MINISTERIO DEL INTERIOR

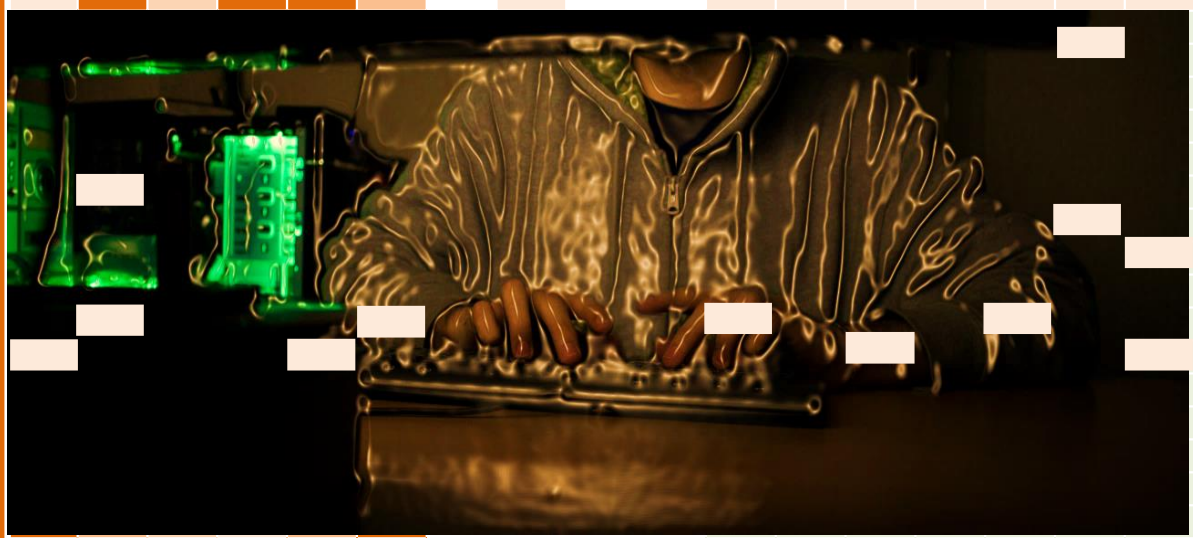
SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

seC Sistema Estadístico de Criminalidad

2018

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

Sistema Estadístico de Criminalidad

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

AUTORES

GABINETE DE COORDINACIÓN Y ESTUDIOS.
SECRETARÍA DE ESTADO DE SEGURIDAD

JAIME CERECEDA FERNÁNDEZ-ORUÑA
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 126-19-018-9

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

0 INDICE

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

Sistema Estadístico de Criminalidad

2018

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1

INTRODUCCIÓN >>

1.-INTRODUCCIÓN

La Ciberdelincuencia, se ha convertido en un fenómeno global y multidisciplinar, que requiere la acción conjunta de planes, estrategias y recursos tanto materiales como humanos, para que de una manera eficaz permitan atajar los efectos dañinos que ésta provoca. Uno de los aspectos en los que se debe incidir es la concienciación sobre la implementación en nuestros hábitos cotidianos, de una cultura de la ciberseguridad. Para impulsar dicha concienciación, se convierte en elemento facilitador la publicación de informes que alerten sobre los peligros reales y potenciales, a la par que se detalle aspectos relevantes de la realidad de este fenómeno criminal.

Desde el Ministerio del Interior, se ha decidido abordar la publicación del *VI Informe sobre Cibercriminalidad* correspondiente a la delincuencia informática registrada en el año 2018, para dar cuenta de la realidad que nos aqueja en esta materia.

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 (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra y distintos Cuerpos de Policía Local), proceden del Sistema Estadístico de Criminalidad (SEC), y de los incidentes que registra el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) en función de su ámbito de actuación y competencias.

Este documento aglutina datos del año 2018 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 información publicada por otros organismos nacionales (INE, ONTSI) e internacionales (EUROSTAT, Comisión Europea), en relación a aquellas características más relevantes que permiten perfilar los rasgos distintivos de la sociedad española en relación a las tecnologías, grado de conectividad, el uso de Internet y el acceso a los contenidos, las comunicaciones y las transacciones en línea que se realizan, así como cuál es el nivel real y de desarrollo de la sociedad digital en España.

A continuación, de manera detallada y específica, en un segundo y tercer bloque del informe se explican los datos procedentes del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC), así como los extraídos del Sistema Estadístico de Criminalidad (SEC), registrados por las Fuerzas y Cuerpos de Seguridad, y aquéllos.

Información, que es desglosada en diferentes apartados (hechos conocidos, distribución territorial, perfil de víctimas, detenciones efectuadas, incidentes por comunidad de referencia, por sector estratégico, etc.), que permite mostrar la realidad de la cibercriminalidad en nuestro país

Hay que tener 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, a los que se le ha añadido por el volumen y la importancia de la cifra registrada, las siguientes infracciones penales:

- Delitos contra el honor.
- Amenazas y coacciones.

La respuesta a la Cibercriminalidad, como ha quedado referenciado anteriormente, tiene que venir de la mano de una acción conjunta y bien planificada. En España, actualmente los actores involucrados en dar respuesta a todas las problemáticas que se puedan presentar, son principalmente los siguientes:

- El ***Consejo Nacional de Ciberseguridad***, es un órgano de apoyo del Consejo de Seguridad Nacional de los previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que corresponde ejercer las funciones asignadas por aquel en el ámbito de la ciberseguridad y en el marco del Sistema de Seguridad Nacional. Se encuentra regulado por la Orden PRA/33/2018, de 22 de enero. La composición del este Consejo reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad. En el Consejo podrán participar otros actores relevantes del sector privado y especialistas

cuya contribución se considere necesaria. Dicha composición se detalla en la siguiente infografía:

Infografía nº 1- Composición del Consejo Nacional de Ciberseguridad[1]

- El ***CCN-CERT*** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del ***Centro Criptológico Nacional, CCN***, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes o centros de operaciones de ciberseguridad existentes.

[1] https://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad#collapseTwo

- El ***INCIBE-CERT*** es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el ***Instituto Nacional de Ciberseguridad (INCIBE)***[2], dependiente del Ministerio de Economía y Empresa. En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y CNPIC, Centro Nacional de Protección de Infraestructuras y Ciberseguridad del Ministerio del Interior.

- El ***Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)*** es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio. El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

- El ***Departamento de Seguridad Nacional (DSN)*** del Gabinete de la Presidencia del Gobierno es el órgano de asesoramiento al Presidente del Gobierno en materia de Seguridad Nacional. Mantendrá y asegurará el adecuado funcionamiento del Centro de Situación del Departamento de Seguridad Nacional para el ejercicio de las funciones de seguimiento y gestión de crisis, así como las comunicaciones especiales de la Presidencia del Gobierno. El Departamento de Seguridad Nacional fue creado por el Real Decreto 1119/2012 de 20 de julio, de modificación del Real Decreto

[2] El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos. Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional

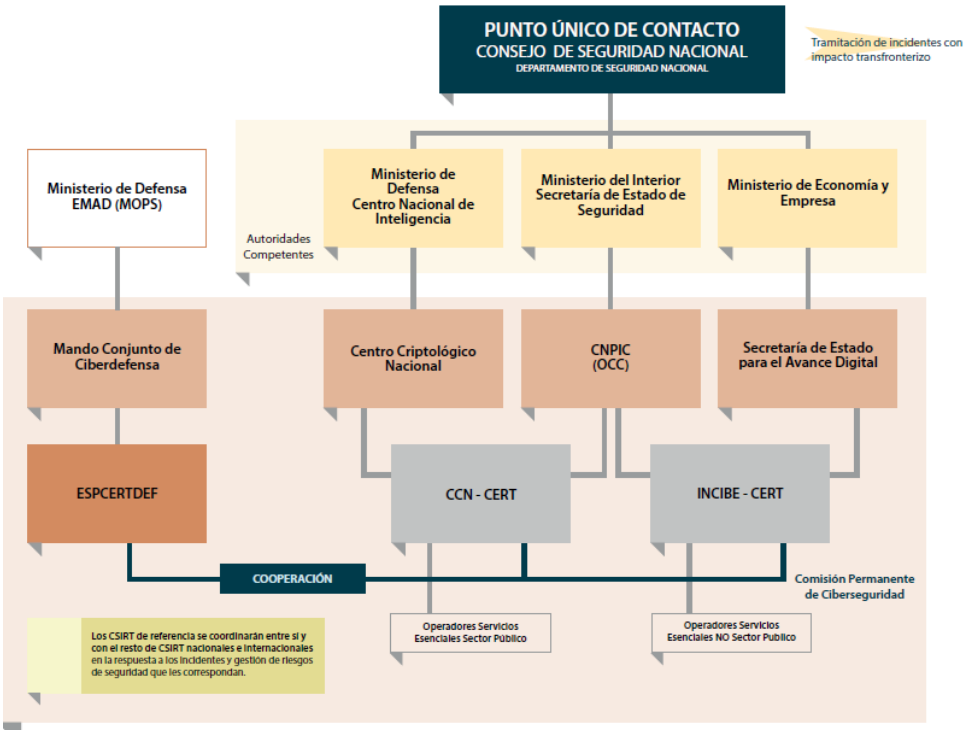
83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno.

- El ***Mando Conjunto de Ciberdefensa (MCCD***) es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. El 19 de febrero de 2013, el Ministro de Defensa promulgó la "Orden Ministerial 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa".

- El ***Grupo de Delitos Telemáticos (GDT)*** fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet. El esfuerzo principal del GDT y de los Equipos de Investigación Tecnológica (EDITE,s) ha sido, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia.

- La ***Unidad de Investigación Tecnológica (UIT)***: asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía.

Esquemáticamente las funciones de los organismos aludidos anteriormente, se pueden mostrar en la siguiente infografía:



Infografía nº 2- Organismos encargados de la Ciberseguridad[3]

Durante 2018 y dentro del aspecto normativo ha tenido importancia la transposición de la Directiva UE 2016/1148[4] relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta directiva posteriormente ha sido incorporada a la normativa española mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información[5]. Según se expone en la web del Departamento de Seguridad Nacional, este Real Decreto-ley aprobado determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten, así como a los que se aplicará. Además recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información en España haciendo énfasis en la cooperación entre autoridades públicas. También se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, se tipifican una serie de infracciones y sanciones, y se establecen las obligaciones de

[3] https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/16-decalogo-ciberseguridad-2018/file

[4] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

[5] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

seguridad de los operadores. Finalmente se regula la notificación de incidentes, con especial atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión.

Otro aspecto legislativo a destacar durante el año 2018, viene relacionado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[6]. Esta nueva ley señala en su preámbulo que:

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

Dentro de esos nuevos derechos digitales que se contemplan en el título X de la LO 3/2018, se encuentran los siguientes:

- Derecho a la neutralidad de Internet.
- Derecho de acceso universal a Internet.
- Derecho a la seguridad digital.
- Derecho a la educación digital.
- Protección de los menores en Internet.
- Derecho de rectificación en Internet.
- Derecho a la actualización de informaciones en medios de comunicación digitales.
- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Derecho a la desconexión digital en el ámbito laboral.
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
- Derechos digitales en la negociación colectiva.
- Protección de datos de los menores en Internet.

[6] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

- Derecho al olvido en búsquedas de Internet.
- Derecho al olvido en servicios de redes sociales y servicios equivalentes.
- Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.
- Derecho al testamento digital.

Por otro lado, cabe resaltar la sofisticación con la que actúan los cibercriminales como se aprecia en la operación por la que se detuvo en España al cerebro de Carbanak[7], una de las mayores bandas de ciberdelincuentes de la historia. Tanto el modus operandi empleado, como la posterior ocultación del dinero obtenido, convirtiéndolo en criptomonedas, hablan a las claras de la dificultad con la que se encuentran los investigadores, a la hora de perseguir estos tipos de delitos. La forma de actuar de los delincuentes era pues la siguiente:

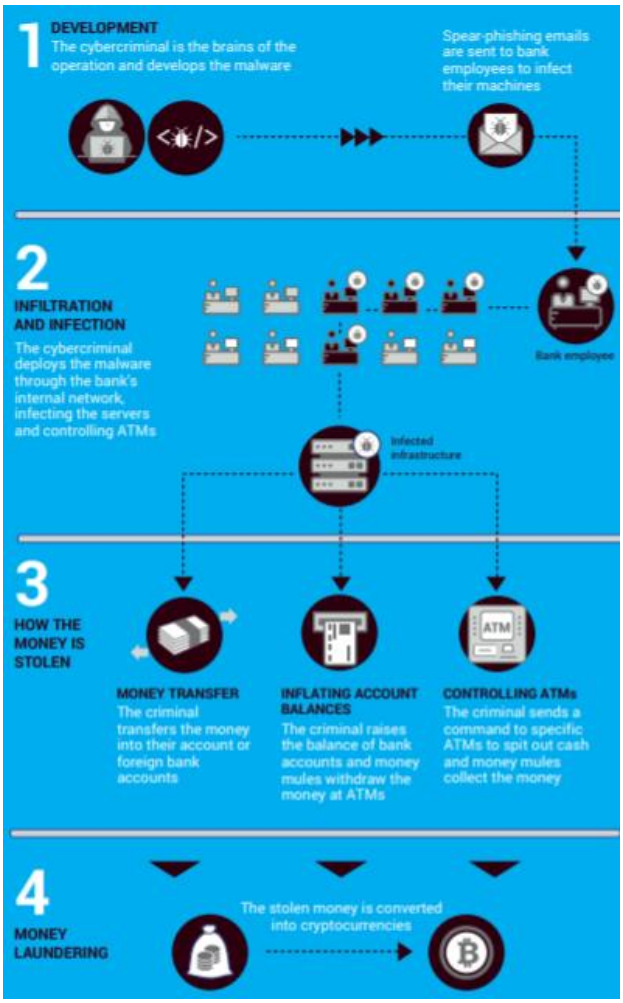
El modus operandi utilizado desde el inicio de sus actividades criminales era similar. El ataque comenzaba con el envío masivo de correos electrónicos fraudulentos suplantando la identidad de organismos o empresas legítimas y dirigidas a una multitud de direcciones de correo electrónico de empleados de entidades bancarias de todo el mundo. Estos correos adjuntaban un fichero, generalmente en formato .RTF o .DOC, que contenían un código malicioso que hacía posible explotar alguna vulnerabilidad no actualizada en los sistemas informáticos de las víctimas.

Una vez el empleado recibía el correo electrónico y abría el fichero adjunto, y en aquellos casos en los que la vulnerabilidad no se encontraba debidamente actualizada en el ordenador del empleado, se ejecutaba en su ordenador un código malicioso. Este iniciaba la descarga de un paquete del software que permitía, posteriormente, el control remoto del mismo desde servidores de comando y control.

Desde el ordenador infectado del empleado intentaban escalar privilegios dentro del sistema comprometido y se movían lateralmente a otros dispositivos de la red interna bancaria, hasta que tomaban el control de sistemas críticos del banco (sistema de transacciones o infraestructura de cajeros automáticos). Una vez los cibercriminales conseguían el control, manejaban a su antojo los cajeros automáticos ordenándoles remotamente que expidieran dinero, ejecutaban modificaciones de saldo en cuentas

[7] http://www.interior.gob.es/prensa/noticias/asset_publisher/GHU8Ap6ztgsg/content/id/8539872

concretas para realizar posteriormente extracciones con tarjetas asociadas, o desviaban transferencias de grandes cantidades de dinero a cuentas de la organización.



Infografía nº 3- Esquema de Carbanak/Cobalt[8]

Toda esta nueva forma de proceder por parte de los criminales, conlleva a que las Fuerzas y Cuerpos de Seguridad, tengan que estar constantemente alerta para intentar atajar estos fenómenos. Para ello, es necesario la conjunción tanto de una alta preparación como la dotación de herramientas legales y materiales, para llevar a cabo la detección de estas tipos de conductas. Dentro de las nuevas formas de responder a la criminalidad, podemos situar la figura del agente encubierto informático, figura legal que fue aprobada tras la reforma de la Ley de Enjuiciamiento Criminal en el año 2015 (art. 282 bis apartado 6 LEC).

[8] https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

En una de las operaciones realizadas el año pasado, utilizando la figura del agente encubierto informático, se llegaron a detener 19 personas por un presunto delito de tenencia y/o distribución de pornografía infantil. Las investigaciones comenzaron tras conocerse que en determinados grupos cerrados o secretos de una conocida red social, se intercambiaban enlaces en los que, tras clicar en ellos, se accedía directamente a grupos de mensajería instantánea, que compartían abundantes archivos de pornografía infantil.[9] Mediante este método, por el que los agentes se hicieron pasar por un usuario más, se comprobó la existencia de estos grupos y analizó varios de ellos en los que se distribuía abundante pornografía infantil. En estos grupos había varios números de teléfono repartidos tanto por todo el territorio nacional, como por el extranjero. Una vez analizados todos los números de teléfono de los usuarios de los diferentes grupos de mensajería, se procedió a explotar la operación, con la realización de 20 registros domiciliarios en 14 localidades y se detuvo a 19 personas, como presuntos autores de un delito de tenencia y/o distribución de pornografía infantil.

No cabe duda, que las administraciones públicas deben estar alertas y en continua vanguardia en lo que se refiere a la protección del ciberespacio. Para ello, se constituye en una herramienta esencial la información que se aporta a la ciudadanía. Dentro de estas iniciativas podemos señalar la "Guía Nacional de notificación y gestión de ciberincidentes[10]", que fue aprobada por el Consejo Nacional de Ciberseguridad el día 09 de enero de 2019, dentro de esta guía se proporciona a los Responsables de Seguridad de la Información (RSI) las directrices para el cumplimiento de las obligaciones de reporte de incidentes de ciberseguridad acaecidos en el seno de las Administraciones Públicas, las infraestructuras críticas y operadores estratégicos de su competencia, así como el resto de entidades comprendidas en el ámbito de aplicación del Real Decreto-Ley 12/2018.

Otro capítulo donde cabe incidir directamente es en el uso de las redes sociales. Este entorno, es un punto donde muchos cibercriminales encuentran "un caladero de

[9] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/8244008

[10] http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf/19676087-0253-4c58-bbb0-2fc58a5fd63b

información personal" para cometer sus ilícitos penales. Recientemente, el Centro Criptológico Nacional, publicó un manual de "Buenas prácticas en redes sociales"[11]

Por otro lado, cabe reseñar que los cibercriminales se van adaptando con mayor rapidez a ciertos entornos, como pueden ser el mayor uso por parte de los usuarios de los dispositivos móviles. En este sentido, en el Informe Anual 2018 de "Dispositivos y comunicaciones móviles[12]", del Centro Criptológico Nacional, se analizan diversos riesgos de seguridad asociados a los mismos como son: la adopción de las últimas versiones de los sistemas operativos, el mecanismo de autentificación biométrica, el desbloqueo y extracción forense datos, los mecanismos de seguridad avanzada y código dañino, y la privacidad en plataformas móviles. En general, se aprecia un aumento global del malware móvil, extremo que se ve confirmado por otros informes internacionales.

Respecto a la protección de los menores ante las nuevas tecnologías, es una preocupación constante de los progenitores, debido a los inciertos peligros a los que se enfrentan. Cada vez más, los menores acceden en mayor volumen a las nuevas tecnologías y lo hacen a una edad más temprana. Es por ello, que iniciativas como la "Guía para un uso seguro y responsable de internet por los menores_itinerario de mediación parental[13]", se convierten en una magnífica herramienta de ayuda.

Otro hecho importante es la puesta en marcha por parte de la Unión Europea del Código de conducta contra el odio en las redes. La cuarta evaluación del Código de conducta de la UE indica que esta iniciativa de la Comisión arroja resultados positivos. Las empresas informáticas evalúan ahora el 89 % de los contenidos señalados en un plazo de 24 horas y retiran el 72 % de los contenidos que se consideran constitutivos de incitación ilegal al odio, en comparación con el 40 % y el 28 %, respectivamente, cuando el Código se puso en marcha en 2016[14].

[11] https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes-sociales/file.html

[12] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

[13] https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_internet.pdf

[14] http://europa.eu/rapid/press-release_IP-19-805_es.pdf

Por último, cabe señalar que en el Anexo I, se adjunta el Módulo de consulta de cibercriminalidad con las principales tipologías penales cometidas con las nuevas tecnologías, que son computadas en el Sistema Estadístico de Criminalidad (SEC).

2.-RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

En este *VI Informe sobre Cibercriminalidad*, en el que se publican los datos estadísticos de cibercriminalidad y las amenazas que han sido descubiertas a lo largo del año 2018 en nuestro país, también se hace referencia a una serie de datos relativos al uso de las TIC por parte de la sociedad española en general. Para ello, se toman como referencia estudios y encuestas de opinión realizadas por otros organismos públicos, tanto de ámbito nacional (INE, ONTSI) como europeos (EUROSTAT).

La Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2018), 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.

Este estudio se realiza con periodicidad anual desde 2002, sin embargo en los años 2005 y 2006 se obtuvieron además datos para el 2º semestre.

A lo largo del capítulo 2 de esta 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 2018 con respecto al año 2017. Siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2009-2018).

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 2009.

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 98,5 % 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 49,1% 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 2017, siendo el incremento más acusado en la edad de 65 a 74 años.

Por sexo, es mayor el uso de ordenador por parte de los hombres frente a las mujeres. No obstante, tan sólo le separan un punto porcentual.

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, con el 91,3%y 92,8, respectivamente. Por sexos, es muy pequeña la diferencia. En 2018, el 90,4% de los niños afirmaron haber utilizado un ordenador en los últimos tres meses, frente al 92,2% de las niñas, siendo el 92,5% cuando se hace referencia al acceso a Internet en relación al 93,2% de las niñas. Hay que significar, que si bien en el conjunto de la población española, existe una ligera diferencia a favor de los hombres en el uso del ordenador y acceso a internet,

en el caso de los menores se invierte esa polaridad, pasando las mujeres a tener más altos porcentajes.

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 2009 el comercio electrónico se ha triplicado, puesto que el 43,5 % de las personas encuestadas en 2018 reconocen haber realizado alguna compra empleando esta vía, mientras que en el año 2009 solo lo hacían el 15,2%. Por sexo, los hombres aventajan a las mujeres en cifras porcentuales (44,6% frente al 42,3%).

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 (60,9%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 12’0% 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 la cifra de viviendas con acceso a Internet en los diferentes países de la Unión Europea (28-UE) (Punto 2.5. Comparativa internacional), en la serie histórica 2009-2018. España se encuentra está por debajo de la media de la UE-28, con un 86% frente al 89% de la Unión Europea.

En el apartado 2.6, se incluyen datos extraídos del Índice de Economía y Sociedad Digital (DESI por sus siglas en inglés). Se trata de un índice compuesto desarrollado por la Comisión Europea (DG CNECT) 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.

En el DESI 2018 España forma parte del grupo de países que avanza a un ritmo más rápido que la UE, ya que el rendimiento de nuestro país en el uso de tecnologías digitales por parte de las empresas y en la prestación de servicios públicos en línea son dos importantes signos de evolución en este ámbito. Hay que reseñar que España ha avanzado dos puestos en ese índice, pasando de ocupar el puesto doce (12) en el año 2017, al décimo (10) en el año 2018.

A nivel nacional, desde el Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI), del Ministerio de Energía, Turismo y Agenda Digital se publica de manera periódica un informe que recoge los principales indicadores de la Sociedad de la Información en España (2.7). Éste señala que, en 2018, el 75,11% de las empresas españolas usan firma electrónica para relacionarse con las Administraciones Públicas. Asimismo, la evolución del Indicador de economía y sociedad digital, muestra una tendencia creciente de España, llegando a superar en el año 2018 nuestro país la media de la Unión Europea. Respecto, a las empresas que venden por Internet al menos el 1% del total de ventas, es de destacar, que España en el año 2017 estaba un punto porcentual por encima de media de la Unión Europea. Esta misma tendencia, se repite en el porcentaje de población que realiza compras online transfronterizas, así como en los particulares que han utilizado internet para tratar con las administraciones públicas.

3.-INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

En la introducción al capítulo se detallan los aspectos más relevantes en esta materia.

4.-DATOS ESTADÍSTICOS 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 Gabinete de Coordinación y Estudios asumió las funciones en materia de estadística de criminalidad, que continuaron tras la publicación del Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

Fue el 31 de enero de 2013, cuando se dictó la Instrucción 1/2013 de la Secretaría de Estado de Seguridad, sobre la Estadística Nacional de Criminalidad, cuyo objeto es "*dictar las directrices básicas para el desarrollo y gestión de la Estadística Nacional de Criminalidad, determinando los elementos que la componen – especialmente el Sistema Estadístico de Criminalidad –, definiendo los actores que interactúan en la misma y fijando las responsabilidades de cada uno de ellos*".

Así pues, y según reza 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 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 (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 2015-2018 (excluidos datos de Ertzaintza y Mossos d'Esquadra), 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 2015 a 2018, como hecho irrefutable extraído de los resultados registrados por las Fuerzas y Cuerpos de Seguridad se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2018, se ha conocido un total de 110.613 hechos, lo que supone un 36,0% más con respecto al año anterior. De esta cantidad, el 80,2 % corresponde a fraudes informáticos (estafas) y el 10,8% a amenazas y coacciones.

Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Pero otro hecho, innegable es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad. Como

se puede observar en la tabla nº 1, hemos pasado del año 2011, donde nos situábamos en el 2,1% al año 2018 con el 7,0%.

2011	2,1%
2012	2,5%
2013	2,6%
2014	3,1%
2015	3,9%
2016	4,3%
2017	5,3%
2018	7,0%

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/investigadoslos gráficos del apartado) evidencian de manera esquemática los datos correspondientes a los hechos conocidos, esclarecidos y la cifra de las detenciones e investigaciones resgistradas por las Fuerzas y Cuerpos de Seguridad, en el periodo 2015 a 2018.

En relación al porcentaje de hechos esclarecidos, en el año 2018, éste supone el 22,4% del total de los hechos conocidos. Por otra parte, los detenidos e investigados han alcanzado la cifra de 5.697.

La distribución de la ciberdelincuencia, desde el punto de vista geográfico (4.3. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2018, sitúa a 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, Valencia, Illes Balears, A Coruña, Alicante, y Sevilla. Hay que significar, que los datos de Cataluña y País Vasco, están infrarrepresentados, al no disponer información facilitada por Mossos d'Esquadra y Ertzaintza.

Los datos de la sección 4.4, 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 2018, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de 84.607[15], es decir, un 35,5% más que en el año 2017. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (52,2%), tienen entre 26 a 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y acceso e interceptación ilícita. 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, contra el honor, los delitos sexuales y falsificación informática.

Además, en el punto 4.5 (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 2018, el 35,1 % 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 4.6). 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 4.7), el 90,3% de ellas son españolas, y el 9,7% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Rumanía, Italia y Marruecos las que aúnan valores más elevados.

Al igual que en el informe pasado, en este *VI 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 4.8. 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.

[15] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (110.613) y el de victimizaciones registradas (84.607), 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.

Del análisis de la información extraída del SEC, se puede observar que el comportamiento de las víctimas incluidas en el grupo menores de edad, no sigue el patrón o el modelo de las víctimas mayores de edad. Las víctimas menores de edad son más vulnerables a otro tipo de hechos delictivos, en concreto a las amenazas y coacciones, tal y como refleja la tabla del apartado 4.8.

Igualmente, en este estudio, se consignan datos relativos a la edad de la víctima (Punto 4.9.Edad de la víctima). Por lo que, en el año 2018, de las 84.607 victimizaciones registradas, 29.690 se encuadran dentro del rango de edad que comprende los 26 a 40 años, y 20.907 entre los 41 y 50 años. Los menores de edad suman un total de 2.319.

La sección 4.10 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, de 2018.

De la cifra total de detenciones e investigaciones (5.697) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 77,2% 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 (4.11. Detenciones/investigaciones según grupo de edad y sexo.), se observa que la mayor cifra de los responsables de ciberdelincuencia se ubican en el grupo de edad 26 a 40 años.

Por lo que respecta a las diferentes infracciones penales (4.12. Detenciones/investigaciones por tipología penal y sexo), los datos establecen que las causas por las que las personas de sexo masculino han sido objeto de la detención/investigación ha sido principalmente por estafas, amenazas, y la pornografía de menores. Asimismo, se puede observar que las estafas, amenazas e usurpación de estado civil predominan entre las razones para actuar contra los responsables de sexo femenino.

La mayoría de los detenidos/investigados por ciberdelincuencia son de nacionalidad española (83,6%) (4.13). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Rumanía, Marruecos, Nigeria y Colombia, 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, con excepción del grupo de edad de 41 a 50 en los delitos contra la propiedad industrial e intelectual (4.14).

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN >>

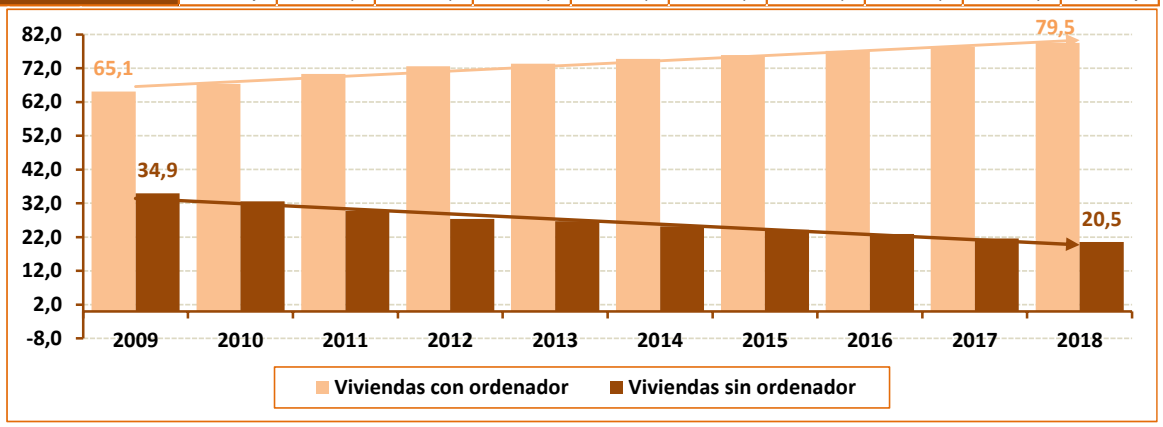
ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

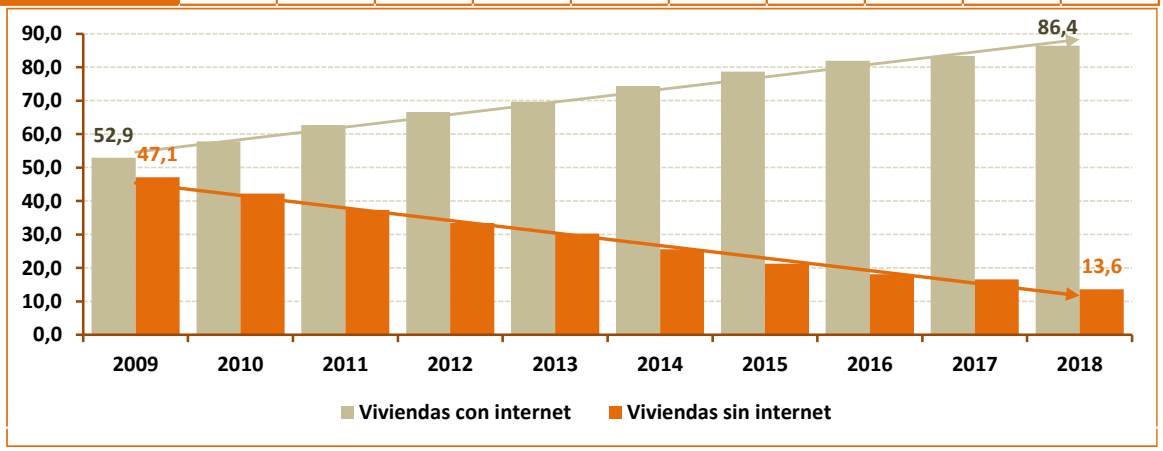
(Fuente de datos: INE)

>> 2.1. Hogares

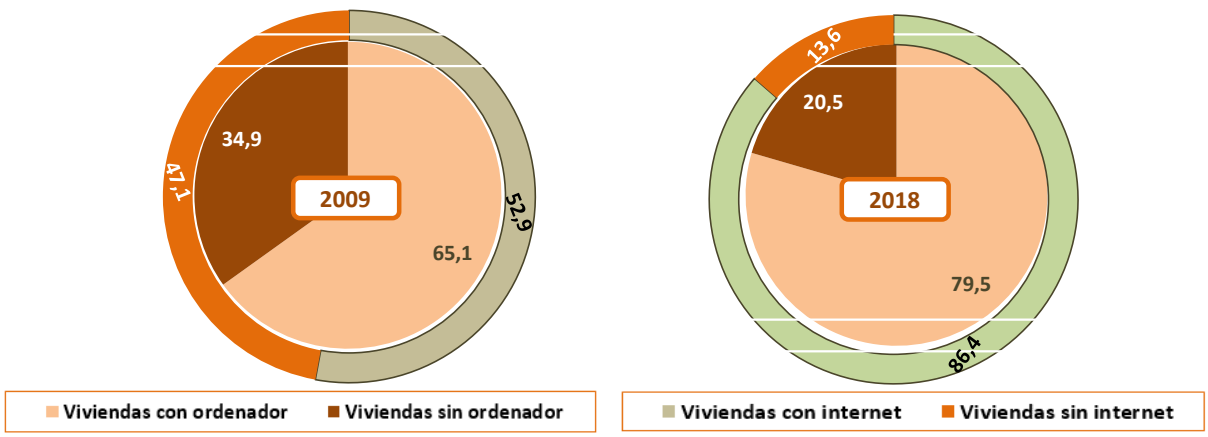
	PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Viviendas con ordenador	**65,1**	67,4	70,3	72,6	73,3	74,8	75,9	77,1	78,4	**79,5**
Viviendas sin ordenador	**34,9**	32,6	29,7	27,4	26,7	25,2	24,1	22,9	21,6	**20,5**



	PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Viviendas con internet	**52,9**	57,8	62,7	66,6	69,7	74,4	78,7	81,9	83,4	**86,4**
Viviendas sin internet	**47,1**	42,2	37,3	33,4	30,3	25,6	21,3	18,1	16,6	**13,6**



CONTRASTE EVOLUTIVO DE LAS VIVIENDAS 2009 - 2018



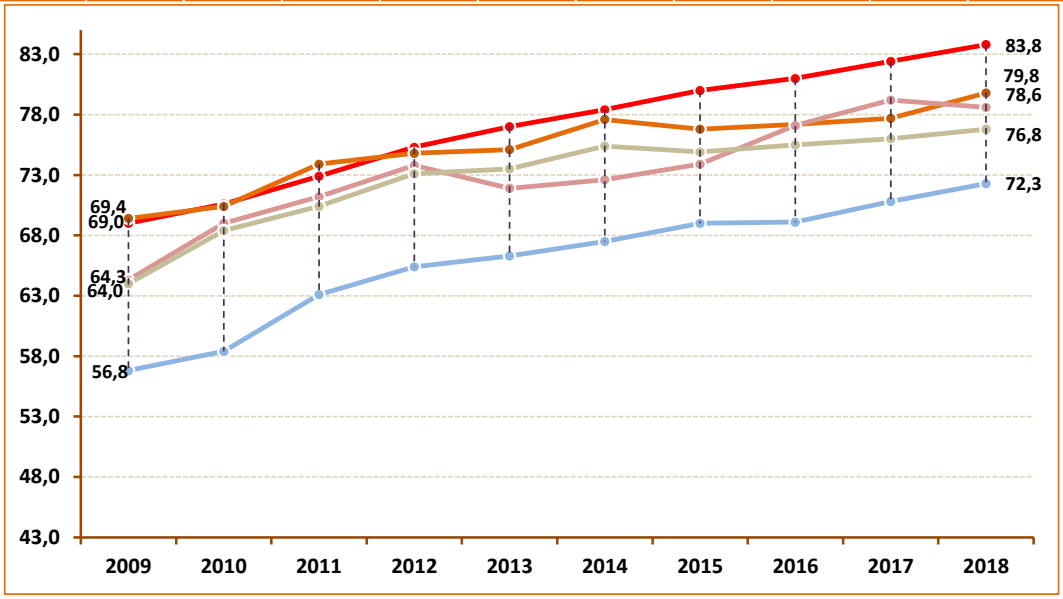
ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

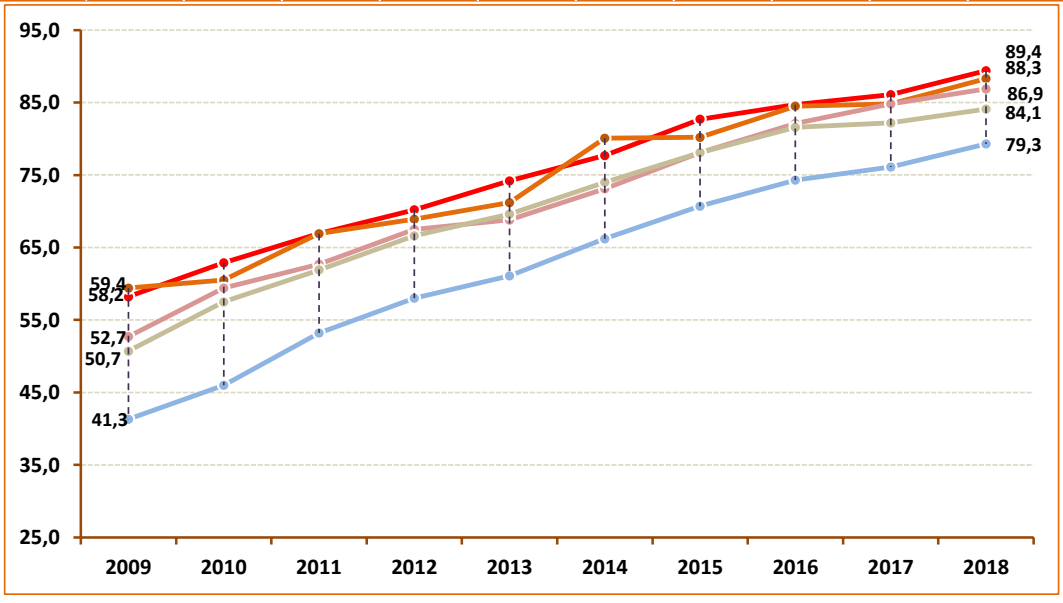
(Fuente de datos: INE)

>> 2.1. Hogares. Por tipo de hábitat

	PORCENTAJE DE VIVIENDAS CON ORDENADOR									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Más de 100.000 hab.	**69,0**	70,6	72,9	75,3	77,0	78,4	80,0	81,0	82,4	**83,8**
De 50.000 a 100.000 hab.	**69,4**	70,4	73,9	74,8	75,1	77,6	76,8	77,2	77,7	**79,8**
De 20.000 a 50.000 hab.	**64,3**	69,0	71,2	73,8	71,9	72,6	73,9	77,1	79,2	**78,6**
De 10.000 a 20.000 hab.	**64,0**	68,4	70,4	73,1	73,5	75,4	74,9	75,5	76,0	**76,8**
Menos de 10.000 hab.	**56,8**	58,4	63,1	65,4	66,3	67,5	69,0	69,1	70,8	**72,3**



	PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Más de 100.000 hab.	**58,2**	62,9	66,9	70,2	74,2	77,7	82,7	84,7	86,1	**89,4**
De 50.000 a 100.000 hab.	**59,4**	60,5	66,9	68,9	71,2	80,1	80,2	84,5	84,8	**88,3**
De 20.000 a 50.000 hab.	**52,7**	59,4	62,7	67,5	68,8	73,1	78,1	82,1	84,8	**86,9**
De 10.000 a 20.000 hab.	**50,7**	57,5	61,9	66,6	69,6	74,0	78,1	81,6	82,2	**84,1**
Menos de 10.000 hab.	**41,3**	46,0	53,2	58,0	61,1	66,2	70,7	74,3	76,1	**79,3**

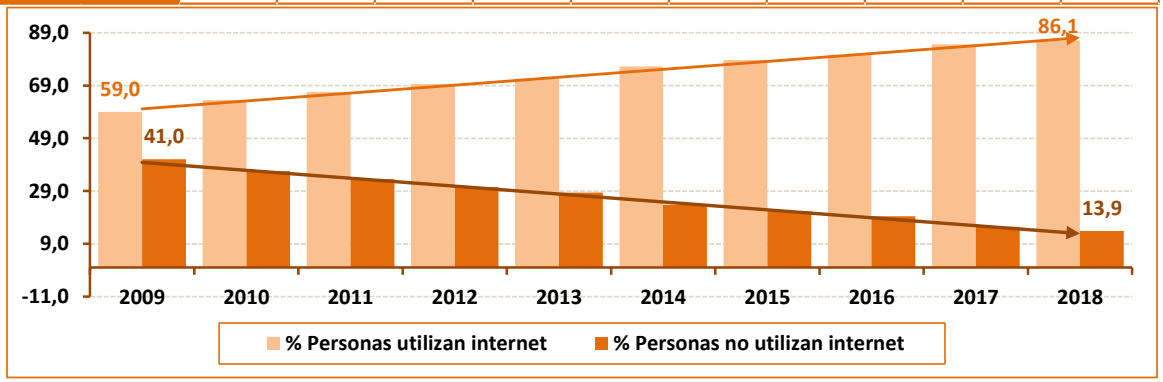


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

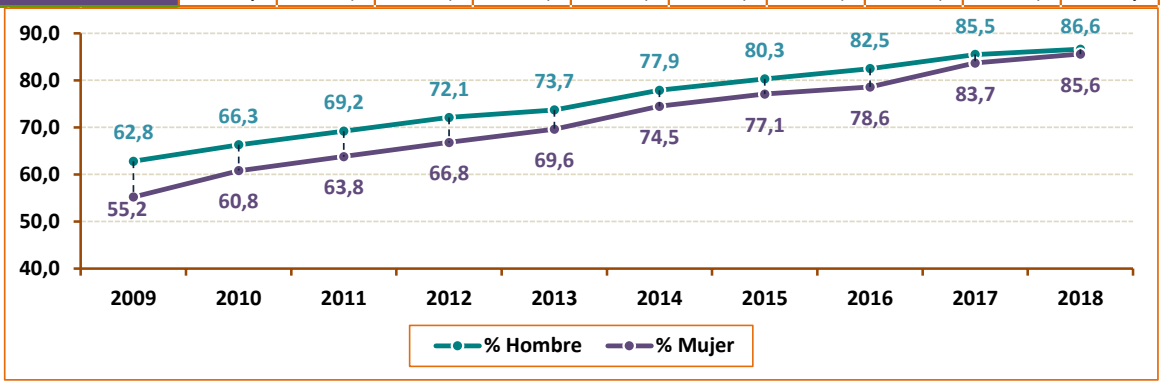
(Fuente de datos: INE)

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

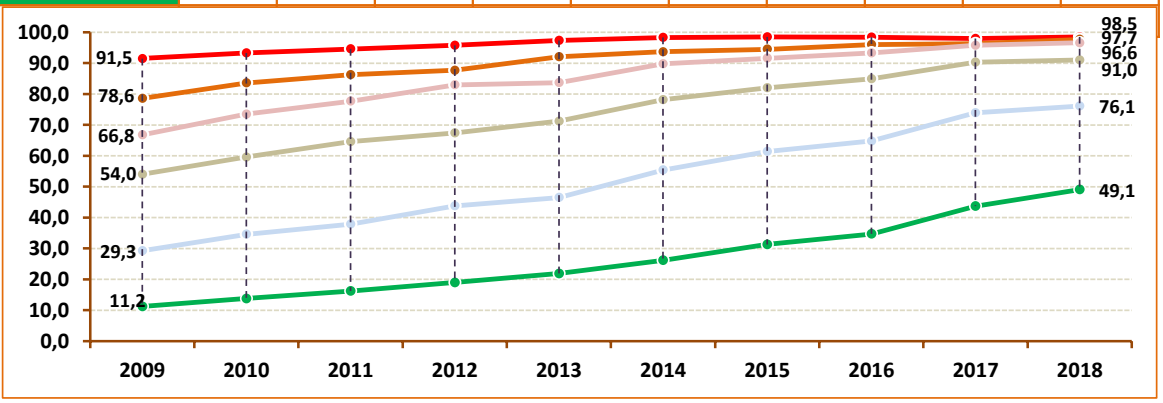
% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Utilizado internet	**59,0**	63,5	66,5	69,5	71,6	76,2	78,7	80,6	84,6	**86,1**
No utilizado internet	**41,0**	36,5	33,5	30,5	28,4	23,8	21,3	19,4	15,4	**13,9**



% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hombre	**62,8**	66,3	69,2	72,1	73,7	77,9	80,3	82,5	85,5	**86,6**
Mujer	**55,2**	60,8	63,8	66,8	69,6	74,5	77,1	78,6	83,7	**85,6**



% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Edad: De 16 a 24 años	**91,5**	93,3	94,6	95,8	97,4	98,3	98,5	98,4	98,0	**98,5**
Edad: De 25 a 34 años	**78,6**	83,6	86,3	87,7	92,1	93,7	94,5	96,0	96,3	**97,7**
Edad: De 35 a 44 años	**66,8**	73,5	77,7	83,0	83,7	89,8	91,6	93,3	95,8	**96,6**
Edad: De 45 a 54 años	**54,0**	59,6	64,6	67,4	71,2	78,2	82,0	84,9	90,3	**91,0**
Edad: De 55 a 64 años	**29,3**	34,6	37,9	43,8	46,5	55,4	61,4	64,8	73,9	**76,1**
Edad: De 65 a 74 años	**11,2**	13,8	16,2	19,0	21,9	26,2	31,3	34,7	43,7	**49,1**

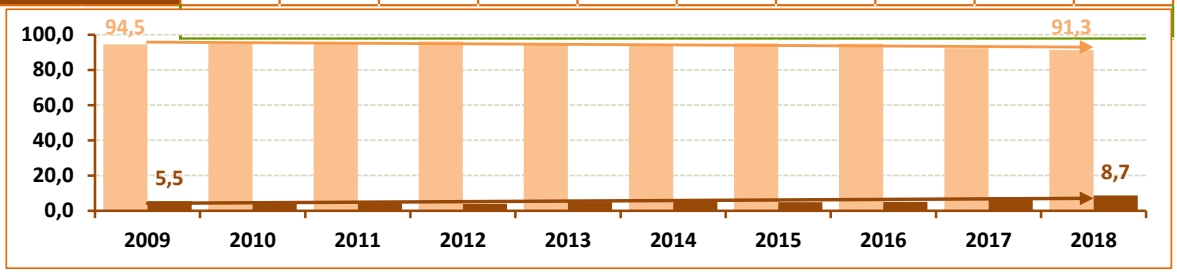


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

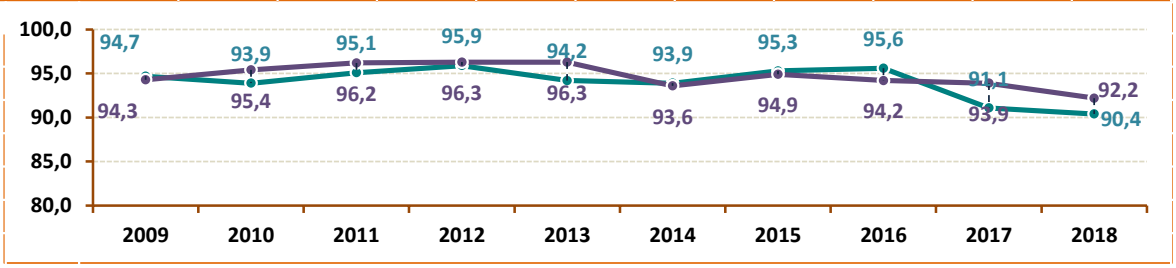
(Fuente de datos: INE)

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

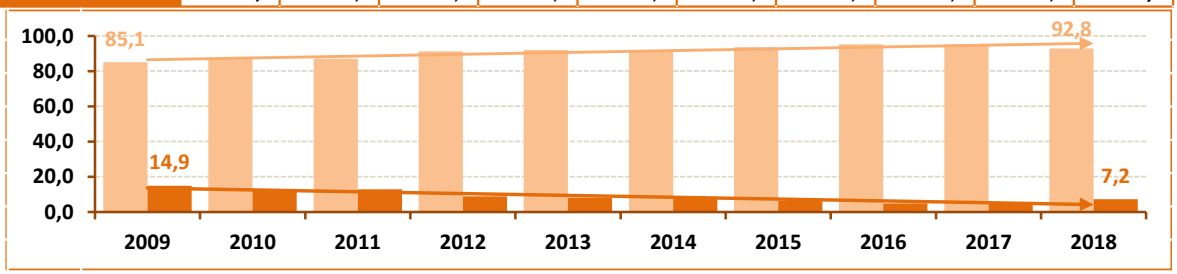
% DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Utilizado ordenador	**94,5**	94,6	95,6	96,1	95,2	93,8	95,1	94,9	92,4	**91,3**
No utilizado ordenador	**5,5**	5,4	4,4	3,9	4,8	6,2	4,9	5,1	7,6	**8,7**



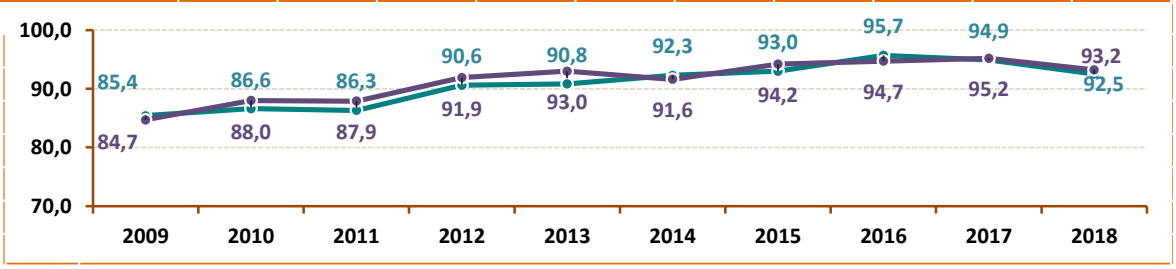
% POR SEXO DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hombre	**94,7**	93,9	95,1	95,9	94,2	93,9	95,3	95,6	91,1	**90,4**
Mujer	**94,3**	95,4	96,2	96,3	96,3	93,6	94,9	94,2	93,9	**92,2**



% DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Utilizado internet	**85,1**	87,3	87,1	91,2	91,9	92,0	93,6	95,2	95,1	**92,8**
No utilizado internet	**14,9**	12,7	12,9	8,8	8,1	8,0	6,4	4,8	4,9	**7,2**



% POR SEXO DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hombre	**85,4**	86,6	86,3	90,6	90,8	92,3	93,0	95,7	94,9	**92,5**
Mujer	**84,7**	88,0	87,9	91,9	93,0	91,6	94,2	94,7	95,2	**93,2**

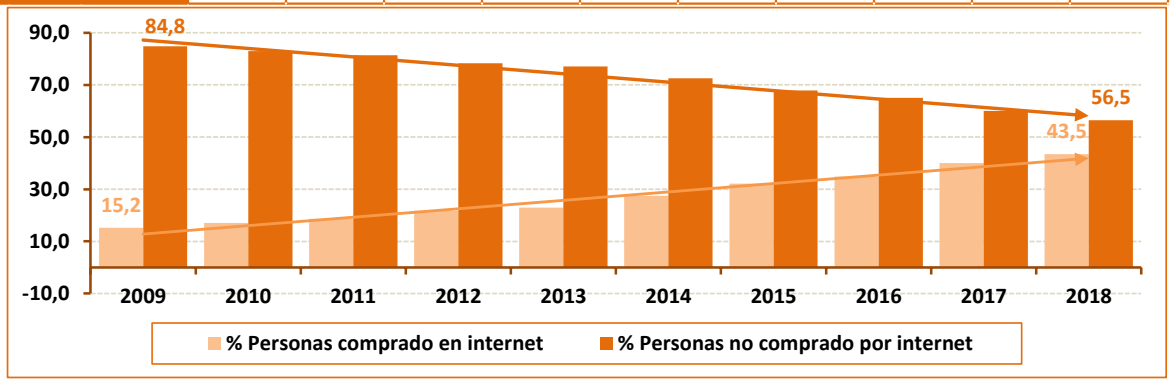


2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

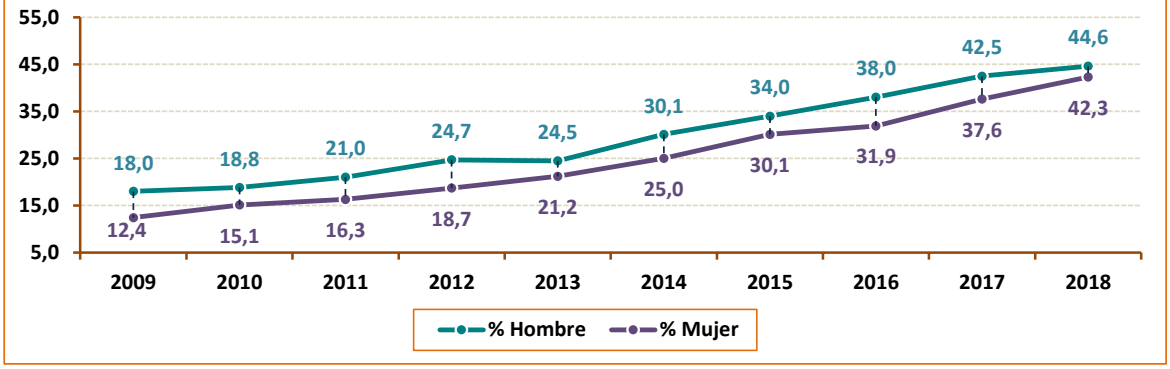
(Fuente de datos: INE)

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

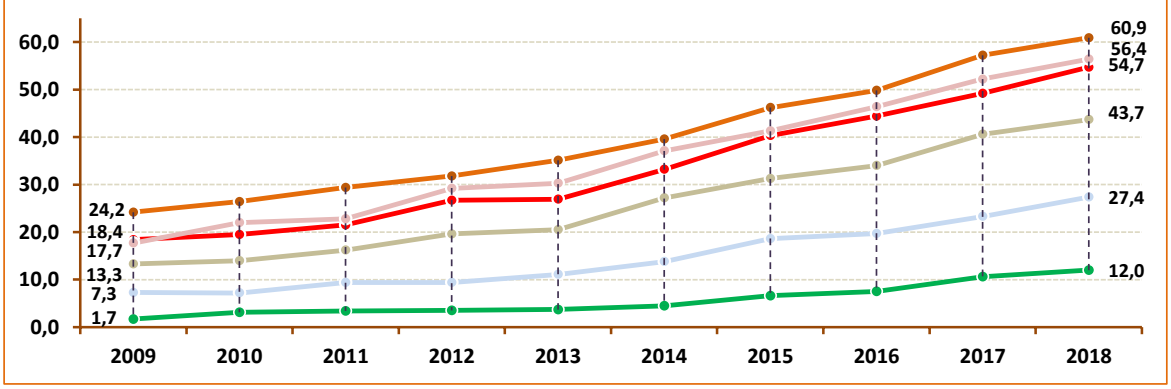
	% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Comprado en internet	**15,2**	17,0	18,6	21,7	22,9	27,5	32,1	34,9	40,0	**43,5**
No comprado en internet	**84,8**	83,0	81,4	78,3	77,1	72,5	67,9	65,1	60,0	**56,5**



	% POR SEXO DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hombre	**18,0**	18,8	21,0	24,7	24,5	30,1	34,0	38,0	42,5	**44,6**
Mujer	**12,4**	15,1	16,3	18,7	21,2	25,0	30,1	31,9	37,6	**42,3**



	% POR GRUPO DE EDAD DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Edad: De 16 a 24 años	**18,4**	19,5	21,5	26,7	26,9	33,2	40,3	44,4	49,2	**54,7**
Edad: De 25 a 34 años	**24,2**	26,4	29,4	31,8	35,1	39,6	46,2	49,8	57,2	**60,9**
Edad: De 35 a 44 años	**17,7**	22,0	22,8	29,2	30,3	37,1	41,3	46,4	52,2	**56,4**
Edad: De 45 a 54 años	**13,3**	14,0	16,2	19,6	20,5	27,2	31,3	34,0	40,6	**43,7**
Edad: De 55 a 64 años	**7,3**	7,2	9,4	9,4	11,1	13,8	18,6	19,7	23,3	**27,4**
Edad: De 65 a 74 años	**1,7**	3,1	3,4	3,5	3,7	4,5	6,6	7,5	10,6	**12,0**



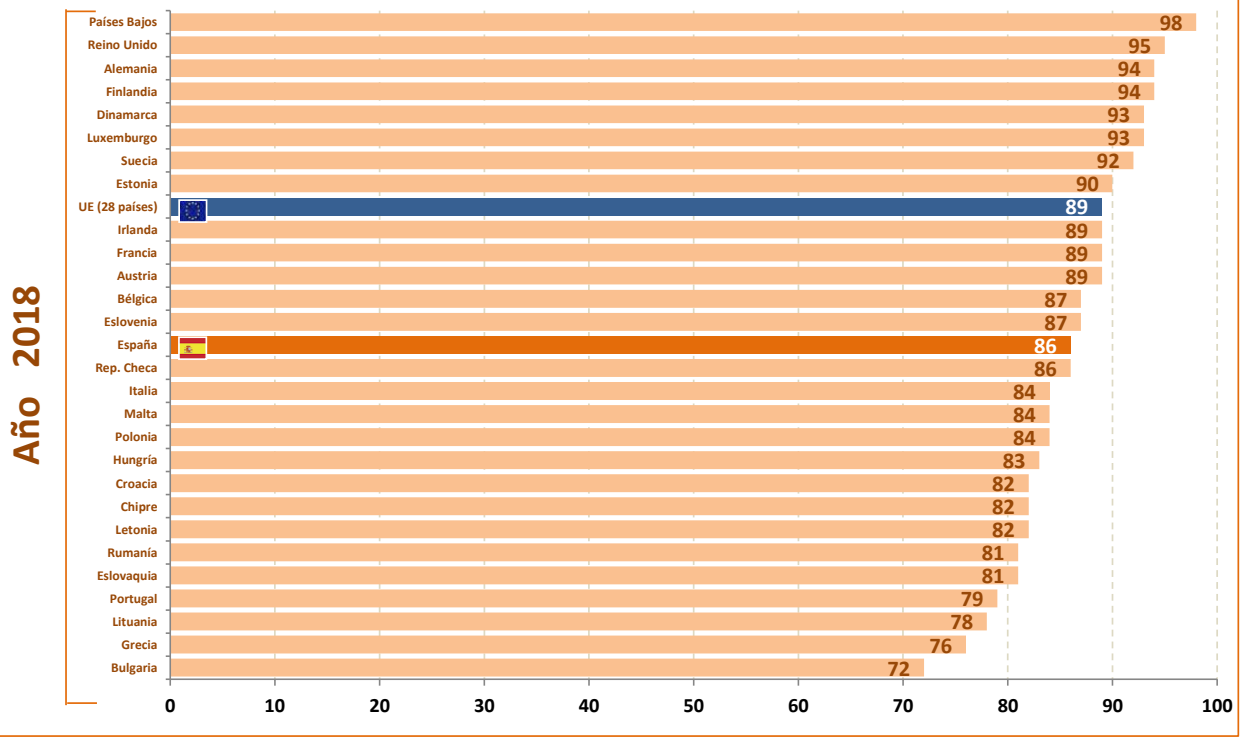
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: EUROSTAT)

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

PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
UE (28 países)	66	70	73	76	79	81	83	85	87	89
Bélgica	67	73	77	78	80	83	82	85	86	87
Bulgaria	30	33	45	51	54	57	59	64	67	72
Rep. Checa	54	61	67	65	73	78	79	82	83	86
Dinamarca	83	86	90	92	93	93	92	94	97	93
Alemania	79	82	83	85	88	89	90	92	93	94
Estonia	62	67	69	74	79	83	88	86	88	90
Irlanda	67	72	78	81	82	82	85	87	88	89
Grecia	38	46	50	54	56	66	68	69	71	76
España	53	58	63	67	70	74	79	82	83	86
Francia	69	74	76	80	82	83	83	86	86	89
Croacia	50	56	61	66	65	68	77	77	76	82
Italia	53	59	62	63	69	73	75	79	81	84
Chipre	53	54	57	62	65	69	71	74	79	82
Letonia	58	60	64	69	72	73	76	77	79	82
Lituania	60	61	60	60	65	66	68	72	75	78
Luxemburgo	87	90	91	93	94	96	97	97	97	93
Hungría	53	58	63	67	70	73	76	79	82	83
Malta	64	70	75	77	79	81	82	82	85	84
Países Bajos	90	91	94	94	95	96	96	97	98	98
Austria	70	73	75	79	81	81	82	85	89	89
Polonia	59	63	67	70	72	75	76	80	82	84
Portugal	48	54	58	61	62	65	70	74	77	79
Rumanía	38	42	47	54	58	61	68	72	76	81
Eslovenia	64	68	73	74	76	77	78	78	82	87
Eslovaquia	62	67	71	75	78	78	79	81	81	81
Finlandia	78	81	84	87	89	90	90	92	94	94
Suecia	86	88	91	92	93	90	91	94	95	92
Reino Unido	77	80	83	87	88	90	91	93	94	95



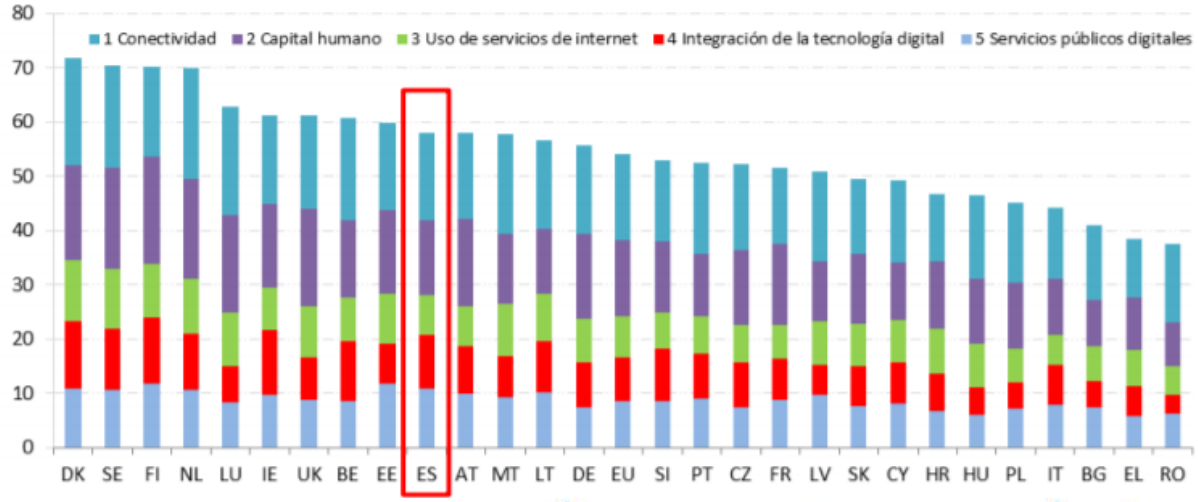
2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

(Fuente de datos: Comisión Europea)

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

	España		Grupo	UE
	puesto	puntuación	puntuación	puntuación
DESI 2018	**10**	**58,0**	**54,7**	**54,0**
DESI 2017	12	53,3	51,5	50,8

Clasificación del Índice de la Economía y la Sociedad Digitales (DESI) de 2018



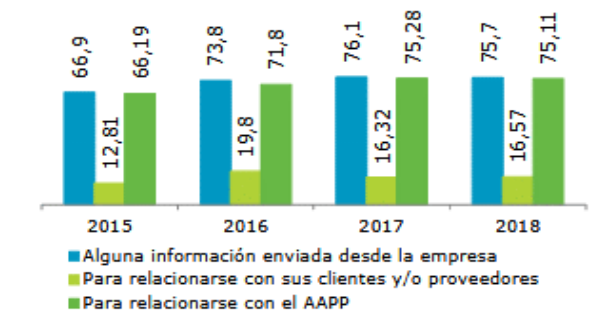
	España				UE
	DESI 2018		DESI 2017		DESI 2018
	valor	puesto	valor	puesto	valor
1.a.1. Cobertura de banda ancha fija % hogares	96 % ↑ 2017	21	95 % 2016	21	97 % 2017
1.a.2. Implantación de la banda ancha fija % hogares	73 % ↑ 2017	15	71 % 2016	15	75 % 2017
1.b.1. Cobertura 4G % hogares (media de operadores)	92 % ↑ 2017	16	86 % 2016	21	91 % 2017
1.b.2. Implantación de la banda ancha móvil Abonos por cada 100 personas	92 ↑ 2017	11	86 2016	10	90 2017
1.c.1. Cobertura de la banda ancha de nueva generación (NGA) % hogares con capacidad VDSL, FTTP o Docsis 3.0	85 % ↑ 2017	14	81 % 2016	15	80 % 2017
1.c.2. Implantación de la banda ancha rápida % de hogares con >= 30Mbps	43 % ↑ 2017	12	35 % 2016	14	33 % 2017
1.d.1. Cobertura de banda ancha ultrarrápida % hogares con capacidad FTTP o Docsis 3.0	84 % 2017	9	NA		58 % 2017
1.d.2. Implantación de la banda ancha ultrarrápida % de hogares con >= 100Mbps	17,6 % ↑ 2017	11	15,4 % 2016	9	15,4 % 2017
1.e.1. Índice de precios de la banda ancha Puntuación (0 a 100)	74 ↑ 2017	22	70 2016	23	87 2017

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

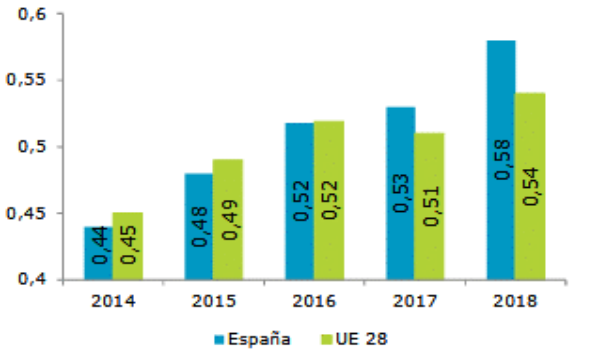
>> 2.7. Indicadores de la sociedad de la información (Publicación: Indicadores destacados de la sociedad de la información)

Empresas que usan firma digital (%)



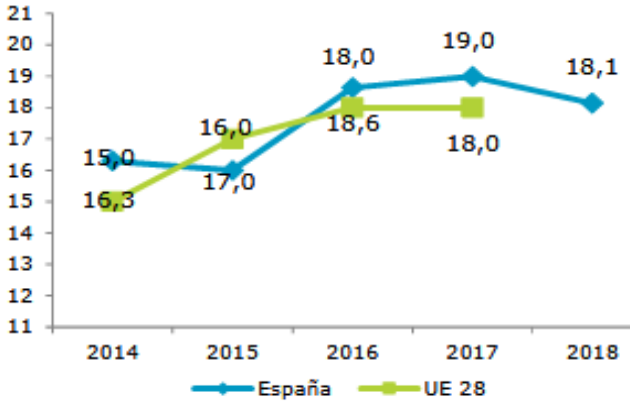
Fuente: INE

Evolución del Indicador de economía y sociedad digital (valoración de 0 a 1)



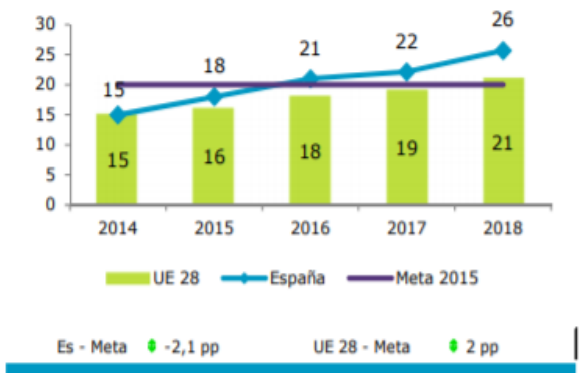
Fuente: CE

Empresas que venden por Internet (al menos 1% del total de ventas) (%)



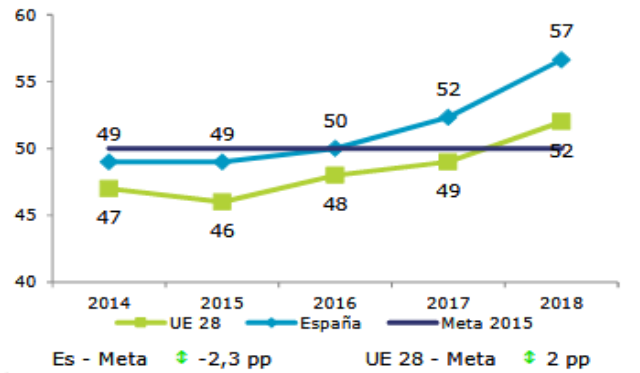
Fuente: INE y Eurostat

Población que realiza compras online transfronterizas (%)



Fuente: INE y Eurostat

Particulares que han utilizado Internet para tratar con la AAPP (%)



Fuente: INE y Eurostat

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD >>

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

La OCC es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del Secretario de Estado de Seguridad 15/2014, de 19 de noviembre. Sus funciones están reguladas por el Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC (Centro Nacional de Protección de Infraestructuras y Ciberseguridad).

La OCC ejerce como canal específico de comunicación entre los Equipos de Respuesta a Incidentes (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 agosto, relativa a los ataques contra los sistemas de información.

El INCIBE-CERT es el CSIRT nacional de referencia competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas de titularidad privada.

Operado técnicamente por el instituto Nacional de Ciberseguridad de España (INCIBE) y el CNPIC para el ámbito competencial de Protección de Infraestructuras Críticas (PIC), el INCIBE-CERT se constituyó en 2012 a través de un Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la *Secretaría de Estado de Seguridad* (SES) y la *Secretaría de Estado para la Sociedad de la Información y Agenda Digital*.

Los operadores de infraestructuras críticas de titularidad privada, designados en virtud de la aplicación de la *Ley 8/2011 de 28 de abril* por la que se establecen medidas para la protección de las infraestructuras críticas, tienen en el INCIBE-CERT su punto de referencia para la notificación y respuesta ante incidentes de ciberseguridad acaecidos en las infraestructuras de información y comunicación que puedan tener afectación a la prestación de servicios esenciales.

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

El INCIBE-CERT gestionó un total de 111.519 incidentes de ciberseguridad en España durante el año 2018, lo que supone una disminución del 9,38% respecto al número de incidentes de ciberseguridad tratados en el año 2017.

Analizando el número de incidentes por la tipología asignada, puede observarse en los datos aportados que *Fraude* se ha convertido en el año 2018 en el tipo más frecuente de incidente registrado con un porcentaje del 50,15%, seguido de *Malware* con un 24,23% respecto del total de incidentes registrados. En la serie puede observarse que se ha introducido un cambio de taxonomía o clasificación para conseguir a adaptarse a la Guía Nacional de Notificación y Gestión de Ciberincidentes, lo que conlleva que categorías como *SPAM* tengan asignado un valor nulo al haber desaparecido, y que aparezcan nuevas categorías como son *Contenido Abusivo, Recolección de información y Sistema vulnerable.*

>> 3.2. Incidentes gestionados en relación con los Operadores Críticos (entidades privadas)

A lo largo del año se ha comenzado a prestar servicio a QUINCE (15) Operadores Críticos nuevos, si bien el número de incidentes de ciberseguridad ha disminuido en un 18,41% con respecto al año anterior, gestionando durante 2018 un total de SETECIENTOS VEINTIDÓS (722) incidentes. Este valor decreciente respecto al año anterior puede explicarse por el hecho de que operadores de titularidad pública de acuerdo a la ley Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público,

han comenzado a reportar los incidentes que registran en sus redes y sistemas de información a su CSIRT de referencia.

El 31,02% de los incidentes relacionados con el ámbito competencial de Protección de Infraestructuras Críticas (PIC), estuvo relacionado con *Sistemas vulnerables*, los cuales fueron detectados en su gran mayoría por los servicios proactivos que presta el INCIBE-CERT. Por otro lado, el 27,70% de los incidentes detectados en Operadores Críticos estuvo relacionado con *Malware*.

>> 3.3. Incidentes gestionados por comunidad de referencia

En relación a los incidentes gestionados en función de su *constituency* o comunidad de referencia, *Ciudadanos y empresas* representa la gran mayoría, con un valor porcentual del 92,84%, seguido por un 7,52% de valores relativos a *Red académica (RedIris)*, y finalmente un 1% relativo a los incidentes registrados en el ámbito de las Infraestructuras Críticas.

>> 3.4. Incidentes gestionados por Sector Estratégico

Los sectores PIC donde se detectaron mayor número de incidentes fueron el Sector Tributario y Financiero (29,64%), seguido del Sector Transporte (26,59%), y el Sector Energía (20,64%).

>> 3.5. Empresas que firmaron acuerdo de confidencialidad con el CNPIC e INCIBE.

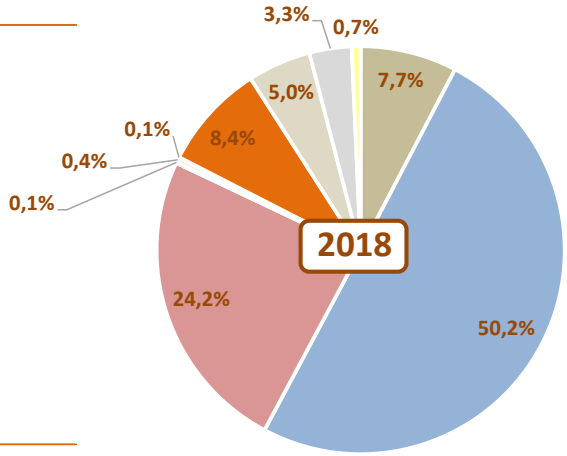
Durante el año 2018 se firmaron QUINCE (15) nuevos acuerdos de confidencialidad (NDA) con operadores estratégicos.

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.1. Incidentes gestionados por el INCIBE-CERT

Tipo de incidente	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Intrusión	16.054	14.373	19.275	8.541
Fraude	13.410	11.843	11.959	55.932
Malware	15.177	76.811	81.090	27.016
SPAM	1.275	10.279	7.957	0
Disponibilidad	794	495	514	100
Intento de intrusión	335	381	1.435	396
Robos de información	26	37	47	63
Contenido Abusivo				9.353
Recolección de información				5.605
Sistema Vulnerable				3.731
Otros	2.905	1.038	787	782

Porcentaje del total de incidentes gestionados

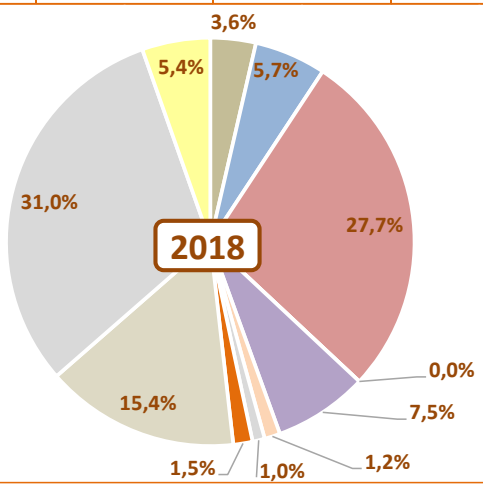


*Véase metadatos explicativos

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

Tipo de incidente	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Intrusión	15	39	97	26
Fraude	8	13	66	41
Malware	75	311	387	200
SPAM	0	8	21	0
Disponibilidad	10	28	55	54
Intento de intrusión	7	24	159	9
Robos de información	2	1	1	7
Contenido Abusivo				11
Recolección de información				111
Sistema Vulnerable				224
Otros	13	55	99	39

Porcentaje del total de incidentes gestionados



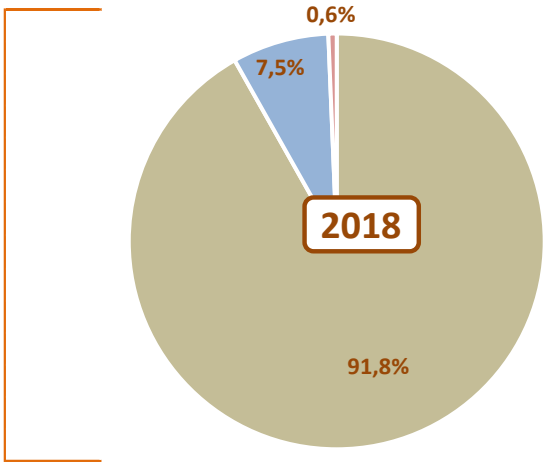
*Véase metadatos explicativos

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.3. Incidentes gestionados por comunidad de referencia

Incidentes por público objetivo	INCIDENTES GESTIONADOS			
	2015	2016	2017	2018
Ciudadanos y empresas	45.693	110.293	116.642	102.414
Red académica (RedIris)	4.153	4.485	5.537	8.383
Infraestructuras Críticas (IICC)	130	479	885	722

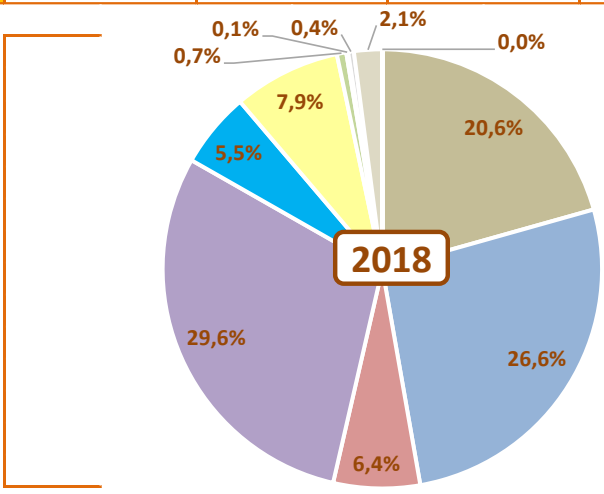
Porcentaje del total de incidentes gestionados



>> 3.4. Incidentes gestionados por sector estratégico

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

Porcentaje del total de incidentes gestionados



3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.5. Empresas que firmaron acuerdo de confidencialidad entre INCIBE Y CNPIC

Sector estratégico	ACUERDOS DE CONFIDENCIALIDAD FIRMADOS			
	2015	2016	2017	2018
Energía	0	2	2	0
Transporte	3	17	5	5
Tegnologías Informac. y Comunicac. (TIC)	1	1	1	1
Sistema tributario y financiero	7	10	3	2
Alimentación	0	2	0	5
Agua	0	14	4	0
Industria nuclear	1	0	0	0
Administración	0	0	0	0
Espacio	0	0	3	1
Industria química	0	0	6	1
Instalaciones de Investigación	0	0	0	0
Salud	0	0	0	0

COMUNIDAD DE PRESTACIÓN DE SERVICIOS A EMPRESAS ESTRATÉGICAS

Durante el año 2018, hubo 15 Operadores Estratégicos que firmaron acuerdos de confidencialidad, en virtud a lo cual el INCIBE-CERT brindó sus servicios de ciberseguridad en relación a mitigación y resolución de incidentes de ciberseguridad. Durante el año 2017 se pusieron en marcha 24 acuerdos, 46 durante el año 2016, y 12 durante el año 2015.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD >>

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

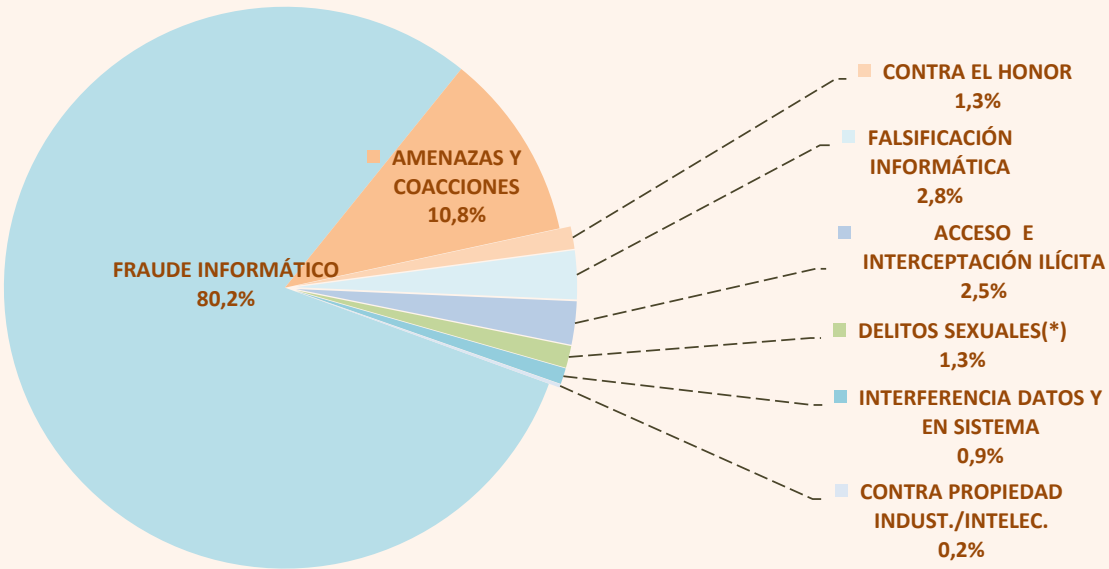
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2015	2016	2017	2018
ACCESO E INTERCEPTACIÓN ILÍCITA	2.386	2.579	2.505	2.750
AMENAZAS Y COACCIONES	10.112	11.473	11.270	11.960
CONTRA EL HONOR	2.131	1.524	1.537	1.423
CONTRA PROPIEDAD INDUST./INTELEC.	167	121	109	217
DELITOS SEXUALES(*)	1.233	1.188	1.312	1.393
FALSIFICACIÓN INFORMÁTICA	2.361	2.697	2.961	3.095
FRAUDE INFORMÁTICO	40.864	45.894	60.511	88.760
INTERFERENCIA DATOS Y EN SISTEMA	900	1.110	1.102	1.015
Total HECHOS CONOCIDOS	**60.154**	**66.586**	**81.307**	**110.613**

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



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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

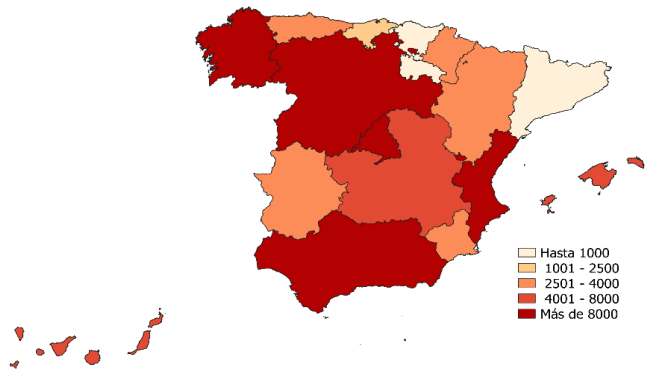
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.3. Representación territorial de hechos denunciados de cibercriminalidad. Año 2018

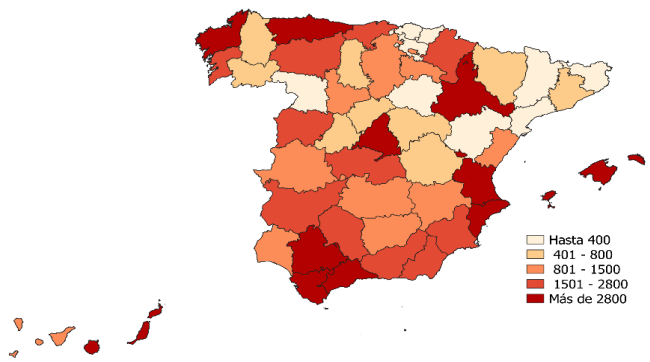
Hechos denunciados de CIBERCRIMINALIDAD - 2018

Hechos conocidos:	110.613	
Esclarecimiento:	24.767	**22,4%**
Detenciones/invest:	5.697	

CCAA	Hechos
MADRID (COMUNIDAD DE)	20.134
ANDALUCÍA	20.089
COMUNITAT VALENCIANA	14.189
GALICIA	8.364
CASTILLA Y LEÓN	8.042
BALEARS (ILLES)	6.277
CASTILLA - LA MANCHA	6.006
CANARIAS	4.445
EN EL EXTRANJERO	4.077
ARAGÓN	3.769
ASTURIAS (PRINCIPADO DE)	2.809
MURCIA (REGIÓN DE)	2.672
NAVARRA (COMUNIDAD FORAL DE)	2.574
EXTREMADURA	2.520
CANTABRIA	2.000
CATALUÑA	970
RIOJA (LA)	808
PAÍS VASCO	426
CIUDAD AUTÓNOMA DE MELILLA	229
CIUDAD AUTÓNOMA DE CEUTA	213



Hechos denunciados de CIBERCRIMINALIDAD - 2018



Provincias más afectadas:	Hechos
Madrid	20.134
Valencia/València	7.993
Balears (Illes)	6.277
Coruña (A)	4.824
Alicante/Alacant	4.732
Sevilla	4.442
EN EL EXTRANJERO	4.077
Málaga	3.651
Cádiz	3.290
Palmas (Las)	3.086
Zaragoza	2.963
Asturias	2.809
Murcia	2.672
Navarra	2.574
Toledo	2.352
Granada	2.317
Pontevedra	2.132
Córdoba	2.068
Cantabria	2.000
León	1.969

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

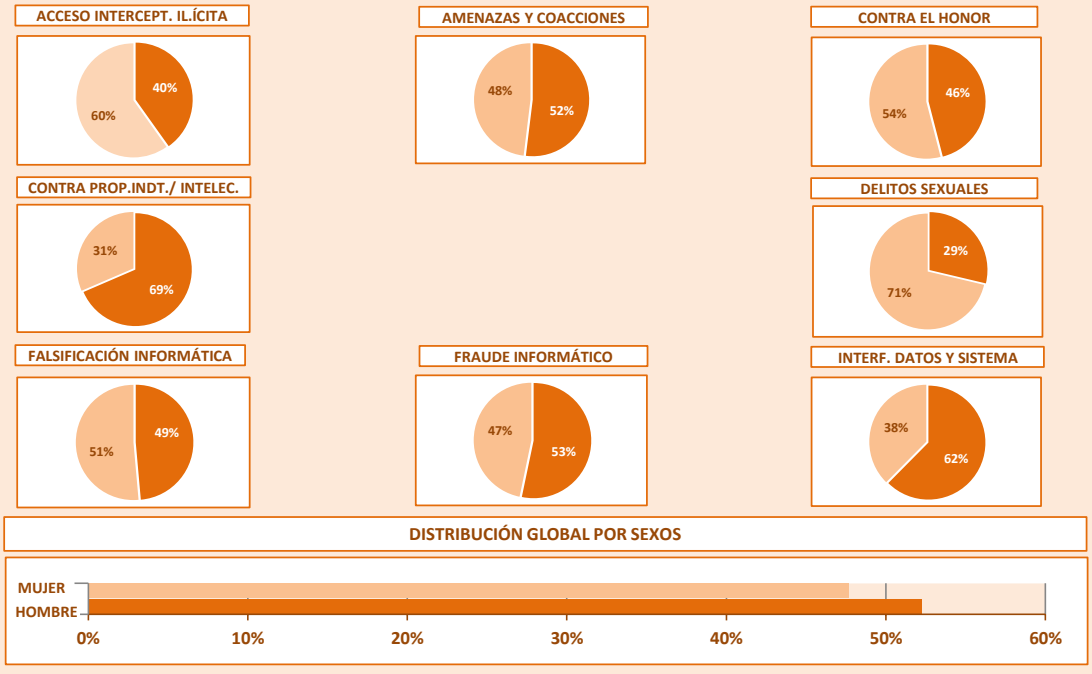
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.4. Victimizaciones registradas según grupo penal y sexo. Año 2018

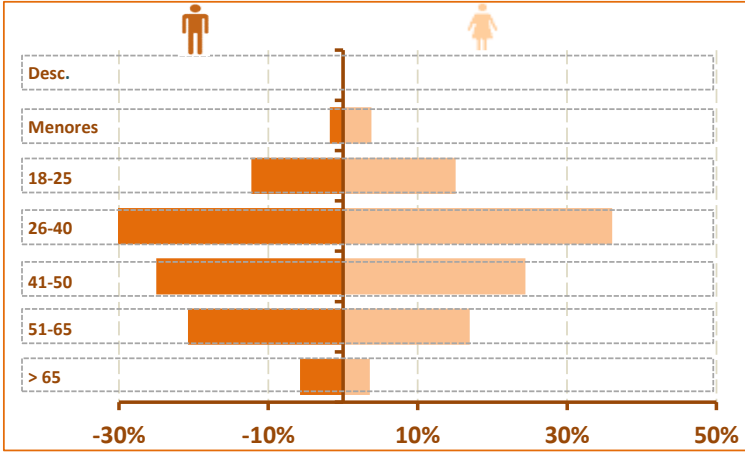
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.019	1.519	2	2.540
AMENAZAS Y COACCIONES	6.454	5.972	32	12.458
CONTRA EL HONOR	680	799	13	1.492
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	37	17	0	54
DELITOS SEXUALES (*)	267	663	6	936
FALSIFICACIÓN INFORMÁTICA	1.049	1.110	2	2.161
FRAUDE INFORMÁTICO	34.159	29.954	35	64.148
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	510	307	1	818
Total VICTIMIZACIONES	**44.175**	**40.341**	**91**	**84.607**

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

DISTRIBUCIÓN PORCENTUAL DE LAS VÍCTIMAS POR GRUPO PENAL SEGÚN SEXO



>> 4.5. Victimizaciones según grupo de edad y sexo. Año 2018



Grupo de edad	Hombre	Mujer	Descon.
Edad descon.	84	52	14
Menores de edad	787	1.528	4
De 18 a 25 años	5.423	6.088	0
De 26 a 40 años	15.132	14.543	15
De 41 a 50 años	11.041	9.846	20
De 51 a 65 años	9.170	6.845	23
Mayores 65 años	2.538	1.439	15
TOTAL	**44.175**	**40.341**	**91**

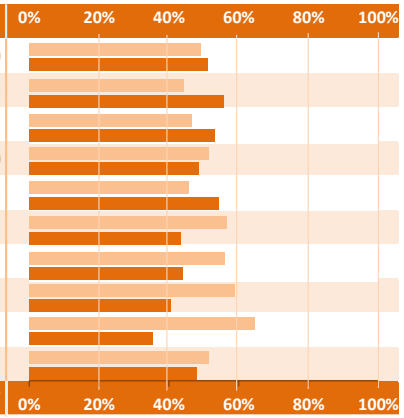
ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

(Fuente de datos: Sistema Estadístico de Criminalidad)

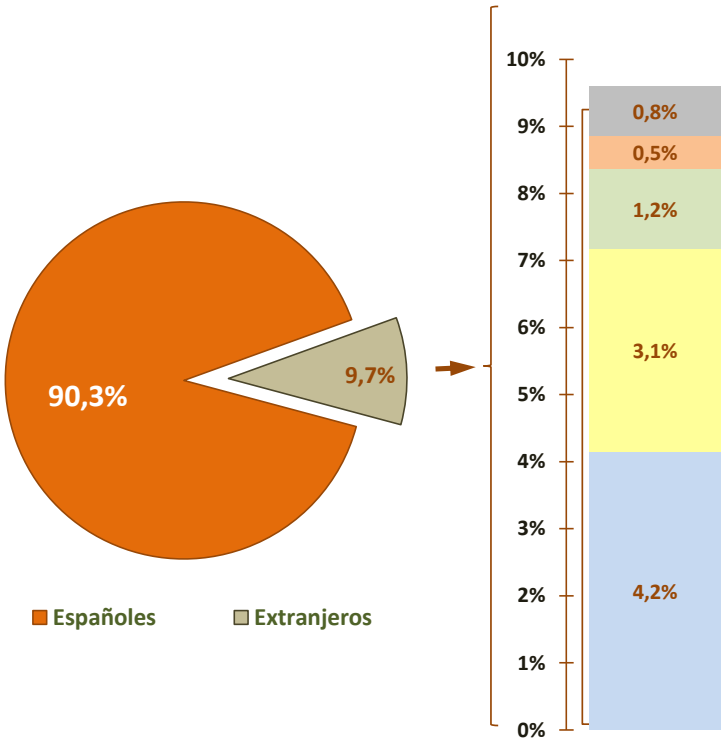
>> 4.6. Victimizaciones por tipología penal y sexo. Año 2018

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS TARJ CRÉDITO, DÉB. Y CHEQ.VIAJE	16.712	16.072	6	32.790
OTRAS ESTAFAS	16.351	12.963	25	29.339
AMENAZAS	5.718	5.014	31	10.763
USURPACIÓN DE ESTADO CIVIL	1.049	1.109	2	2.160
ESTAFA BANCARIA	1.096	919	4	2.019
COACCIONES	734	958	1	1.693
ACCESO ILEGAL INFORMÁTICO	610	775	0	1.385
INJURIAS	468	680	5	1.153
DESCUBRIMI./REVELACIÓN DE SECRETOS	408	743	2	1.153
RESTO	1.029	1.108	15	2.152
Total VICTIMIZACIONES	**44.175**	**40.341**	**91**	**84.607**



>> 4.7. Nacionalidad de la víctima. Año 2018

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	**76.402**	**90,3%**
2.- EXTRANJEROS	**8.205**	**9,7%**
2.1.- UNIÓN EUROPEA	**3.536**	**4,2%**
Rumanía	994	1,2%
Italia	689	0,8%
Reino Unido	356	0,4%
Bulgaria	260	0,3%
Alemania	245	0,3%
Resto	992	1,2%
2.2.- AMÉRICA	**2.597**	**3,1%**
Colombia	390	0,5%
Venezuela	332	0,4%
Ecuador	276	0,3%
Resto	1.599	1,9%
2.3.- ÁFRICA	**1.014**	**1,2%**
Marruecos	592	0,7%
Argelia	82	0,1%
Resto	340	0,4%
2.4.- ÁSIA	**420**	**0,5%**
China	147	0,2%
Pakistán	64	0,1%
Resto	209	0,2%
2.5.- RESTO PAÍSES	**638**	**0,8%**
Ucrania	157	0,2%
Rusia	115	0,1%
Otros	366	0,4%
TOTAL	**84.607**	**100%**



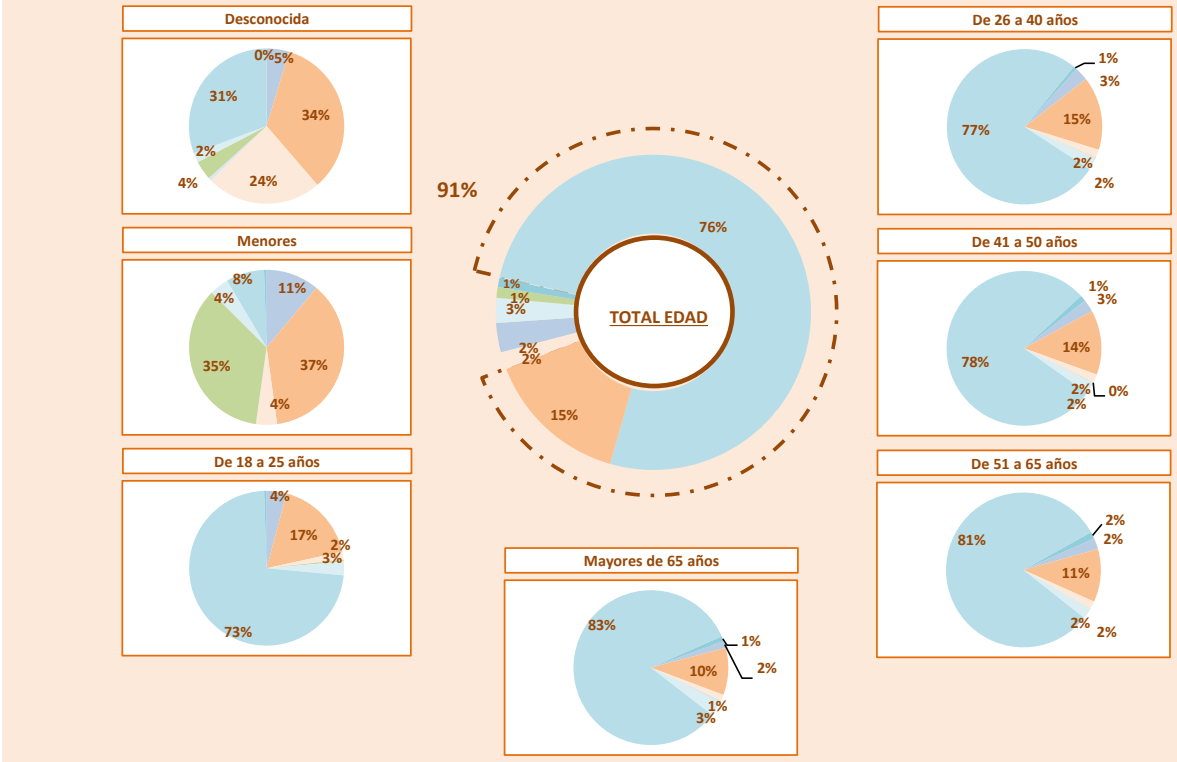
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

(Fuente de datos: Sistema Estadístico de Criminalidad)

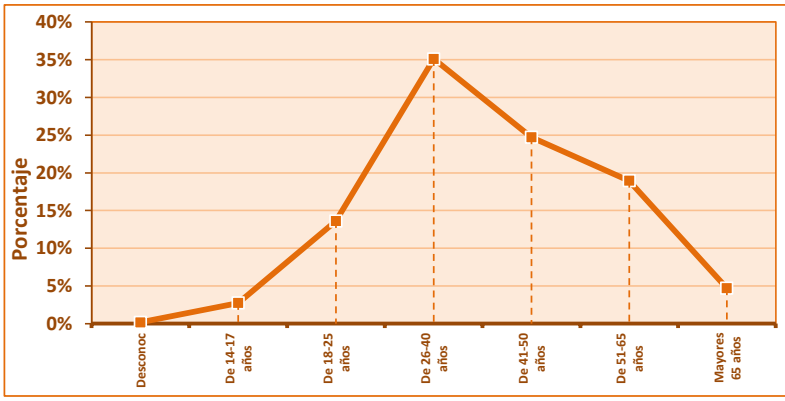
>> 4.8. Victimizaciones registradas según grupo penal y edad. Año 2018

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	7	258	480	831	539	368	57
AMENAZAS Y COACCIONES	51	851	2.003	4.555	2.824	1.780	394
CONTRA EL HONOR	36	102	190	502	355	258	49
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	8	14	12	17
DELITOS SEXUALES(*)	6	818	44	31	23	11	3
FALSIFICACIÓN INFORMÁTICA	3	93	328	772	498	347	120
FRAUDE INFORMÁTICO	46	185	8.407	22.776	16.389	13.035	3.310
INTERFERENCIA EN DATOS Y EN SISTEMA	0	12	57	215	265	227	42
Total VICTIMIZACIONES	**150**	**2.319**	**11.511**	**29.690**	**20.907**	**16.038**	**3.992**

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



>> 4.9. Edad de la víctima. Año 2018



Grupo de edad	Víctimas
Edad desconocida	150
Menores de edad	2.319
De 18 a 25 años	11.511
De 26 a 40 años	29.690
De 41 a 50 años	20.907
De 51 a 65 años	16.038
Mayores 65 años	3.992
TOTAL	**84.607**

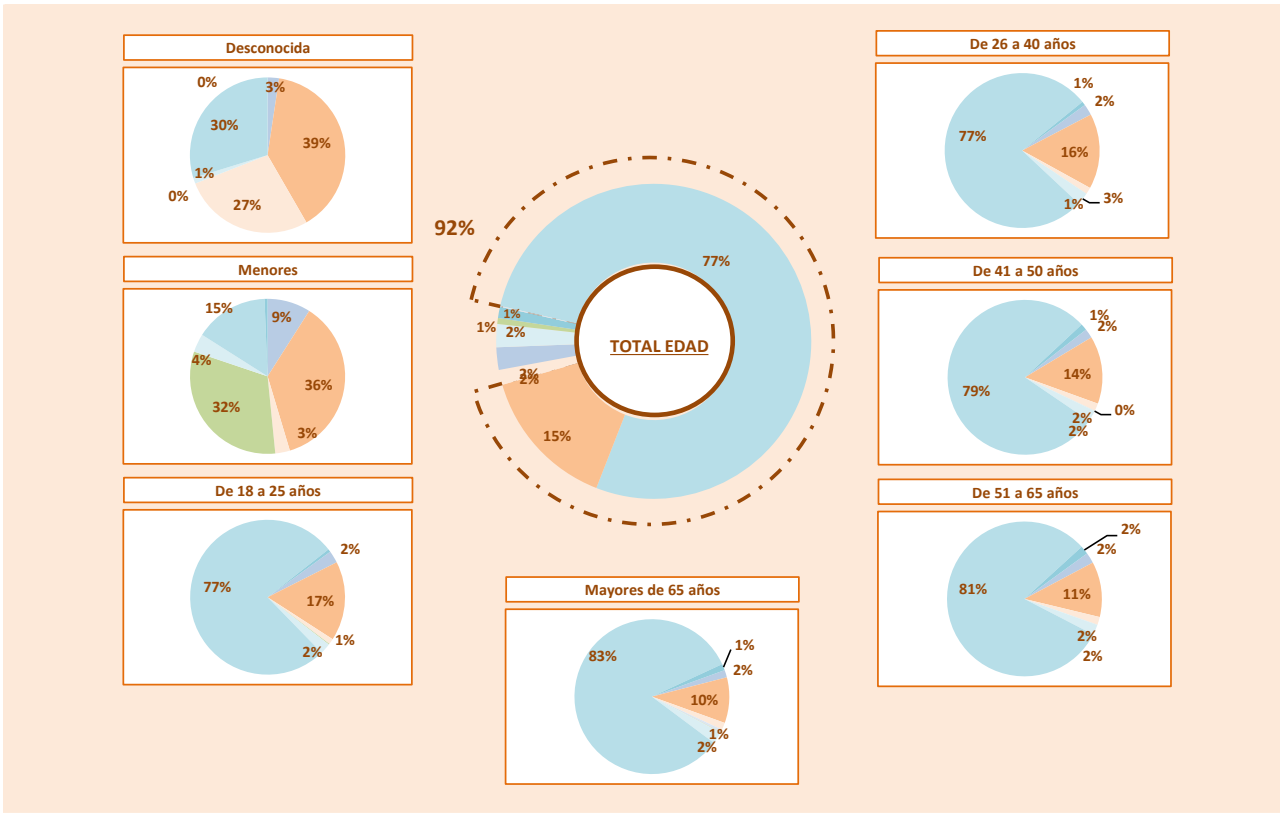
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (HOMBRE)

(Fuente de datos: Sistema Estadístico de Criminalidad)

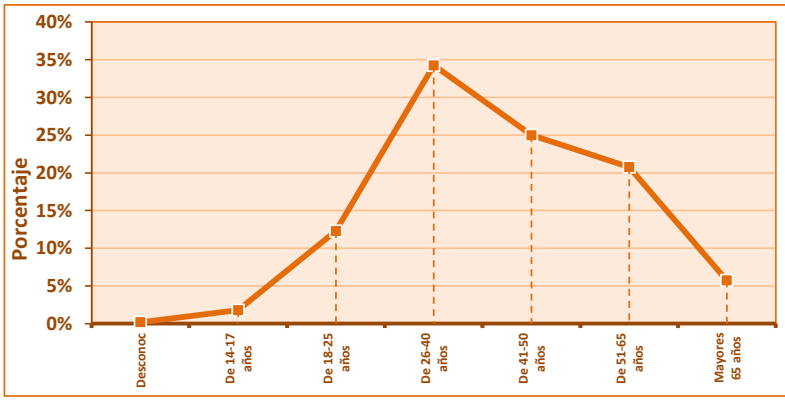
>> 4.10. Victimizaciones registradas según grupo penal y edad. Año 2018

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	2	71	138	351	214	204	39
AMENAZAS Y COACCIONES	33	286	899	2.375	1.561	1.058	242
CONTRA EL HONOR	23	24	62	210	174	149	38
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	4	10	6	15
DELITOS SEXUALES(*)	0	250	9	3	2	1	2
FALSIFICACIÓN INFORMÁTICA	1	30	122	382	254	196	64
FRAUDE INFORMÁTICO	25	121	4.158	11.684	8.673	7.394	2.104
INTERFERENCIA EN DATOS Y EN SISTEMA	0	5	33	123	153	162	34
Total VICTIMIZACIONES	**84**	**787**	**5.423**	**15.132**	**11.041**	**9.170**	**2.538**

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



>> 4.11. Edad de la víctima. Año 2018



Grupo de edad	Víctimas
Edad desconocida	84
Menores de edad	787
De 18 a 25 años	5.423
De 26 a 40 años	15.132
De 41 a 50 años	11.041
De 51 a 65 años	9.170
Mayores 65 años	2.538
TOTAL	**44.175**

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

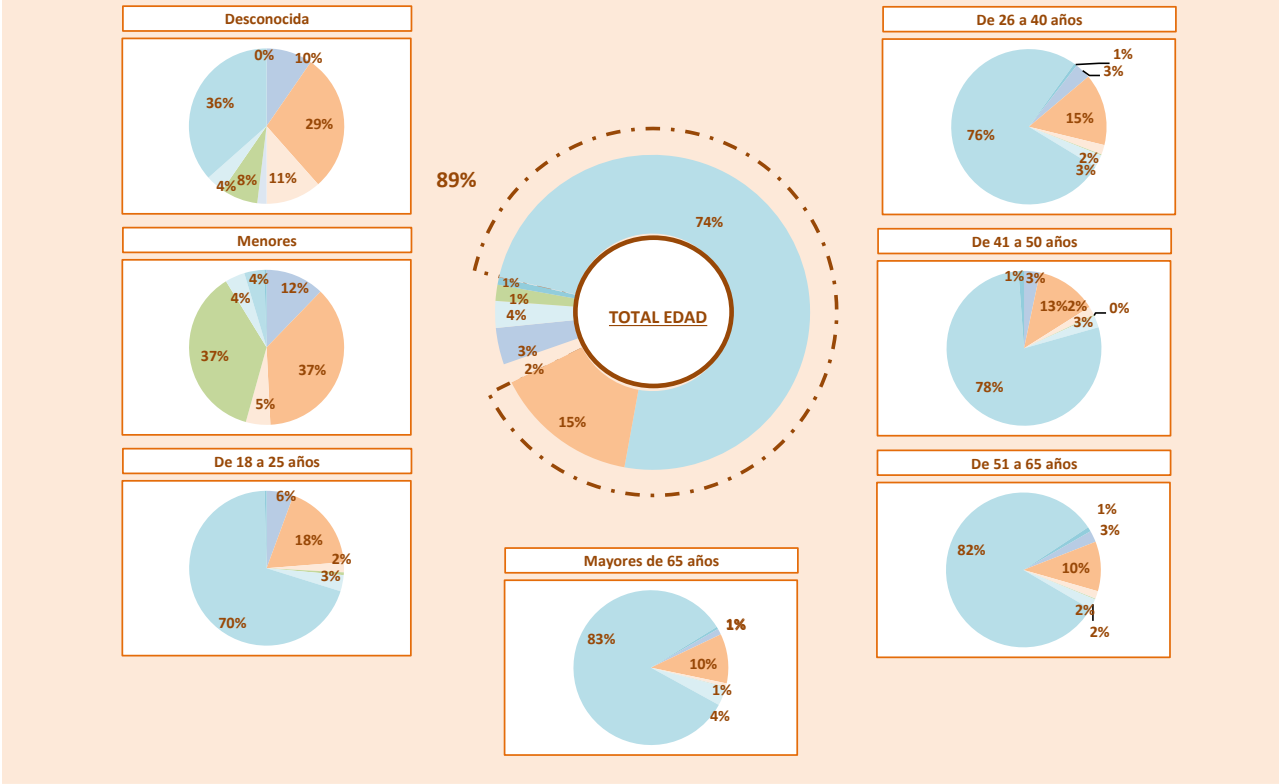
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (MUJER)

(Fuente de datos: Sistema Estadístico de Criminalidad)

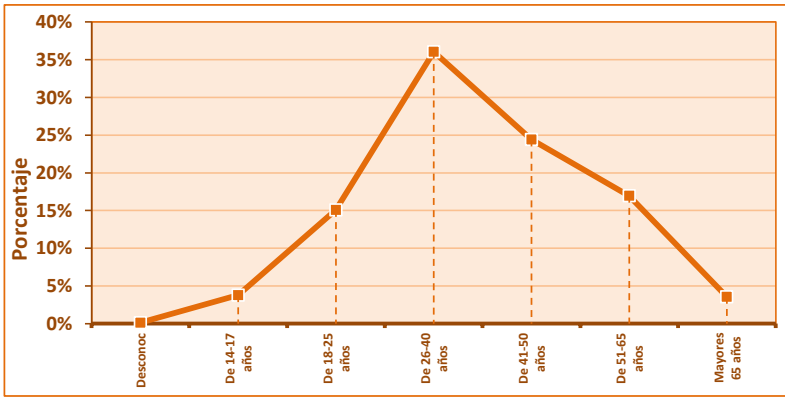
>> 4.12. Victimizaciones registradas según grupo penal y edad. Año 2018

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	5	187	342	478	325	164	18
AMENAZAS Y COACCIONES	15	565	1.104	2.174	1.255	710	149
CONTRA EL HONOR	6	78	128	290	181	106	10
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	0	4	4	6	2
DELITOS SEXUALES(*)	4	564	35	28	21	10	1
FALSIFICACIÓN INFORMÁTICA	2	63	206	389	244	151	55
FRAUDE INFORMÁTICO	19	64	4.249	11.088	7.704	5.633	1.197
INTERFERENCIA EN DATOS Y EN SISTEMA	0	7	24	92	112	65	7
Total VICTIMIZACIONES	**52**	**1.528**	**6.088**	**14.543**	**9.846**	**6.845**	**1.439**

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



>> 4.13. Edad de la víctima. Año 2018



Grupo de edad	Víctimas
Edad desconocida	52
Menores de edad	1.528
De 18 a 25 años	6.088
De 26 a 40 años	14.543
De 41 a 50 años	9.846
De 51 a 65 años	6.845
Mayores 65 años	1.439
TOTAL	**40.341**

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

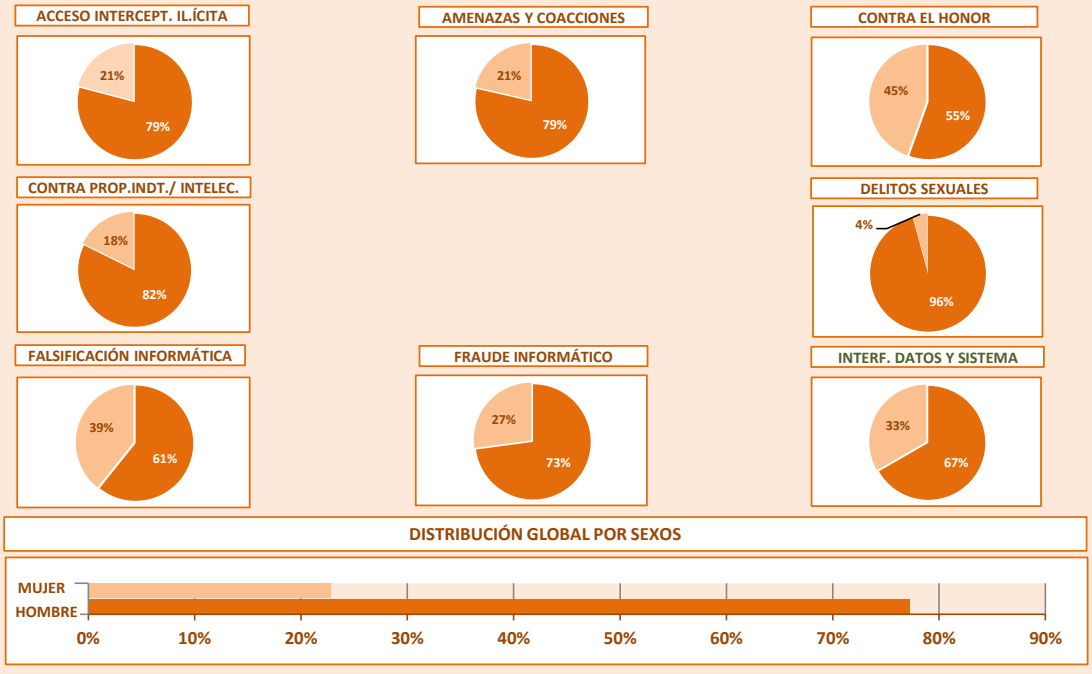
(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.14. Detenciones/investigados registrados según grupo penal y sexo. Año 2018

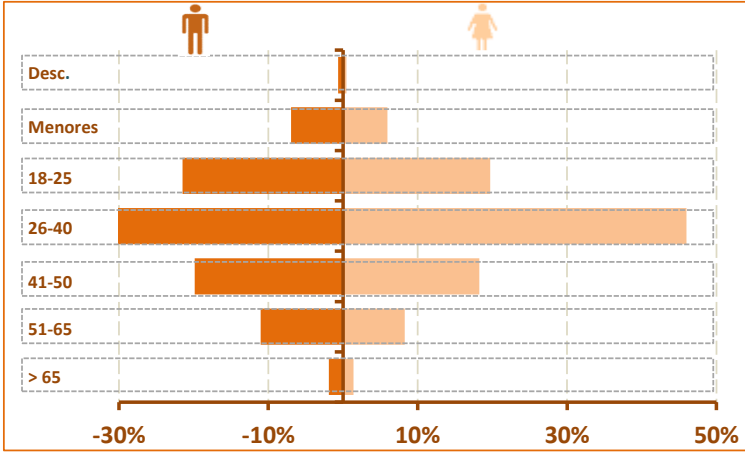
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	223	59	282
AMENAZAS Y COACCIONES	969	264	1.233
CONTRA EL HONOR	66	53	119
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	191	41	232
DELITOS SEXUALES(*)	862	38	900
FALSIFICACIÓN INFORMÁTICA	232	150	382
FRAUDE INFORMÁTICO	1.842	686	2.528
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	14	7	21
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**4.399**	**1.298**	**5.697**

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

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



>> 4.15. DETENCIONES/INVESTIGADOS según grupo de edad y sexo. Año 2018



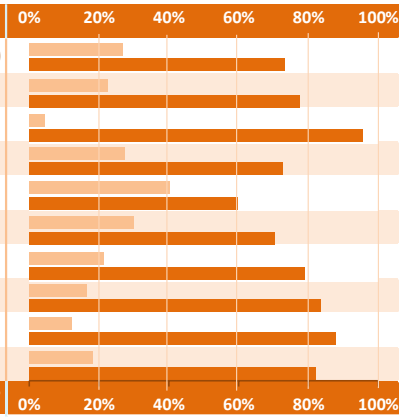
Grupo de edad	Hombre	Mujer
Edad desconocida	28	6
De 14 a 17 años	306	77
De 18 a 25 años	946	256
De 26 a 40 años	1.678	597
De 41 a 50 años	873	237
De 51 a 65 años	485	107
Mayores 65 años	83	18
TOTAL	**4.399**	**1.298**

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

(Fuente de datos: Sistema Estadístico de Criminalidad)

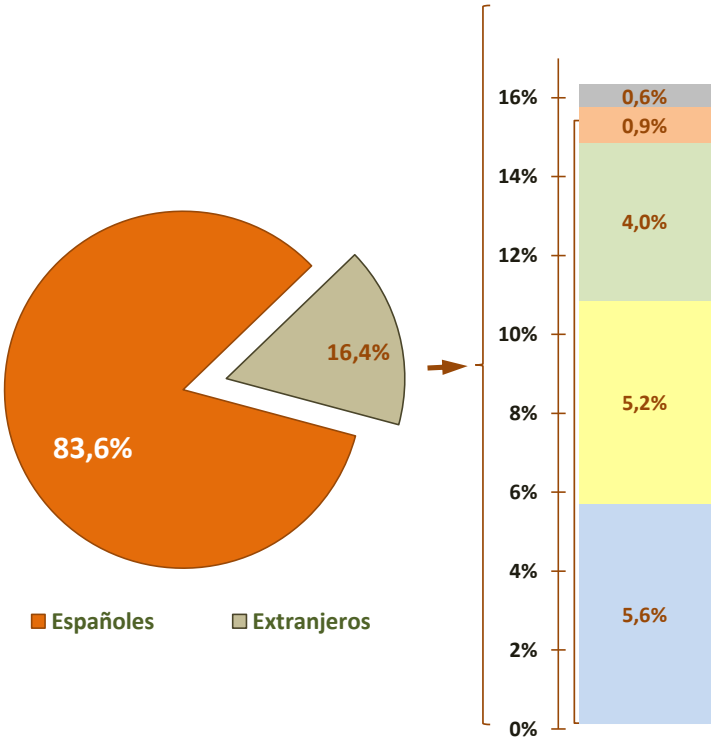
>> 4.16. Detenciones/investigados por tipología penal y sexo. Año 2018

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	1.399	511	1.910
AMENAZAS	793	229	1.022
PORNOGRAFÍA DE MENORES	566	26	592
ESTAFAS TARJ CRÉDITO, DÉB. Y CHEQ.VIAJE	271	102	373
USURPACIÓN DE ESTADO CIVIL	223	150	373
ESTAFA BANCARIA	172	73	245
DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	185	50	235
COACCIONES	176	35	211
CONTRA LA PROPIEDAD INTELECTUAL	159	22	181
RESTO	455	100	555
Total VICTIMIZACIONES CIBERCRIMINALIDAD	**4.399**	**1.298**	**5.697**



>> 4.17. Nacionalidad de los detenciones/investigados. Año 2018

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	**4.764**	**83,6%**
2.- EXTRANJEROS	**933**	**16,4%**
2.1.- UNIÓN EUROPEA	**320**	**5,6%**
Rumania	181	3,2%
Bulgaria	24	0,4%
Italia	22	0,4%
Reino Unido	20	0,4%
Alemania	13	0,2%
Resto	60	1,1%
2.2.- AMÉRICA	**298**	**5,2%**
Colombia	61	1,1%
Ecuador	46	0,8%
Venezuela	38	0,7%
Resto	153	2,7%
2.3.- ÁFRICA	**230**	**4,0%**
Marruecos	104	1,8%
Nigeria	66	1,2%
Resto	60	1,1%
2.4.- ÁSIA	**52**	**0,9%**
China	28	0,5%
Pakistán	14	0,2%
Resto	10	0,2%
2.5.- RESTO PAÍSES	**33**	**0,6%**
Rusia	13	0,2%
Ucrania	8	0,1%
Otros	12	0,2%
TOTAL	**5.697**	**100%**



ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

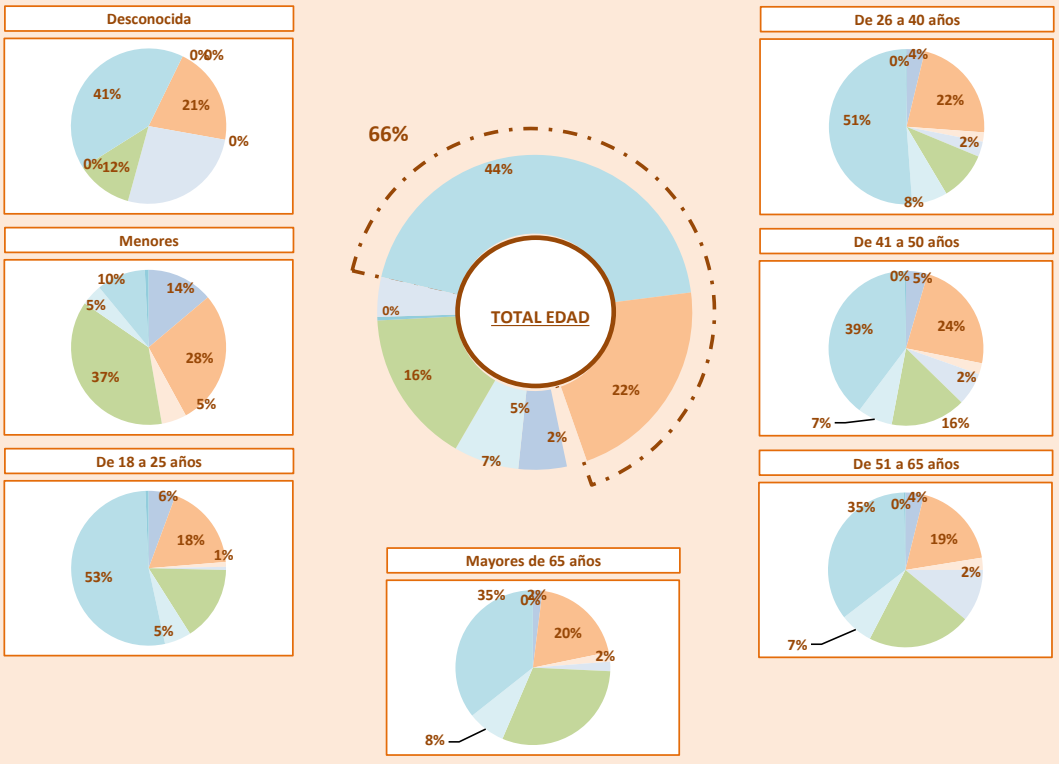
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

(Fuente de datos: Sistema Estadístico de Criminalidad)

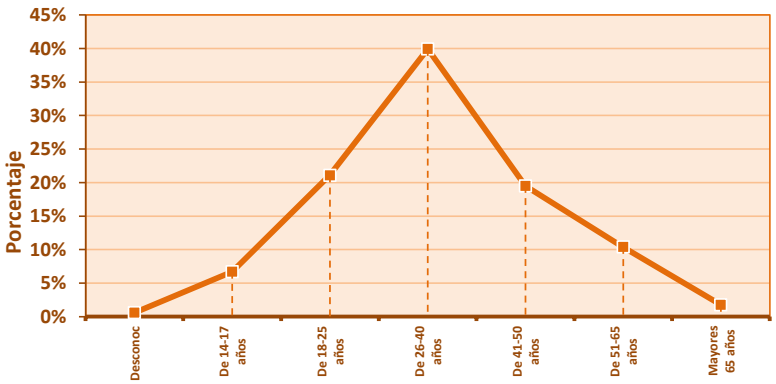
>> 4.18. Detenciones/investigados registradas según grupo penal y edad. Año 2018

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	53	68	86	50	23	2
AMENAZAS Y COACCIONES	7	108	217	509	262	110	20
CONTRA EL HONOR	0	20	12	44	26	15	2
CONTRA PROPIEDAD INDUST./INTELEC.	9	0	8	72	76	65	2
DELITOS SEXUALES(*)	4	143	188	232	174	128	31
FALSIFICACIÓN INFORMÁTICA	0	17	67	168	81	41	8
FRAUDE INFORMÁTICO	14	39	634	1159	438	208	36
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	8	5	3	2	0
Total DETENCIONES/INVESTIGADOS	**34**	**383**	**1.202**	**2.275**	**1.110**	**592**	**101**

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



>> 4.19. Edad de las personas detenidas/investigadas. Años 2018



Grupo de edad	Det./Inv.
Edad desconocida	34
De 14 a 17 años	383
De 18 a 25 años	1.202
De 26 a 40 años	2.275
De 41 a 50 años	1.110
De 51 a 65 años	592
Mayores 65 años	101
TOTAL	**5.697**

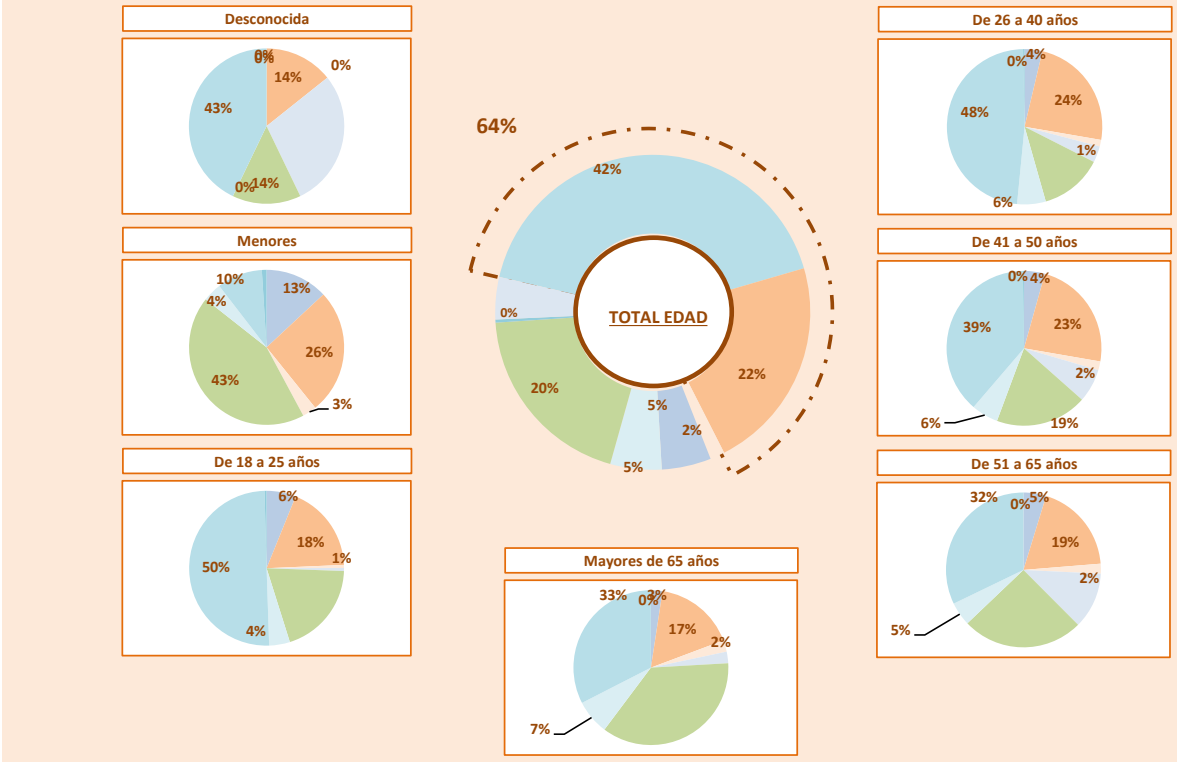
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

(Fuente de datos: Sistema Estadístico de Criminalidad)

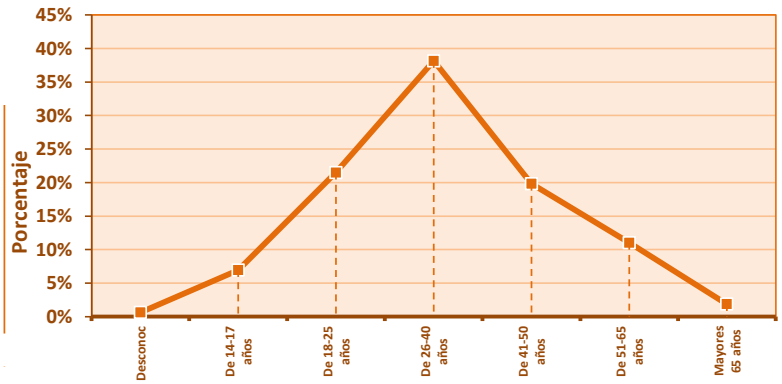
>> 4.20. Detenciones/investigados registradas según grupo penal y edad. Año 2018

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	40	58	62	38	23	2
AMENAZAS Y COACCIONES	4	80	172	403	204	92	14
CONTRA EL HONOR	0	9	6	23	16	10	2
CONTRA PROPIEDAD INDUST./INTELEC.	8	0	6	57	61	57	2
DELITOS SEXUALES(*)	4	133	185	220	167	123	30
FALSIFICACIÓN INFORMÁTICA	0	12	41	100	49	24	6
FRAUDE INFORMÁTICO	12	29	474	808	336	156	27
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	4	5	2	0	0
Total DETENCIONES/INVESTIGADOS	**28**	**306**	**946**	**1.678**	**873**	**485**	**83**

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



>> 4.21. Edad de las personas detenidas/investigadas. Años 2018



Grupo de edad	Det./Inv.
Edad desconocida	28
De 14 a 17 años	306
De 18 a 25 años	946
De 26 a 40 años	1.678
De 41 a 50 años	873
De 51 a 65 años	485
Mayores 65 años	83
TOTAL	**4.399**

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

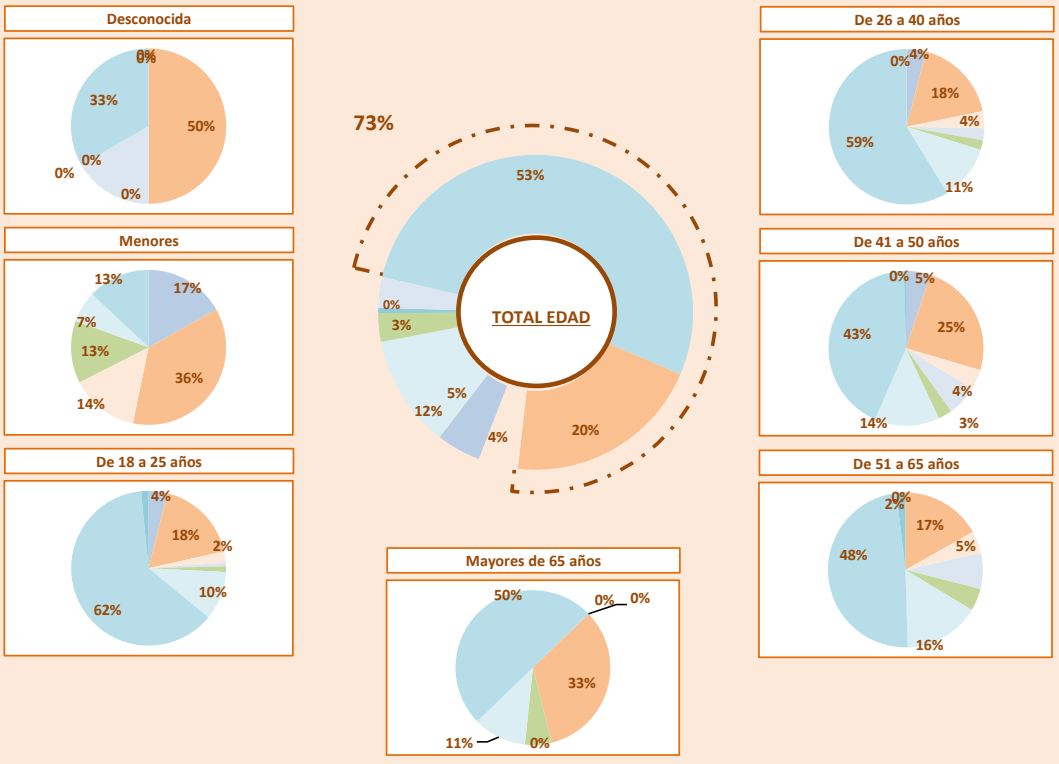
4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

(Fuente de datos: Sistema Estadístico de Criminalidad)

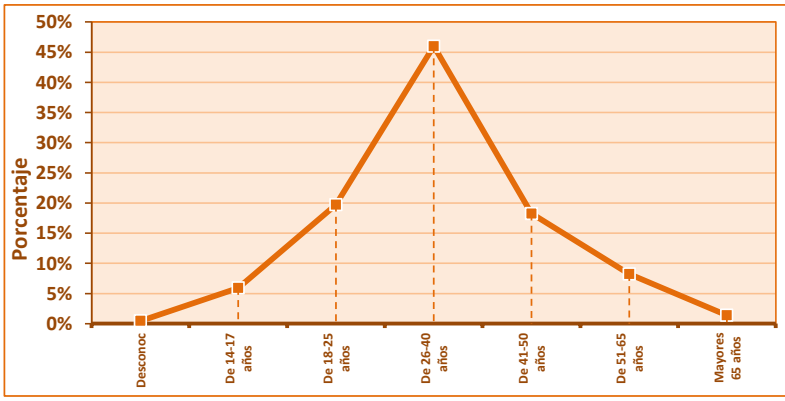
>> 4.22. Detenciones/investigados registradas según grupo penal y edad. Año 2018

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	13	10	24	12	0	0
AMENAZAS Y COACCIONES	3	28	45	106	58	18	6
CONTRA EL HONOR	0	11	6	21	10	5	0
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	15	15	8	0
DELITOS SEXUALES(*)	0	10	3	12	7	5	1
FALSIFICACIÓN INFORMÁTICA	0	5	26	68	32	17	2
FRAUDE INFORMÁTICO	2	10	160	351	102	52	9
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	4	0	1	2	0
Total DETENCIONES/INVESTIGADOS	**6**	**77**	**256**	**597**	**237**	**107**	**18**

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



>> 4.23. Edad de las personas detenidas/investigadas. Años 2018



Grupo de edad	Det./Inv.
Edad desconocida	6
De 14 a 17 años	77
De 18 a 25 años	256
De 26 a 40 años	597
De 41 a 50 años	237
De 51 a 65 años	107
Mayores 65 años	18
TOTAL	**1.298**

ESTUDIO 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 2018)

Porcentaje de viviendas con / sin algún tipo de ordenador
Porcentaje de viviendas con / sin acceso a internet
Contraste evolutivo de las viviendas 2009-2018
Porcentaje de viviendas con ordenador por tipo hábitat
Porcentaje de viviendas con acceso a internet por tipo hábitat
http://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=01001.px

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 2018)

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.
http://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=01002.px

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 2018)

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.

http://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=01005.px

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 2018)

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

http://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2018/l0/&file=02002.px&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 2018. Spain (Comisión Europea)

http://ec.europa.eu/information_society/newsroom/image/document/2018-20/es-desi_2018-country-profile-lang_4AA8143E-CA74-9BD7-2FBD36EBA0B95CCB_52357.pdf

2.7. Indicadores de la sociedad de la información

Indicadores destacados de la Sociedad de la Información (diciembre 2018-ONTSI)

https://www.ontsi.red.es/ontsi/sites/ontsi/files/IndicadoresDestacadosDiciembre2018.pdf

>> Datos estadísticos de criminalidad

Origen de los datos

Los datos han sido obtenidos del Sistema Estadístico de Criminalidad (SEC). Para su cómputo se tienen en cuenta los hechos de los que han tenido conocimiento los siguientes cuerpos policiales: Guardia Civil, Cuerpo Nacional de Policía, Policía Foral de Navarra y las Policías Locales que facilitan datos al Sistema Estadístico de Criminalidad (SEC).

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 criminalidad 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 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.

El porcentaje de esclarecimiento se obtiene dividiendo el total de hechos esclarecidos por el total de hechos conocidos y multiplicando el resultado por 100.

Se considera que una persona física o jurídica, está investigada a causa de la atribución de participación en un hecho penal, sin adoptar medidas restrictivas de libertad para esa persona investigada. La detención va más allá realizando todo el proceso que lleva a la lectura de derechos de la persona física, privándole de libertad y poniéndolo a disposición judicial, por la atribución de la comisión de una infracción penal.

El concepto de victimización viene referido al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal. Se diferencia del concepto de víctima, ya que éste se refiere a personas individuales.

En una denuncia pueden darse varios hechos conjuntamente, e incluso pueden existir varias víctimas o perjudicados, siendo las victimizaciones el término que engloba a los diferentes hechos que afectan a una determinada víctima.

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

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

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SEC A UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ACCESO ILEGAL INFORMÁTICO	Ninguna
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	DAÑOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ATAQUES INFORMÁTICOS	Ninguna
Falsificación informática	Arts CP 388-389, 399 bis, 400 y 401	FALSIFICACION DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE UTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude Informático	Arts. CP 248 a 251 y 623.4	ESTAFA BANCARIA	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE VIAJE	
		OTRAS ESTAFAS	
Delitos sexuales	Arts. CP 181, 183.1, 183 bis, 184, 185, 186, 189	EXHIBICIONISMO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		PROVOCACIÓN SEXUAL	
		ACOSO SEXUAL	
		ABUSO SEXUAL	
		CORRUPCIÓN DE MENORES/INCAPACITADOS	
		PORNOGRAFIA DE MENORES	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		INJURIAS	
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	AMENAZAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	
		COACCIONES	