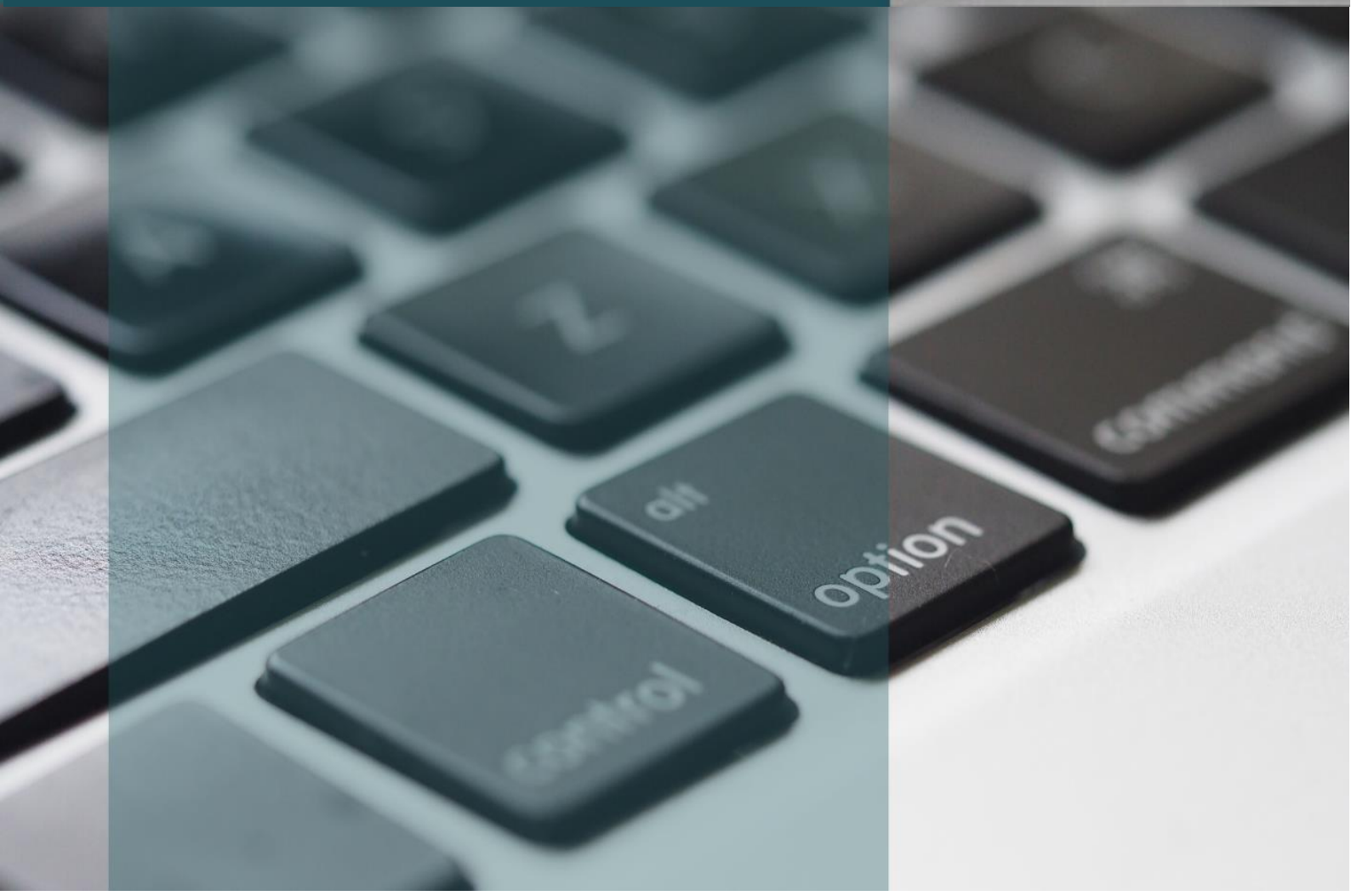
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS

Sistema Estadístico de Criminalidad

2021

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Dirección General de Coordinación y Estudios

Secretaría de Estado de Seguridad

AUTORES / AUTORAS

JAVIER LÓPEZ GUTIÉRREZ

FRANCISCO SÁNCHEZ JIMÉNEZ

DAVID HERRERA SÁNCHEZ

FRANCISCO MARTÍNEZ MORENO

MARCOS RUBIO GARCÍA

Mª. VICTORIA GIL PÉREZ

ANA Mª. SANTIAGO OROZCO

MIGUEL A. GÓMEZ MARTÍN

NIPO: 126-20-021-2

ÍNDICE

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

Sistema Estadístico de Criminalidad

2021

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 ***IX Informe sobre Cibercriminalidad***, correspondiente a la delincuencia informática registrada en el año 2021.

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** (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y Cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad), tanto en la vertiente de los hechos conocidos, victimizaciones, como de las detenciones e investigados.

Para el capítulo de victimizaciones, se añaden para el año 2021 datos de la Ertzaintza, hecho que no se produce en informes anteriores a éste.

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, los datos que proporcionan cada Cuerpo policial en cuestión.

Este Informe aglutina datos del año 2021, no solo en relación a la información estadística sobre delitos informáticos en nuestro país, además, en un primer apartado y a modo introductorio, una serie de informaciones publicadas por otros organismos nacionales (INE) e internacionales (EUROSTAT, Comisión Europea), en relación a aquellas características más relevantes que permiten perfilar los rasgos distintivos de la sociedad española en relación a las tecnologías de la información y las comunicaciones (TIC).

En el segundo y tercer 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 conceptuaciones que emplea el Convenio de Budapest[1], 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.

Un aspecto que es necesario resaltar es el previsible aumento de la ciberdelincuencia. En palabras de las propias instituciones europeas[2], "*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*".

[1] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
[2] https://www.consilium.europa.eu/es/policies/cybersecurity/

En las siguientes infografías se muestran[3] datos y cifras sobre las principales ciberamenazas que ha sufrido la Unión Europea entre abril de 2020 y julio de 2021.

[3] https://www.consilium.europa.eu/es/infographics/cyber-threats-eu/

Violaciones de la seguridad de los datos y fugas de datos

Divulgación de datos sensibles, confidenciales o protegidos en un entorno no fiable.

*Se ha producido un **aumento de las violaciones de seguridad de datos sanitarios**.*

Ataques distribuidos de denegación de servicio

Ataques que impiden a los usuarios de una red o sistema acceder a información, servicios u otros recursos pertinentes.

*Se han producido más de **10 millones de ataques distribuidos de denegación de servicio** debido a la COVID-19.*

Desinformación

Ataque intencionado consistente en crear o divulgar información falsa o engañosa para manipular a la opinión pública.

*La **COVID-19** es uno de los principales temas de los **ataques de desinformación**.*

Amenazas no malintencionadas

En su mayoría se deben a errores humanos, aunque también pueden darse como consecuencia de catástrofes naturales que causan daños en las infraestructuras informáticas.

*El **50 %** de estos ataques se deben a **fallos de configuración**.*

Infografía nº 1.-Principales ciberamenazas en la UE (Fuente Consejo de Europa)

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 ciberseguridad, entre las que destacan:

[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

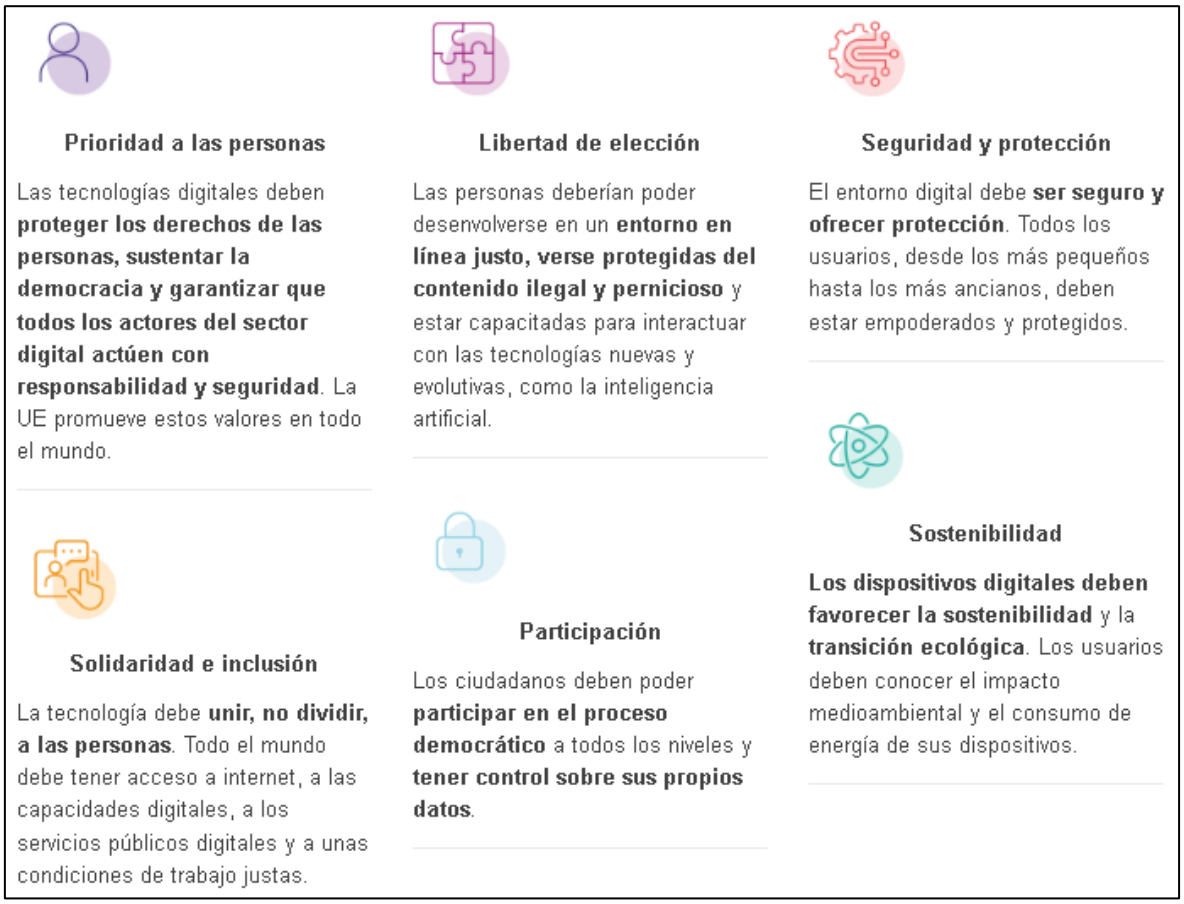
*Identidad Digital Europea: permitirá a todos los europeos acceder a los servicios en línea sin tener que utilizar métodos de identificación privada ni compartir datos personales sin necesidad.

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

Infografía nº 2: Metas digitales para 2030 de la Unión Europea.

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

[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



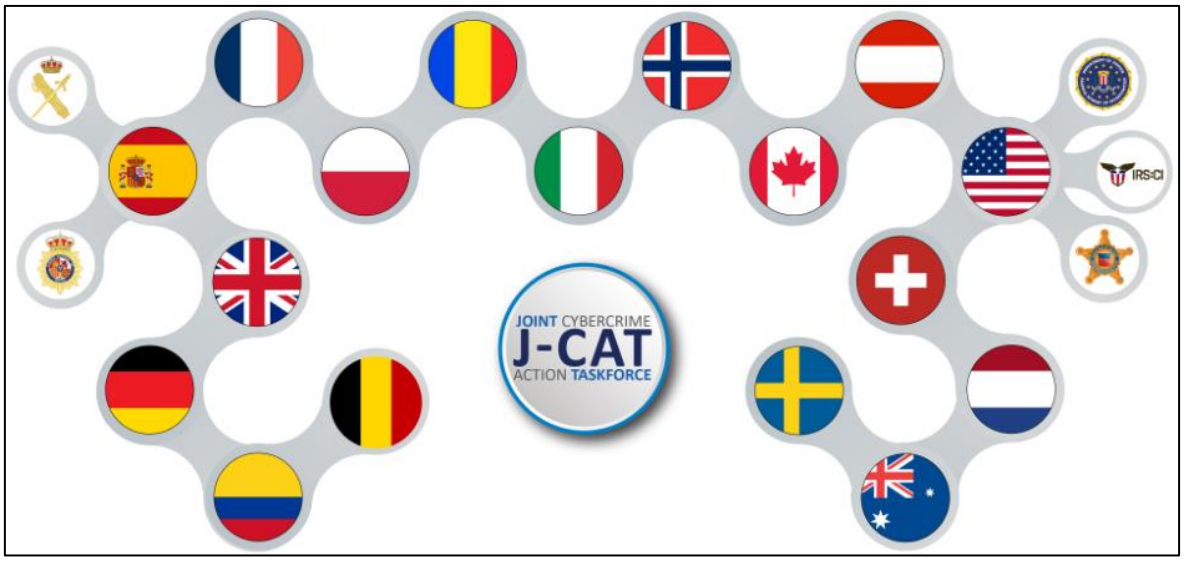
Infografía nº 3: Derechos y principios digitales en la UE (Fuente Comisión Europea)[8]

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

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 4: 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, SPACE 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 particular[11]:

"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

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 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

[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

malintencionada o criminal y robo de credenciales. Asimismo, aporta otro dato a tener en cuenta: "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 por lo tanto 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 1150/2021[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 servicios, 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.

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

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 2021[18], 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 phising, 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.

Por otro lado, una prueba de que la Cibercriminalidad, es un hecho que afecta de manera global a todas las personas y entidades, jurídicas y públicas, está relacionada con la actitud que las grandes empresas relacionadas con las nuevas tecnologías vienen adoptando en los tiempos actuales. A continuación, se ofrece un ejemplo de dos titulares de prensa aparecidos recientemente:

[17]https://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

- Google desmonta una red de bots que infectó a un millón de ordenadores Windows[19]

- Microsoft desarticula al grupo de cibercriminales chino Nickel, que había atacado a EE.UU. y otros 28 países.[20]

En línea con lo apuntado en párrafos anteriores y dentro del ámbito de las Fuerzas y Cuerpos de Seguridad, durante el año 2021 se realizó una intensa labor de lucha contra los ciberdelincuentes. Como botón de muestra caben citar dos operaciones:

-La primera de ellas realizada por Policía Nacional, donde se desarticuló una organización que habría defraudado más de 12.000.000 de euros[21]. En esta operación denominada "SECRETO", fueron detenidas 105 personas, e imputadas otras 14, en una macrooperación en la que se llevaron a cabo 88 registros simultáneos en cuatro países europeos.

La red desmantelada creaba empresas fantasmas en Estados Unidos y, tras dotarlas de una falsa solvencia económica, solicitaban la expedición de tarjetas de débito con el máximo importe disponible con el pretexto de utilizarlas en sus viajes a Europa.

Una vez en España, las tarjetas americanas eran utilizadas en establecimientos conniventes por elevados importes mediante el sistema de preautorización, aprovechando la diferencia de aceptación del pago existente entre los bancos americanos y españoles.

La investigación, que comenzó hace un año y medio, fue liderada por la Policía Nacional de manera conjunta con el Servicio Secreto Americano, contando con la participación de EUROPOL además de los cuerpos policiales de Grecia, Austria, Dinamarca, Reino Unido, Alemania, Polonia y Ucrania.

Los líderes del grupo, de origen albanés, utilizaban documentación falsa griega y contaban con personal de confianza, todos ellos españoles, que trabajaban para la organización realizando diversas funciones. Por un lado, estaban los que captaban establecimientos conniventes, empresarios o autónomos que permitieran pasar tarjetas americanas en el datafono de su comercio a cambio de una comisión del 15% del importe. Una vez se encontrase el dinero en la cuenta del connivente, éste tendría que reintegrar el 85% restante mediante transferencia bancaria a una de las muchas cuentas que manejaban

[19] https://www.europapress.es/portaltic/ciberseguridad/noticia-google-desmota-red-bots-infecto-millon-ordenadores-windows-20211208160421.html

[20] https://www.europapress.es/portaltic/ciberseguridad/noticia-microsoft-desarticula-grupo-cibercriminales-chino-nickel-atacado-eeuu-otros-28-paises-20211208114233.html

[21] https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=8401#

los principales miembros de la organización tanto en España como en diferentes países de Europa. Para justificar la supuesta transacción elaboraban facturas falsas a nombre de las mercantiles americanas que figuraban en la tarjeta, con la finalidad de simular haber comprado productos o prestado algún servicio.

-Otra operación en el ámbito de la Cibercriminalidad a destacar fue la realizada por la Guardia Civil, al disolver grupos de más de 100.000 miembros de una conocida app de mensajería dedicados al carding en una operación contra el fraude informático.

En el marco de la operación "RECOLECTOR"[22] desarrollada por la Guardia Civil se consiguió la desarticulación de una organización criminal de carácter internacional dedicada a la comisión de delitos relacionados con el fraude informático en todo su espectro, procediéndose a la detención e investigación de once personas en España y Chile.

La principal actividad del entramado de ciberdelincuentes era la obtención ilícita de datos relacionados con las credenciales de pago (generalmente tarjetas de crédito), tanto para su explotación directa en plataformas de comercio online por la propia organización, como para proceder a su venta en canales de una conocida app de mensajería y en foros de la DarkWeb, este conjunto de actividades delictivas es conocida en el mundo del cibercrimen como CARDING.

El modus operandi identificado se basaba, fundamentalmente, en la suplantación de sitios web reales, método conocido como phishing, pertenecientes a entidades bancarias nacionales e internacionales, así como de conocidas empresas de servicios de contenidos en multimedia en streaming, y obtener con ello de esa manera los datos de las víctimas.

Para la consecución de sus objetivos delictivos hicieron uso de diferentes tipos de malware como el troyano bancario Zeus y TinyBanker, keyloggers, herramientas para ataques de denegación de servicio, bots, redes botnet, y diversos tipos de ransomware que se encontraban a su disposición.

A la organización se le imputaron más de 2.500 hechos delictivos con más de 300 empresas a nivel nacional afectadas, estimándose un perjuicio patrimonial que podría alcanzar el millón de euros, obteniéndose información del uso de más de 42.000 tarjetas de crédito por parte de los diferentes integrantes de la organización delictiva. Se han

22 https://www.guardiacivil.es/es/prensa/noticias/7942.html#:~:text=Tambi%C3%A9n%20se%20ha%20conseguido%20el,pago%20de%20tarjetas%20de%20cr%C3%A9dito.

localizado tarjetas de crédito utilizadas por los ciberdelincuentes de 47 países en todo el mundo, destacando especialmente las de EE.UU. y países de la Unión Europea.

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

En este *IX Informe sobre Cibercriminalidad*, en el que se publican los datos estadísticos de cibercriminalidad y las amenazas que han sido descubiertas a lo largo del año 2021 en nuestro país, también se hace referencia a una serie de datos relativos al uso de las TIC por parte de la sociedad española en general. Para ello, se toman como referencia estudios y encuestas de opinión realizadas por otros organismos públicos, tanto de ámbito nacional (INE) como europeos (EUROSTAT).

La Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2021), del Instituto Nacional de Estadística (INE), se trata de una investigación dirigida a las personas de 16 años en adelante, residentes en viviendas familiares, que recoge información sobre los diversos productos de tecnologías de información y comunicación de los hogares españoles, así como los usos que hacen los españoles de estos productos, de Internet y del comercio electrónico. Se dedica una atención especial al uso que los niños hacen de la tecnología, por lo que obtiene igualmente información de los menores de 10 a 15 años.

A lo largo de este Capítulo 2 del Informe, en sus diferentes apartados, se traza y esquematiza un perfil de la sociedad española enlazado al uso de las tecnologías e Internet.

Los datos del punto 2.1 (Hogares y porcentaje de vivienda con/sin acceso a Internet), procedentes de la Encuesta del INE, reflejan el porcentaje de viviendas que poseen ordenador y aquellas que no disponen de estos dispositivos, así como las que tienen contratado un servicio de acceso a Internet. En primer lugar, de un análisis genérico de los datos expuestos se aprecia que el porcentaje de viviendas que poseen ordenador y las que disponen de acceso a Internet se ha incrementado en 2021 con respecto al año 2020. Siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2012-2021).

Además, se puede observar que los índices sobre las viviendas que poseen o no dispositivos de esta naturaleza, así como la existencia de que éstas estén conectadas a

Internet, es más elevado, en ambos casos, cuanto mayor es la población de la localidad en la que se ubican los hogares.

En el apartado 2.2 (Perfil del ciudadano ante la sociedad de la información. Uso de Internet), se hace referencia a la información correspondiente, según los datos publicados por el INE, al número de personas que afirman haber accedido a Internet en los últimos tres meses. De esta forma, se puede observar que también esta variable aumenta año a año desde 2012.

Con los datos reflejados en la *Encuesta anual del INE* se pueden extraer una serie de particularidades que permiten establecer los rasgos que delimitan el perfil del usuario español ante la sociedad de la información.

Si atendemos a la edad del usuario, los grupos de edad más temprana son los que más hacen uso de las tecnologías. En este sentido, el 99,7 % de los jóvenes, entre 16 a 24 años, afirman haber accedido a la red en los últimos tres meses. Es de destacar, que todos los grupos de edad, se encuentran por encima del 90% de acceso a Internet, con excepción de los comprendidos entre los 65 a 74 años, si bien éstos aumentan de manera notable, al situarse en una franja del 73,3%, dato que casi cuadruplica los que los efectuaban en el año 2012.

Por sexos, y en línea con años recientes, se iguala el porcentaje de uso de Internet de mujeres y hombres.

Un aspecto importante se visualiza en el punto 2.3 (Perfil del menor de edad ante la sociedad de la información), donde se detalla que el porcentaje de los menores de edad (10 a 15 años) que han utilizado un ordenador y han accedido a Internet en los tres últimos meses, con el 95,1%. Por sexos, es pequeña la diferencia, aunque hay que reflejar que la mujer muestra mayores porcentajes en ambas categorías. En 2021, el 94,5% de los niños afirmaron haber utilizado un ordenador en los últimos tres meses, frente al 95,8% de las niñas, siendo el 97,4% de los chicos que se referencia su acceso a Internet en relación al 97,6% de las chicas.

El INE, asimismo, proporciona datos sobre el perfil de las personas que han comprado alguna vez por internet (2.4). Así pues, se puede apreciar que desde el año 2012 el comercio electrónico se ha llegado casi a triplicar, puesto que el 55,2 % de las personas encuestadas en 2021 reconocen haber realizado alguna compra empleando esta vía,

mientras que en el año 2012 solo lo hacían el 21,7%. Por sexo, los hombres muestran ligeramente mayores cifras porcentuales que las mujeres (55,7 frente al 54,8%), aunque esta diferencia con el paso de los años se viene reduciendo paulatinamente.

Por grupos o rangos de edad, son las personas con edades comprendidas entre los 25 y 34 años las que realizan más compras a través de Internet (74,3%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 23,0% realiza compras por Internet, aunque es un valor al alza como se puede corroborar por el hecho de esta franja de edad en el año 2012, sólo efectuaban compras por Internet el 3,5%.

Por otra parte, en este Capítulo se incluyen datos que tratan de recrear una comparación de la sociedad española con las tecnologías de la información en relación a los demás países de la Unión Europea, en función de la información obtenida de EUROSTAT.

Así, en un primer momento, se exponen los porcentajes de viviendas con acceso a Internet en los diferentes países de la Unión Europea (27-UE) (Punto 2.5 Comparativa internacional), en la serie histórica 2012-2021. Un hecho que se viene produciendo en los últimos años es que ***España, se encuentra por encima de la media de la UE***, con un 96% frente al 92% de la Unión Europea.

En el apartado 2.6, se incluyen datos extraídos del Índice de Economía y Sociedad Digital (DESI por sus siglas en inglés). Se trata de un índice compuesto desarrollado por la Comisión Europea para evaluar los avances de los países de la UE hacia una economía y una sociedad digitales. ***España destaca en las dimensiones de "Conectividad" y "Servicios públicos digitales"***, con valores muy por encima de la media de la UE.

3.- 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.

4.- 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 responsables[23], se llevará a cabo la explotación estadística de los datos que se conozcan por las por las Fuerzas y Cuerpos de Seguridad del Estado (Cuerpo Nacional de Policía y Guardia Civil), las Fuerzas y Cuerpos de Seguridad dependientes de las Comunidades Autónomas (Mossos d' Esquadra, Ertzaintza 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.

[23] Actuaciones policiales y responsables: son dos operaciones estadísticas dadas de alta en el Inventario de Operaciones Estadísticas del INE)

Datos globales

El apartado 4.1 (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 2017-2021 (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 2017 a 2021, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2021, se han conocido un total de 305.477 hechos, lo que supone un 6,1% más con respecto al año anterior. De esta cifra, el 87,4 % corresponde a fraudes informáticos (estafas) y el 5,7% 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. No obstante, durante el año 2021 su peso proporcional ha disminuido ligeramente sobre el año 2020. A este respecto, hay que recordar que ese último año, tiene connotaciones especiales por todo lo relacionado con la pandemia generada por la Covid-19. Como se puede observar en la tabla nº 2, hemos pasado del año 2017, donde nos situábamos en el 5,7%, al año 2021 con el 15,6%.

2017	5,7%
2018	7,5%
2019	9,9%
2020	16,3%
2021	15,6%

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

Las gráficas del punto 4.2 (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 2017 a 2021.

En relación al porcentaje de hechos esclarecidos, en el año 2021, éste supone el 15,9% del total de los hechos conocidos, lo que implica un aumento con respecto al año anterior, que alcanzó el porcentaje de esclarecimiento del 14%. Por otra parte, los detenidos e investigados han alcanzado la cifra de 13.801, lo que supone un aumento de un 22,3% con respecto al año 2020, en el que se registraron 11.280 detenidos e investigados.

En el apartado 4.3 y 4.4 se detallan datos por meses, observándose que durante el 2021, el mes de mayor incidencia delictiva fue el mes de diciembre.

La distribución de la Cibercriminalidad, desde el punto de vista geográfico (4.5. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2021, sitúa a Madrid, Cataluña, 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, Bizkaia y Málaga.

Los datos de la sección 4.6, 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 (Ertzaintza comienza a facilitar datos de victimizaciones a partir de 2021).

En 2021, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 240.100 [24], es decir, un 11,4% más que en el año 2020. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (51,9%), tienen entre 26 a 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y falsificación informática. Sin embargo, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino cuando se trata de hechos relacionados con la falsificación informática (usurpación del estado civil), acceso e interceptación ilícita (descubrimiento y revelación de secretos), contra el honor (injurias) y los delitos sexuales [delito de contacto mediante tecnología con menor de 16 años con fines sexuales (grooming)].

Además, en el punto 4.7 (Victimizaciones según grupo de edad y sexo) tal y como figura en la información registrada en el Sistema Estadístico de Criminalidad (SEC), se aprecia que, en 2021, el 29,0 % del conjunto de las víctimas recae sobre el grupo de edad de 26 a 40 años. Siendo este grupo de edad el mayoritario tanto para las víctimas de sexo masculino como femenino.

Por otra parte, se publican datos relativos a las victimizaciones desglosadas por tipología penal y sexo (Punto 4.8). 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 4.9), el 87,5% de ellas son españolas, y el 12,5% 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.

[24] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (305.477) y el de victimizaciones registradas (240.100), 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. Asimismo, para el conjunto de hechos conocidos, se tienen datos de todos los cuerpos policiales, extremo que no sucede con las victimizaciones que no se poseen datos de la Ertzaintza.

Al igual que en el informe de 2021 (datos de 2020), en este *IX Informe sobre Cibercriminalidad,* 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 4.10 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 4.10.

Igualmente, en este estudio se consignan datos detallados de las victimizaciones según el sexo de la misma. En las secciones 4.12 y 4.13 se aportan los del sexo masculino y las 4.14 y 4.15, las del sexo femenino. Como primera diferencia entre ambas, se aprecia que las victimizaciones de mujeres son cuantitativamente superiores en menores y en la franja de edad de 18 a 30 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 4.16 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, de 2021.

De la cifra total de detenciones e investigaciones (13.801) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 71,3% 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 (4.18 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 (79,3%) (4.19). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Marruecos, Rumanía y República Dominicana, los que aglutinan un mayor número de casos.

Al desglosar la información según los distintos rangos de edad predeterminados (4.20 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 RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN >>

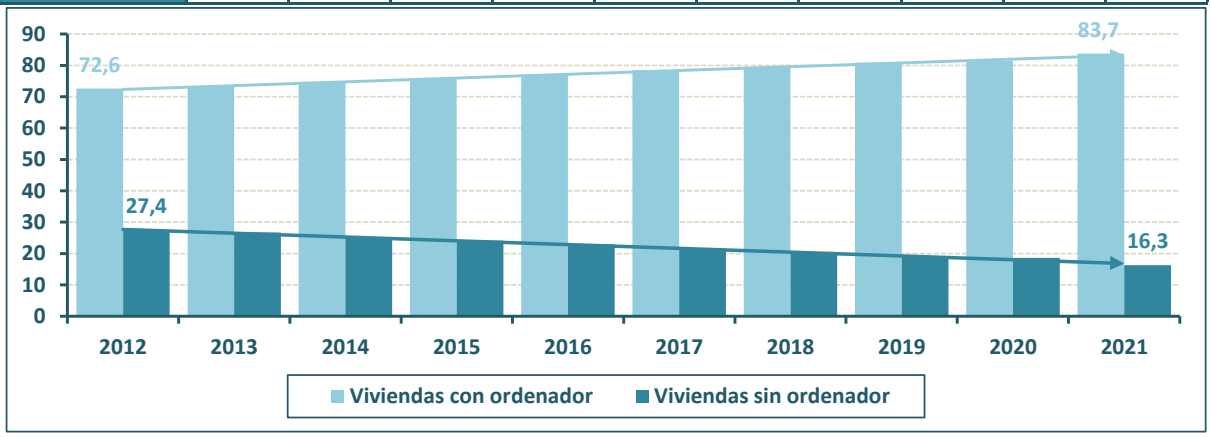
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: INE)

>> 2.1. Hogares

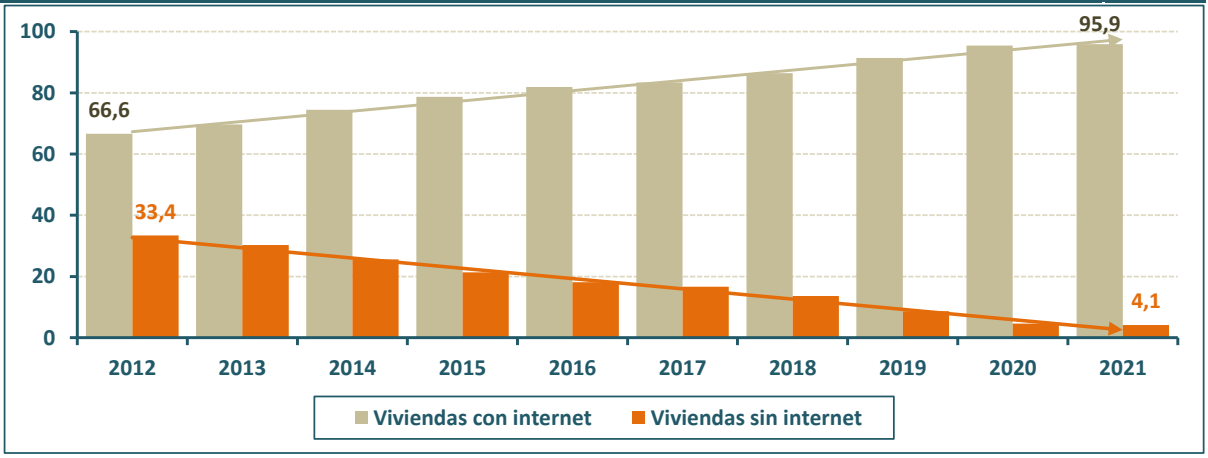
PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Viviendas con ordenador	**72,6**	73,3	74,8	75,9	77,1	78,4	79,5	80,9	81,4	**83,7**
Viviendas sin ordenador	**27,4**	26,7	25,2	24,1	22,9	21,6	20,5	19,1	18,6	**16,3**

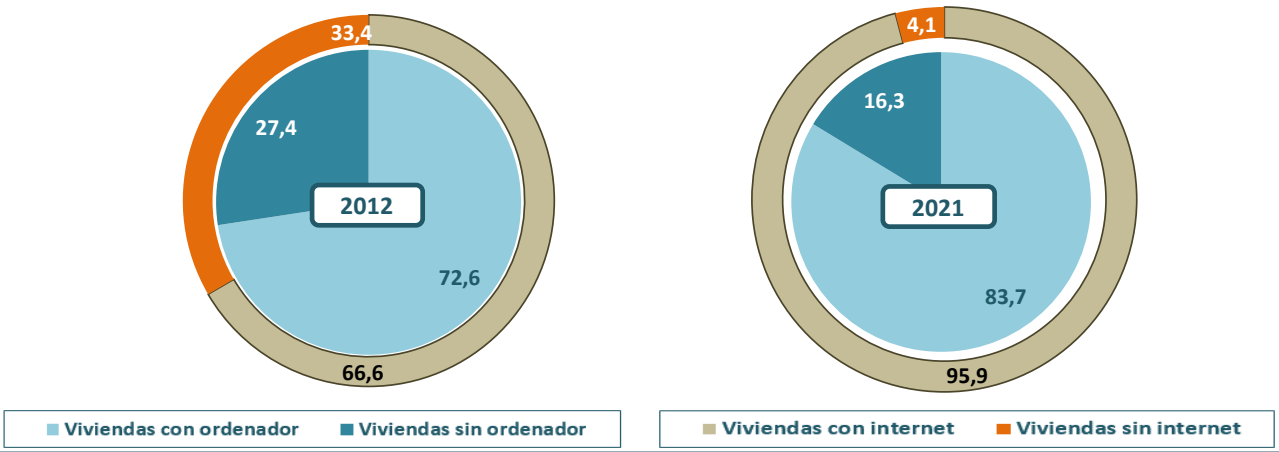


PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Viviendas con internet	**66,6**	69,7	74,4	78,7	81,9	83,4	86,4	91,4	95,4	**95,9**
Viviendas sin internet	**33,4**	30,3	25,6	21,3	18,1	16,6	13,6	8,6	4,6	**4,1**



CONTRASTE EVOLUTIVO DE LAS VIVIENDAS 2012 - 2021

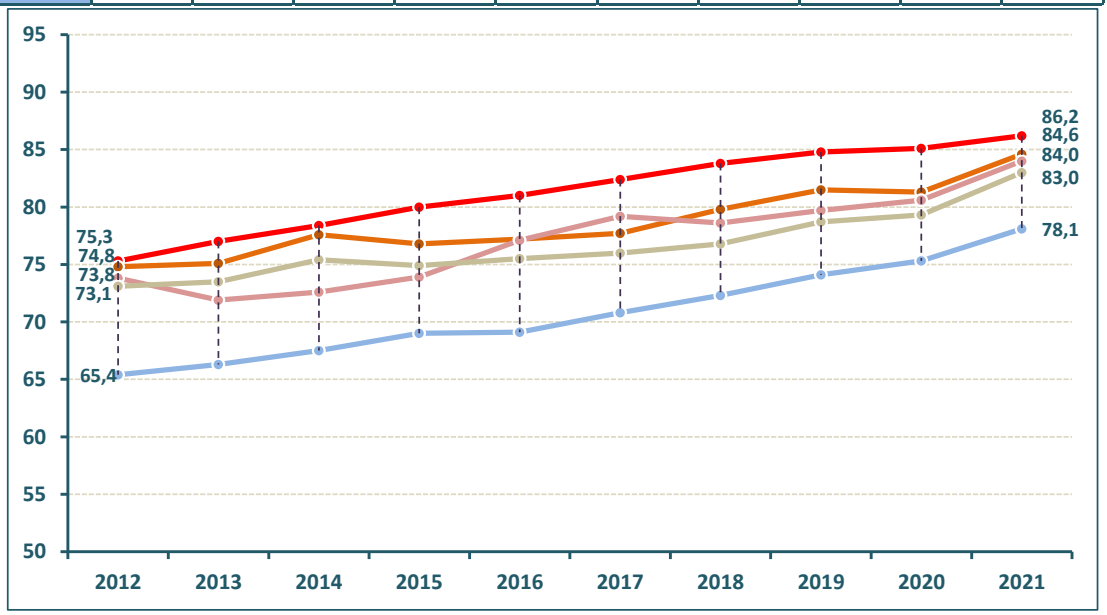


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

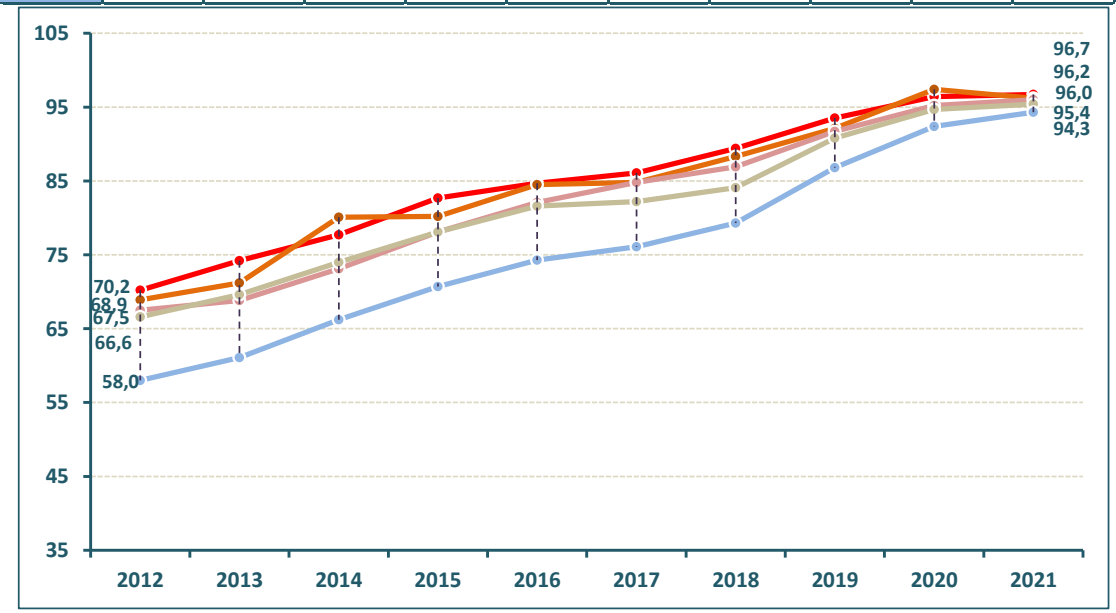
(Fuente de datos: INE)

>> 2.1. Hogares. Por tipo de hábitat

	PORCENTAJE DE VIVIENDAS CON ORDENADOR									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Más de 100.000 hab.	**75,3**	77,0	78,4	80,0	81,0	82,4	83,8	84,8	85,1	**86,2**
De 50.000 a 100.000 hab.	**74,8**	75,1	77,6	76,8	77,2	77,7	79,8	81,5	81,3	**84,6**
De 20.000 a 50.000 hab.	**73,8**	71,9	72,6	73,9	77,1	79,2	78,6	79,7	80,6	**84,0**
De 10.000 a 20.000 hab.	**73,1**	73,5	75,4	74,9	75,5	76,0	76,8	78,7	79,3	**83,0**
Menos de 10.000 hab.	**65,4**	66,3	67,5	69,0	69,1	70,8	72,3	74,1	75,3	**78,1**



	PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Más de 100.000 hab.	**70,2**	74,2	77,7	82,7	84,7	86,1	89,4	93,5	96,4	**96,7**
De 50.000 a 100.000 hab.	**68,9**	71,2	80,1	80,2	84,5	84,8	88,3	92,1	97,4	**96,2**
De 20.000 a 50.000 hab.	**67,5**	68,8	73,1	78,1	82,1	84,8	86,9	91,7	95,2	**96,0**
De 10.000 a 20.000 hab.	**66,6**	69,6	74,0	78,1	81,6	82,2	84,1	90,8	94,7	**95,4**
Menos de 10.000 hab.	**58,0**	61,1	66,2	70,7	74,3	76,1	79,3	86,8	92,4	**94,3**

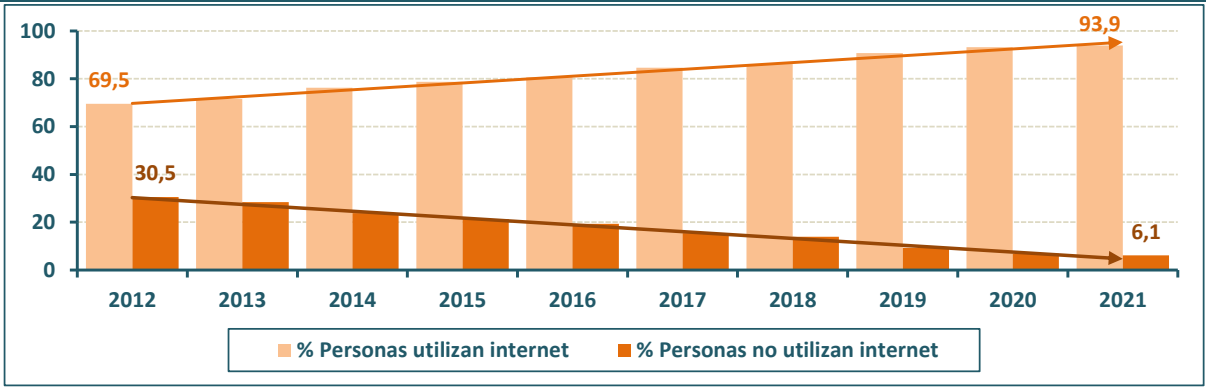


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

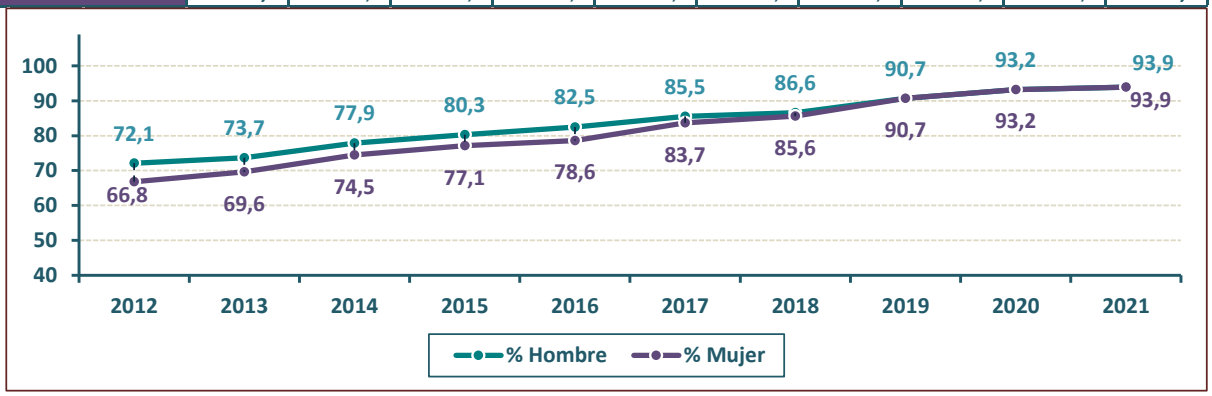
(Fuente de datos: INE)

>> 2.2. Perfil del ciudadano ante la sociedad de la información. Uso de Internet

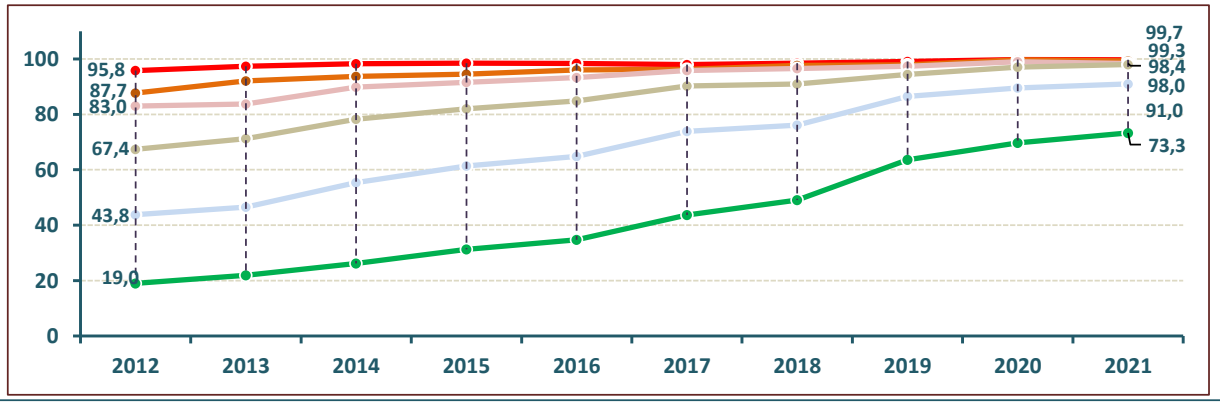
% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Utilizado internet	69,5	71,6	76,2	78,7	80,6	84,6	86,1	90,7	93,2	93,9
No utilizado internet	30,5	28,4	23,8	21,3	19,4	15,4	13,9	9,3	6,8	6,1



% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Hombre	72,1	73,7	77,9	80,3	82,5	85,5	86,6	90,7	93,2	93,9
Mujer	66,8	69,6	74,5	77,1	78,6	83,7	85,6	90,7	93,2	93,9



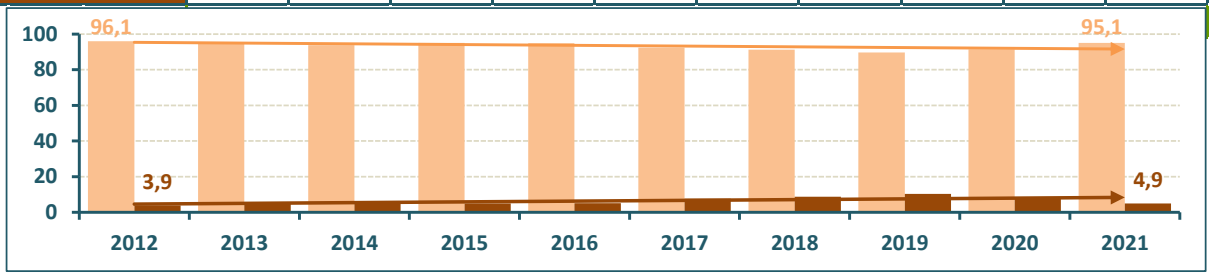
% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Edad: De 16 a 24 años	95,8	97,4	98,3	98,5	98,4	98,0	98,5	99,1	99,8	99,7
Edad: De 25 a 34 años	87,7	92,1	93,7	94,5	96,0	96,3	97,7	97,9	99,7	99,3
Edad: De 35 a 44 años	83,0	83,7	89,8	91,6	93,3	95,8	96,6	97,4	99,0	98,4
Edad: De 45 a 54 años	67,4	71,2	78,2	82,0	84,9	90,3	91,0	94,4	97,1	98,0
Edad: De 55 a 64 años	43,8	46,5	55,4	61,4	64,8	73,9	76,1	86,5	89,5	91,0
Edad: De 65 a 74 años	19,0	21,9	26,2	31,3	34,7	43,7	49,1	63,6	69,7	73,3



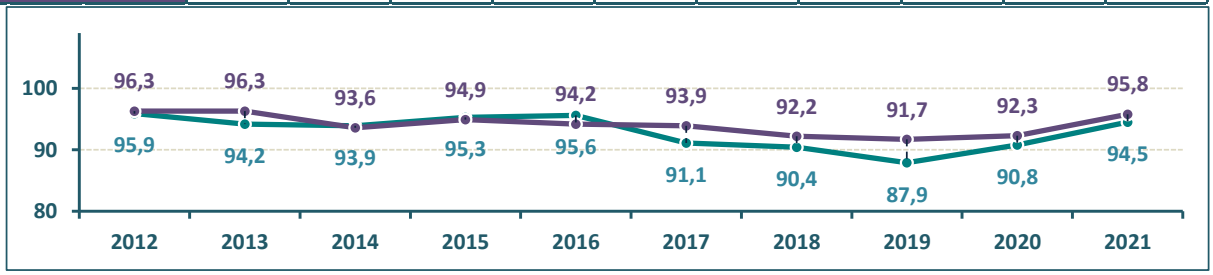
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN (Fuente de datos: INE)

>> 2.3. Perfil del menor de edad (10 a 15 años) ante la sociedad de la información

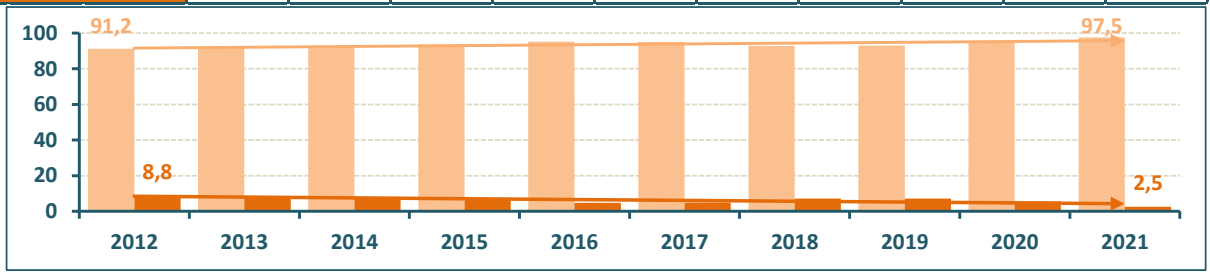
% DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Utilizado ordenador	96,1	95,2	93,8	95,1	94,9	92,4	91,3	89,7	91,5	95,1
No utilizado ordenador	3,9	4,8	6,2	4,9	5,1	7,6	8,7	10,3	8,5	4,9



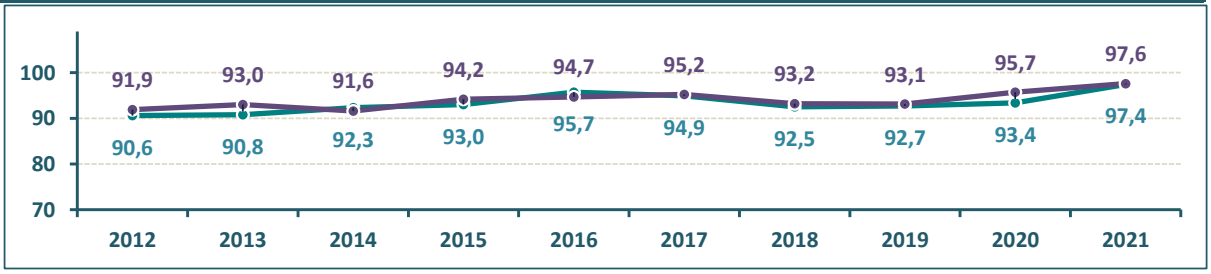
% POR SEXO DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Hombre	95,9	94,2	93,9	95,3	95,6	91,1	90,4	87,9	90,8	94,5
Mujer	96,3	96,3	93,6	94,9	94,2	93,9	92,2	91,7	92,3	95,8



% DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Utilizado internet	91,2	91,9	92,0	93,6	95,2	95,1	92,8	92,9	94,5	97,5
No utilizado internet	8,8	8,1	8,0	6,4	4,8	4,9	7,2	7,1	5,5	2,5



% POR SEXO DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Hombre	90,6	90,8	92,3	93,0	95,7	94,9	92,5	92,7	93,4	97,4
Mujer	91,9	93,0	91,6	94,2	94,7	95,2	93,2	93,1	95,7	97,6

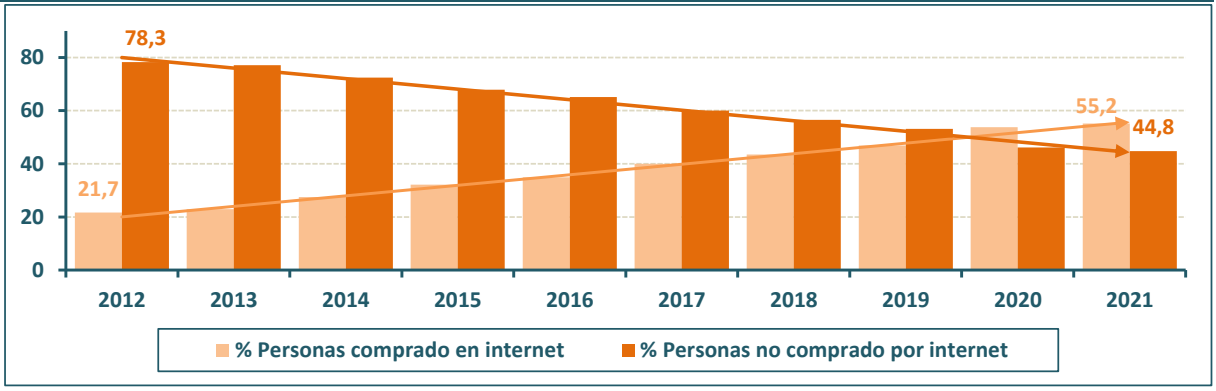


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

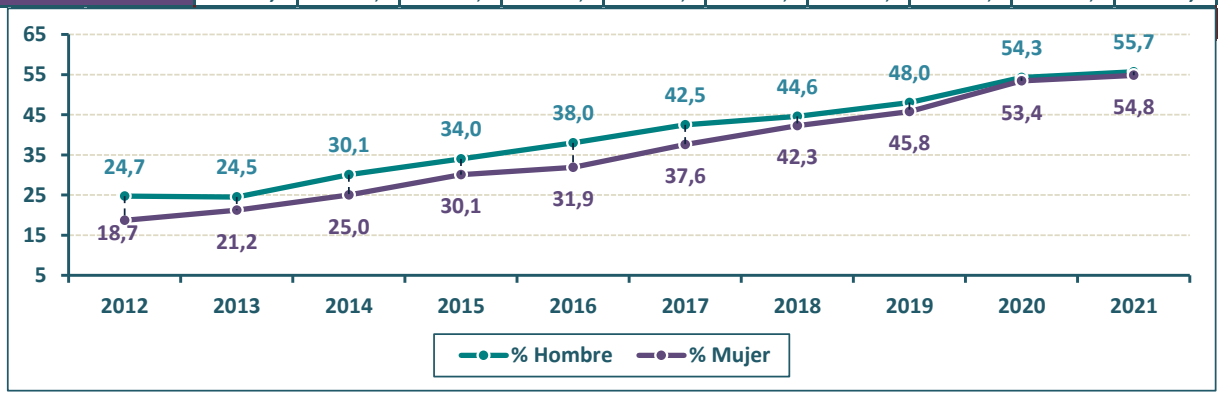
(Fuente de datos: INE)

>> 2.4. Perfil de las personas que han comprado alguna vez por Internet

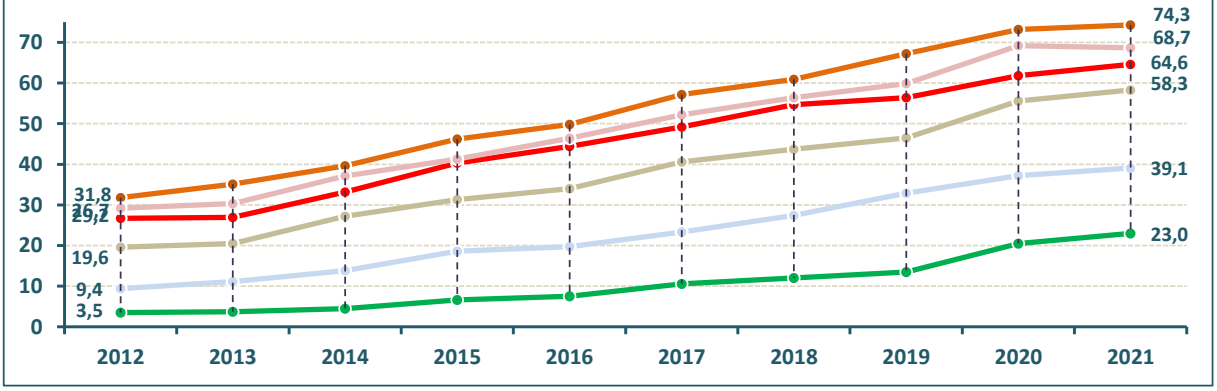
	% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Comprado en internet	21,7	22,9	27,5	32,1	34,9	40,0	43,5	46,9	53,8	55,2
No comprado en internet	78,3	77,1	72,5	67,9	65,1	60,0	56,5	53,1	46,2	44,8



	% POR SEXO DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Hombre	24,7	24,5	30,1	34,0	38,0	42,5	44,6	48,0	54,3	55,7
Mujer	18,7	21,2	25,0	30,1	31,9	37,6	42,3	45,8	53,4	54,8



	% POR GRUPO DE EDAD DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Edad: De 16 a 24 años	26,7	26,9	33,2	40,3	44,4	49,2	54,7	56,4	61,8	64,6
Edad: De 25 a 34 años	31,8	35,1	39,6	46,2	49,8	57,2	60,9	67,2	73,2	74,3
Edad: De 35 a 44 años	29,2	30,3	37,1	41,3	46,4	52,2	56,4	59,9	69,2	68,7
Edad: De 45 a 54 años	19,6	20,5	27,2	31,3	34,0	40,6	43,7	46,5	55,6	58,3
Edad: De 55 a 64 años	9,4	11,1	13,8	18,6	19,7	23,3	27,4	32,9	37,2	39,1
Edad: De 65 a 74 años	3,5	3,7	4,5	6,6	7,5	10,6	12,0	13,5	20,5	23,0



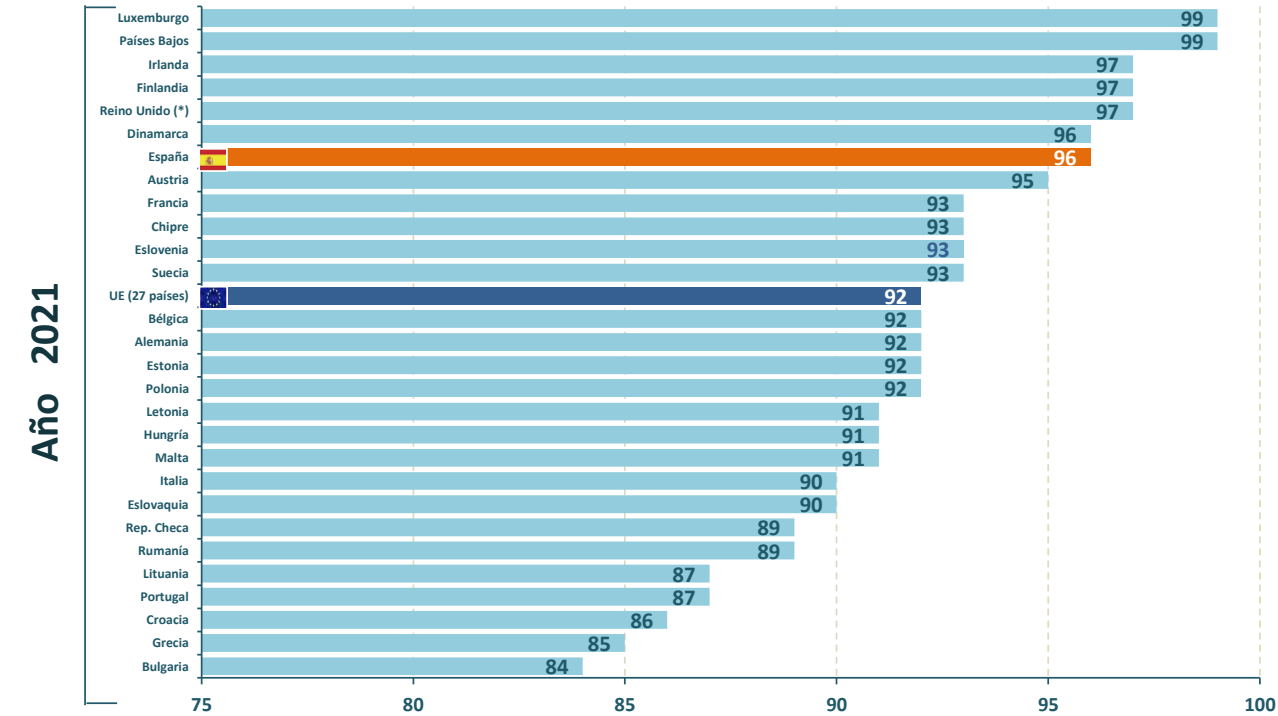
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: EUROSTAT)

>> 2.5. Comparativa internacional. Viviendas con acceso a Internet

PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
UE (27 países)	75	77	80	81	84	86	88	90	91	92
Bélgica	78	80	83	82	85	86	87	90	91	92
Bulgaria	51	54	57	59	64	67	72	75	79	84
Rep. Checa	73	73	78	79	82	83	86	87	88	89
Dinamarca	92	93	93	92	94	97	93	95	95	96
Alemania	85	88	89	90	92	93	94	95	96	92
Estonia	74	79	83	88	86	88	90	90	90	92
Irlanda	81	82	82	85	87	88	89	91	92	97
Grecia	54	56	66	68	69	71	76	79	80	85
España	67	70	74	79	82	83	86	91	95	96
Francia	80	82	83	83	86	86	89	90		93
Croacia	66	65	68	77	77	76	82	81	85	86
Italia	63	69	73	75	79	81	84	85	88	90
Chipre	62	65	69	71	74	79	82	90	93	93
Letonia	69	72	73	76	77	79	82	85	90	91
Lituania	60	65	66	68	72	75	78	82	82	87
Luxemburgo	93	94	96	97	97	97	93	95	94	99
Hungría	67	70	73	76	79	82	83	86	88	91
Malta	77	78	80	81	81	85	84	86	90	91
Países Bajos	94	95	96	96	97	98	98	98	97	99
Austria	79	81	81	82	85	89	89	90	90	95
Polonia	70	72	75	76	80	82	84	87	90	92
Portugal	61	62	65	70	74	77	79	81	84	87
Rumanía	54	58	61	68	72	76	81	84	86	89
Eslovenia	74	76	77	78	78	82	87	89	90	93
Eslovaquia	75	78	78	79	81	81	81	82	86	90
Finlandia	87	89	90	90	92	94	94	94	96	97
Suecia	92	93	90	91	94	95	92	96	94	93
Reino Unido (*)	87	88	90	91	93	94	95	96	97	97

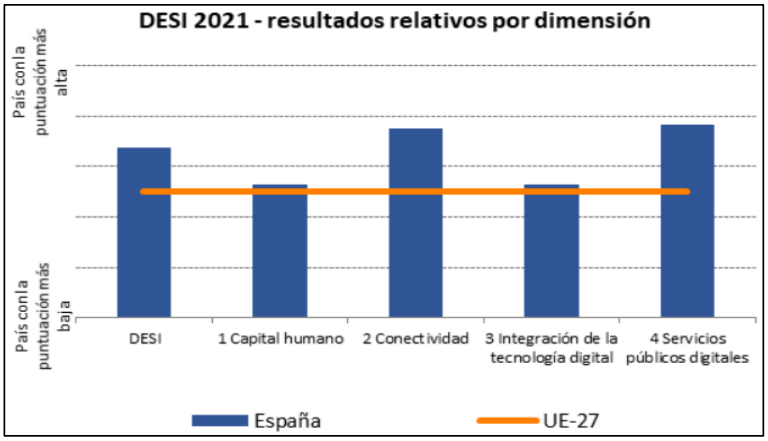


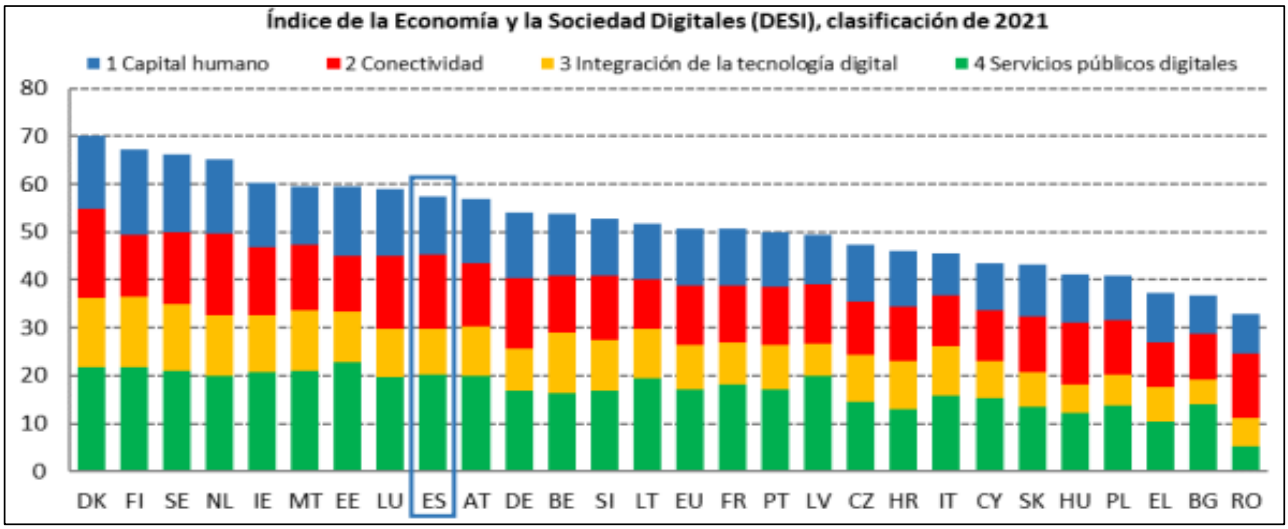
(*) Los últimos datos que se poseen de Reino Unido corresponden al año 2020.

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: Comisión Europea)

>> 2.6. Indice de Economía y Sociedad Digital (DESI). Comparativa España-Unión Europea





	España			UE
	DESI 2019	DESI 2020	DESI 2021	DESI 2021
2a1 Implantación global de la banda ancha fija % hogares	77 % 2018	78 % 2019	82 % 2020	77 % 2020
2a2 Implantación de banda ancha fija de al menos 100 Mbps % hogares	30 % 2018	53 % 2019	65 % 2020	34 % 2020
2a3 Implantación de al menos 1 Gbps % hogares	NP	<0,01 % 2019	<0,01 % 2020	1,3 % 2020
2b1 Cobertura de banda ancha de nueva generación (NGA) % hogares	88 % 2018	90 % 2019	92 % 2020	87 % 2020
2b2 Cobertura de la red fija de muy alta capacidad % hogares	77 % 2018	89 % 2019	92 % 2020	59 % 2020
2c1 Cobertura 4G % áreas pobladas	99,5 % 2018	99,8 % 2019	99,9 % 2020	99,7 % 2020
2c2 Preparación para 5G Espectro asignado como un % del total del espectro 5G armonizado	30 % 2019	30 % 2020	65 % 2021	51 % 2021
2c3 Cobertura 5G % áreas pobladas	NP	NP	13 % 2020	14 % 2020
2c4 Implantación de la banda ancha móvil % personas	80 % 2018	86 % 2019	86 % 2019	71 % 2019
2d1 Índice de precios de la banda ancha Puntuación (0 a 100)	NP	52 2019	73 2020	69 2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD >>

3.- 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

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-l 12/2018.

>> 3.1. Incidentes gestionados por el INCIBE-CERT (entidades privadas)

El INCIBE-CERT gestionó un total de 109.126 incidentes de ciberseguridad en España durante el año 2021.

Analizando el número de incidentes en función de su tipología, se concluye que los incidentes tipo *malware* son los más frecuentes según el registro del pasado año; con un porcentaje del 29,88%, respecto del total; seguido de los *Fraudes* con un 28,60%.

Con respecto a los tipos de ***malware*** con mayor relevancia, y efectos, en el año 2021, significar los siguientes:

Emotet: Funciona como "*downloader"* permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima, desde credenciales de usuario hasta información bancaria.

Las campañas de *Emotet* más habituales durante el año 2021 implicaron el envío de correos electrónicos *phishing* con archivos adjuntos maliciosos que contenían macros que funcionaban como descargadores de malware. La mayoría de los archivos adjuntos se identificaron como ficheros de Microsoft Office, si bien, se observaron archivos con otros formatos tales como ZIP y PDF.

Mekotio: También conocido como BestaFera, representa una amenaza grave para todos aquellos usuarios que hacen uso de servicios de banca *online* o de criptodivisas, concretamente de Bitcoins, ya que se trata de un troyano bancario que afecta a todas las versiones del sistema operativo Windows, comprendidas entre Windows XP y Windows 10.

Funciona como "*downloader*" permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima.

Las campañas de Mekotio más habituales durante el año 2021 implicaron el envío de correos electrónicos *phishing* con archivos adjuntos maliciosos que contenían macros que funcionaban como descargadores de *malware*.

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.

Anatsa: *Malware* de tipo troyano para dispositivos Android que ha sido analizado, en paralelo, por diferentes organizaciones asignándole diferentes nombres como: Anatsa, TeaBot o Toddler.

Al igual que en Flubot, una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones iniciadas, 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.

Hive: *Malware* de tipo *ransomware* que implementa las funcionalidades de cifrado de la información de un equipo infectado, imposibilitando la recuperación de los datos de forma sencilla.

Por otro lado, con respecto a los incidentes relativos al **fraude** significar que, durante el año 2021 han continuado proliferando campañas de suplantación de la identidad de clientes o proveedores, mediante vía telefónica y correo electrónico, con un total de 31.529 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.

>> 3.2. Incidentes gestionados de Operadores Críticos del sector privado

A lo largo del año 2021, el número de incidentes de ciberseguridad disminuyó en un 21,02% con respecto al año anterior, gestionándose un total de 680 incidentes.

Con respecto a los tipos de incidentes con mayor relevancia se encuentran los relacionados con **sistemas vulnerables**, con un 49,85%, seguido por ***malware*** y **robo de información** con un 26,03% y un 17,21%, respectivamente.

>> 3.3. Incidentes gestionados por Sector Estratégico

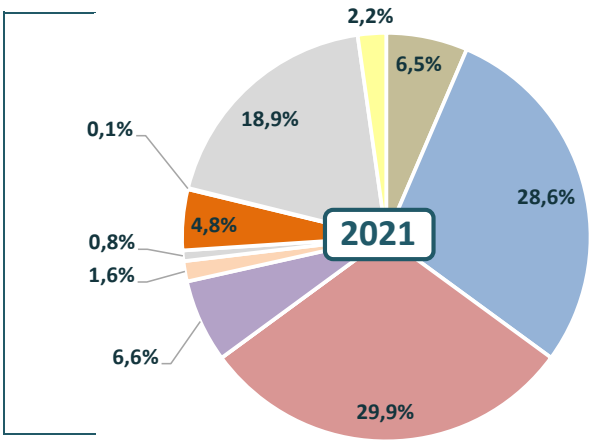
Los sectores PIC donde se han detectado un mayor número de incidentes han sido el sector **Energía**, con un 30,44%, seguido del sector **Tributario y Financiero**, con un 25,29% y el sector **Agua**, con un 17,21%.

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.1. Incidentes gestionados por el INCIBE-CERT

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

Porcentaje del total de incidentes gestionados

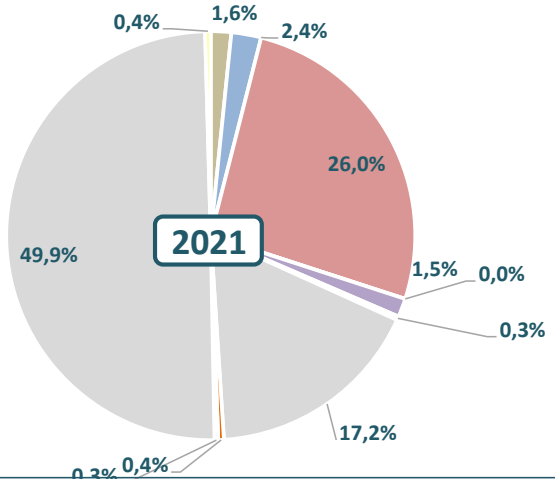


*Véase metadatos explicativos

>> 3.2. Incidentes gestionados en relación con las infraestructuras críticas

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

Porcentaje del total de incidentes gestionados



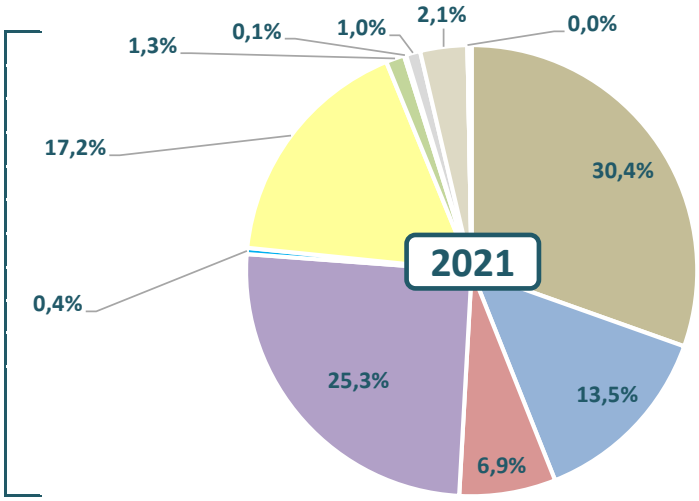
*Véase metadatos explicativos

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.3. Incidentes gestionados por sector estratégico

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

Porcentaje del total de incidentes gestionados



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD >>

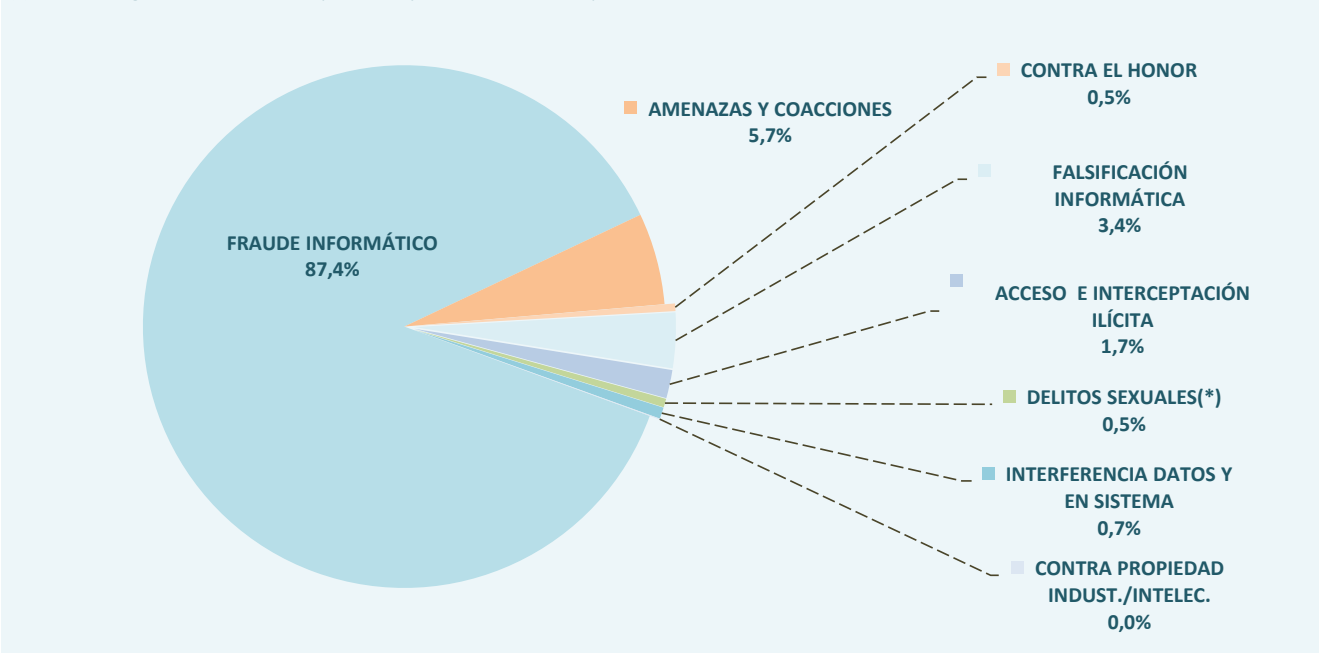
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2017	2018	2019	2020	2021
ACCESO E INTERCEPTACIÓN ILÍCITA	3.150	3.384	4.004	4.653	5.342
AMENAZAS Y COACCIONES	11.812	12.800	12.782	14.066	17.319
CONTRA EL HONOR	1.561	1.448	1.422	1.550	1.426
CONTRA PROPIEDAD INDUST./INTELEC.	121	232	197	125	137
DELITOS SEXUALES(*)	1.392	1.581	1.774	1.783	1.628
FALSIFICACIÓN INFORMÁTICA	3.280	3.436	4.275	6.289	10.476
FRAUDE INFORMÁTICO	94.792	136.656	192.375	257.907	267.011
INTERFERENCIA DATOS Y EN SISTEMA	1.291	1.192	1.473	1.590	2.138
Total HECHOS CONOCIDOS	**117.399**	**160.729**	**218.302**	**287.963**	**305.477**

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



>> 4.2. Evolución global de hechos conocidos, esclarecidos y detenciones / investigados

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

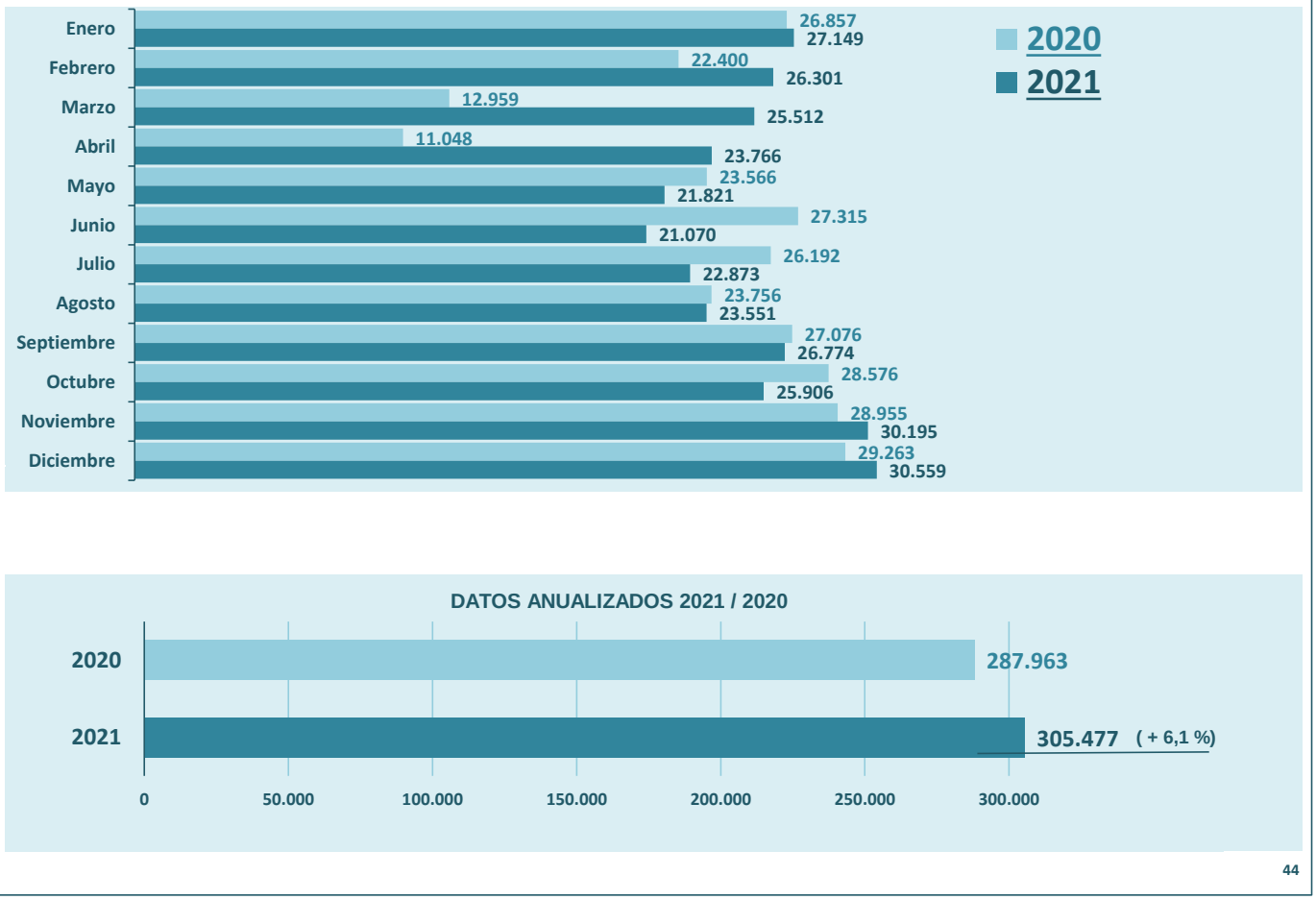
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.3. Distribución mensual de hechos conocidos. Año 2021

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	637	577	597	531	542	398	348	315	380	340	335	342	**5.342**
AMENAZAS Y COACCIONES	1.257	1.370	1.576	1.448	1.465	1.508	1.505	1.516	1.503	1.394	1.358	1.419	**17.319**
CONTRA EL HONOR	121	137	154	144	103	115	101	116	118	103	133	81	**1.426**
CONTRA PROPIEDAD INDUST./INTELEC.	14	18	14	10	7	12	15	2	12	12	10	11	**137**
DELITOS SEXUALES(*)	117	162	159	156	150	148	131	78	124	128	182	93	**1.628**
FALSIFICACIÓN INFORMÁTICA	1.077	1.096	940	885	915	751	693	658	813	828	899	921	**10.476**
FRAUDE INFORMÁTICO	23.688	22.720	21.752	20.330	18.419	17.984	19.963	20.752	23.702	22.986	27.156	27.559	**267.011**
INTERFERENCIA DATOS Y EN SISTEMA	238	221	320	262	220	154	117	114	122	115	122	133	**2.138**
Total HECHOS CONOCIDOS	**27.149**	**26.301**	**25.512**	**23.766**	**21.821**	**21.070**	**22.873**	**23.551**	**26.774**	**25.906**	**30.195**	**30.559**	**305.477**

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

>> 4.4. Comparativa de la distribución mensual de hechos conocidos 2021 / 2020



4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

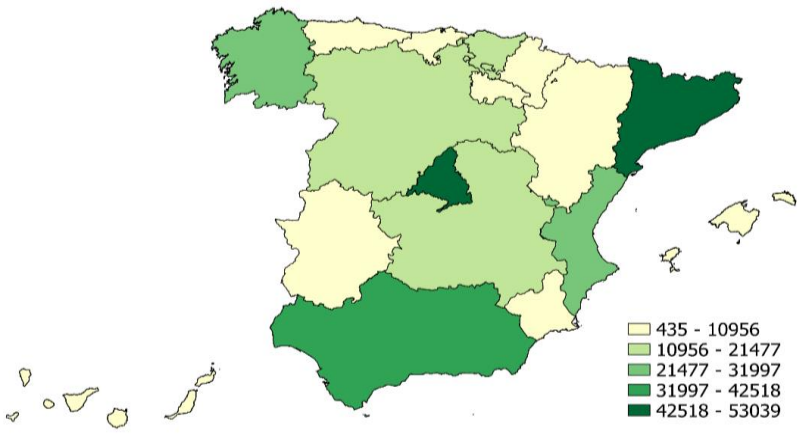
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2021

Hechos denunciados de CIBERCRIMINALIDAD - 2021

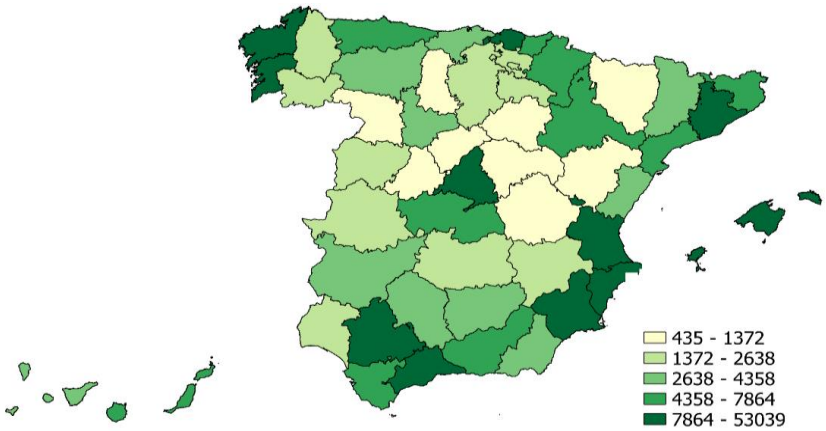
Hechos conocidos:	305.477	
Esclarecimiento (*):	46.141	**15,9%**
Detenciones/invest:	13.801	

CCAA	Hechos
MADRID (COMUNIDAD DE)	53.039
CATALUÑA	49.755
ANDALUCÍA	42.493
COMUNITAT VALENCIANA	29.508
GALICIA	22.010
PAÍS VASCO	16.798
CASTILLA Y LEÓN	16.680
CASTILLA - LA MANCHA	11.657
CANARIAS	10.875
ARAGÓN	8.461
BALEARS (ILLES)	8.294
MURCIA (REGIÓN DE)	8.009
ASTURIAS (PRINCIPADO DE)	6.906
EXTREMADURA	5.538
NAVARRA (COMUNIDAD FORAL DE)	4.362
EN EL EXTRANJERO	4.255
CANTABRIA	3.782
RIOJA (LA)	2.104
CIUDAD AUTÓNOMA DE CEUTA	516
CIUDAD AUTÓNOMA DE MELILLA	435



(*) 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 - 2021



Provincias más afectadas:	Hechos
Madrid	53.039
Barcelona	36.008
Valencia/València	16.679
Sevilla	10.357
Alicante/Alacant	10.133
Bizkaia	9.382
Málaga	8.894
Coruña (A)	8.888
Pontevedra	8.743
Balears (Illes)	8.294
Murcia	8.009
Cádiz	7.283
Asturias	6.906
Palmas (Las)	6.645
Zaragoza	6.463
Girona	5.624
Tarragona	4.865
Gipuzkoa	4.792
Granada	4.597
Toledo	4.572

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

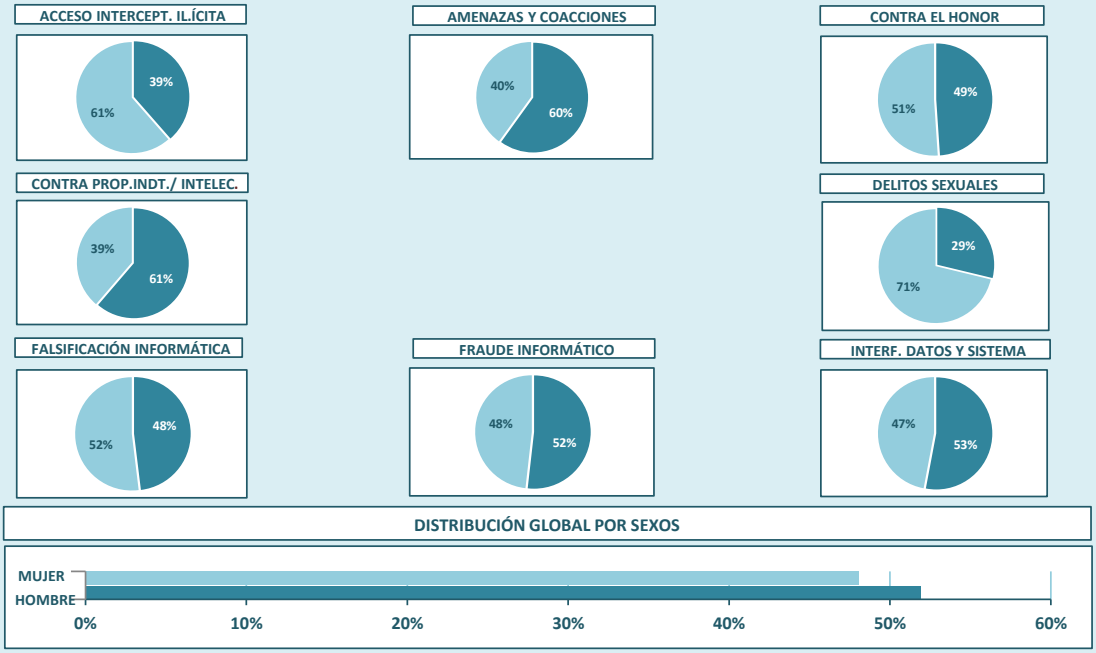
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales, excepto Ertzaintza)

>> 4.6. Victimizaciones registradas según grupo penal y sexo. Año 2021

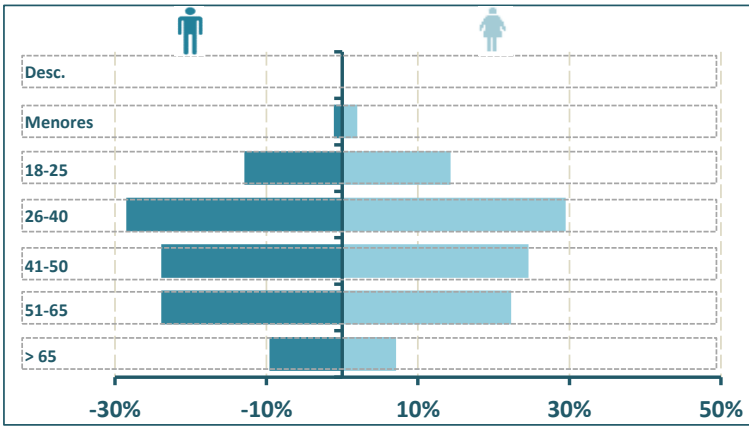
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.755	2.799	1	4.555
AMENAZAS Y COACCIONES	10.530	7.031	25	17.586
CONTRA EL HONOR	714	745	2	1.461
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	38	24	0	62
DELITOS SEXUALES (*)	340	842	16	1.198
FALSIFICACIÓN INFORMÁTICA	3.926	4.242	7	8.175
FRAUDE INFORMÁTICO	106.279	98.913	88	205.280
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	944	838	1	1.783
Total VICTIMIZACIONES	**124.526**	**115.434**	**140**	**240.100**

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

DISTRIBUCIÓN PORCENTUAL DE LAS VÍCTIMAS POR GRUPO PENAL SEGÚN SEXO



>> 4.7. Victimizaciones según grupo de edad y sexo. Año 2021



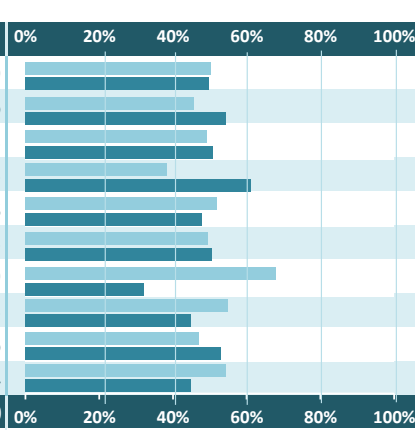
Grupo de edad	Hombre	Mujer	Descon.
Edad descon.	132	118	19
Menores de edad	1.396	2.320	17
De 18 a 25 años	16.091	16.509	4
De 26 a 40 años	35.437	34.096	11
De 41 a 50 años	29.762	28.448	29
De 51 a 65 años	29.775	25.785	42
Mayores 65 años	11.933	8.158	18
TOTAL	**124.526**	**115.434**	**140**

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

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

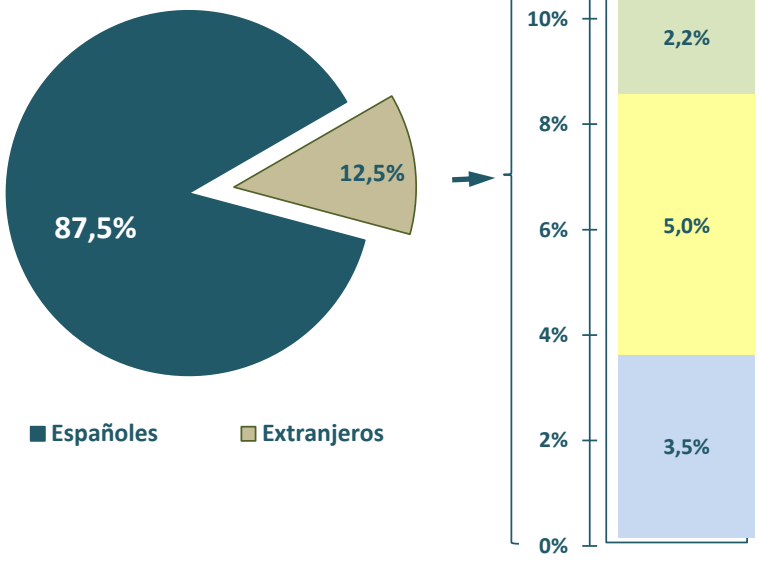
>> 4.8. Victimizaciones por tipología penal y sexo. Año 2021

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS TARJ CRÉD, DÉB. Y CHEQUES DE VIAJE	45.796	46.394	9	92.199
OTRAS ESTAFAS	45.114	37.797	65	82.976
ESTAFA BANCARIA	14.687	14.167	9	28.863
AMENAZAS	9.342	5.868	25	15.235
USURPACIÓN DE ESTADO CIVIL	3.911	4.230	7	8.148
COACCIONES	1.184	1.161	0	2.345
DESCUBRIMIENTO/REVELACIÓN DE SECRETO	734	1.554	1	2.289
ACCESO ILEGAL INFORMÁTICO	1.020	1.245	0	2.265
ATAQUES INFORMÁTICOS	923	823	0	1.746
RESTO	1.815	2.195	24	4.034
Total VICTIMIZACIONES	**124.526**	**115.434**	**140**	**240.100**



>> 4.9. Nacionalidad de la víctima. Año 2021

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	**210.198**	**87,5%**
2.- EXTRANJEROS	**29.902**	**12,5%**
2.1.- UNIÓN EUROPEA	**8.297**	**3,5%**
RUMANÍA	2.939	1,2%
ITALIA	1.560	0,6%
FRANCIA	764	0,3%
BULGARIA	695	0,3%
PORTUGAL	560	0,2%
Resto	1.779	0,7%
2.2.- AMÉRICA	**11.894**	**5,0%**
COLOMBIA	1.868	0,8%
VENEZUELA	1.731	0,7%
ECUADOR	1.321	0,6%
Resto	6.974	2,9%
2.3.- ÁFRICA	**5.241**	**2,2%**
MARRUECOS	3220	1,3%
SENEGAL	460	0,2%
Resto	1.561	0,7%
2.4.- ASIA	**1.897**	**0,8%**
CHINA POPULAR	626	0,3%
PAQUISTÁN	447	0,2%
Resto	824	0,3%
2.5.- RESTO PAÍSES	**2.573**	**1,1%**
UCRANIA	534	0,2%
REINO UNIDO	514	0,2%
Otros	1.525	0,6%
TOTAL	**240.100**	**100%**



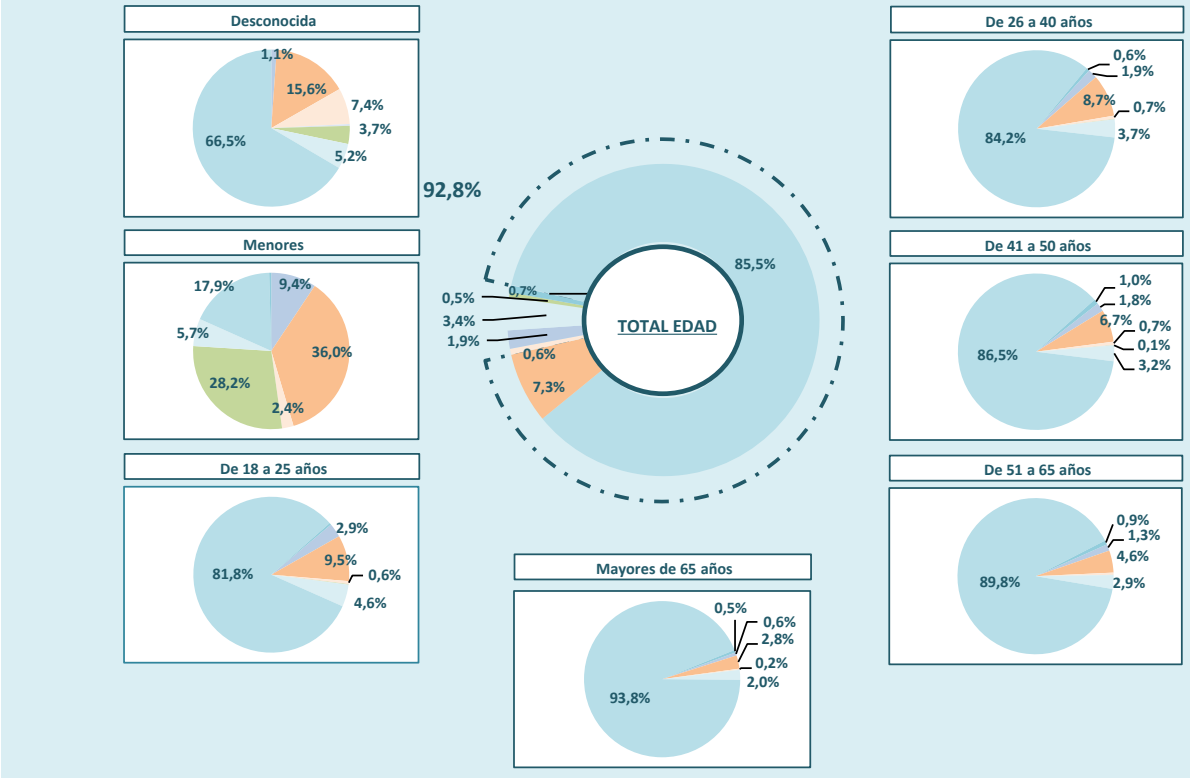
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

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

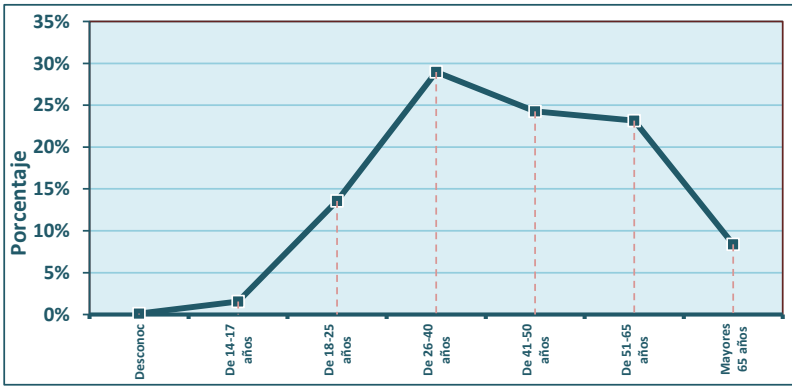
>> 4.10. Victimizaciones registradas según grupo penal y edad. Año 2021

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	350	944	1.341	1.039	748	130
AMENAZAS Y COACCIONES	42	1.345	3.111	6.072	3.907	2.555	554
CONTRA EL HONOR	20	89	201	470	394	244	43
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	14	26	17	2
DELITOS SEXUALES(*)	10	1.053	36	50	30	16	3
FALSIFICACIÓN INFORMÁTICA	14	212	1.494	2.561	1.892	1.590	412
FRAUDE INFORMÁTICO	179	668	26.684	58.587	50.357	49.949	18.856
INTERFERENCIA EN DATOS Y EN SISTEMA	0	16	132	449	594	483	109
Total VICTIMIZACIONES	**269**	**3.733**	**32.604**	**69.544**	**58.239**	**55.602**	**20.109**

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



>> 4.11. Edad de la víctima. Año 2021



Grupo de edad	Víctimas
Edad desconocida	269
Menores de edad	3.733
De 18 a 25 años	32.604
De 26 a 40 años	69.544
De 41 a 50 años	58.239
De 51 a 65 años	55.602
Mayores 65 años	20.109
TOTAL	**240.100**

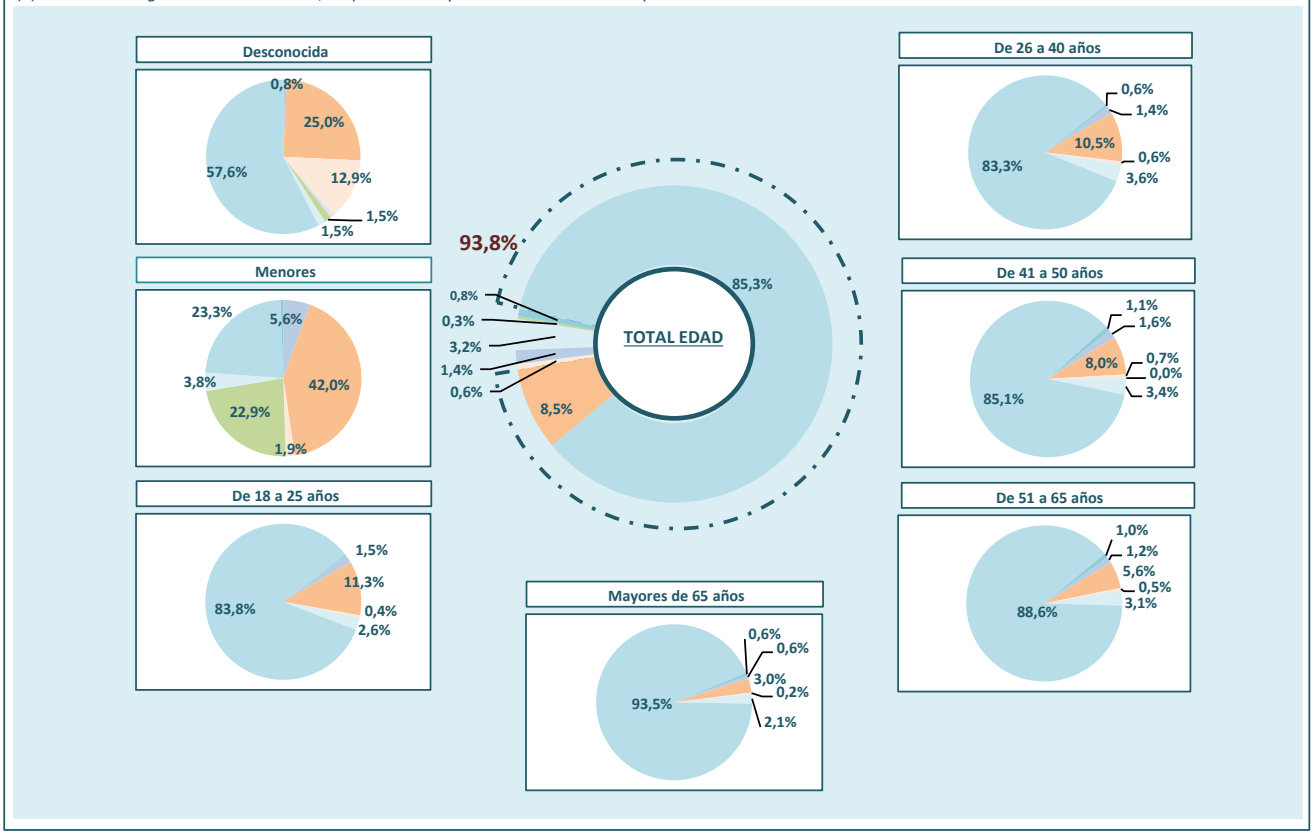
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (HOMBRE)

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

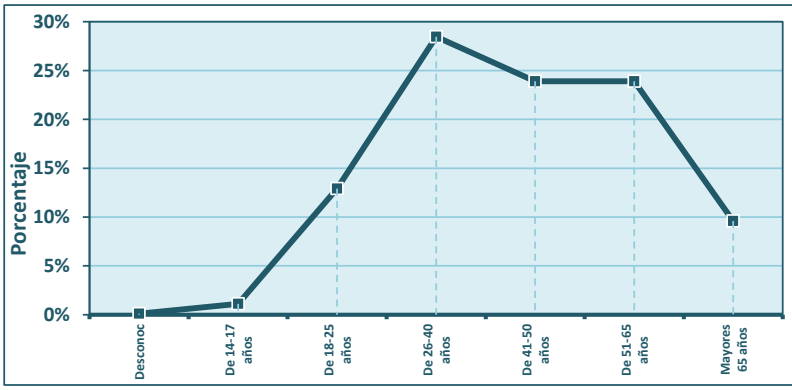
>> 4.12. Victimizaciones registradas según grupo penal y edad. Año 2021

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	78	239	512	484	368	73
AMENAZAS Y COACCIONES	33	587	1.819	3.704	2.377	1.657	353
CONTRA EL HONOR	17	26	72	218	213	141	27
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	0	7	15	15	0
DELITOS SEXUALES(*)	2	319	2	5	5	7	0
FALSIFICACIÓN INFORMÁTICA	2	53	420	1.274	1.014	917	246
FRAUDE INFORMÁTICO	76	325	13.487	29.517	25.325	26.387	11.162
INTERFERENCIA EN DATOS Y EN SISTEMA	0	8	52	200	329	283	72
Total VICTIMIZACIONES	**132**	**1.396**	**16.091**	**35.437**	**29.762**	**29.775**	**11.933**

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



>> 4.13. Edad de la víctima. Año 2021



Grupo de edad	Víctimas
Edad desconocida	132
Menores de edad	1.396
De 18 a 25 años	16.091
De 26 a 40 años	35.437
De 41 a 50 años	29.762
De 51 a 65 años	29.775
Mayores 65 años	11.933
TOTAL	**124.526**

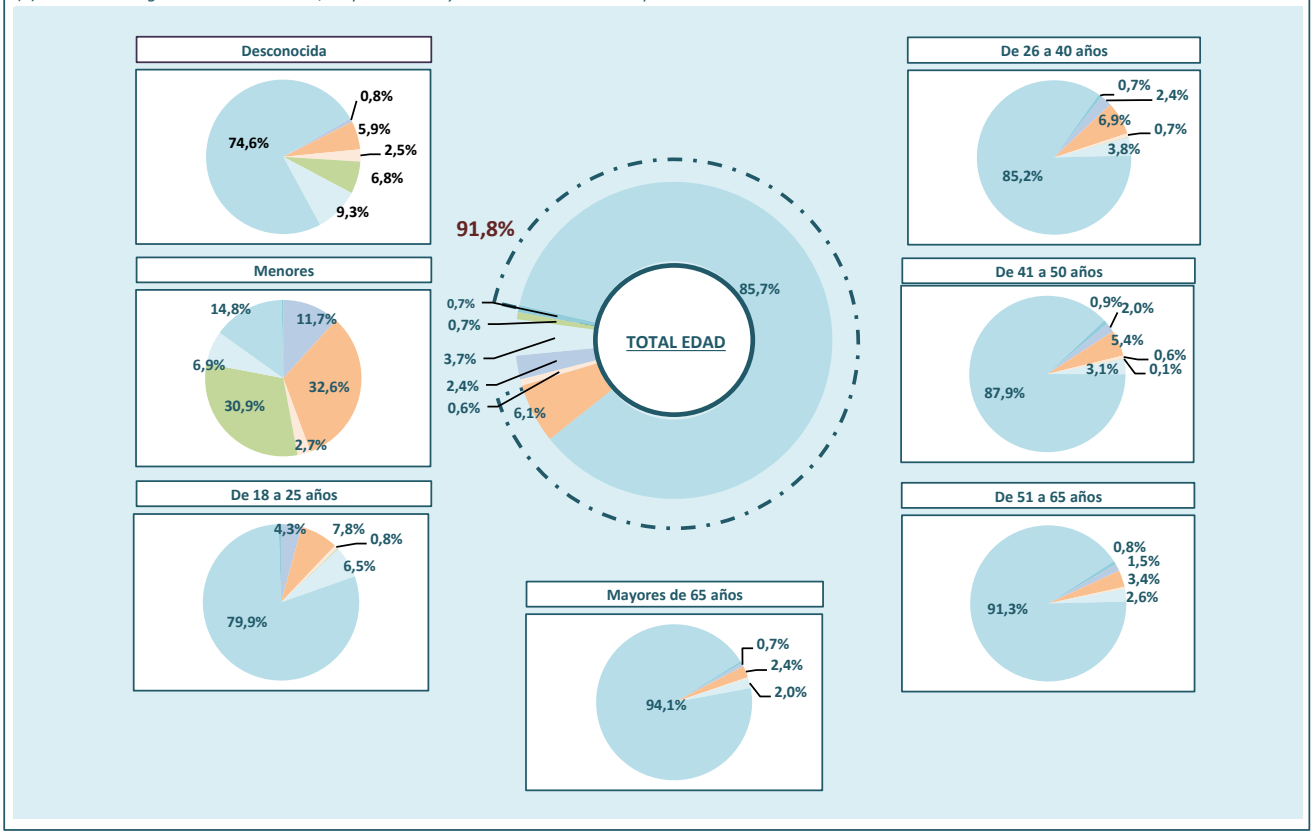
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (MUJER)

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

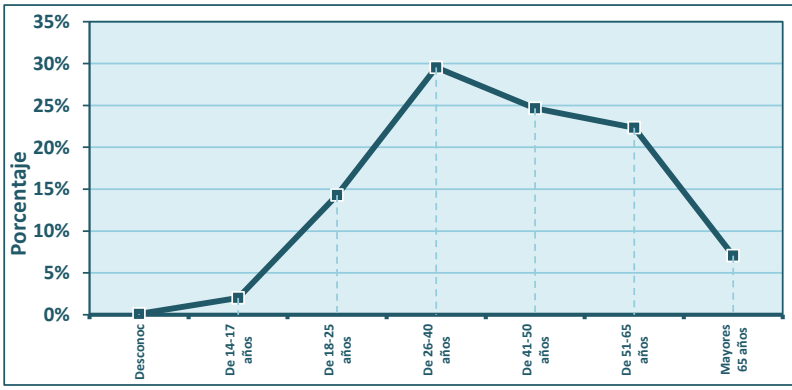
>> 4.14. Victimizaciones registradas según grupo penal y edad. Año 2021

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	272	705	829	555	380	57
AMENAZAS Y COACCIONES	7	757	1.291	2.366	1.524	888	198
CONTRA EL HONOR	3	63	129	252	180	102	16
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	7	11	2	2
DELITOS SEXUALES(*)	8	718	34	45	25	9	3
FALSIFICACIÓN INFORMÁTICA	11	159	1.073	1.287	877	670	165
FRAUDE INFORMÁTICO	88	343	13.195	29.061	25.011	23.535	7.680
INTERFERENCIA EN DATOS Y EN SISTEMA	0	8	80	249	265	199	37
Total VICTIMIZACIONES	**118**	**2.320**	**16.509**	**34.096**	**28.448**	**25.785**	**8.158**

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



>> 4.15. Edad de la víctima. Año 2021



Grupo de edad	Víctimas
Edad desconocida	118
Menores de edad	2.320
De 18 a 25 años	16.509
De 26 a 40 años	34.096
De 41 a 50 años	28.448
De 51 a 65 años	25.785
Mayores 65 años	8.158
TOTAL	**115.434**

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

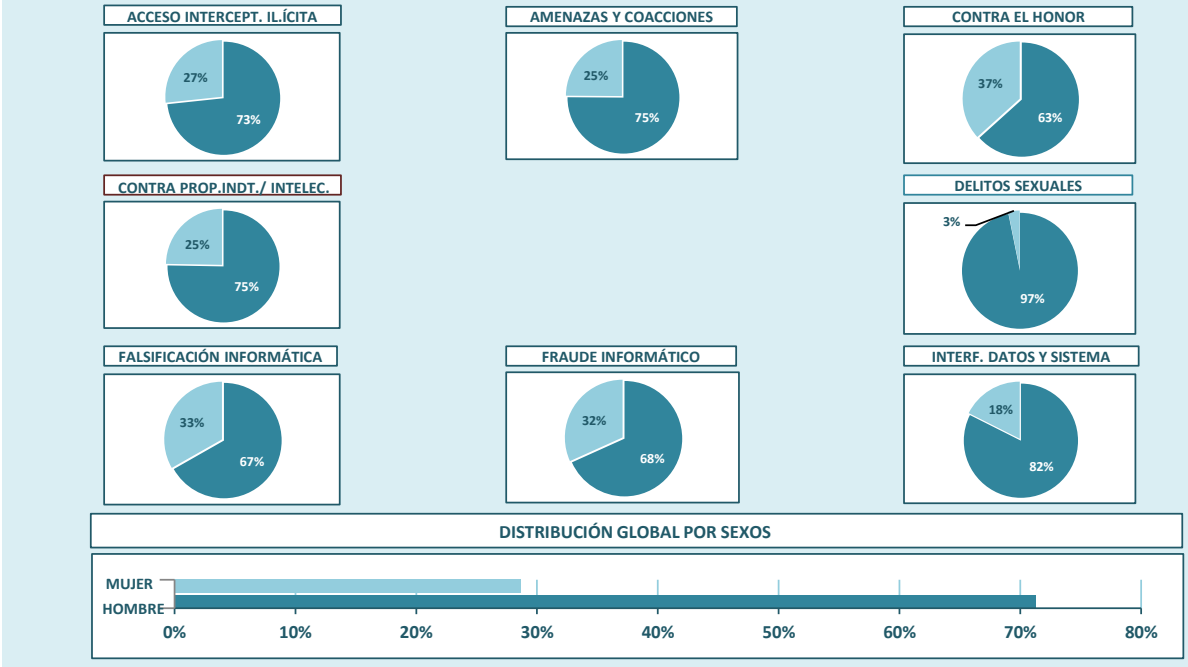
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 4.16. Detenciones/investigados registrados según grupo penal y sexo. Año 2021

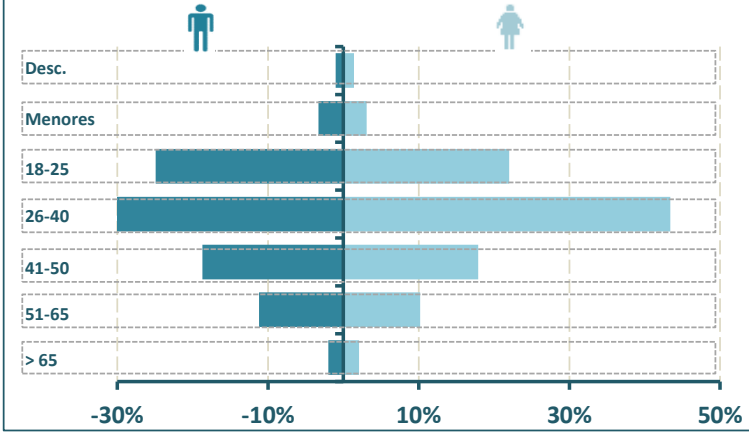
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	294	107	401
AMENAZAS Y COACCIONES	1.937	642	2.579
CONTRA EL HONOR	88	51	139
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	67	22	89
DELITOS SEXUALES(*)	728	24	752
FALSIFICACIÓN INFORMÁTICA	404	201	605
FRAUDE INFORMÁTICO	6.243	2.902	9.145
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	75	16	91
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**9.836**	**3.965**	**13.801**

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

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



>> 4.17. DETENCIONES/INVESTIGADOS según grupo de edad y sexo. Año 2021



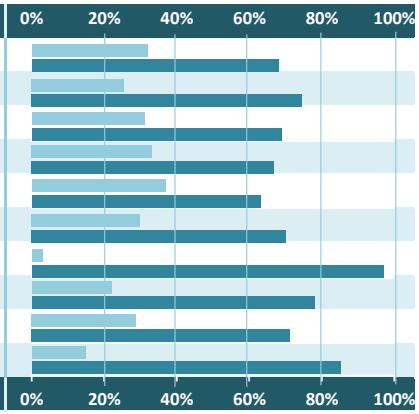
Grupo de edad	Hombre	Mujer
Edad desconocida	98	54
De 14 a 17 años	325	123
De 18 a 25 años	2.452	871
De 26 a 40 años	3.828	1.720
De 41 a 50 años	1.837	709
De 51 a 65 años	1.098	406
Mayores 65 años	198	82
TOTAL	**9.836**	**3.965**

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

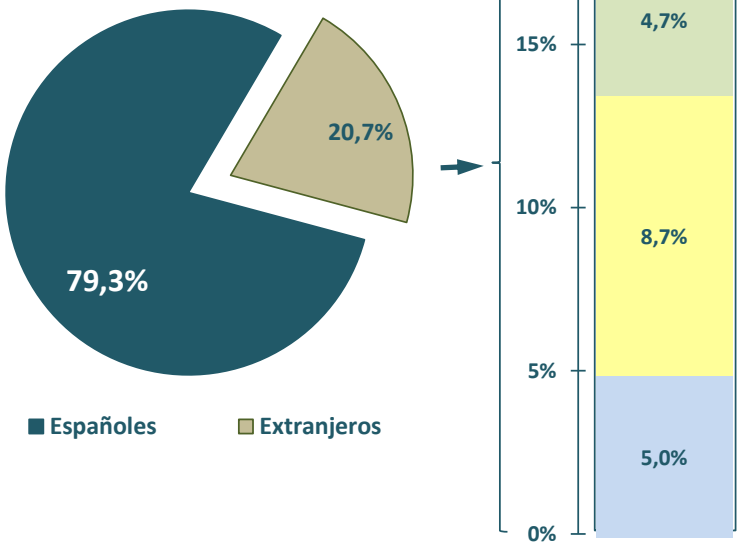
>> 4.18. Detenciones/investigados por tipología penal y sexo. Año 2021

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	4.538	2.126	6.664
AMENAZAS	1.631	555	2.186
ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQU	963	434	1.397
ESTAFAS INFORMÁTICAS	374	185	559
USURPACIÓN DE ESTADO CIVIL	333	195	528
ESTAFA BANCARIA	368	157	525
PORNOGRAFÍA DE MENORES	414	13	427
COACCIONES	305	86	391
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	243	98	341
RESTO	667	116	783
Total VICTIMIZACIONES CIBERCRIMINALIDAD	**9.836**	**3.965**	**13.801**



>> 4.19. Nacionalidad de los detenciones/investigados. Año 2021

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	**10.945**	**79,3%**
2.- EXTRANJEROS	**2.856**	**20,7%**
2.1.- UNIÓN EUROPEA	**687**	**5,0%**
RUMANÍA	288	2,1%
ITALIA	85	0,6%
BULGARIA	80	0,6%
PORTUGAL	57	0,4%
FRANCIA	56	0,4%
Resto	121	0,9%
2.2.- AMÉRICA	**1.201**	**8,7%**
DOMINICANA	263	1,9%
VENEZUELA	213	1,5%
COLOMBIA	206	1,5%
Resto	519	3,8%
2.3.- ÁFRICA	**653**	**4,7%**
MARRUECOS	407	2,9%
NIGERIA	42	0,3%
Resto	204	1,5%
2.4.- ASIA	**106**	**0,8%**
CHINA POPULAR	40	0,3%
PAQUISTÁN	36	0,3%
Resto	30	0,2%
2.5.- RESTO PAÍSES	**209**	**1,5%**
PAIS DESCONOCIDO	92	0,7%
UCRANIA	33	0,2%
Otros	84	0,6%
TOTAL	**13.801**	**100%**



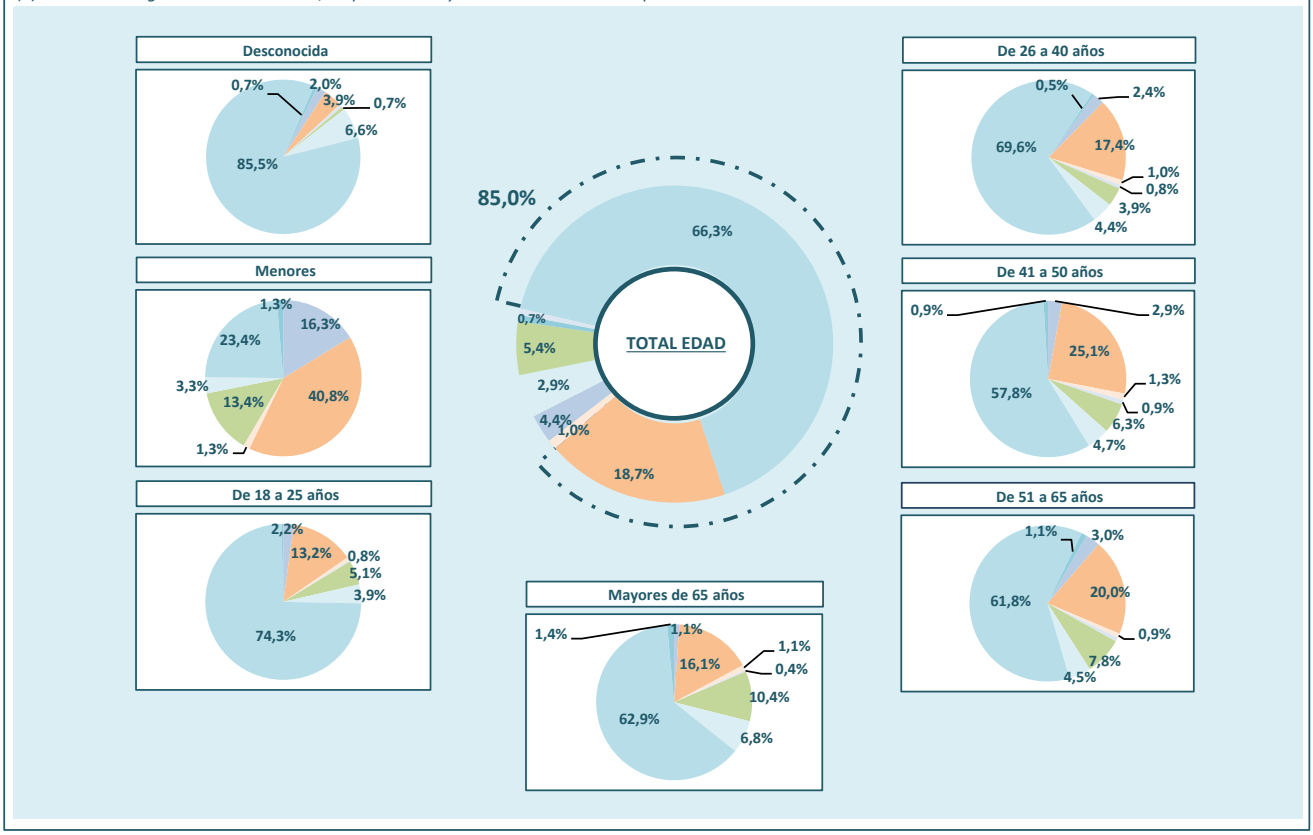
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

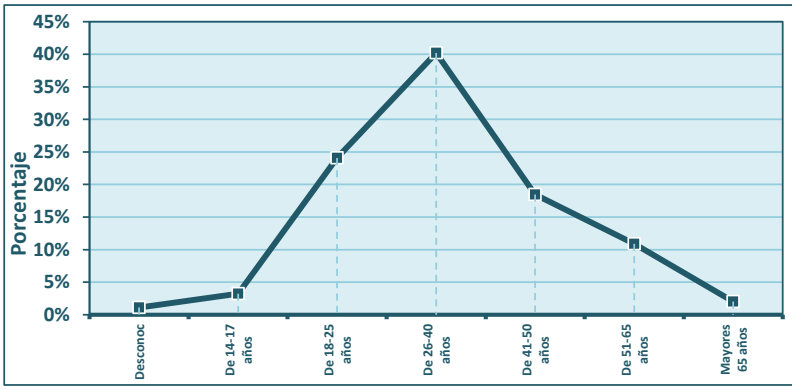
>> 4.20. Detenciones/investigados registradas según grupo penal y edad. Año 2021

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	3	73	72	132	73	45	3
AMENAZAS Y COACCIONES	6	183	439	965	640	301	45
CONTRA EL HONOR	0	6	25	58	34	13	3
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	7	43	24	13	1
DELITOS SEXUALES(*)	1	60	168	216	160	118	29
FALSIFICACIÓN INFORMÁTICA	10	15	130	244	119	68	19
FRAUDE INFORMÁTICO	130	105	2470	3863	1.472	929	176
INTERFERENCIA EN DATOS Y EN SISTEMA	1	6	12	27	24	17	4
Total DETENCIONES/INVESTIGADOS	**152**	**448**	**3.323**	**5.548**	**2.546**	**1.504**	**280**

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



>> 4.21. Edad de las personas detenidas/investigadas. Años 2021



Grupo de edad	Det./Inv.
Edad desconocida	152
De 14 a 17 años	448
De 18 a 25 años	3.323
De 26 a 40 años	5.548
De 41 a 50 años	2.546
De 51 a 65 años	1.504
Mayores 65 años	280
TOTAL	**13.801**

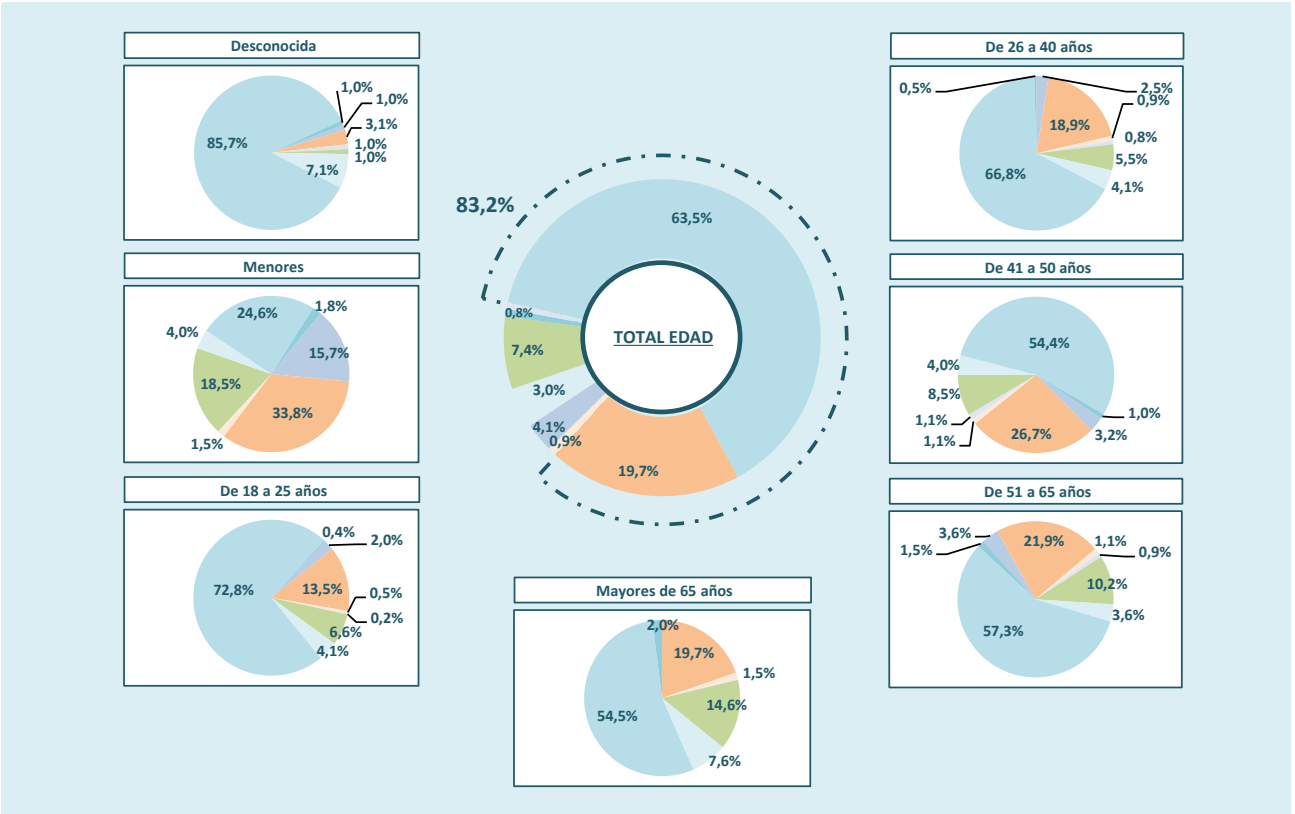
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

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

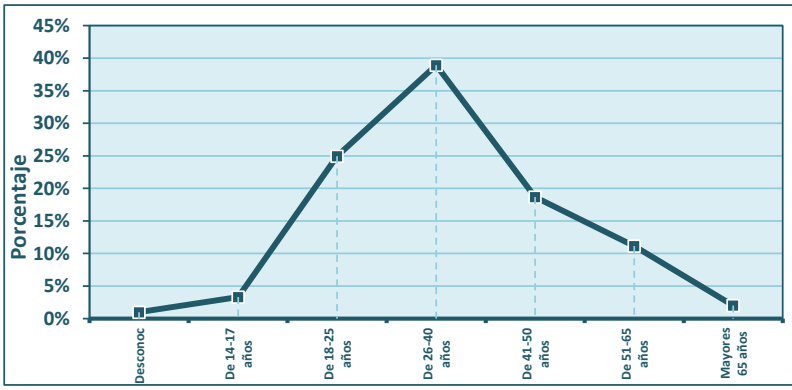
>> 4.22. Detenciones/investigados registradas según grupo penal y edad. Año 2021

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	51	50	95	58	39	0
AMENAZAS Y COACCIONES	3	110	331	723	490	241	39
CONTRA EL HONOR	0	5	13	35	20	12	3
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	4	31	21	10	0
DELITOS SEXUALES(*)	1	60	161	209	156	112	29
FALSIFICACIÓN INFORMÁTICA	7	13	100	156	74	39	15
FRAUDE INFORMÁTICO	84	80	1.784	2.559	999	629	108
INTERFERENCIA EN DATOS Y EN SISTEMA	1	6	9	20	19	16	4
Total DETENCIONES/INVESTIGADOS	**98**	**325**	**2.452**	**3.828**	**1.837**	**1.098**	**198**

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



>> 4.23. Edad de las personas detenidas/investigadas. Años 2021



Grupo de edad	Det./Inv.
Edad desconocida	98
De 14 a 17 años	325
De 18 a 25 años	2.452
De 26 a 40 años	3.828
De 41 a 50 años	1.837
De 51 a 65 años	1.098
Mayores 65 años	198
TOTAL	**9.836**

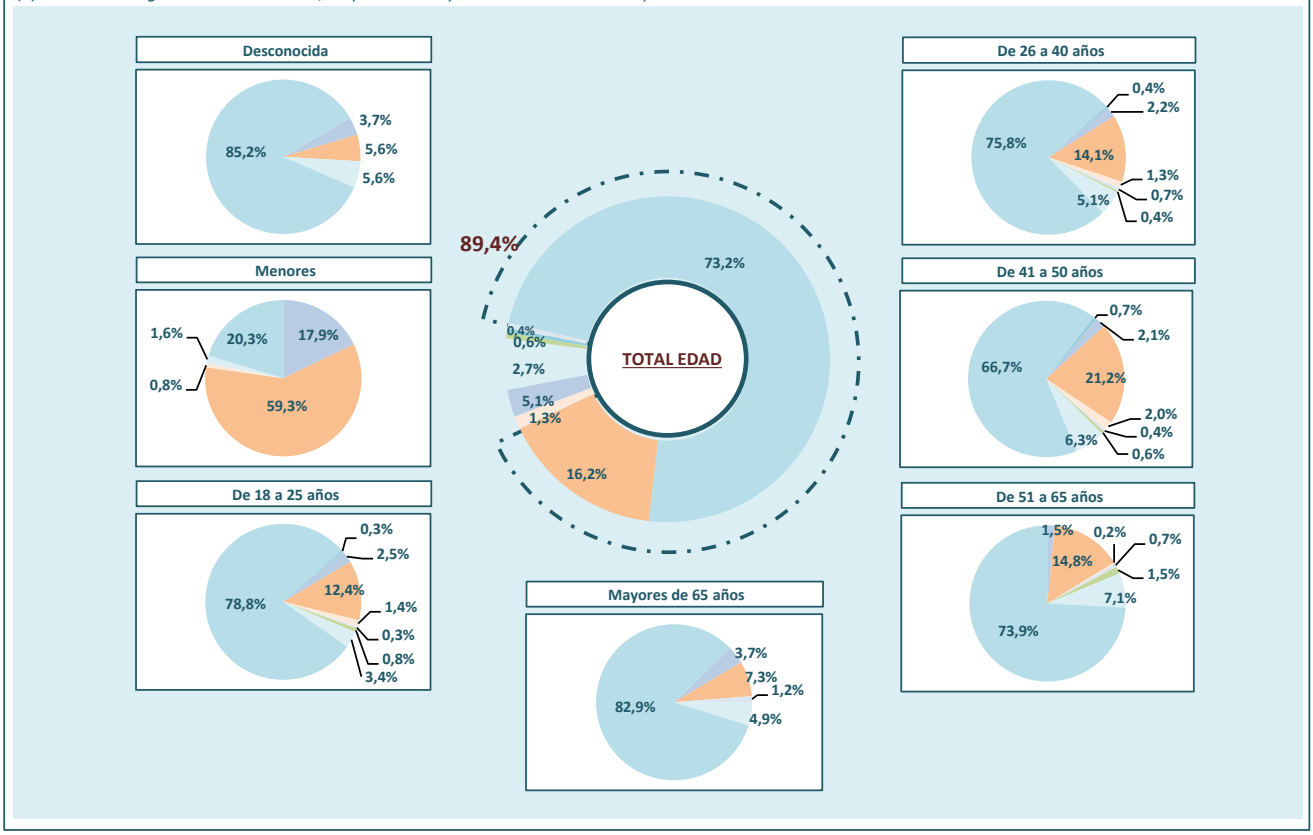
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

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

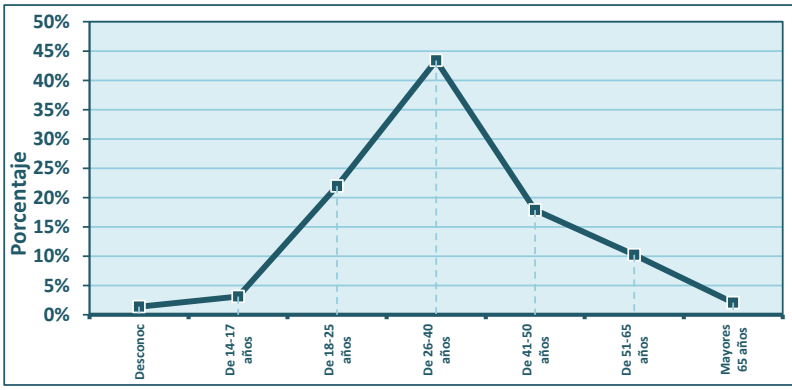
>> 4.24. Detenciones/investigados registradas según grupo penal y edad. Año 2021

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	2	22	22	37	15	6	3
AMENAZAS Y COACCIONES	3	73	108	242	150	60	6
CONTRA EL HONOR	0	1	12	23	14	1	0
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	3	12	3	3	1
DELITOS SEXUALES(*)	0	0	7	7	4	6	0
FALSIFICACIÓN INFORMÁTICA	3	2	30	88	45	29	4
FRAUDE INFORMÁTICO	46	25	686	1.304	473	300	68
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	3	7	5	1	0
Total DETENCIONES/INVESTIGADOS	**54**	**123**	**871**	**1.720**	**709**	**406**	**82**

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



>> 4.25. Edad de las personas detenidas/investigadas. Años 2021



Grupo de edad	Det./Inv.
Edad desconocida	54
De 14 a 17 años	123
De 18 a 25 años	871
De 26 a 40 años	1.720
De 41 a 50 años	709
De 51 a 65 años	406
Mayores 65 años	82
TOTAL	**3.965**

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

5

METADATA >>

5.- METADATA

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

>> Radiografía de la sociedad de la sociedad de la información

2.1-Hogares. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2021)

Porcentaje de viviendas con / sin algún tipo de ordenador

Porcentaje de viviendas con / sin acceso a Internet

Contraste evolutivo de las viviendas 2012-2021

Porcentaje de viviendas con ordenador por tipo hábitat

Porcentaje de viviendas con acceso a Internet por tipo hábitat

https://www.ine.es/jaxi/Tabla.htm?tpx=50092&L=0

2.2.-Perfil del ciudadano ante la sociedad de la información. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2021)

Porcentaje de personas que han utilizado o no Internet últimos 3 meses.

Porcentaje por sexo de personas que han utilizado Internet últimos 3 meses.

Porcentaje por grupo de edad de personas que han utilizado Internet últimos 3 meses.

https://www.ine.es/jaxi/Tabla.htm?tpx=50093&L=0

2.3.-Perfil del menor de edad (10 a 15 años de edad) ante la sociedad de la información. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2021)

Porcentaje de menores que han utilizado ordenador últimos 3 meses.

Porcentaje por sexo de menores que han utilizado ordenador últimos 3 meses.

Porcentaje de menores que han utilizado Internet últimos 3 meses.

Porcentaje por sexo de menores que han utilizado Internet últimos 3 meses.

https://www.ine.es/jaxi/Tabla.htm?tpx=50095&L=0

2.4.-Perfil de las personas que han comprado alguna vez por Internet. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2021)

Porcentaje personas que han comprado alguna vez por Internet últimos 3 meses.

https://www.ine.es/jaxi/Tabla.htm?tpx=50094&L=0

Porcentaje por sexo de personas que han comprado alguna vez por Internet.

Porcentaje por grupo de edad de personas que han comprado alguna vez por Internet

https://www.ine.es/jaxi/Tabla.htm?tpx=50093&L=0

2.5.- Comparativa internacional. Viviendas con acceso a Internet (Fuente datos: EUROSTAT)

Porcentaje de viviendas con acceso a Internet. ICT usage in households and by individuals. Connection to the Internet and computer use. Households - level of Internet Access (EUROSTAT)

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en

2.6. Índice de Economía y Sociedad Digital (DESI). Comparativa España-Unión Europea

Digital Economy and Society Index 2021. Spain

https://administracionelectronica.gob.es/pae_Home/dam/jcr:580a4fc8-a552-448e-b89b-cd2f88ec0b5c/DESI_2021_Spain_es.pdf

>> 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. Con respecto a las victimizaciones sólo existen disponibles datos para este Cuerpo policial a partir del año 2021.

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

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

de información y comunicación (TIC), se pueden encuadrar dentro de los delitos tecnológicos las siguientes tipologías delictivas:

- Delitos contra el honor.
- 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 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 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).

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).

Hay que significar, que como se ha reseñado anteriormente, la Ertzaintza facilita datos de victimizaciones a partir del año 2021.

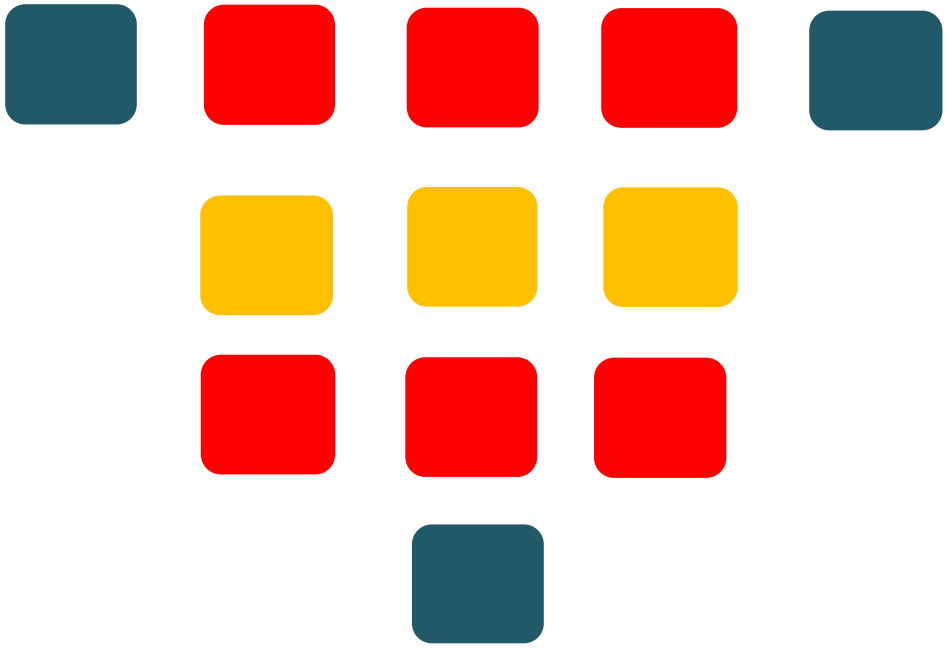
MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	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	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ACCESO ILEGAL INFORMÁTICO	Ninguna
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	DAÑOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ATAQUES INFORMÁTICOS	Ninguna
Falsificación informática	Arts CP 388-389, 399 bis, 400 y 401	FALSIFICACION DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE UTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude Informático	Arts. CP 248 a 251 y 623.4	ESTAFA BANCARIA	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE VIAJE	
		OTRAS ESTAFAS	
Delitos sexuales	Arts. CP 181, 183.1, 183.bis, 184, 185, 186, 189	EXHIBICIONISMO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		PROVOCACIÓN SEXUAL	
		ACOSO SEXUAL	
		ABUSO SEXUAL	
		CORRUPCIÓN DE MENORES/INCAPACITADOS	
		PORNOGRAFIA DE MENORES	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP(Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		INJURIAS	
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	AMENAZAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	
		COACCIONES	

- **ÍNDICE DE ABREVIATURAS EMPLEADAS EN EL INFORME:**

CCN	Centro Criptológico Nacional
CEPOL	Escuela Europea de Policía
DESI	Índice de Economía y Sociedad Digital
DMA	Ley de Mercados Digitales
DSA	Ley de Servicios Digitales
EC3	Centro Europeo de Ciberdelincuencia de Europol
EE.UU.	Estados Unidos
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
EPE	Plataforma de Expertos de Europol
ESN	Estrategia de Seguridad Nacional
EUCTF	Grupo de trabajo sobre ciberdelincuencia de la Unión Europea
EU-CYCLONe	Red Europea de Organización de Enlace de Crisis Cibernéticas
EUROPOL	Agencia de la Unión Europea para la Cooperación Policial
EUROSTAT	Oficina Estadística Europea
INCIBE-CERT	Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad
INE	Instituto Nacional de Estadística
IOCTA	Internet Organised Crime Threat Assessment
J-CAT	Grupo de trabajo conjunto de acción contra el ciberdelito
OCC	Oficina de Coordinación de Ciberseguridad
PES	Programa Estadístico de Criminalidad
PESC	Política Exterior y de Seguridad Común
SEC	Sistema Estadístico de Criminalidad
SPACE	Secure Platform for Accredited Cybercrime Experts
TIC	Tecnologías de la información y las comunicaciones
UE	Unión Europea

ESPAÑA



2021

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

2021