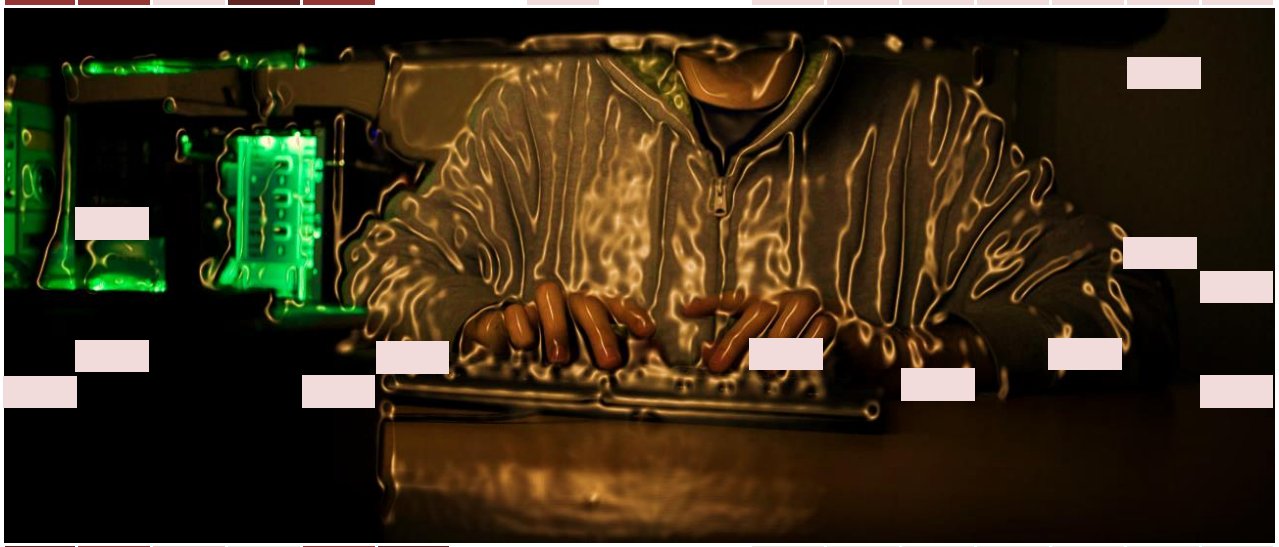
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS

Sistema Estadístico de Criminalidad

2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



AUTORES

DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS
SECRETARÍA DE ESTADO DE SEGURIDAD

JAVIER LÓPEZ GUTIÉRREZ
FRANCISCO SÁNCHEZ JIMÉNEZ
DAVID HERRERA SÁNCHEZ
FRANCISCO MARTÍNEZ MORENO
MARCOS RUBIO GARCÍA
VICTORIA GIL PÉREZ
ANA Mª SANTIAGO OROZCO
MIGUEL ÁNGEL GÓMEZ MARTÍN

Edita:

MINISTERIO DEL INTERIOR — SECRETARÍA GENERAL TÉCNICA

NIPO 126-20-021-2

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

0 INDICE

1. Introducción 4

2. Radiografía de la sociedad de la información 26

3. Infraestructuras críticas y ciberseguridad 34

4. Datos estadísticos de cibercriminalidad 40

5. Metadata 54

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

Sistema Estadístico de Criminalidad

2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1

INTRODUCCIÓN >>

1.- INTRODUCCIÓN

La ciberdelincuencia 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 ***VIII Informe sobre Cibercriminalidad***, correspondiente a la delincuencia informática registrada en el año 2020.

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. Por segunda vez se aúnan en este tipo de informe los **datos de todos los cuerpos policiales del territorio nacional** (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y distintos Cuerpos de Policía Local), tanto en la vertiente de los hechos conocidos como de las detenciones e investigados. Por dicha razón, se han reconstruido y actualizado en el presente Informe los datos de las series históricas.

Para el capítulo de victimizaciones, con la excepción de la Ertzaintza, se detallan igualmente datos de todas las Fuerzas y Cuerpos de Seguridad. Es por ello, que las series históricas publicadas hasta la fecha, se han visto modificadas, como consecuencia del nuevo suministro de datos por estos cuerpos policiales referenciados anteriormente.

Los datos proceden del Sistema Estadístico de Criminalidad (SEC), y de los incidentes que registra la Oficina de Coordinación de Ciberseguridad, 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 2020 no solo en relación a la información estadística sobre delitos informáticos en nuestro país, sino, además, en un primer apartado y a modo introductorio, una serie de informaciones publicadas por otros organismos nacionales (INE) e internacionales (EUROSTAT, Comisión Europea).

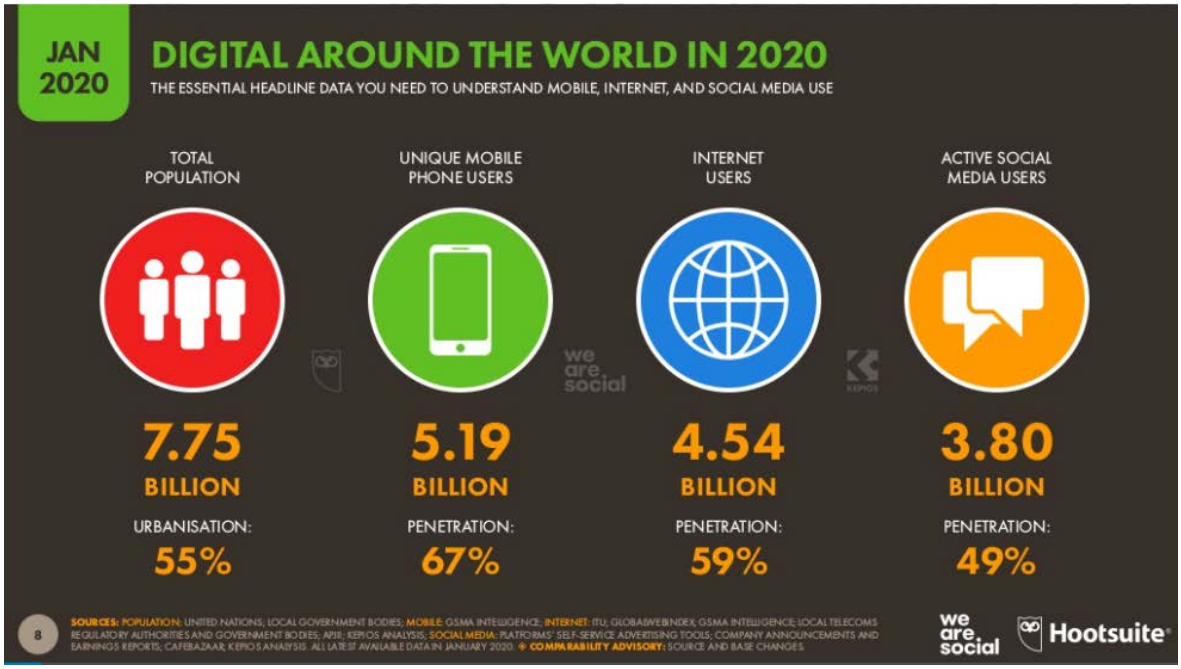
En el segundo y tercer bloque del Informe se explican los datos procedentes de la Oficina de Coordinación de Ciberseguridad, así como los extraídos del Sistema Estadístico de Criminalidad (SEC), registrados por las Fuerzas y Cuerpos de Seguridad. Información que es desglosada en diferentes apartados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

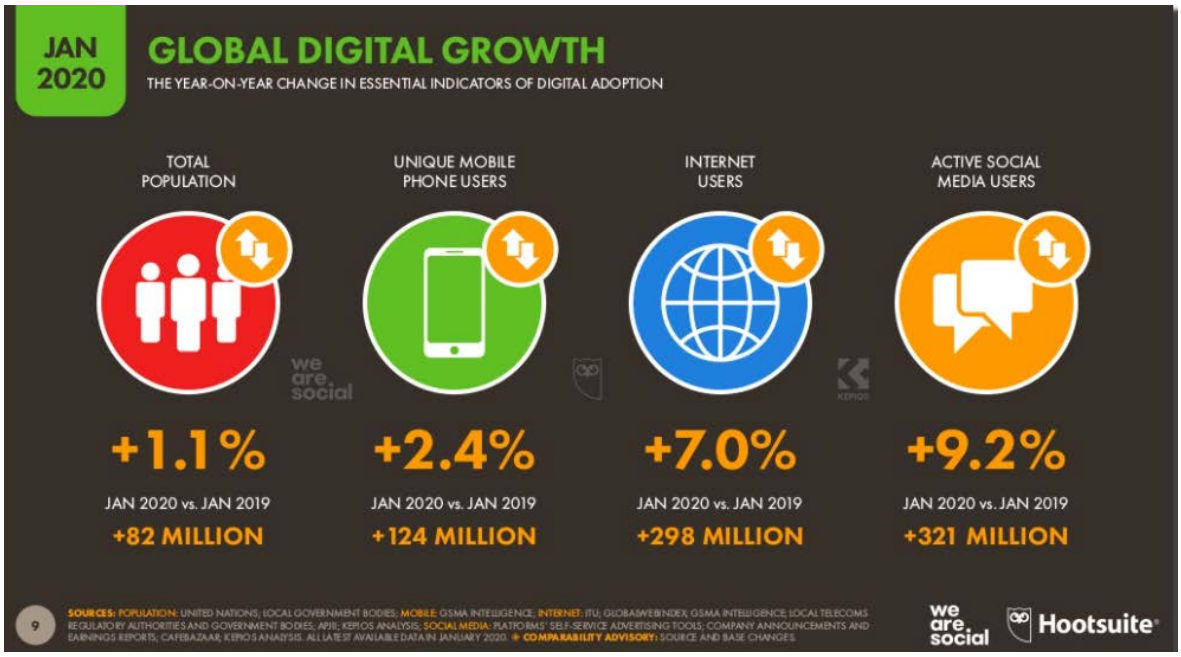
La tipificación de las conductas sigue las mismas conceptuaciones que emplea el Convenio de Budapest[1], a los que se le ha añadido por el volumen y la importancia de la cifra registrada, las siguientes infracciones penales: *a)* delitos contra el honor; *b)* amenazas y *c)* coacciones.

Como primer aspecto a destacar, cabe poner de relieve el alto índice de uso de las nuevas tecnologías. Para tener una visión global a nivel mundial de esta afirmación, podemos referenciar al *Digital Report 2020: Global Digital Overview*.

[1] Véase el Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 («BOE» núm. 226, de 17 de septiembre de 2010).



Infografía nº 1.- Usuarios de nuevas tecnologías a nivel mundial[2].



Infografía nº 2.- Incremento de usuarios de nuevas tecnologías a nivel mundial[3].

Como se puede comprobar en la infografía nº 1, existe un 55% de penetración de los usuarios de internet a nivel mundial. Tan sólo en el último año (2020), se ha visto

[2] https://wearesocial.com/digital-2020
[3] https://wearesocial.com/digital-2020

incrementado en casi +300 millones de personas el número total de usuarios de internet (ver infografía número dos).

Infografía nº 3.- Incremento de usuarios de nuevas tecnologías a nivel mundial[4].

En relación a la situación de España respecto al resto de países, se observa que ocupamos el puesto número 18 a nivel mundial, según el incremento experimentado de usuarios de internet durante el último año. Hay que poner de relieve, que los primeros puestos de esta clasificación, están ocupados por países con mayor déficit en infraestructuras que el resto de países más industrializados.

Durante el pasado año 2020, y según el Centro Criptológico Nacional (Informe Ciberamenazas y tendencias Edición 2020[5]), muchos de los aspectos relacionados con la cibercriminalidad, se han visto íntimamente relacionados con la COVID-19. Las principales conclusiones que se pueden extraer del informe elaborado por este organismo son las siguientes:

- La situación provocada por la pandemia ha supuesto un elemento disruptivo que ha propiciado el incremento de numerosos y variados ataques. Esta situación ha influido, desde múltiples puntos de vista, en el panorama de la ciberseguridad global; en especial, ha sido aprovechado por actores hostiles para, al amparo de la

[4] https://wearesocial.com/digital-2020
[5] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

situación sufrida, potenciar desde operaciones de influencia o robo de información hasta campañas de *ransomware*.

- Incremento de las acciones ligadas a actores Estado en el ámbito de las operaciones de influencia, propaganda, desinformación, etcétera.

- Mejora significativa de las capacidades técnicas y operativas de actores ligados a la delincuencia económica (*fraude al CEO, Human Operated Ransomware*[6], etc.).

- Incremento de los impactos contra sistemas ciberfísicos, bien como objetivo final, bien como daño colateral en ataques a infraestructura IT.

- Explotación de sistemas expuestos a internet por todo tipo de actores, hecho que se ha visto incrementado por la situación de pandemia y el incremento del teletrabajo (y la exposición no controlada de muchas organizaciones a Internet).

- Refuerzo de la normativa y regulación del ámbito de la seguridad, tanto en España como en el panorama internacional.

- Necesidad, y tendencia, de los elementos ligados a inteligencia artificial en el ámbito de la seguridad, tanto para los atacantes como para los defensores.

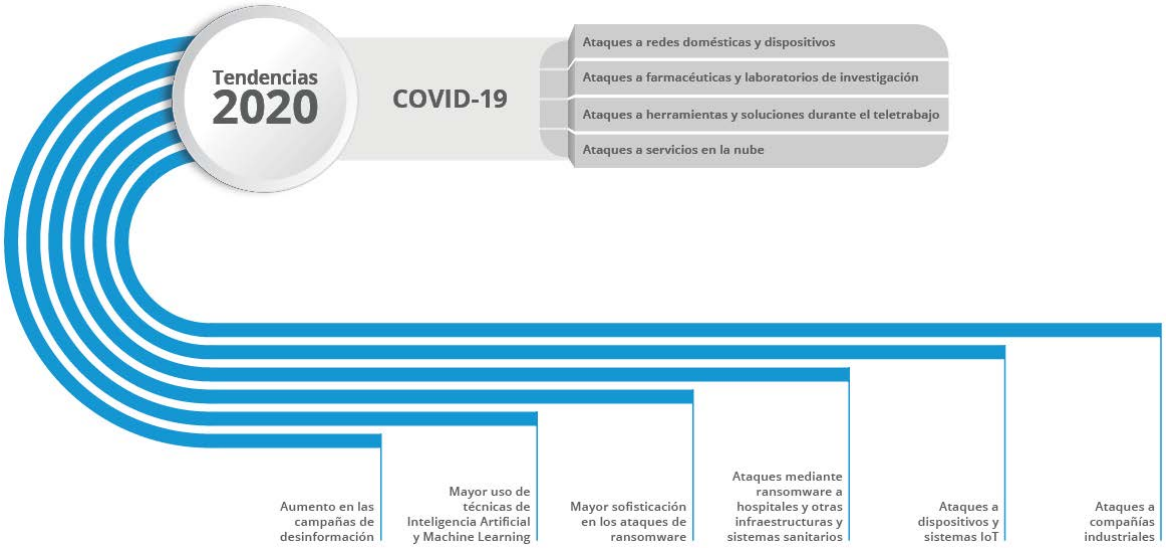
En cuanto a las tendencias previstas a corto plazo, tal y como señala el mismo documento, la pandemia de la COVID-19 seguirá marcando muchas de las amenazas y riesgos en los próximos meses, muchos de estos directamente relacionados con el aumento del teletrabajo. En este sentido, el mayor uso de soluciones en la nube, conexiones VPN, servicios de escritorio remoto virtual (VDI), redes de confianza cero y gestión de identidades, servicios y tecnologías para el acceso remoto, uso de herramientas colaborativas, aplicaciones de videoconferencia, etcétera, generará que los ataques a estos entornos, en especial a los sistemas públicamente expuestos, sigan creciendo.

Por otro lado, es previsible que los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales se incrementen. El objetivo no será otro que

[6] En estos enlaces webs se explicitan las acciones cometidas por estas formas delictivas de cibercriminalidad: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo https://docs.microsoft.com/es-es/security/compass/human-operated-ransomware#:~:text=Las%20caracter%C3%ADsticas%20distintivas%20de%20un,Estos%20ataques%20pueden%20ser%20catastr%C3%B3ficos.

acceder a la infraestructura de la organización del empleado para conseguir diferentes fines, entre los que el ciberespionaje será uno de los principales.

Por último, y también en el marco de la pandemia, es de esperar que los ataques a farmacéuticas, laboratorios de investigación dedicados a la COVID-19 o víctimas relacionadas con el sector, aumenten.



Infografía nº 4.- Ciberamenazas y tendencias. Fuente: CCN-CERT.

Por otro lado, Interpol ha analizado el efecto de la Covid-19 en la ciberdelincuencia[7]. En el caso concreto de Europa ha destacado cuatro conclusiones principales:

- Dos tercios de los países miembros de Europa han informado del considerable aumento de dominios maliciosos registrados con las palabras clave "COVID" o "corona" para sacar partido del número creciente de personas que buscan información en Internet sobre la COVID-19.

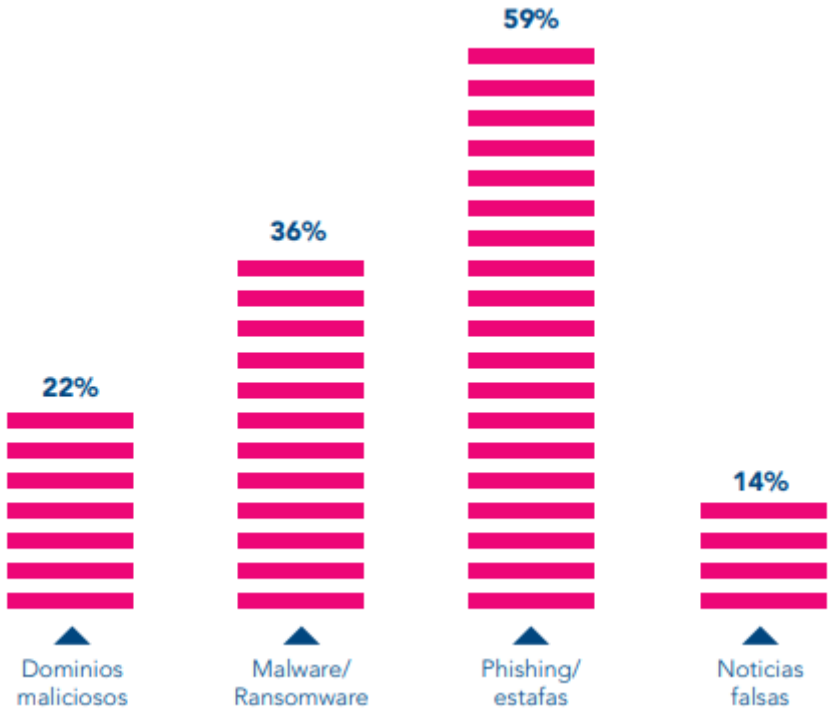
- Los ciberdelincuentes están aprovechando la pandemia para lanzar ataques de *ransomware* contra las infraestructuras esenciales e instituciones sanitarias encargadas de hacer frente a la COVID-19.

[7] https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

- Cada vez hay más casos de clonación de sitios web gubernamentales para robar datos confidenciales de usuarios y después utilizarlos en otros ciberataques.

- Los organismos encargados de la aplicación de la ley europeos han registrado una proliferación de las campañas de *phishing*.

Asimismo, Interpol sobre la base del exhaustivo análisis de los datos facilitados por los países miembros, los socios privados, y el Centro de Intercambio de Información sobre la Ciberdelincuencia, ha determinado cuales son las principales ciberamenazas identificadas en relación con la pandemia de la COVID-19.



Infografía nº 4.- Proporción de las principales ciberamenazas relacionadas con la COVID-19. Fuente: Interpol.

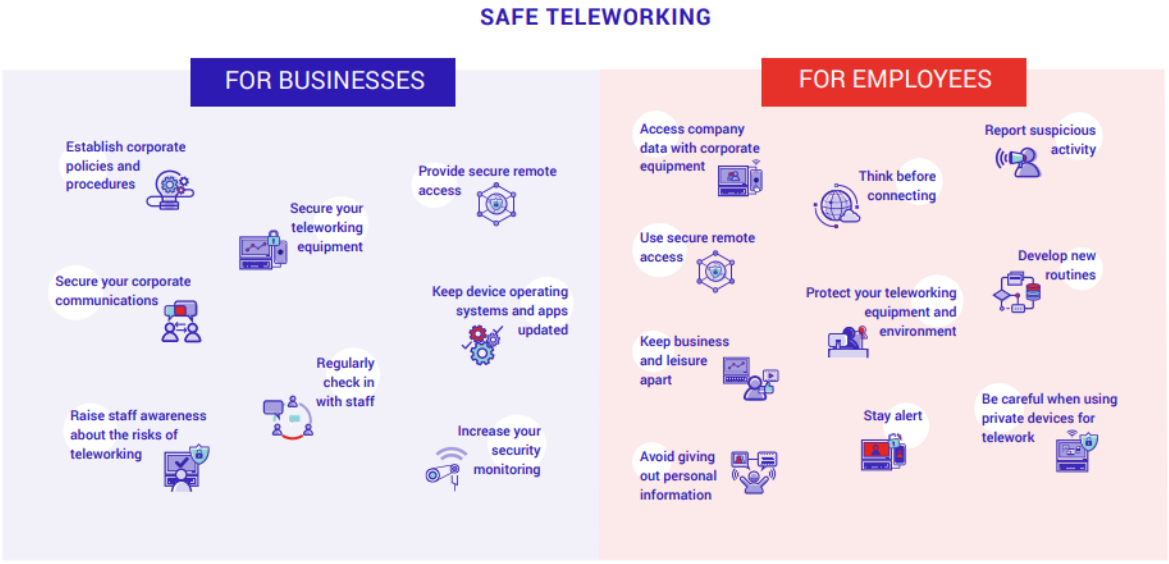
Es de destacar, que hay ciertos fenómenos que presentan disminución respecto a los años precedentes, como es el caso del *hacktivismo*. Según el CCN-CERT[8] durante 2020 se mantuvo la tendencia, ya reportada en años previos, de un *hacktivismo* desideologizado y oportunista, actuando preferentemente motivado por el exhibicionismo egocéntrico de

[8] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5933-ccn-cert-ia-17-21-informe-anual-2020-hacktivismo-y-ciberyihadismo-1/file.html

atacantes que vulneran sitios web para inyectar sobre ellos su firma. Este *hacktivismo* individualista de oportunidad se ha concentrado durante 2020 principalmente en desfigurar webs privadas de personas o de pequeños negocios.

No obstante, según el CCN-CERT se observa una deriva peligrosa, por cuanto se viene desarrollando una derivación del *hacktivismo* hacia la pequeña cibercriminalidad con ánimo de lucro ilícito. Esta posibilidad viene avalada porque, al menos en los últimos tres años, se está documentando que incidentes por desfiguración de sitios web se realizan, además de para inyectar una firma *hacktivista* del atacante, infectar esos sitios con código software malicioso, generalmente al servicio de la práctica conocida como *SEO Spam*.

Relacionado con la pandemia generada por la COVID-19, uno de los aspectos que ha podido influir en las tendencias sobre cibercriminalidad, está relacionado con el aumento del teletrabajo tanto en el sector público como en el privado. Es necesario que todos los organismos públicos y privados realicen una revisión de las políticas de seguridad, con el fin de intentar limitar los accesos ilegales por terceros. En este sentido, hay una serie de recomendaciones básicas que algunos organismos europeos (como Europol[9]) han elaborado al respecto.



Infografía nº 5.- Consejos para un teletrabajo seguro. Fuente: IOCTA 2020 (Europol).

9 https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Relacionado con los avances tecnológicos, una de las técnicas más habituales que están usando los ciberdelincuentes contra las empresas es el uso de *ransomware*. Como se puede ver en la imagen siguiente, se exige el pago de una cantidad para o bien no desvelar secretos empresariales o tener "secuestrado" la actividad normal.

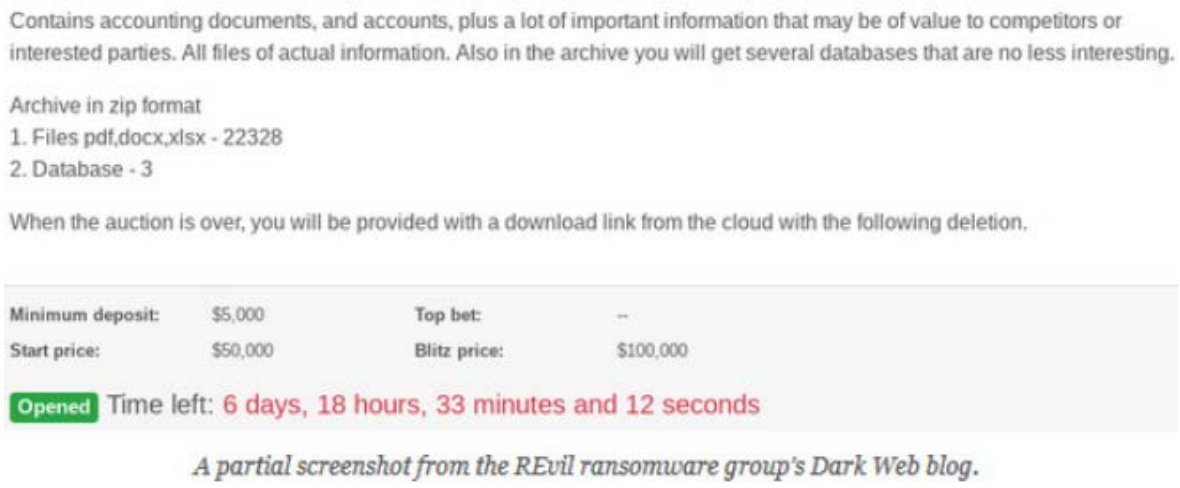


Imagen nº 6.- Captura de pantalla de una sesión de subasta de datos en línea.
Fuente: IOCTA 2020 (Europol).

No cabe duda, que la actuación de los Poderes Públicos tiene que avanzar en la articulación de mecanismos que coadyuven a disminuir cualquier factor que afecte a la seguridad pública, como es el caso que nos ocupa de la cibercriminalidad. Para ello, y entre otras medidas, en abril de 2021, el Consejo de la Unión Europea dio luz verde a la creación de un Centro de Competencia en Ciberseguridad para poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad. El nuevo organismo, que tendrá su sede en Bucarest (Rumanía), canalizará la financiación relacionada con la ciberseguridad de Horizonte Europa y del programa Europa Digital (2021-2027).

Este Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad trabajará de forma conjunta con una Red de Centros Nacionales de Coordinación designados por los Estados miembros.

El Centro también reunirá a las principales partes interesadas europeas, entre ellas la industria, las organizaciones académicas y de investigación y otras asociaciones pertinentes de la sociedad civil, para formar una Comunidad de Competencias en

Ciberseguridad, con el fin de reforzar y difundir los conocimientos especializados en materia de ciberseguridad en toda la Unión Europea[10].

En el ámbito nacional, se vienen desarrollando una serie de medidas entre las que cabe mencionar las siguientes:

1. Constitución del Foro Nacional de Ciberseguridad (22 de julio de 2020), que es un espacio de colaboración público-privada impulsado por el Consejo de Seguridad Nacional. Las líneas de trabajo están centradas en generar cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y una oportunidad para la formación y el talento en ciberseguridad; todas ellas alineadas con las medidas recogidas en la Estrategia Nacional de Ciberseguridad 2019.

2. Entre las principales leyes dictadas el pasado año en la materia que nos ocupa, cabe citar a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza; Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información; y Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

3. En el Consejo de Ministros de 22 de diciembre de 2020 se anunció que se desplegará la agenda España Digital 2025 con el fin de impulsar la conectividad y la ciberseguridad, la digitalización de la administración y del tejido productivo, las competencias digitales del conjunto de la sociedad y la innovación disruptiva en el ámbito de la inteligencia artificial[11].

4. España se ha situado en el cuarto puesto a nivel mundial en el *Global Cibersecurity Index* de 2020[12], ocupando el tercero en la "región europea", tras el Reino Unido y Estonia. Este índice, que realiza la Unión Internacional de Telecomunicaciones (sus siglas en inglés, ITU, la Agencia especializada de la ONU para las TIC), otorga una puntuación de 98,52 sobre 100 a España.

[10] https://www.consilium.europa.eu/es/policies/cybersecurity/
[11] https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2020/refc20201222.aspx
[12] https://www.itu.int/myitu/-/media/Publications/2021-Publications/Global-Cybersecurity-Index-2020.pdf

El Índice de Ciberseguridad Global fue lanzado por primera vez en 2015 por la Unión Internacional de Telecomunicaciones para medir el compromiso de 193 Estados miembros de la UIT y el Estado de Palestina con la ciberseguridad, con el fin de ayudarles a identificar áreas de mejora y animar a los países a tomar medidas, a través de la sensibilización sobre el estado de la ciberseguridad en todo el mundo. A medida que evolucionan los riesgos, las prioridades y los recursos en materia de ciberseguridad, el índice también se ha adaptado para ofrecer una instantánea más precisa de las medidas de ciberseguridad adoptadas por los países.

El objetivo del mencionado índice es comprender mejor los compromisos de los países en materia de ciberseguridad, identificar las lagunas, fomentar la incorporación de buenas prácticas y proporcionar información útil para que los países mejoren sus posturas en materia de ciberseguridad.

El índice se confecciona mediante 82 parámetros que se encuentran agrupados en cinco indicadores principales, y España ha obtenido la máxima puntuación en tres: “cuestiones legales”; “capacidad de desarrollo”; y en “cooperación”. Los otros dos indicadores son la “aplicación de las capacidades técnicas a través de los organismos nacionales y sectoriales” (19,54 puntos) y “las estrategias nacionales y las organizaciones que aplican la ciberseguridad” (18,98 puntos).

5. Por su parte el Ministerio del Interior ha elaborado y puesto en marcha un Plan Estratégico contra la Cibercriminalidad con el objetivo de potenciar las capacidades para detectar, prevenir y perseguir esta modalidad delictiva y generar un nuevo impulso operativo que garantice la protección de los derechos y libertades y la seguridad ciudadana. El ministro del Interior, Fernando Grande-Marlaska, informó del contenido de este plan estratégico al Consejo de Seguridad Nacional (CSN).

En relación precisamente al plan estratégico diseñado por la Secretaría de Estado de Seguridad, pone el foco en la prevención; en la cooperación entre las diferentes Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE) y los operadores jurídicos; en la dotación de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas; en la colaboración con la industria y los operadores relevantes en

materia de ciberseguridad en el sector público y privado; y en el respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales.

Desde estos principios, el plan diseña una estrategia global para alcanzar los siguientes objetivos específicos:

- Promover la cultura de prevención de la cibercriminalidad entre la ciudadanía y la empresa.

- Impulsar la formación y la especialización de los miembros de las FFCCSE en materia de ciberseguridad y cibercriminalidad.

- Incrementar y mejorar el uso y disposición de las herramientas tecnológicas e implementar el ámbito de la I+D+i.

- Gestionar adecuadamente la información disponible en el ciberespacio.

- Promover un marco legal e institucional que dé solución a los desafíos que surjan relacionados con la ciberseguridad y la cibercriminalidad.

- Impulsar la coordinación a nivel nacional e internacional y favorecer la colaboración entre el sector público y privado.

Para la consecución de estos objetivos, el plan contempla cuarenta y nueve líneas de acción concretas que se articulan en torno a seis ejes estratégicos: cultura de prevención de la cibercriminalidad; potenciación de capacidades; generación de ciberinteligencia; coordinación nacional y cooperación internacional; generación de un marco normativo adecuado; y colaboración público-privada[13].

Entre otras actuaciones que se están llevando a cabo merece poner de relieve, la reforma del Sistema Estadístico de Criminalidad (SEC), mediante la creación de un Grupo de Trabajo liderado por el Área del Sistema Estadístico y Atención a Víctimas de la Dirección General de Coordinación y Estudios, donde están representados todas las Fuerzas y Cuerpos de Seguridad (Policía Nacional, Guardia Civil, Ertzaintza, Mossos d'Esquadra y Policía Foral de Navarra), así como representantes de la Dirección General de Coordinación

[13] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13014439

y Estudios de la Secretaría de Estado de Seguridad (Área de Sistema Estadístico y Atención a Víctimas, además de la Oficina de Coordinación de Ciberseguridad).

Por otro lado, entre las operaciones policiales desarrolladas para combatir la cibercriminalidad, cabe situar nuevas formas criminales asociadas a las monedas electrónicas. En una operación conjunta desarrollada durante 2020 agentes de la Policía Nacional y de la Guardia Civil detuvieron al responsable ejecutivo de una empresa con sede en Canarias que, supuestamente, defraudaba mediante inversiones en criptomonedas haciendo uso de una estafa tipo "Ponzi". Este tipo de estafa consiste en una operación fraudulenta de inversión que implica el pago de intereses a los inversores de su propio dinero invertido o del dinero de nuevos inversores. Se trata de un proceso en el que las ganancias que obtienen los primeros inversionistas son generadas gracias al dinero aportado por ellos mismos o por otros nuevos inversores que caen engañados por las promesas de obtener, en algunos casos, grandes beneficios. El sistema funciona solamente si crece la cantidad de nuevas víctimas.[14]

En general, el uso de internet, se ha convertido en aliado de muchos delincuentes para expandir su actividad criminal. Buen ejemplo de ello, son las operaciones realizadas por Policía Nacional por la que se detuvo a una mujer que vendía certificados falsos de PCR[15], o la efectuada por Guardia Civil mediante la cual desarticuló una red de tráfico de armas para el crimen organizado, las cuales adquiría en el extranjero y posteriormente vendía en España a través de Internet y de aplicaciones de mensajería instantánea encriptada.[16]

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

En este *VIII Informe sobre Cibercriminalidad*, en el que se publican los datos estadísticos de cibercriminalidad y las amenazas en este ámbito que han sido descubiertas a lo largo del año 2020 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

[14] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/12569239
[15] https://www.elmundo.es/madrid/2020/12/14/5fd747bffc6c831d308b45f4.html
[16] https://www.eldiario.es/politica/desarticulada-una-red-de-trafico-de-armas-para-el-crimen-organizado_1_6082579.html

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 2020), del Instituto Nacional de Estadística (INE) se trata de una investigación dirigida a las personas de 16 y más años 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 información de los menores de 10 a 15 años.

A lo largo del capítulo 2 de este Informe (Radiografía de la sociedad de la Información), en sus diferentes apartados, se trata de trazar y esquematizar 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 Instituto Nacional de Estadística (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 2020 con respecto al año 2019. Siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2011-2020).

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 2011.

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 99,8 % de los jóvenes, entre 16 a 24 años, afirman haber accedido a la Red en los últimos tres meses, porcentaje que se reduce a un 69,7% entre las personas con edades comprendidas entre los 65 y 74 años. Si bien, la mayoría de los porcentajes de los rangos de edad que comprende este análisis han experimentado un incremento con respecto a 2019, siendo el incremento más acusado en la edad de 65 a 74 años.

Por sexo, y ***por segunda vez en la serie histórica, se iguala el porcentaje de uso de internet de mujeres y hombres***.

Resulta llamativo, en el punto 2.3 (Perfil del menor de edad ante la sociedad de la información), 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, que se sitúa en el 91,5% y 94,5, respectivamente. Por sexos, habría que establecer dos tipos diferentes de comparaciones, la primera es con respecto a los menores que usan el ordenador, en los que el 90,8% de los niños afirmaron haber utilizado en los últimos tres meses, frente al 92,3% de las niñas. Por otro lado, otra escala para establecer diferencias entre sexos es la relativa al acceso de internet, donde las niñas lo realizan en un 95,7% frente al 93,4% de los niños. Es decir, en ambas categorías las niñas tienen porcentajes más altos que los niños, extremo que no se da en la población en general.

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 2011 el comercio electrónico se ha llegado casi a triplicar, puesto que el 53,8 % de las personas encuestadas en 2020 reconocen haber realizado alguna compra empleando esta vía, mientras que en el año 2011 solo lo hacían el 18,6%. Por sexo, los hombres muestran mayores cifras porcentuales que las mujeres (54,3% frente al 53,4%), 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 (73,2%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 20,5% realiza compras por internet.

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 2011-2020. Un hecho destacable es que ***España por segunda vez, se encuentra por encima de la media de la UE-27***, con un 95% frente al 91% de la Unión Europea. En la actualidad, ***España ocupa el quinto lugar compartido con Dinamarca, como el país de la UE con más viviendas con acceso a internet.***

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. Este índice agrega una serie de indicadores pertinentes, estructurados en torno a cinco dimensiones: conectividad; capital humano; uso de internet; integración de la tecnología digital; y servicios públicos digitales. ***España destaca con un segundo puesto en la dimensión de "Servicios públicos digitales"***, que evalúa la transformación digital de la Administración Pública, donde obtiene sus mejores resultados, muy por encima de la media de la UE.

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

Durante el año 2020 INCIBE-CERT gestionó un total de CIENTO TREINTA Y TRES MIL CIENTO CINCUENTA Y CINCO (133.155) incidentes de ciberseguridad en España, siendo los más frecuentes los de tipo *malware*, seguidos de los *fraudes*.

En cuanto a los incidentes gestionados de Operadores Críticos del sector privado, a lo largo del año 2020 si bien no se ha comenzado a prestar servicio a ningún operador crítico nuevo, el número de incidentes de ciberseguridad se ha incrementado en un 5,25% con respecto al año anterior, gestionando durante 2020 un total de OCHOCIENTOS SESENTA Y UN (861) incidentes, destacándose el gran aumento experimentado con los ataques tipo *Malware.*

Por último, en los incidentes gestionados por sector estratégico, destacan los cometidos en el Sector Tributario y Financiero, seguido del Sector Transporte y el Sector Energía (14,05%).

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 asumió las funciones en materia de estadística de criminalidad, que continuaron tras la publicación del actual Real Decreto 734/2020, de 04 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 núm. 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 se contempla en esta Instrucción, a partir del Sistema Estadístico de Criminalidad (SEC), que se compone de la Base de Datos que registra las actuaciones policiales, se llevará a cabo la explotación estadística de los datos que se anoten 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.

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

Datos globales

El apartado 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 2016-2020 (la información de los Cuerpos que facilitan datos 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 tecnologías de la información y la comunicación (TIC). De esta forma, se añaden categorías como las siguientes:

- Delitos contra el honor.
- Amenazas y coacciones.

En el periodo comprendido entre 2016 a 2020, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2020, se ha conocido un total de 287.963 hechos, lo que supone un 31,9% más con respecto al año anterior. De esta cifra, el 89,6 % corresponde a fraudes informáticos (estafas) y el 4,9% a amenazas y coacciones. Hay que recordar, lo expuesto al comienzo de la Introducción, en el sentido de que con motivo de la incorporación de los datos de Ertzaintza y Mossos d'Esquadra, todos los datos de la serie histórica se han visto alterados.

Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Sin embargo, otro efecto innegable es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad. Como se puede observar en la tabla nº 1, se ha pasado del año 2016, de un 4,6%, al año 2020 con el 16,3%.

2016	2017	2018	2019	2020
4,6%	5,7%	7,5%	9,9%	16,3%

Tabla nº 1. % 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 2016 a 2020.

En relación al porcentaje de hechos esclarecidos, en el año 2020, éste supone el 14,0% del total de los hechos conocidos[17]. Por otra parte, los detenidos e investigados han alcanzado la cifra de 11.280.

La distribución de la ciberdelincuencia, desde el punto de vista geográfico (4.5. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2020, sitúa a Cataluña, Madrid, Andalucía y Comunitat Valenciana entre las Comunidades Autónomas que concentran más infracciones penales en este ámbito. A nivel provincial, se encuentran a la cabeza del ránking Madrid, Barcelona, Valencia, Illes Balears, Bizkaia y Sevilla.

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, con excepción de la Ertzaintza.

En 2020, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 215.507[18], es decir, un 29,7% más que en el año 2019. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (51,8%), tienen mayoritariamente entre 26 y 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones, así como 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 el acceso e interceptación ilícita, falsificación informática y los delitos sexuales.

[17] 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.

[18] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (287.963) y el de victimizaciones registradas (215.507), 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.

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 2020, el 30,7 % 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 87,6% de ellas son españolas, y el 12,4% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Rumanía, Marruecos e Italia las que aúnan valores más elevados.

Al igual que en el informe pasado, en este *VIII 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 de los 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 relativos a la edad de la víctima (Punto 4.11 Edad de la víctima). Por lo que, en el año 2020, de las 215.507 victimizaciones registradas, 66.150 se encuadran dentro del rango de edad que comprende los 26 a 40 años, y 52.730 entre los 41 y 50 años. Los menores de edad suman un total de 3.430.

La sección 4.16 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, durante el año 2020.

De la cifra total de detenciones e investigaciones (11.280) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 73,3% 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.

Al desglosar la información según los distintos rangos de edad predeterminados (4.17 Detenciones/investigaciones según grupo de edad y sexo), se observa que la mayor cifra de los responsables de ciberdelincuencia se ubica en el grupo de edad de 26 a 40 años.

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 han 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 (79,2%) (4.19). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Marruecos, Rumanía, Venezuela y República Dominicana, los que aglutinan un mayor número de casos.

El colectivo de 26 a 40 años de los detenidos/investigados es el más numeroso de todos los rangos establecidos (4.21).

2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

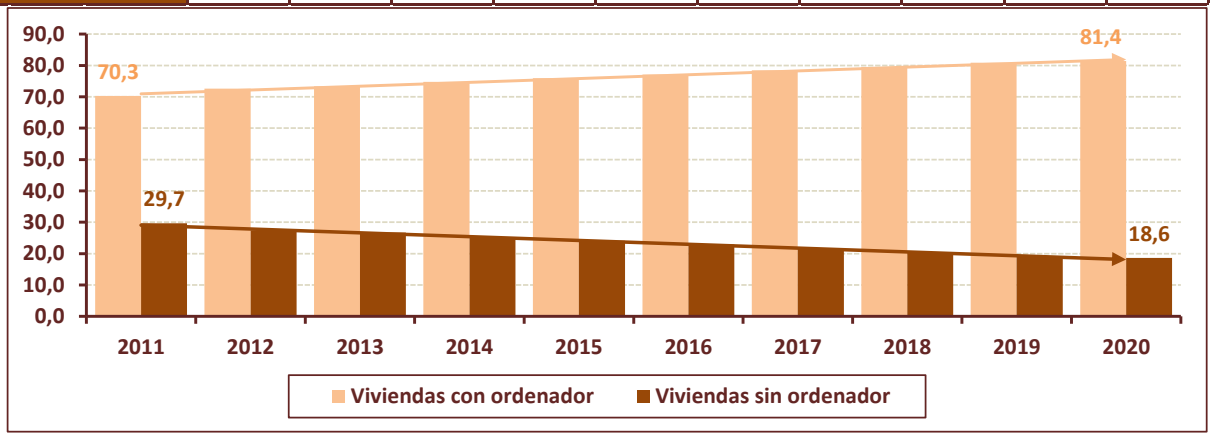
RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN >>

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

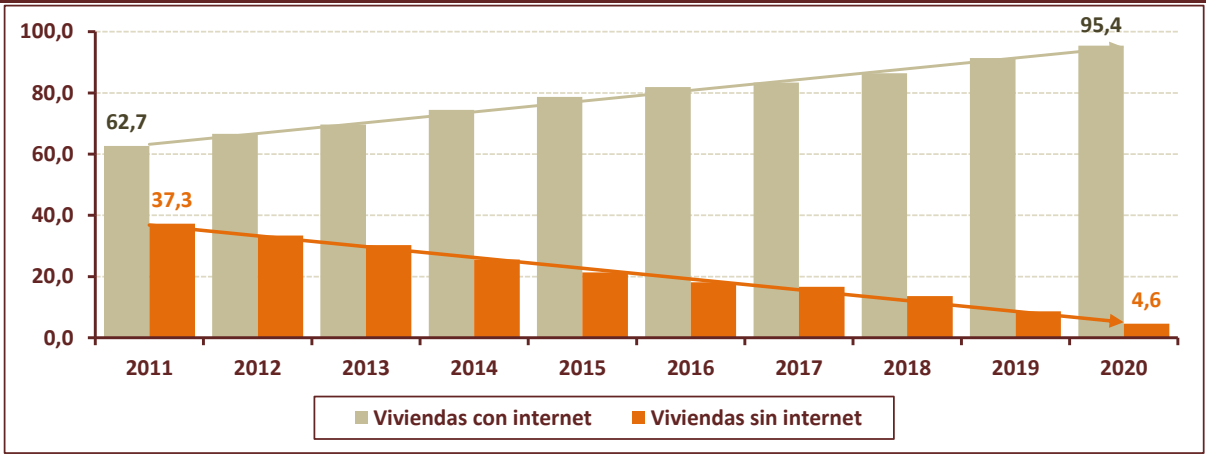
(Fuente de datos: INE)

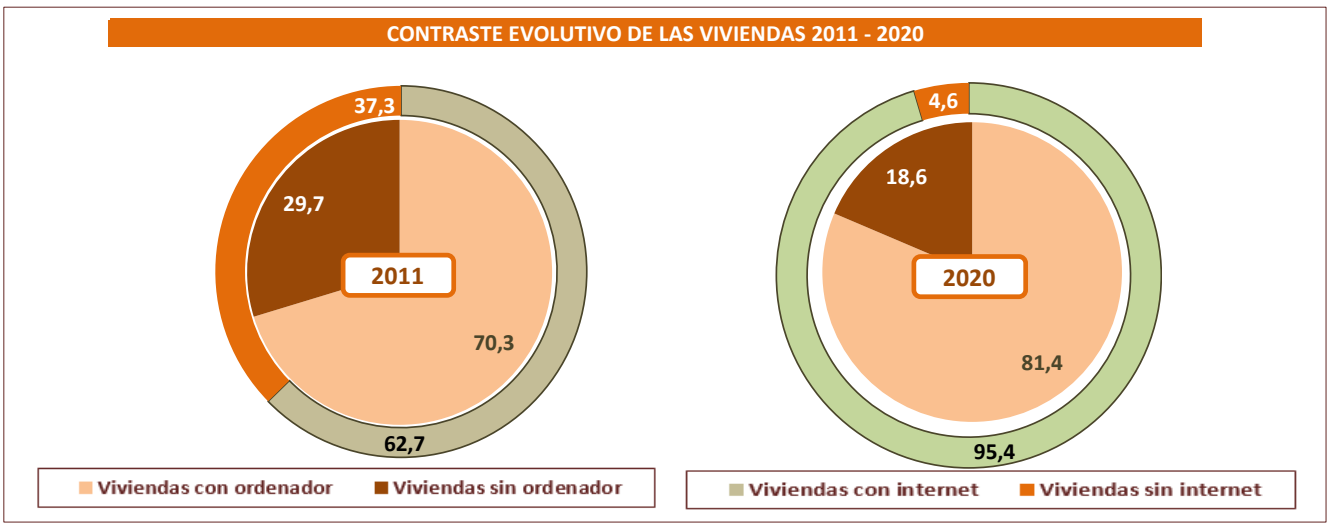
>> 2.1. Hogares

PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Viviendas con ordenador	**70,3**	72,6	73,3	74,8	75,9	77,1	78,4	79,5	80,9	**81,4**
Viviendas sin ordenador	**29,7**	27,4	26,7	25,2	24,1	22,9	21,6	20,5	19,1	**18,6**



PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Viviendas con internet	**62,7**	66,6	69,7	74,4	78,7	81,9	83,4	86,4	91,4	**95,4**
Viviendas sin internet	**37,3**	33,4	30,3	25,6	21,3	18,1	16,6	13,6	8,6	**4,6**



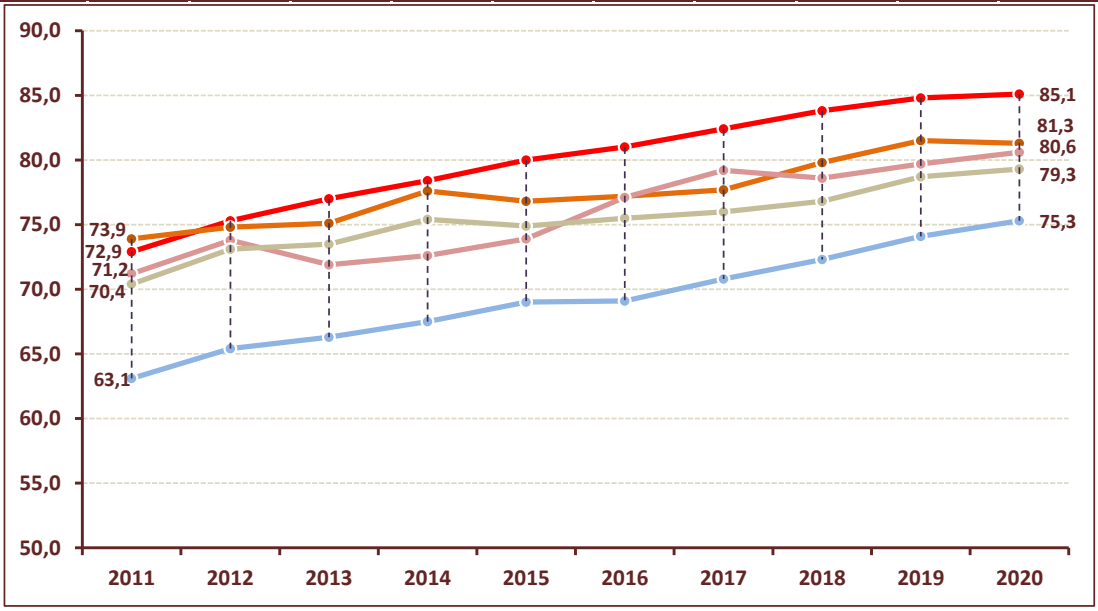


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

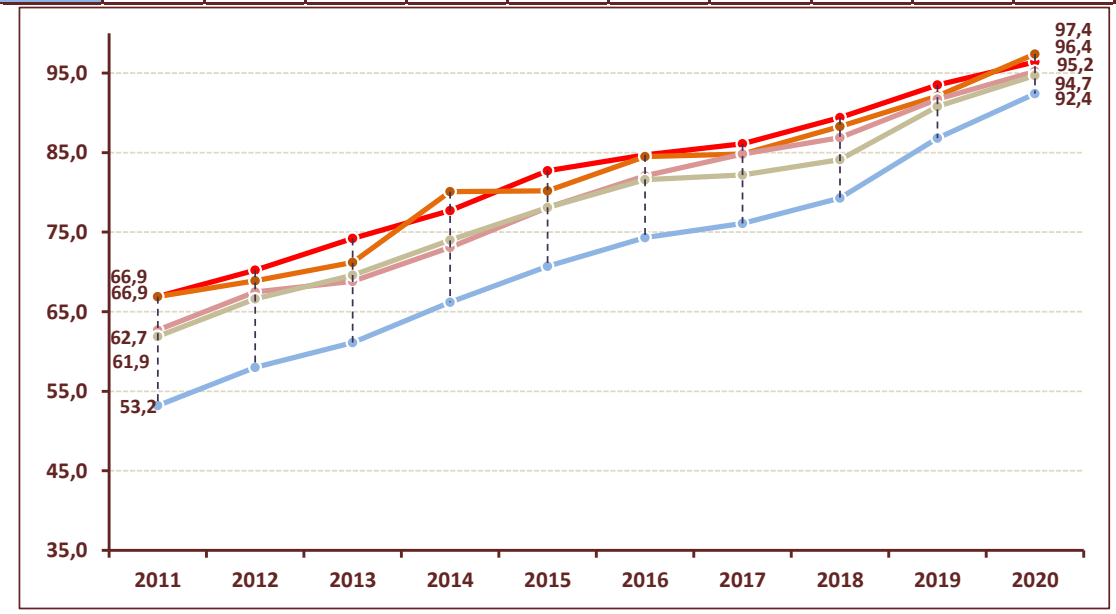
(Fuente de datos: INE)

>> 2.1. Hogares. Por tipo de hábitat

	PORCENTAJE DE VIVIENDAS CON ORDENADOR									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Más de 100.000 hab.	**72,9**	75,3	77,0	78,4	80,0	81,0	82,4	83,8	84,8	**85,1**
De 50.000 a 100.000 hab.	**73,9**	74,8	75,1	77,6	76,8	77,2	77,7	79,8	81,5	**81,3**
De 20.000 a 50.000 hab.	**71,2**	73,8	71,9	72,6	73,9	77,1	79,2	78,6	79,7	**80,6**
De 10.000 a 20.000 hab.	**70,4**	73,1	73,5	75,4	74,9	75,5	76,0	76,8	78,7	**79,3**
Menos de 10.000 hab.	**63,1**	65,4	66,3	67,5	69,0	69,1	70,8	72,3	74,1	**75,3**



	PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Más de 100.000 hab.	**66,9**	70,2	74,2	77,7	82,7	84,7	86,1	89,4	93,5	**96,4**
De 50.000 a 100.000 hab.	**66,9**	68,9	71,2	80,1	80,2	84,5	84,8	88,3	92,1	**97,4**
De 20.000 a 50.000 hab.	**62,7**	67,5	68,8	73,1	78,1	82,1	84,8	86,9	91,7	**95,2**
De 10.000 a 20.000 hab.	**61,9**	66,6	69,6	74,0	78,1	81,6	82,2	84,1	90,8	**94,7**
Menos de 10.000 hab.	**53,2**	58,0	61,1	66,2	70,7	74,3	76,1	79,3	86,8	**92,4**

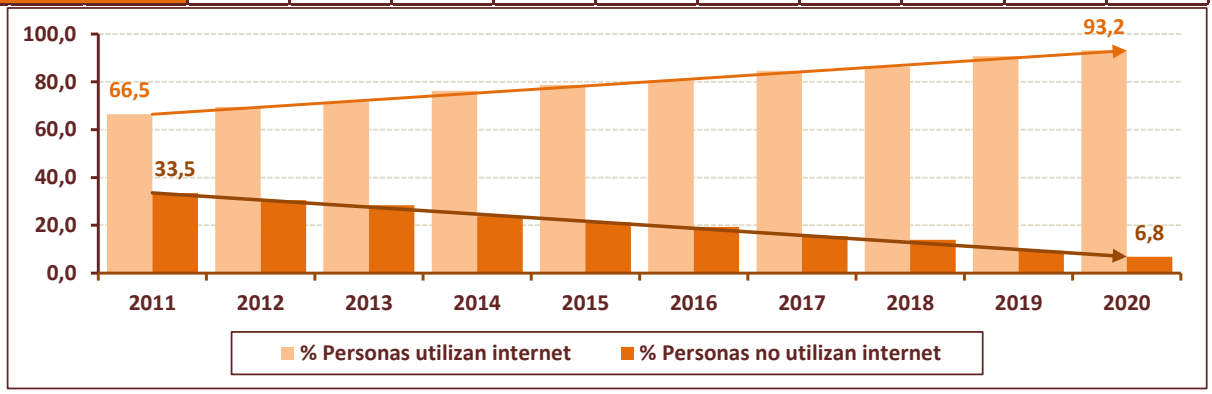


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

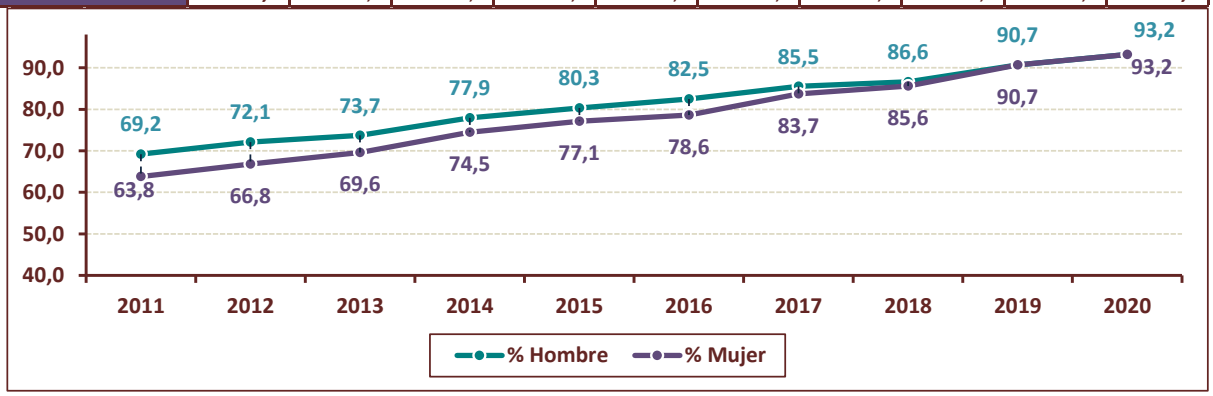
(Fuente de datos: INE)

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

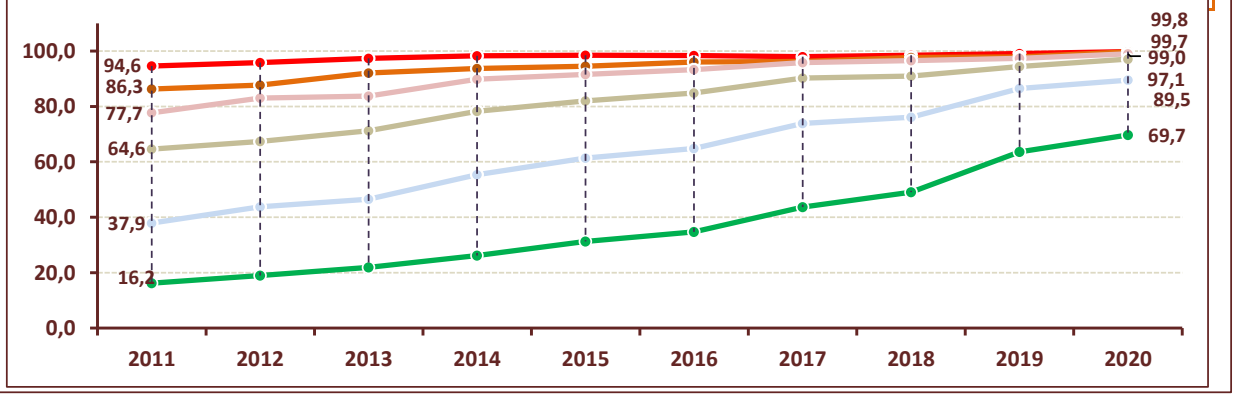
% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Utilizado internet	**66,5**	69,5	71,6	76,2	78,7	80,6	84,6	86,1	90,7	**93,2**
No utilizado internet	**33,5**	30,5	28,4	23,8	21,3	19,4	15,4	13,9	9,3	**6,8**



% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hombre	**69,2**	72,1	73,7	77,9	80,3	82,5	85,5	86,6	90,7	**93,2**
Mujer	**63,8**	66,8	69,6	74,5	77,1	78,6	83,7	85,6	90,7	**93,2**



% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Edad: De 16 a 24 años	**94,6**	95,8	97,4	98,3	98,5	98,4	98,0	98,5	99,1	**99,8**
Edad: De 25 a 34 años	**86,3**	87,7	92,1	93,7	94,5	96,0	96,3	97,7	97,9	**99,7**
Edad: De 35 a 44 años	**77,7**	83,0	83,7	89,8	91,6	93,3	95,8	96,6	97,4	**99,0**
Edad: De 45 a 54 años	**64,6**	67,4	71,2	78,2	82,0	84,9	90,3	91,0	94,4	**97,1**
Edad: De 55 a 64 años	**37,9**	43,8	46,5	55,4	61,4	64,8	73,9	76,1	86,5	**89,5**
Edad: De 65 a 74 años	**16,2**	19,0	21,9	26,2	31,3	34,7	43,7	49,1	63,6	**69,7**

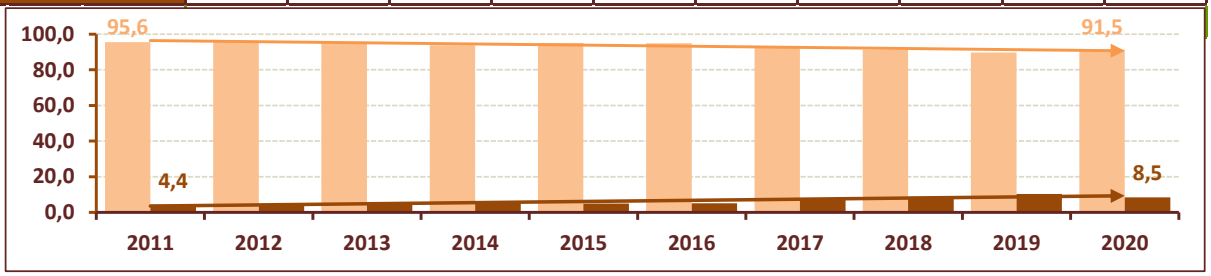


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

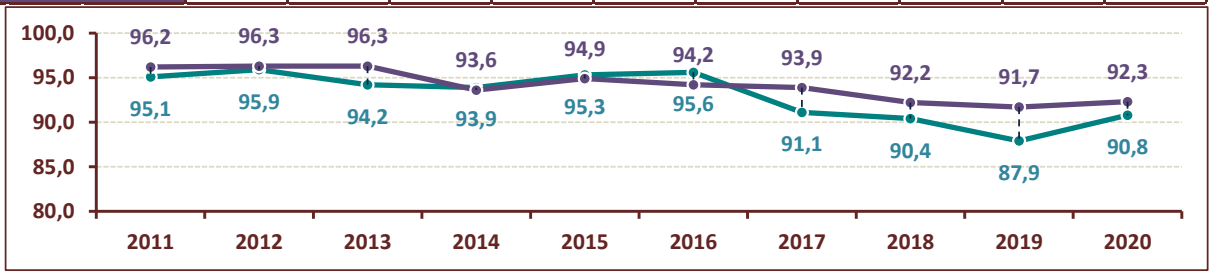
(Fuente de datos: INE)

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

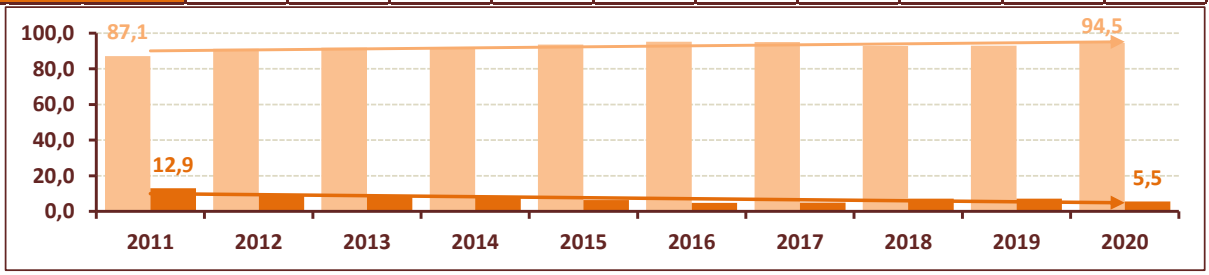
% DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Utilizado ordenador	**95,6**	96,1	95,2	93,8	95,1	94,9	92,4	91,3	89,7	**91,5**
No utilizado ordenador	**4,4**	3,9	4,8	6,2	4,9	5,1	7,6	8,7	10,3	**8,5**



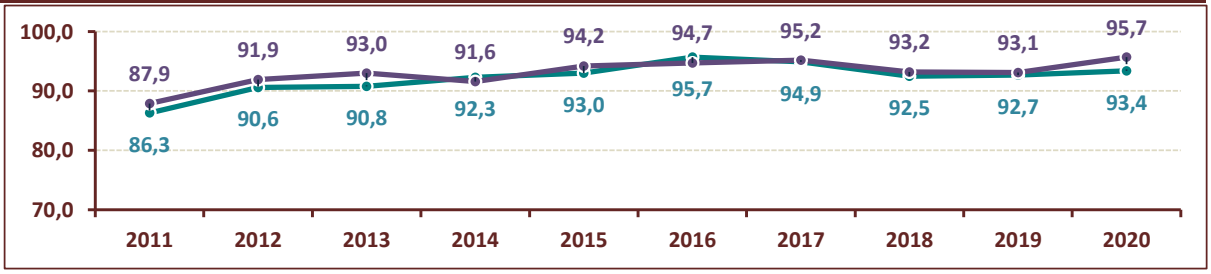
% POR SEXO DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hombre	**95,1**	95,9	94,2	93,9	95,3	95,6	91,1	90,4	87,9	**90,8**
Mujer	**96,2**	96,3	96,3	93,6	94,9	94,2	93,9	92,2	91,7	**92,3**



% DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Utilizado internet	**87,1**	91,2	91,9	92,0	93,6	95,2	95,1	92,8	92,9	**94,5**
No utilizado internet	**12,9**	8,8	8,1	8,0	6,4	4,8	4,9	7,2	7,1	**5,5**



% POR SEXO DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hombre	**86,3**	90,6	90,8	92,3	93,0	95,7	94,9	92,5	92,7	**93,4**
Mujer	**87,9**	91,9	93,0	91,6	94,2	94,7	95,2	93,2	93,1	**95,7**

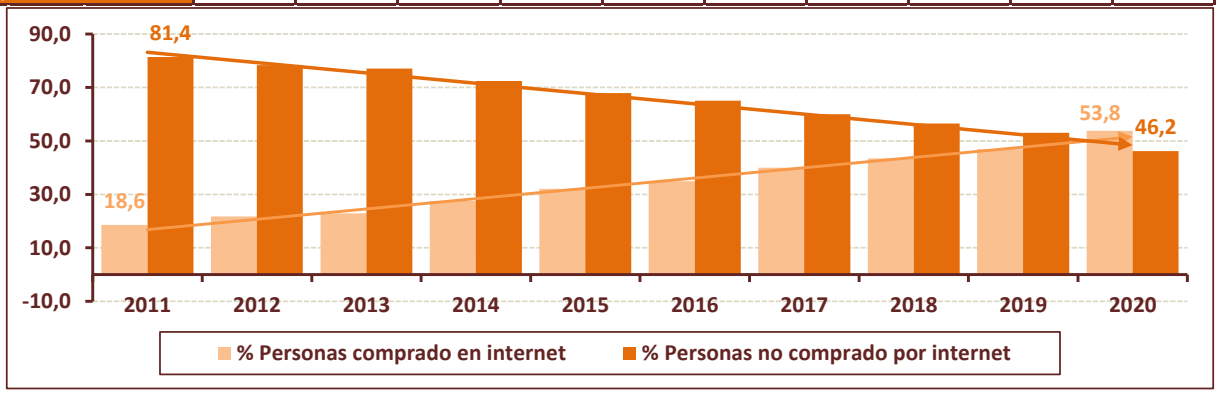


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

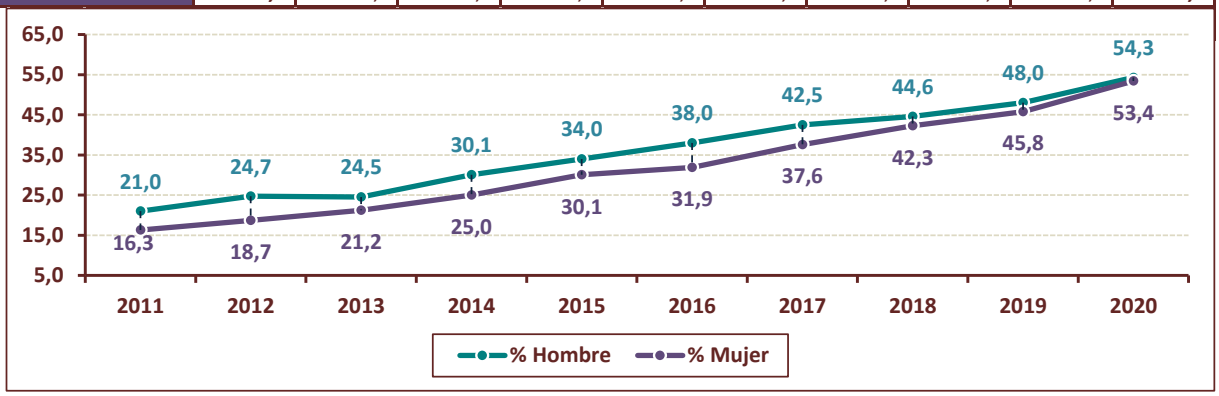
(Fuente de datos: INE)

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

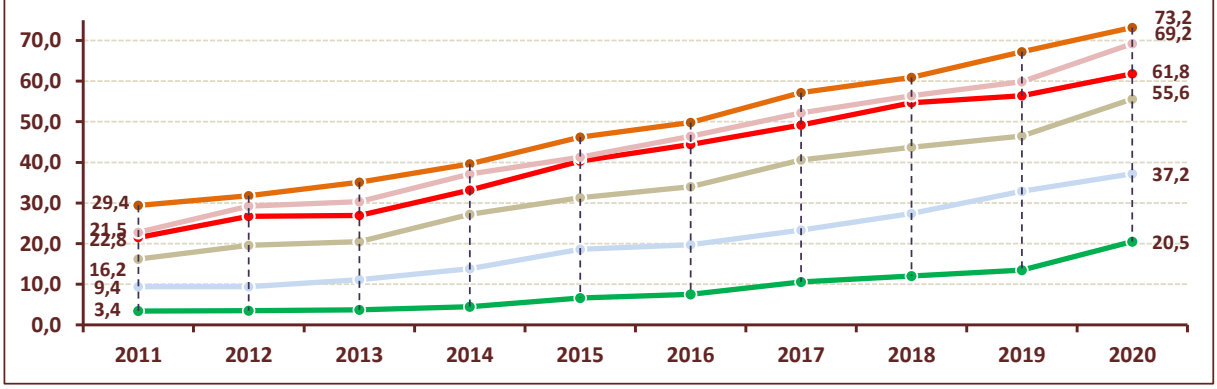
	% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Comprado en internet	18,6	21,7	22,9	27,5	32,1	34,9	40,0	43,5	46,9	53,8
No comprado en internet	81,4	78,3	77,1	72,5	67,9	65,1	60,0	56,5	53,1	46,2



	% POR SEXO DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hombre	21,0	24,7	24,5	30,1	34,0	38,0	42,5	44,6	48,0	54,3
Mujer	16,3	18,7	21,2	25,0	30,1	31,9	37,6	42,3	45,8	53,4



	% POR GRUPO DE EDAD DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Edad: De 16 a 24 años	21,5	26,7	26,9	33,2	40,3	44,4	49,2	54,7	56,4	61,8
Edad: De 25 a 34 años	29,4	31,8	35,1	39,6	46,2	49,8	57,2	60,9	67,2	73,2
Edad: De 35 a 44 años	22,8	29,2	30,3	37,1	41,3	46,4	52,2	56,4	59,9	69,2
Edad: De 45 a 54 años	16,2	19,6	20,5	27,2	31,3	34,0	40,6	43,7	46,5	55,6
Edad: De 55 a 64 años	9,4	9,4	11,1	13,8	18,6	19,7	23,3	27,4	32,9	37,2
Edad: De 65 a 74 años	3,4	3,5	3,7	4,5	6,6	7,5	10,6	12,0	13,5	20,5



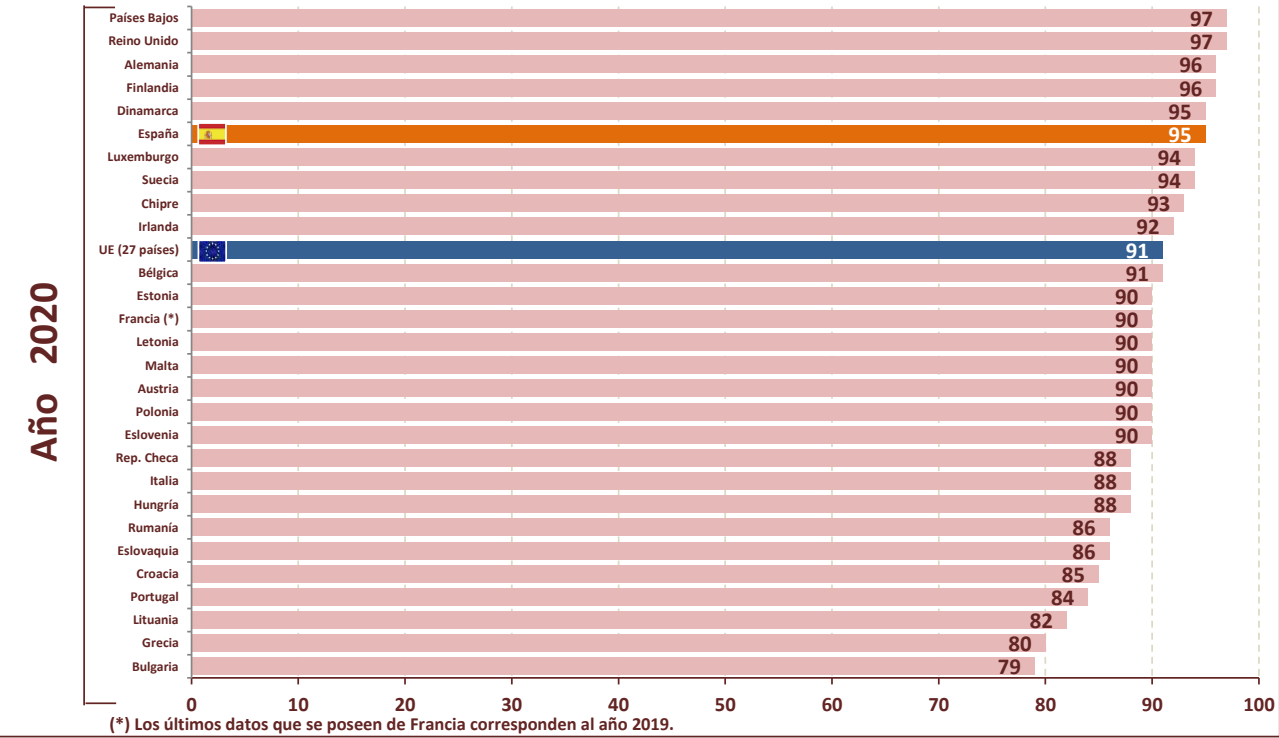
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: EUROSTAT)

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

PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
UE (27 países)	72	75	77	80	81	84	86	88	90	91
Bélgica	77	78	80	83	82	85	86	87	90	91
Bulgaria	45	51	54	57	59	64	67	72	75	79
Rep. Checa	67	73	73	78	79	82	83	86	87	88
Dinamarca	90	92	93	93	92	94	97	93	95	95
Alemania	83	85	88	89	90	92	93	94	95	96
Estonia	69	74	79	83	88	86	88	90	90	90
Irlanda	78	81	82	82	85	87	88	89	91	92
Grecia	50	54	56	66	68	69	71	76	79	80
España	63	67	70	74	79	82	83	86	91	95
Francia (*)	76	80	82	83	83	86	86	89	90	90
Croacia	61	66	65	68	77	77	76	82	81	85
Italia	62	63	69	73	75	79	81	84	85	88
Chipre	57	62	65	69	71	74	79	82	90	93
Letonia	64	69	72	73	76	77	79	82	85	90
Lituania	60	60	65	66	68	72	75	78	82	82
Luxemburgo	91	93	94	96	97	97	97	93	95	94
Hungría	63	67	70	73	76	79	82	83	86	88
Malta	75	77	78	80	81	81	85	84	86	90
Países Bajos	94	94	95	96	96	97	98	98	98	97
Austria	75	79	81	81	82	85	89	89	90	90
Polonia	67	70	72	75	76	80	82	84	87	90
Portugal	58	61	62	65	70	74	77	79	81	84
Rumanía	47	54	58	61	68	72	76	81	84	86
Eslovenia	73	74	76	77	78	78	82	87	89	90
Eslovaquia	71	75	78	78	79	81	81	81	82	86
Finlandia	84	87	89	90	90	92	94	94	94	96
Suecia	91	92	93	90	91	94	95	92	96	94
Reino Unido	83	87	88	90	91	93	94	95	96	97



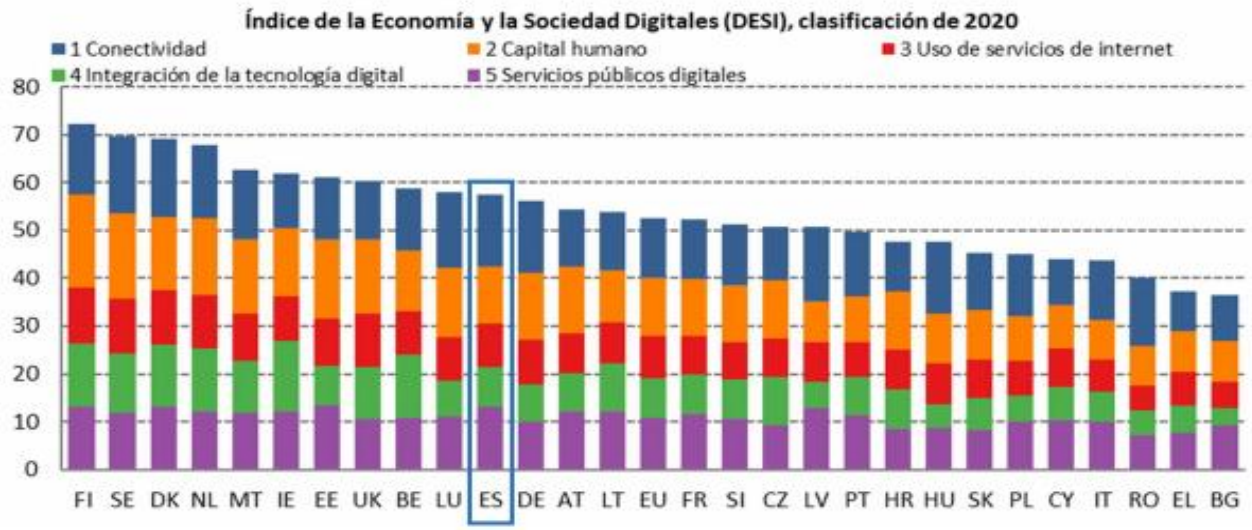
(*) Los últimos datos que se poseen de Francia corresponden al año 2019.

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
	puesto	puntuación	puntuación
DESI 2020	**11**	**57,5**	**52,6**
DESI 2019	10	53,6	49,4
DESI 2018	10	50,2	46,5



5 Servicios públicos digitales	España		UE
	puesto	puntuación	puntuación
DESI 2020	**2**	**87,3**	**72,0**
DESI 2019	4	80,9	67,0
DESI 2018	4	76,6	61,8

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.

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

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

El INCIBE-CERT gestionó un total de CIENTO TREINTA Y TRES MIL CIENTO CINCUENTA Y CINCO (133.155) incidentes de ciberseguridad en España durante el año 2020.

Analizando el número de incidentes en función de su tipología, puede concluirse que los incidentes tipo Malware se han convertido en el año 2020 en el tipo más frecuente de incidente registrado con un porcentaje del 35,22%, seguido de los *Fraudes* con un 32,02% respecto del total de incidentes registrados.

Con respecto a los principales tipos de Malware con mayor relevancia y efectos en el 2020 podemos resumir:

Emotet: Ha funcionado 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 2020 han implicado el envío de correos electrónicos *phishing* con archivos adjuntos maliciosos conteniendo macros funcionando como descargadores de malware. La mayoría de los archivos adjuntos se han identificado como ficheros de Microsoft Office, no obstante, también se han observado el uso de archivos de otros formatos como ZIP y PDF.

Trickbot: Conjunto de herramientas que han permitido realizar múltiples actividades ilegales como la sustracción de datos, la criptominería o enumeración de hosts. Las campañas de *Trickbot* más destacadas han utilizado el envío de correos electrónicos *phishing* con archivos o enlaces maliciosos para iniciar macros de Microsoft Office y descargar *Trickbots*. Los operadores del malware se han aprovechado de la confianza depositada en las autoridades de certificación mediante el uso de cargadores firmados y malware para evadir la detección de productos de seguridad.

Ryuk: Sirviéndose del compromiso previo de los sistemas mediante *Emotet* o *Trickbot*, ha identificado y cifrado archivos o sistemas esenciales para su objetivo y deshabilitado la restauración de los sistemas, dificultando la recuperación tras un ataque. Este proceso viene seguido de la solicitud de un rescate a cambio de una clave de descifrado.

Metasploit: Plataforma modular de pruebas de penetración diseñada para escribir y ejecutar código de explotación, que ha permitido enumerar redes, ejecutar ataques e incluso evadir la detección, entre otras acciones. Los errores de programación y privilegios obtenidos en sistemas o software vulnerados han sido empleados con fines fraudulentos con la finalidad de explotación.

Powershell Empire: Ha posibilitado evadir soluciones de seguridad y ser identificado por los equipos de defensa, operando de manera encubierta, permitiendo el control total de los atacantes sobre los sistemas comprometidos y empleando un tráfico de *Command&Control* asíncrono, cifrado y diseñado para integrarse con la actividad normal de la red.

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

A lo largo del año 2020 si bien no se ha comenzado a prestar servicio a ningún operador crítico nuevo, el número de incidentes de ciberseguridad se ha incrementado en un 5,25% con respecto al año anterior, gestionando durante 2020 un total de OCHOCIENTOS SESENTA Y UN (861) incidentes.

Este valor creciente se ha visto motivado por un aumento de la actividad de los Operadores Críticos en el ámbito del ciberespacio como resultado de las diferentes restricciones derivadas de pandemia de la Covid-19.

Este incremento ha supuesto un aumento en la actividad de los diferentes cibercriminales, alcanzando en el ámbito competencial de Protección de Infraestructuras Críticas (PIC) un mayor porcentaje de incidentes relacionados con ataques a *Sistemas Vulnerables* (40,77%), siendo estos detectados y mitigados en su gran mayoría por los servicios proactivos prestados por el INCIBE-CERT.

Significar que con respecto a los incidentes detectados en Operadores Críticos y relacionados con ataques tipo *Malware* descritos se ha detectado un gran aumento con respecto al año anterior *(*40,42%), doblando en cantidad al total generado en el 2019 mediante algunas de las principales campañas comentadas previamente.

>> 3.3. Incidentes gestionados por Sector Estratégico

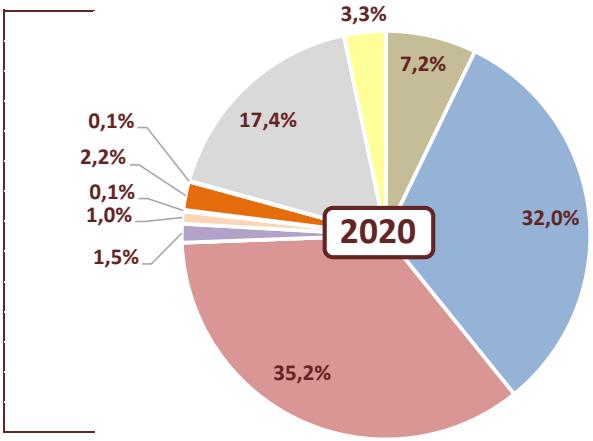
Los sectores PIC donde se han detectado un mayor número de incidentes han sido el Sector Tributario y Financiero (52,50%) seguido del Sector Transporte (24,08%) y el Sector Energía (14,05%).

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.1. Incidentes gestionados por el INCIBE-CERT

Tipo de incidente	INCIDENTES GESTIONADOS					
	2015	2016	2017	2018	2019	2020
Intrusión	16.054	14.373	19.275	8.541	6.479	9.557
Fraude	13.410	11.843	11.959	55.932	31.938	42.641
Malware	15.177	76.811	81.090	27.016	27.358	46.893
SPAM	1.275	10.279	7.957	0	0	0
Disponibilidad	794	495	514	100	58	1.971
Intento de intrusión	335	381	1.435	396	1.518	1.289
Robos de información	26	37	47	63	77	161
Contenido Abusivo				9.353	4.064	2.986
Recolección de información				5.605	84	87
Sistema Vulnerable				3.731	31.414	23.161
Otros	2.905	1.038	787	782	4.407	4.409

Porcentaje del total de incidentes gestionados

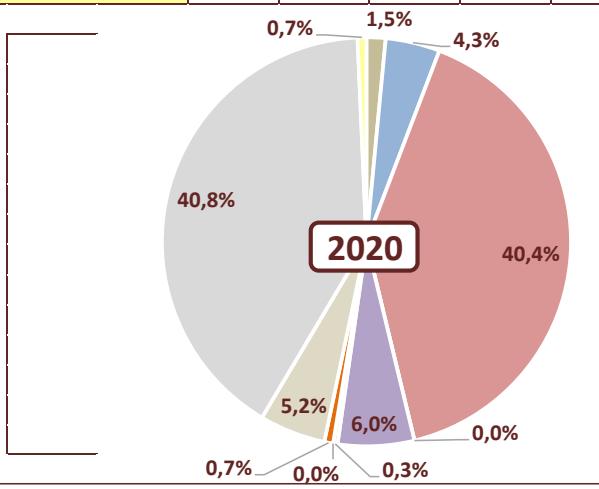


*Véase metadatos explicativos

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

Tipo de incidente	INCIDENTES GESTIONADOS					
	2015	2016	2017	2018	2019	2020
Intrusión	15	39	97	26	14	13
Fraude	8	13	66	41	78	37
Malware	75	311	387	200	166	348
SPAM	0	8	21	0	0	0
Disponibilidad	10	28	55	54	12	52
Intento de intrusión	7	24	159	9	7	3
Robos de información	2	1	1	7	8	0
Contenido Abusivo				11	6	6
Recolección de información				111	1	45
Sistema Vulnerable				224	514	351
Otros	13	55	99	39	12	6

Porcentaje del total de incidentes gestionados



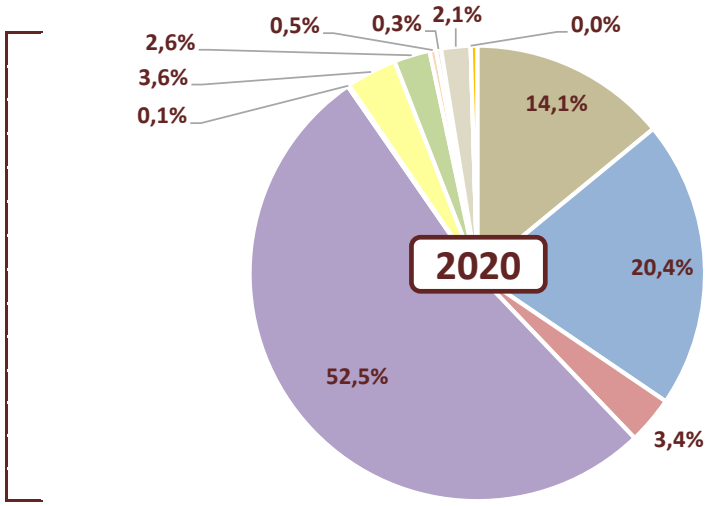
*Véase metadatos explicativos

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.3. Incidentes gestionados por sector estratégico

Sector estratégico	INCIDENTES GESTIONADOS					
	2015	2016	2017	2018	2019	2020
Energía	46	126	213	149	151	121
Transporte	24	90	152	192	197	176
Tecnologías Informac. y Comunicac. (TIC)	17	17	40	46	50	29
Sistema tributario y financiero	17	152	250	214	266	452
Alimentación	12	47	42	40	57	1
Agua	5	40	134	57	64	31
Industria nuclear	5	4	12	5	18	22
Administración	1	2	10	1	0	4
Espacio	0	0	1	3	4	3
Industria química	0	0	0	15	11	18
Instalaciones de Investigación	0	0	0	0	0	0
Salud	0	0	1	0	0	0
Todos los sectores afectados	3	1	0	0	0	4

Porcentaje del total de incidentes gestionados



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD >>

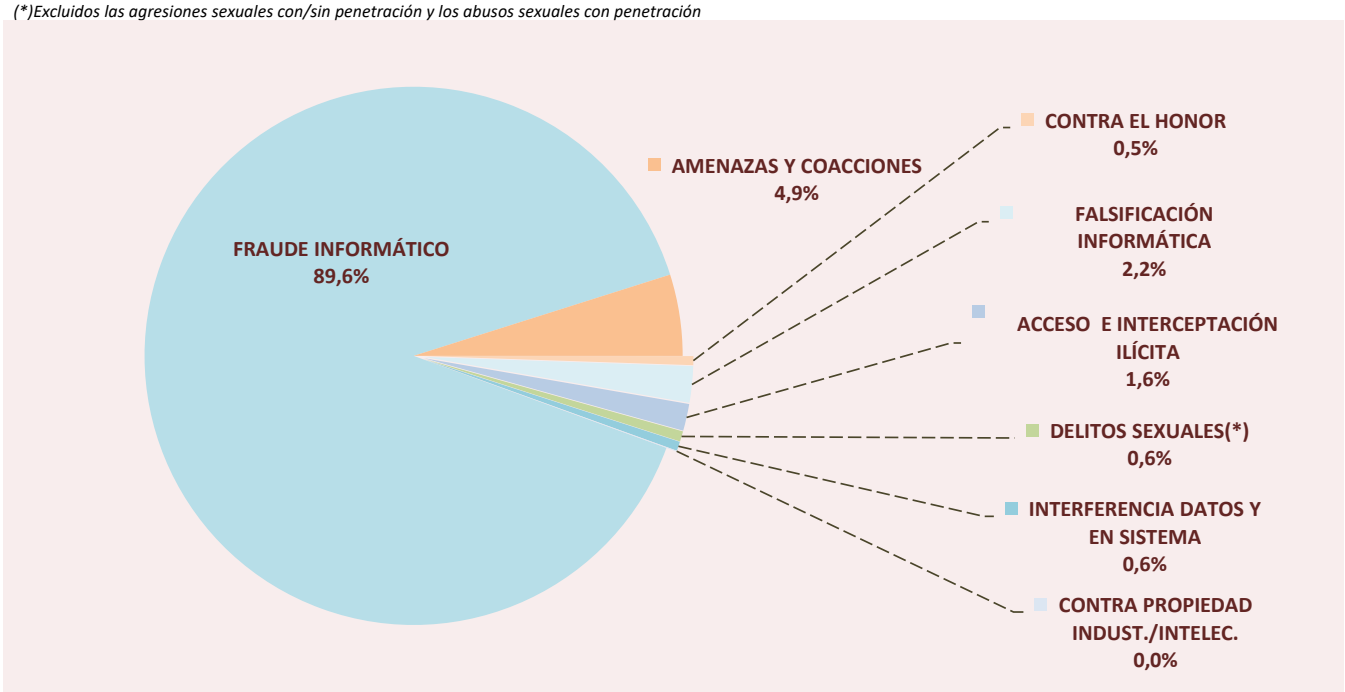
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2016	2017	2018	2019	2020
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004	4.653
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782	14.066
CONTRA EL HONOR	1.546	1.561	1.448	1.422	1.550
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197	125
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774	1.783
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275	6.289
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375	257.907
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473	1.590
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**	**287.963**

(*)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

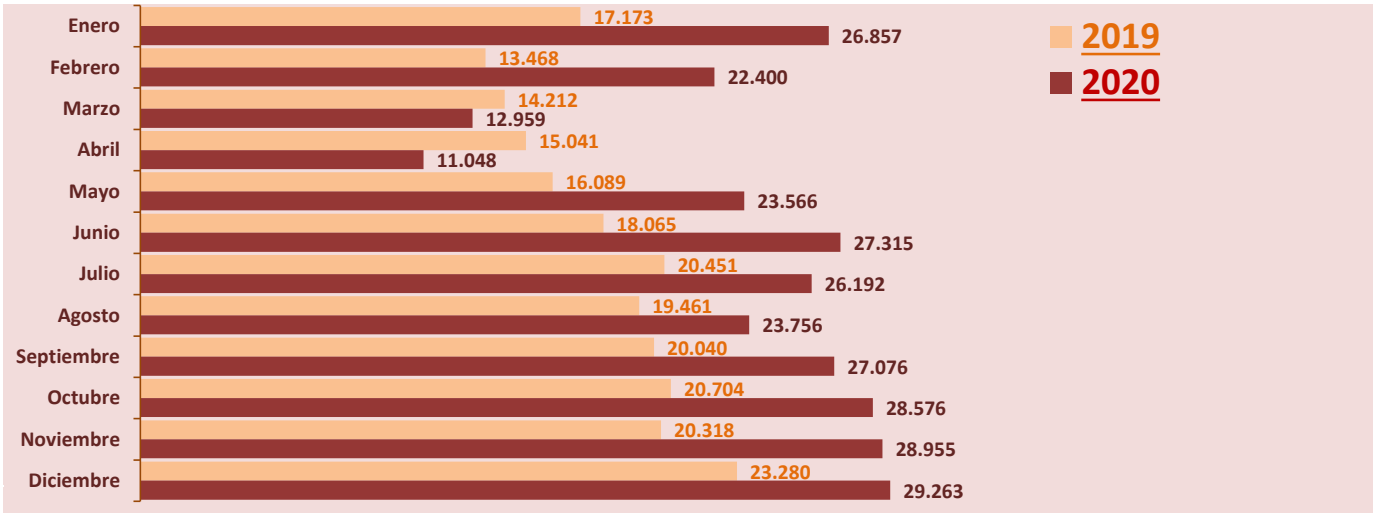
(Fuente de datos: Sistema Estadístico de Criminalidad)

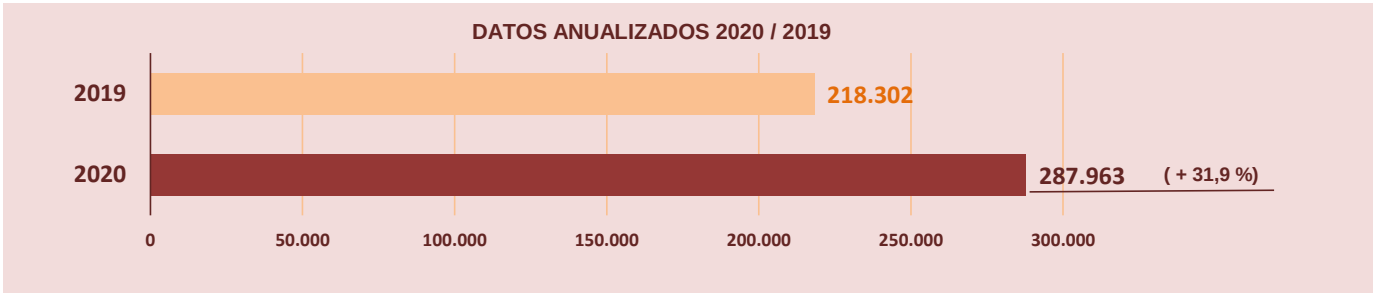
>> 4.3. Distribución mensual de hechos conocidos. Año 2020

HECHOS CONOCIDOS	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic	TOTAL
ACCESO E INTERCEPTACIÓN ILÍCITA	381	420	226	243	433	423	441	374	360	423	442	487	**4.653**
AMENAZAS Y COACCIONES	1.055	1.106	685	698	1.133	1.314	1.452	1.461	1.404	1.294	1.235	1.229	**14.066**
CONTRA EL HONOR	133	123	85	78	128	150	162	128	162	126	149	126	**1.550**
CONTRA PROPIEDAD INDUST./INTELEC.	10	10	9	2	8	10	14	8	18	8	11	17	**125**
DELITOS SEXUALES(*)	163	178	102	123	160	188	139	120	152	130	214	114	**1.783**
FALSIFICACIÓN INFORMÁTICA	457	488	326	228	483	533	571	529	565	656	679	774	**6.289**
FRAUDE INFORMÁTICO	24.515	19.930	11.448	9.600	21.121	24.581	23.252	21.034	24.298	25.760	26.058	26.310	**257.907**
INTERFERENCIA DATOS Y EN SISTEMA	143	145	78	76	100	116	161	102	117	179	167	206	**1.590**
Total HECHOS CONOCIDOS	**26.857**	**22.400**	**12.959**	**11.048**	**23.566**	**27.315**	**26.192**	**23.756**	**27.076**	**28.576**	**28.955**	**29.263**	**287.963**

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

>> 4.4. Comparativa de la distribución mensual de hechos conocidos 2020 / 2019





4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

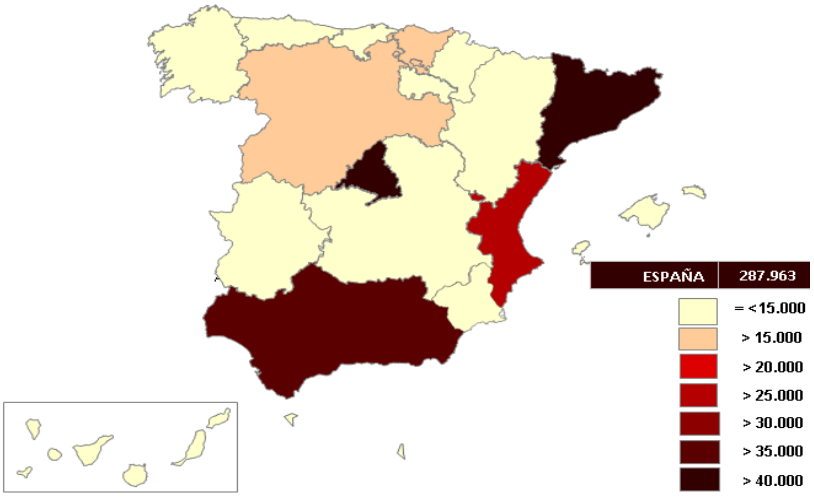
>> 4.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2020

Hechos denunciados de CIBERCRIMINALIDAD - 2020

Hechos conocidos:	287.963
Esclarecimiento (*):	38.046
Detenciones/invest:	11.280

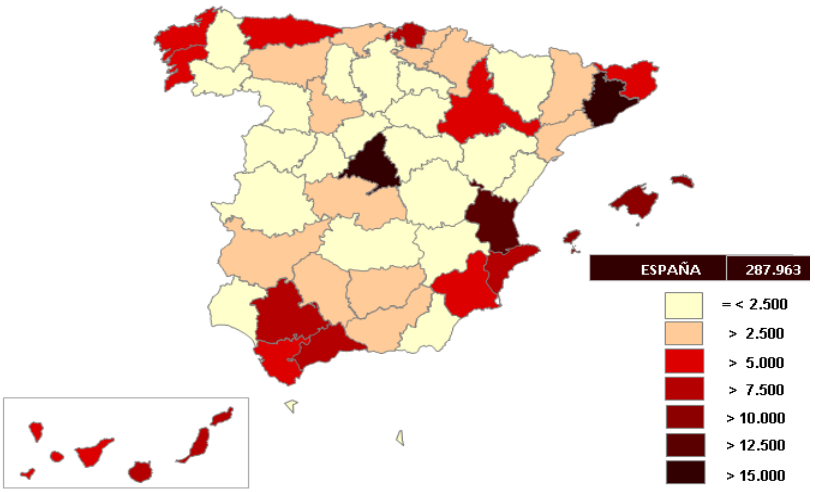
14,0%

CCAA	Hechos
CATALUÑA	48.794
MADRID (COMUNIDAD DE)	48.678
ANDALUCÍA	39.157
COMUNITAT VALENCIANA	25.732
PAÍS VASCO	17.866
CASTILLA Y LEÓN	15.457
GALICIA	14.632
CANARIAS	14.449
BALEARS (ILLES)	11.800
CASTILLA - LA MANCHA	9.963
ARAGÓN	7.826
MURCIA (REGIÓN DE)	6.828
ASTURIAS (PRINCIPADO DE)	6.225
EN EL EXTRANJERO	5.726
EXTREMADURA	4.638
NAVARRA (COMUNIDAD FORAL DE)	4.465
CANTABRIA	2.885
RIOJA (LA)	1.992
CIUDAD AUTÓNOMA DE CEUTA	436
CIUDAD AUTÓNOMA DE MELILLA	414



(*) 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 - 2020



Provincias más afectadas:	Hechos
Madrid	48.678
Barcelona	35.708
Valencia/València	14.525
Balears (Illes)	11.800
Bizkaia	9.985
Sevilla	9.630
Málaga	9.183
Alicante/Alacant	8.956
Palmas (Las)	8.942
Murcia	6.828
Coruña (A)	6.304
Asturias	6.225
Cádiz	6.203
Zaragoza	6.057
EN EL EXTRANJERO	5.726
Santa Cruz de Tenerife	5.507
Girona	5.376
Pontevedra	5.312
Gipuzkoa	4.962
Tarragona	4.683

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

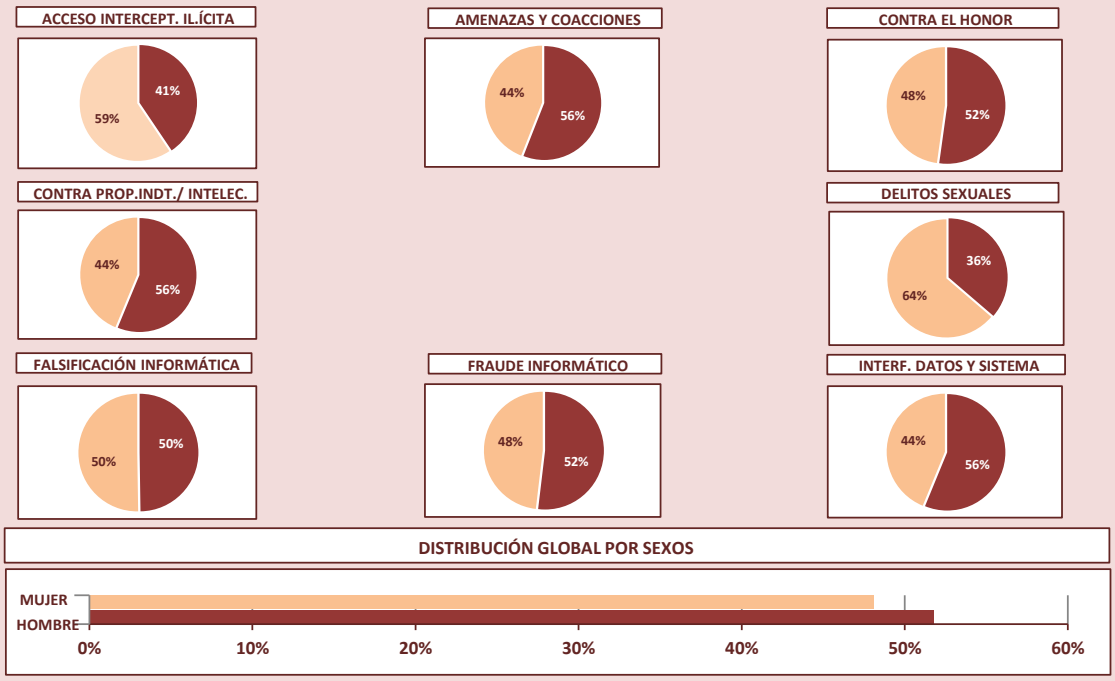
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales, excepto Ertzaintza)

>> 4.6. Victimizaciones registradas según grupo penal y sexo. Año 2020

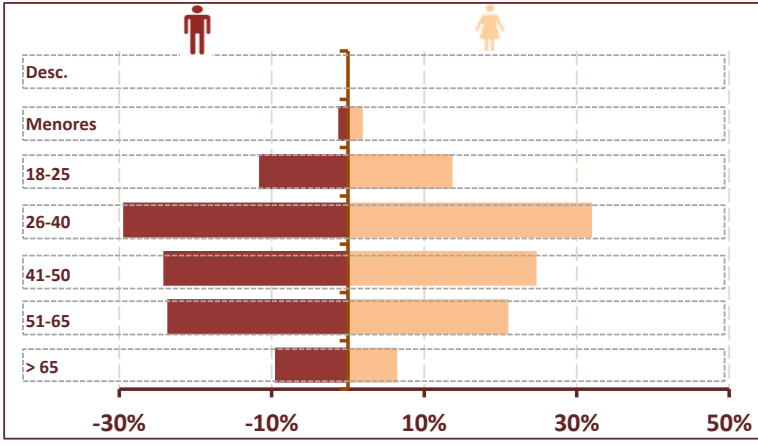
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.580	2.315	1	3.896
AMENAZAS Y COACCIONES	7.887	6.205	25	14.117
CONTRA EL HONOR	845	774	10	1.629
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	36	28	0	64
DELITOS SEXUALES (*)	487	855	5	1.347
FALSIFICACIÓN INFORMÁTICA	2.147	2.168	7	4.322
FRAUDE INFORMÁTICO	97.970	90.828	54	188.852
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	719	560	1	1.280
Total VICTIMIZACIONES	**111.671**	**103.733**	**103**	**215.507**

(*)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 2020



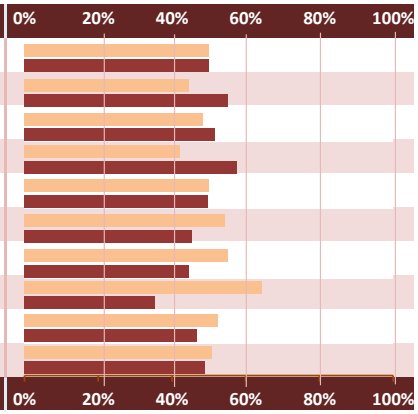
Grupo de edad	Hombre	Mujer	Descon.
Edad descon.	130	89	21
Menores de edad	1.403	2.024	3
De 18 a 25 años	13.036	14.207	0
De 26 a 40 años	32.909	33.229	12
De 41 a 50 años	27.035	25.663	32
De 51 a 65 años	26.480	21.811	27
Mayores 65 años	10.678	6.710	8
TOTAL	**111.671**	**103.733**	**103**

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

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

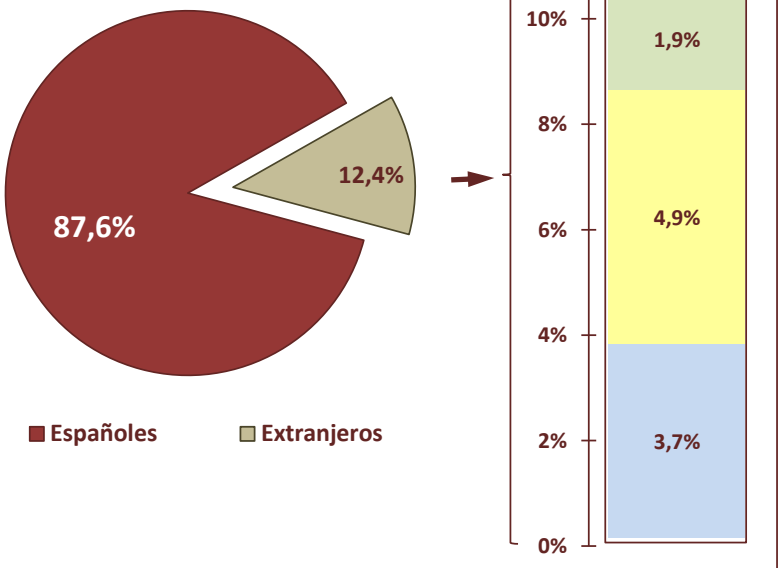
>> 4.8. Victimizaciones por tipología penal y sexo. Año 2020

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS CON TARJETAS CRÉDITO, DÉBITO Y CHEQUES	50.090	50.006	20	100.116
OTRAS ESTAFAS	31.364	25.324	26	56.714
ESTAFA BANCARIA	16.516	15.498	8	32.022
AMENAZAS	7.018	5.134	23	12.175
USURPACIÓN DE ESTADO CIVIL	2.146	2.168	7	4.321
ACCESO ILEGAL INFORMÁTICO	893	1.068	0	1.961
COACCIONES	865	1.069	2	1.936
DESCUBRIMIENTO/REVELACIÓN SECRETOS	686	1.245	1	1.932
INJURIAS	555	620	8	1.183
RESTO	1.538	1.601	8	3.147
Total VICTIMIZACIONES	**111.671**	**103.733**	**103**	**215.507**



>> 4.9. Nacionalidad de la víctima. Año 2020

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	**188.824**	**87,6%**
2.- EXTRANJEROS	**26.683**	**12,4%**
2.1.- UNIÓN EUROPEA	**7.987**	**3,7%**
RUMANÍA	2.535	1,2%
ITALIA	1.715	0,8%
FRANCIA	774	0,4%
BULGARIA	648	0,3%
ALEMANIA	584	0,3%
Resto	1.731	0,8%
2.2.- AMÉRICA	**10.529**	**4,9%**
VENEZUELA	1.615	0,7%
COLOMBIA	1.535	0,7%
ECUADOR	1.239	0,6%
Resto	6.140	2,8%
2.3.- ÁFRICA	**4.160**	**1,9%**
MARRUECOS	2527	1,2%
SENEGAL	380	0,2%
Resto	1.253	0,6%
2.4.- ASIA	**1.638**	**0,8%**
CHINA POPULAR	546	0,3%
FILIPINAS	241	0,1%
Resto	851	0,4%
2.5.- RESTO PAÍSES	**2.369**	**1,1%**
REINO UNIDO	587	0,3%
UCRANIA	477	0,2%
Otros	1.305	0,6%
TOTAL	**215.507**	**100%**



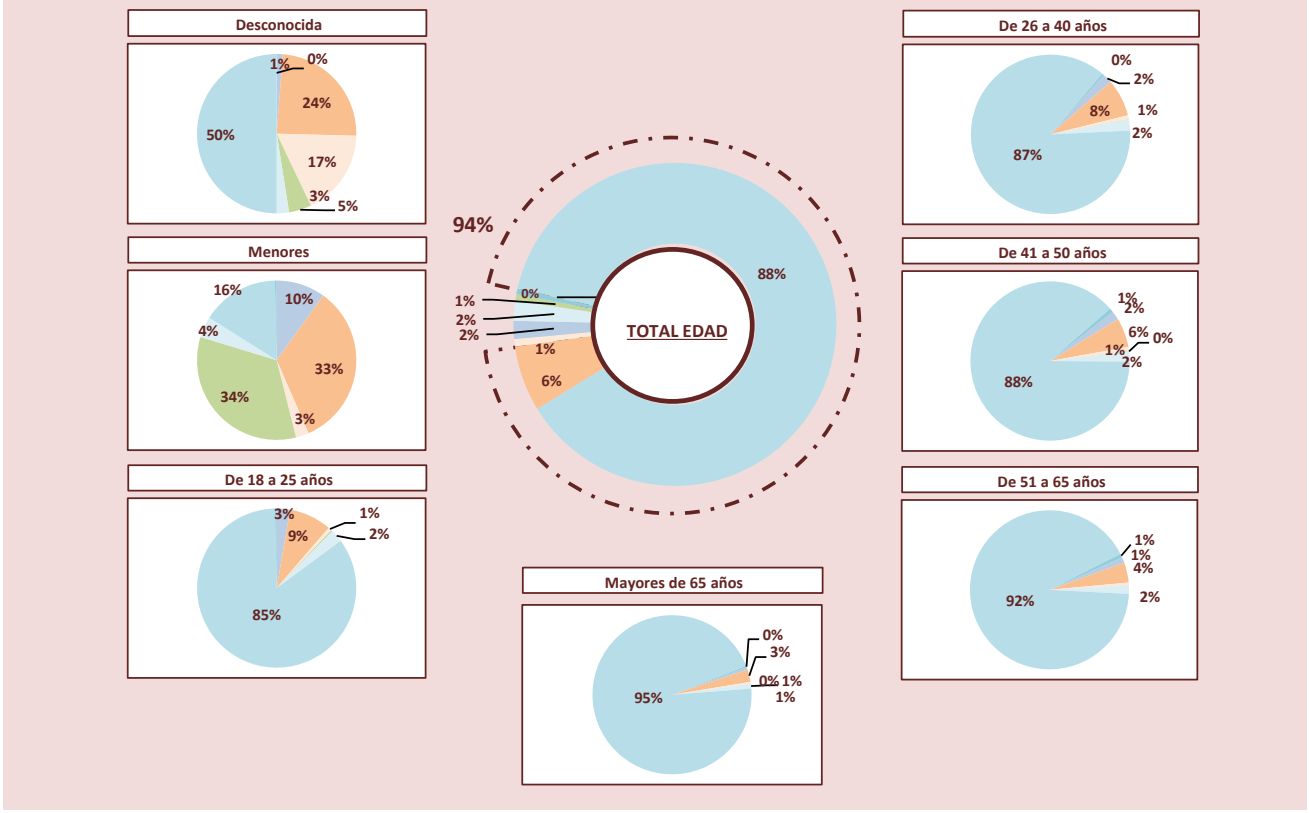
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

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

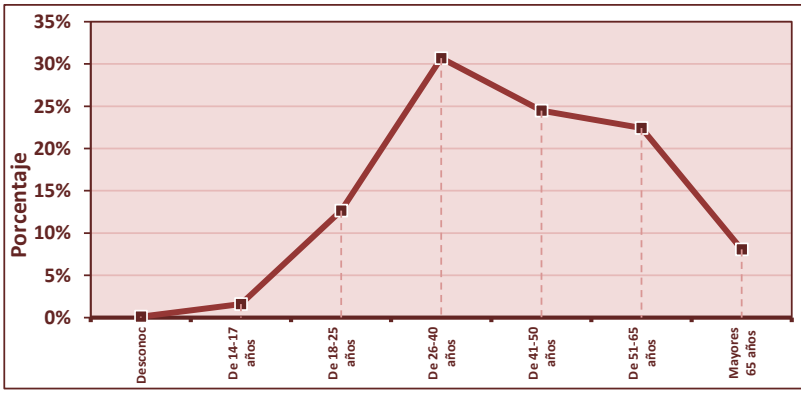
>> 4.10. Victimizaciones registradas según grupo penal y edad. Año 2020

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	3	341	739	1.262	918	552	81
AMENAZAS Y COACCIONES	58	1.149	2.352	5.010	3.147	1.964	437
CONTRA EL HONOR	42	90	187	522	442	293	53
CONTRA PROPIEDAD INDUST./INTELEC.	0	1	3	22	20	14	4
DELITOS SEXUALES(*)	11	1.153	77	54	42	6	4
FALSIFICACIÓN INFORMÁTICA	6	145	693	1.458	1.059	790	171
FRAUDE INFORMÁTICO	120	539	23.099	57.540	46.645	44.322	16.587
INTERFERENCIA EN DATOS Y EN SISTEMA	0	12	93	282	457	377	59
Total VICTIMIZACIONES	**240**	**3.430**	**27.243**	**66.150**	**52.730**	**48.318**	**17.396**

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



>> 4.11. Edad de la víctima. Año 2020



Grupo de edad	Víctimas
Edad desconocida	240
Menores de edad	3.430
De 18 a 25 años	27.243
De 26 a 40 años	66.150
De 41 a 50 años	52.730
De 51 a 65 años	48.318
Mayores 65 años	17.396
TOTAL	**215.507**

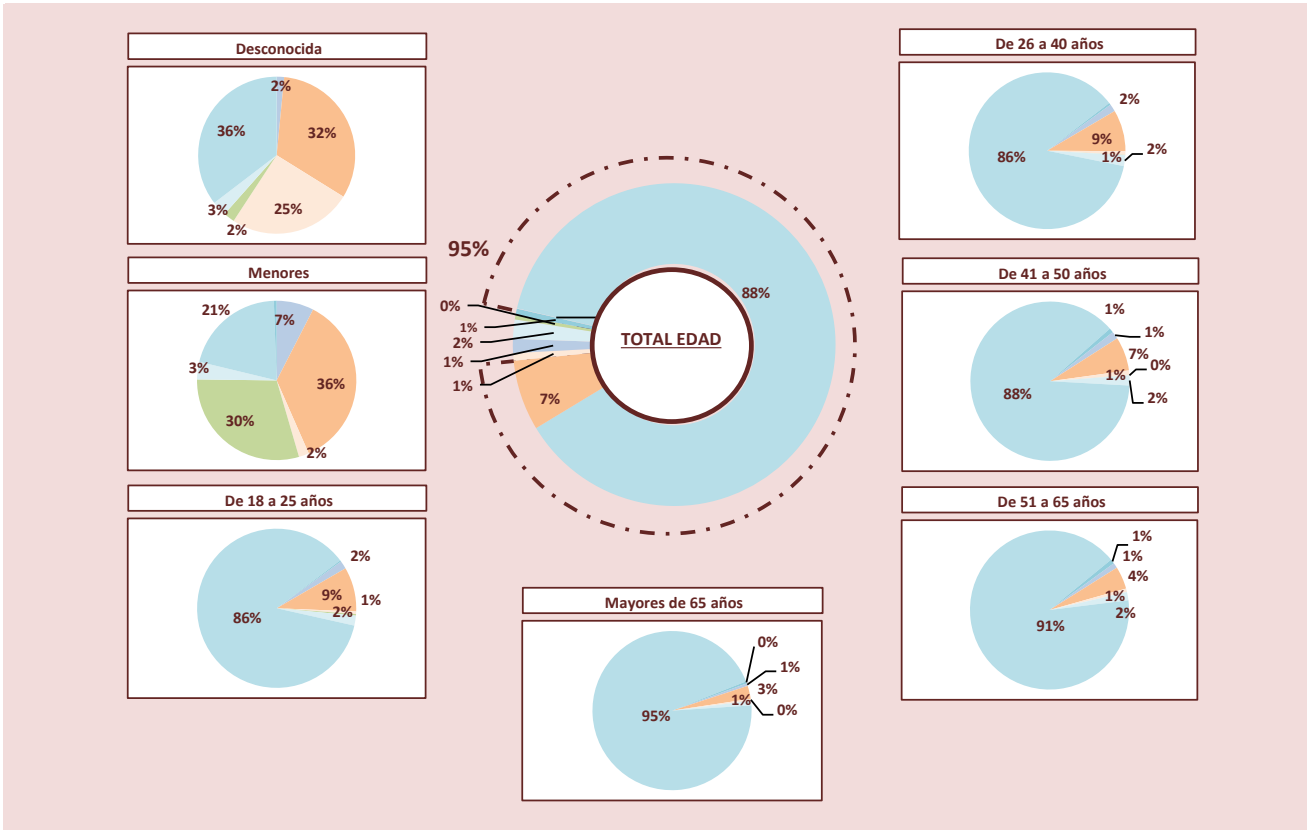
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (HOMBRE)

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

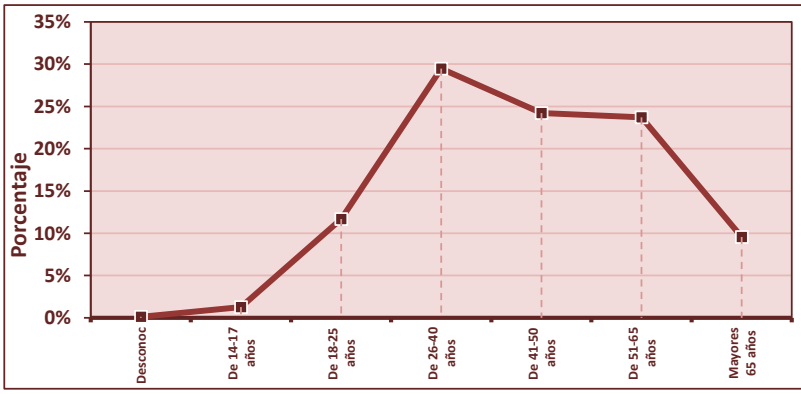
>> 4.12. Victimizaciones registradas según grupo penal y edad. Año 2020

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	2	106	213	510	408	284	57
AMENAZAS Y COACCIONES	42	503	1.174	2.813	1.858	1.213	284
CONTRA EL HONOR	33	29	68	245	253	180	37
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	1	7	13	11	4
DELITOS SEXUALES(*)	3	417	41	15	9	0	2
FALSIFICACIÓN INFORMÁTICA	4	50	263	741	548	443	98
FRAUDE INFORMÁTICO	46	290	11.240	28.437	23.698	24.109	10.150
INTERFERENCIA EN DATOS Y EN SISTEMA	0	8	36	141	248	240	46
Total VICTIMIZACIONES	**130**	**1.403**	**13.036**	**32.909**	**27.035**	**26.480**	**10.678**

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



>> 4.13. Edad de la víctima. Año 2020



Grupo de edad	Víctimas
Edad desconocida	130
Menores de edad	1.403
De 18 a 25 años	13.036
De 26 a 40 años	32.909
De 41 a 50 años	27.035
De 51 a 65 años	26.480
Mayores 65 años	10.678
TOTAL	**111.671**

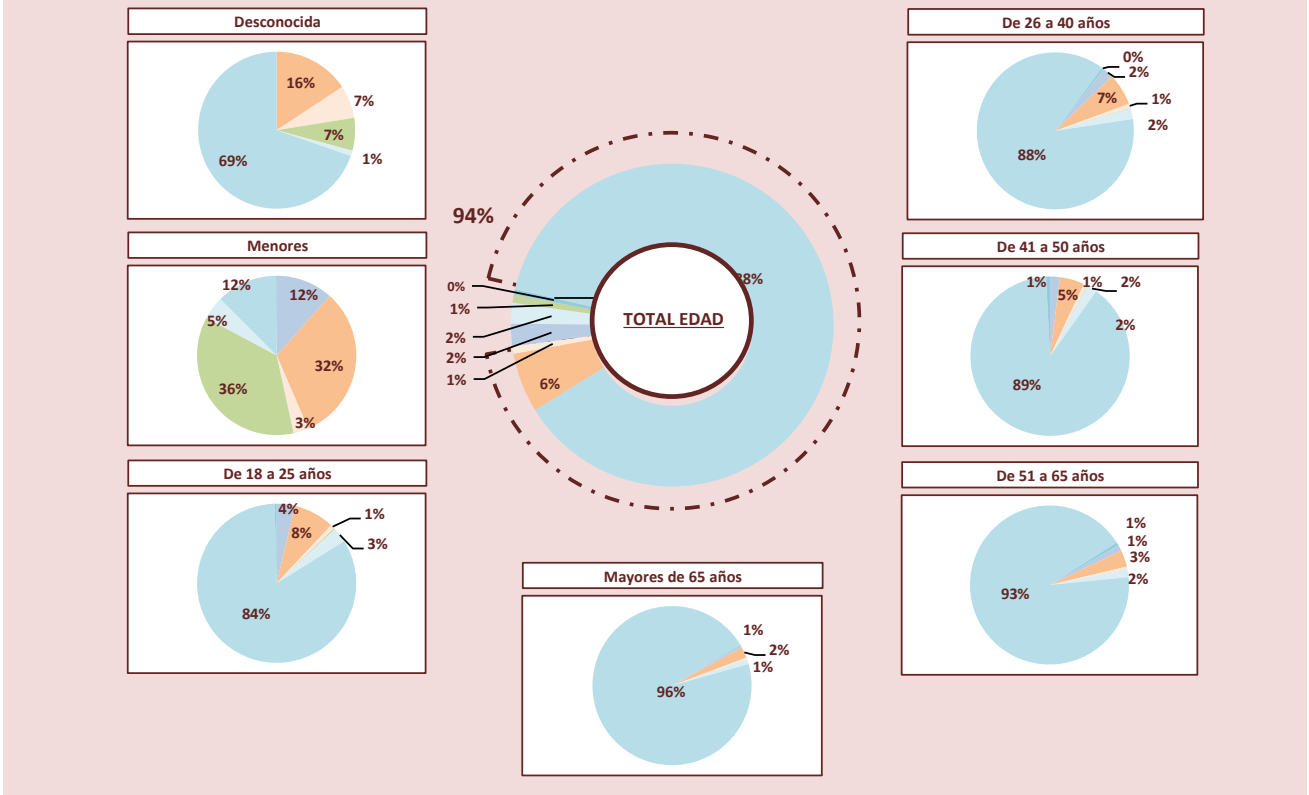
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (MUJER)

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

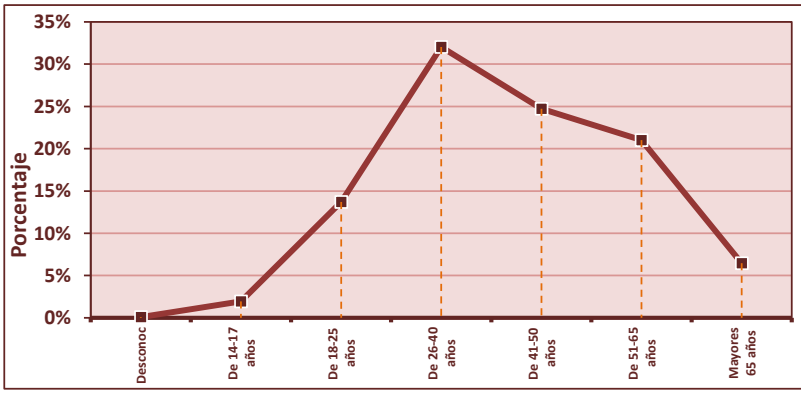
>> 4.14. Victimizaciones registradas según grupo penal y edad. Año 2020

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	235	526	752	510	268	24
AMENAZAS Y COACCIONES	14	646	1.178	2.196	1.280	740	151
CONTRA EL HONOR	6	61	119	276	185	112	15
CONTRA PROPIEDAD INDUST./INTELEC.	0	1	2	15	7	3	0
DELITOS SEXUALES(*)	6	733	36	39	33	6	2
FALSIFICACIÓN INFORMÁTICA	1	95	430	716	509	344	73
FRAUDE INFORMÁTICO	62	249	11.859	29.094	22.930	20.202	6.432
INTERFERENCIA EN DATOS Y EN SISTEMA	0	4	57	141	209	136	13
Total VICTIMIZACIONES	**89**	**2.024**	**14.207**	**33.229**	**25.663**	**21.811**	**6.710**

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



>> 4.15. Edad de la víctima. Año 2020



Grupo de edad	Víctimas
Edad desconocida	89
Menores de edad	2.024
De 18 a 25 años	14.207
De 26 a 40 años	33.229
De 41 a 50 años	25.663
De 51 a 65 años	21.811
Mayores 65 años	6.710
TOTAL	**103.733**

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

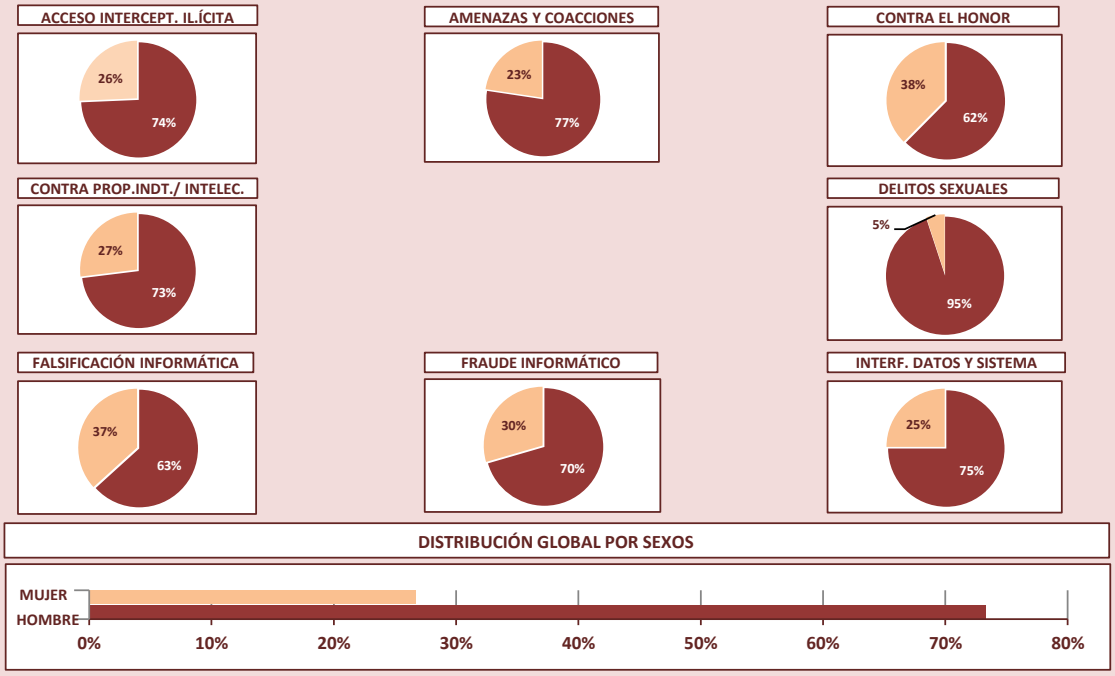
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 4.16. Detenciones/investigados registrados según grupo penal y sexo. Año 2020

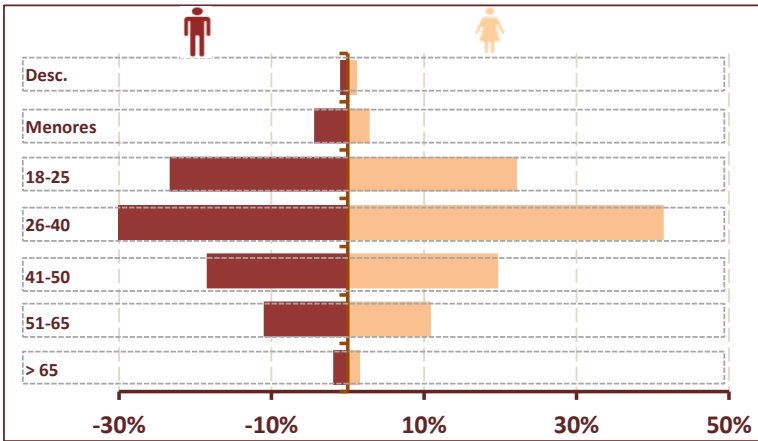
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	333	115	448
AMENAZAS Y COACCIONES	1.676	490	2.166
CONTRA EL HONOR	108	65	173
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	84	31	115
DELITOS SEXUALES(*)	734	39	773
FALSIFICACIÓN INFORMÁTICA	267	155	422
FRAUDE INFORMÁTICO	5.047	2.112	7.159
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	18	6	24
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**8.267**	**3.013**	**11.280**

(*)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 2020



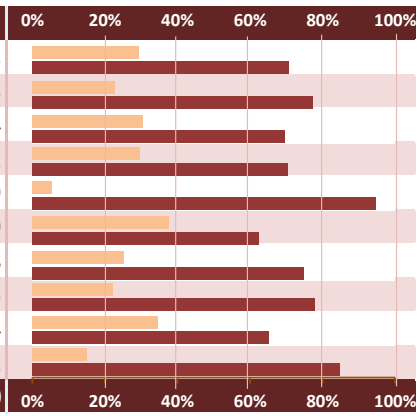
Grupo de edad	Hombre	Mujer
Edad desconocida	84	37
De 14 a 17 años	366	87
De 18 a 25 años	1.931	669
De 26 a 40 años	3.285	1.249
De 41 a 50 años	1.530	594
De 51 a 65 años	913	329
Mayores 65 años	158	48
TOTAL	**8.267**	**3.013**

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

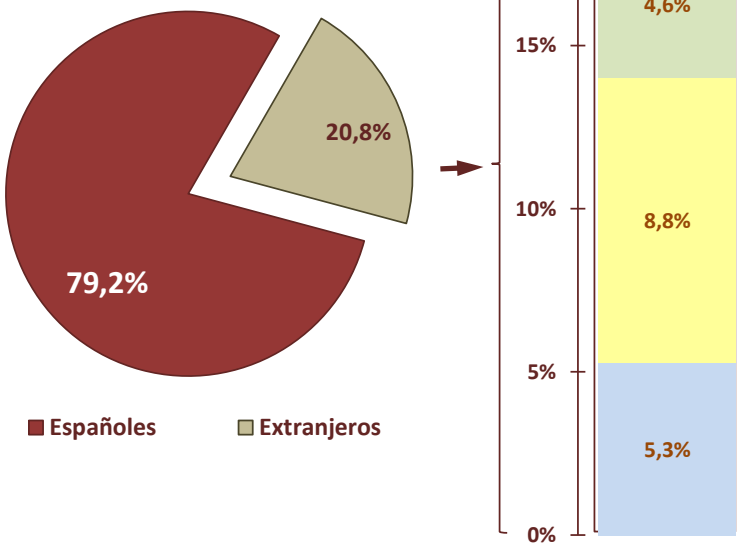
>> 4.18. Detenciones/investigados por tipología penal y sexo. Año 2020

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	3.575	1.478	5.053
AMENAZAS	1.425	420	1.845
ESTAFAS CON TARJETAS CRÉDITO, DÉBITO Y CHEQUES	914	400	1.314
ESTAFA BANCARIA	558	234	792
PORNOGRAFÍA DE MENORES	387	22	409
USURPACIÓN DE ESTADO CIVIL	255	154	409
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	283	95	378
COACCIONES	245	70	315
INJURIAS	81	43	124
RESTO	544	97	641
Total VICTIMIZACIONES CIBERCRIMINALIDAD	**8.267**	**3.013**	**11.280**



>> 4.19. Nacionalidad de los detenciones/investigados. Año 2020

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	**8.929**	**79,2%**
2.- EXTRANJEROS	**2.351**	**20,8%**
2.1.- UNIÓN EUROPEA	**603**	**5,3%**
RUMANÍA	297	2,6%
PORTUGAL	60	0,5%
BULGARIA	58	0,5%
FRANCIA	54	0,5%
ITALIA	48	0,4%
Resto	86	0,8%
2.2.- AMÉRICA	**997**	**8,8%**
VENEZUELA	222	2,0%
DOMINICANA	154	1,4%
COLOMBIA	151	1,3%
Resto	470	4,2%
2.3.- ÁFRICA	**517**	**4,6%**
MARRUECOS	325	2,9%
NIGERIA	59	0,5%
Resto	133	1,2%
2.4.- ASIA	**86**	**0,8%**
CHINA POPULAR	27	0,2%
PAQUISTÁN	23	0,2%
Resto	36	0,3%
2.5.- RESTO PAÍSES	**148**	**1,3%**
REINO UNIDO	24	0,2%
RUSIA	22	0,2%
Otros	102	0,9%
TOTAL	**11.280**	**100%**



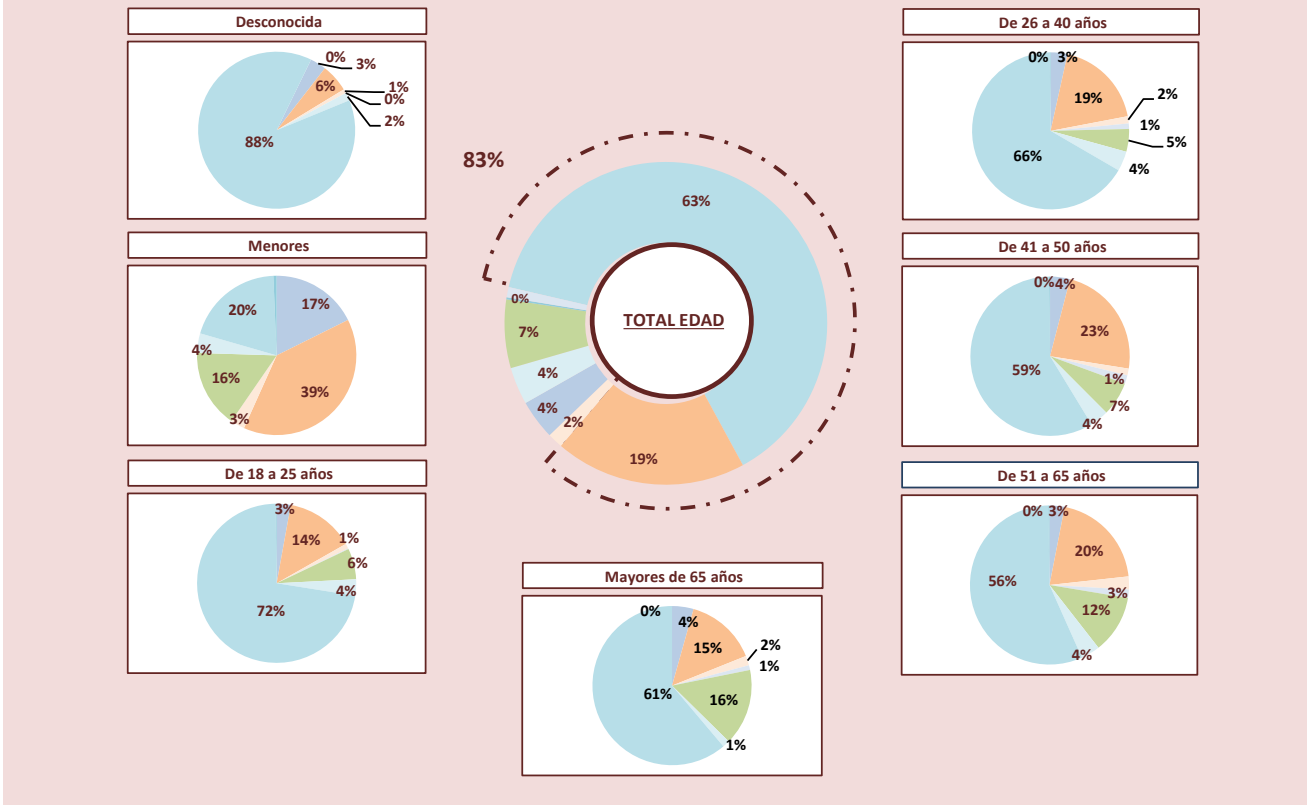
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

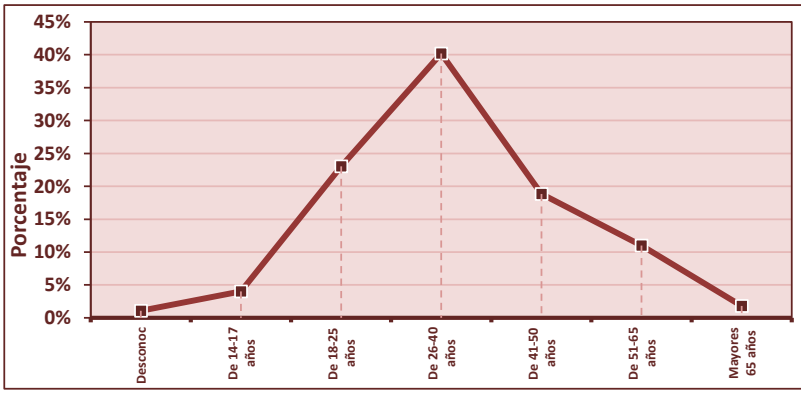
>> 4.20. Detenciones/investigados registradas según grupo penal y edad. Año 2020

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	4	80	74	157	86	38	9
AMENAZAS Y COACCIONES	7	177	362	841	498	251	30
CONTRA EL HONOR	1	13	26	67	29	33	4
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	4	51	37	21	2
DELITOS SEXUALES(*)	0	72	163	212	147	147	32
FALSIFICACIÓN INFORMÁTICA	2	18	86	185	80	48	3
FRAUDE INFORMÁTICO	107	90	1879	3013	1.243	701	126
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	6	8	4	3	0
Total DETENCIONES/INVESTIGADOS	**121**	**453**	**2.600**	**4.534**	**2.124**	**1.242**	**206**

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



>> 4.21. Edad de las personas detenidas/investigadas. Años 2020



Grupo de edad	Det./Inv.
Edad desconocida	121
De 14 a 17 años	453
De 18 a 25 años	2.600
De 26 a 40 años	4.534
De 41 a 50 años	2.124
De 51 a 65 años	1.242
Mayores 65 años	206
TOTAL	**11.280**

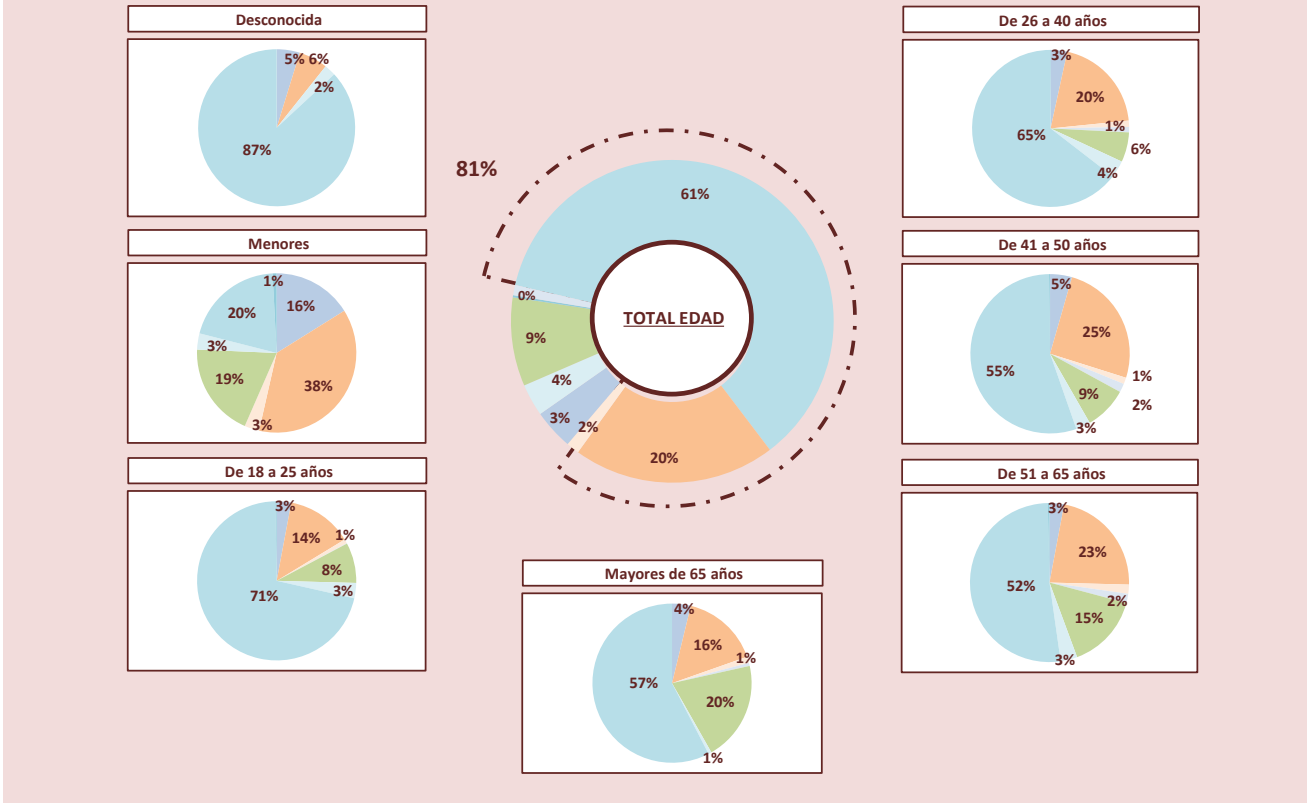
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

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

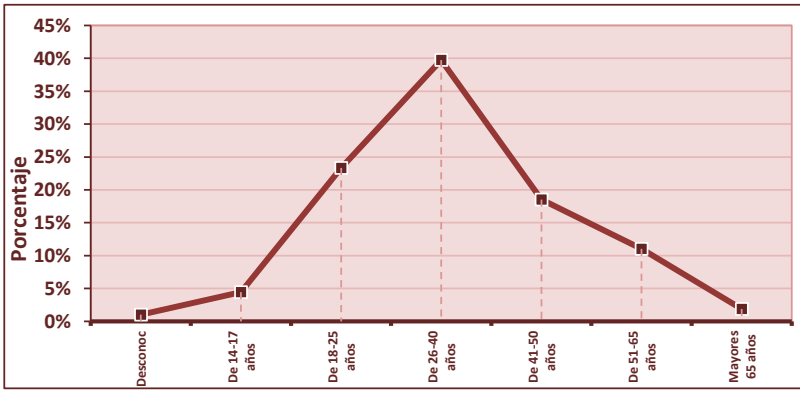
>> 4.22. Detenciones/investigados registradas según grupo penal y edad. Año 2020

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	4	59	57	112	68	27	6
AMENAZAS Y COACCIONES	5	137	258	657	389	205	25
CONTRA EL HONOR	0	11	16	42	20	17	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	37	27	17	1
DELITOS SEXUALES(*)	0	70	158	201	134	139	32
FALSIFICACIÓN INFORMÁTICA	2	12	60	116	45	31	1
FRAUDE INFORMÁTICO	73	74	1.375	2.116	844	474	91
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	5	4	3	3	0
Total DETENCIONES/INVESTIGADOS	**84**	**366**	**1.931**	**3.285**	**1.530**	**913**	**158**

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



>> 4.23. Edad de las personas detenidas/investigadas. Años 2020



Grupo de edad	Det./Inv.
Edad desconocida	84
De 14 a 17 años	366
De 18 a 25 años	1.931
De 26 a 40 años	3.285
De 41 a 50 años	1.530
De 51 a 65 años	913
Mayores 65 años	158
TOTAL	**8.267**

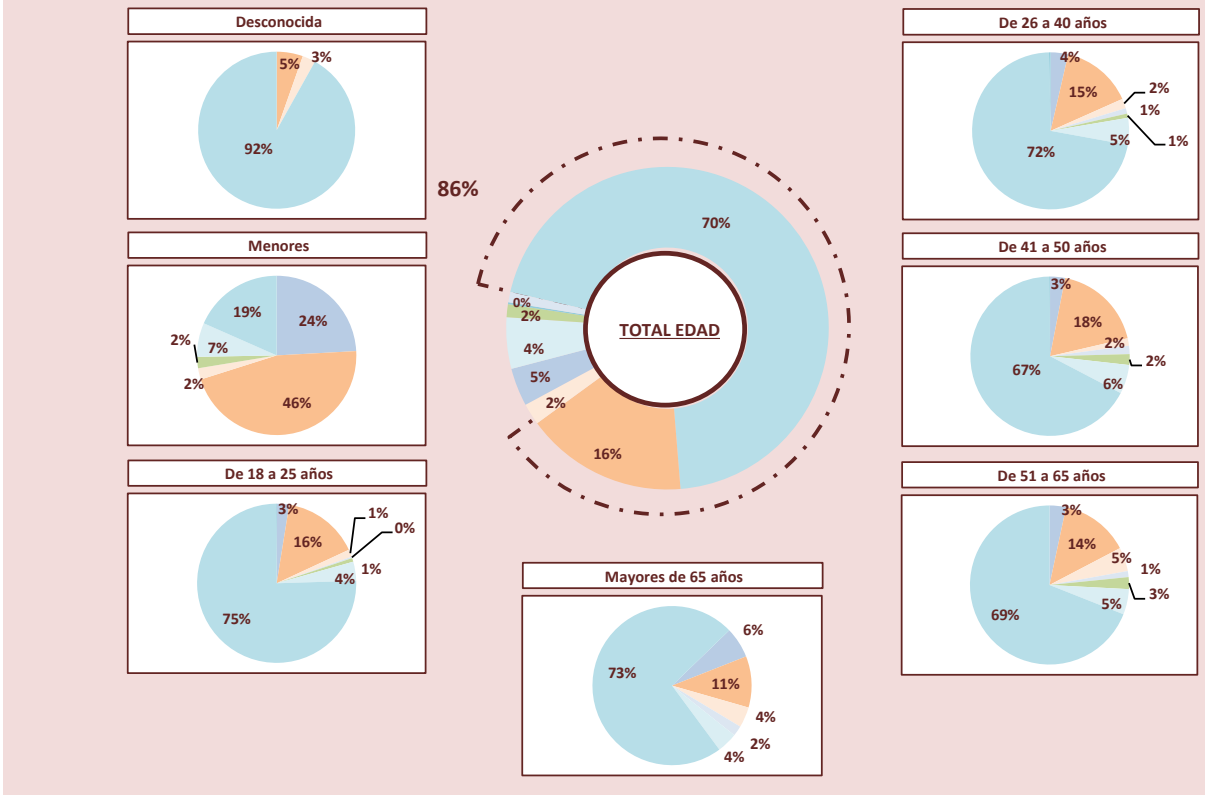
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

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

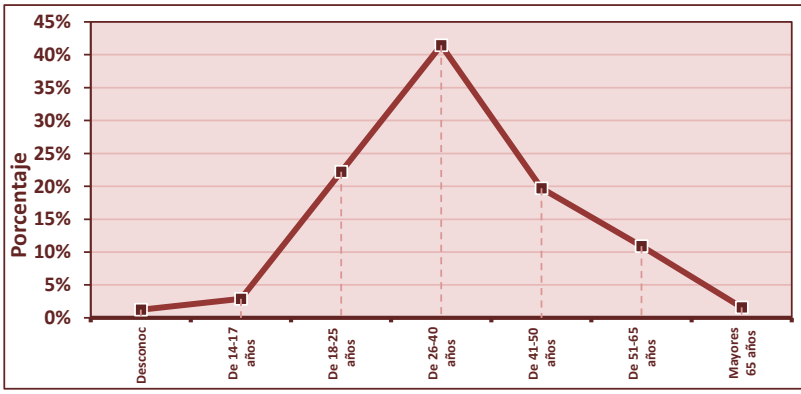
>> 4.24. Detenciones/investigados registradas según grupo penal y edad. Año 2020

GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	21	17	45	18	11	3
AMENAZAS Y COACCIONES	2	40	104	184	109	46	5
CONTRA EL HONOR	1	2	10	25	9	16	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	14	10	4	1
DELITOS SEXUALES(*)	0	2	5	11	13	8	0
FALSIFICACIÓN INFORMÁTICA	0	6	26	69	35	17	2
FRAUDE INFORMÁTICO	34	16	504	897	399	227	35
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	1	4	1	0	0
Total DETENCIONES/INVESTIGADOS	**37**	**87**	**669**	**1.249**	**594**	**329**	**48**

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



>> 4.25. Edad de las personas detenidas/investigadas. Años 2020



Grupo de edad	Det./Inv.
Edad desconocida	37
De 14 a 17 años	87
De 18 a 25 años	669
De 26 a 40 años	1.249
De 41 a 50 años	594
De 51 a 65 años	329
Mayores 65 años	48
TOTAL	**3.013**

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 2020)

Porcentaje de viviendas con / sin algún tipo de ordenador

Porcentaje de viviendas con / sin acceso a internet

Contraste evolutivo de las viviendas 2011-2020

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=39397&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 2020)

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=39398&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 2020)

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=39526&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 2020)

Porcentaje personas que han comprado alguna vez por internet

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=39393&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 2020. Spain (Comisión Europea)

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66959

>> 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 y victimizaciones. Como consecuencia de la incorporación al presente informe de los datos de la Ertzaintza y Mossos d' Esquadra, las series históricas publicadas hasta la fecha se han visto alteradas.

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. Se adjunta cuadro explicativo al final de la metadata.

No obstante, además de las conductas que introduce el Convenio de Budapest, nuestra realidad criminal denota que existen otras categorías distintas que conviene reseñar. Es pues, que cuando los medios empleados en su comisión sean las tecnologías de la información y la 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 muerto.
- 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.

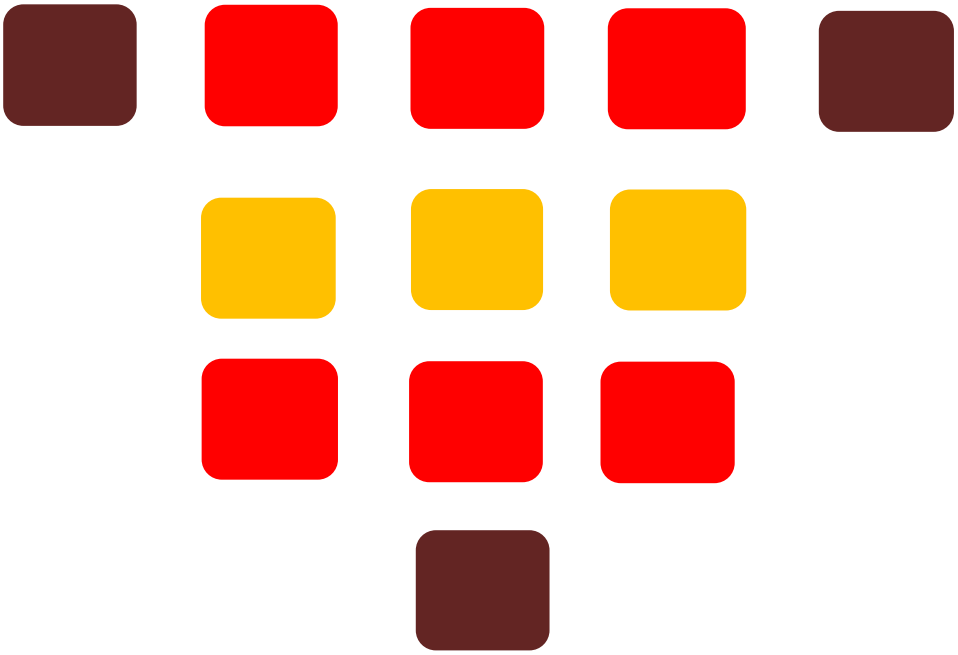
- Total denuncias: 1
- Total víctimas: 2
- Total victimizaciones: 5 (3 hechos de malos tratos al denunciante + 1 delito de amenazas al denunciante + 1 hecho de malos tratos al niño).

Hay que significar, que como se ha apuntado anteriormente, sólo hay datos de victimizaciones 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 victimizaciones del País Vasco están infrarrepresentados.

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 CREDITO, DEBITO 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	

ESPAÑA



2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

2020