor incidencia delictiva fue el mes de septiembre.

La distribución de la Cibercriminalidad, desde el punto de vista geográfico (3.5. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2022, sitúa a Cataluña, Madrid, Andalucía y Comunitat Valenciana entre las Comunidades Autónomas que concentran más infracciones penales en este ámbito. A nivel provincial, se encuentran a la cabeza del ránking estadístico, Madrid, Barcelona, Valencia, Sevilla, Alicante/Alacant, Málaga y Bizkaia.

Los datos de la sección 3.6, relativos a las victimizaciones registradas según grupo penal y sexo, precisan las características y el perfil de la víctima de los delitos informáticos en España. En este apartado se facilitan datos de todos los Cuerpos policiales.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

En 2022, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 298.319²⁰, es decir, un 24,2% más que en el año 2021; de las que un 49,99% pertenecen al sexo masculino y un 50,01% al sexo femenino. La mayoría de las víctimas de ciberdelincuencia se sitúa entre 26 a 40 años en ambos sexos, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y falsificación informática.

Por otra parte, se publican datos relativos a las victimizaciones desglosadas por tipología penal y sexo (Punto 3.8). Por ello, se puede decir que entre los principales hechos conocidos cometidos contra las víctimas de ambos sexos se encuentran las estafas, las amenazas y la usurpación de estado civil.

En relación a la nacionalidad de la víctima (apartado 3.9), el 87,2% de ellas son españolas, y el 12,8% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Marruecos, Rumanía y Colombia las que aúnan valores más elevados.

Al igual que en el informe de 2021, en este *Informe sobre Cibercriminalidad 2022*, se introducen datos que permiten realizar y establecer una relación entre los rangos de edad de las víctimas y la tipología penal de la que han sido objeto (Punto 3.10 Victimizaciones registradas según grupo penal y edad). Así pues, según los datos registrados, el fraude informático es la tipología delictiva con mayor incidencia en todos los grupos de edad establecidos (a excepción de los menores de edad), y de manera especial en los rangos de edad que va de los 26 años en adelante. Destacan sobre todo en términos porcentuales, que no cuantitativos, el grupo de mayores de 65 años.

Del análisis de la información extraída del SEC se puede observar que el comportamiento de las víctimas incluidas en el grupo menores de edad no sigue el patrón o el modelo de las víctimas mayores de edad. Las víctimas menores de edad son más vulnerables a otro tipo de hechos delictivos, en concreto a las amenazas y coacciones y delitos sexuales, tal y como refleja la tabla del apartado 3.10.

Igualmente, en este estudio se consignan datos detallados de las victimizaciones según el sexo de la misma. En las secciones 3.12 y 3.13 se aportan los del sexo masculino y

²⁰ Se puede apreciar una diferencia entre el número de hechos ilícitos conocidos (374.737) y el de victimizaciones registradas (298.319), debido a que ambos conceptos no contabilizan la misma información. En este sentido, cuando hablamos de victimizaciones nos referimos al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal, contabilizada dentro del ámbito de la ciberdelincuencia. En muchas ocasiones no se poseen datos de dichas víctimas.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

las 3.14 y 3.15, las del sexo femenino. Como primera diferencia entre ambas, se aprecia que las victimizaciones de mujeres son cuantitativamente superiores en las franjas de edad comprendidas hasta los 50 años, siendo la de los hombres superiores en el resto de grupos de edad. Por otro lado, comparten ambos sexos una característica común ligada al hecho de que la ciberdelincuencia sexual tiene la más amplia incidencia en los menores de edad, siendo los valores más altos en los del sexo femenino. Otra característica común está referenciada a que el grupo de edad de mayores de 65 años tiene los valores más altos en términos porcentuales en la categoría de fraude informático sobre la cifra absoluta de la Cibercriminalidad para el total de cada grupo de edad.

La sección 3.16 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, de 2022.

De la cifra total de detenciones e investigaciones (15.097) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 71,9% corresponden a personas de sexo masculino, teniendo lugar, principalmente, por la comisión de fraudes informáticos, delitos de amenazas y coacciones y delitos sexuales. La mayoría de las detenciones/investigaciones de personas de sexo femenino se han llevado a cabo por fraudes informáticos, amenazas y coacciones, y por el delito de falsificación informática.

Por lo que respecta a las diferentes infracciones penales (3.18 Detenciones/investigaciones por tipología penal y sexo), los datos establecen que las causas por las que las personas de sexo masculino han sido objeto de la detención/investigación ha sido principalmente por estafas, amenazas, y la pornografía de menores. Asimismo, se puede observar que las estafas, amenazas e usurpación de estado civil predominan entre las razones para actuar contra los responsables de sexo femenino.

La mayoría de los detenidos/investigados por ciberdelincuencia son de nacionalidad española (76,9%) (3.19). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Marruecos, República Dominicana y Colombia, los que aglutinan un mayor número de casos.

Al desglosar la información según los distintos rangos de edad predeterminados (3.20 Detenciones/investigaciones según grupo de edad y sexo), se observa que las mayores cifras de los responsables de ciberdelincuencia se ubican en el grupo de edad 26 a 40 años.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.-


INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD



La Oficina de Coordinación de Ciberseguridad (OCC) es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, estando sus funciones reguladas por el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior y su posterior modificación en el Real Decreto 146/2021, de 9 de marzo.

La OCC, incardinada en la Dirección General de Coordinación y Estudios, ejerce como canal específico de comunicación entre los Centros de Respuesta a Incidentes de Seguridad Informáticas (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes. Además, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE, de 12 de julio, relativa a los ataques contra los Sistemas de Información.

Por otro lado, y en base al Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, así como el Real Decreto 43/2021, de 26 de enero, que desarrolla el anterior, la Oficina de Coordinación de Ciberseguridad es el organismo encargado de recibir todas aquellas notificaciones de incidentes que tengan carácter obligatorio al amparo de ese Real Decreto-Ley y de la Guía Nacional de Notificación y Gestión de Ciberincidentes.

 El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, es el CSIRT al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, conforme el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es decir las entidades privadas.

El INCIBE-CERT está operado conjuntamente por el INCIBE y la Oficina de Coordinación de Ciberseguridad en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.



El Centro Criptológico Nacional, es el CSIRT de referencia para el sector público sujeto a la Ley 40/2015, y según el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

En este documento no se presentan los datos relativos a incidentes del sector público procedentes del CCN-CERT debido a que la mayoría de los incidentes reportados se corresponden a vulnerabilidades de sistemas detectados por sondas, así como sucesos de ciberseguridad gestionados que no tienen la consideración de incidentes, al no llegar a traducirse en afectaciones de la confidencialidad, la integridad o la disponibilidad de

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

los sistemas. Por esta razón, se ha estimado que su presencia únicamente genera sesgos al no permitir una comparación con lo dispuesto en el Título III del RD-I 12/2018.

>> 2.1. Incidentes gestionados por el INCIBE-CERT (entidades privadas)

El INCIBE-CERT gestionó un total de 118.820 incidentes de ciberseguridad en España durante el año 2022.

Analizando el número de incidentes en función de su tipología, se concluye que los incidentes tipo *Sistema vulnerable* son los más frecuentes según el registro del pasado año; con un porcentaje del 43,5%, respecto del total; seguido de los *Fraudes* con un 28,3%.

Con respecto a los tipos de **malware** con mayor relevancia, y efectos, en el año 2022, significar los siguientes:

Flubot: *Software* malicioso de tipo troyano para dispositivos Android. Las campañas más habituales implicaron el envío de SMS fraudulentos que avisaban de la recepción de un paquete suplantando a diferentes empresas logísticas, como FedEx, DHL o Correos.

Estos mensajes invitan al receptor a instalar una aplicación en su dispositivo móvil con el incentivo de que éste pueda conocer el paradero del paquete. Una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones que se inicien, con la capacidad de inyectar páginas superpuestas al detectar un inicio de sesión en una de las aplicaciones objetivo, de forma que el usuario se confía en que está introduciendo las credenciales en la web original cuando, en realidad, las está enviando al servidor de mando y control controlado por los operadores del código dañino.

Uupay: Caballo de troya para sistemas operativos móviles Android que roba información del dispositivo comprometido, pudiendo descargar *malware* adicional. El contagio se produce mediante la instalación de aplicaciones infectadas.

Incluye funcionalidades de recogida de información del dispositivo, lista de nombres de puntos de acceso, envío de mensajes SMS, lectura de mensajes SMS recibidos, activación o desactivación de la conectividad de la red del dispositivo y descarga e instalación de aplicaciones adicionales.

Andrómeda: *Botnet* que afecta ordenadores con sistema operativo Windows. Existen muchos métodos de infección, siendo generalmente por medio de enlaces de confianza enviados a través de correos electrónicos de phishing o mediante redes sociales, y copiándose a sí mismo en dispositivos removibles o de red.

Los ordenadores infectados con este *malware* pasan a ser parte de una *botnet*, los cuales son capaces de descargar datos y configuraciones de sitios remotos y ejecuta archivos arbitrarios. Entre las funcionalidades de la *botnet* se incluyen la descargar y ejecución de software adicional, el robo de credenciales de acceso a algunos sitios web, la creación de proxy de salida en la máquina infectada.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Por otro lado, con respecto a los incidentes relativos al **fraude**; significar que, durante el año 2022 han continuado proliferando campañas de suplantación de la identidad de clientes o proveedores, mediante vía telefónica y correo electrónico, con un total de 33.576 incidentes entre todos los ámbitos del sector privado:

Suplantación de identidad (Fraude al CEO): envío de correo electrónico personalizado, tras un análisis exhaustivo de la víctima, para que realice una transferencia, modifique la cuenta de pago de la factura de un proveedor, etc., a una cuenta contralada por los delincuentes.

Phishing: Consiste principalmente en la recepción por parte de la víctima de un correo electrónico destinado a engañarla y que comparta, normalmente a través de un enlace a una web fraudulenta, credenciales, datos personales, números de cuenta bancaria, datos de tarjetas de crédito o cualquier otro dato confidencial.

>> 2.2. Incidentes gestionados de Operadores Críticos del sector privado

A lo largo del año 2022, el número de incidentes de ciberseguridad disminuyó en un 19,7% con respecto al año anterior, gestionándose un total de 546 incidentes.

Con respecto a los tipos de incidentes con mayor relevancia se encuentran los relacionados con **sistemas vulnerables**, con un 60,8%, seguido por **robo de información, malware e intrusión** con un 20,9%, 4,8% y 4,8%, respectivamente.

>> 2.3. Incidentes gestionados por Sector Estratégico

Los sectores PIC donde se han detectado un mayor número de incidentes han sido el sector **Energía**, con un 37,2%, seguido del sector **Tributario y Financiero**, con un 17,4% y el sector **TIC**, con un 15,9%, y el sector **Transporte**, con un 15,2%.

2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD



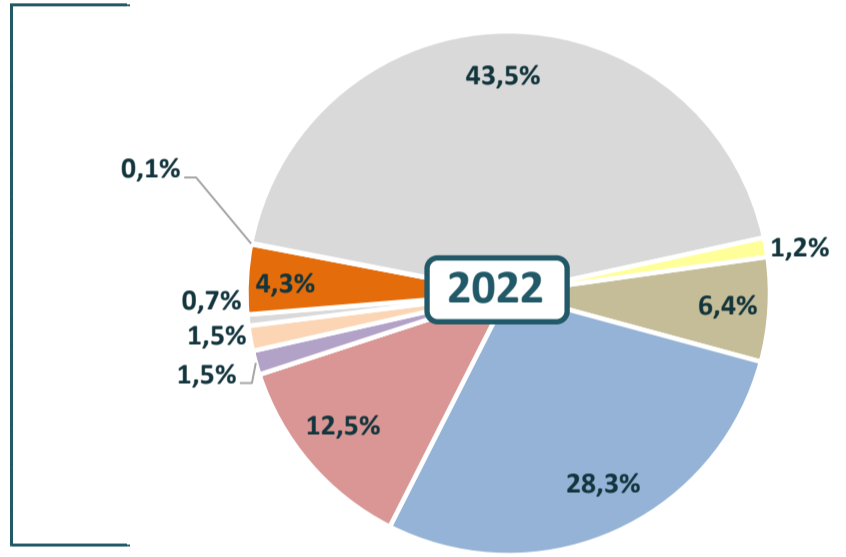
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 2.1. Incidentes gestionados por el INCIBE-CERT

Tipo de incidente	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039	7.649
Fraude	11.843	11.959	55.932	31.938	42.641	31.213	33.576
Malware	76.811	81.090	27.016	27.358	46.893	32.605	14.855
SPAM	10.279	7.957	0	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177	1.768
Intento de intrusión	381	1.435	396	1.518	1.289	1.753	1.839
Robos de información	37	47	63	77	161	920	823
Contenido Abusivo			9.353	4.064	2.986	5.253	5.110
Recolección de información			5.605	84	87	106	73
Sistema Vulnerable			3.731	31.414	23.161	20.609	51.711
Otros	1.038	787	782	4.407	4.409	2.451	1.416

Porcentaje del total de incidentes gestionados

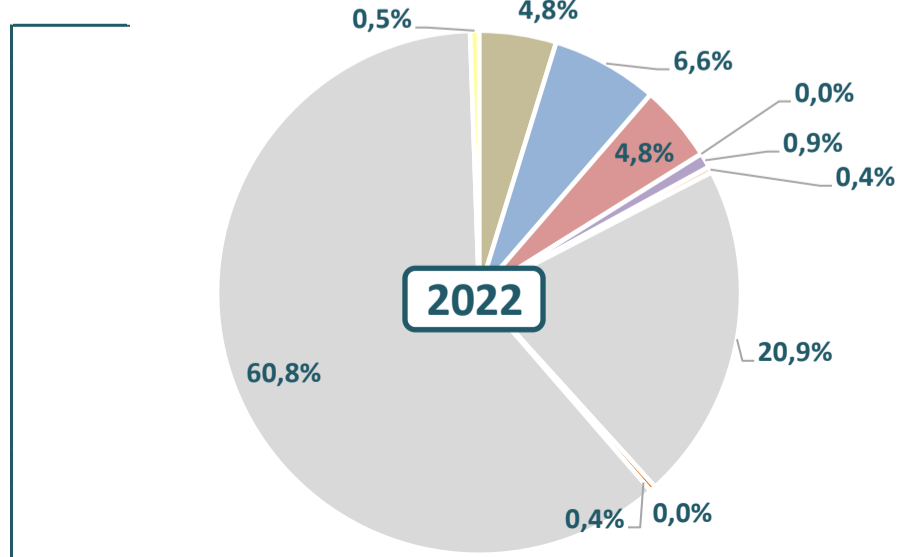


*Véase metadatos explicativos

>> 2.2. Incidentes gestionados en relación con las infraestructuras críticas

Tipo de incidente	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Intrusión	39	97	26	14	13	11	26
Fraude	13	66	41	78	37	16	36
Malware	311	387	200	166	348	177	26
SPAM	8	21	0	0	0	0	0
Disponibilidad	28	55	54	12	52	10	5
Intento de intrusión	24	159	9	7	3	2	2
Robos de información	1	1	7	8	0	117	114
Contenido Abusivo			11	6	6	3	2
Recolección de información			111	1	45	2	0
Sistema Vulnerable			224	514	351	339	332
Otros	55	99	39	12	6	3	3

Porcentaje del total de incidentes gestionados



*Véase metadatos explicativos

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

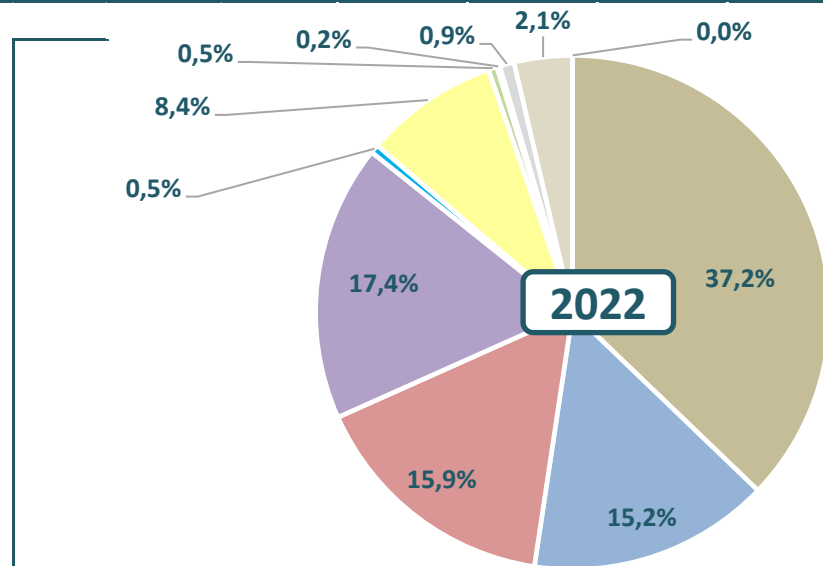
2.-

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 2.3. Incidentes gestionados por sector estratégico

Sector estratégico	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Energía	126	213	149	151	121	207	203
Transporte	90	152	192	197	176	92	83
Tecnologías Informac. y Comunicac. (TIC)	17	40	46	50	29	47	87
Sistema tributario y financiero	152	250	214	266	452	172	95
Alimentación	47	42	40	57	1	3	3
Agua	40	134	57	64	31	117	46
Industria nuclear	4	12	5	18	22	9	3
Administración	2	10	1	0	4	1	1
Espacio	0	1	3	4	3	7	5
Industria química	0	0	15	11	18	23	20
Instalaciones de Investigación	0	0	0	0	0	0	0
Salud	0	1	0	0	0	0	0
Todos los sectores afectados	1	0	0	0	4	2	0

Porcentaje del total de incidentes gestionados



2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

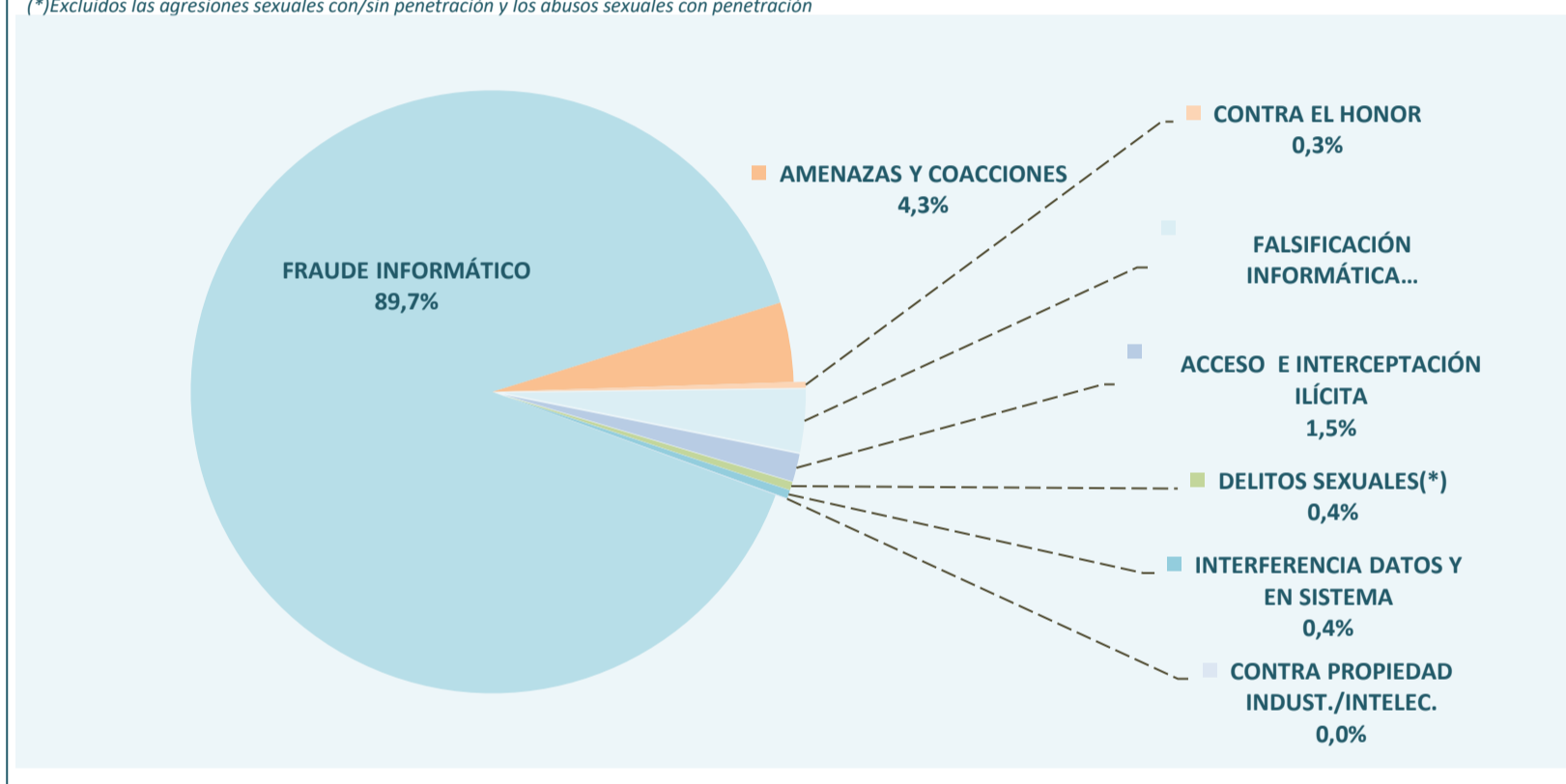
3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2018	2019	2020	2021	2022
ACCESO E INTERCEPTACIÓN ILÍCITA	3.384	4.004	4.653	5.342	5.578
AMENAZAS Y COACCIONES	12.800	12.782	14.066	17.319	15.982
CONTRA EL HONOR	1.448	1.422	1.550	1.426	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	232	197	125	137	114
DELITOS SEXUALES(*)	1.581	1.774	1.783	1.628	1.646
FALSIFICACIÓN INFORMÁTICA	3.436	4.275	6.289	10.476	12.569
FRAUDE INFORMÁTICO	136.656	192.375	257.907	267.011	335.995
INTERFERENCIA DATOS Y EN SISTEMA	1.192	1.473	1.590	2.138	1.662
Total HECHOS CONOCIDOS	160.729	218.302	287.963	305.477	374.737

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



>> 3.2. Evolución global de hechos conocidos, esclarecidos y detenciones / investigados



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

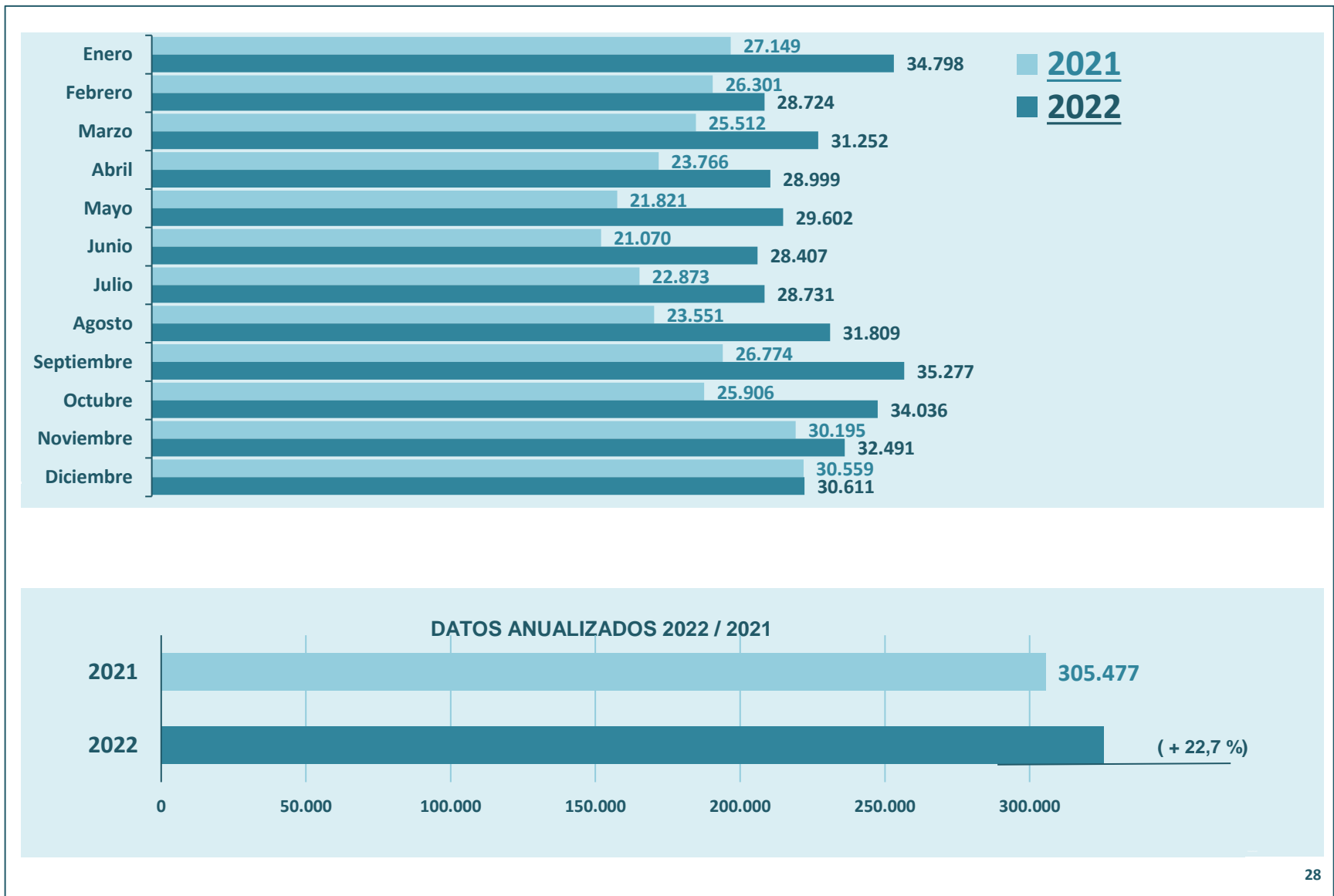
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.3. Distribución mensual de hechos conocidos. Año 2022

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	307	367	426	420	538	502	529	466	575	457	570	421	5.578
AMENAZAS Y COACCIONES	1.326	1.434	1.570	1.282	1.319	1.403	1.322	1.340	1.288	1.295	1.255	1.148	15.982
CONTRA EL HONOR	78	104	127	91	91	107	107	101	114	103	90	78	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	9	12	16	9	1	13	5	13	12	10	6	8	114
DELITOS SEXUALES(*)	168	135	195	119	159	145	90	128	138	139	137	93	1.646
FALSIFICACIÓN INFORMÁTICA	910	1.075	1.239	1.045	1.200	1.074	962	925	1.045	1.014	1.143	937	12.569
FRAUDE INFORMÁTICO	31.873	25.471	27.545	25.878	26.147	25.026	25.582	28.681	31.973	30.890	29.166	27.763	335.995
INTERFERENCIA DATOS Y EN SISTEMA	127	126	134	155	147	137	134	155	132	128	124	163	1.662
Total HECHOS CONOCIDOS	34.798	28.724	31.252	28.999	29.602	28.407	28.731	31.809	35.277	34.036	32.491	30.611	374.737

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

>> 3.4. Comparativa de la distribución mensual de hechos conocidos 2022 / 2021



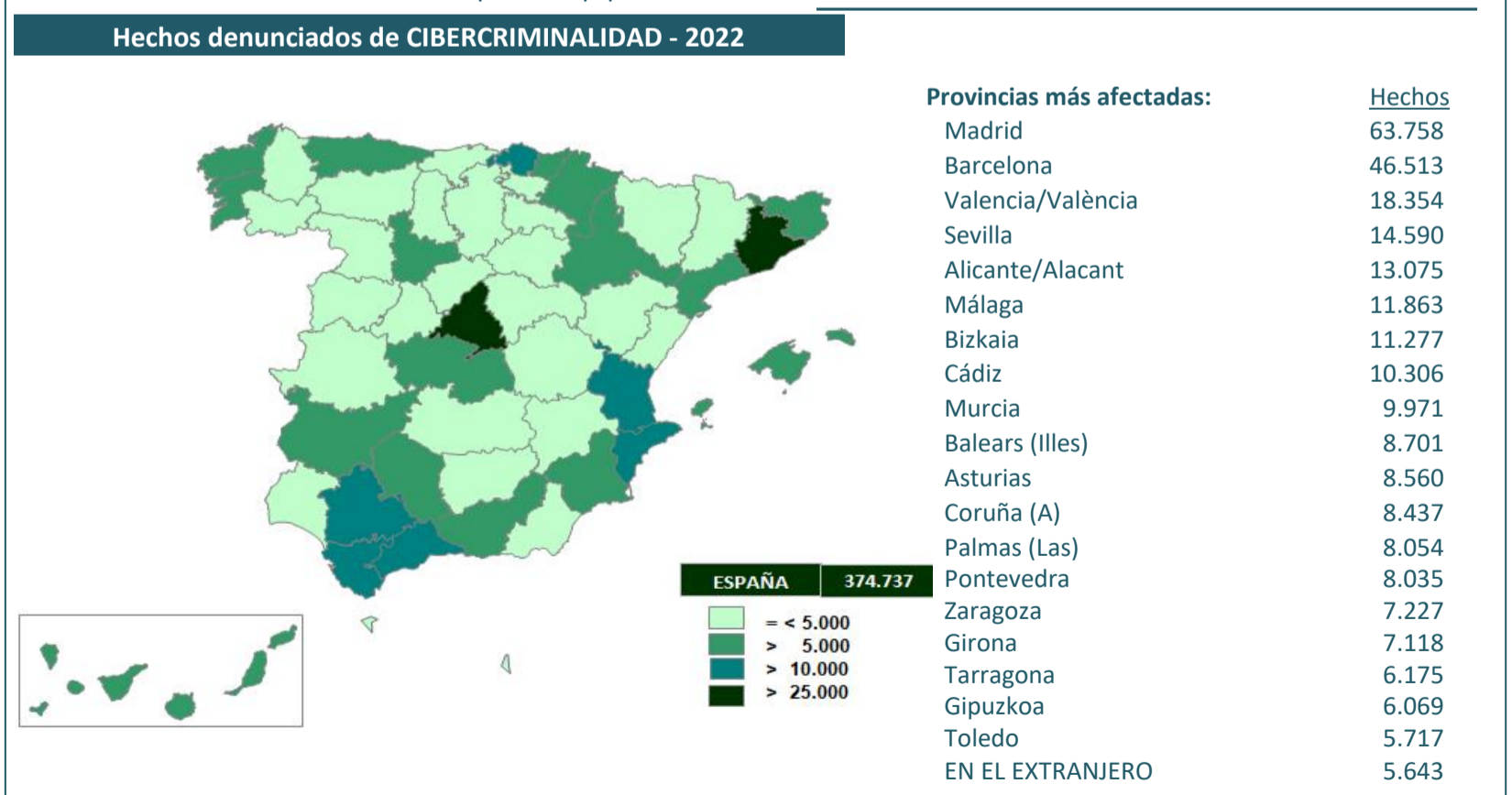
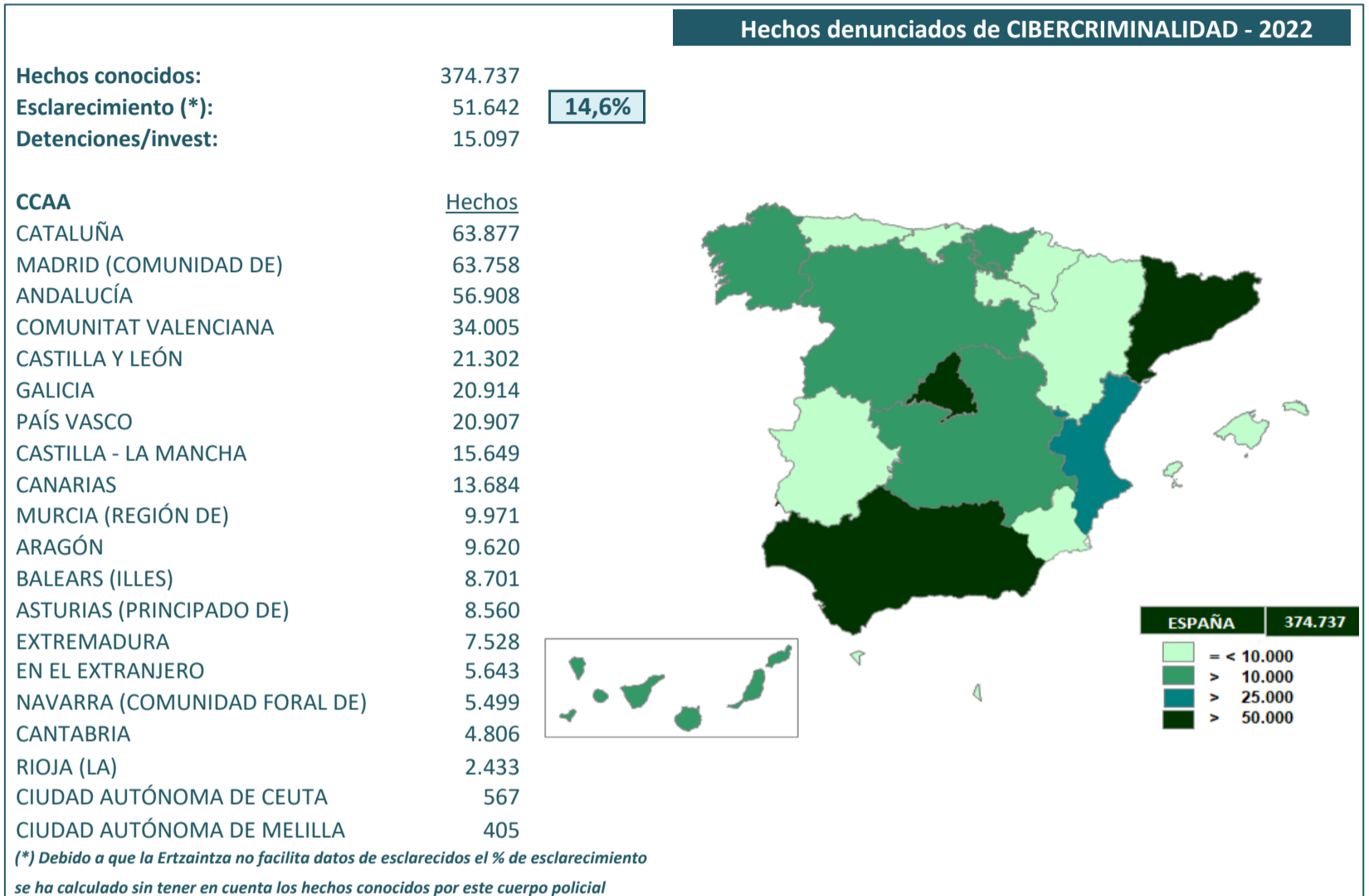
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2022



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

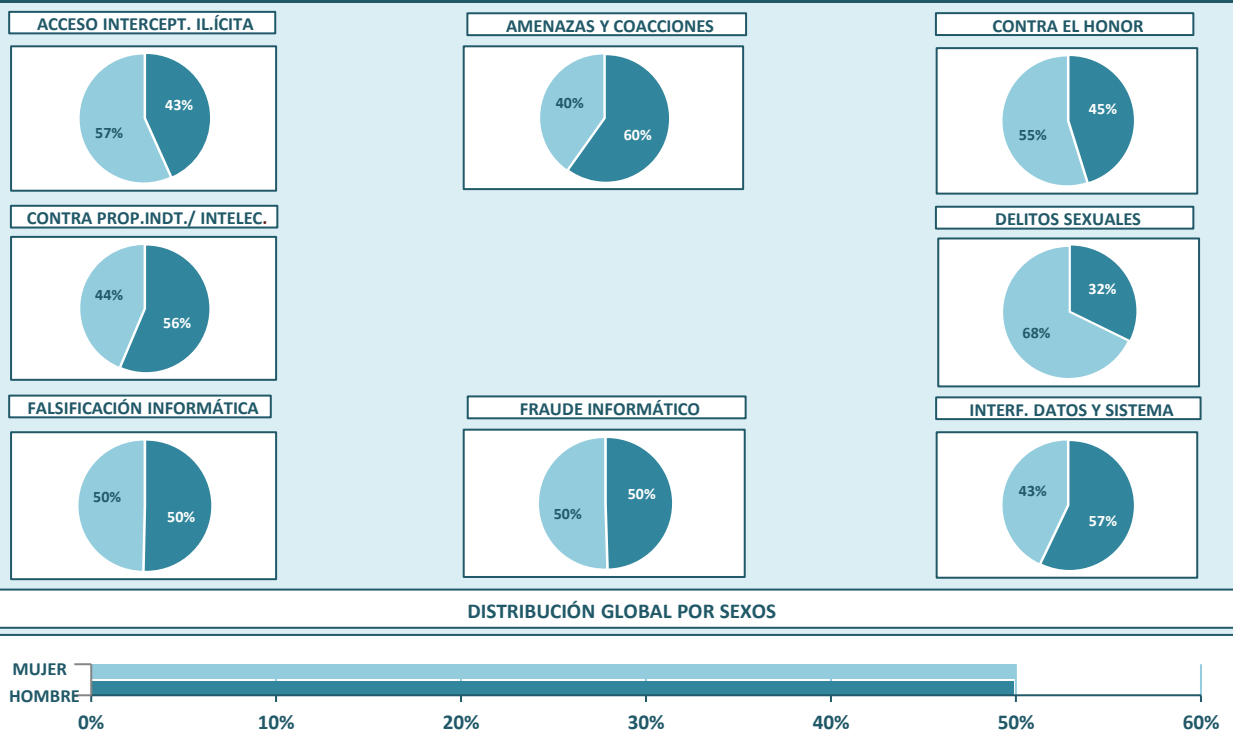
>> 3.6. Victimizaciones registradas según grupo penal y sexo. Año 2022



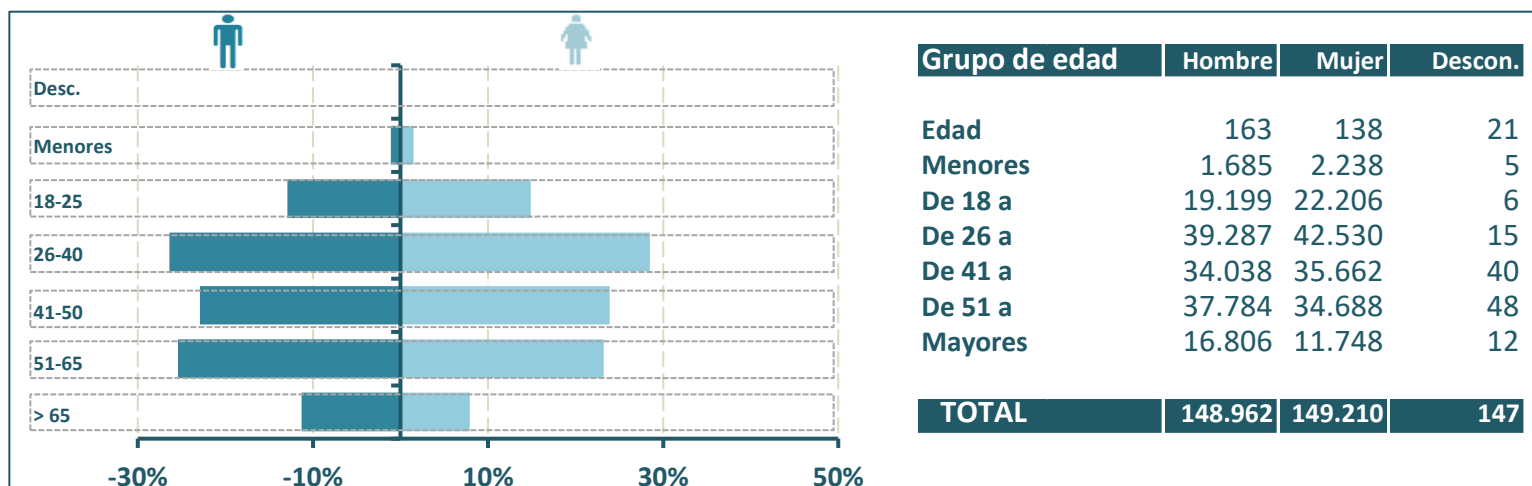
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	2.213	2.898	2	5.113
AMENAZAS Y COACCIONES	9.895	6.643	32	16.570
CONTRA EL HONOR	558	677	5	1.240
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	31	24	0	55
DELITOS SEXUALES (*)	364	765	6	1.135
FALSIFICACIÓN INFORMÁTICA	4.912	4.842	8	9.762
FRAUDE INFORMÁTICO	130.152	132.732	91	262.975
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	837	629	3	1.469
Total VICTIMIZACIONES	148.962	149.210	147	298.319

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

DISTRIBUCIÓN PORCENTUAL DE LAS VÍCTIMAS POR GRUPO PENAL SEGÚN SEXO



>> 3.7. Victimizaciones según grupo de edad y sexo. Año 2022



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

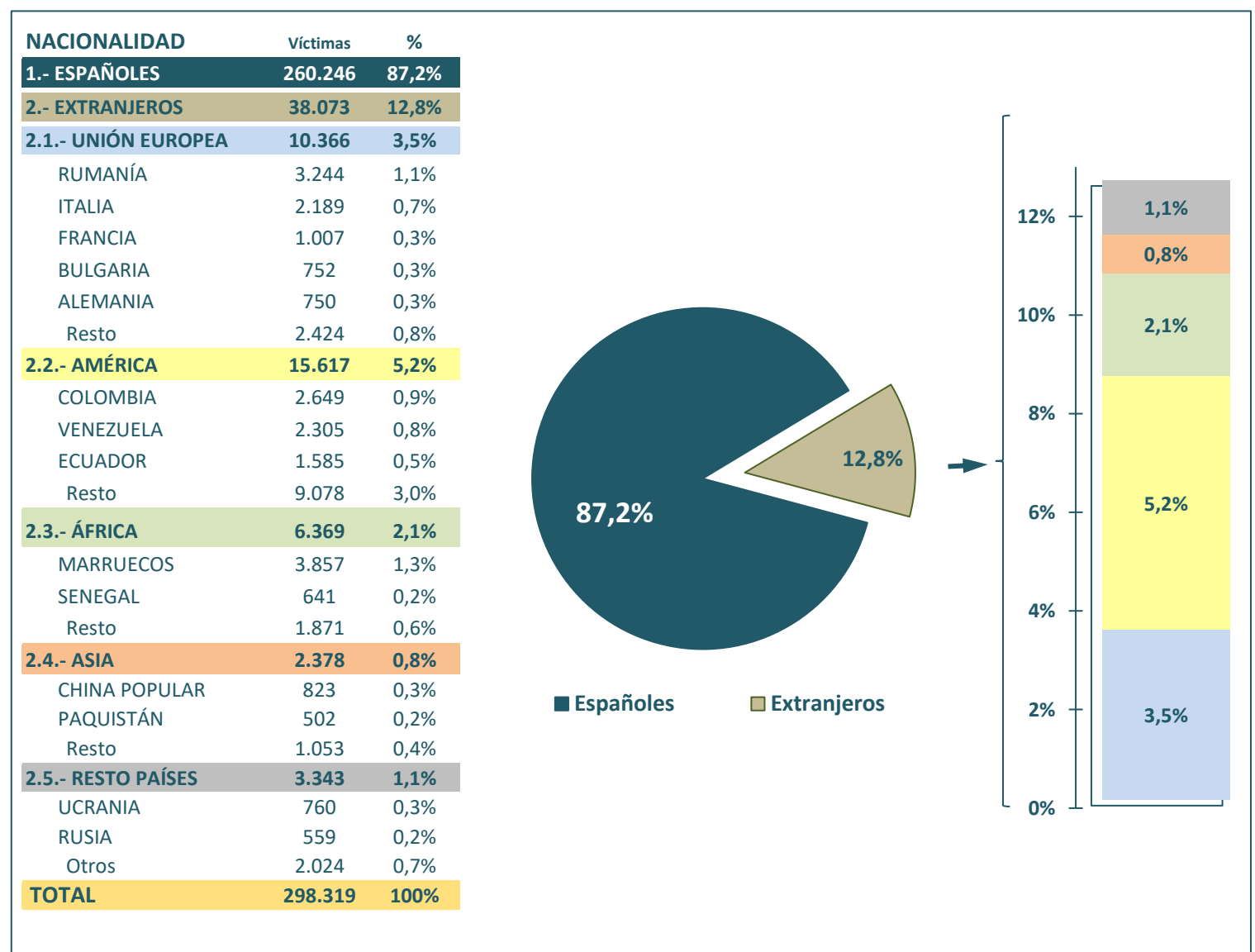
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.8. Victimizaciones por tipología penal y sexo. Año 2022



TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL	0%	20%	40%	60%	80%	100%
ESTAFAS TARJ CRÉD, DÉBITO Y CHEQUES VIAJE	55.274	59.644	35	114.953						
OTRAS ESTAFAS	47.597	44.670	31	92.298						
ESTAFA BANCARIA	20.905	21.877	1	42.783						
AMENAZAS	8.680	5.614	30	14.324						
ESTAFAS INFORMÁTICAS	6.376	6.541	24	12.941						
USURPACIÓN DE ESTADO CIVIL	4.887	4.826	8	9.721						
ACCESO ILEGAL INFORMÁTICO	1.317	1.465	1	2.783						
DESCUBRIMIENTO/REVELACIÓN SECRETOS	896	1.431	1	2.328						
COACCIONES	1.214	1.027	2	2.243						
RESTO	1.816	2.115	14	3.945						
Total VICTIMIZACIONES	148.962	149.210	147	298.319	0%	20%	40%	60%	80%	100%

>> 3.9. Nacionalidad de la víctima. Año 2022



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

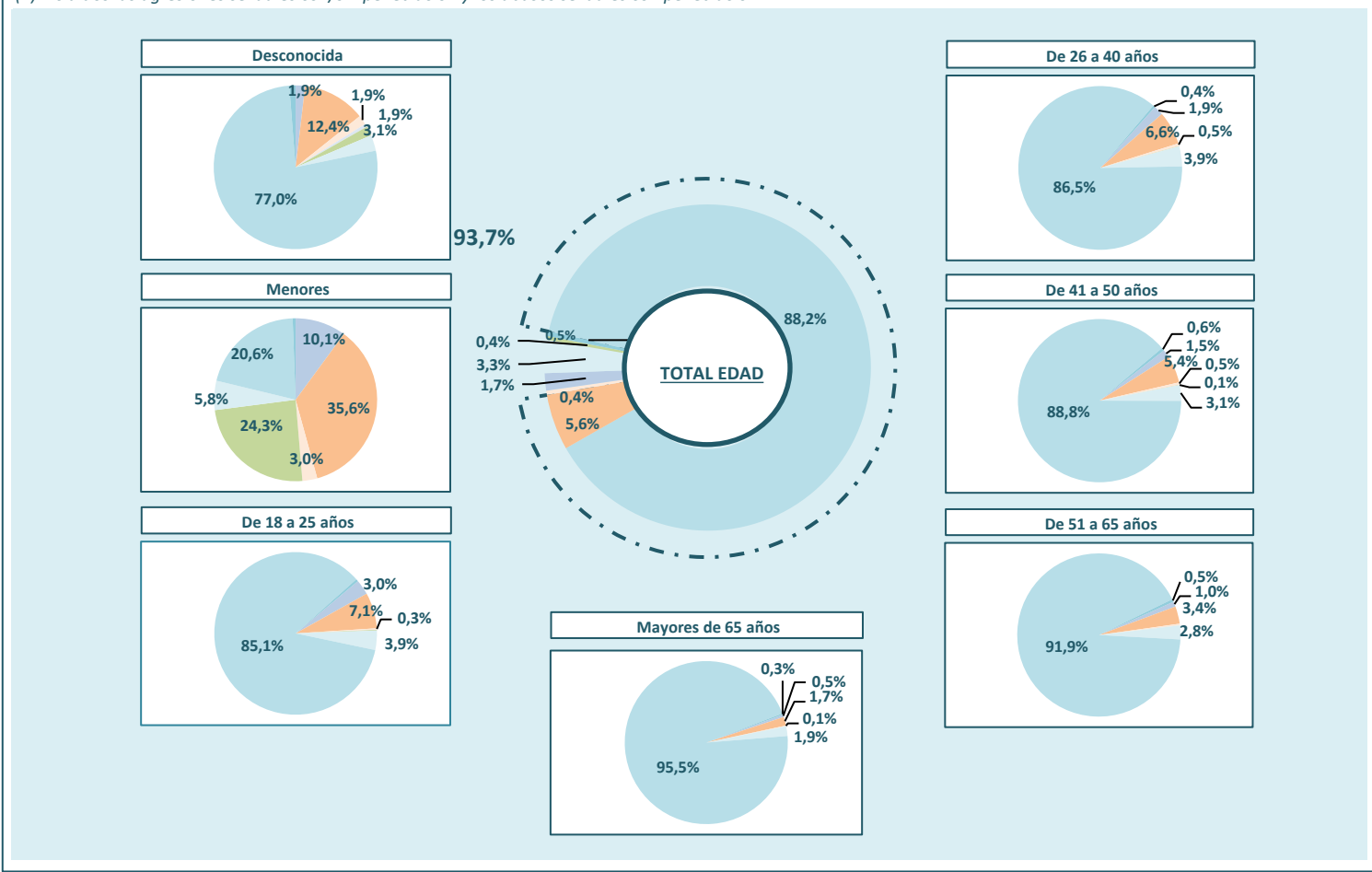
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.10. Victimizaciones registradas según grupo penal y edad. Año 2022

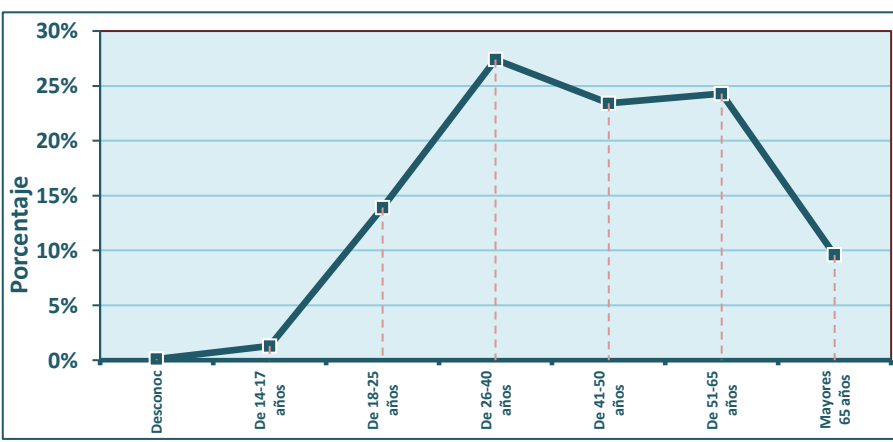


GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	6	396	1.239	1.550	1.057	728	137
AMENAZAS Y COACCIONES	40	1.400	2.947	5.397	3.793	2.501	492
CONTRA EL HONOR	6	116	120	417	330	216	35
CONTRA PROPIEDAD INDUST./INTELEC.	2	0	3	13	19	14	4
DELITOS SEXUALES(*)	6	954	59	60	40	14	2
FALSIFICACIÓN INFORMÁTICA	10	228	1.597	3.230	2.153	1.997	547
FRAUDE INFORMÁTICO	248	811	35.247	70.797	61.947	66.653	27.272
INTERFERENCIA EN DATOS Y EN SISTEMA	4	23	199	368	401	397	77
Total VICTIMIZACIONES	322	3.928	41.411	81.832	69.740	72.520	28.566

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



>> 3.11. Edad de la víctima. Año 2022



Grupo de edad	Víctimas
Edad desconocida	322
Menores de edad	3.928
De 18 a 25 años	41.411
De 26 a 40 años	81.832
De 41 a 50 años	69.740
De 51 a 65 años	72.520
Mayores 65 años	28.566
TOTAL	298.319

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (HOMBRE)

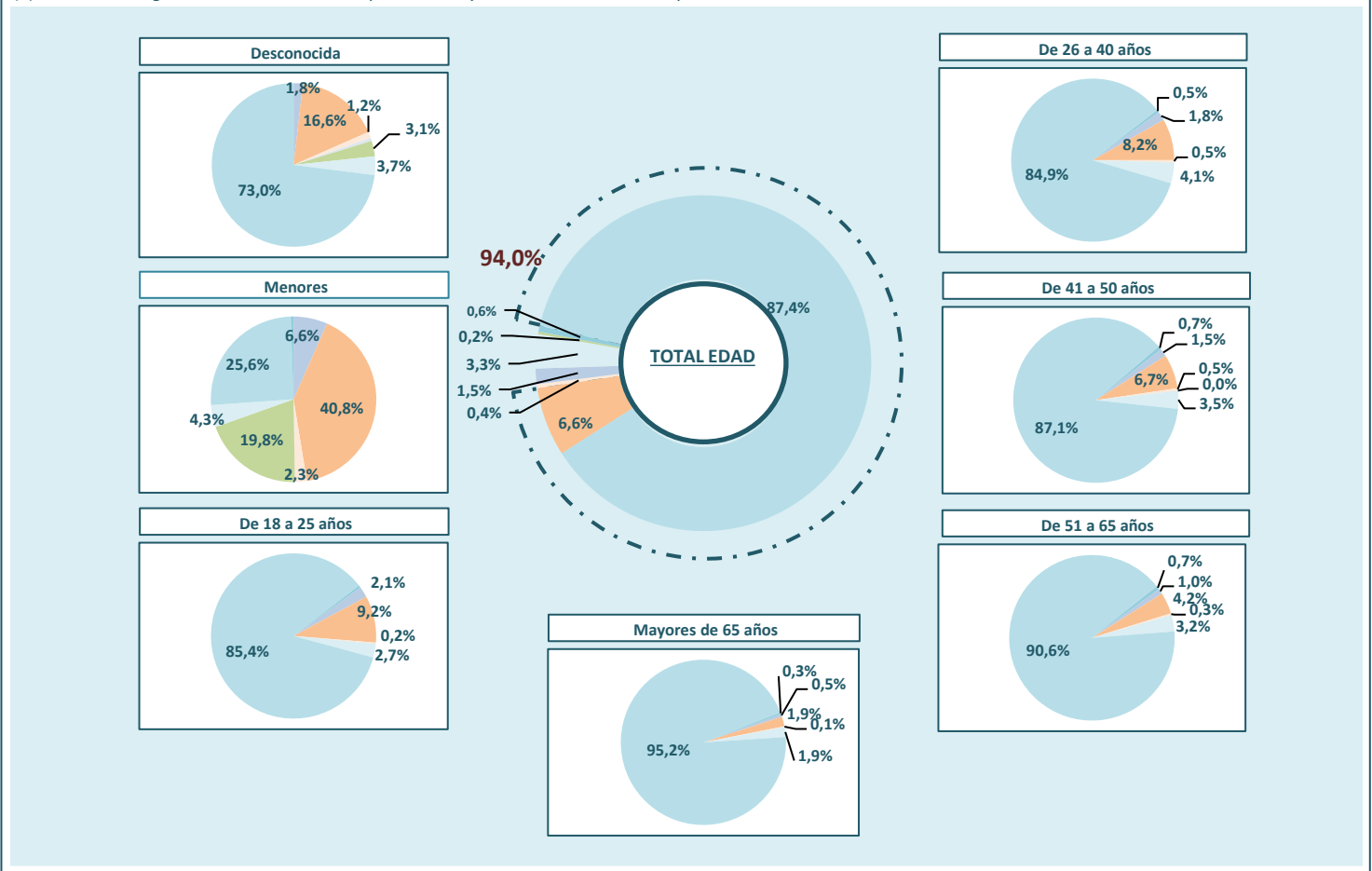
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> **3.12. Victimizaciones registradas según grupo penal y edad. Año 2022**

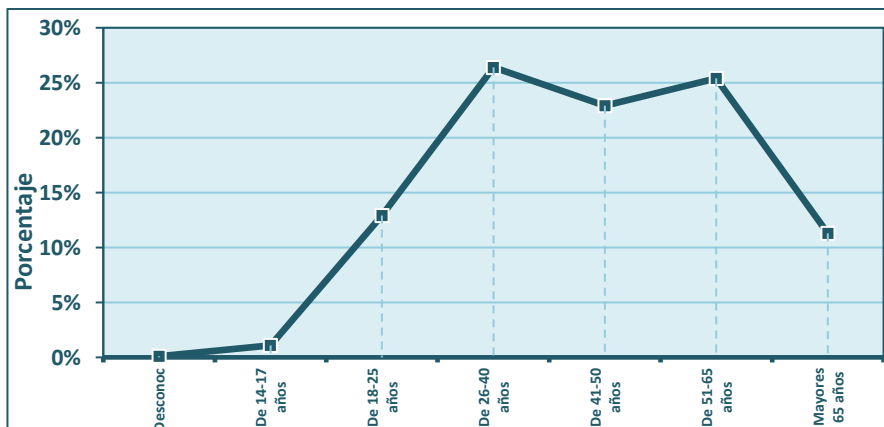


GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	112	408	696	516	387	91
AMENAZAS Y COACCIONES	27	687	1.759	3.227	2.286	1.587	322
CONTRA EL HONOR	2	39	43	180	155	119	20
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	9	6	11	2
DELITOS SEXUALES(*)	5	334	5	10	7	3	0
FALSIFICACIÓN INFORMÁTICA	6	73	509	1.600	1.195	1.204	325
FRAUDE INFORMÁTICO	119	431	16.388	33.361	29.643	34.219	15.991
INTERFERENCIA EN DATOS Y EN SISTEMA	0	9	85	204	230	254	55
Total VICTIMIZACIONES	163	1.685	19.199	39.287	34.038	37.784	16.806

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



>> **3.13. Edad de la víctima. Año 2022**



Grupo de edad	Víctimas
Edad desconocida	163
Menores de edad	1.685
De 18 a 25 años	19.199
De 26 a 40 años	39.287
De 41 a 50 años	34.038
De 51 a 65 años	37.784
Mayores 65 años	16.806
TOTAL	148.962

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (MUJER)

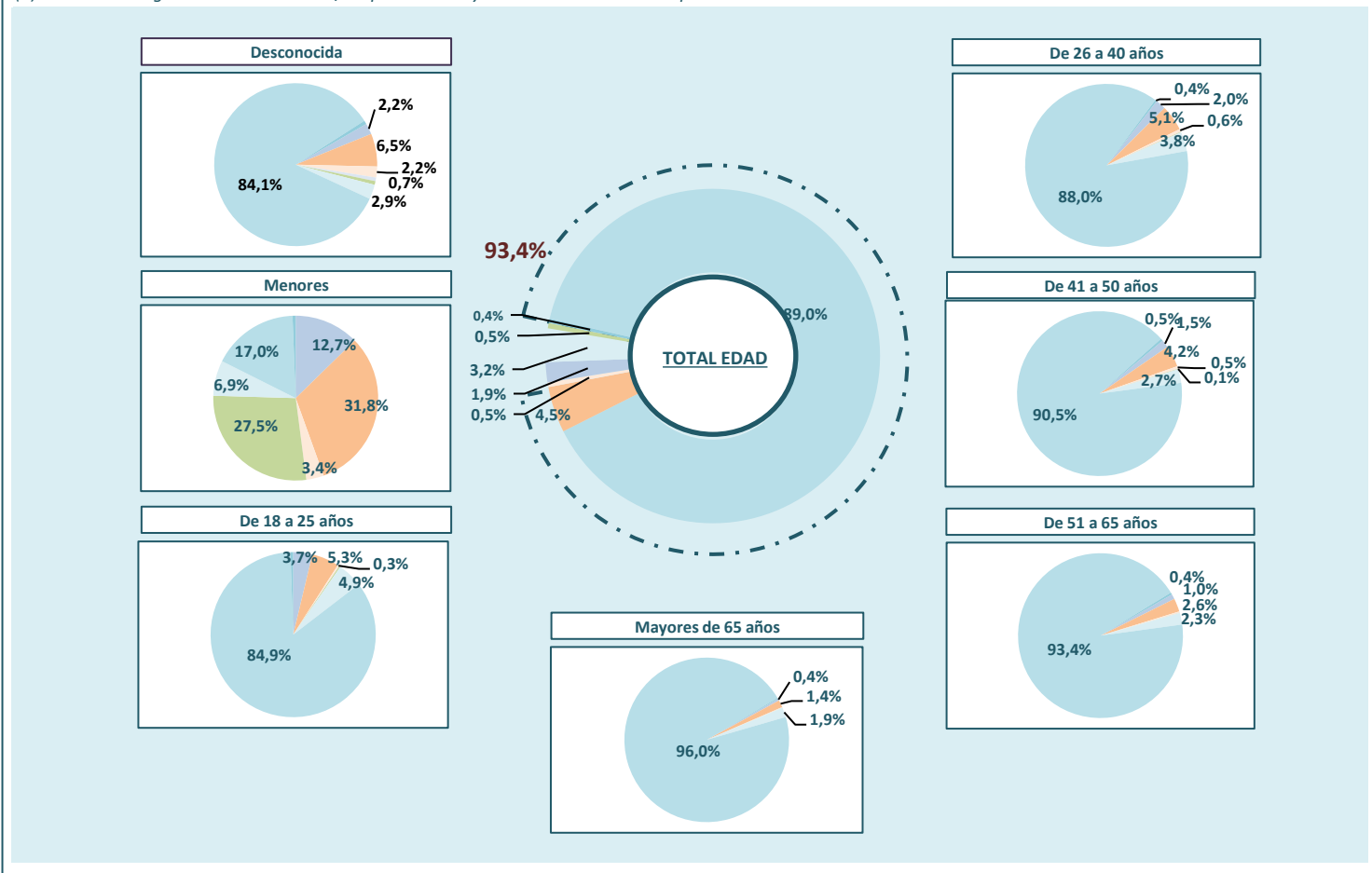
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.14. Victimizaciones registradas según grupo penal y edad. Año 2022

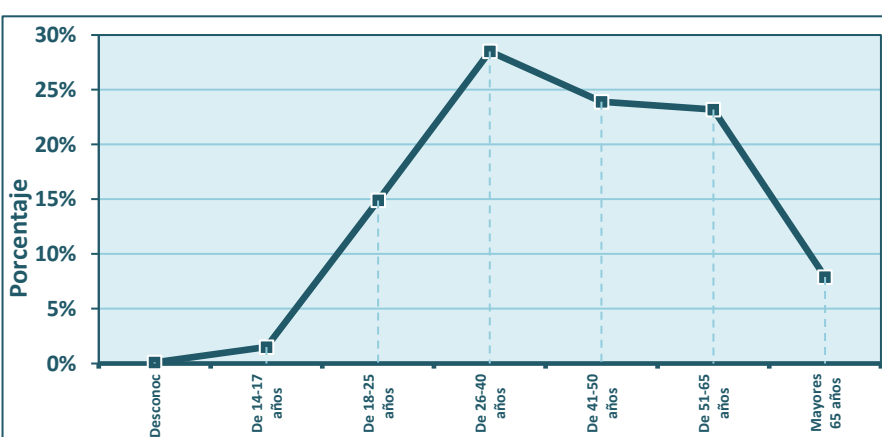


GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	284	831	854	540	340	46
AMENAZAS Y COACCIONES	9	712	1.186	2.167	1.499	903	167
CONTRA EL HONOR	3	77	77	236	175	96	13
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	4	13	3	2
DELITOS SEXUALES(*)	1	616	53	50	32	11	2
FALSIFICACIÓN INFORMÁTICA	4	155	1.088	1.629	954	790	222
FRAUDE INFORMÁTICO	116	380	18.856	37.426	32.278	32.402	11.274
INTERFERENCIA EN DATOS Y EN SISTEMA	1	14	114	164	171	143	22
Total VICTIMIZACIONES	138	2.238	22.206	42.530	35.662	34.688	11.748

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



>> 3.15. Edad de la víctima. Año 2022



Grupo de edad	Víctimas
Edad desconocida	138
Menores de edad	2.238
De 18 a 25 años	22.206
De 26 a 40 años	42.530
De 41 a 50 años	35.662
De 51 a 65 años	34.688
Mayores 65 años	11.748
TOTAL	149.210

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

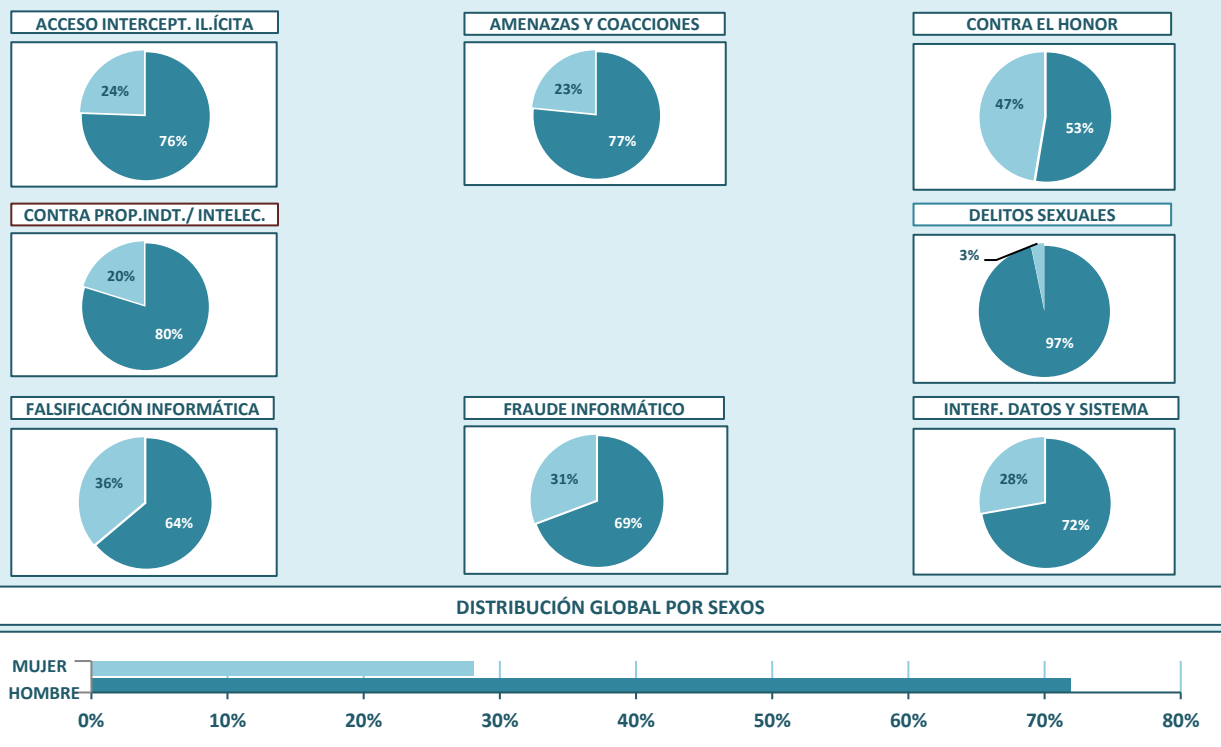


>> 3.16. Detenciones/investigados registrados según grupo penal y sexo. Año 2022

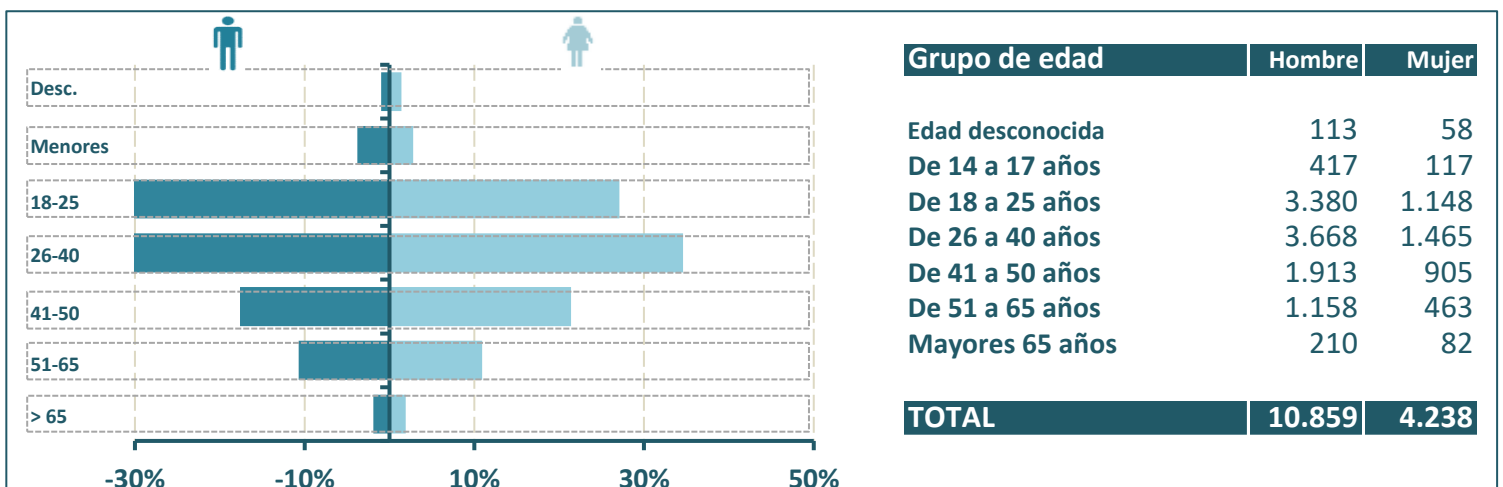
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	300	97	397
AMENAZAS Y COACCIONES	2.041	624	2.665
CONTRA EL HONOR	40	36	76
CONTRA LA PROPIEDAD INDUSTRIAL/INTELLECTUAL	154	39	193
DELITOS SEXUALES(*)	711	24	735
FALSIFICACIÓN INFORMÁTICA	366	207	573
FRAUDE INFORMÁTICO	7.221	3.201	10.422
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	26	10	36
Total DETENCIONES/INVESTIGADOS REGISTRADOS	10.859	4.238	15.097

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

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



>> 3.17. DETENCIONES/INVESTIGADOS según grupo de edad y sexo. Año 2022



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

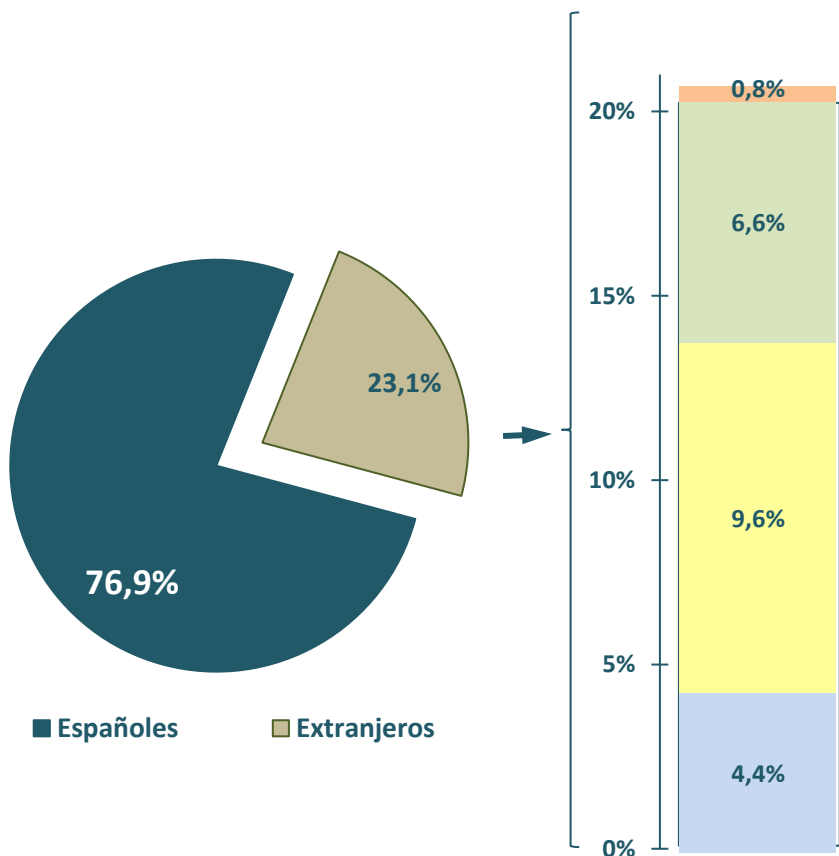
>> 3.18. Detenciones/investigados por tipología penal y sexo. Año 2022



TIPO DE HECHO	Hombres	Mujeres	TOTAL	0%	20%	40%	60%	80%	100%
OTRAS ESTAFAS	4.811	2.221	7.032						
AMENAZAS	1.748	544	2.292						
ESTAFAS TARJETAS CRÉDITO, DÉBITO Y CHEQUES VIAJE	1.440	583	2.023						
ESTAFAS INFORMÁTICAS	767	324	1.091						
USURPACIÓN DE ESTADO CIVIL	344	202	546						
PORNOGRAFÍA DE MENORES	426	13	439						
COACCIONES	293	79	372						
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	262	80	342						
ESTAFA BANCARIA	203	73	276						
RESTO	565	119	684						
Total VICTIMIZACIONES CIBERCRIMINALIDAD	10.859	4.238	15.097						

>> 3.19. Nacionalidad de los detenciones/investigados. Año 2022

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	11.604	76,9%
2.- EXTRANJEROS	3.493	23,1%
2.1.- UNIÓN EUROPEA	667	4,4%
RUMANÍA	245	1,6%
ITALIA	82	0,5%
BULGARIA	67	0,4%
FRANCIA	46	0,3%
PORTUGAL	40	0,3%
Resto	187	1,2%
2.2.- AMÉRICA	1.448	9,6%
REPÚB. DOMINICANA	302	2,0%
COLOMBIA	257	1,7%
VENEZUELA	195	1,3%
Resto	694	4,6%
2.3.- ÁFRICA	998	6,6%
MARRUECOS	497	3,3%
NIGERIA	120	0,8%
Resto	381	2,5%
2.4.- ASIA	123	0,8%
PAQUISTÁN	42	0,3%
CHINA POPULAR	37	0,2%
Resto	44	0,3%
2.5.- RESTO PAÍSES	257	1,7%
UCRANIA	68	0,5%
RUSIA	32	0,2%
Otros	157	1,0%
TOTAL	15.097	100%



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

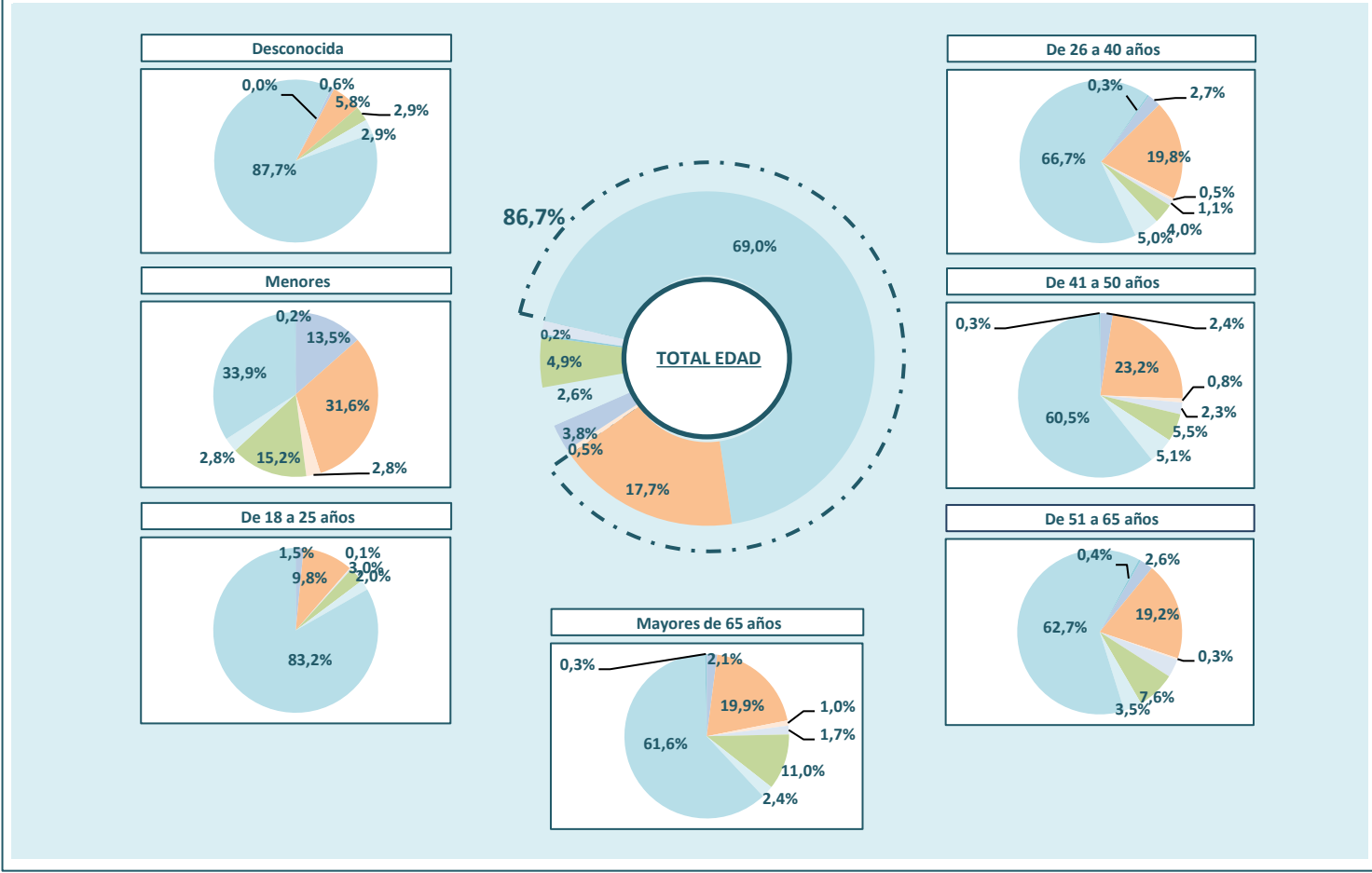
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> **3.20. Detenciones/investigados registradas según grupo penal y edad. Año 2022**

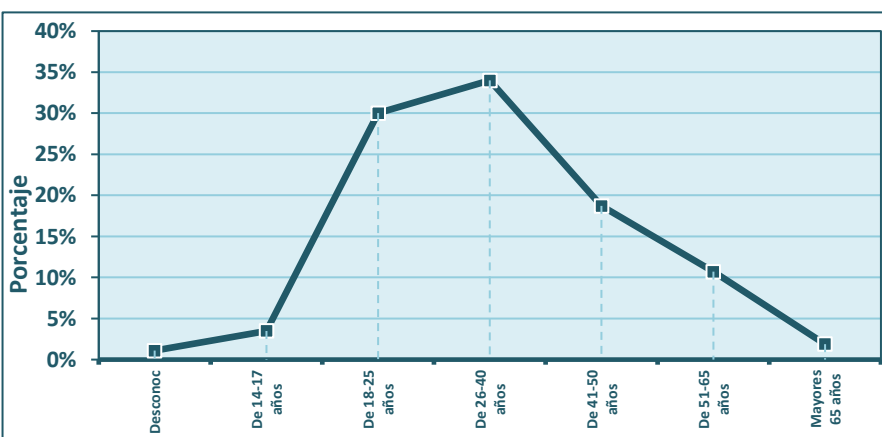


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	72	70	137	69	42	6
AMENAZAS Y COACCIONES	10	169	446	1.017	653	312	58
CONTRA EL HONOR	0	15	5	26	22	5	3
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	11	54	65	58	5
DELITOS SEXUALES(*)	5	81	135	205	154	123	32
FALSIFICACIÓN INFORMÁTICA	5	15	90	256	143	57	7
FRAUDE INFORMÁTICO	150	181	3768	3422	1.704	1.017	180
INTERFERENCIA EN DATOS Y EN SISTEMA	0	1	3	16	8	7	1
Total DETENCIONES/INVESTIGADOS	171	534	4.528	5.133	2.818	1.621	292

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



>> **3.21. Edad de las personas detenidas/investigadas. Año 2022**



Grupo de edad	Det./Inv.
Edad desconocida	171
De 14 a 17 años	534
De 18 a 25 años	4.528
De 26 a 40 años	5.133
De 41 a 50 años	2.818
De 51 a 65 años	1.621
Mayores 65 años	292
TOTAL	15.097

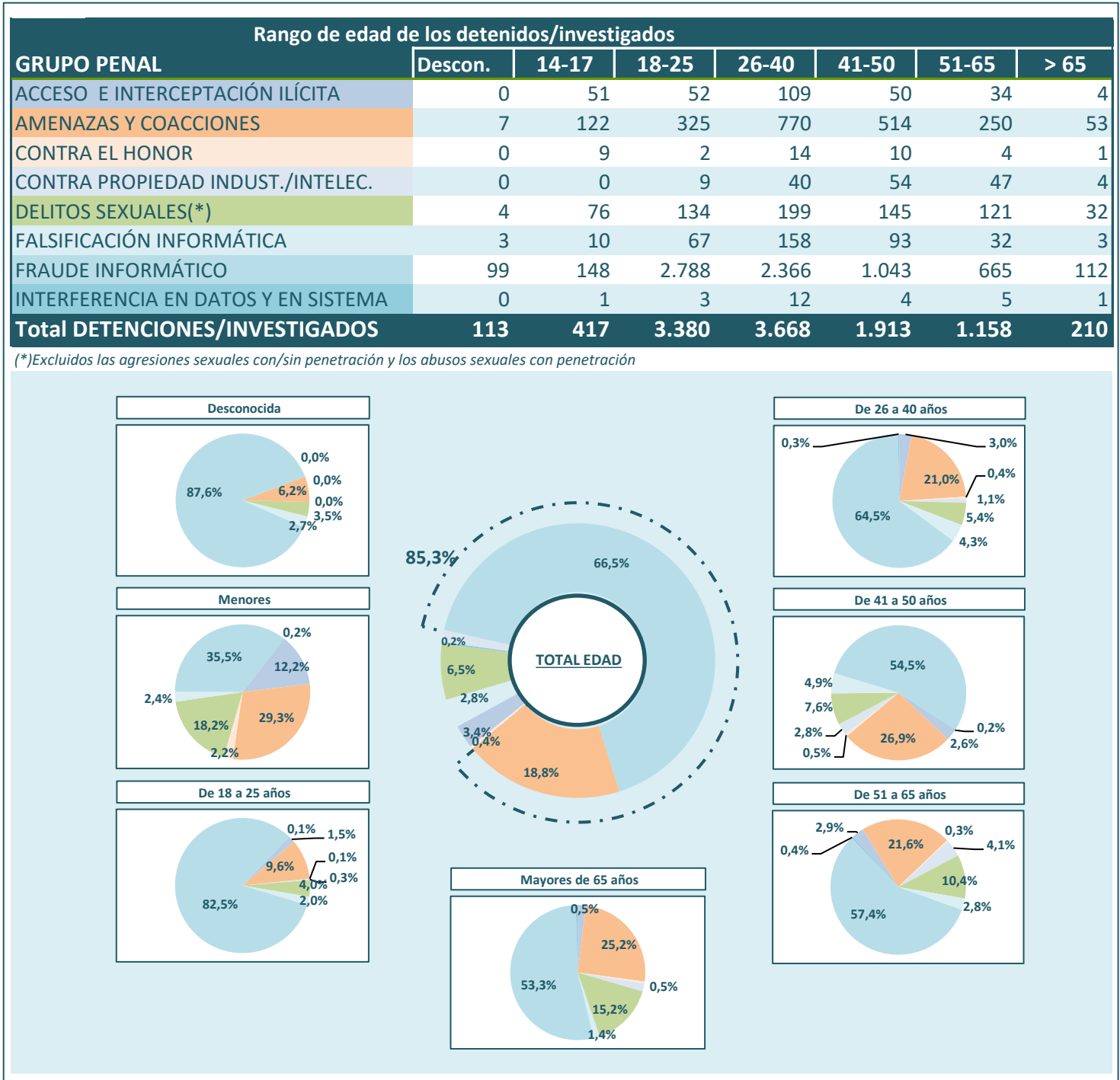
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.-

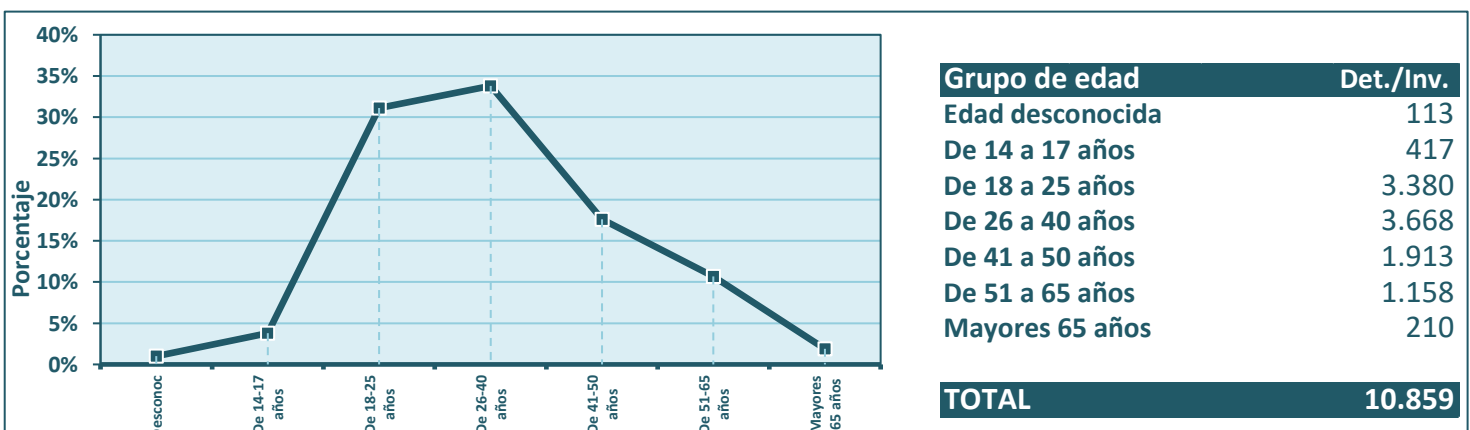
DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.22. Detenciones/investigados registradas según grupo penal y edad. Año 2022



>> 3.23. Edad de las personas detenidas/investigadas. Año 2022



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

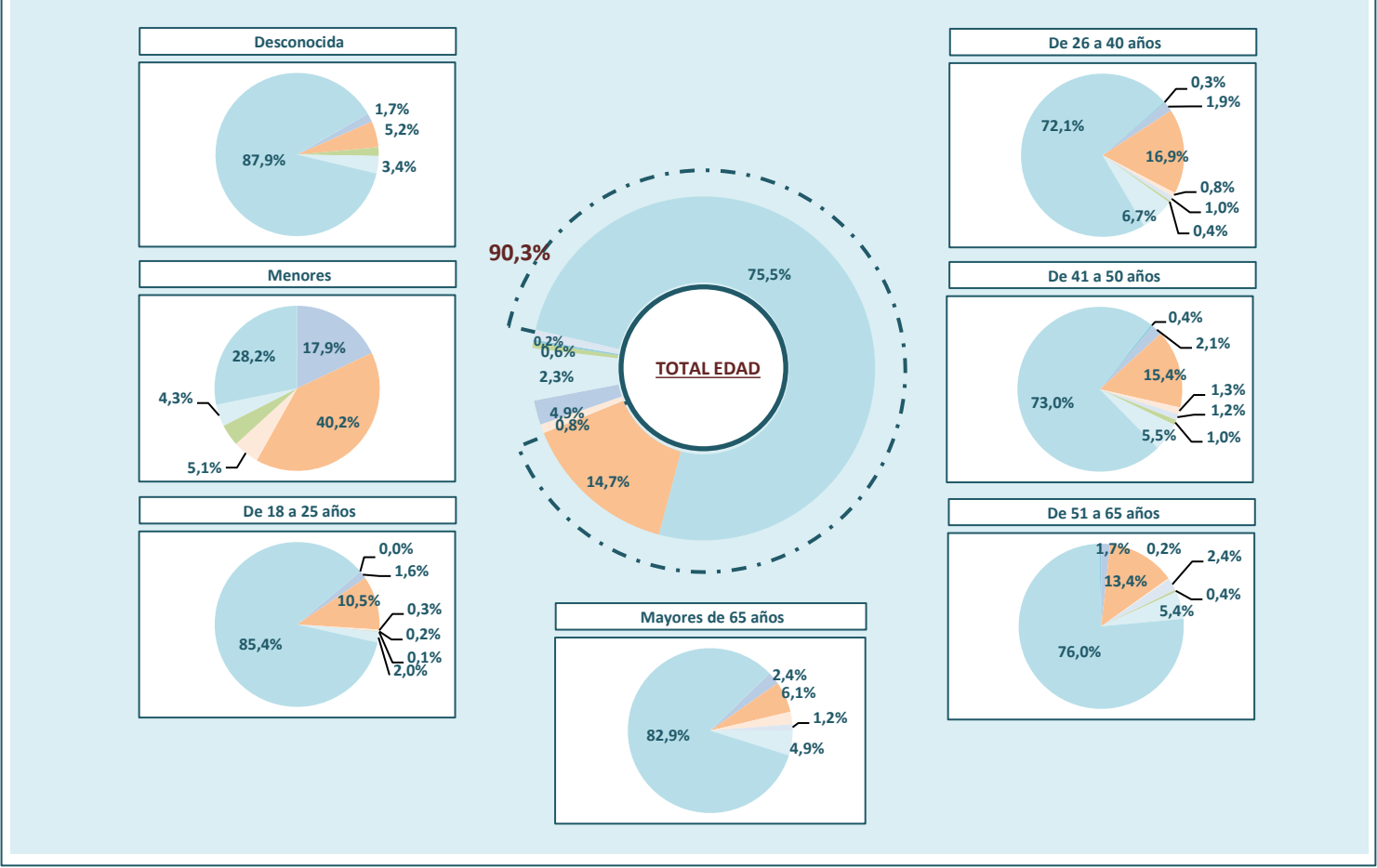
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.24. Detenciones/investigados registradas según grupo penal y edad. Año 2022

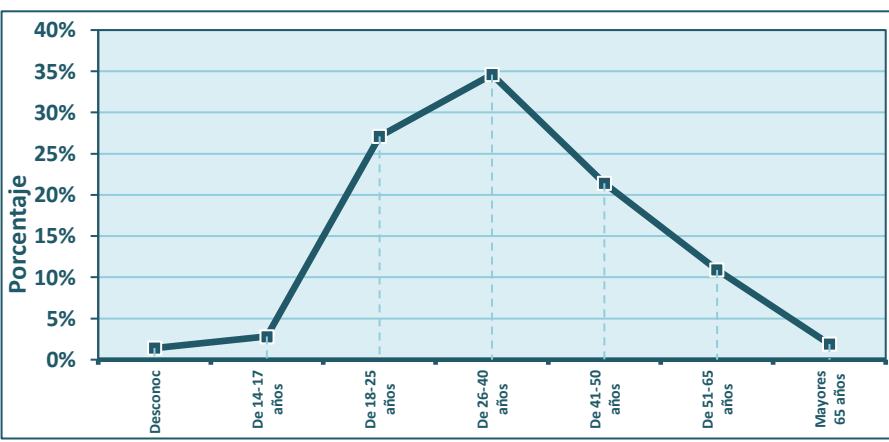


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	21	18	28	19	8	2
AMENAZAS Y COACCIONES	3	47	121	247	139	62	5
CONTRA EL HONOR	0	6	3	12	12	1	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	14	11	11	1
DELITOS SEXUALES(*)	1	5	1	6	9	2	0
FALSIFICACIÓN INFORMÁTICA	2	5	23	98	50	25	4
FRAUDE INFORMÁTICO	51	33	980	1.056	661	352	68
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	0	4	4	2	0
Total DETENCIONES/INVESTIGADOS	58	117	1.148	1.465	905	463	82

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



>> 3.25. Edad de las personas detenidas/investigadas. Año 2022



Grupo de edad	Det./Inv.
Edad desconocida	58
De 14 a 17 años	117
De 18 a 25 años	1.148
De 26 a 40 años	1.465
De 41 a 50 años	905
De 51 a 65 años	463
Mayores 65 años	82
TOTAL	4.238

2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4

METADATA >>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.-

METADATOS

Los datos utilizados 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 Sistema Estadístico de Criminalidad (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 Sistema Estadístico de Criminalidad (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 Sistema Estadístico de Criminalidad (SEC), siguiendo la clasificación adoptada por el Convenio sobre Cibercriminalidad o Convenio de Budapest¹. Se adjunta cuadro explicativo al final de la metadata.

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

- Delitos contra el honor.

¹ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- Amenazas y coacciones.

La explotación estadística se hace en base a 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 conocidos, esclarecidos, detenciones/investigados y victimizaciones

Por hechos conocidos se entiende el conjunto de infracciones penales y administrativas, 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 Sistema Estadístico de Criminalidad (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 por el total de hechos conocidos y multiplicando el resultado por 100. Dado

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

que la Ertzaintza no aporta datos de esclarecidos, el cálculo de este porcentaje se ha obtenido teniendo en cuenta solamente los hechos conocidos y esclarecidos de Policía Nacional, Guardia Civil, Mossos d'Esquadra, Policía Foral de Navarra y cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad (SEC).

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.

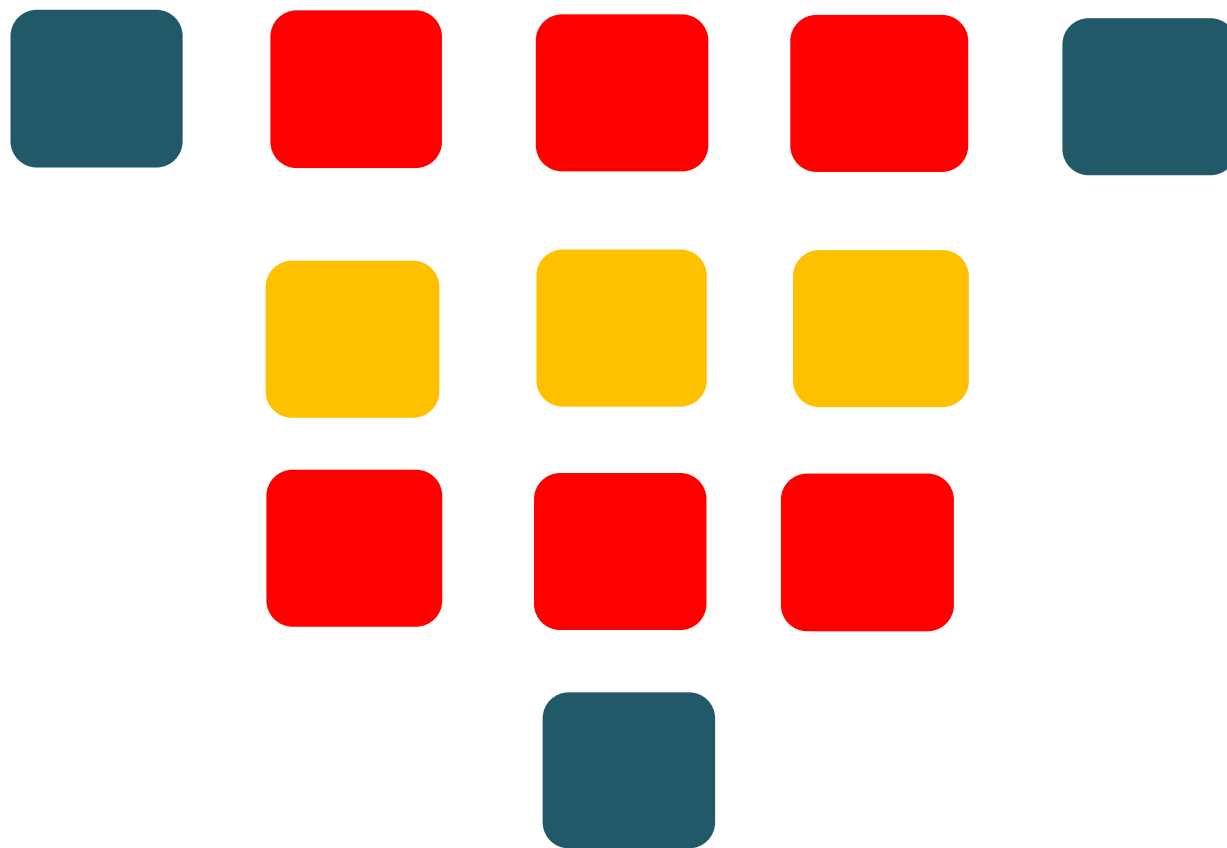
Los contrastes entre victimización y víctima se pueden ejemplificar con el siguiente supuesto: una persona presenta una denuncia y manifiesta que, en un determinado período de tiempo, ha sido objeto de 3 hechos de malos tratos en el ámbito familiar y un delito de amenazas. Además, en esta misma denuncia 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).

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD				
DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SES	VARIABLES SEC A UTILIZAR	
Acceso e interceptación ilícita	Art. 197 A 201. Descubrimiento y revelación de secretos Art. 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	Ámbito cibercrimen	
		DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS E INFORMACIONES RELATIVAS A LA DEFENSA NACIONAL	Ámbito cibercrimen	
		ACCESO ILEGAL A SISTEMAS INFORMÁTICOS	Ninguna	
		INTERCEPTACIÓN, TRANSMISIONES NO PÚBLICAS DE DATOS INFORMÁTICOS	Ninguna	
		FACILITACIÓN DE DISPOSITIVOS, PROGRAMAS O CLAVES PARA ACCEDER ILEGALMENTE A DATOS O SISTEMAS INFORMÁTICOS	Ninguna	
		SEXTING	Ámbito cibercrimen	
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Ámbito cibercrimen	
		DAÑOS	Ámbito cibercrimen	
		FACILITACIÓN DE DISPOSITIVOS, PROGRAMAS O CLAVES PARA COMETER ATAQUES INFORMÁTICOS	Ninguna	
		ATAQUES A DATOS O PROGRAMAS INFORMÁTICOS	Ninguna	
Interferencia en los datos y en el sistema	Arts. 263 a 267 Daños y daños informáticos	ATAQUES A SISTEMAS INFORMÁTICOS	Ninguna	
		FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS	Ámbito cibercrimen	
		FALSIFICACIÓN/TRÁFICO TARJETAS CRÉDITO Y DÉBITO/CHEQUES VIAJE	Ámbito cibercrimen	
		FALSIFICACIÓN/TRÁFICO DE DNI/PASAPORTE	Ámbito cibercrimen	
		OTRAS FALSIFICACIONES DOCUMENTOS	Ámbito cibercrimen	
		FABRICACIÓN/TENENCIA DE ÚTILES PARA FALSIFICAR	Ámbito cibercrimen	
		USURPACIÓN DE ESTADO CIVIL	Ámbito cibercrimen	
		USURPACIÓN DE FUNCIONES PÚBLICAS	Ámbito cibercrimen	
		INTRUSISMO	Ámbito cibercrimen	
		ESTAFAS BANCARIAS (hasta 2021)	Ámbito cibercrimen	
Falsificación informática	Arts. 386 al 403	ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE VIAJE (248.2.c CP)	Ámbito cibercrimen	
		OTRAS ESTAFAS	Ámbito cibercrimen	
		ESTAFAS DE INVERSORES	Ninguna	
		ESTAFAS INFORMÁTICAS (arts. 248.2.a.b CP)	Ámbito cibercrimen	
		AGRESIÓN SEXUAL	Ámbito cibercrimen	
		AGRESIÓN SEXUAL CON PENETRACIÓN	Ámbito cibercrimen	
		ABUSO SEXUAL (hasta 07/10/2022)	Ámbito cibercrimen	
		ABUSO SEXUAL CON PENETRACIÓN (hasta 07/10/2022)	Ámbito cibercrimen	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 16 AÑOS CON FINES SEXUALES (GROOMING)	(sin ámbito)	
		ACOSO SEXUAL	Ámbito cibercrimen	
Fraude Informático	Arts. CP 248 a 251	EXHIBICIONISMO	Ámbito cibercrimen	
		PROVOCACIÓN SEXUAL	Ámbito cibercrimen	
		CORRUPCIÓN DE MENORES/CON DISCAPACIDAD/DIVERSIDAD FUNCIONAL	Ámbito cibercrimen	
		DELITOS RELATIVOS A LA PROSTITUCIÓN	Ámbito cibercrimen	
		PORNOGRAFÍA DE MENORES	Ámbito cibercrimen	
		DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Ámbito cibercrimen	
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	Ámbito cibercrimen	
		ACCESO FRAUDULENTO A SERVICIOS DE RADIODIFUSIÓN/TV/OTROS	Ámbito cibercrimen	
		DELITO DE ESPIONAJE INDUSTRIAL Y SECRETO PROFESIONAL (ARTS. 278 A 280 CP)	Ámbito cibercrimen	
		CALUMNIAS	Ámbito cibercrimen	
Delitos sexuales	Arts. CP 178 a 189	INJURIAS	Ámbito cibercrimen	
		INJURIAS Y CALUMNIAS A FUNCIONARIO PÚBLICO, AUTORIDAD O AGENTE DE LA AUTORIDAD (ARTS. 205 Y 215 CP)	Ámbito cibercrimen	
		AMENAZAS	Ámbito cibercrimen	
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	Ámbito cibercrimen	
		COACCIONES	Ámbito cibercrimen	
		EXTORSIÓN	Ámbito cibercrimen	
		TRATO DEGRADANTE	Ámbito cibercrimen	
		ACOSO LABORAL Y FUNCIONARIAL	Ámbito cibercrimen	
		ACOSO CONTRA LA LIBERTAD DE LAS PERSONAS	Ámbito cibercrimen	
		PERFILES FALSOS CON FINES ACOSO/HOSTIGAMIENTO/HUMILLACIÓN	Ámbito cibercrimen	
Contra la propiedad industrial/intelectual	Arts. 270 a 277 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Ámbito cibercrimen	
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	Ámbito cibercrimen	
		ACCESO FRAUDULENTO A SERVICIOS DE RADIODIFUSIÓN/TV/OTROS	Ámbito cibercrimen	
		DELITO DE ESPIONAJE INDUSTRIAL Y SECRETO PROFESIONAL (ARTS. 278 A 280 CP)	Ámbito cibercrimen	
		CALUMNIAS	Ámbito cibercrimen	
		INJURIAS	Ámbito cibercrimen	
		INJURIAS Y CALUMNIAS A FUNCIONARIO PÚBLICO, AUTORIDAD O AGENTE DE LA AUTORIDAD (ARTS. 205 Y 215 CP)	Ámbito cibercrimen	
		AMENAZAS	Ámbito cibercrimen	
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	Ámbito cibercrimen	
		COACCIONES	Ámbito cibercrimen	
Contra el honor	Arts. 205 a 210 del Código Penal	AMENAZAS	Ámbito cibercrimen	
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	Ámbito cibercrimen	
		COACCIONES	Ámbito cibercrimen	
		EXTORSIÓN	Ámbito cibercrimen	
		TRATO DEGRADANTE	Ámbito cibercrimen	
		ACOSO LABORAL Y FUNCIONARIAL	Ámbito cibercrimen	
		ACOSO CONTRA LA LIBERTAD DE LAS PERSONAS	Ámbito cibercrimen	
		PERFILES FALSOS CON FINES ACOSO/HOSTIGAMIENTO/HUMILLACIÓN	Ámbito cibercrimen	
		AMENAZAS Y COACCIONES	Arts 169 a 173 del C. Penal	Ámbito cibercrimen

ESPAÑA



2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Síguenos en Twitter

@interiorgob



www.interior.gob.es

2022