

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 conceptualizaciones 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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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



Infografía nº 1- Composición del Consejo Nacional de Ciberseguridad¹

- 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>

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- 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

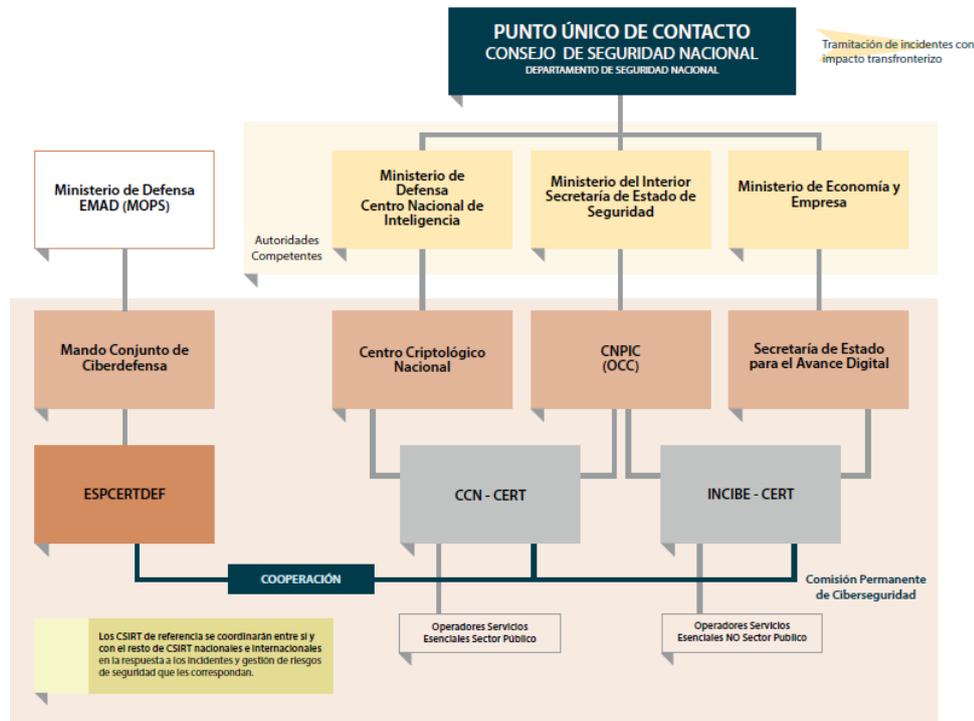
ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 cibercrimen 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:

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Infografía nº 2- Organismos encargados de la Ciberseguridad³

Durante 2018 y dentro del aspecto normativo ha tenido importancia la transposición de la Directiva UE 2016/1148⁴ 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 información⁵. 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>

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 digitales⁶. 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>

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- 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 Carbanak⁷, una de las mayores bandas de ciberdelincentes 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 delincentes 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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 ciberincidentes¹⁰”, 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>

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 móviles¹²”, 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 autenticación 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 parental¹³”, 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 2016¹⁴.

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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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,

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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”*.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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 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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

En 2018, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de 84.607¹⁵, 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 puede 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.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

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.



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 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.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

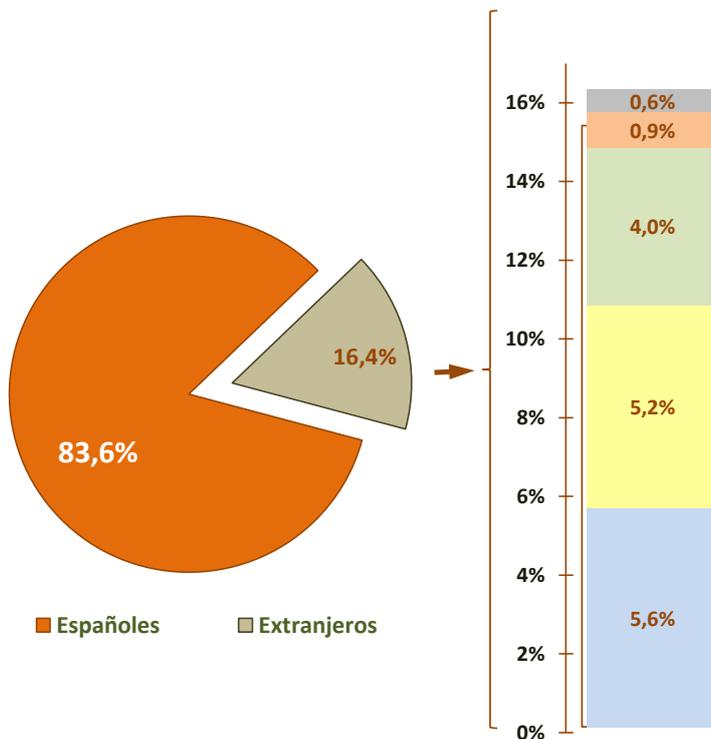
(Fuente de datos: Sistema Estadístico de Criminalidad)

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



>> 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.- ASIA	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

>> 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.

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD			
DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SECA UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos	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.
	Art. CP 278 a 285. Delitos relativos al mercado y los consumidores (espionaje industrial)	ACCESO ILEGAL INFORMÁTICO	Ninguna
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	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.
		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.
Falsificación informática	Arts. 388-389, 399 bis, 400 y 401	ATAQUES INFORMÁTICOS	Ninguna
		FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE ÚTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
Fraude informático	Arts. CP 248 a 251 y 623.4	ESTAFAS BANCARIAS ESTAFAS CON TÍTULOS DE CRÉDITO Y CHEQUES DE VALOR OTRAS ESTAFAS	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		EXHIBICIONISMO	Ninguna
Delitos sexuales	Arts. CP 181, 183.1, 183 bis, 184, 185, 186, 189	PROVOCACIÓN SEXUAL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		ACOSO SEXUAL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		ABUSO SEXUAL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		CORUPCIÓN DE MENORES/INCAPACITADOS	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		PORNOGRAFÍA DE MENORES	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
Contra la propiedad industrial/intelectual	Arts. 270 a 277 y 623.5 del CP (Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
Contra el honor	Arts. 205 a 210 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
		INJURIAS	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.
Amenazas y coacciones	Arts. 169 a 172 y 620 del 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 RELIGIOSO COACCIONES	Medio Empleado: Internet/Informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas; páginas de enlaces, blogs y correos electrónicos; redes sociales.