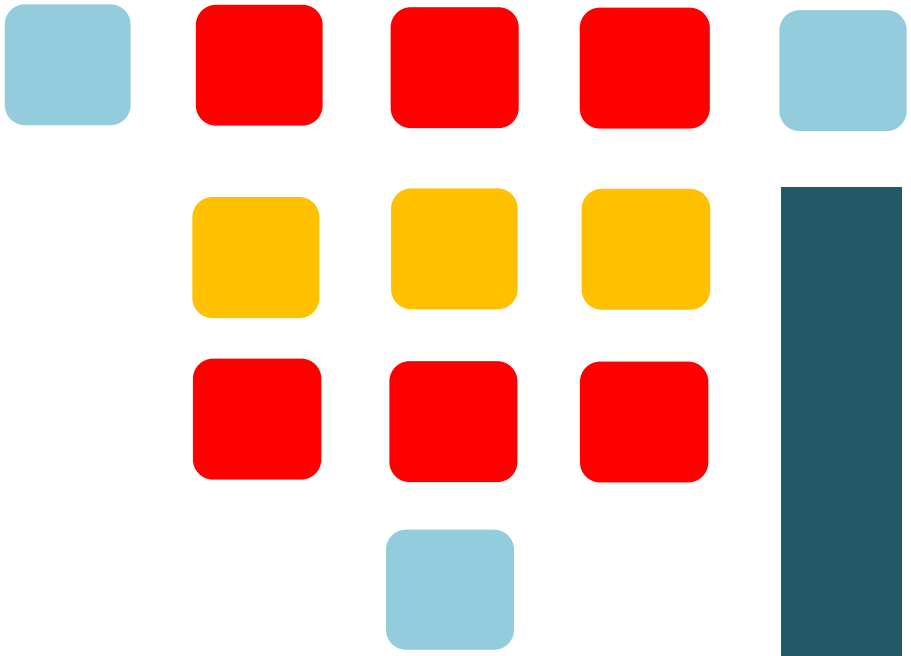
2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS
seC Sistema Estadístico de Criminalidad

2023

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

seC Sistema Estadístico de Criminalidad

2023

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 Mª SANTIAGO OROZCO
MIGUEL ÁNGEL GÓMEZ MARTÍN

Edita:

MINISTERIO DEL INTERIOR | SECRETARÍA GENERAL TÉCNICA

NIPO 126-20-021-2

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

0 INDICE

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

seC Sistema Estadístico de Criminalidad

2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1 INTRODUCCIÓN >>

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 durante el año 2023.

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 proporciona cada Cuerpo policial.

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 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

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.), y 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 conceptuaciones que emplea el Convenio de Budapest[2], 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

Situación actual de la Cibercriminalidad en España y dentro del marco internacional

Un aspecto que es necesario resaltar es el previsible aumento de la ciberdelincuencia. En palabras de las propias instituciones europeas[3], "*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 2019[5].

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.

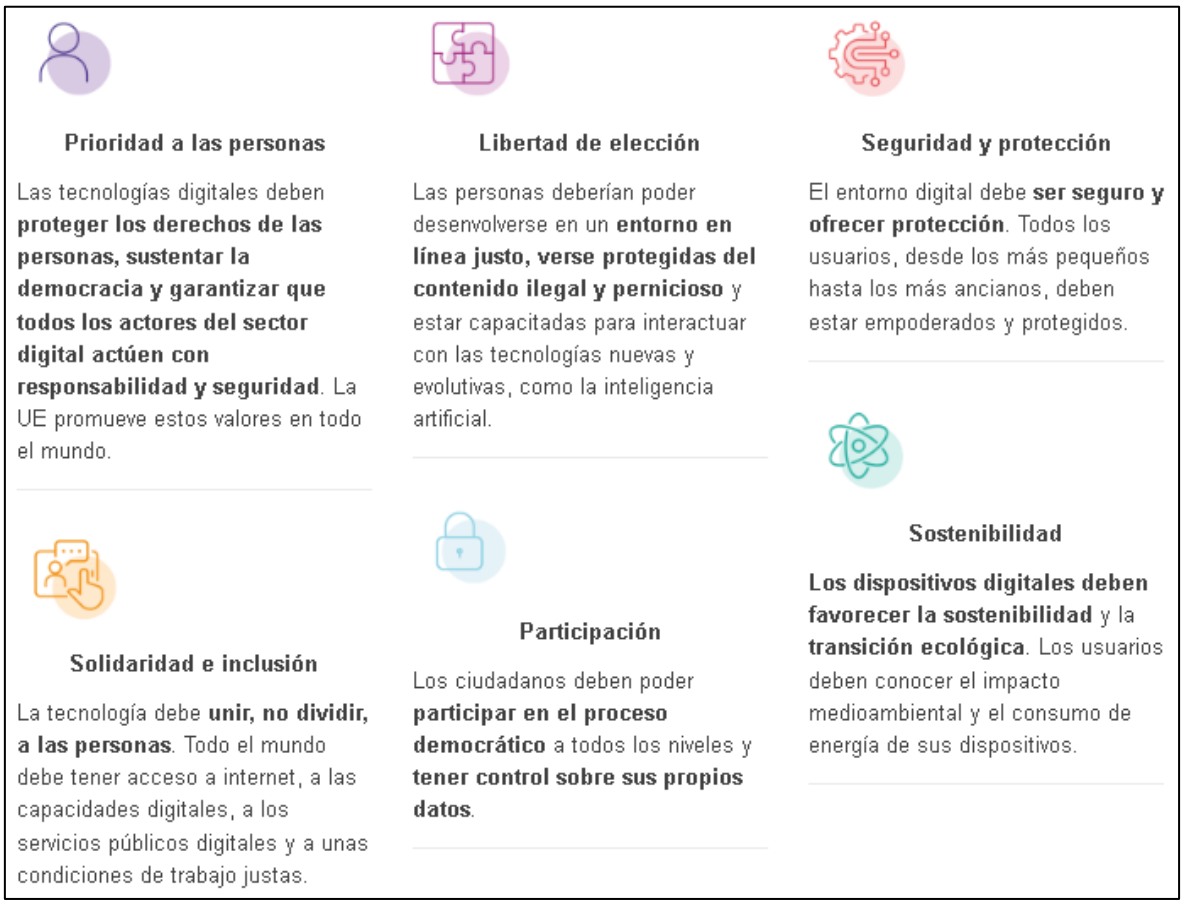
[3] https://www.consilium.europa.eu/es/policies/cybersecurity/
[4] https://www.consilium.europa.eu/es/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/
[5] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02019D0797-20201124&from=EN

*Brújula Digital[6] para la Década Digital de la UE: que persigue los siguientes objetivos para 2030.[7]

Infografía nº 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

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



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

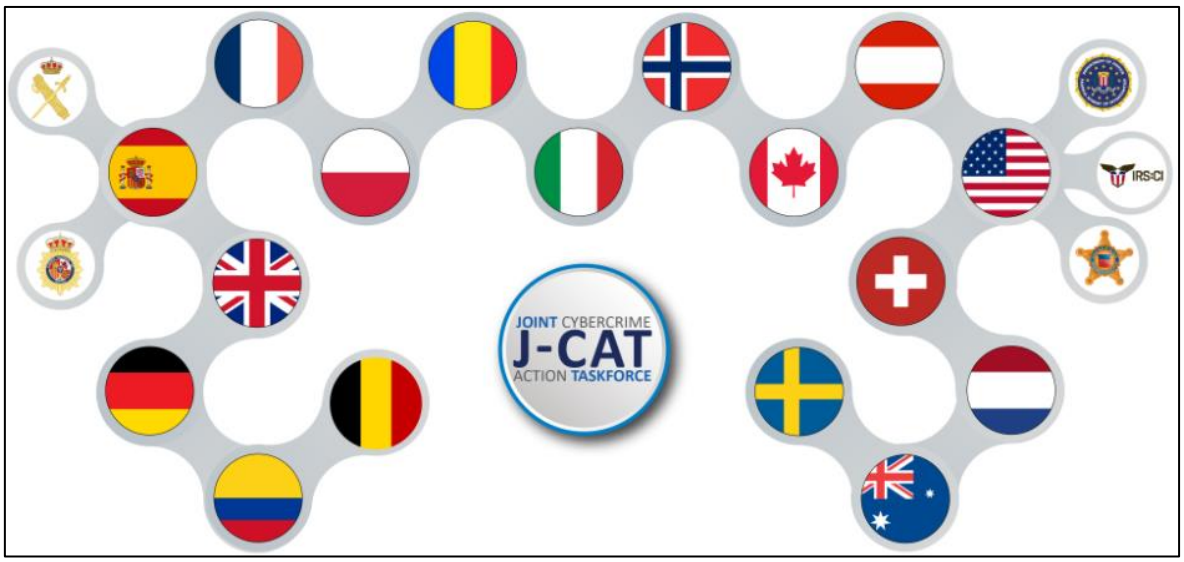
Sumado a todo lo anterior, un aspecto destacado en la lucha contra la Cibercriminalidad, es la respuesta policial que se da dentro del ámbito europeo. Para ello, se dispone de una serie de herramientas dentro del seno de EUROPOL, tales como:

- 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

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

HOME identifiquen, discutan y prioricen los principales desafíos y acciones en la lucha contra el ciberdelito. [9]

- 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 2022/2555[11] de 14 de diciembre de 2022, también denominada NIS2. Esta Directiva establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros. Los estados miembros habrán de

[9] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf
[10] https://www.europol.europa.eu/cms/sites/default/files/documents/space_flyer-2019.pdf
[11] https://www.boe.es/doue/2022/333/L00080-00152.pdf

adoptar y publicar las medidas necesarias para dar cumplimiento a lo establecido en la directiva antes del 18 de octubre de 2024, fecha en la que habrán de entrar en vigor.

Las medidas incluyen:

- Desarrollo de estrategias de ciberseguridad por parte de los Estados miembros.
- Designación o establecimiento de autoridades competentes en ciberseguridad.
- Creación de autoridades encargadas de gestionar crisis relacionadas con la ciberseguridad.
- Obligación de informar sobre incidentes de seguridad graves a las autoridades competentes.

Por último, es de destacar que la Comisión Europea[12] 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 para tener en cuenta:

[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

"el 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 28 de diciembre de 2021, mediante Real Decreto 1150/2021[15]. 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 ultraterreste, se promueve el avance en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

En la Estrategia Nacional de Ciberseguridad 2019[16], aprobada por orden PCI(487/2019 del Consejo de Seguridad Nacional se afirma que la Cibercriminalidad es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos.

En dicha estrategia se define la cibercriminalidad como "el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los

[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.boe.es/buscar/doc.php?id=BOE-A-2019-6347

daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo".

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 2023[18], se extraen una serie de conclusiones:

- Se ha observado un aumento en el uso de ransomware, con la utilización de los datos obtenidos para realizar extorsión sobre las víctimas. Se aprovecha el aumento generalizado del teletrabajo.
- También se están utilizando otros métodos de coacción como llamadas telefónicas a periodistas, clientes y socios de las víctimas.
- La cibercriminalidad sigue experimentando un crecimiento durante todos estos años.
- La digitalización acelerada debido a la pandemia de COVID, ha influido significativamente en el desarrollo de amenazas cibernéticas. La "infraestructura gris" como servicios de cifrado extremo a extremo, VPN y criptomonedas, sigue facilitando una amplia gama de actividades delictivas.
- Se ha observado un aumento en la técnica del phishing, donde los ciberdelincuentes se hacen pasar por terceros para obtener información confidencial.

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"[19]. La citada agencia, establece cuatro tipos de objetivos que persigue la desinformación, catalogando los medios con los que se lleva cada uno de ellos.

[17] https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023
[18] https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[19] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

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 el Informe Anual de Seguridad Nacional 2023[20] se afirma que "las tensiones globales están llevando a un incremento de la difusión de campañas de desinformación, con un aumento de las narrativas antioccidentales y antieuropeas". Este aspecto ha ido evolucionando hacia el concepto de interferencia por manipulación de la información, en el que prima la intencionalidad sobre la veracidad. Respecto a este particular, en el informe ENISA 2023[21] se afirma lo siguiente:

"La 'Manipulación e interferencia de información extranjera' (FIMI, por sus siglas en inglés) describe un patrón de comportamiento en su mayoría no ilegal que amenaza o tiene el potencial de afectar negativamente los valores, procedimientos y procesos políticos. Esta actividad es manipuladora en su carácter, llevada a cabo de manera intencional y coordinada. Aquellos que realizan esta actividad pueden ser actores estatales o no estatales, incluyendo a sus intermediarios dentro y fuera de su propio territorio[22]."

Este informe de ENISA (ETL por sus siglas en inglés) *"ha estado monitoreando la manipulación de información como 'Desinformación - Información errónea' desde 2021. En esta edición del ETL, optamos por el término más general de manipulación de información para reflejar un conjunto más amplio de amenazas potenciales. En consecuencia, la amenaza de manipulación de información persistió en la edición de este año, estableciéndose como una tendencia estable. Aunque la desinformación es una parte destacada de la manipulación de información, 'manipulación de información' pone énfasis*

[20] https://www.dsn.gob.es/es/file/9710/download?token=lUW0ytDb
[21] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport
[22] https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

en el comportamiento en lugar de la veracidad del contenido y, por lo tanto, se ha preferido sobre el término 'desinformación'. La noción de comportamiento manipulador es consistente con las otras categorías de amenazas en el ETL, dado que indica claramente la intención de llevar a cabo acciones maliciosas que tienen un impacto adverso. Por lo tanto, se considera más adecuado para la definición de lo que constituye una amenaza de ciberseguridad".

Otro de los riesgos de la desinformación, del que ya se viene advirtiendo desde el Plan de Acción contra la desinformación[23], presentado y aprobado en el Consejo Europeo de los días 13 y 14 de diciembre de 2018 y en el European Democracy Action Plan[24] de 2020, es su potencial efecto perjudicial en los procesos electorales democráticos.

En el Real Decreto 207/2024, de 24 de febrero de estructura del Ministerio del Interior, se constituye el Observatorio de la Cibercriminalidad, a través de la Oficina de Coordinación de Ciberseguridad (OCC), a fin de entre otros cometidos, combatir la desinformación. El Ministerio del Interior, a través de la OCC, participa en la Comisión Permanente contra la Desinformación, creada por Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional.

2.- INCIDENTES DE CIBERSEGURIDAD (OCC)

En la introducción al Capítulo se detallan los aspectos más relevantes en esta materia, entre los que se incluyen datos sobre incidentes gestionados por Oficina de Coordinación de Ciberseguridad (OCC).

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

[23] https://data.consilium.europa.eu/doc/document/ST-15431-2018-INIT/es/pdf

[24] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_2250/IP_20_2250_EN.pdf

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, y del último Real Decreto 207/2024, de 24 de febrero, por los que se ha venido desarrollando la estructura orgánica básica del Ministerio del Interior.

El 31 de enero de 2013, 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 responsables[25], se llevará a cabo la explotación estadística de los datos que se 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.

[25] Actuaciones policiales y responsables: son dos operaciones estadísticas dadas de alta en el Inventario de Operaciones Estadísticas del INE https://ine.es/dyngs/IOE/index.htm

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 2019-2023 (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 2019 a 2023, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2023, se han conocido un total de 472.125 hechos, lo que supone un 26% más con respecto al año anterior. De esta cifra, el 90,5% corresponde a fraudes informáticos (estafas) y el 3,7% 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 9,9% en el año 2019, a un 19,2% en el año 2023.

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

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 2019 a 2023.

En relación al porcentaje de hechos esclarecidos, en el año 2023, éste supone el 13,5% del total de los hechos conocidos, lo que implica un descenso con respecto al año anterior, que alcanzó el porcentaje de esclarecimiento del 14,6%. Por otra parte, los detenidos e investigados han alcanzado la cifra de 17.173, lo que supone un aumento de un 13,8% con respecto al año 2022, en el que se registraron 15.097 detenidos e investigados.

En el apartado 3.3 y 3.4 se detallan datos por meses, observándose que durante el 2023, el mes de mayor incidencia delictiva fue el mes de noviembre.

La distribución de la Cibercriminalidad, desde el punto de vista geográfico (3.5. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2023, sitúa a Andalucía, Madrid, Cataluña 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, Málaga, Alicante/Alacant 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.

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

[26] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (472.125) y el de victimizaciones registradas (354.610), 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 ocasiones no se poseen datos de dichas víctimas.

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 con la nacionalidad de la víctima (apartado 3.9), el 86,9% de ellas son españolas, y el 13,1% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Marruecos, Colombia y Rumanía las que aúnan valores más elevados.

Al igual que en el informe de 2022, en este *Informe sobre Cibercriminalidad 2023,* 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 las 3.14 y 3.15, las del sexo femenino. 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 2023.

De la cifra total de detenciones e investigaciones (17.173) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 72,5% 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 y 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 (76,7%) (3.19). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Marruecos, Colombia y Rumanía, 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 18 a 25 años.

2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2

INCIDENTES DE CIBERSEGURIDAD (OCC) >>

2.- INCIDENTES DE CIBERSEGURIDAD (OCC)

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 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

La OCC, incardinada en la Dirección General de Coordinación y Estudios, 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**, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información; así mismo, ejerce como **canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia** y la Secretaría de Estado de Seguridad, y se constituye en **Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior de apoyo a la Policía Judicial (CSIRT-MIR-PJ)**, con la finalidad de dar soporte técnico y coordinar a las unidades de investigación de la ciberdelincuencia de las Fuerzas y Cuerpos de Seguridad del Estado en los supuestos que se determinen.

Asimismo, la **OCC** desempeña las funciones que, conforme a lo dispuesto en el **Real Decreto-ley 12/2018**, de 7 de septiembre, de seguridad de las redes y sistemas de información, tiene asignadas la **Secretaría de Estado de Seguridad como autoridad competente** en materia de seguridad de las redes y sistemas de información para los operadores de servicios esenciales que sean, además, designados operadores críticos, de modo que 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.

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.

>> 2.1. Incidentes gestionados con afectación en operadores críticos de nivel alto, muy alto o crítico

Se han gestionado un total de **NOVENTA (90)** incidentes de ciberseguridad en España durante el año 2023, **con niveles de peligrosidad e impacto alto, muy alto o crítico**, en base a la Instrucción nacional de notificación y gestión de ciberincidentes contenida 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. Este valor significa un aumentó en un 23% con respecto al año anterior, 2022.

Analizando el número de incidentes en función de su tipología, se concluye que los incidentes tipo *Disponibilidad* son los más frecuentes según el registro del pasado año, con un porcentaje del 30%, respecto del total; seguido de los incidentes tipo *Compromiso de la información*, con un porcentaje del 18,89%.

Entre los incidentes más relevantes destacan las campañas de *Denegación Distribuida de Servicio (DDoS)* llevadas a cabo por el actor prorruso **NoName057(16)** con afectación en operadores de servicios esenciales de diferentes sectores estratégicos, motivado por el escenario geopolítico actual.

Entre los incidentes que han generado un mayor impacto en los operadores, se encuentran los ataques tipo ***ransomware***, tipo de *malware* que cifra los documentos ubicados en los sistemas infectados para, posteriormente, solicitar dinero a cambio del descifrado y la no publicación de los datos obtenidos. Con respecto a las familias de *ransomware* con mayor relevancia y efectos en el año 2023, significar los siguientes:

Babuk: esta familia entra dentro de lo que se conoce como *Ransomware-as-a-Service (RaaS)*, donde un actor malicioso desarrolla un *ransomware* y lo ofrece como servicio con el fin de que otros actores lo utilicen para infectar a las víctimas, consiguiendo de esta forma un porcentaje de los pagos recibidos por los rescates. Frecuentemente, tras proceder a la exfiltración y cifrado de los datos, los atacantes solicitan un rescate ofreciendo su descifrado, amenazando además con la publicación de los datos filtrados.

CryptoMix: virus criptográfico que cifra los archivos almacenados en los sistemas infectados. Durante el cifrado, este virus secuestrador de equipos añade al nombre de cada archivo cifrado una extensión determinada. El propósito del programa es deshabilitar numerosas herramientas de seguridad que se ejecutan en el equipo para que pueda cifrar de manera efectiva los datos de la víctima.

Por otro lado, con respecto a los incidentes relativos al **fraude**; significar que, durante el año 2023 han continuado proliferando campañas de suplantación de la identidad de clientes o proveedores, mediante vía telefónica y correo electrónico, con un total de CATORCE (14) incidentes entre todos los ámbitos del sector público y 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 por Sector Estratégico con afectación en operadores críticos de nivel alto, muy alto o crítico

Entre los incidentes gestionados con afectación en operadores de servicios esenciales, **con niveles de peligrosidad o impacto alto, muy alto o crítico**, los sectores donde se han detectado un mayor número de incidentes han sido el sector **Transporte**, con un 27,78%, seguido del sector **TIC** y del sector **Tributario y Financiero**, con porcentajes del 23,33% y 21,11%, respectivamente.

>> 2.3. Incidentes remitidos a ENISA como autoridad española NIS

A lo largo del año 2023, se han comunicado **TREINTA (30) incidentes de ciberseguridad** a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) a través del Punto de Contacto Nacional (DSN), en base al artículo 27 del Real Decreto-ley 12/2018, aumentando en un 30,43% con respecto al año anterior.

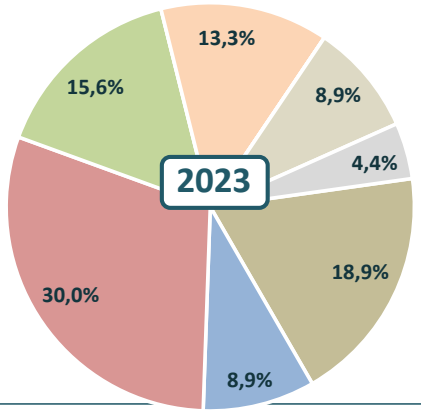
Con respecto a los tipos de incidentes con mayor relevancia se encuentran los relacionados con *Disponibilidad*, con un 50%, seguido por *Intrusión*, *Fraude* y *Contenido dañino* con un 16,7%, 13,3% y 10%, respectivamente.

2.- INCIDENTES DE CIBERSEGURIDAD (OCC)

>> 3.1. Incidentes gestionados de Operadores Críticos

Tipo de incidente	INCIDENTES GESTIONADOS			
	2020	2021	2022	2023
Compromiso de la información	8	18	27	17
Contenido dañino	41	27	14	8
Disponibilidad	5	5	5	27
Fraude	31	20	16	14
Intento de intrusión	3	1	1	0
Intrusión	1	8	7	12
Contenido abusivo	0	0	0	0
Obtención de información	1	0	0	0
Vulnerabilidad	23	4	1	8
Otros	1	2	2	4

Porcentaje del total de incidentes gestionados

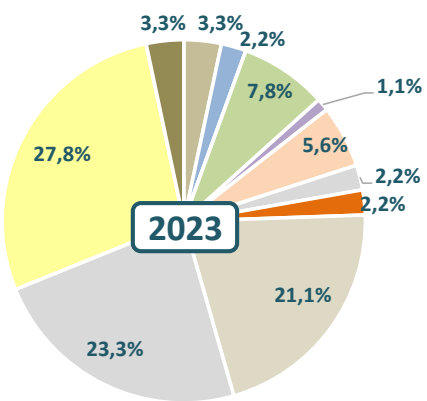


*Véase metadatos explicativos

>> 2.2. Incidentes gestionados por Sector Estratégico

Sector Estratégico	INCIDENTES GESTIONADOS			
	2020	2021	2022	2023
Administración	3	6	2	3
Agua	2	1	1	2
Alimentación	12	0	0	0
Energía	16	4	13	7
Espacio	1	0	0	1
Industria nuclear	21	4	1	5
Industria química	11	11	8	2
Salud	4	0	2	2
Sistema tributario y financiero	21	17	13	19
Tecnologías Informac. y Comunicac. (TIC)	12	18	11	21
Transporte	9	19	16	25
Instalaciones de investigación	0	0	0	0
Varios sectores afectados	2	5	6	3

Porcentaje del total de incidentes gestionados



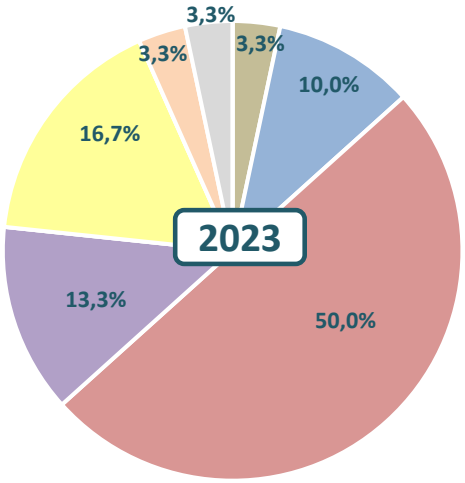
*Véase metadatos explicativos

2.- INCIDENTES DE CIBERSEGURIDAD (OCC)

>> 2.3. Incidentes remitidos a ENISA como autoridad española NIS

Tipo de incidente	INCIDENTES GESTIONADOS			
	2020	2021	2022	2023
Compromiso de la información	1	3	6	1
Contenido dañino	8	11	3	3
Disponibilidad	3	3	4	15
Fraude	5	2	0	4
Intento de intrusión	0	0	1	0
Intrusión	0	5	6	5
Contenido abusivo	0	0	0	0
Obtención de información	0	0	3	1
Vulnerabilidad	0	0	0	1
Otros	1	0	0	0

Porcentaje del total de incidentes gestionados



2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD >>

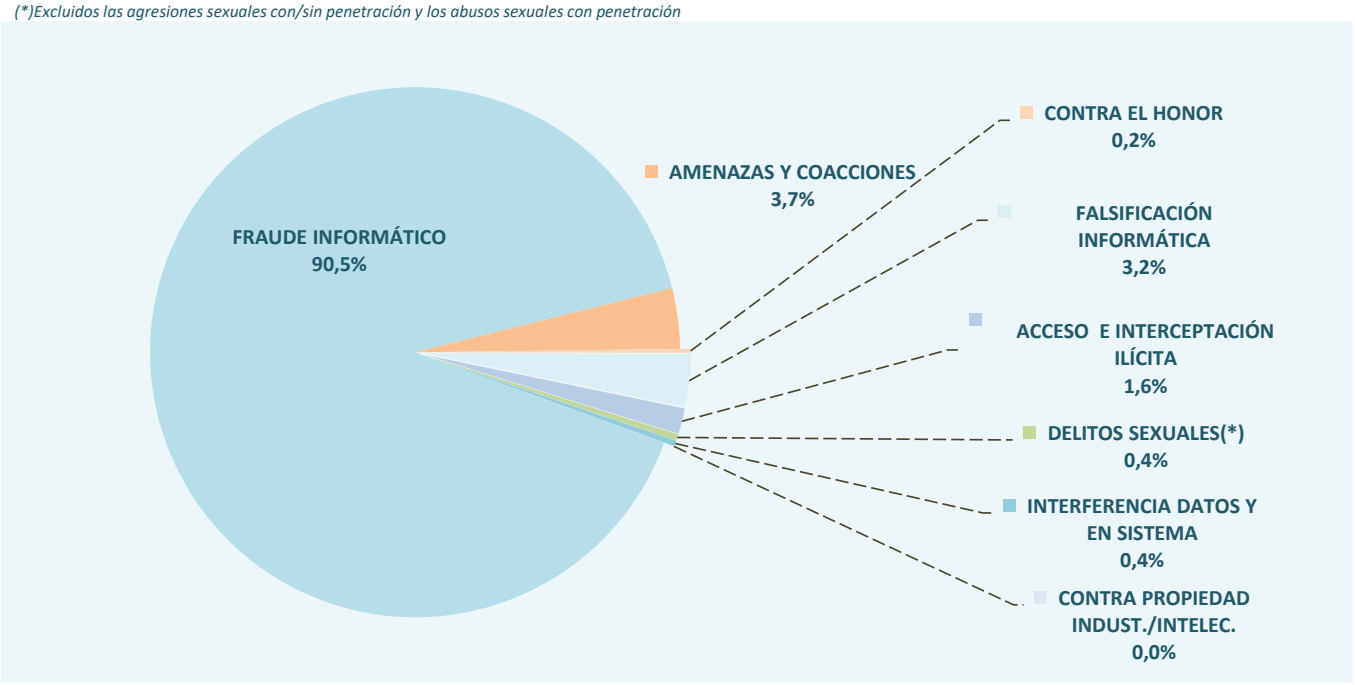
3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2019	2020	2021	2022	2023
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174
CONTRA PROPIEDAD INDUST./INTELEC.	197	125	137	114	64
DELITOS SEXUALES(*)	1.774	1.783	1.628	1.646	1.804
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448
INTERFERENCIA DATOS Y EN SISTEMA	1.473	1.590	2.138	1.662	1.659
Total HECHOS CONOCIDOS	**218.302**	**287.963**	**305.477**	**374.737**	**472.125**

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



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

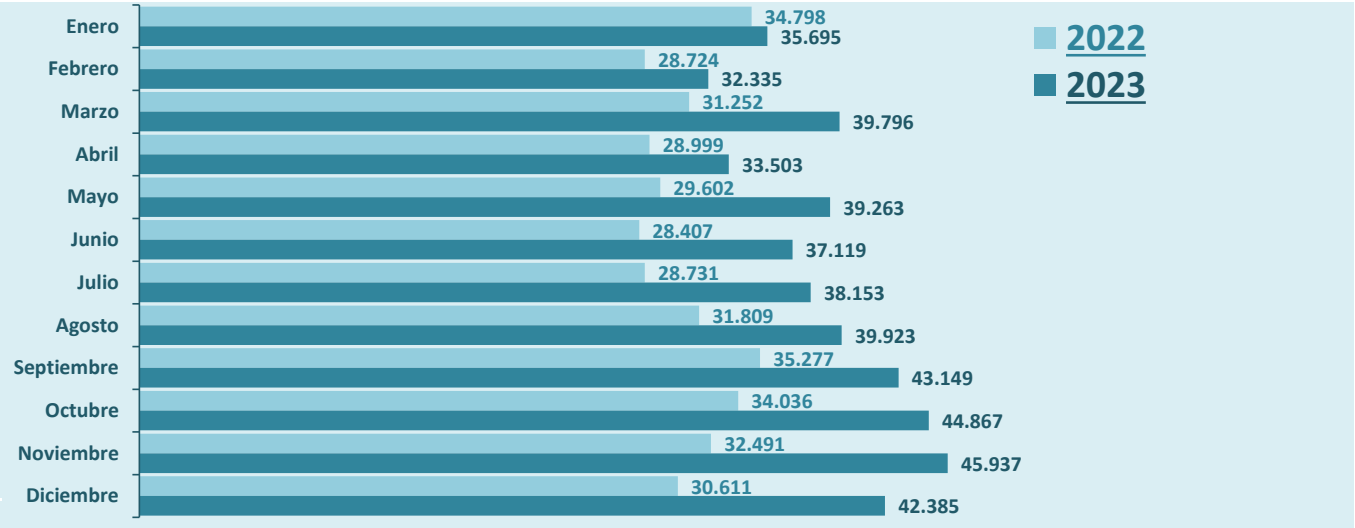
3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

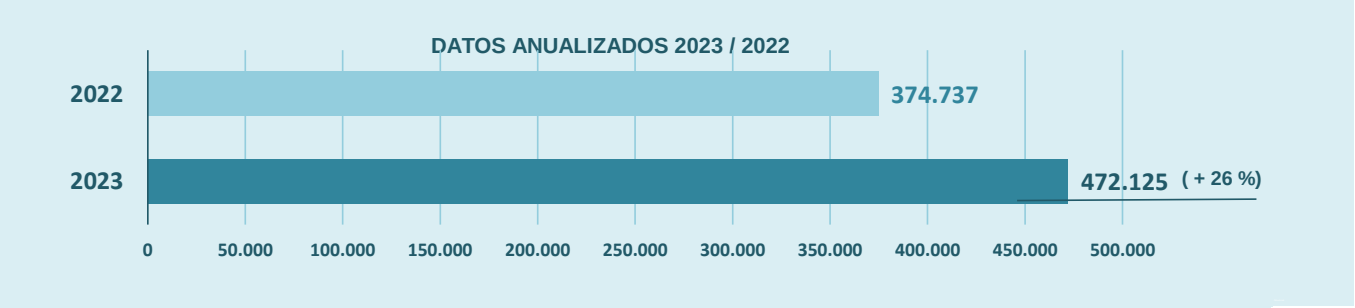
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.3. Distribución mensual de hechos conocidos. Año 2023

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	558	544	655	445	607	587	550	557	684	682	900	598	**7.367**
AMENAZAS Y COACCIONES	1.357	1.292	1.556	1.278	1.551	1.474	1.416	1.577	1.559	1.452	1.619	1.341	**17.472**
CONTRA EL HONOR	76	108	103	81	159	108	82	90	90	100	89	88	**1.174**
CONTRA PROPIEDAD INDUST./INTELEC.	4	7	3	6	3	6	3	3	3	6	3	17	**64**
DELITOS SEXUALES	141	145	174	115	145	187	125	171	121	139	209	132	**1.804**
FALSIFICACIÓN INFORMÁTICA	1.178	1.507	1.555	1.059	1.203	1.380	934	996	1.228	1.353	1.610	1.134	**15.137**
FRAUDE INFORMÁTICO	32.274	28.614	35.594	30.400	35.449	33.250	34.918	36.412	39.326	40.983	41.296	38.932	**427.448**
INTERFERENCIA DATOS Y EN SISTEMA	107	118	156	119	146	127	125	117	138	152	211	143	**1.659**
Total HECHOS CONOCIDOS	**35.695**	**32.335**	**39.796**	**33.503**	**39.263**	**37.119**	**38.153**	**39.923**	**43.149**	**44.867**	**45.937**	**42.385**	**472.125**

>> 3.4. Comparativa de la distribución mensual de hechos conocidos 2023 / 2022





3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

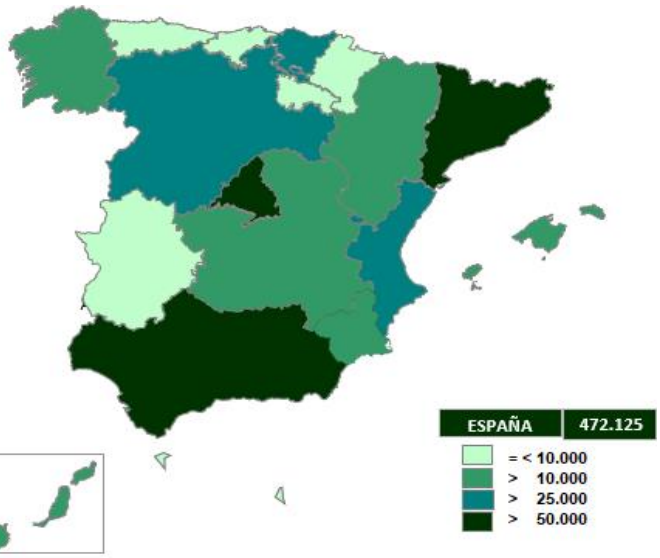
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2023

Hechos denunciados de CIBERCRIMINALIDAD - 2023

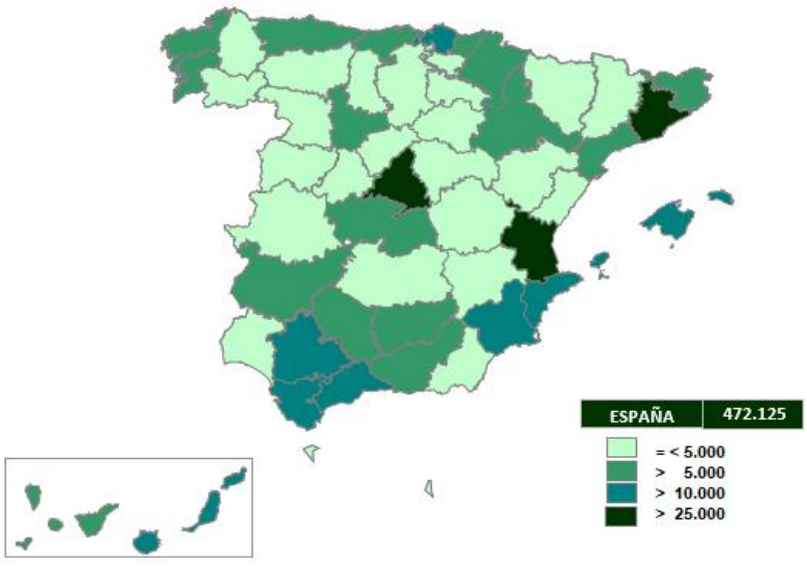
Hechos conocidos:	472.125
Esclarecimiento (*):	60.197 **13,5%**
Detenciones/invest:	17.173

CCAA	Hechos
ANDALUCÍA	81.315
MADRID (COMUNIDAD DE)	78.877
CATALUÑA	76.126
COMUNITAT VALENCIANA	47.056
PAÍS VASCO	27.899
CASTILLA Y LEÓN	25.540
GALICIA	21.730
CASTILLA - LA MANCHA	19.454
CANARIAS	17.668
MURCIA (REGIÓN DE)	13.747
ARAGÓN	12.184
BALEARS (ILLES)	11.482
EXTREMADURA	8.817
ASTURIAS (PRINCIPADO DE)	8.647
NAVARRA (COMUNIDAD FORAL DE)	7.474
CANTABRIA	5.968
EN EL EXTRANJERO	4.704
RIOJA (LA)	2.364
CIUDAD AUTÓNOMA DE CEUTA	592
CIUDAD AUTÓNOMA DE MELILLA	481



(*) Debido a que la Ertzaintza no facilita datos de esclarecidos el % de esclarecimiento se ha calculado sin tener en cuenta los hechos conocidos por este cuerpo policial

Hechos denunciados de CIBERCRIMINALIDAD - 2023



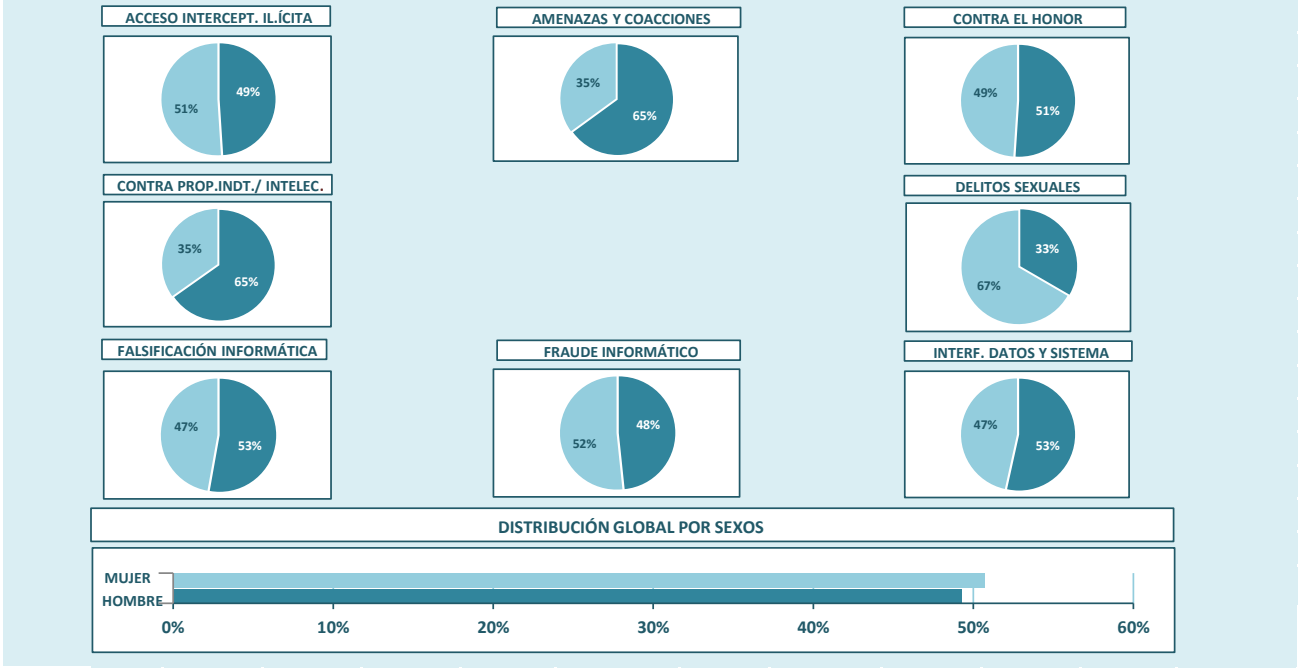
Provincias más afectadas:	Hechos
Madrid	78.877
Barcelona	54.898
Valencia/València	25.191
Sevilla	18.959
Málaga	17.988
Alicante/Alacant	17.907
Bizkaia	14.488
Murcia	13.747
Cádiz	12.869
Balears (Illes)	11.482
Palmas (Las)	10.342
Granada	9.935
Coruña (A)	8.904
Zaragoza	8.782
Gipuzkoa	8.760
Girona	8.671
Asturias	8.647
Pontevedra	8.525
Tarragona	7.824
Córdoba	7.670

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

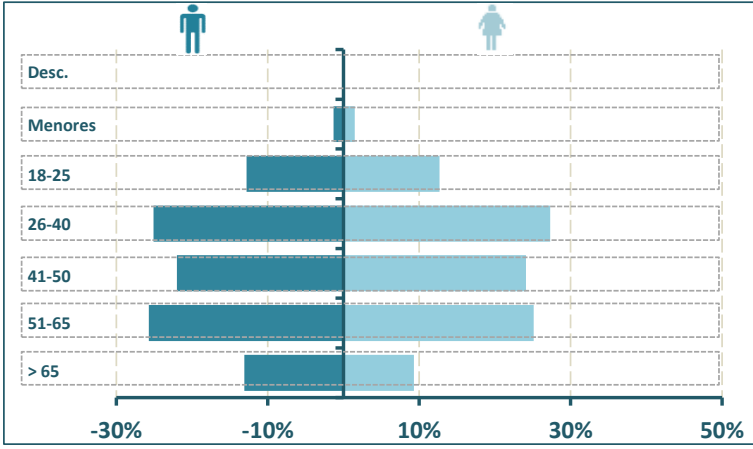
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.6. Victimizaciones registradas según grupo penal y sexo. Año 2023

VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	3.323	3.461	2	6.786
AMENAZAS Y COACCIONES	11.493	6.198	16	17.707
CONTRA EL HONOR	614	589	2	1.205
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	15	8	0	23
DELITOS SEXUALES	409	817	5	1.231
FALSIFICACIÓN INFORMÁTICA	6.150	5.496	18	11.664
FRAUDE INFORMÁTICO	151.988	162.460	91	314.539
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	778	677	0	1.455
Total VICTIMIZACIONES	**174.770**	**179.706**	**134**	**354.610**



>> 3.7. Victimizaciones según grupo de edad y sexo. Año 2023



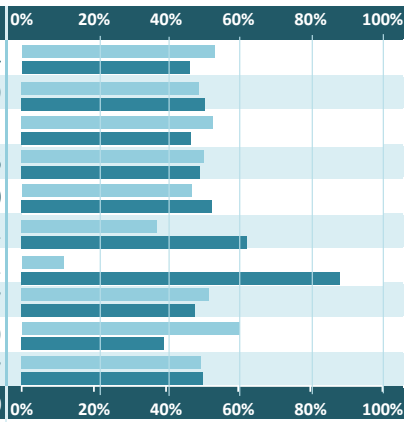
Grupo de edad	Hombre	Mujer	Descon.
Edad desconocida	159	160	20
Menores de edad	2.238	2.651	7
De 18 a 25 años	22.286	22.841	3
De 26 a 40 años	43.843	48.973	14
De 41 a 50 años	38.428	43.382	30
De 51 a 65 años	44.921	45.049	40
Mayores 65 años	22.895	16.650	20
TOTAL	**174.770**	**179.706**	**134**

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

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

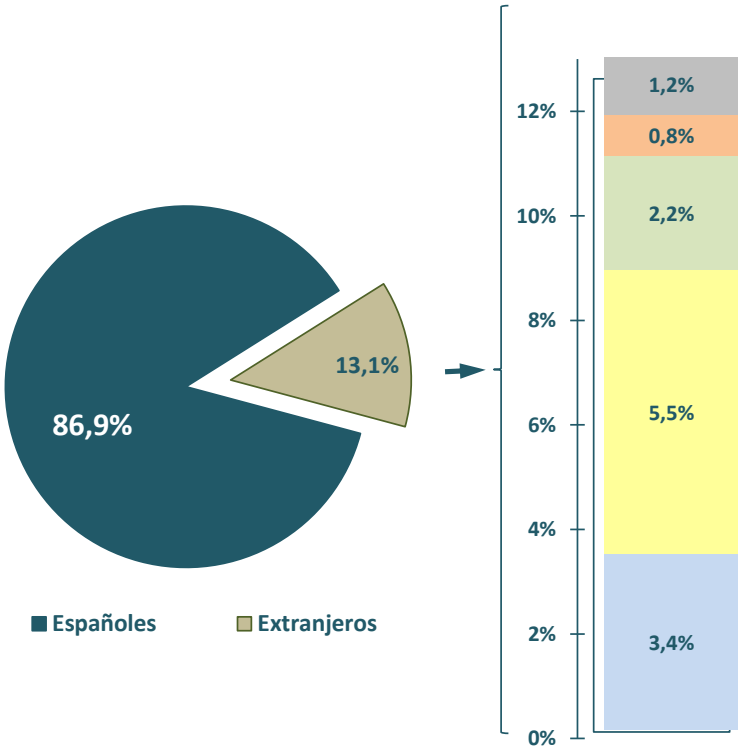
>> 3.8. Victimizaciones por tipología penal y sexo. Año 2023

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS TARJ CRÉD, DÉBITO Y CHEQUES VIAJE	66.495	76.391	38	142.924
OTRAS ESTAFAS	55.963	54.089	37	110.089
ESTAFA BANCARIA	18.814	21.251	0	40.065
ESTAFAS INFORMÁTICAS	10.349	10.561	16	20.926
USURPACIÓN DE ESTADO CIVIL	5.816	5.198	16	11.030
AMENAZAS	6.598	3.963	10	10.571
EXTORSIÓN	3.490	460	2	3.952
ACCESO ILEGAL SISTEMAS INFORMÁTICOS	1.232	1.335	0	2.567
DESCUBRIMIENTO/REVELACIÓN SECRETOS	924	1.413	2	2.339
RESTO	5.089	5.045	13	10.147
Total VICTIMIZACIONES	**174.770**	**179.706**	**134**	**354.610**



>> 3.9. Nacionalidad de la víctima. Año 2023

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	**308.041**	**86,9%**
2.- EXTRANJEROS	**46.569**	**13,1%**
2.1.- UNIÓN EUROPEA	**12.013**	**3,4%**
RUMANÍA	3.443	1,0%
ITALIA	2.627	0,7%
FRANCIA	1.164	0,3%
BULGARIA	897	0,3%
ALEMANIA	886	0,2%
Resto	2.996	0,8%
2.2.- AMÉRICA	**19.433**	**5,5%**
COLOMBIA	3.600	1,0%
VENEZUELA	2.755	0,8%
ECUADOR	1.815	0,5%
Resto	11.263	3,2%
2.3.- ÁFRICA	**7.914**	**2,2%**
MARRUECOS	4.656	1,3%
SENEGAL	839	0,2%
Resto	2.419	0,7%
2.4.- ASIA	**2.860**	**0,8%**
CHINA POPULAR	934	0,3%
PAQUISTÁN	611	0,2%
Resto	1.315	0,4%
2.5.- RESTO PAÍSES	**4.349**	**1,2%**
UCRANIA	1.074	0,3%
REINO UNIDO	778	0,2%
Otros	2.497	0,7%
TOTAL	**354.610**	**100%**

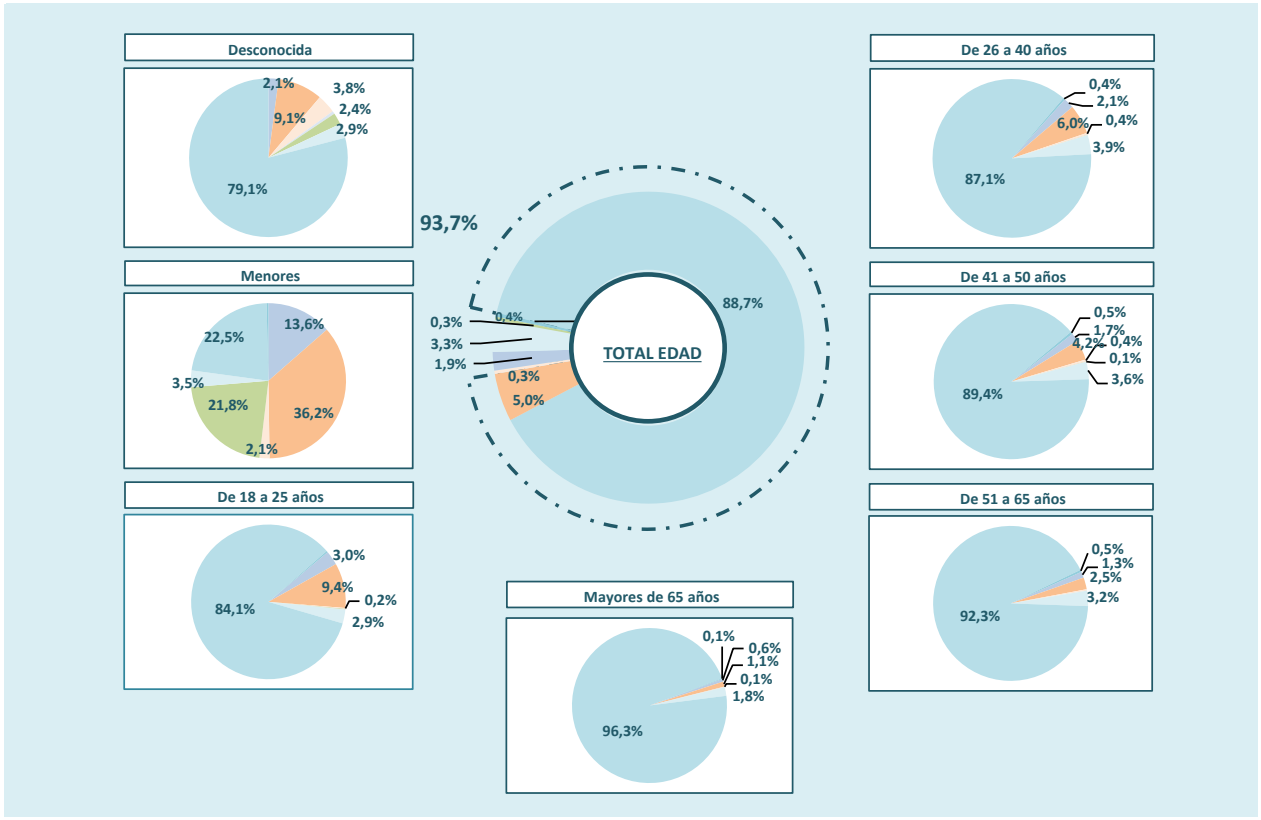


3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

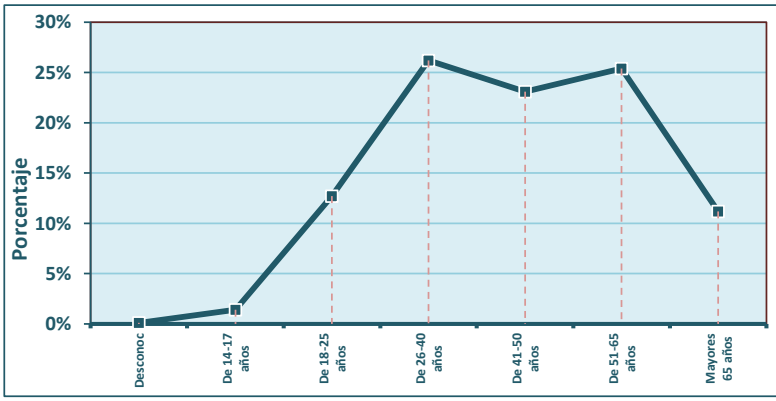
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.10. Victimizaciones registradas según grupo penal y edad. Año 2023

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	7	664	1.347	1.969	1.428	1.145	226
AMENAZAS Y COACCIONES	31	1.773	4.240	5.582	3.450	2.212	419
CONTRA EL HONOR	13	102	85	365	340	258	42
CONTRA PROPIEDAD INDUST./INTELEC.	2	0	3	5	5	7	1
DELITOS SEXUALES	8	1.068	55	40	44	13	3
FALSIFICACIÓN INFORMÁTICA	10	170	1.312	3.625	2.968	2.865	714
FRAUDE INFORMÁTICO	268	1.100	37.949	80.852	73.175	83.094	38.101
INTERFERENCIA EN DATOS Y EN SISTEMA	0	19	139	392	430	416	59
Total VICTIMIZACIONES	**339**	**4.896**	**45.130**	**92.830**	**81.840**	**90.010**	**39.565**



>> 3.11. Edad de la víctima. Año 2023



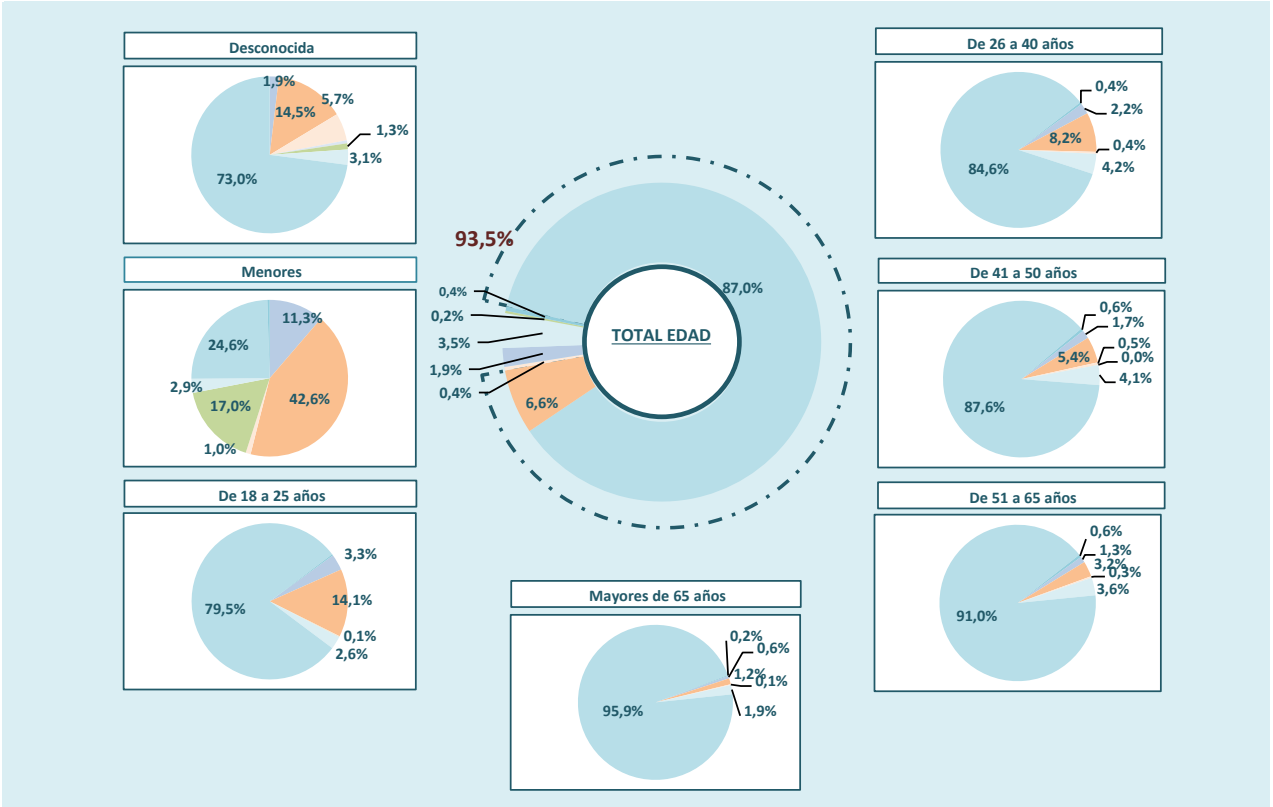
Grupo de edad	Víctimas
Edad desconocida	339
Menores de edad	4.896
De 18 a 25 años	45.130
De 26 a 40 años	92.830
De 41 a 50 años	81.840
De 51 a 65 años	90.010
Mayores 65 años	39.565
TOTAL	**354.610**

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

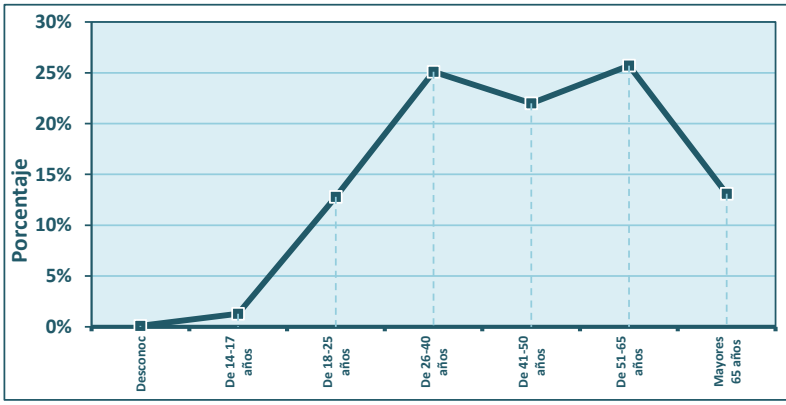
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.12. Victimizaciones registradas según grupo penal y edad. Año 2023

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	253	741	971	667	562	126
AMENAZAS Y COACCIONES	23	954	3.134	3.588	2.072	1.437	285
CONTRA EL HONOR	9	23	31	179	195	143	34
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	3	3	5	1
DELITOS SEXUALES	2	381	12	3	8	3	0
FALSIFICACIÓN INFORMÁTICA	5	65	588	1.823	1.585	1.639	445
FRAUDE INFORMÁTICO	116	551	17.716	37.081	33.677	40.884	21.963
INTERFERENCIA EN DATOS Y EN SISTEMA	0	11	62	195	221	248	41
Total VICTIMIZACIONES	**159**	**2.238**	**22.286**	**43.843**	**38.428**	**44.921**	**22.895**



>> 3.13. Edad de la víctima. Año 2023



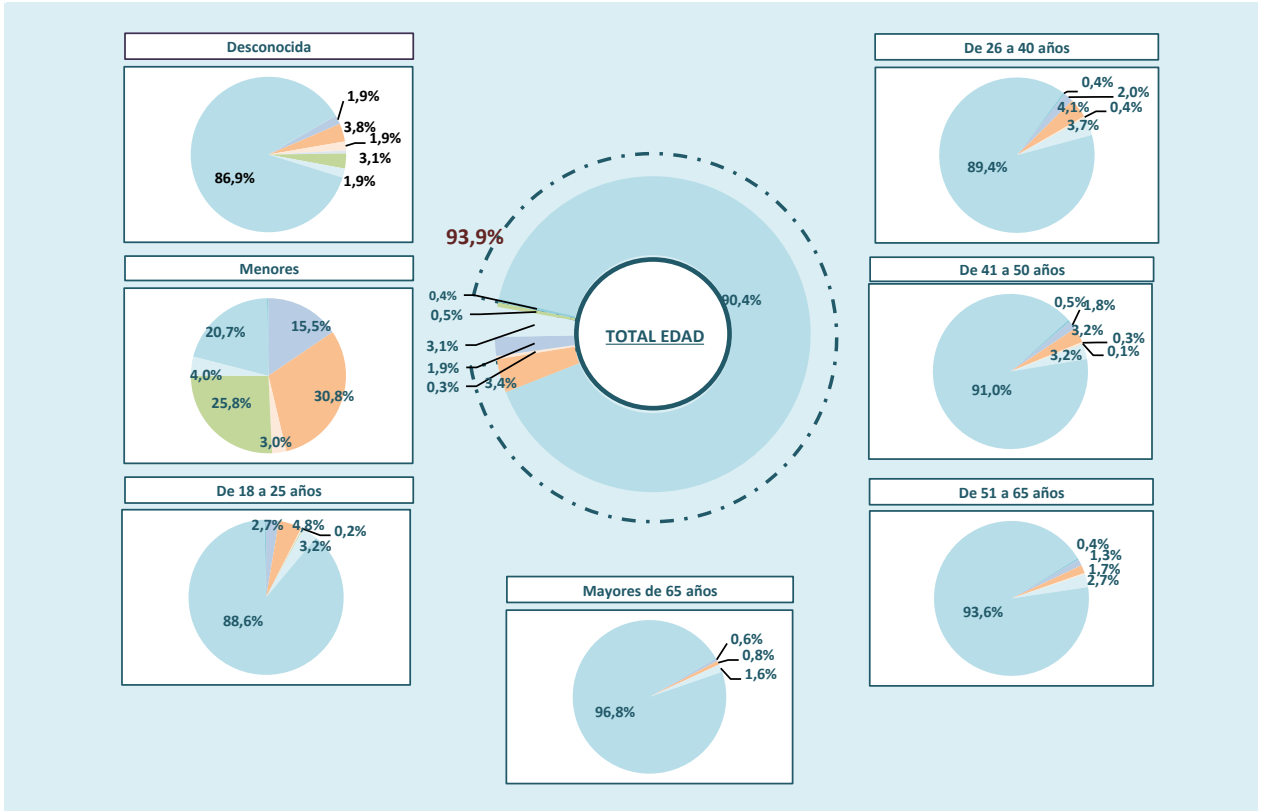
Grupo de edad	Víctimas
Edad desconocida	159
Menores de edad	2.238
De 18 a 25 años	22.286
De 26 a 40 años	43.843
De 41 a 50 años	38.428
De 51 a 65 años	44.921
Mayores 65 años	22.895
TOTAL	**174.770**

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

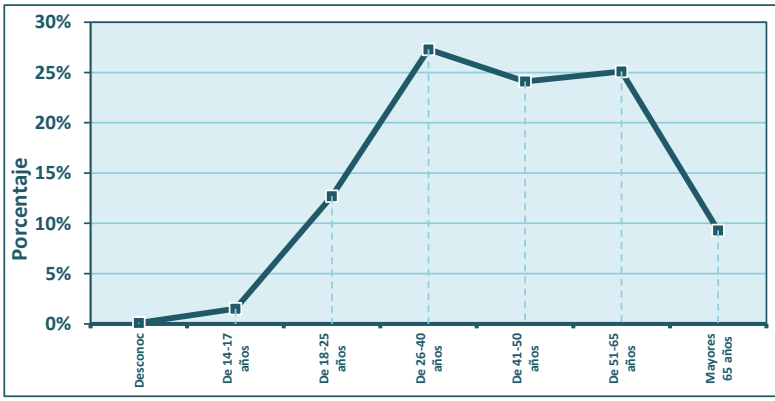
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.14. Victimizaciones registradas según grupo penal y edad. Año 2023

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	411	606	997	761	583	100
AMENAZAS Y COACCIONES	6	816	1.106	1.993	1.373	772	132
CONTRA EL HONOR	3	79	54	186	145	114	8
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	2	2	2	0
DELITOS SEXUALES	5	683	43	37	36	10	3
FALSIFICACIÓN INFORMÁTICA	3	105	724	1.801	1.377	1.219	267
FRAUDE INFORMÁTICO	139	549	20.230	43.760	39.479	42.181	16.122
INTERFERENCIA EN DATOS Y EN SISTEMA	0	8	77	197	209	168	18
Total VICTIMIZACIONES	**160**	**2.651**	**22.841**	**48.973**	**43.382**	**45.049**	**16.650**



>> 3.15. Edad de la víctima. Año 2023



Grupo de edad	Víctimas
Edad desconocida	160
Menores de edad	2.651
De 18 a 25 años	22.841
De 26 a 40 años	48.973
De 41 a 50 años	43.382
De 51 a 65 años	45.049
Mayores 65 años	16.650
TOTAL	**179.706**

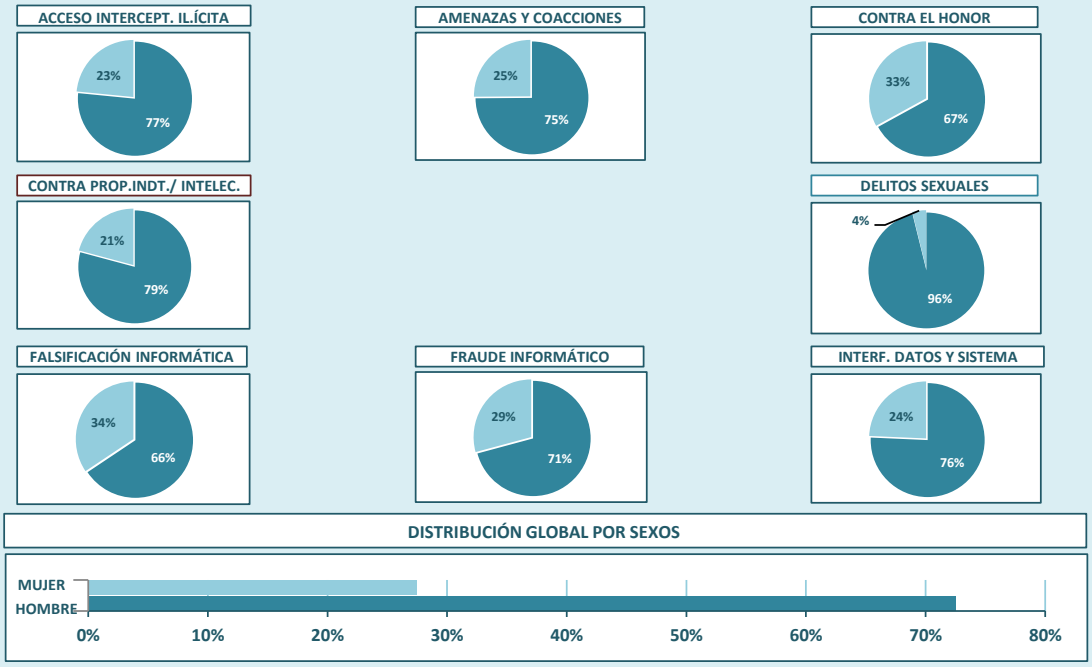
3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

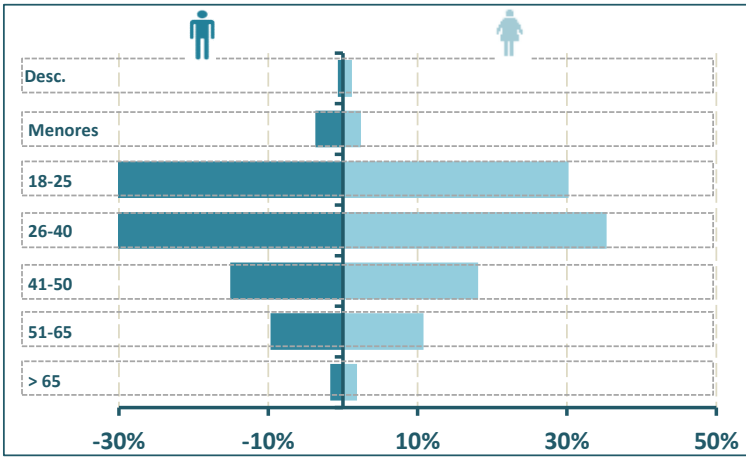
>> 3.16. Detenciones/investigados registrados según grupo penal y sexo. Año 2023

DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	356	109	465
AMENAZAS Y COACCIONES	1.685	565	2.250
CONTRA EL HONOR	65	32	97
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	19	5	24
DELITOS SEXUALES	775	31	806
FALSIFICACIÓN INFORMÁTICA	420	220	640
FRAUDE INFORMÁTICO	9.052	3.732	12.784
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	81	26	107
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**12.453**	**4.720**	**17.173**

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



>> 3.17. DETENCIONES/INVESTIGADOS según grupo de edad y sexo. Año 2023



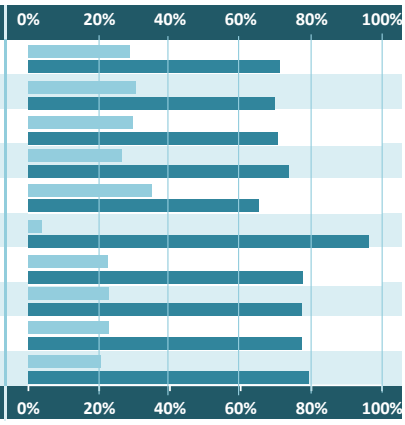
Grupo de edad	Hombre	Mujer
Edad desconocida	87	57
De 14 a 17 años	459	114
De 18 a 25 años	4.512	1.425
De 26 a 40 años	4.093	1.668
De 41 a 50 años	1.882	852
De 51 a 65 años	1.205	512
Mayores 65 años	215	92
TOTAL	**12.453**	**4.720**

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

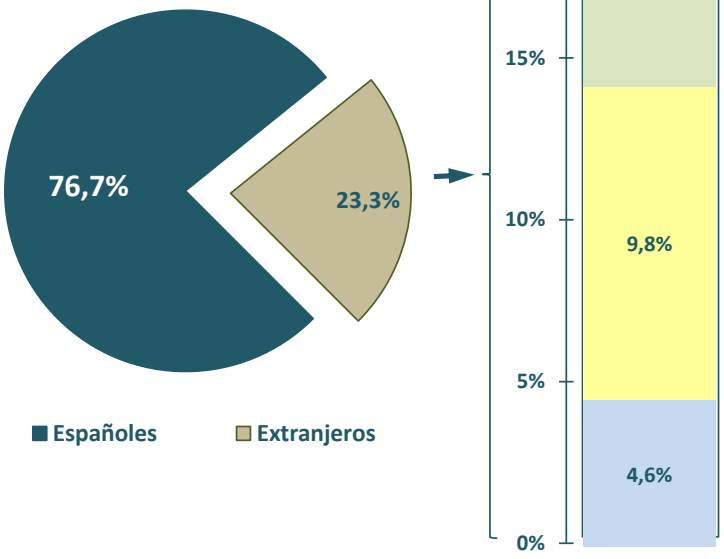
>> 3.18. Detenciones/investigados por tipología penal y sexo. Año 2023

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	5.721	2.316	8.037
ESTAFAS TARJETA CRÉD, DÉBITO Y CHEQUES VIAJE	1.881	818	2.699
ESTAFAS INFORMÁTICAS	1.320	553	1.873
AMENAZAS	1.093	391	1.484
USURPACIÓN DE ESTADO CIVIL	360	192	552
PORNOGRAFÍA DE MENORES	500	19	519
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	213	62	275
EXTORSIÓN	190	56	246
COACCIONES	186	55	241
RESTO	989	257	1.246
Total VICTIMIZACIONES CIBERCRIMINALIDAD	**12.453**	**4.720**	**17.173**



>> 3.19. Nacionalidad de los detenciones/investigados. Año 2023

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	**13.175**	**76,7%**
2.- EXTRANJEROS	**3.998**	**23,3%**
2.1.- UNIÓN EUROPEA	**783**	**4,6%**
RUMANÍA	331	1,9%
BULGARIA	90	0,5%
ITALIA	88	0,5%
FRANCIA	53	0,3%
PORTUGAL	51	0,3%
Resto	170	1,0%
2.2.- AMÉRICA	**1.689**	**9,8%**
COLOMBIA	346	2,0%
REP. DOMINICANA	301	1,8%
VENEZUELA	244	1,4%
Resto	798	4,6%
2.3.- ÁFRICA	**1.066**	**6,2%**
MARRUECOS	537	3,1%
NIGERIA	119	0,7%
Resto	410	2,4%
2.4.- ASIA	**141**	**0,8%**
BANGLADESH	38	0,2%
PAQUISTÁN	34	0,2%
Resto	69	0,4%
2.5.- RESTO PAÍSES	**319**	**1,9%**
UCRANIA	98	0,6%
RUSIA	41	0,2%
Otros	180	1,0%
TOTAL	**17.173**	**100%**

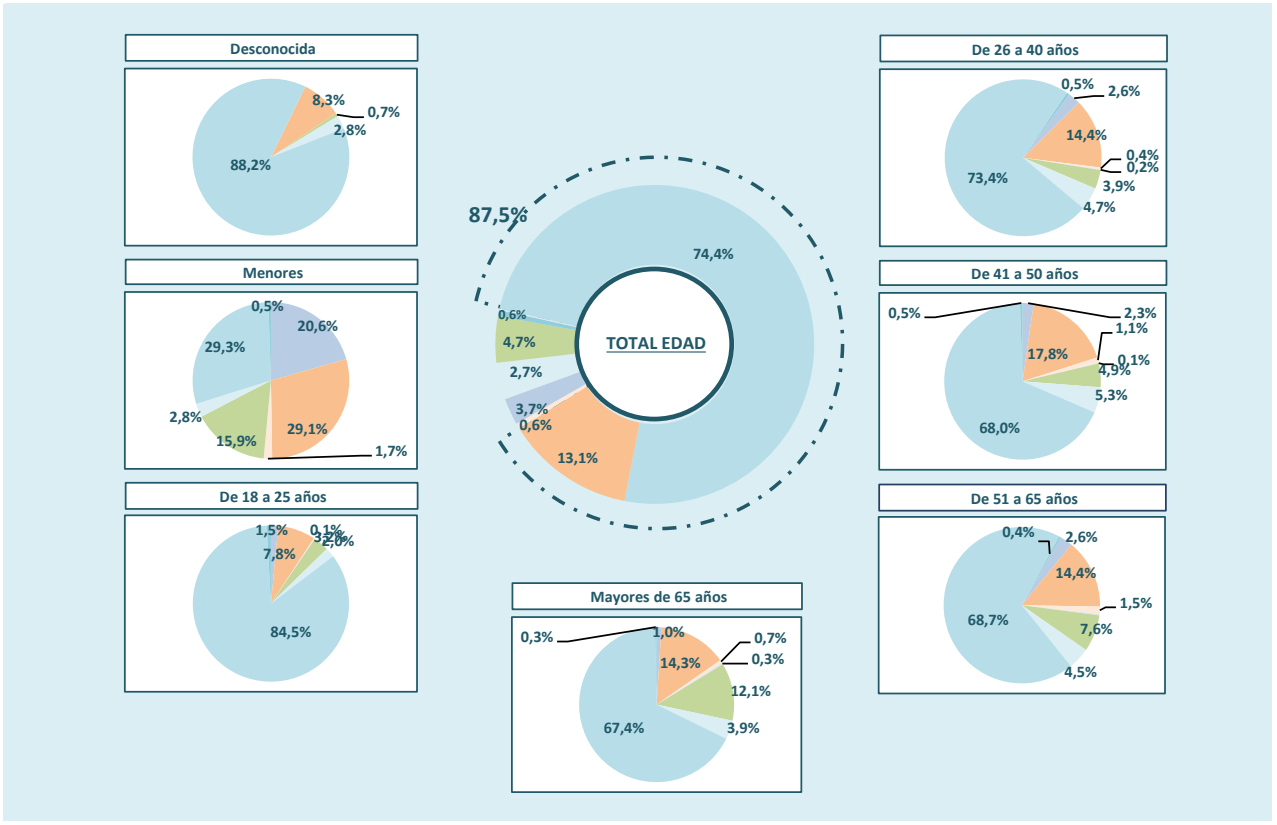


3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

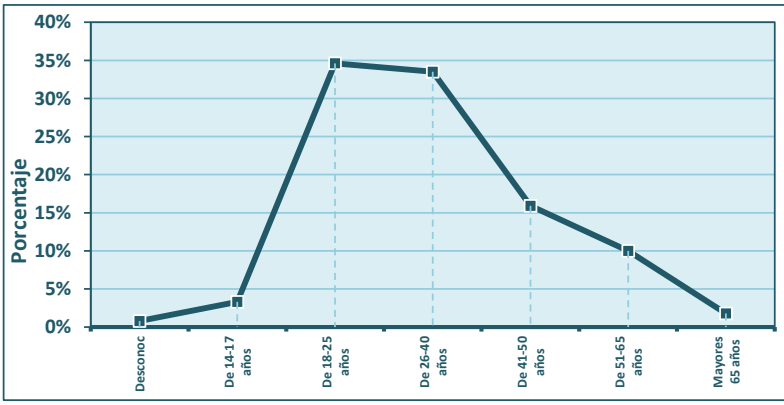
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.20. Detenciones/investigados registradas según grupo penal y edad. Año 2023

	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	0	118	90	148	62	44	3
AMENAZAS Y COACCIONES	12	167	461	832	487	247	44
CONTRA EL HONOR	0	10	7	21	31	26	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	6	9	3	5	1
DELITOS SEXUALES	1	91	188	224	134	131	37
FALSIFICACIÓN INFORMÁTICA	4	16	117	270	144	77	12
FRAUDE INFORMÁTICO	127	168	5017	4226	1.859	1.180	207
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	51	31	14	7	1
Total DETENCIONES/INVESTIGADOS	**144**	**573**	**5.937**	**5.761**	**2.734**	**1.717**	**307**



>> 3.21. Edad de las personas detenidas/investigadas. Año 2023



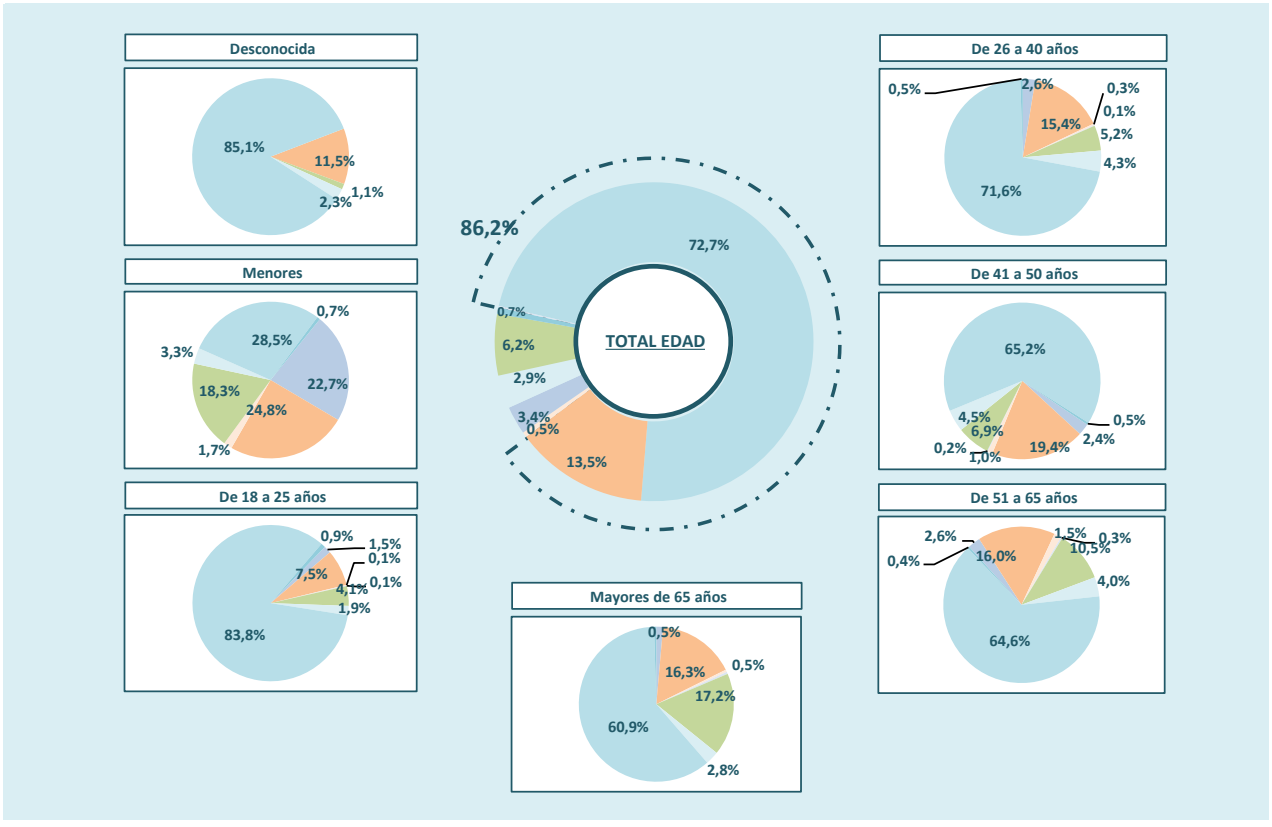
Grupo de edad	Det./Inv.
Edad desconocida	144
De 14 a 17 años	573
De 18 a 25 años	5.937
De 26 a 40 años	5.761
De 41 a 50 años	2.734
De 51 a 65 años	1.717
Mayores 65 años	307
TOTAL	**17.173**

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

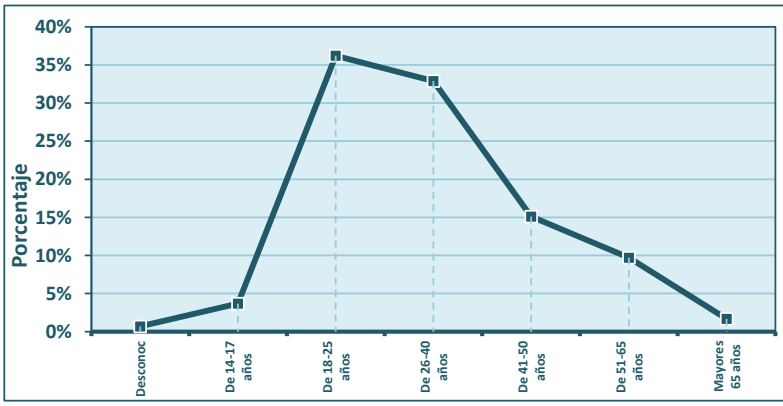
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.22. Detenciones/investigados registradas según grupo penal y edad. Año 2023

	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	0	104	68	105	45	31	3
AMENAZAS Y COACCIONES	10	114	339	629	365	193	35
CONTRA EL HONOR	0	8	6	13	19	18	1
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	5	6	3	4	1
DELITOS SEXUALES	1	84	184	213	129	127	37
FALSIFICACIÓN INFORMÁTICA	2	15	87	177	85	48	6
FRAUDE INFORMÁTICO	74	131	3.781	2.929	1.227	779	131
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	42	21	9	5	1
Total DETENCIONES/INVESTIGADOS	**87**	**459**	**4.512**	**4.093**	**1.882**	**1.205**	**215**



>> 3.23. Edad de las personas detenidas/investigadas. Año 2023



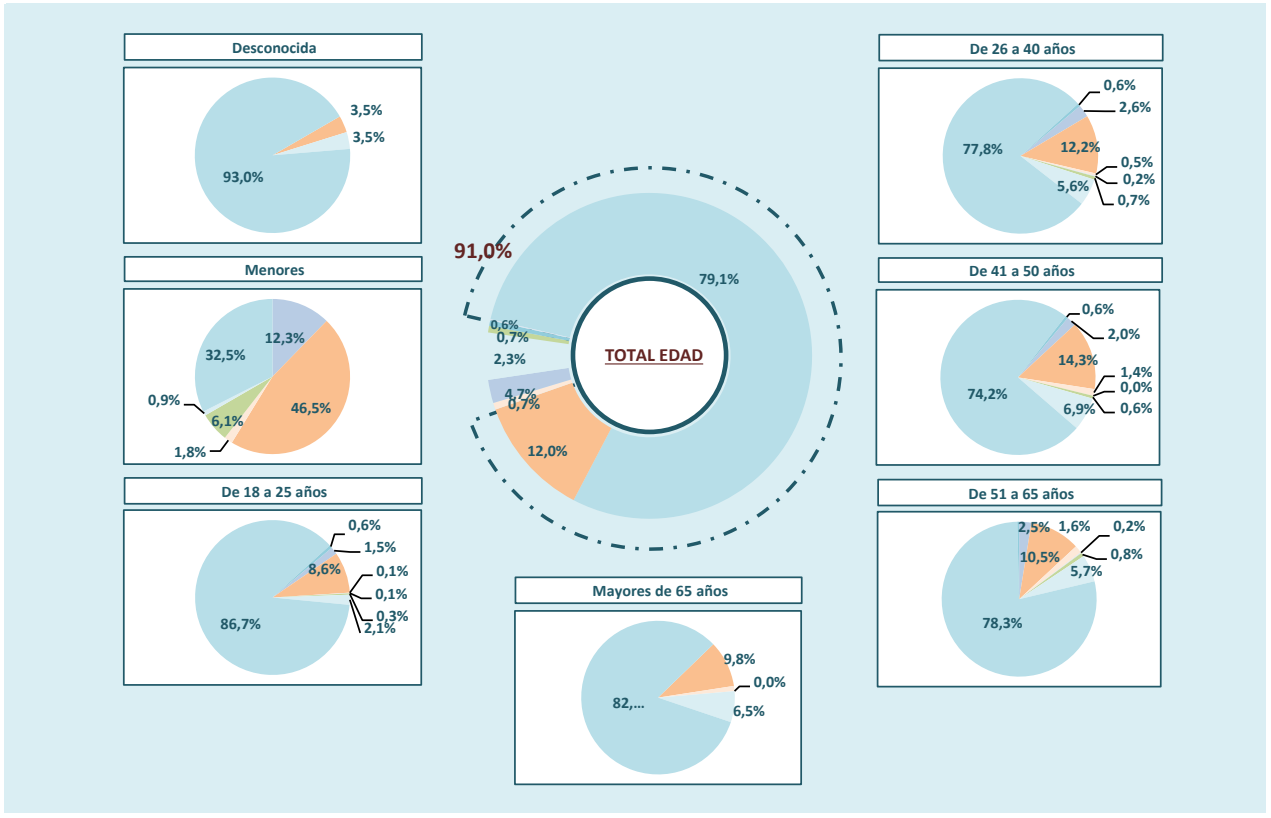
Grupo de edad	Det./Inv.
Edad desconocida	87
De 14 a 17 años	459
De 18 a 25 años	4.512
De 26 a 40 años	4.093
De 41 a 50 años	1.882
De 51 a 65 años	1.205
Mayores 65 años	215
TOTAL	**12.453**

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

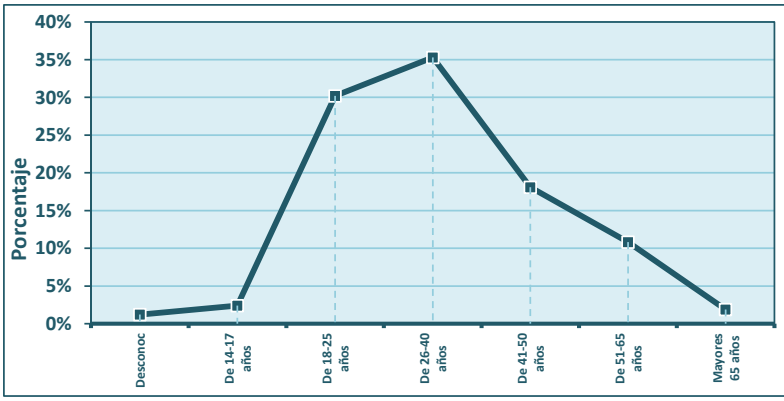
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.24. Detenciones/investigados registradas según grupo penal y edad. Año 2023

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	14	22	43	17	13	0
AMENAZAS Y COACCIONES	2	53	122	203	122	54	9
CONTRA EL HONOR	0	2	1	8	12	8	1
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	1	3	0	1	0
DELITOS SEXUALES	0	7	4	11	5	4	0
FALSIFICACIÓN INFORMÁTICA	2	1	30	93	59	29	6
FRAUDE INFORMÁTICO	53	37	1.236	1.297	632	401	76
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	9	10	5	2	0
Total DETENCIONES/INVESTIGADOS	**57**	**114**	**1.425**	**1.668**	**852**	**512**	**92**



>> 3.25. Edad de las personas detenidas/investigadas. Año 2023



Grupo de edad	Det./Inv.
Edad desconocida	57
De 14 a 17 años	114
De 18 a 25 años	1.425
De 26 a 40 años	1.668
De 41 a 50 años	852
De 51 a 65 años	512
Mayores 65 años	92
TOTAL	**4.720**

2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4 METADATA >>

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 Budapest[1]. 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

- 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 que han sido conocidas por las distintas Fuerzas y Cuerpos de Seguridad, bien por medio de denuncia interpuesta o por actuación policial realizada motu propio (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

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).

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SES	VARIABLES SEC A UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/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
Interferencia en los datos y en el sistema	Arts. 263 a 267 Daños y daños informáticos	DAÑOS	Ámbito cibercrimen
		FACILITACIÓN DE DISPOSITIVOS, PROGRAMAS O CLAVES PARA COMETER ATAQUES INFORMATICOS	Ninguna
		ATAQUES A DATOS O PROGRAMAS INFORMÁTICOS	Ninguna
		ATAQUES A SISTEMAS INFORMÁTICOS	Ninguna
Falsificación informática	Arts. 386 al 403	FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS	Ámbito cibercrimen
		FALSIFICACIÓN/TRÁFICO TARJETAS CRÉDITO Y DÉBITO/CHEQUES VIAJE	
		FALSIFICACIÓN/TRÁFICO DE DNI/PASAPORTE	
		OTRAS FALSIFICACIONES DOCUMENTOS	
		FABRICACIÓN/TENENCIA DE ÚTILES PARA FALSIFICAR	
		USURPACIÓN DE ESTADO CIVIL	
		USURPACIÓN DE FUNCIONES PÚBLICAS	
		INTRUSISMO	
Fraude Informático	Arts. CP 248 a 251	ESTAFA BANCARIA (hasta 2021)	Ámbito cibercrimen
		ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE VIAJE (248.2.c CP)	
		OTRAS ESTAFAS	
		ESTAFA DE INVERSORES	
		ESTAFAS INFORMÁTICAS (arts. 248.2.a.b CP)	Ninguna
Delitos sexuales	Arts. CP 178 a 189	AGRESIÓN SEXUAL	Ámbito cibercrimen
		AGRESIÓN SEXUAL CON PENETRACIÓN	
		ABUSO SEXUAL (hasta 07/10/2022)	
		ABUSO SEXUAL CON PENETRACIÓN (hasta 07/10/2022)	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 16 AÑOS CON FINES SEXUALES (GROOMING)	(sin ámbito)
		LA DISTRIBUCIÓN/DIFUSIÓN PÚBLICA POR NUEVAS NNTT EN LA PROMOCIÓN DELITOS CONTRA LA PROSTITUCIÓN Y LIBERTAD SEXUAL DE MENORES (art. 189bis)	
		ACOSO SEXUAL	Ámbito cibercrimen
		EXHIBICIONISMO	
		PROVOCACIÓN SEXUAL	
		CORRUPCIÓN DE MENORES/CON DISCAPACIDAD/DIVERSIDAD FUNCIONAL	
		DELITOS RELATIVOS A LA PROSTITUCIÓN	
		PORNOGRAFÍA DE MENORES	
Contra la propiedad industrial/intelectual	Arts 270 a 277 del CP(Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Ámbito cibercrimen
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	
		ACCESO FRAUDULENTO A SERVICIOS DE RADIODIFUSIÓN/TV/OTROS	
		DELITO DE ESPIONAJE INDUSTRIAL Y SECRETO PROFESIONAL (ARTS. 278 A 280 CP)	
Contra el honor	Arts. 205 a 210 del Código Penal	CALUMNIAS	Ámbito cibercrimen
		INJURIAS	
		INJURIAS Y CALUMNIAS A FUNCIONARIO PÚBLICO, AUTORIDAD O AGENTE DE LA AUTORIDAD (ARTS. 205 Y 215 CP)	
Amenazas y coacciones	Arts 169 a 173 del C.Penal	AMENAZAS	Ámbito cibercrimen
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	
		COACCIONES	
		EXTORSIÓN	
		TRATO DEGRADANTE	
		ACOSO LABORAL Y FUNCIONARIAL	
		ACOSO CONTRA LA LIBERTAD DE LAS PERSONAS	
		PERFILES FALSOS CON FINES ACOSO/HOSTIGAMIENTO/HUMILLACIÓN	

ESPAÑA

2023

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

seC Sistema Estadístico de Criminalidad

Síguenos en Twitter
@interiorgob
www.interior.gob.es

2023