

Introducción

La progresiva tecnificación de nuestra sociedad se ha acentuado en los últimos 20 años, de forma que nos ha ido y nos va haciendo cada vez más tecnológicamente dependientes y vulnerables. Esta ambivalencia es especialmente significativa en el caso de las tecnologías de la información y de la comunicación (TIC). Desde la aparición del primer ordenador personal en 1981, nuestro tiempo ha sido testigo de la creación, despliegue y popularización de Internet. En efecto, la red forma parte del día a día de casi todos los ciudadanos del primer mundo. Hemos asumido el uso cotidiano de la ofimática, los teléfonos inteligentes y las redes sociales. La información digital y los medios de acceso a la misma configuran, pues, la interfaz preferencial de obtención, análisis e intercambio de conocimiento.

Esa digitalización de nuestro tiempo, por ejemplo, ha convertido las conversaciones familiares en intercambios de mensajes en grupos de WhatsApp, ha configurado las redes sociales como medio principal de acceso a las noticias en perjuicio de los medios tradicionales de información (periódico de papel, radio y televisión) y también ha posibilitado una gestión más automatizada y eficiente de recursos como el agua y la energía eléctrica. Consecuentemente, existe una imbricación de ese mundo artificial de intercambio y procesamiento de datos, el ciberespacio,

en nuestro mundo físico. El ciberespacio no es un mero anexo del mundo real, sino uno de los elementos que actualmente lo configuran a través de una relación bidireccional que es de carácter problemático.

El trasvase operacional que existe entre el mundo físico y el ciberespacio convierte a las personas, empresas y organismos en usuarios de las cibertecnologías. Del mismo modo que hay acciones que pueden poner en peligro los intereses y derechos de los sujetos y agentes del mundo físico, también tendremos operaciones propias del ciberespacio que impiden que los usuarios vean satisfechas sus expectativas al usar cibertecnologías. Así, por ejemplo, el robo de un coche tiene su análogo en el robo de información de clientes en plataformas de comercio electrónico, los secuestros de personas tienen su equivalente en el *ransomware* o secuestro de información, etc. Es más, hemos de tener en cuenta que los usos y abusos del ámbito cibernético tienen un impacto más allá del ciberespacio, tal y como se han puesto de manifiesto en incidentes de seguridad nacional e internacional como el famoso ataque Stuxnet, del que hablaremos más adelante. Dicho de otra forma, el ciberespacio no es simplemente un marco operativo, sino que se puede constituir en causa y efecto en el mundo físico por mor de los denominados *sistemas ciberfísicos*.

Por todo ello, hemos de hablar de ciberamenazas, ciberdelitos y del ciberriesgo como elementos de igual importancia que las amenazas, delitos y riesgos de nuestro mundo físico. En este sentido es de destacar el Convenio de Budapest (CETS n°185) sobre ciberdelincuencia (o convenio sobre cibercrimen), que es el primer tratado internacional que pretende hacer frente a los ciberdelitos¹. Tal convenio es, de hecho, el único acuerdo internacional vinculante sobre este tema.

En la actualidad, hay más de 50 países que se han adherido al convenio. España lo firmó el 23 de noviembre de 2001

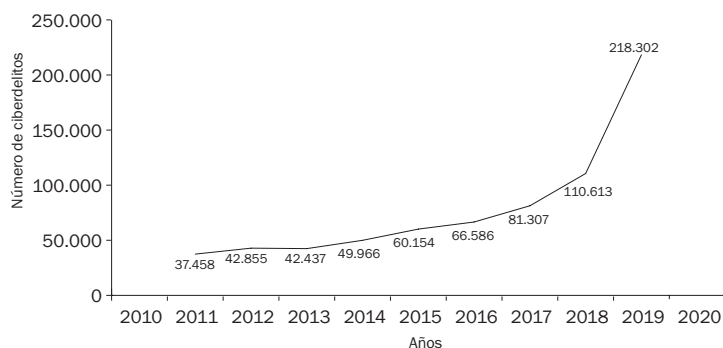
1. Más información en <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

y lo ratificó el 1 de octubre de 2010. Tal ratificación ha tenido como consecuencia que, en la reforma del Código Penal español, de 2015, se introdujeran artículos para tipificar diferentes tipos de cibercrímenes, como el acceso no autorizado a sistemas informáticos.

Fruto de todo ello es la lucha constante de los Fuerzas y Cuerpos de Seguridad del Estado de España contra la ciberdelincuencia. Para tener una idea de la importancia de este tipo de delitos, cabe destacar el número de los mismos que se han llevado a cabo en los últimos años y su evolución creciente (figura 1). Así, solo en 2019 se cometieron 218.302 delitos, lo que representa el 10% de todos los delitos cometidos y supone un crecimiento del 35,81% respecto al año 2018. De todos ellos, 192.375 estuvieron relacionados con el fraude informático, 12.782 fueron amenazas y coacciones, se llevaron a cabo 4.275 falsificaciones informáticas y 4.004 accesos e interceptaciones ilícitas, 1.422 fueron delitos contra el honor, 1.774 delitos sexuales, 1.473 se relacionaron con la interferencia en los datos y en los sistemas, y 197 lo fueron contra la propiedad industrial/intelectual. Las tres comunidades autónomas con mayor índice de ciberdelitos fueron: Cataluña con 41.577, Madrid con 37.016 y Andalucía con 28.655.

FIGURA 1

Evolución del número de ciberdelitos entre 2011 y 2019.



FUENTE: [HTTPS://OEDI.ES/ESTADISTICAS/](https://oedi.es/estadisticas/)

Es de destacar que la mayor parte de estos delitos en 2019, un 88,1%, corresponden a fraudes informáticos o estafas, cuyo crecimiento en los últimos años ha sido muy destacable. Por el contrario, el número de delitos contra la salud pública ha ido disminuyendo paulatinamente, desde los 46 que se informaron en 2011, hasta llegar a 0 en 2015, valor que se ha mantenido hasta la fecha.

Según el VII Informe sobre Cibercriminalidad de la Secretaría de Estado de Seguridad (SES, 2020), de todos los delitos cometidos en 2019, se han resuelto unos 31.000 (algo menos del 15%), lo que permitió la investigación de cerca de 9.000 presuntos responsables. Según este informe, el perfil más común del ciberdelincuente en España es un varón de nacionalidad española de entre 26 y 40 años.

La ciberseguridad surge como mecanismo de control del ciberriesgo. De forma más precisa, podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización.

De forma general, el ciudadano, las empresas y organizaciones se ven obligadas, en función de su especialización, a delegar parte de su confianza en los expertos que desarrollan herramientas y soluciones para proteger los activos mencionados. Ahora bien, esta cesión de confianza debe estar respaldada por un conjunto de soluciones que sean de fácil de uso y transparentes para los usuarios de las cibertecnologías. En efecto, un gran número de propuestas de seguridad han sido descartadas por los usuarios debido a su alta complejidad. Además, en el momento actual son muchos los servicios de gestión de información que han proporcionado casos concretos de abuso en el tratamiento de datos personales. En resumidas cuentas, la correcta implementación de

la ciberseguridad debe combinar de modo equilibrado elementos de seguridad, de privacidad y de usabilidad.

La ciberseguridad es una ciencia de reciente cuño y que aún está por definir de modo preciso. Este libro pretende proporcionar una introducción al campo multidisciplinar de la ciberseguridad, y lo hace con una doble intención: pedagógica y de concienciación. Así, y como primer estadio del texto, se llevará a cabo un análisis de los principales recursos con los que contamos para generar, almacenar e intercambiar información en el ciberespacio. Todas esas modalidades de gestión de información determinarán distintos ámbitos de operación, a los que denominaremos *dominios de la ciberseguridad*. Cada uno de estos dominios reúne una serie de rasgos específicos en lo relativo a las posibilidades de computación y gestión de información, pero también en lo concerniente a las ciberamenazas que afectan a sus activos de información. Así, no es lo mismo almacenar la información personal en el disco duro de nuestro ordenador en casa que hacerlo, por ejemplo, en Google Drive (es decir, ‘la nube’). Además, es muy diferente acceder a la información desde nuestro ordenador, que hacerlo mediante un dispositivo móvil conectado a la wifi pública de un restaurante. También se introducirán las principales ciberamenazas de los distintos dominios de la ciberseguridad. La correcta concreción de tales amenazas se hará de acuerdo con las restricciones concretas de casos de uso en el ámbito personal, empresarial y gubernamental. Finalmente, el análisis de las ciberamenazas y su impacto se complementará con un resumen de mecanismos y procedimientos para la protección de los activos de información en el ciberespacio.

De forma más detallada, el libro consta de esta introducción y cuatro capítulos más. En el capítulo 1 se explicarán las principales ciberamenazas a la ciberseguridad de individuos y organizaciones. El capítulo 2 está dedicado a los dominios de la ciberseguridad, donde se discutirán las principales características, en términos de seguridad, de los ordenadores, los dispositivos móviles, la computación en la nube, el internet de las cosas (IoT, *internet of things*), etc. Una vez han sido

introducidos los dominios que afectan a la gestión y procesamiento de información, en el capítulo 3 se presentarán los principales ámbitos de uso y aplicación de la ciberseguridad, es decir, la gestión personal y empresarial de la información, así como sus repercusiones sociales (uso de correo electrónico, mensajería instantánea, redes sociales, redes de comunicación, etc.). Cada uno de estos ámbitos de aplicación es susceptible de ser atacado en virtud de un uso negligente de las tecnologías o de sus posibles vulnerabilidades. En el capítulo 4 se incluye un conjunto de soluciones y recomendaciones a modo de guía de buenas prácticas para paliar en la medida de lo posible el impacto de los ciberataques. Finalmente, el libro termina con el capítulo de conclusiones en el que se muestran aquellas relacionadas con los desafíos que supone la implantación de la ciberseguridad en nuestra sociedad.