

11

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 M^a SANTIAGO OROZCO
MIGUEL ÁNGEL GÓMEZ MARTÍN


**MINISTERIO
DEL INTERIOR**

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

10

54

2020
5050

1

INTRODUCCIÓN >>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

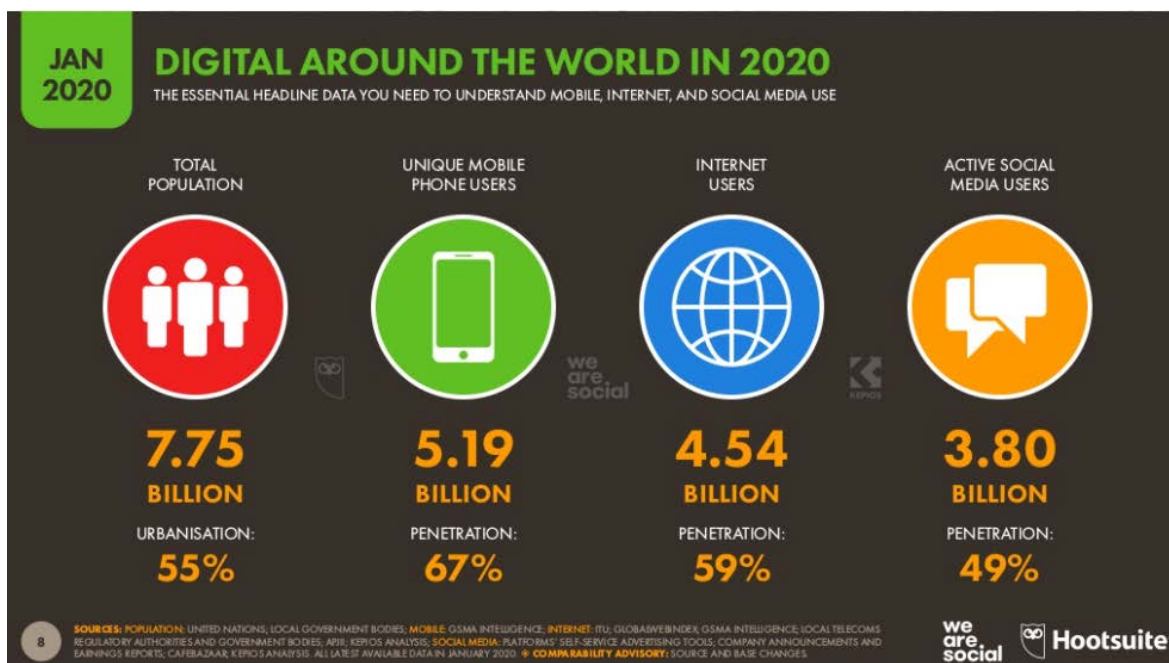
A tales fines responde la publicación de este **VIII Informe sobre Cibercriminalidad**, correspondiente a la delincuencia informática registrada en el año 2020.

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 añan 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.

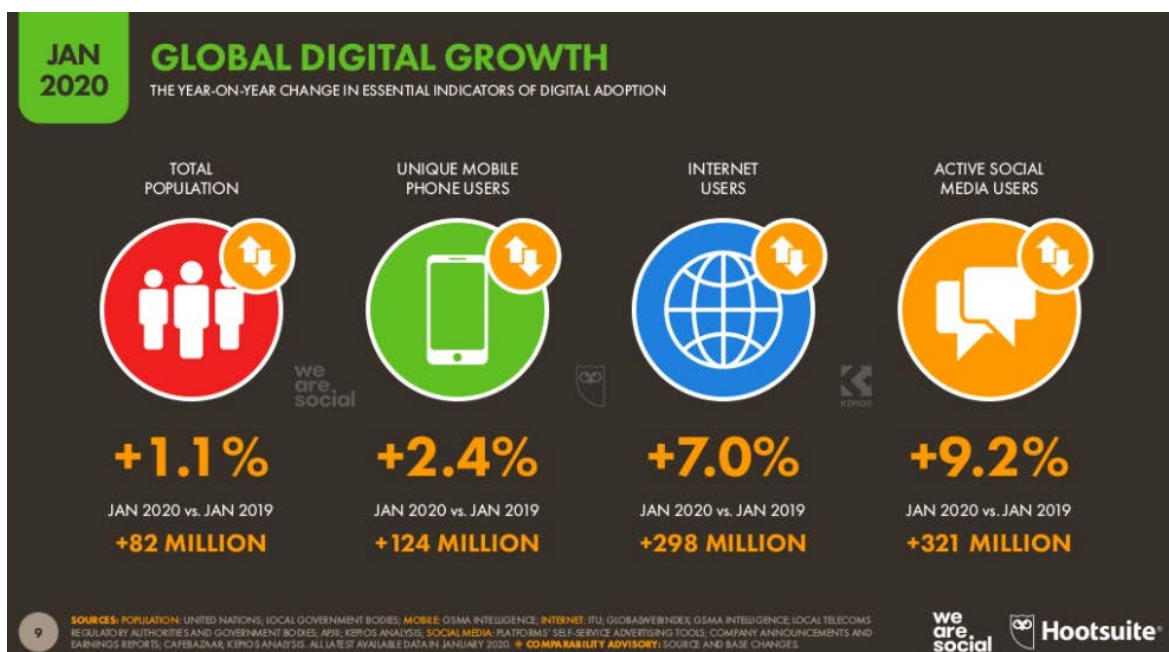
Para el capítulo de victimizaciones, con la excepción de la Ertzaintza, se detallan igualmente datos de todas las Fuerzas y Cuerpos de Seguridad. Es por ello, que las series históricas publicadas hasta la fecha, se han visto modificadas, como consecuencia del nuevo suministro de datos por estos cuerpos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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Infografía nº 1.- Usuarios de nuevas tecnologías a nivel mundial².



Infografía nº 2.- Incremento de usuarios de nuevas tecnologías a nivel mundial³.

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>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 mundial⁴.

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 2020⁵), 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>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

acceder a la infraestructura de la organización del empleado para conseguir diferentes fines, entre los que el ciberspionaje 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 ciberdelincuencia⁷. En el caso concreto de Europa ha destacado cuatro conclusiones principales:

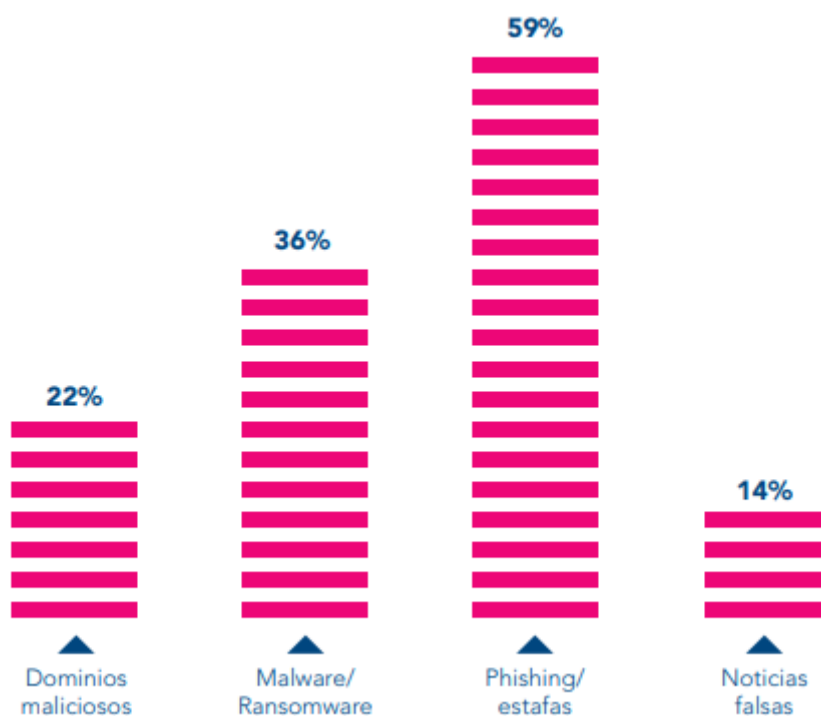
- Dos tercios de los países miembros de Europa han informado del considerable aumento de dominios maliciosos registrados con las palabras clave “COVID” o “corona” para sacar partido del número creciente de personas que buscan información en Internet sobre la COVID-19.
- Los ciberdelincuentes están aprovechando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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- 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-CERT⁸ 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>

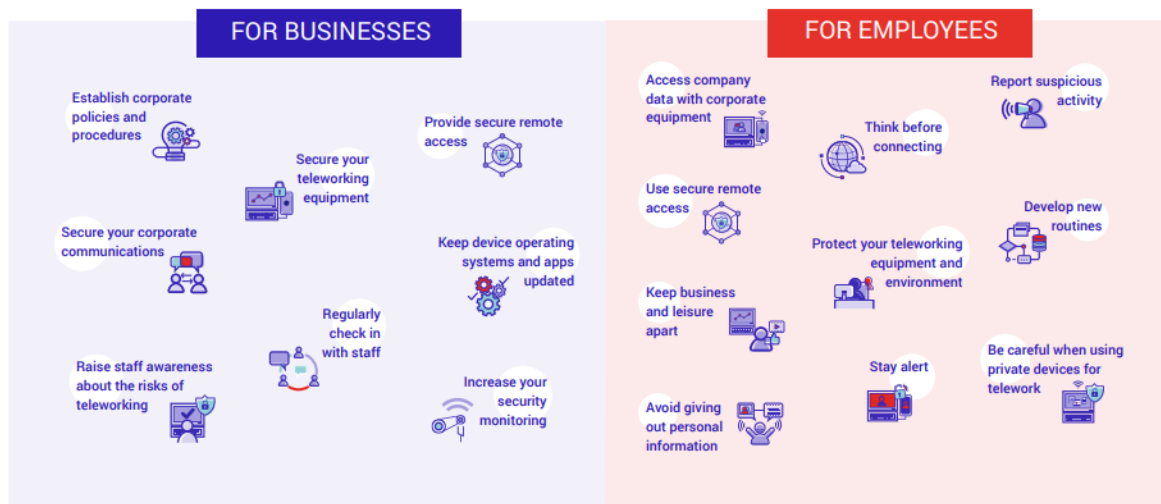
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 Europol⁹) han elaborado al respecto.

SAFE TELEWORKING



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

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.

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

A partial screenshot from the REvil ransomware group's Dark Web blog.

*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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Ciberseguridad, con el fin de reforzar y difundir los conocimientos especializados en materia de ciberseguridad en toda la Unión Europea¹⁰.

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 artificial¹¹.
4. España se ha situado en el cuarto puesto a nivel mundial en el *Global Cybersecurity Index* de 2020¹², 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>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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-privada¹³.

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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 PCR¹⁵, 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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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*.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 conocidos¹⁷. 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 ranking 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 215.507¹⁸, 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 puede 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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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
5050

11

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

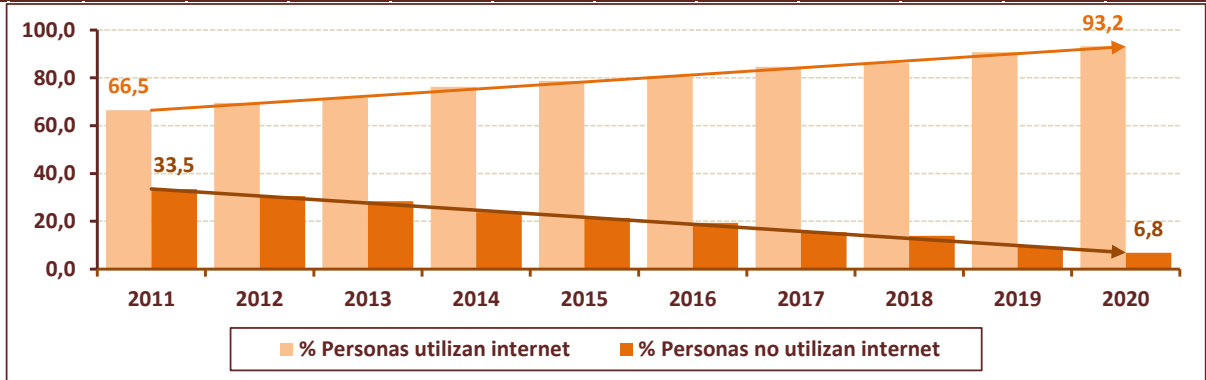
2.-

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

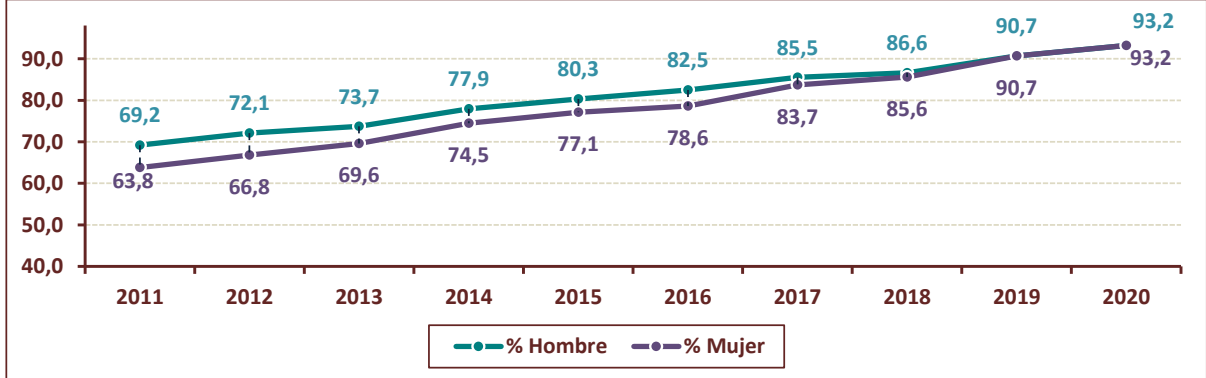
(Fuente de datos: INE)

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

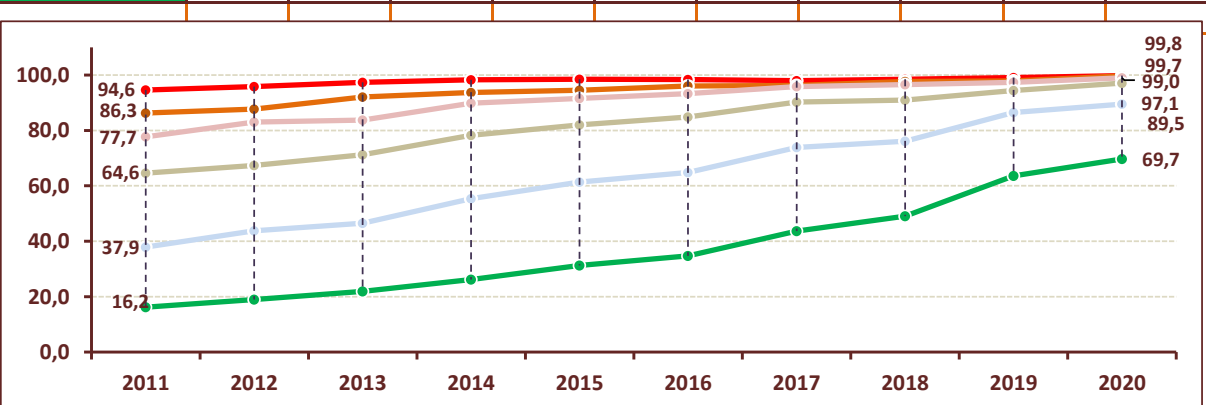
	% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Utilizado internet	66,5	69,5	71,6	76,2	78,7	80,6	84,6	86,1	90,7	93,2
No utilizado internet	33,5	30,5	28,4	23,8	21,3	19,4	15,4	13,9	9,3	6,8



	% 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



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

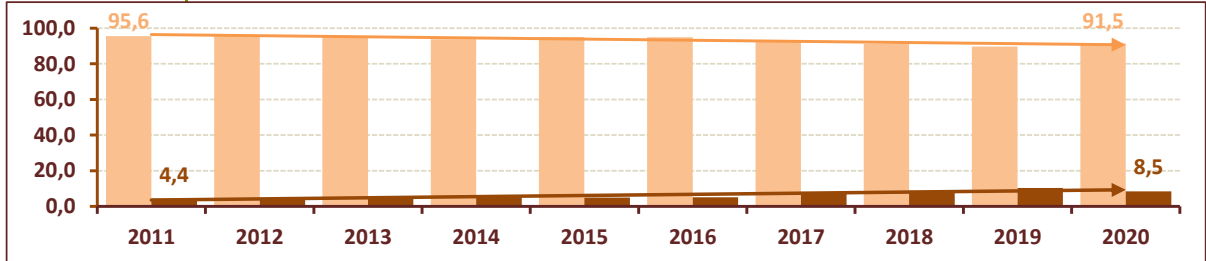
2.-

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

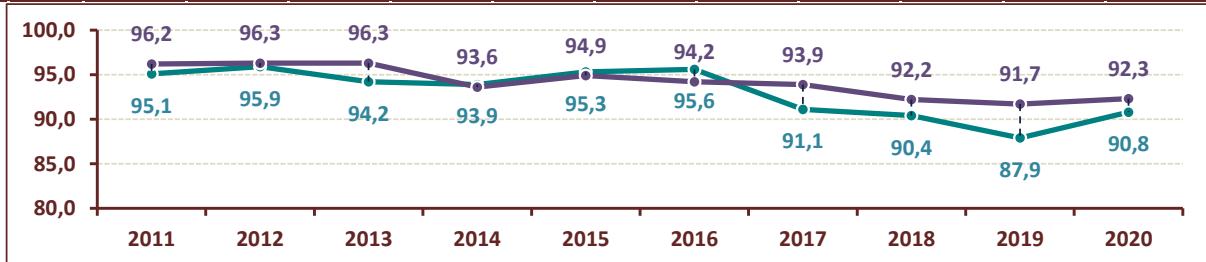
(Fuente de datos: INE)

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

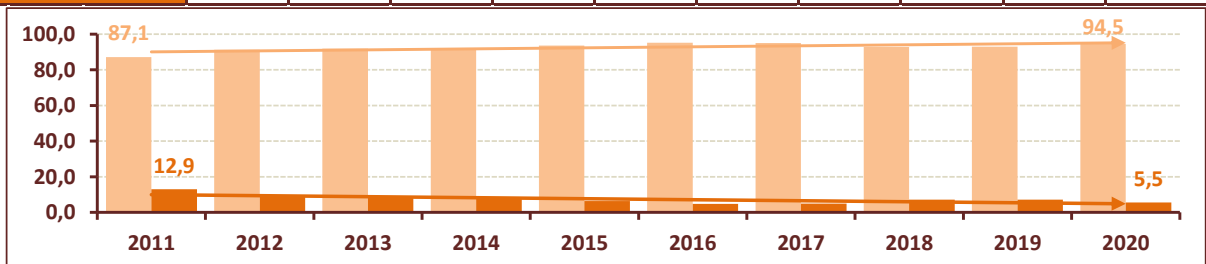
	% DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Utilizado ordenador	95,6	96,1	95,2	93,8	95,1	94,9	92,4	91,3	89,7	91,5
No utilizado ordenador	4,4	3,9	4,8	6,2	4,9	5,1	7,6	8,7	10,3	8,5



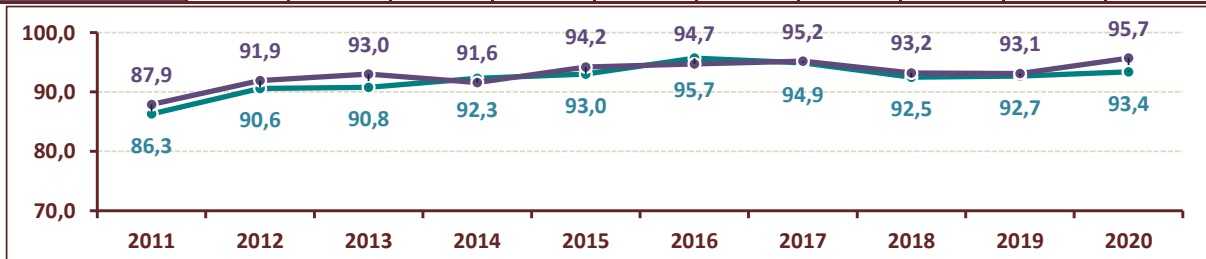
	% POR SEXO DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Hombre	95,1	95,9	94,2	93,9	95,3	95,6	91,1	90,4	87,9	90,8
Mujer	96,2	96,3	96,3	93,6	94,9	94,2	93,9	92,2	91,7	92,3



	% 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



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

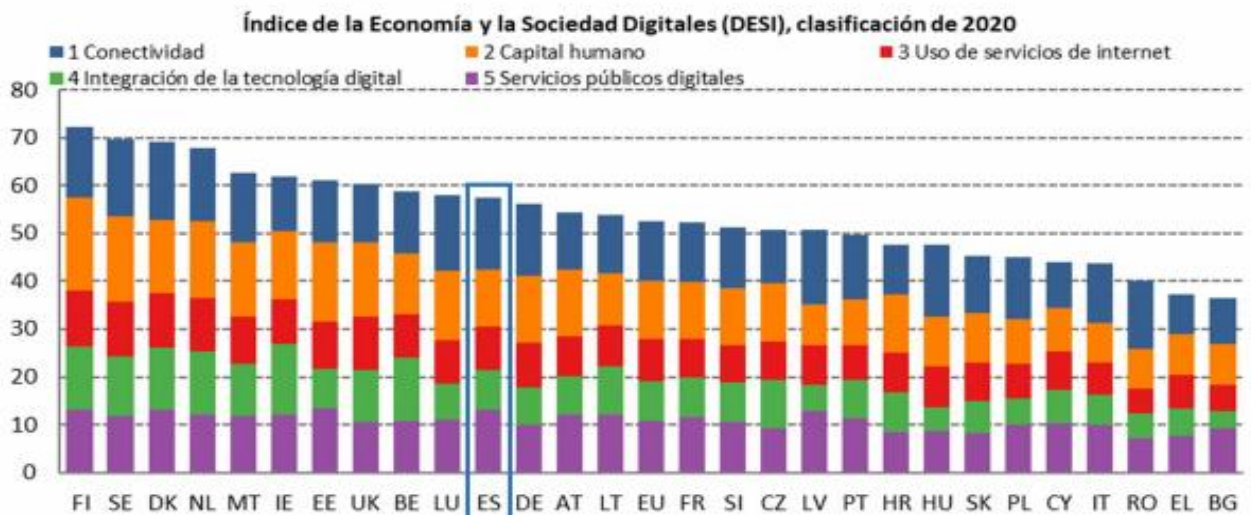
2.-

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: Comisión Europea)

>> 2.6. Índice 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



2020
5050

3

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD



3.-



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

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%).

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

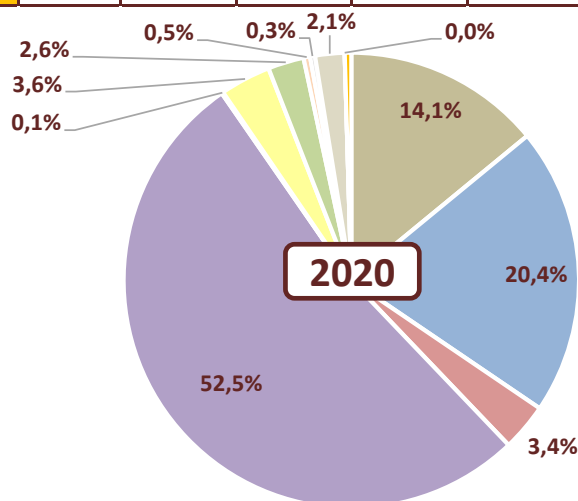
3.-

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**



2020
5050

11

4

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

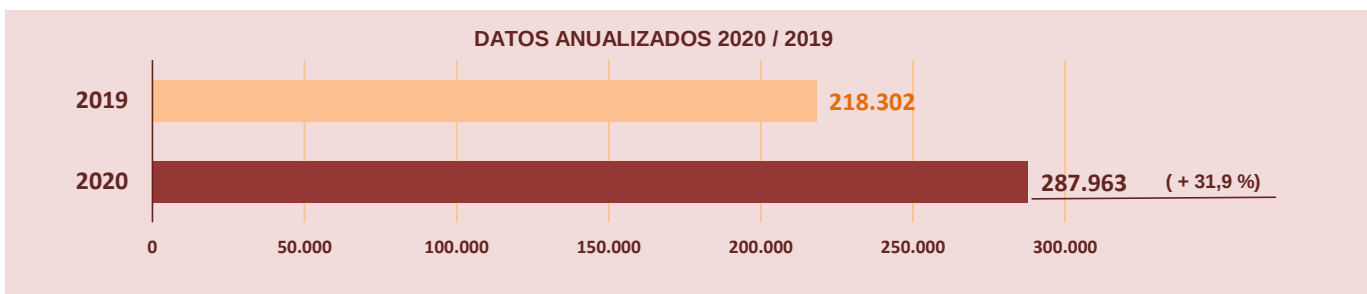
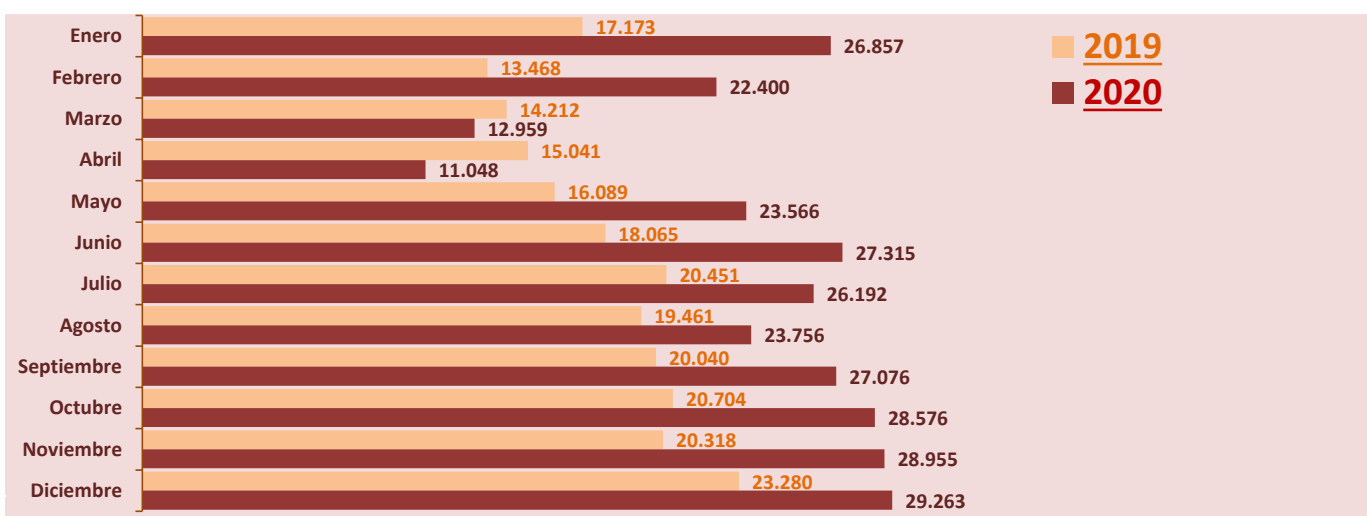
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 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



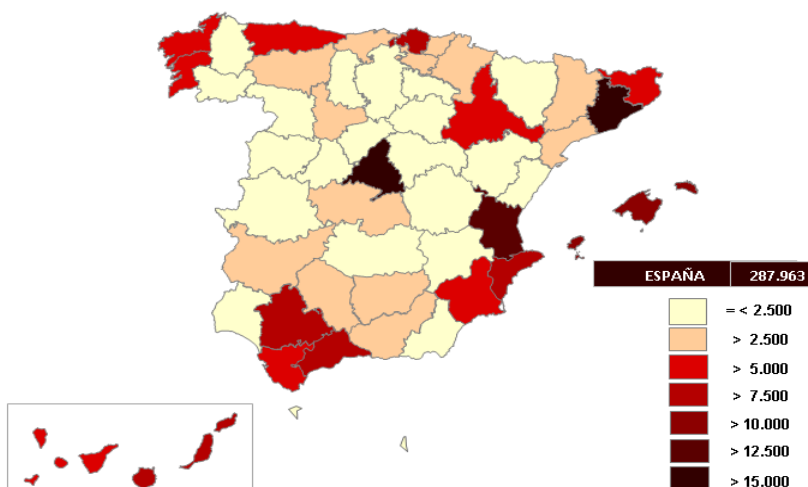
(Fuente de datos: Sistema Estadístico de Criminalidad)

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

ESPAÑA	287.963
	= <15.000
	> 15.000
	> 20.000
	> 25.000
	> 30.000
	> 35.000
	> 40.000

(*) 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

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



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

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

ACCESO INTERCEPT. ILÍCITA

Sexo	Porcentaje
Mujer	59%
Hombre	41%

AMENAZAS Y COACCIONES

Sexo	Porcentaje
Mujer	44%
Hombre	56%

CONTRA EL HONOR

Sexo	Porcentaje
Mujer	48%
Hombre	52%

CONTRA PROP.INDT./ INTELEC.

Sexo	Porcentaje
Mujer	44%
Hombre	56%

DELITOS SEXUALES

Sexo	Porcentaje
Mujer	64%
Hombre	36%

FALSIFICACIÓN INFORMÁTICA

Sexo	Porcentaje
Mujer	50%
Hombre	50%

FRAUDE INFORMÁTICO

Sexo	Porcentaje
Mujer	48%
Hombre	52%

INTERF. DATOS Y SISTEMA

Sexo	Porcentaje
Mujer	44%
Hombre	56%

DISTRIBUCIÓN GLOBAL POR SEXOS

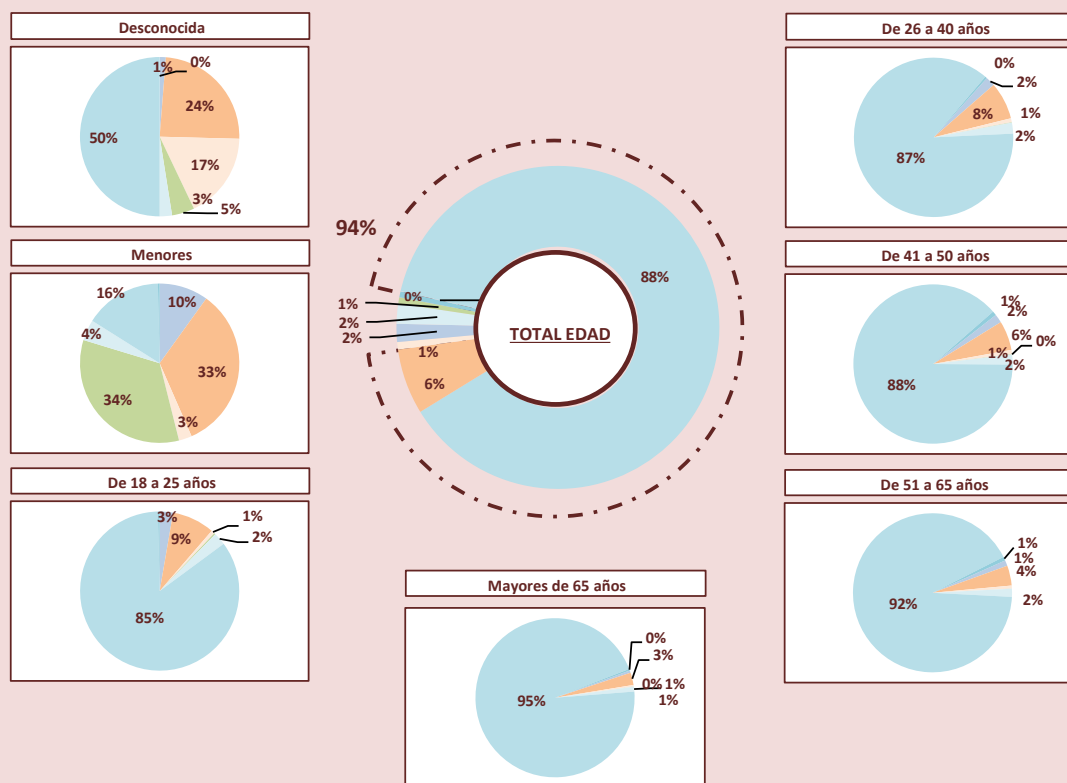
Sexo	Porcentaje
Mujer	48%
Hombre	52%

Faixa Etária	Homens (%)	Mulheres (%)
Desc.	~5	~5
Menores	~5	~5
18-25	~12	~12
26-40	~28	~32
41-50	~25	~28
51-65	~22	~25
> 65	~10	~8

44

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

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



Este gráfico de líneas ilustra la distribución por edad de la población que se identifica como LGBT. El eje vertical representa el porcentaje, variando de 0% a 35% en incrementos de 5%. El eje horizontal muestra las categorías de edad: Desconoc, De 14-17 años, De 18-25 años, De 25-40 años, De 41-50 años, De 51-65 años, y Mayores 65 años. La línea roja con marcadores cuadrados muestra un aumento progresivo desde la juventud hasta el grupo de 25-40 años, donde se registra el porcentaje más alto (aproximadamente 31%). Posteriormente, el porcentaje disminuye en los grupos de 41-50 años (aproximadamente 25%), 51-65 años (aproximadamente 23%) y Mayores 65 años (aproximadamente 8%).

Edad	Porcentaje
Desconoc	0%
De 14-17 años	2%
De 18-25 años	13%
De 25-40 años	31%
De 41-50 años	25%
De 51-65 años	23%
Mayores 65 años	8%

46

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

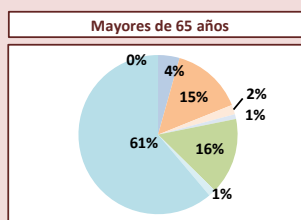
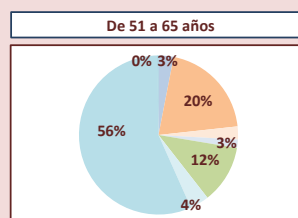
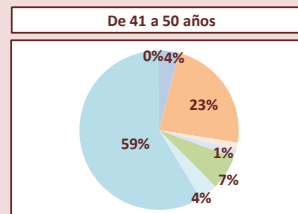
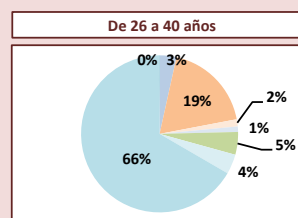
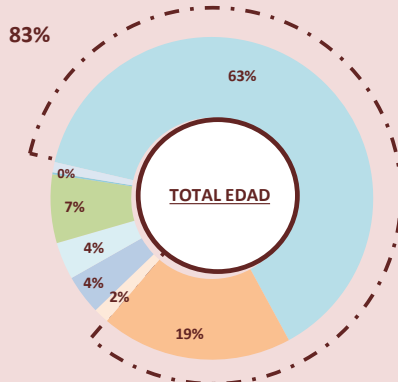
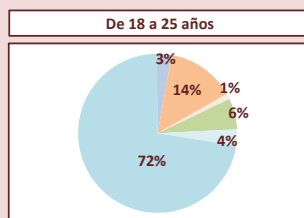
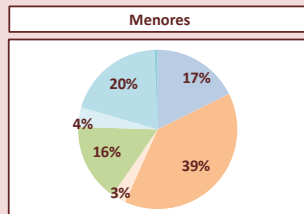
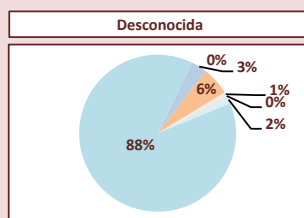
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

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

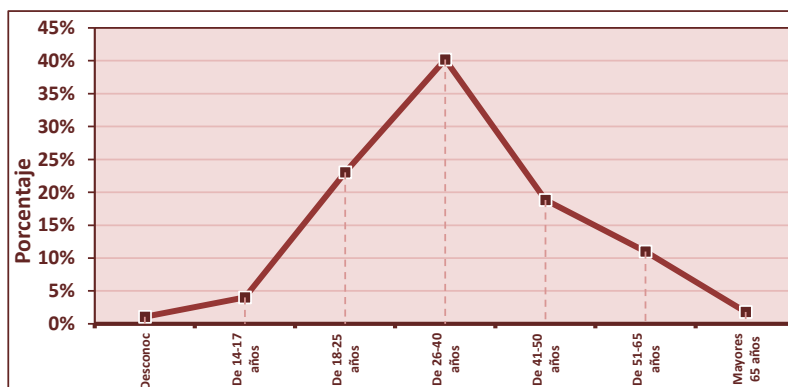


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	4	80	74	157	86	38	9
AMENAZAS Y COACCIONES	7	177	362	841	498	251	30
CONTRA EL HONOR	1	13	26	67	29	33	4
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	4	51	37	21	2
DELITOS SEXUALES(*)	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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

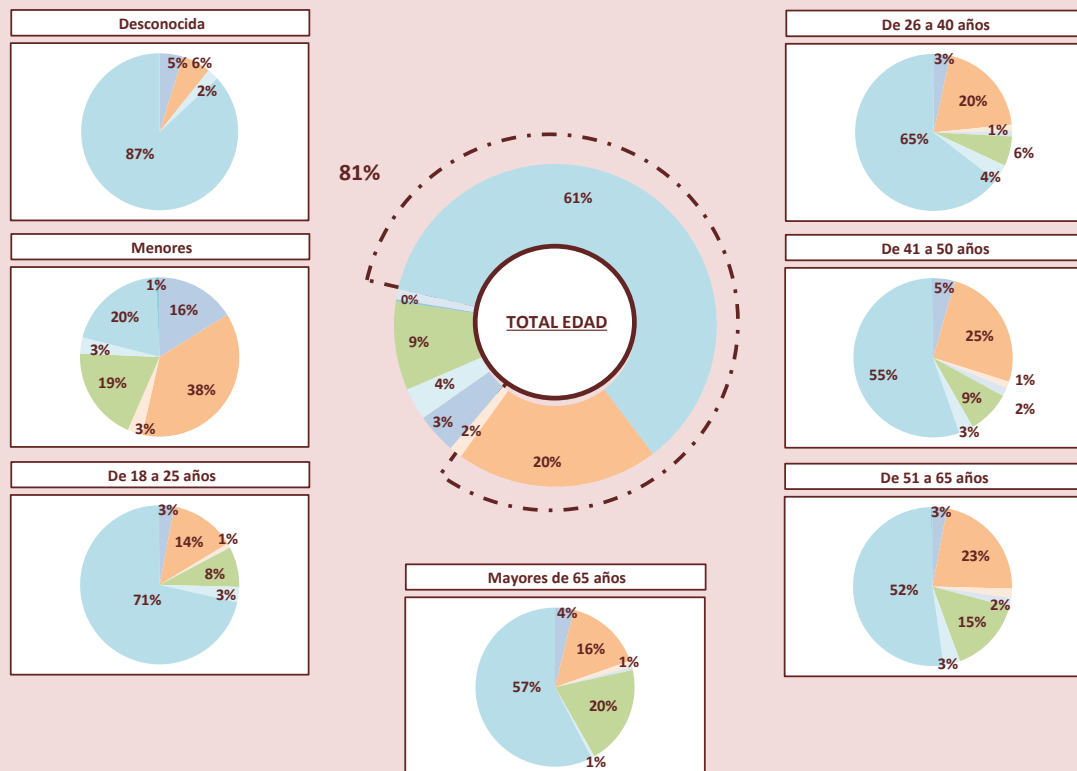
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

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

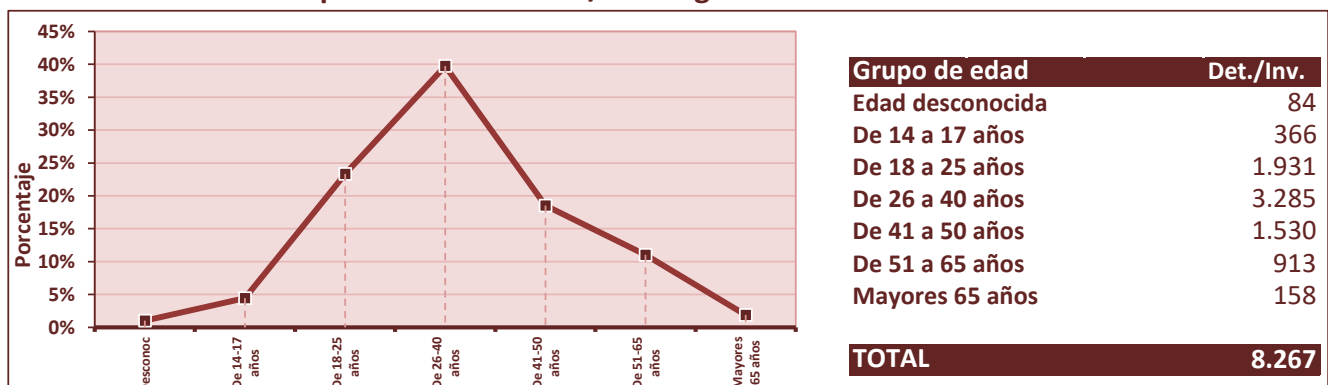


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	4	59	57	112	68	27	6
AMENAZAS Y COACCIONES	5	137	258	657	389	205	25
CONTRA EL HONOR	0	11	16	42	20	17	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	37	27	17	1
DELITOS SEXUALES(*)	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



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.-

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

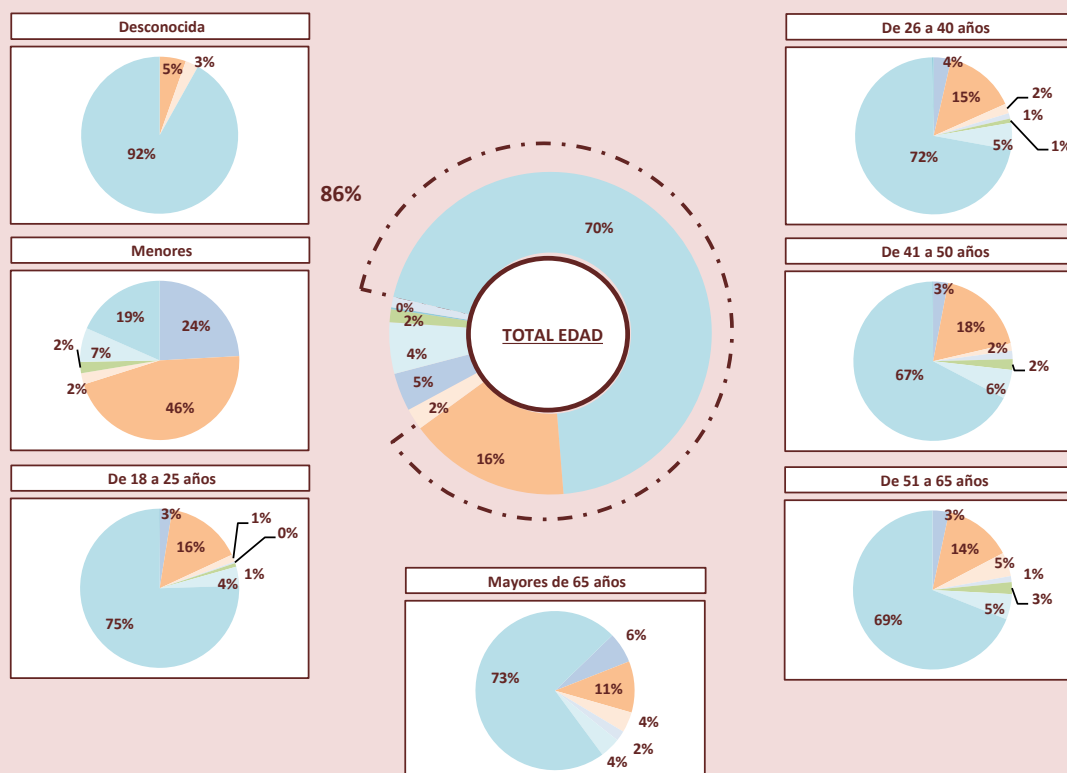
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

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

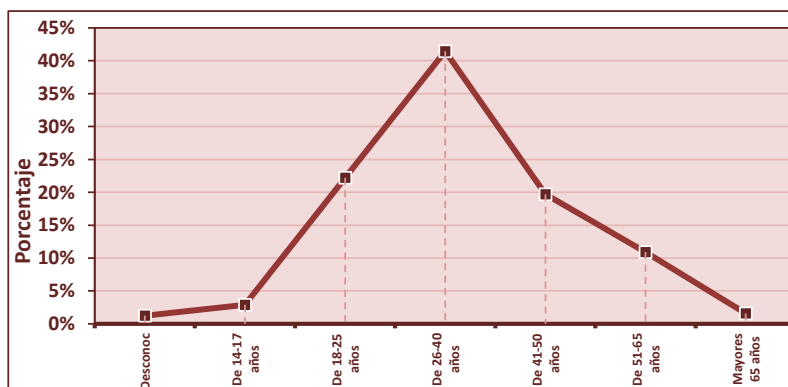


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	21	17	45	18	11	3
AMENAZAS Y COACCIONES	2	40	104	184	109	46	5
CONTRA EL HONOR	1	2	10	25	9	16	2
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	14	10	4	1
DELITOS SEXUALES(*)	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

2020
5050

11

5

METADATA >>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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)

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

>> 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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

Concepto de conocidos, esclarecidos, detenciones/investigados y victimizaciones

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

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

- Detención del autor “in fraganti”.
- Identificación plena del autor, o alguno de los autores, sin necesidad de que esté detenido, aunque se encuentre en situación de libertad provisional, huido o 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

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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).

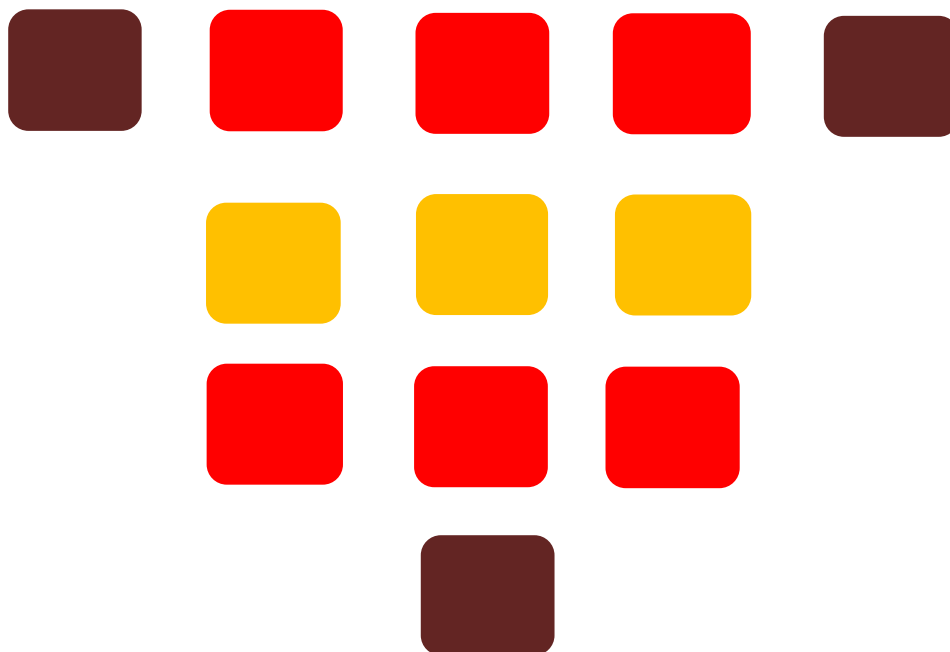
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD									
DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SECA 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 LEGAL 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	FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE ÚTILES 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	ESTAFAS	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.						
		OTRAS ESTAFAS	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 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	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.						
		ACOSO SEXUAL	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.						
		ABUSO SEXUAL	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.						
		CORUPCIÓN DE MENORES/INCAPACITADOS	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.						
		PORNOGRAFÍA DE MENORES	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.						
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna						
		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	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.						
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	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 y coacciones	Arts 169 a 172 y 620 del CP 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 RELIGIOSO	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.						
		COACCIONES	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.						

ESPAÑA



2020

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Síguenos en Twitter

@interiorgob

www.interior.gob.es

2020