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

CIBERCRIMINALIDAD

> El Anuario Estadístico del Ministerio del Interior, que será publicado próximamente, introduce un apartado dedicado a la cibercriminalidad.
>
> El presente estudio tiene por objeto analizar qué se entiende por cibercriminalidad, el análisis de la situación actual, la importancia de la cooperación policial internacional en este ámbito y las conclusiones que se obtienen de los datos analizados.

CONTENIDO

DESCRIPCIÓN DEL FENÓMENO

El empleo de términos como delincuencia informática, cibercriminalidad, delitos informáticos, etc., se ha convertido en una constante en nuestra sociedad actual. El nacimiento y la rápida difusión de las redes informáticas, están propiciando que la cibercriminalidad sea uno de los ámbitos delictivos con más rápido crecimiento.

La rapidez, el anonimato, la comodidad y la amplitud de alcance que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas, tanto tradicionales aprovechando los nuevos medios, como otras nuevas nacidas dentro de este ámbito.

Ataques contra sistemas informáticos, robo y manipulación de datos, usurpación de identidad, actividades pedófilas, estafas comerciales y bancarias mediantes distintas técnicas como el phishing, difusión de malware, creación de botnets para distintos fines, etc., constituyen parte de estas actividades delictivas cometidas utilizando medios informáticos.

El alcance mundial y la rápida difusión de este tipo de actividades han causado que gobiernos de todo el mundo empiecen a implementar en sus legislaciones medidas para combatirlas y tratar de evitar y prevenir los efectos nocivos que puedan causar en sus ciudadanos.

CONVENIO DE BUDAPEST

El **Convenio sobre cibercriminalidad o Convenio de Budapest** es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet. España ratificó este convenio el 1 de octubre de 2010.

Las conductas ilícitas definidas en este Convenio y transpuestas a nuestra legislación son las siguientes:

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**:

   - **Acceso ilícito**. Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático.

   - **Interceptación ilícita**. Interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos.

   - **Interferencia en los datos**. La comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

   - **Interferencia en los sistemas**. La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

   - **Abuso de los dispositivos**. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos anteriormente o una contraseña, un código de acceso o datos informáticos similares, que permitan tener acceso a la totalidad o a una parte de un sistema informático.

2. **Delitos informáticos:**

   - **Falsificación informática.** La introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

   - **Fraude informático.** Los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, o mediante cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

3. **Delitos relacionados con el contenido:**

   - **Delitos relacionados con la pornografía infantil**. La producción, la oferta, la puesta a disposición, difusión, adquisición y posesión de pornografía infantil con vistas a su difusión por medio de un sistema informático**.**

4. **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.**

TIPOLOGÍAS DELICTIVAS DE INTERÉS POLICIAL, EN EL ÁMBITO DE LA CIBERCRIMINALIDAD

Existen muchas tipologías penales que pueden cometerse mediante el uso de lo que han venido a denominarse las “nuevas tecnologías”.

Para establecer unos criterios metodológicos que permitieran la comparación con los países de nuestro entorno, se ha decido en un primer lugar emplear las tipologías penales descritos en el Convenio sobre Cibercriminalidad de Budapest.

No obstante, existen otras tipologías, que aunque no están contempladas en el Convenio de Budapest, interesa observar, cuando los medios empleados en su comisión sean las nuevas tecnologías, dado el volumen y la importancia que están adquiriendo:

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

DATOS DEL SISTEMA ESTADÍSTICO DE CRIMINALIDAD REFERENTES A CIBERCRIMINALIDAD Y TIPOLOGÍAS DE INTERÉS POLICIAL QUE SERÁN INCLUIDOS EN EL ANUARIO ESTADÍSTICO DEL MINISTERIO DEL INTERIOR

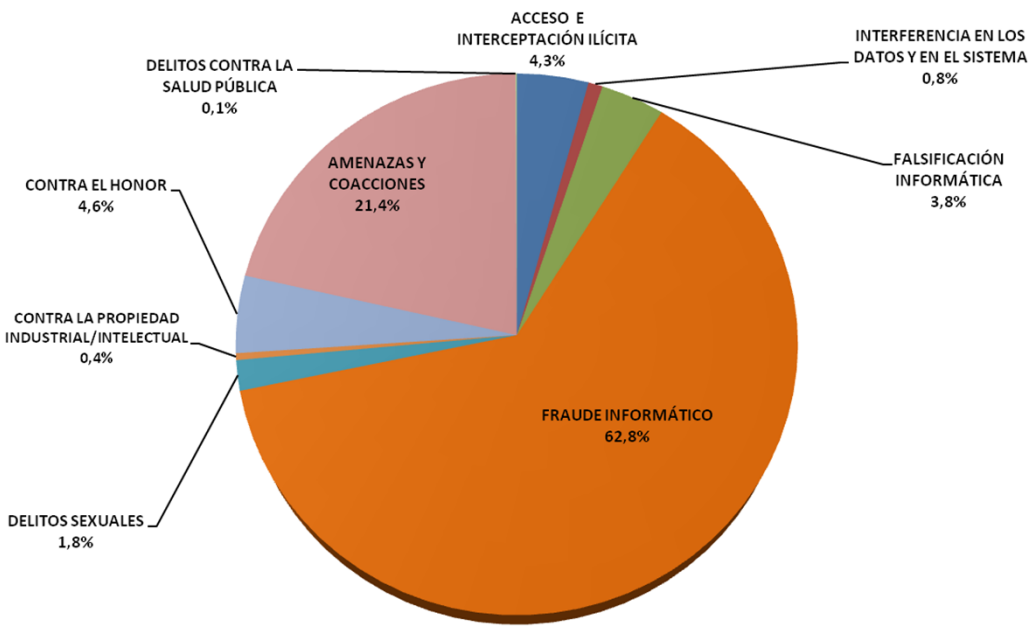
Los datos referentes a cibercriminalidad que se incluirán en el Anuario Estadístico del Ministerio del Interior aúnan las tipologías referidas en el Convenio de Budapest, y aquéllas otras que se han considerado de interés policial. Durante los años 2011 a 2013, los datos sobre el número de infracciones penales conocidas son los siguientes:

GRUPOS DELICTIVOS	2011	2012	2013
ACCESO E INTERCEPTACIÓN ILÍCITA	1.492	1.701	1.805
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	228	298	359
FALSIFICACIÓN INFORMÁTICA	1.860	1.625	1.608
FRAUDE INFORMÁTICO	21.075	27.231	26.664
DELITOS SEXUALES	755	715	768
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172
CONTRA EL HONOR	1.941	1.891	1.963
AMENAZAS Y COACCIONES	9.839	9.207	9.064
DELITOS CONTRA LA SALUD PÚBLICA	46	43	34
TOTAL	**37.458**	**42.855**	**42.437**

Entre los tipos penales más frecuentes se sitúan los fraudes informáticos, seguidos a cierta distancia por las amenazas y coacciones.

Estos datos corresponden a la actividad registrada, por las Fuerzas y Cuerpos de Seguridad del Estado y la Policía Foral de Navarra. También se incluyen datos de los cuerpos de Policía Local que facilitaron datos al Sistema Estadístico de Criminalidad durante el año 2013.

DATOS DEL SISTEMA ESTADÍSTICO DE CRIMINALIDAD REFERENTES A CIBERCRIMINALIDAD Y TIPOLOGÍAS DE INTERÉS POLICIAL QUE SERÁN INCLUIDOS EN EL ANUARIO ESTADÍSTICO DEL MINISTERIO DEL INTERIOR



La distribución porcentual de estas tipologías muestra que casi dos tercios de las infracciones penales registradas corresponden a los fraudes informáticos. Las amenazas y coacciones suponen algo más del 20 % del total. El resto de tipologías suponen porcentajes del total muy inferiores.

En los gráficos anteriores se observa la evolución del número de hechos conocidos, número de hechos esclarecidos y número de detenidos e imputados.

DATOS DEL SISTEMA ESTADÍSTICO DE CRIMINALIDAD REFERENTES A CIBERCRIMINALIDAD Y TIPOLOGÍAS DE INTERÉS POLICIAL QUE SERÁN INCLUIDOS EN EL ANUARIO ESTADÍSTICO DEL MINISTERIO DEL INTERIOR

En el año 2012 se produce un incremento en el número de hechos conocidos, reduciéndose luego ligeramente en 2013. Se han producido aumentos progresivos en el número de hechos esclarecidos y en el número de detenidos e imputados.

INFRACCIONES PENALES	2011	2012	2013
TOTAL	2.285.525	2.268.867	2.172.133
ÁMBITO CIBERCRIMINALIDAD Y DE INTERÉS POLICIAL	37.458	42.855	42.437
PORCENTAJE CIBERCRIMINALIDAD SOBRE TOTAL	1,64%	1,89%	1,95%

Por último, hay que hacer notar como se observa en la tabla anterior, que estas tipologías representan en 2013, algo menos del 2% de la cifra total de hechos conocidos, si bien, se ha experimentado un incremento durante los últimos años, más acentuado en el período comprendido entre 2011 a 2012, que entre 2012 y 2013.

COOPERACIÓN POLICIAL INTERNACIONAL

En todos los delitos de carácter transnacional la cooperación policial internacional es fundamental para la prevención y la persecución, más si cabe en el ámbito de la cibercriminalidad dado que su comisión se produce en un espacio virtual donde no existen fronteras físicas.

Con este objetivo la Comisión Europea decidió establecer un **Centro Europeo del Cibercrimen[1] (EC3)** en Europol que constituyese un punto central en la lucha de la Unión Europea contra la ciber-criminalidad, contribuyendo a acelerar las reacciones contra los delitos online.

Dará apoyo a las instituciones de los Estados Miembros de la Unión Europea para la construcción de una capacidad operacional y analítica para las investigaciones y cooperación con socios internacionales.

El EC3 ha comenzado oficialmente sus actividades el 1 de enero de 2013 con un mandato de abordar las siguientes áreas de cibercriminalidad.

- ✓ Los cometidos por grupos organizados para generar grandes beneficios delictivos, como el fraude en línea.
- ✓ Los que causen daños graves a las víctimas como la explotación infantil en línea.
- ✓ Los que afecten a las infraestructuras críticas y los sistemas de información de la Unión Europea.

En 2013 la Unión Europea ha publicado **la directiva 2013/40/UE[2]**, relativa a ataques contra los sistemas de información que establece unas normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información, teniendo también por objeto facilitar la prevención de dichas infracciones y la mejora en la cooperación entre las autoridades judiciales y otras autoridades competentes.

1 https://www.europol.europa.eu/ec3.1.html

2 http://www.boe.es/doue/2013/218/L00008-00014.pdf

Finalmente hay que indicar que la Comisión Europea, a través de su **programa de investigación Horizonte 2020**[3], subvenciona proyectos de investigación tecnológicos, entre los cuáles se encuentran los relacionados con la seguridad digital; este programa está dirigido a empresas, organismos oficiales y Universidades y cuenta para el período 2014-2020 con un presupuesto de 76.880 millones de Euros.

De esta manera la Comisión Europea continua la inversión realizada hasta ahora dentro del 7º Programa Marco de Investigación y Desarrollo Tecnológico y de los **programas de financiación gestionados por la Dirección General de Home Affairs**, con los que, entre otros se ha puesto en marcha el Centro Nacional de Excelencia en Ciberseguridad en la Universidad Autónoma de Madrid.

3 http://www.eshorizonte2020.es/

ESTRATEGIAS ESPAÑOLAS DE SEGURIDAD Y DE CIBERSEGURIDAD

El 5 de diciembre de 2013 el Consejo de Ministros aprobó la nueva Estrategia de Ciberseguridad Nacional[4]. Se articula en torno a cinco capítulos en los que describe el ciberespacio y su seguridad, detalla el propósito y los principios rectores de la ciberseguridad en España, expone los objetivos de la ciberseguridad, las líneas de actuación, y cómo se articula la ciberseguridad dentro del Sistema de Seguridad Nacional.

El Consejo de Seguridad Nacional ha impulsado la elaboración de la Estrategia de Ciberseguridad Nacional con el fin de dar respuesta al enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él.

Respecto a la protección de las infraestructuras críticas, en el Ministerio del Interior se creó el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)[5], que entre otros cometidos se encarga de la ciberseguridad en estas infraestructuras. El CNPIC se incluye dentro de la Estrategia Española de Seguridad[6] (pág. 77) que aprobó el Consejo de Ministros el 31 de mayo de 2013.

[4] Enlace a Estrategia de Ciberseguridad Nacional 2013 en PDF

[5] El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es competente en la protección de las infraestructuras críticas según la Ley 8/2011 y el Real Decreto 704/2011

[6] Enlace a Estrategia Española de Seguridad en PDF

La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo de colaboración en materia de ciberseguridad en el que, entre otros aspectos, se sientan las bases para la colaboración del CNPIC e Instituto Nacional de Tecnologías de la Comunicación (INTECO) en materia de Respuesta a Incidentes para las Tecnologías de la Información de los operadores estratégicos nacionales y el sector privado en general. Por otra parte, la Oficina de Coordinación Cibernética (OCC), dependiente orgánicamente del CNPIC, se ha erigido en órgano coordinador en materia de ciberseguridad en el ámbito del Ministerio del Interior, agilizando las actividades que se llevan a cabo de forma conjunta con INTECO. De esta forma INTECO se convierte en una herramienta de apoyo a la OCC en la gestión de incidentes de ciberseguridad[7] y en la implantación de medidas preventivas.

Como iniciativa conjunta del Ministerio del Interior (Guardia Civil y Cuerpo Nacional de Policía), el Instituto de Ciencias Forenses y de Seguridad de la Universidad Autónoma de Madrid y el Grupo S21Sec, se constituyó a partir del año 2011, el Centro Nacional de Excelencia en Ciberseguridad (CNEC[8]), dedicado a la formación, entrenamiento, investigación y desarrollo tecnológico de excelencia en materia de ciberseguridad y ciberinteligencia para el incremento de la eficacia de la lucha contra la criminalidad.

[7] http://www.cnpic-es.es/Ciberseguridad/1_Respuesta_a_incidentes/index.html

[8] http://cnec.icfs.uam.es/es

CONCLUSIONES

- En primer lugar se puede destacar la gran importancia que el fenómeno de la cibercriminalidad tiene en el ámbito internacional, así como para la seguridad nacional, no sólo por la amenaza que representa para los ciudadanos en general, sino también por los peligros que supone para la economía y las infraestructuras críticas.

- En el Sistema Estadístico de Criminalidad se recogen datos tanto de los delitos propuestos en el Convenio de Budapest, como de otros delitos cometidos con medios informáticos, de especial interés policial por su comportamiento.

- En 2013 se esclarecieron 2.167 de los 42.437 hechos conocidos en el ámbito de la cibercriminalidad, un 5,1%, porcentaje todavía muy bajo en comparación con el porcentaje de esclarecimientos de las infracciones penales (delitos y faltas) del mismo año (37%), o con el porcentaje de esclarecimiento de los delitos contra el patrimonio (23,9%).

- En 2013 se detuvieron a 5.054 personas en los 2.167 hechos esclarecidos, es decir 2,33 personas por hecho, lo que parece indicar que los autores no suelen serlo a título individual sino formando parte de grupos organizados.

- Por último señalar que la preocupación a nivel internacional y doméstico no sólo está conduciendo a la modificación de las legislaciones nacionales, sino a la creación y financiación de diversas estructuras para combatir este nuevo ámbito delictivo.