MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

II Informe sobre Cibercriminalidad 2014

II Informe sobre Cibercriminalidad - 2014

SUMARIO

1.- Introducción 3

2.- Conceptos básicos 6

3.- Tendencias en materia de cibercriminalidad y ciberseguridad . . . 10

4.- Infraestructuras críticas y ciberseguridad 13

5.- Los nuevos delitos tecnológicos en la Ley Orgánica 1/2015, de reforma del Código Penal 20

6.-Datos Estadísticos sobre el uso de las nuevas tecnologías 27

A nivel nacional 28
A nivel europeo 37

7.-Datos Estadísticos de Cibercriminalidad: Sistemas Estadístico de Criminalidad (SEC) 41

Datos globales 42
Perfil de la VÍCTIMA: grupo penal, sexo y edad 45
Perfil del RESPONSABLE: grupo penal, sexo y edad 49

ANEXO 53

1.- Introducción

La globalización digital ha llevado a que las tecnologías de la información y las comunicaciones (TIC) constituyan una herramienta básica empleada diariamente por una gran mayoría de los ciudadanos. Sin duda, su uso masivo en todos los ámbitos de nuestra vida, personal, social, económico, laboral, etc., se ha convertido en una realidad incuestionable.

Ante esta realidad, las ciberamenazas, en un conjunto de variantes diversas, persiguen una finalidad fundamental: atentar, desde el ciberespacio, a la seguridad de las personas y de las infraestructuras.

Los objetivos de estas ciberamenazas se centran y afectan a casi todos los sectores económicos y sociales. No obstante, los que se encuentran relacionados con el mundo de la banca y las finanzas, el sector empresarial, las comunicaciones, la defensa, las infraestructuras críticas, y las tecnologías de la información son los que más pueden verse afectados.

Por dicho motivo, el pasado año se publicó, por parte del Ministerio del Interior, el primer Informe sobre Cibercriminalidad, en nuestro país.

Siguiendo con la iniciativa tomada hace un año, y con el intento de conocer el panorama delictivo de este fenómeno, la Ciberdelincuencia, se ha elaborado un segundo estudio que aglutina un mayor aporte de datos. Y muestra de ello, es que en este informe se recopila información estadística sobre la delincuencia conocida y facilitada por las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra y distintos Cuerpos de Policía Local), que figura en el Sistema Estadístico de Criminalidad (SEC), así como aquélla que registra el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Todo ello, con la finalidad de ofrecer una visión más real de la Cibercriminalidad.

El objeto del estudio de Cibercriminalidad relativo al año 2014, persigue, en primer lugar, presentar una definición sobre lo que se entiende por cibercriminalidad y ciberseguridad, así como otros conceptos claves en la materia.

No se puede obviar, sin duda, que desde un punto de vista jurídico en el término cibercriminalidad se incluyen todas aquellas conductas ilícitas definidas por el

Convenio sobre cibercriminalidad o Convenio de Budapest, del Consejo de Europa, de 23 de noviembre de 2001, y que han sido transpuestas a nuestra legislación[1]. Estas tipologías delictivas en el ámbito de la criminalidad se recogen de forma detallada en el primer Informe sobre Cibercriminalidad (2013), editado y de acceso libre en la web pública del Ministerio del Interior. [2]

Además, se introducen, en este estudio, otros apartados como son las mejoras legales aprobadas en nuestro país y las tendencias en materia de cibercriminalidad.

Los datos incorporados a este segundo Informe sobre Cibercriminalidad tratan de dibujar las amenazas que presenta la ciberdelincuencia, presente en España, y que afectan a todos los sectores de la sociedad. De ahí, el interés en mostrar datos que referencian el uso de las tecnologías por parte de la sociedad en general, teniendo en cuenta los resultados obtenidos por otros entes públicos, tanto nacionales (INE, Ministerio del Interior, ONTSI) como europeos (EUROSTAT) que recopilan información relativa a esta materia. Todos por tanto resultados provenientes de estudios y de encuestas de opinión realizadas durante los últimos años.

Los datos obtenidos del Sistema Estadístico de Criminalidad, registrados por las Fuerzas y Cuerpos de Seguridad y los procedentes del CNPIC, permiten dibujar un perfil de la víctima y del autor de esta tipología delictiva tan específica.

Por último, es importante tener en cuenta que en nuestro país, el Instrumento de Ratificación 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 el pasado día 1 de abril. De esta forma, en este segundo informe sobre Cibercriminalidad no se recogen, de forma expresa y diferenciada, datos concretos relativos a esta materia, al no estar registrados en el Sistema Estadístico de Criminalidad (SEC).

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

-Instrumento de Ratificación 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 (BOE núm. 26, de 30 de enero de 2015)

[2] http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

2.- Conceptos básicos

Según el diccionario de la Real Academia de la Lengua Española, *informática* es el "*conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*", y *ciberespacio* el "*ámbito artificial creado por medios informáticos"*.

La Estrategia de Ciberseguridad Nacional, en su Capítulo 1 "*El ciberespacio y su seguridad*", dice que *el ciberespacio* es el "*nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas"*[3].

Por otra parte, y en términos similares a los de la Estrategia de Ciberseguridad Nacional, la Orden Ministerial 10/2013 de 19 de febrero, por la que se crea el Mando Conjunto de la Ciberdefensa, en su artículo 2.1 establece que *el ciberespacio* consiste en el "*dominio global y dinámico compuesto por infraestructuras de tecnología de la información —incluyendo internet—, redes de telecomunicaciones y sistemas de información*".

Otro concepto a tener en cuenta en este ámbito es el de *sistema de información*. En este sentido, el Convenio del Consejo de Europa sobre la Ciberdelincuencia de Budapest, de 23 de junio de 2001, establece como tal "*todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa*."

La ciberdelincuencia, los delitos informáticos, la delincuencia informática, la criminalidad informática, o la delincuencia de sistemas informáticos, denominaciones empleadas por la doctrina para abordar este fenómeno, abarcan por lo general una amplia gama de actividades delictivas en las que los ordenadores y los sistemas de información se utilizan como principales herramientas para delinquir o son objeto principal para la comisión del delito.

[3] http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

La ciberdelincuencia comprende delitos tradicionales (por ejemplo, fraude, falsificación o usurpación de identidad), delitos relacionados con los contenidos (distribución en línea de pornografía infantil o incitación al odio racial) y delitos exclusivos de ordenadores y sistemas de información (ataques contra los sistemas de información, denegación de servicio o programas maliciosos)[4].

Asimismo, el Convenio sobre cibercriminalidad de Budapest del 23 noviembre 2001, define como *ciberdelitos* "*los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos*".

Por otra parte, en la Estrategia de Seguridad Nacional: un proyecto compartido, 2013[5] se establece que la ciberseguridad tiene por objeto "*garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques*", en desarrollo de sus previsiones en materia de protección del ciberespacio. Al mismo tiempo, en la Estrategia de Ciberseguridad Nacional se identifica el objetivo global de "*lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques*". De esta forma particular, ésta última Estrategia Nacional, establece además como una de las líneas de acción a llevar a cabo la potenciación de las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio.

En sentido jurídico, la definición de ciberseguridad existente dentro de nuestro ordenamiento jurídico la recoge el artículo 2.3 de la Orden Ministerial 10/2013 de 19 de febrero, por la que se crea el Mando Conjunto de la Ciberdefensa. En este artículo se dice que la *ciberseguridad* es el "*conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan*".

De igual forma, en la citada Orden Ministerial, en el artículo 2.2, se regula una definición de *ciberataque*. Se dice expresamente que *ciberataque* es una "*acción producida en el ciberespacio que compromete la disponibilidad, integridad y*

[4] Definición recogida en la Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 7 de febrero de 2013: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», nota 5 a pie de página.
http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

[5] http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan".

Además, en la Estrategia de ciberseguridad de la Unión Europea: *"Un ciberespacio abierto, protegido y seguro"*, se dice que la *ciberseguridad* abarca, por lo general, las salvaguardias y medidas que pueden utilizarse para proteger el ciberespacio, en los ámbitos tanto civil como militar, de las amenazas inherentes a sus redes interdependientes e infraestructuras de información, o que pueden dañarlas. La ciberseguridad tiene como objetivo mantener la disponibilidad e integridad de las redes e infraestructuras y la confidencialidad de la información que contienen[6].

Para finalizar, y teniendo en cuenta la información que se detalla en el presente informe, otro de los términos empleados es el de *infraestructura crítica*. Este término fue inicialmente definido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, en particular en su artículo 2. De forma adicional, la reforma de la Ley Orgánica 10/1995, del Código Penal, de 23 de noviembre por parte de la Ley Orgánica 1/2015, de 31 de marzo, define, en el artículo 264.2, 4º), a efectos penales, lo que se entiende por *infraestructura crítica*. En concreto señala que es "*un elemento, sistema o parte de éste que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.*"

[6] Definición recogida en la Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 7 de febrero de 2013: «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», nota 4 a pie de página.
http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

3.- Tendencias en materia de criminalidad y ciberseguridad

Recientemente, fue publicado el "*Informe sobre Seguridad Nacional 2014*"[7], que ha sido elaborado por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. En este documento se analizan, entre los ámbitos de la seguridad nacional, la ciberseguridad. En el capítulo dedicado a esta materia, se desarrollan cuáles serán las tendencias en materia de ciberseguridad en nuestro país, en un futuro próximo.

En primer lugar, el Informe sobre Seguridad Nacional determina que debido al uso masivo de servicios en la "nube" de Internet, las tecnologías móviles y las redes sociales, el riesgo en estas áreas se verá incrementado de forma proporcional al mismo.

De igual forma, a corto y medio plazo, el documento puntualiza que pueda darse una mayor "*explotación de las vulnerabilidades presentes en los equipos y dispositivos que componen los sistemas de control industrial de las infraestructuras críticas*".

Como medidas para reforzar las capacidades de prevención, detección, investigación y respuesta ante las ciberamenazas, se persigue adoptar una "*cultura de ciberseguridad*". Cultura basada en pilares como la concienciación, la sensibilización y la formación, extendida a todos los ámbitos de la sociedad, y que busca ahondar en la cooperación, la colaboración y la coordinación a la hora de intercambiar información entre todos los sectores involucrados (sector financiero, energético, etc.).

A nivel europeo, el Centro Europeo de Ciberdelincuencia (EC3) de Europol, ha emitido su primer "*Informe iOCTA 2014*"[8], tras su puesta en marcha el 11 de enero de 2013. El objeto prioritario de dicho organismo consiste en luchar contra la ciberdelincuencia y proteger a las empresas y a los ciudadanos europeos frente a este fenómeno.

Según el *iOCTA 2014*, a nivel mundial se estima que 2.800 millones de personas y más de 10 mil millones de dispositivos habilitados acceden a Internet. De esta forma,

[7] http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/150424_Informe%20Anual%20de%20Seguridad%20Nacional_14.pdf
[8] https://www.europol.europa.eu/iocta/2014/toc.html

lo que permite este incremento del uso de Internet son mayores oportunidades para las organizaciones criminales a la hora de delinquir. Especialmente, si se tiene presente la clara correlación existente entre el uso de las nuevas tecnologías y los flujos económicos y de comercialización online, así como empleo de sistemas de pago a través de la red.

La evidente naturaleza transnacional de la delincuencia informática, como una característica inherente de la ciberdelincuencia, se plantea como un reto importante, y genera nuevos desafíos para las Fuerzas y Cuerpos de Seguridad a la hora de hacer frente a este tipo de hechos delictivos, fundamentalmente ante la dificultad de obtener pruebas en los países de donde proceden los ciberataques.

Para el EC3, la ciberdelincuencia tiene un impacto cada vez mayor en nuestras sociedades, y aunque no existen datos fiables al respecto, la tendencia indica que también irá en aumento el número y los tipos de ataques, así como el número de víctimas y daños económicos derivados. Todo ello es debido, entre otras cosas, a que los delincuentes cibernéticos tienen la capacidad de afectar a un gran número de personas de forma simultánea mediante ataques masivos.

Son las propias características de Internet las que están siendo aprovechadas por los ciberdelincuentes, siendo, como determina el *iOCTA 2014*, el carácter anónimo que proporciona la red, el cifrado y el empleo de monedas virtuales, las más destacables.

El EC3 reconoce que todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario, denominados malware, son cada vez más sofisticados, inteligentes, versátiles, y afectan a una gama más amplia de objetivos y dispositivos.

Y por último, cabe añadir, un aspecto curioso, y es que Europol confirma que los tentáculos de la cibercriminalidad se extienden, cada vez más, entre las organizaciones criminales de corte tradicional, como son las que se dedican al tráfico de drogas y de armas, la venta de bienes robados, el fraude bancario, la falsificación de documentación, y el tráfico de los seres humanos, así como entre delincuentes cuyo objetivo es atentar contra un colectivo vulnerable, los menores de edad, mediante la comisión de hechos delictivos diversos (abusos sexuales o pornografía infantil).

4.- Infraestructuras críticas y ciberseguridad

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano competente para la dirección y coordinación de todos los asuntos relativos a la Protección de las Infraestructuras Críticas, según establece la Ley 8/2011[9] y el Real Decreto 704/2011[10].

En este contexto, y para mejorar las capacidades existentes en materia de ciberseguridad, la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información suscribieron, en 2012, un acuerdo marco de colaboración en el que, entre otros aspectos, se sientan las bases para la colaboración del CNPIC y del Instituto Nacional de Ciberseguridad (INCIBE), fundamentalmente en lo referente a la respuesta a incidentes de ciberseguridad que puedan afectar a las Infraestructuras Críticas ubicadas en España.

En particular, ambas entidades pusieron en marcha, en el año 2013, el Equipo de Respuesta a Incidentes de Seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica, denominado CERT de Seguridad e Industria (CERTSI_). De este modo, este Equipo de Respuesta se convierte en el CERT especializado en la gestión de incidentes y problemas de seguridad cibernéticos relacionados con las Infraestructuras Críticas a nivel nacional, aunque de forma general presta servicio a tres comunidades de referencia: empresas, infraestructuras críticas y Red Académica y de Investigación (RedIRIS)[11].

En este sentido, se entiende por problema de seguridad cibernético cualquier incidente que, empleando o estando dirigido a elementos tecnológicos, afecte al correcto funcionamiento de la infraestructura afectada, como por ejemplo ataques dirigidos a lograr la detención o inutilización de servicios tecnológicos, accesos no autorizados a información de carácter privado o sensible, alteración de información para manipular de forma fraudulenta los sistemas tecnológicos y la información que manejan, etc.

9 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
10 Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
11 https://www.incibe.es/extfrontinteco/img/File/actividad_2014.pdf

A continuación, se muestra un análisis de las actividades del CERTSI_, referente a aquellas actuaciones que se han ejercido para minimizar el impacto de los distintos tipos de incidentes gestionados.

INCIDENTES GESTIONADOS	
Tipo de incidente	**Total**
SPAM	1.006
Virus, troyanos, gusanos, spyware	1.745
Escaneos de red	426
Acceso no autorizado	6.785
Denegación de servicio	788
Robo de información	80
Fraude	4.274
Otros	2.781

Tabla 1: Total de incidentes gestionados 2014 (Fuente CERTSI_)

De los datos que se representan gráficamente (tabla 1), resulta de importancia resaltar los 17.885 incidentes gestionados durante el año 2014.

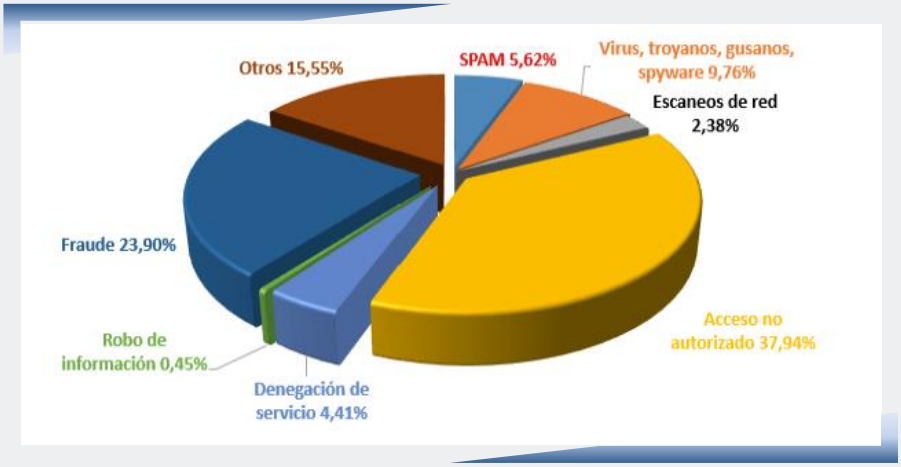

Gráfico 1: Porcentaje del total de incidentes gestionados 2014 (Fuente CERTSI_)

Asimismo, desde un análisis de los incidentes gestionados y su clasificación en función del tipo de agresión, se aprecia que las categorías de "*acceso no autorizado*" (37,94%) y "*fraude*" (23,90%) son las que aúnan mayor número de casos (gráfico 1).

Sin embargo, si se analizan, en particular, los incidentes gestionados que han afectado a las Infraestructuras Críticas (IICC), la tendencia es diferente a la anteriormente señalada.

INCIDENTES GESTIONADOS

Tipo de incidente	Total
SPAM	0
Virus, troyanos, gusanos, spyware	31
Escaneos de red	1
Acceso no autorizado	2
Denegación de servicio	2
Robo de información	9
Fraude	6
Otros	12

Tabla 2: Número de incidentes gestionados en relación a la infraestructuras críticas 2014 (Fuente CERTSI_)

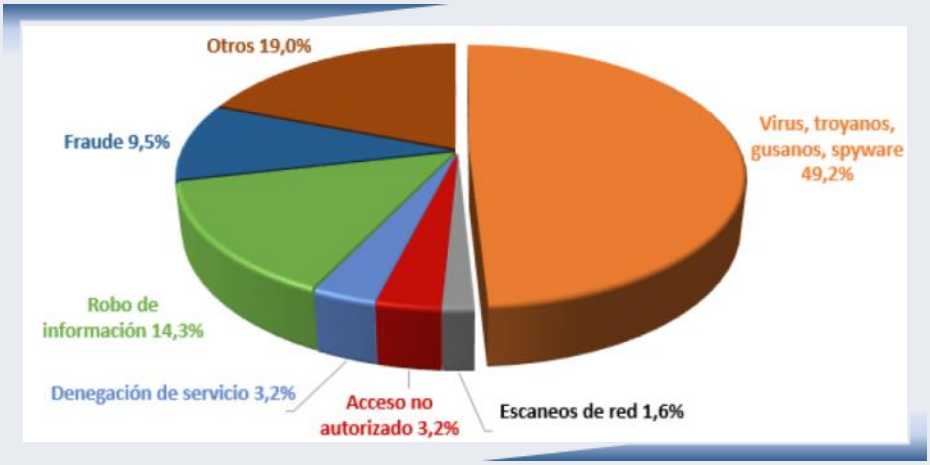

Gráfico 2: Porcentaje de incidentes gestionados en relación a las infraestructuras críticas 2014 (Fuente CERTSI_)

En relación a las IICC, se han gestionado un total de 63 incidentes (tabla 2), siendo la categoría correspondiente a los "*virus, troyanos gusanos y spyware*[12]" la más cuantiosa, alcanzando el 49,2% del conjunto de incidentes en 2014 (gráfico 2).

[12] Spyware: programas espías

Por otra parte, a continuación se detallan las cifras correspondientes a los incidentes gestionados para cada una de las comunidades de referencia a las que el CERTSI_ presta servicio (ciudadanos y empresas, Red Académica e Infraestructuras Críticas), durante el pasado año.

Incidentes por público objetivo	Total
Ciudadanos y empresas	14.715
Red Académica (RedIris)	3.107
Infraestructuras Críticas (IICC)	63

Tabla 3: Número de incidentes gestionados por comunidad de referencia 2014 (Fuente CERTSI_)

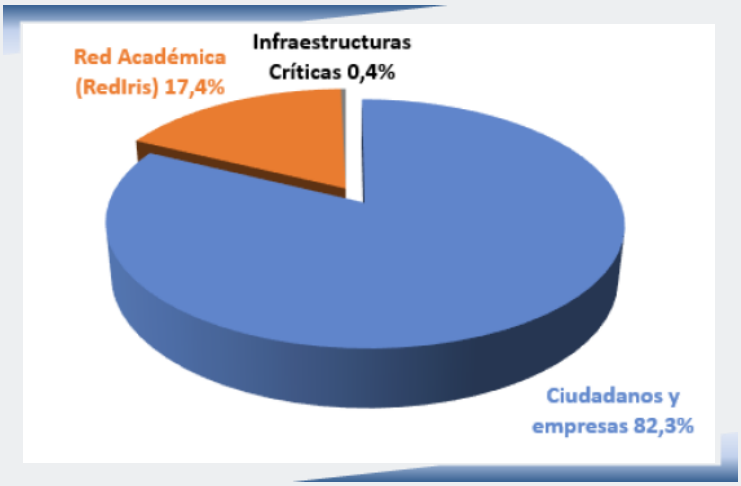

Gráfico 3: Porcentaje de incidentes gestionados por comunidad de referencia 2014 (Fuente CERTSI_)

Como puede apreciarse de los resultados expuestos sobre incidentes gestionados en función de la comunidad de referencia a la que se ha asistido, las cifras denotan que la mayoría de los incidentes lo ha sufrido la comunidad denominada "*ciudadanos y empresas*", con un 82,3% del total (tabla y gráfico 3).

La información que concierne al número de incidentes gestionados por área diferenciada de protección de las Infraestructuras Críticas (IICC), establece que el sector de la "*energía*" (54,0%) y el de los "*transportes*" (22,2%) son los más afectados durante 2014. Entre los dos grupos aglutinan más del 75% de todos los incidentes gestionados (tabla y gráfico 4).

Sector estratégico	Total
Administración	2
Espacio	0
Industria nuclear	4
Industria química	0
Instalaciones de investigación	0
Agua	0
Energía	34
Salud	0
Tecnologías de la Información y las Comunicaciones (TIC)	6
Transporte	14
Alimentación	0
Sistema financiero y tributario	3

Tabla 4: Número de incidentes gestionados por sector estratégico 2014 (Infraestructuras críticas) (Fuente CERTSI_)

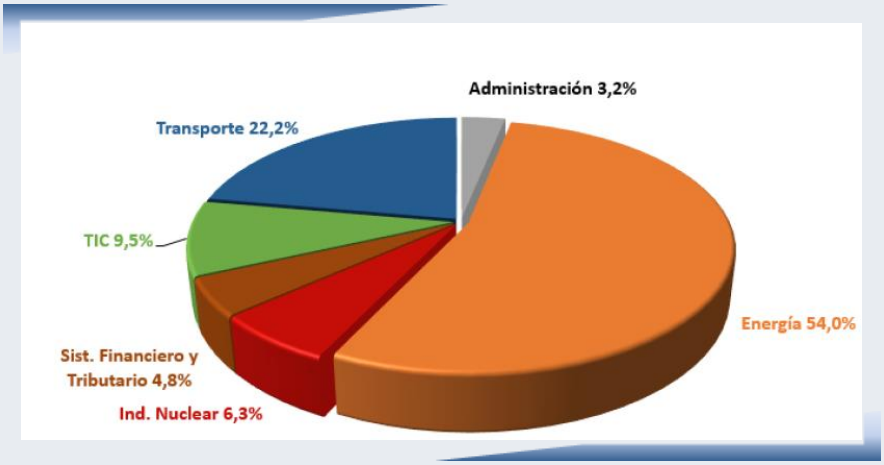

Gráfico 4: Porcentaje de incidentes gestionados por sector estratégico 2014 (Infraestructuras críticas) (Fuente CERTSI_)

Por último, respecto al ámbito de la colaboración público-privada, durante el año 2014, distintas empresas estratégicas, correspondientes a los sectores de la energía, del sistema financiero y tributario, del agua, de las tecnologías de la información y las comunicaciones (TIC) y del transporte han firmado un total de 12 acuerdos de confidencialidad, con el INCIBE y con el CNPIC. La existencia de estos acuerdos es lo que garantiza que el servicio que se presta en materia de detección y respuesta a incidentes desde el CERTSI_ cumple con los requisitos adecuados de seguridad en el intercambio de información entre las partes.

COMUNIDAD DE PRESTACIÓN DE SERVICIOS A EMPRESAS ESTRATÉGICAS

En 2014 las empresas estratégicas han firmado 12 acuerdos de confidencialidad entre éstas, INCIBE y CNPIC por los cuales se les ha conmenzado a prestar a los operadores estratégicos nacionales un canal de respuesta a incidentes cibernéticos

Sector estratégico	Acumulado 2014*
Administración	0
Espacio	0
Industria nuclear	0
Industria química	0
Instalaciones de investigación	0
Agua	2
Energía	5
Salud	0
Tecnologías de la Información y las Comunicaciones (TIC)	1
Transporte	1
Alimentación	0
Sistema financiero y tributario	3

*** en 2013 se pusieron en marcha 18 acuerdos de confidencialidad**

Tabla 5: Empresas que firmaron acuerdo de confidencialidad entre INCIBE y CNPIC, 2014

5.- Los nuevos delitos tecnológicos en la Ley Orgánica 1/2015 de reforma del Código Penal

La variedad de los delitos informáticos y la diversidad de comportamientos constitutivos de esta clase de ilícitos es cada vez mayor. El fenómeno de la cibercriminalidad ha ido evolucionando con la propia sociedad y los cambios sufridos, surgiendo modalidades comisivas caracterizadas cada vez más por su complejidad. Estas formas delictivas han ido adquiriendo la suficiente entidad y gravedad como para constituir ataques serios a intereses jurídicamente protegidos de carácter tradicional, como a otros intereses novedosos y que en la actualidad no poseen una protección específica. Por ello, la necesidad de contrarrestarlas mediante la intervención del derecho penal. Sin duda, los nuevos supuestos de comisión delictiva que engloban a la ciberdelincuencia son fruto de la Sociedad Global.

De esta forma, la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal por parte de la Ley Orgánica 1/2015 regula nuevos tipos penales en este ámbito. La finalidad de esta actualización es la regulación de nuevas tipologías delictivas que traten de responder a la realidad delictual existente en nuestro país.

Esta modificación del Código Penal, viene a completar nuestro ordenamiento jurídico. Hasta el momento, el legislador español había traspuesto a nuestro código las conductas ilícitas reguladas por el Convenio sobre cibercriminalidad o Convenio de Budapest. El primer tratado internacional que buscó hacer frente a los delitos informáticos y los delitos en Internet, y que España ratificó el 1 de octubre de 2010. La clasificación de las conductas que realiza el Convenio se introducen en el *I Informe de Cibercriminalidad (2013)*, elaborado por el Ministerio del Interior[13].

No obstante, además de las conductas que introduce el Convenio de Budapest, nuestra realidad criminalidad denota que existen otras categorías distintas que conviene reseñar, y que se añaden a los datos que recoge este informe. 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 conductas delictivas, teniendo en cuenta, el volumen y la importancia de la

[13] http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

cifra registrada:

- Delitos contra el honor.
- Amenazas y coacciones.
- Delitos contra la salud pública.

La necesidad de incorporar los nuevos delitos informáticos en nuestro Código Penal a través de la reforma de Ley Orgánica 1/2015, viene dada por la adopción de la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo.

Los cambios sufridos tratan de dar una respuesta legal, desde la perspectiva del derecho penal, a la delincuencia informática. En este sentido, los delitos contra los sistemas de información introducidos y modificados por la Ley Orgánica 1/2015, son los que a continuación detallan:

- El delito de acoso electrónico. Artículo 172 ter CP
- Delitos de descubrimiento y revelación de secretos. Artículos 197 a 197 quinquies CP
- Delitos de daños y delitos de interferencia ilegal en sistemas de información o datos. Artículos 264 a 264 quáter CP
- Delitos contra la propiedad intelectual. Artículo 270 CP
- Abusos con fines sexuales cometidos a través de Internet u otros medios de telecomunicación a menores. Artículo 183 ter CP

El delito de acoso electrónico del artículo 172 ter CP, dentro del capítulo "*de las coacciones*", establece que:

> *"1. Será castigado (…) el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*
> *1. La vigile, la persiga o busque su cercanía física.*
> *2. Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.*
> *3. Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.*

4. Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella".

A los delitos de descubrimiento y revelación de secretos existentes (Arts. 197 a 197 quinquies CP), se incorporan nuevas conductas delictivas, y entre ellas se encuentra el Artículo 197 bis, apartado 2, que dice textualmente:

"*El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses*". De esta forma, serán objeto de castigo no únicamente la interceptación de comunicaciones personales, recogidas ya en el CP, sino que a la vez, todas las que se produzcan entre sistemas o equipos.

Además, el artículo 197 ter CP considera que serán castigados todos aquellos que:

"*sin estar debidamente autorizados, produzcan, adquieran para su uso, importen o, de cualquier modo, faciliten a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:*
a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
b) Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

Dentro de este mismo capítulo, se añade el artículo 197 quater CP relativo al denominado "espionaje informático" cuando es cometido en el "*seno de una organización o grupo criminal*". En este supuesto, "*se aplicarán respectivamente las penas superiores en grado*". Además, el artículo 197 quinquies CP contempla la responsabilidad de las personas jurídicas en este ámbito.

En relación a los artículos 264 a 264 quáter CP, el legislador establece una división entre los delitos de daños informáticos (sabotaje informático) y las interferencias en los sistemas de información. Los delitos de daños informáticos tendrán lugar cuando se: "*borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos*".

La reforma dispone una elevación de las penas para esta tipología penal.

Además, se prevé una agravación en la comisión de la figura típica descrita cuando:

> "1. *Se hubiese cometido en el marco de una organización criminal.*
> *2. Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.*
>
> *3. El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.*
> *4. Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones."*

El artículo 264 bis CP reconoce de forma diferenciada el delito de interferencia ilegal en sistemas de información o datos, consistente en la interrupción u obstaculización de sistemas informáticos en su conjunto a través de la manipulación de sus datos informáticos.

Los delitos contra la propiedad intelectual, recogidos en el artículo 270 CP, son objeto de una reforma considerable. Estos delitos se ven una vez más modificados para adecuar a la realidad social la respuesta y protección jurídico penal. Una respuesta que dependerá de la gravedad de la infracción penal. De ahí, que la penalidad del supuesto regulado en el artículo 270.4 CP sea menor. Este apartado cuarto recoge la venta ambulante, y dice expresamente lo siguiente:

> "*en los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.*
> *No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días*".

El artículo 270 CP, en su apartado primero, establece que el que "*con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca,*

plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios".

En este sentido, se introduce la explotación económica por cualquier "*otro modo*" de una obra o prestación protegida. Asimismo, se sustituye el elemento subjetivo del tipo, ánimo de lucro por "*el ánimo de obtener un beneficio económico directo o indirecto*", siendo mucho más amplio al añadir el lucro indirecto.

En el apartado 2 del artículo 270 CP se contempla que a quien "*en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".*

Tiene que constituir una conducta activa, es decir, "no neutral". En este sentido, se hace especial referencia al caso de los buscadores.

En último lugar, cabe mencionar que la protección de los menores frente a los abusos con fines sexuales cometidos a través de Internet u otros medios de telecomunicación, debido a la facilidad de acceso y el anonimato que proporcionan. De esta forma, la reforma añade el artículo 183 ter al nuevo texto del CP, que dice lo siguiente:

> "1. *El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento (...).*
> *2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, (...)".*

Con esta reforma, se eleva la edad del menor con el que se contacte, de 13 a 16 años. La edad de los 13 años es la que figuraba y establecía el anterior artículo 183 del CP. Se persigue fortalecer la protección penal para los menores de 16 años de edad, partiendo de que tal edad es la que se fija en nuestro ordenamiento para tener capacidad de consentimiento sexual tras la modificación del Código Penal.

Es pues que, se sanciona al que a través de medios tecnológicos contacte con un menor de quince años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas.

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 Sistemas Estadístico de Criminalidad (SEC).

6.- Datos estadísticos sobre el uso de las nuevas tecnologías

Los datos incorporados a este *II Informe sobre Cibercriminalidad* tratan de dibujar las amenazas que presenta la ciberdelincuencia actual en nuestro país. De ahí, el interés de mostrar datos que referencian el uso de las tecnologías por parte de la sociedad en general, teniendo en cuenta los resultados obtenidos por otros entes públicos, tanto nacionales (INE, Ministerio del Interior, ONTSI, etc.) como europeos (EUROSTAT), que recopilan información relativa a esta materia, a través de estudios y de encuestas de opinión realizadas.

En el ámbito nacional, el Instituto Nacional de Estadística (INE) ha publicado datos de evolución, desde el año 2006 hasta 2014, en relación con el número 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, desglosados por sexos y grupos de edades.

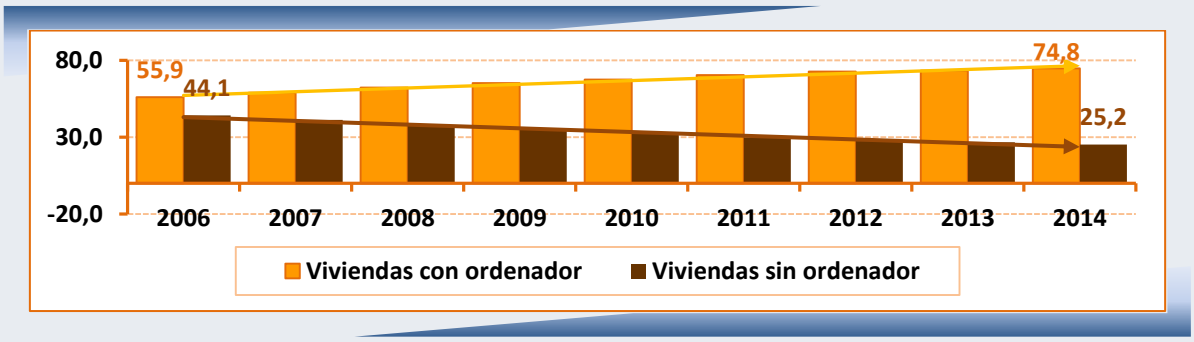

Gráfico 5: Viviendas con o sin ordenador 2006-2014(Fuente INE)

Analizando el primer gráfico puede comprobarse que, lógicamente, el número de viviendas con ordenador ha ido aumentando progresivamente de año en año hasta llegar a un 74,8% en el pasado 2014.

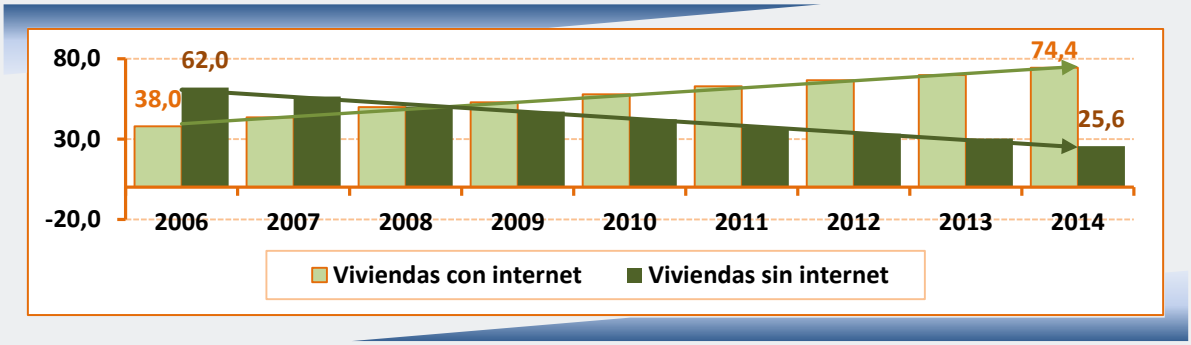

Gráfico 6: Viviendas con o sin acceso a Internet 2006-2014 (Fuente INE)

Si comparamos los datos del gráfico 5 con el porcentaje de viviendas que poseen un servicio de acceso a Internet (gráfico 6), se puede observar que en el año 2006 menos de dos tercios de los ordenadores domésticos estaban conectados a Internet. No obstante, en 2014, casi el 75% de los mismos están conectados a la red. La progresión ascendente es proporcional al incremento de las viviendas que han ido adquiriendo estos dispositivos (ordenadores).

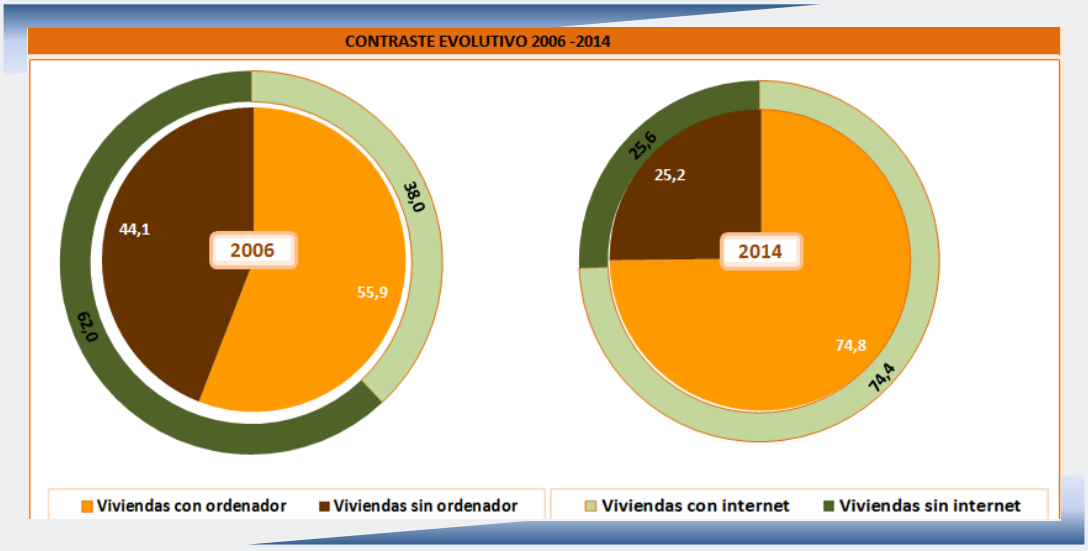

Gráfico 7: Comparativa de viviendas con o sin ordenador y acceso a Internet 2006 y 2014 (Fuente INE)

En el anterior gráfico (7), se relacionan el uso del ordenador e Internet en los hogares españoles en los extremos temporales de la serie histórica relatada en el estudio, 2006 a 2014.

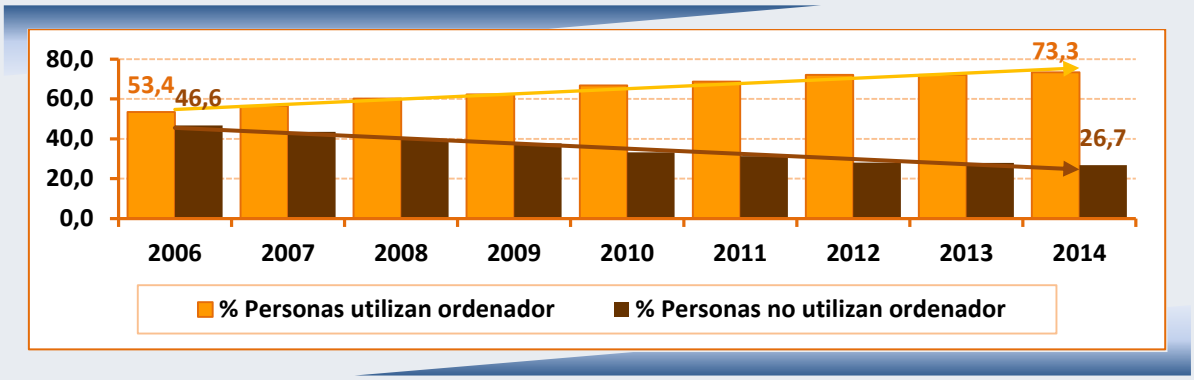

Gráfico 8: Porcentaje de personas que utilizan o no ordenador 2006-2014 (Fuente INE)

Basándonos igualmente en los datos publicados por el INE, se aprecia que el número de personas que afirman haber utilizado un ordenador (gráfico 8) en los últimos tres meses ha evolucionado de una manera idéntica al de número de viviendas con ordenador. El pasado año, el 73,3% de la población afirman haber utilizado algún ordenador en el último trimestre.

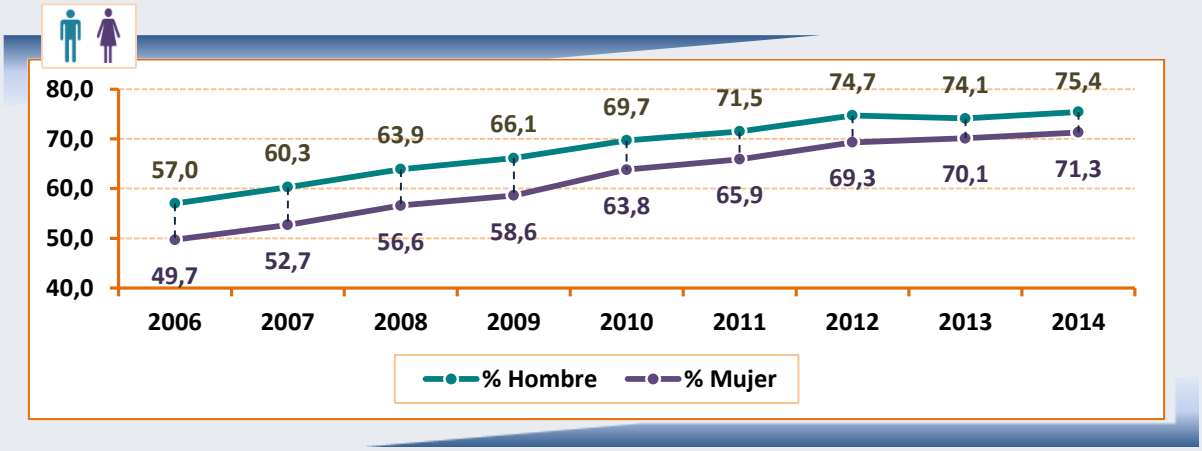

Gráfico 9: Porcentaje de personas que utilizan o no ordenador por sexo 2006-2014 (Fuente INE)

Si analizamos los datos del gráfico 9, es decir el porcentaje de personas que utilizan el ordenador, desglosados por sexos, se aprecia una evolución, un incremento de dicho uso en los últimos años. De esta forma, la utilización de ordenadores por parte del sexo masculino, en el año 2006, se encontraban 7,3 puntos porcentuales por encima de las mujeres. En 2014 aunque los datos se han igualado más, todavía los hombres están 4,1 puntos porcentuales por encima. Parece que, tal y como reflejan las gráficas, éstas tienden a converger en un futuro próximo.

	PORCENTAJE POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES								
	2006	2007	2008	2009	2010	2011	2012	2013	2014
Edad: De 16 a 24 años	**85,1**	88,3	92,4	92,9	94,6	95,1	97,3	96,1	**94,7**
Edad: De 25 a 34 años	**70,9**	76,5	80,7	81,8	85,9	88,0	89,2	90,2	**88,9**
Edad: De 35 a 44 años	**62,2**	63,8	68,8	70,9	77,6	80,2	85,2	84,3	**85,6**
Edad: De 45 a 54 años	**47,5**	51,7	55,2	58,2	64,5	67,7	71,5	72,4	**76,2**
Edad: De 55 a 64 años	**23,3**	25,9	28,7	33,2	38,5	41,5	47,1	49,3	**54,2**
Edad: De 65 a 74 años	**7,5**	7,7	10,0	13,3	15,8	17,4	21,4	23,4	**25,8**

Tabla 6: Personas que utilizan o no ordenador por edad 2006-2014 (Fuente INE)

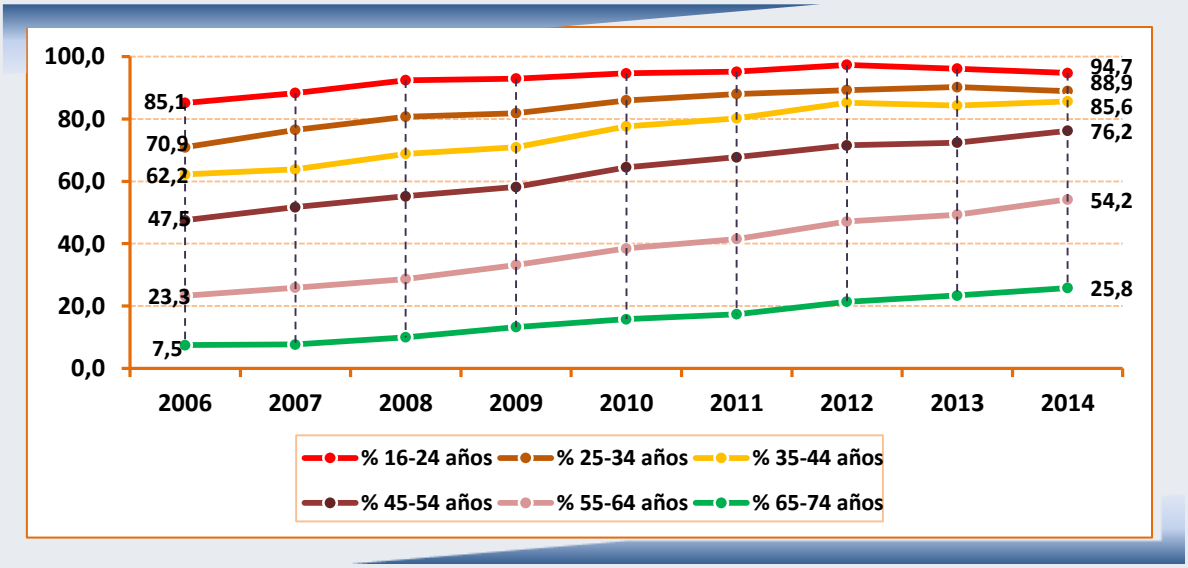

Gráfico 10: Personas que utilizan o no ordenador por edad 2006-2014 (Fuente INE)

En el desglose de la información que facilita el INE por edades (tabla 6, gráfico 10), se detecta que, lógicamente, los grupos de edad más jóvenes son los que más utilizan los ordenadores. Destaca que el 94,7% de los jóvenes, entre 16 a 24 años, afirman haber utilizado el ordenador en los últimos tres meses, porcentaje que se reduce a un 25,8% entre las personas con edades de 65 a 74 años.

En relación al resultado que recoge el porcentaje de personas comprendidas entre los 65 y 74 años que hacen uso del ordenador, es importante detallar el hecho de que en 2006 la cifra ascendía tan sólo a un 7,5%, mientras que el pasado año, este dato era de un 25,8%. Por lo tanto, se puede decir que la evolución experimentada en estos años es significativa.

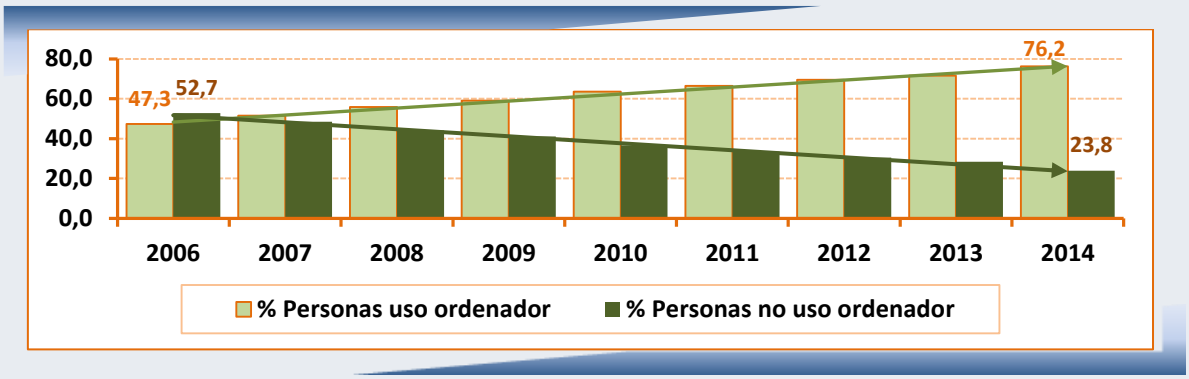

Gráfico 11: Personas que utilizan o no Internet2006-2014 (Fuente INE)

Por otra parte, si cotejamos el porcentaje de personas (gráfico 11) que han utilizado un ordenador en los últimos tres meses con el de personas que han accedido a Internet, observamos que este último es ligeramente superior: 75,4% frente al 76,2%. Sin duda, este hecho es debido a la posibilidad de acceder a la red desde dispositivos móviles y otros (Smartphones, tablets, etc.), y en cualquier lugar.

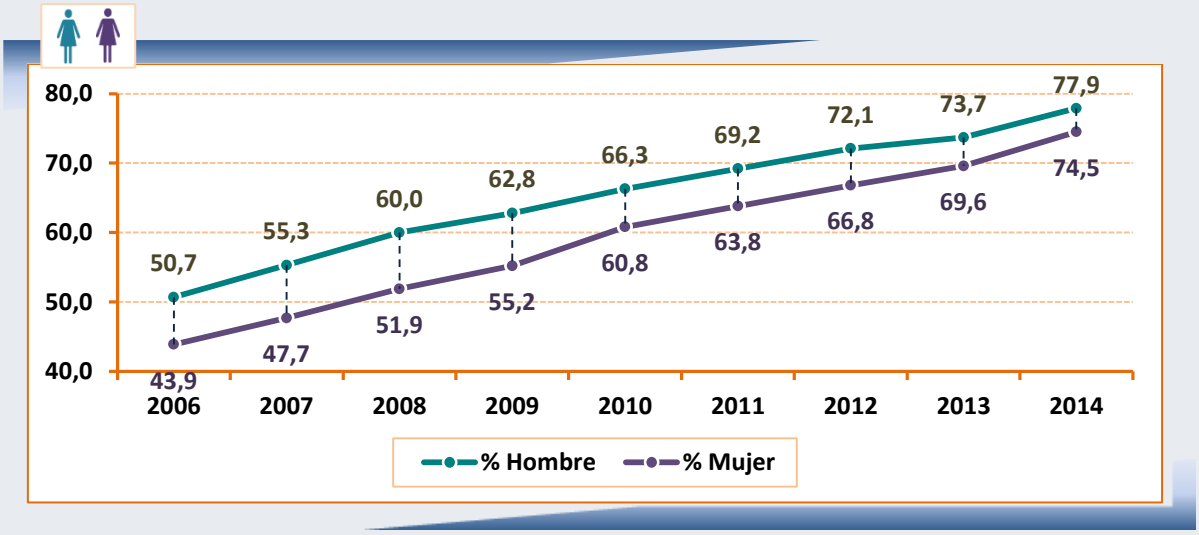

Gráfico 12: Personas que utilizan o no a Internet, por sexo 2006-2014 (Fuente INE)

El desglose de los datos por sexos (gráfico 12) nos da unos resultados completamente análogos al de uso de ordenadores. Si comprobábamos que los hombres superaban a las mujeres en 4,1% puntos porcentuales en 2014 en utilización de ordenadores, esta cifra se transforma en 3,4% puntos porcentuales cuando nos referimos a datos de acceso a la red.

	PORCENTAJE POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES								
	2006	2007	2008	2009	2010	2011	2012	2013	2014
Edad: De 16 a 24 años	**81,3**	85,2	89,4	91,5	93,3	94,6	95,8	97,4	**98,3**
Edad: De 25 a 34 años	**65,1**	71,3	76,9	78,6	83,6	86,3	87,7	92,1	**93,7**
Edad: De 35 a 44 años	**53,3**	56,2	62,1	66,8	73,5	77,7	83,0	83,7	**89,8**
Edad: De 45 a 54 años	**39,6**	45,6	50,1	54,0	59,6	64,6	67,4	71,2	**78,2**
Edad: De 55 a 64 años	**18,1**	21,5	24,6	29,3	34,6	37,9	43,8	46,5	**55,4**
Edad: De 65 a 74 años	**5,1**	6,6	8,6	11,2	13,8	16,2	19,0	21,9	**26,2**

Tabla 7: Personas que utilizan o no a Internet, por edad 2006-2014 (Fuente INE)

Igualmente, la cifra de personas que acceden a Internet (tabla 7), según grupos de edad, nos muestra resultados similares al de utilización de los equipos informáticos. Se puede apreciar que los más jóvenes son los que acceden en mayor medida a la red. En concreto, el porcentaje del grupo de edad comprendido entre 16 a 24 años alcanza un 98,3 %.

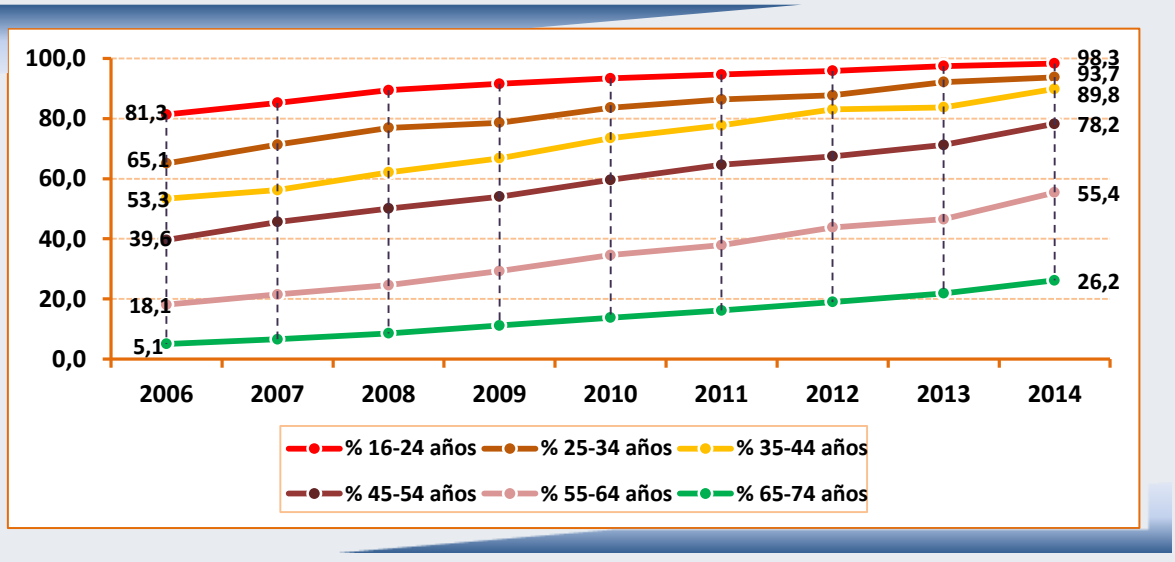

Gráfico 13: Personas utilizan o no a Internet, por sexo 2006-2014 (Fuente INE)

En relación al grupo de edad de 65 a 74 años, la evolución también ha sido relevante en los últimos años. Mientras que en el año 2006 solamente un 5,1% decía haber utilizado Internet, este porcentaje subía hasta el 26,2% en 2014.

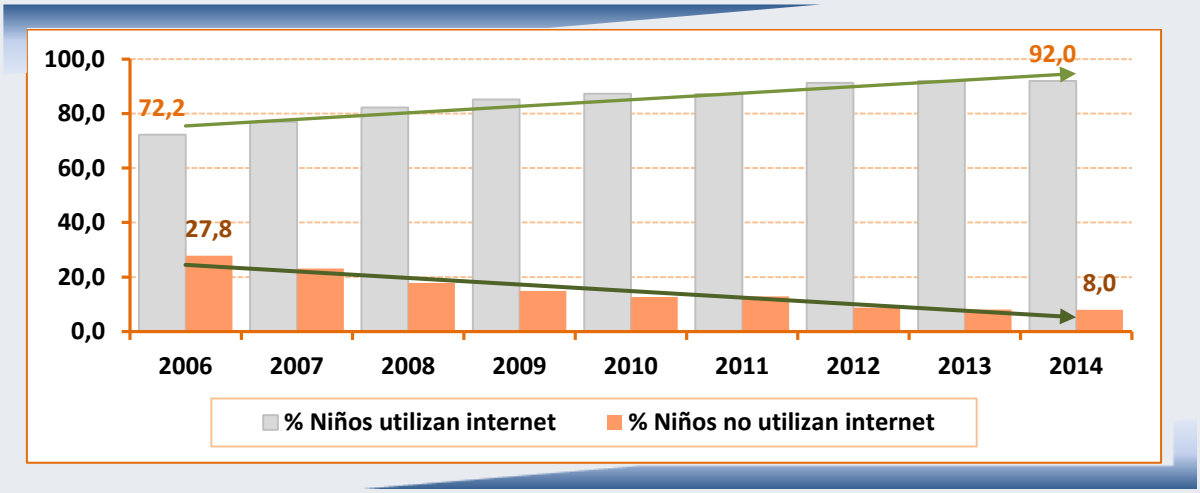

Gráfico 14: Porcentaje de niños que han utilizado o no Internet 2006-2014 (Fuente INE)

Si en las personas mayores el porcentaje de ellas que accede a Internet es mayor que el de las que utilizan el ordenador, en el caso de los niños es al contrario. En 2014, el 93,8% de los niños afirmaron haber utilizado un ordenador en los últimos tres meses, cifra que solo alcanzaba el 92,0% cuando se hace referencia al acceso a Internet, en el mismo periodo de tiempo.

La razón parece deberse al control que se ejerce sobre los menores por parte de sus padres o tutores, como demuestra la "*Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España*" realizada por el Ministerio del Interior en 2014[14].

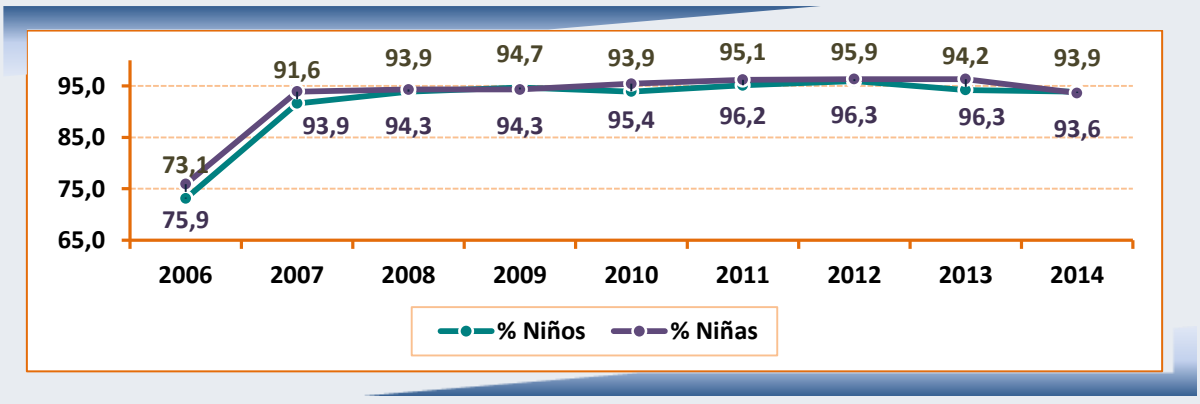

Gráfico 15: Porcentaje de niños que han utilizado el ordenador último trimestre, por sexo 2006-2014 (Fuente INE)

14

http://www.interior.gob.es/documents/10180/2563633/Encuesta+sobre+h%C3%A1bitos+de+uso+y+seguridad+de+internet+de+menores+y+j%C3%B3venes+en+Espa%C3%B1a/b88a590a-514d-49a2-9162-f58b7e2cb354
http://www.interior.gob.es/web/interior/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2735634

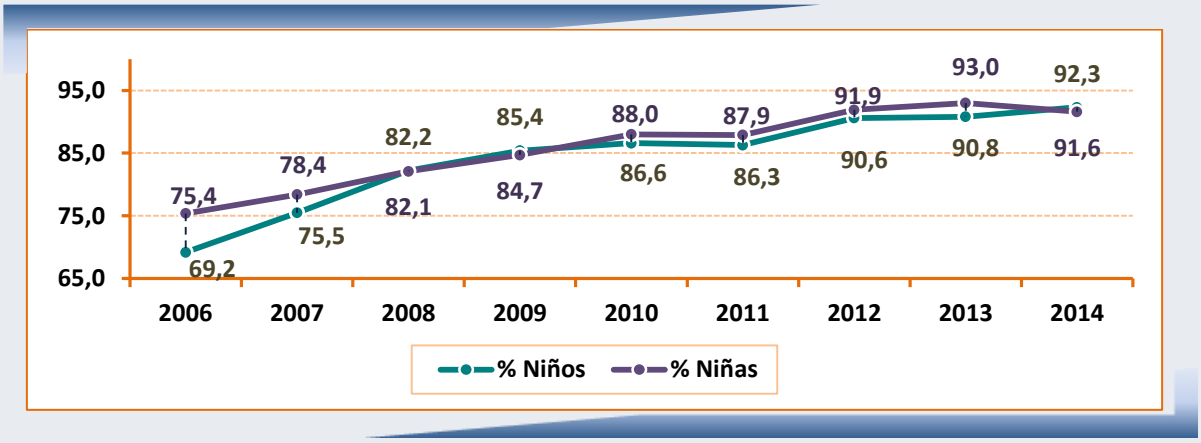

Gráfico 16: Porcentaje de niños de niños que han utilizado o no Internet, por sexo 2006-2014 (Fuente INE)

La distribución por sexos, tanto del porcentaje de niños que han accedido a Internet como de los que han sido usuarios del ordenador en los últimos tres meses (gráfico 15 y 16), muestra que ambos, niños y niñas, lo hacen en niveles similares, lo que parece indicar que la brecha tecnológica desaparecerá de forma paulatina.

Por último, se exponen a continuación, en relación a los resultados obtenidos en la "*Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España"* realizada por el Ministerio del Interior en el año 2014[15], varias conclusiones en relación a esta materia, entre ellas,:

- Los padres confían en el uso que sus hijos hacen de Internet. Si bien, aunque más de la mitad de los progenitores autoriza a los menores a usar Messenger, Whatsapp y a navegar o ver contenidos audiovisuales por Internet en cualquier momento, sin mediar supervisión alguna, casi ninguno permite que sus hijos realicen compras por Internet (menos del 15%).

- Por otra parte, sólo la mitad de los padres, un 54%, habla con sus hijos/as sobre las posibles consecuencias negativas derivadas de visitar páginas inadecuadas en Internet. Sin embargo, un porcentaje mayor, un 62%, comprueba las páginas visitadas por sus hijos/as.

- Además, la encuesta determina que poco más de un tercio de los padres comprueba el perfil que tiene su hijo en las redes sociales, qué amigos añade a

15

http://www.interior.gob.es/documents/10180/2563633/Encuesta+sobre+h%C3%A1bitos+de+uso+y+seguridad+de+internet+de+menores+y+j%C3%B3venes+en+Espa%C3%B1a/b88a590a-514d-49a2-9162-f58b7e2cb354
http://www.interior.gob.es/web/interior/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2735634

su red social o qué grupos de Whatsapp y Messenger posee. Una cuestión que resulta curiosa ante el hecho de que lo que más preocupa a los progenitores es que sus hijos puedan ser contactados por extraños en Internet y que se puedan cometer delitos contra ellos en la red.

- A pesar de la preocupación mencionada, la medida de seguridad más extendida es la instalación de un software para prevenir virus o spams, obviando controles parentales u otro tipo de software para bloquear o realizar un seguimiento de páginas web de contenido inadecuado.

- Entre una de las grandes preocupaciones de los padres españoles se encuentran los contenidos violentos o inapropiados en la red para los menores. Un 15% de los progenitores afirman que sus hijos han visto algo por internet que les ha disgustado o molestado en los últimos 12 meses.
  A pesar, de conocer esta circunstancia, sólo un 20% de los padres han cambiado mucho sus hábitos después del incidente, y un 24% algo. Por ello, un 56% del total no ha tomado ninguna medida al respecto.

- Casi un 60% de los menores entrevistados usa Internet a diario, y la frecuencia de uso más habitual es "entre una y dos horas".

- La frecuencia de uso de Internet aumenta con la edad. De esta forma, en el caso de los mayores de 15 años, el porcentaje de los que utiliza Internet todos los días se eleva hasta el 83%.

- Además, y dentro del grupo de niños mayores de 15 años, el uso de redes sociales y email se sitúa por encima del 90%.

- Asimismo, dos de cada tres menores sube fotos, ve vídeos y comparte música a través de Internet. En este caso, el porcentaje alcanza un 80% en el caso de los niños mayores de 15 años, y un 35% en el caso de los menores de 12 años.

- Dos de cada tres menores tiene perfil en las redes sociales, y de ellos un tercio tiene incluso más de uno.

- Por último, cabe mencionar que de los resultados de la encuesta se observa que un tercio de los contactos que tienen los menores por Internet tienen lugar con personas desconocidas. Llegando casi a la mitad, cuando se trata de los mayores de 12 años (42%).

A nivel europeo, los datos publicados por EUROSTAT nos permiten realizar un análisis comparativo de los datos de nuestro país con otros estados miembros de la Unión Europea.

Gráfico 18: Personas acceden o no a Internet. Países UE (Fuente EUROSTAT)

La gráfica 18 relaciona los países de la UE (15) en orden en función del mayor o menor porcentaje de acceso a Internet en los últimos tres meses. Este diagrama muestra resultados análogos al anterior. En este sentido, Dinamarca continúa siendo el país que más accede a la red con un porcentaje del 96%, e Italia el que menos con un 62%. España queda por debajo de la media europea, con un 76% (la media de la UE (15) es del 81%).

Las conclusiones que se extraen del análisis gráfico efectuado, son las que a continuación se detallan:

- Cada vez más personas afirman utilizar con habitualidad ordenadores.
- Cada vez más personas afirman acceder de una manera frecuente a Internet.
- Hombres y mujeres utilizan ordenadores y acceden a la red casi en la misma medida, superando todavía los hombres ligeramente la cifra de las mujeres.

- A pesar de que los grupos de edad más jóvenes son los que más usan los ordenadores y acceden a la red, es el grupo de las personas de edad más elevada (65 a 74 años) el que más crece en términos porcentuales con respecto a este tema.
- España crece cada año en cultura digital, si bien permanece por debajo de los porcentajes medios de la UE (15).

Por otra parte, el pasado febrero fue publicado el EUROBARÓMETRO[16] Especial 423, relativo a la ciberseguridad. En él se tratan diferentes cuestiones, entre ellas, las siguientes:

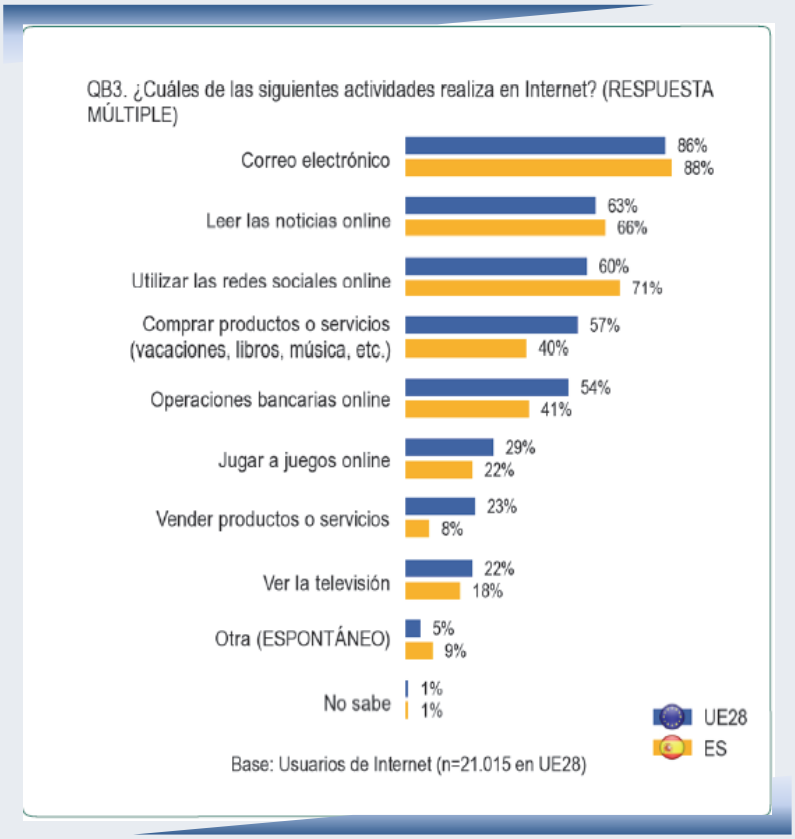

Gráfico 19: Actividades en Internet. Países UE (Fuente EUROBARÓMETRO 423, 2015)

[16] http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

Por lo que se refiere a las actividades que más se realizan a través de Internet por parte de los usuarios españoles (gráfico 19), éstas tienden a coincidir con las que efectúan los usuarios del resto de países de la UE (28). No obstante, cuando el empleo de Internet está enfocado a enviar correos electrónicos, a leer las noticias online o a utilizar las redes sociales los porcentajes nuestro país se encuentra por encima de la media europea. Esto mismo no ocurre, cuando se trata de efectuar operaciones bancarias online o comprar productos o servicios (comercio electrónico).

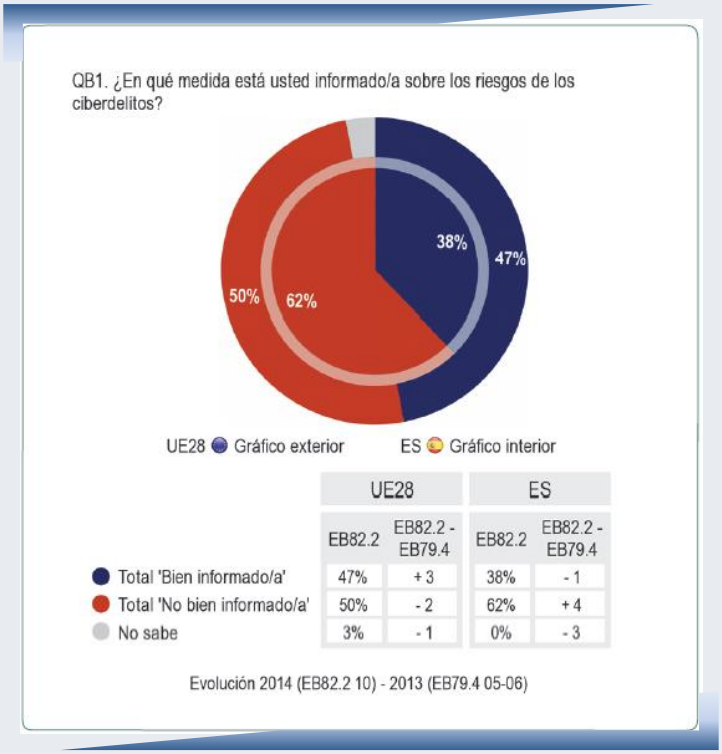

Gráfico 20: Información sobre riesgos de los ciberdelitos. Países UE (Fuente EUROBARÓMETRO 423 2015)

Asimismo, según el EUROBARÓMETRO de febrero de 2015, los españoles se sienten menos informados sobre los riesgos que comportan los ciberdelitos que la media europea (UE 28).

Gráfico 21: Medidas de seguridad ante la utilización de Internet. Países UE (Fuente EUROBARÓMETRO 423 2015)

Las medidas de seguridad más adoptadas por los usuarios españoles al utilizar Internet, al igual que la media europea, son la instalación de un software antivirus así como no acceder a correos electrónicos de remitentes desconocidos (gráfico 21).

7.- Datos estadísticos de Cibercriminalidad: Sistema Estadístico de Criminalidad (SEC)

Por segundo año consecutivo, y tomando como referencia los datos registrados 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 relativos a la cibercriminalidad, el Ministerio del Interior ha elaborado un segundo estudio sobre la esta materia.

Datos globales

En primer lugar, en este apartado se detallan las conductas ilícitas registradas en el SEC, siguiendo la clasificación adoptada por el Convenio sobre cibercriminalidad o Convenio de Budapest.

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.
- Delitos contra la salud pública.

HECHOS CONOCIDOS	2011	2012	2013	2014
ACCESO E INTERCEPTACIÓN ILÍCITA	1.492	1.701	1.805	1.851
AMENAZAS Y COACCIONES	9.839	9.207	9.064	9.559
CONTRA EL HONOR	1.941	1.891	1.963	2.212
CONTRA PROPIEDAD INDUST./INTELEC.	222	144	172	183
DELITOS CONTRA LA SALUD PÚBLICA	46	43	34	31
DELITOS SEXUALES	755	715	768	974
FALSIFICACIÓN INFORMÁTICA	1.860	1.625	1.608	1.874
FRAUDE INFORMÁTICO	21.075	27.231	26.664	32.842
INTERFERENCIA DATOS Y EN SISTEMA	228	298	359	440
Total HECHOS CONOCIDOS	**37.458**	**42.855**	**42.437**	**49.966**

Tabla 8: Total de hechos conocido por categorías Fuerzas y Cuerpos de Seguridad 2011-2014 (Fuente SEC)

En la tabla 8, se relacionan las cifras totales de las infracciones penales conocidas por las Fuerzas y Cuerpos de Seguridad, durante el periodo comprendido entre 2011 y 2014.

Como puede apreciarse, se ha producido un incremento del 33,39 % en dicho espacio temporal. De esta forma, en la serie histórica referenciada se observa que los fraudes informáticos, la tipología delictiva conocida que aglutina un mayor número de hechos, han ido creciendo año a año. Además, las categorías correspondiente a las amenazas y coacciones y contra el honor se han mantenido con una tendencia estable a lo largo de los años objeto de estudio.

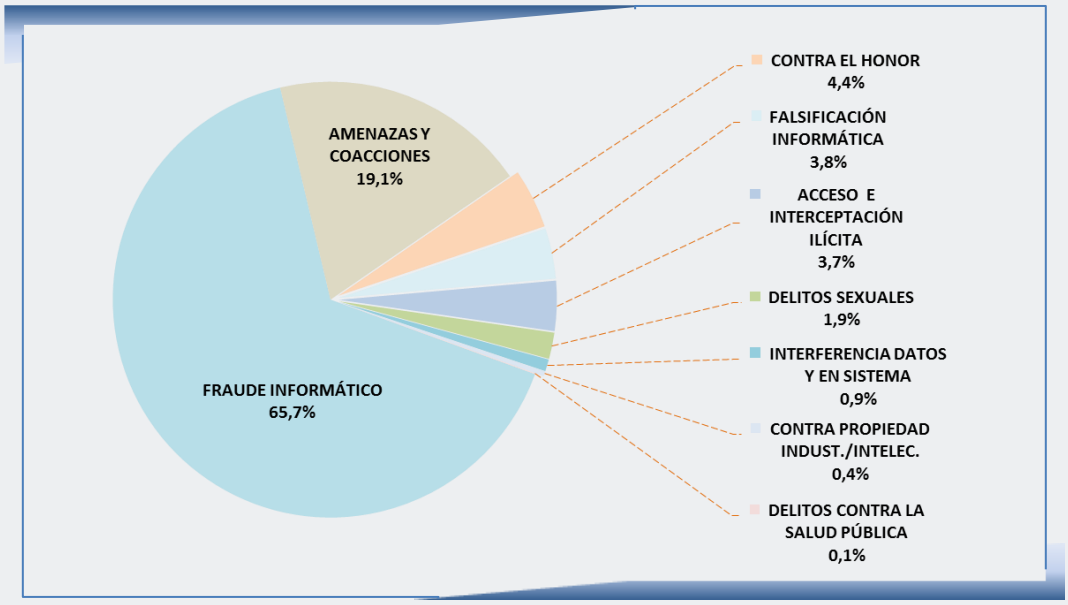

Gráfico 22: Porcentaje de hechos conocido por categorías Fuerzas y Cuerpos de Seguridad 2014 (Fuente SEC)

En el gráfico anterior (22), se detallan los porcentajes de los hechos conocidos, según las categorías más comunes, por las Fuerzas y Cuerpos de Seguridad.

Analizando este diagrama de datos, se puede apreciar que la categoría delictiva que ha registrado mayor incidencia durante 2014, ha sido el fraude informático, con un 65,7% del total de hechos conocidos. A continuación, le siguen las amenazas y las coacciones. Las demás tipologías delictivas registradas presentan menos ocurrencia si las comparamos con las dos principales. Entre ellas, se encuentran, según orden de importancia, los delitos contra el honor, la falsificación informática, el acceso e interceptación ilícita y los delitos sexuales.

En estas gráficas (23) se muestra la información anotada por las Fuerzas y Cuerpos de Seguridad en relación a los hechos conocidos, esclarecidos y la cifra de las detenciones e imputaciones efectuadas.

Gráfico 23: Hechos conocidos, esclarecidos y detenciones e imputaciones 2012-2014 (Fuente SEC)

El porcentaje de hechos esclarecidos alcanza la cifra de un 35,9% de los hechos conocidos en 2014, incrementándose año a año. Por otra parte, la cifra de detenidos e imputados en este ámbito es menor, manteniéndose de forma casi constante a lo largo de los últimos años. Si bien, con respecto a este último punto, se puede detectar que en 2014 ha experimentado un pequeño incremento.

Perfil de la VÍCTIMA: grupo penal, sexo y edad

A continuación, se establece un perfil de la víctima de los ciberdelitos, en nuestro país. Perfil, que se basa en la información estadística proveniente de la delincuencia conocida y facilitada por las Fuerzas y Cuerpos de Seguridad, que figura en el Sistema Estadístico de Criminalidad (SEC).

VICTIMIZACIONES	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	721	1.002	1.723
AMENAZAS Y COACCIONES	5.490	4.836	10.326
CONTRA EL HONOR	1.075	1.330	2.405
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	27	9	36
DELITOS CONTRA LA SALUD PÚBLICA	4	2	6
DELITOS SEXUALES	275	529	804
FALSIFICACIÓN INFORMÁTICA	703	801	1.504
FRAUDE INFORMÁTICO	14.067	9.594	23.661
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	226	99	325
Total VICTIMIZACIONES	**22.588**	**18.202**	**40.790**

Tabla 9: Número de victimizaciones según sexo 2014 (Fuente SEC)

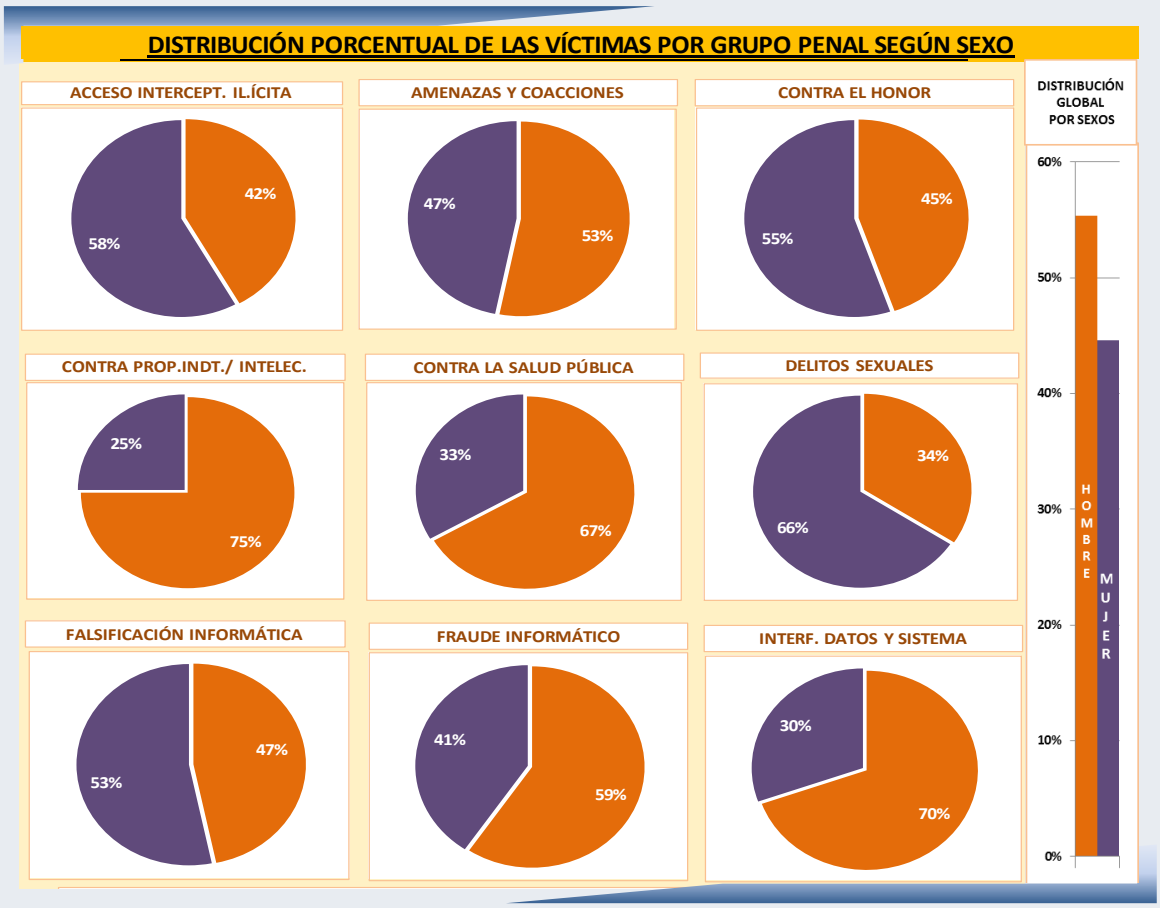

Gráfico 24: Distribución porcentual de la víctimas según sexo 2014 (Fuente SEC)

El total de victimizaciones registradas en el año 2014 por cibercriminalidad asciende a un total de 40.790[17]. El perfil de la víctima de los delitos que se incluyen dentro de este fenómeno, según los datos expuestos en estas tablas y gráficos, determina, en primer lugar, que el 55,37% de las víctimas pertenecen al sexo masculino. No obstante, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino en los hechos delictivos computados relativos al acceso e interceptación ilícita, contra el honor, la falsificación informática y los delitos sexuales.

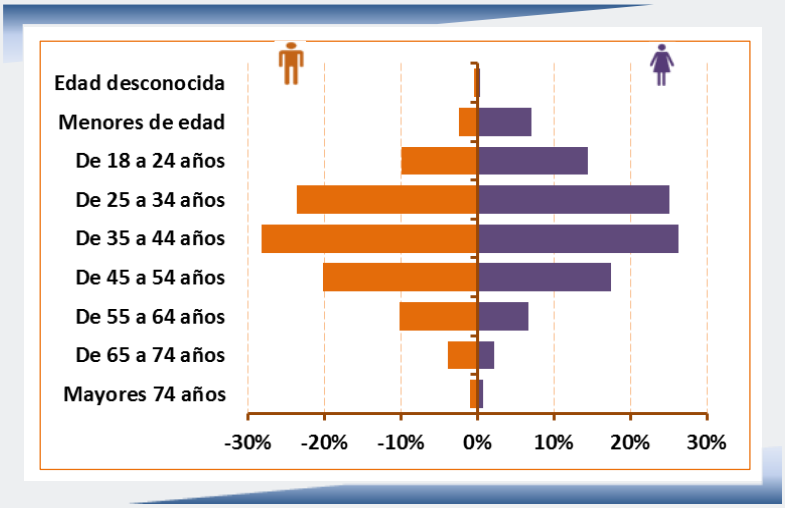

Gráfico 25: Porcentaje de víctimas según grupo de edad y sexo 2014 (Fuente SEC)

Grupo de edad	Hombre	Mujer
Edad desconocida	28	8
De 14 a 17 años	284	113
De 18 a 24 años	760	249
De 25 a 34 años	1.288	383
De 35 a 44 años	1.049	305
De 45 a 54 años	620	155
De 55 a 64 años	201	53
De 65 a 74 años	60	10
Mayores de 74 años	7	0
TOTAL	**4.297**	**1.276**

Tabla 10: Número de victimizaciones según grupo de edad y sexo 2014 (Fuente SEC)

En cuanto a la edad, se observa que el 27,30% del conjunto de las víctimas de ciberdelitos recae sobre el grupo de edad de 35 a 44 años.

[17] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (49.966) y el de victimizaciones registradas (40.790), 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.

>> Nacionalidad de la víctima

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	37.377	91,6%
2.- EXTRANJEROS	3.413	8,4%
2.1.- UNIÓN EUROPEA	1.530	3,8%
Rumanía	522	1,3%
Italia	193	0,5%
Reino Unido	147	0,4%
Francia	133	0,3%
Alemania	123	0,3%
Resto	412	1,0%
2.2.- AMÉRICA	1.036	2,5%
Colombia	146	0,4%
Ecuador	145	0,4%
Argentina	92	0,2%
Resto	653	1,6%
2.3.- ÁFRICA	463	1,1%
Marruecos	283	0,7%
Senegal	46	0,1%
Resto	134	0,3%
2.4.- ÁSIA	164	0,4%
China	49	0,1%
Paquistán	22	0,1%
Resto	93	0,2%
2.5.- RESTO PAÍSES	220	0,5%
Rusia	63	0,2%
Ucrania	49	0,1%
Otros	108	0,3%
TOTAL	40.790	100%

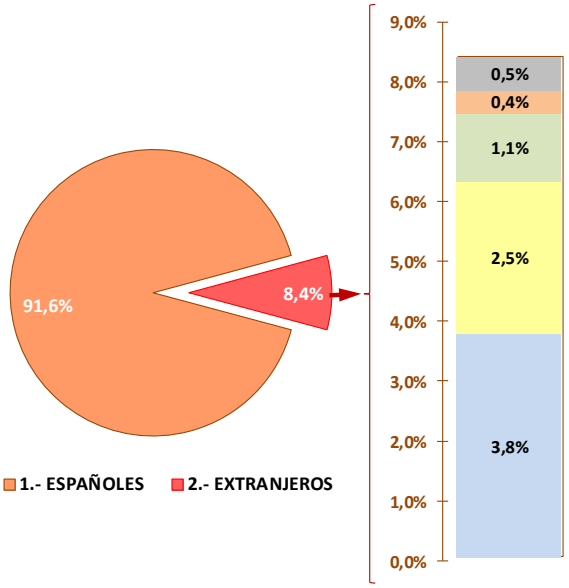

Gráfico 26: Víctimas según nacionalidad 2014 (Fuente SEC)

Según la distribución realizada por nacionalidades (gráfico 26), las víctimas de nacionalidad española ocupan el 91,6% del total de victimizaciones registradas, alcanzando la cifra de víctimas extranjeras, por lo tanto, el 8,4% restante. Dentro del conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Rumanía, Marruecos, Italia, Reino Unido, Colombia y Ecuador las que aúnan valores más elevados.

>> Victimizaciones registradas según grupo penal y edad

	Rango de edad de la víctima								
GRUPO PENAL	Descon.	0-17	18-24	25-34	35-44	45-54	55-64	65-74	> 75
ACCESO E INTERCEPTACIÓN ILÍCITA	3	201	322	392	387	271	104	34	9
AMENAZAS Y COACCIONES	38	693	1.504	2.487	2.859	1.738	676	238	93
CONTRA EL HONOR	37	180	273	519	723	423	184	50	16
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	2	7	8	11	4	1	3
DELITOS CONTRA LA SALUD PÚBLICA	0	3	1	0	0	2	0	0	0
DELITOS SEXUALES	26	614	23	28	63	37	6	3	4
FALSIFICACIÓN INFORMÁTICA	3	69	225	380	362	244	146	58	17
FRAUDE INFORMÁTICO	38	72	2.518	6.052	6.646	4.891	2.327	893	224
INTERFERENCIA EN DATOS Y EN SISTEMA	1	1	18	42	91	105	50	14	3
Total VICTIMIZACIONES	**146**	**1.833**	**4.886**	**9.907**	**11.139**	**7.722**	**3.497**	**1.291**	**369**

Tabla 11: Número de victimizaciones por tipologías delictivas, grupo de edad y sexo 2014 (Fuente SEC))

En este análisis (tabla 11) se trata de establecer una relación entre los rangos de edad de las víctimas y la tipología penal que han sufrido. En este sentido, el fraude informático, la mayor tipología delictiva registrada se establece con mayor incidencia en los rangos de edad de 25 a 44 años, patrón que se observa de igual forma en los delitos de amenazas y coacciones.

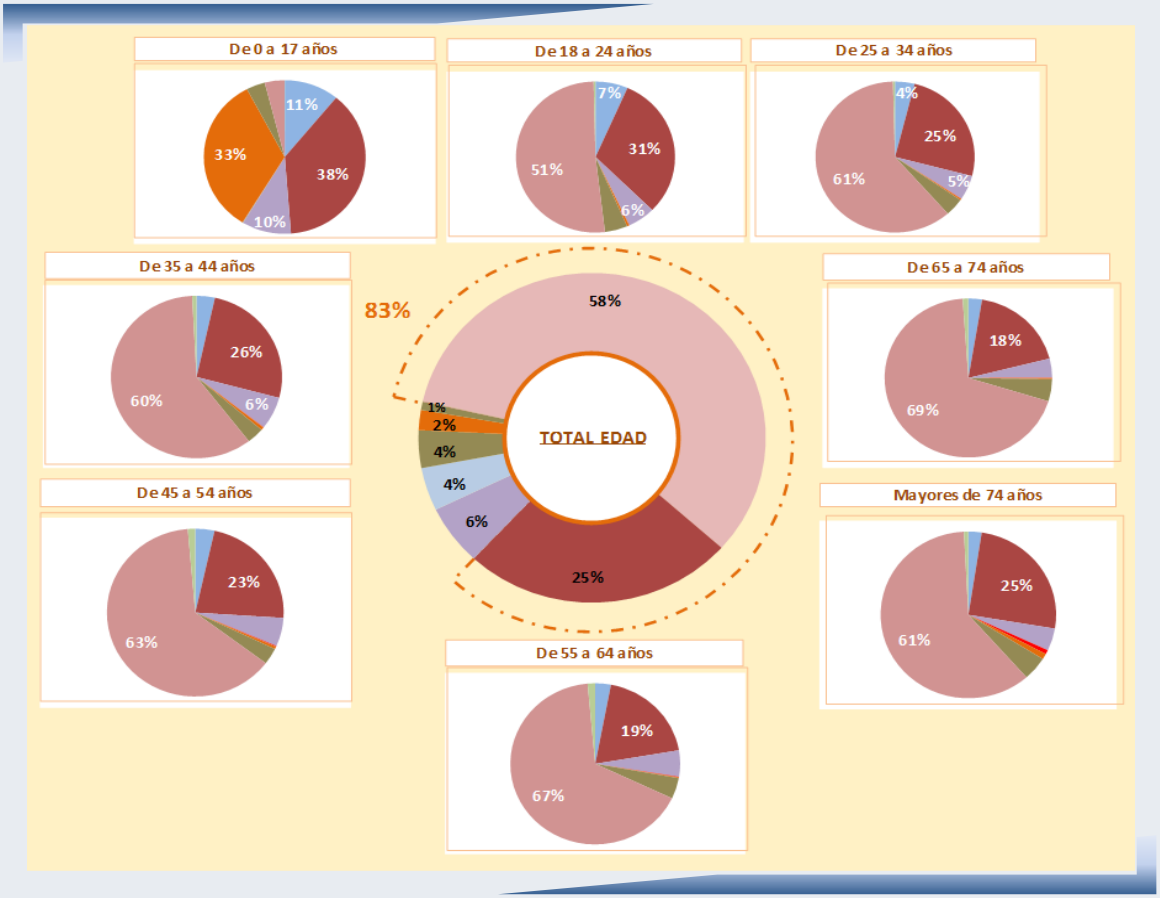

Gráfico 27: Porcentaje de victimizaciones registradas por tipologías delictivas y grupo de edad 2014 (Fuente SEC)

Un hecho interesante, que muestra el multigráfico anterior, es el diferente comportamiento que experimenta el grupo de los menores de edad. En este caso, los componentes de dicho grupo de edad son más propensos a convertirse en víctimas de delitos sexuales y no de fraude informático, siendo este último el mayoritario en el resto de grupos de edad establecidos. Sin duda, parece tratarse de una consecuencia lógica de varios factores como son su vulnerabilidad y la no disponibilidad de medios de pago electrónicos.

Perfil del RESPONSABLE: grupo penal, sexo y edad

>> Detenciones e imputaciones registradas según grupo penal y sexo

DETENCIONES E IMPUTACIONES	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	272	72	344
AMENAZAS Y COACCIONES	1.186	331	1.517
CONTRA EL HONOR	172	112	284
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	179	30	209
DELITOS CONTRA LA SALUD PÚBLICA	84	33	117
DELITOS SEXUALES	628	33	661
FALSIFICACIÓN INFORMÁTICA	143	75	218
FRAUDE INFORMÁTICO	1.613	587	2.200
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	20	3	23
Total DETENCIONES E IMPUTACIONES	**4.297**	**1.276**	**5.573**

Tabla 12: Número de detenciones/imputaciones según grupo penal y sexo 2014 (Fuente SEC)

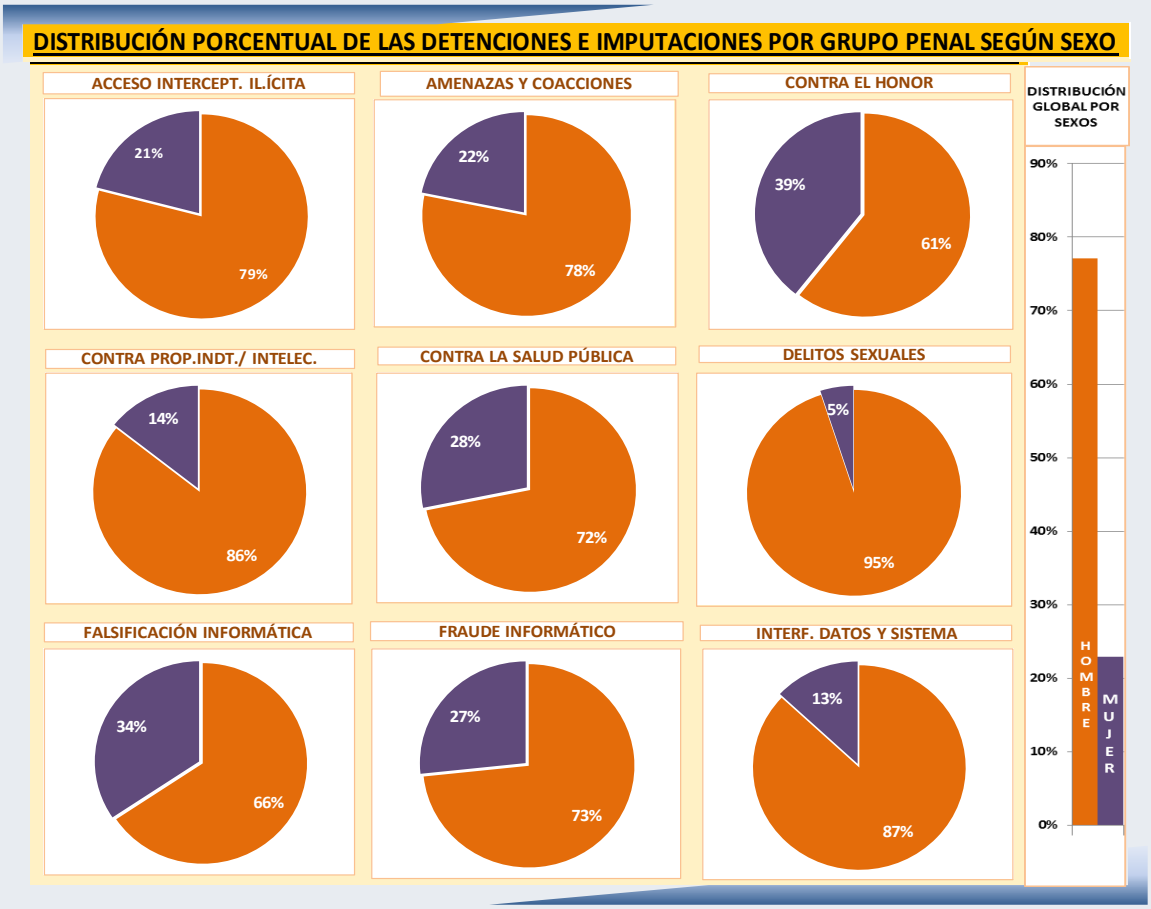

Gráfico 28: Distribución porcentual de las detenciones/imputaciones por grupo penal y sexo 2014 (Fuente SEC)

Se puede apreciar que la cifra de detenciones e imputaciones (tabla 12) efectuadas por las Fuerzas y Cuerpos de Seguridad es mayor entre las personas de sexo masculino, con un 77,10%, que entre las de sexo femenino, prevaleciendo esta tendencia en todas las tipologías delictivas registradas por el Sistema Estadístico de Criminalidad (SEC) (gráfico 28).

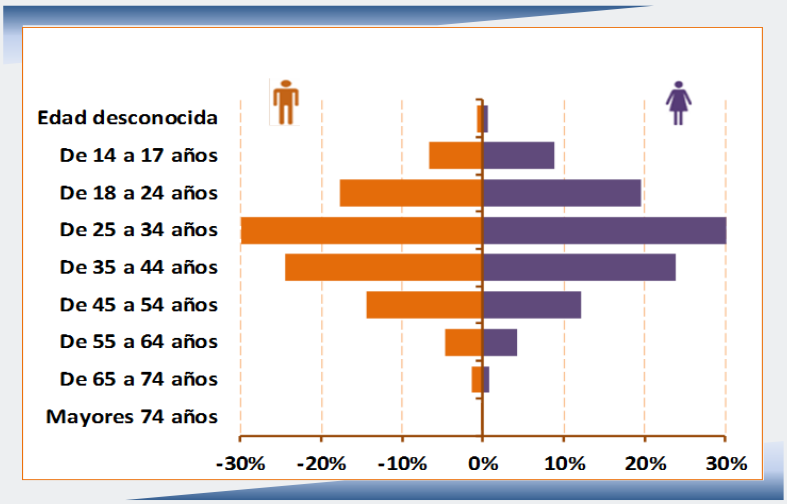

Gráfico 30: Porcentaje de detenidos/imputados según grupo de edad y sexo 2014 (Fuente SEC)

Grupo de edad	Hombre	Mujer
Edad desconocida	28	8
De 14 a 17 años	284	113
De 18 a 24 años	760	249
De 25 a 34 años	1.288	383
De 35 a 44 años	1.049	305
De 45 a 54 años	620	155
De 55 a 64 años	201	53
De 65 a 74 años	60	10
Mayores de 74 años	7	0
TOTAL	**4.297**	**1.276**

Tabla 13: Número de detenidos/imputados según grupo de edad y sexo 2014 (Fuente SEC)

Las franjas de edad determinadas apuntan a que la mayoría de los autores se encuentran englobados en el grupo de edad de comprendido entre 25 a 44 años.

>> Nacionalidad de los detenidos e imputados

NACIONALIDAD	Det./Imp.	%
1.- ESPAÑOLES	4.609	82,7%
2.- EXTRANJEROS	964	17,3%
2.1.- UNIÓN EUROPEA	336	6,0%
Rumanía	205	3,7%
Bulgaria	26	0,5%
Reino Unido	21	0,4%
Portugal	15	0,3%
Alemania	14	0,3%
Resto	55	1,0%
2.2.- AMÉRICA	293	5,3%
Colombia	62	1,1%
Ecuador	57	1,0%
Dominicana	38	0,7%
Resto	136	2,4%
2.3.- ÁFRICA	219	3,9%
Marruecos	97	1,7%
Senegal	67	1,2%
Resto	55	1,0%
2.4.- ÁSIA	82	1,5%
China	45	0,8%
Paquistán	16	0,3%
Resto	21	0,4%
2.5.- RESTO PAÍSES	34	0,6%
Ucrania	15	0,3%
Rusia	8	0,1%
Otros	11	0,2%
TOTAL	5.573	100%

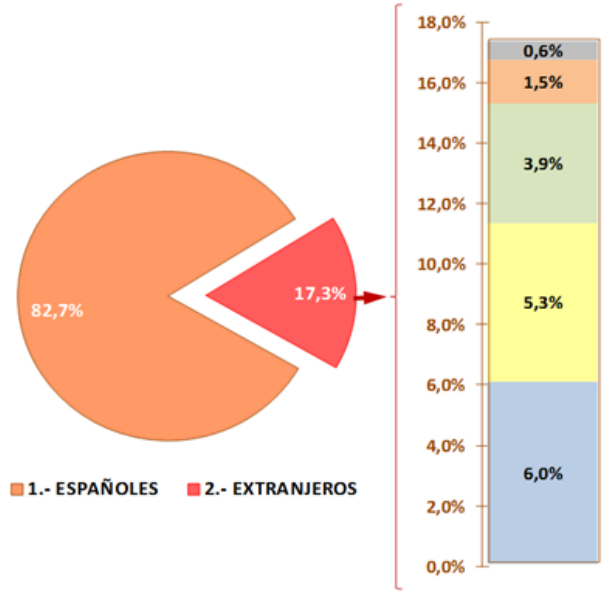

Gráfico 31: Detenidos/imputados según nacionalidad 2014

La mayoría de los detenidos/imputados por ciberdelincuencia son de nacionalidad española (82,7%). Entre los detenidos/imputados de nacionalidad extranjera, son los originarios de Rumanía, Marruecos (al igual que ocurría con las víctimas), Senegal, Colombia, Ecuador y China los que registran una mayor cifra.

>> Detenciones e imputaciones registradas según grupo penal y edad

GRUPO PENAL	Rango de edad de la víctima								
	Descon.	14-17	18-24	25-34	35-44	45-54	55-64	65-74	> 75
ACCESO E INTERCEPTACIÓN ILÍCITA	2	101	70	80	57	31	3	0	0
AMENAZAS Y COACCIONES	8	109	255	400	399	243	79	20	4
CONTRA EL HONOR	0	33	42	77	64	47	15	6	0
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	19	66	76	35	11	2	0
DELITOS CONTRA LA SALUD PÚBLICA	0	0	18	44	30	17	6	2	0
DELITOS SEXUALES	2	113	91	121	134	115	59	25	1
FALSIFICACIÓN INFORMÁTICA	2	14	34	85	47	30	5	1	0
FRAUDE INFORMÁTICO	22	26	479	784	542	255	76	14	2
INTERFERENCIA EN DATOS Y EN SISTEMA	0	1	1	14	5	2	0	0	0
Total DETENCIONES E IMPUTACIONES	**36**	**397**	**1.009**	**1.671**	**1.354**	**775**	**254**	**70**	**7**

Tabla 16: Número de detenciones/imputaciones registradas por tipología penal y edad 2014 (Fuente SEC)

Si analizamos la relación que se establece entre los diferentes rangos de edad de los responsables y la tipología penal por la que han sido detenidos o imputados, se puede apreciar que tanto en los fraudes informáticos como en las amenazas y coacciones, los procedentes del grupo de edad de 25 a 44 concentran la mayor cifra de los mismos.

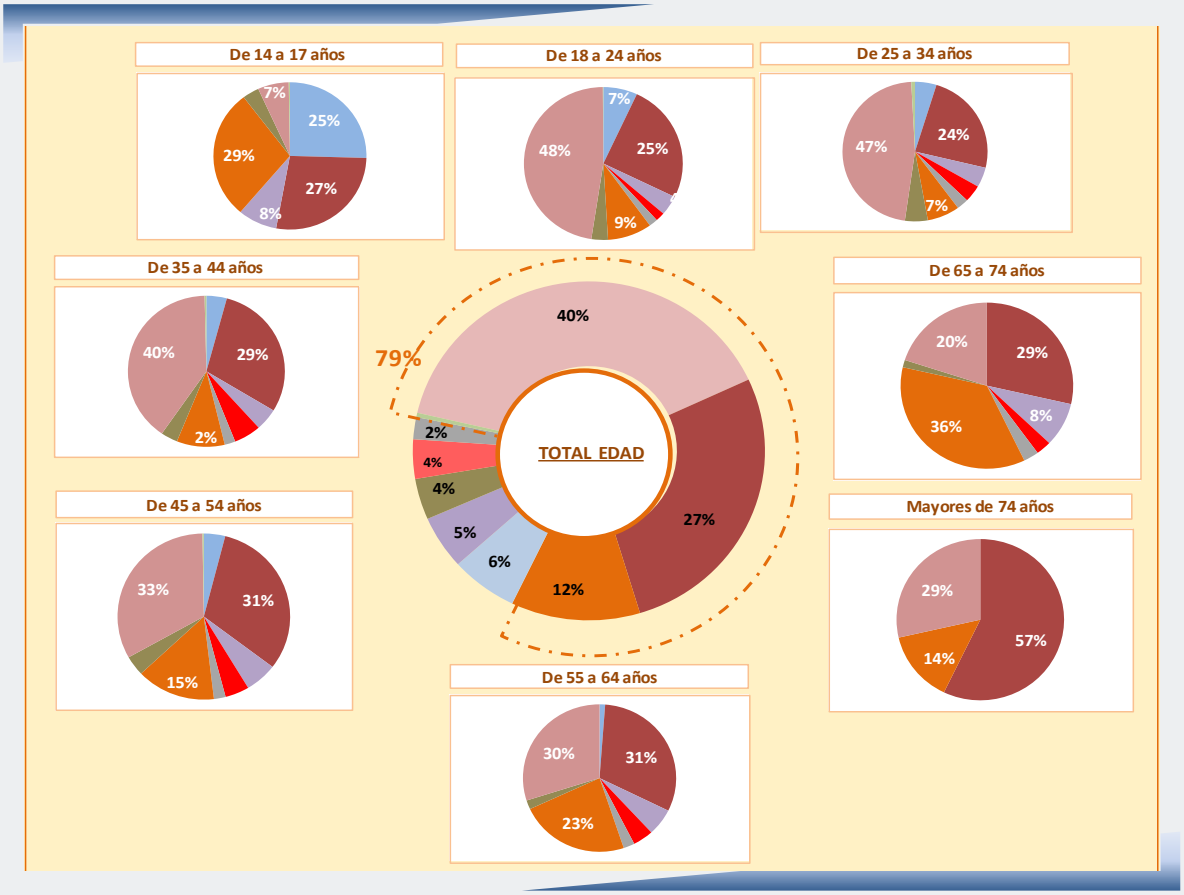

Gráfico 32: Porcentaje de detenidos/imputados registradas por tipologías delictivas y grupo de edad 2014 (Fuente SEC)

El multigráfico anterior, denota que en los grupos de edad correspondientes a menores de edad y mayores de 55 a 74 años se detecta una alta prevalencia de los delitos sexuales. En los demás grupos de edad, se aprecia que los fraudes informáticos, y los delitos de amenazas y coacciones son los más significativos en términos cuantitativos.

Anexos

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SEC A UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ACCESO ILEGAL INFORMÁTICO	Ninguna
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	DAÑOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ATAQUES INFORMÁTICOS	Ninguna
Falsificación informática	Arts CP 388-389, 399 bis, 400 y 401	FALSIFICACION DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE UTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude Informático	Arts. CP 248 a 251 y 623.4	ESTAFA BANCARIA	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ESTAFAS CON TARJETAS DE CREDITO, DEBITO Y CHEQUES DE VIAJE	
		OTRAS ESTAFAS	
Delitos sexuales	Arts. CP 181, 183.1,183.bis,184,185,186, 189	EXHIBICIONISMO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		PROVOCACIÓN SEXUAL	
		ACOSO SEXUAL	
		ABUSO SEXUAL	
		CORRUPCIÓN DE MENORES/INCAPACITADOS	
		PORNOGRAFIA DE MENORES	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP(Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		INJURIAS	
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	AMENAZAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		AMENAZAS A GRUPO ÉTNICO CULTURAL O RELIGIOSO	
		COACCIONES	
Delitos contra la salud pública	Arts. 359 a 371 del Código Penal	TRÁFICO DE DROGAS	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.
		OTROS CONTRA LA SALUD PÚBLICA	

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS

II Informe sobre Cibercriminalidad 2014

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

Síguenos en Twitter

@interiorgob

www.interior.gob.es