Alberto Hernández Moreno*

CIBERSEGURIDAD Y CONFIANZA EN EL ÁMBITO DIGITAL

La dependencia tecnológica de nuestra sociedad unida a las características únicas que posee el nuevo dominio que es el ciberespacio, hacen que la ciberseguridad sea un asunto de máxima importancia para la seguridad de los Estados. Los ciudadanos, empresas, Administraciones Públicas y países están sufriendo ciberataques con consecuencias importantes que van más allá de la mera pérdida económica. Los recientes ciberataques a nivel mundial han dado lugar a verdaderas crisis y han puesto de manifiesto que la ciberseguridad requiere del compromiso y colaboración de todos aquellos organismos y personas que utilizan la tecnología.

Palabras clave: *ciberseguridad, ciberespacio, Internet, tecnología, amenazas, virus informáticos.*
Clasificación JEL: *O31, O33, O38.*

1. Introducción

La mañana del viernes 12 de mayo de 2017 daba comienzo a un fin de semana en el que, tanto en nuestro país como en el resto del mundo, la mayoría de los ciudadanos tomaron por primera vez conciencia de que la ciberseguridad, los ciberataques, las ciberamenazas y, en general, todo lo «ciber» ya no era un tema de ciencia ficción y reservado exclusivamente a informáticos que, trabajando desde casa sin salir, hacían cosas incomprensibles para el resto de los mortales.

WannaCrypt, *WannaCry* o *Wcry* no fue más que un virus informático que aprovechaba una vulnerabilidad conocida en productos Microsoft, pero que se propagó rápidamente alrededor del mundo y produjo una crisis que mantuvo a la sociedad pendiente de los medios de comunicación y preocupada por entender qué pasaba y qué tenía que hacer para protegerse.

La dependencia tecnológica de nuestra sociedad es una realidad. En nuestro ámbito profesional hacemos un uso intensivo de la tecnología, ya sea para comunicarnos con otros profesionales y empresas, para elaborar y almacenar información, para realizar actividades esenciales de los procesos de negocio e incluso para poder acceder a nuestro propio puesto de trabajo. Pensemos por ejemplo en sistemas que forman parte de nuestro día a día como el control de acceso al edificio, la identificación mediante tarjeta electrónica, huella dactilar, PIN o código de acceso, sistemas que pueden pasar desapercibidos como los sistemas automáticos de control de los ascensores, extinción de incendios, detección de intrusos, etc.

Pero esta dependencia tecnológica no es exclusiva de nuestro ámbito profesional. Si miramos la

* Director General del Instituto Nacional de Ciberseguridad de España (INCIBE).

penetración de la tecnología en nuestro ámbito personal, en nuestros hogares nos encontramos con todo tipo de dispositivos: tabletas electrónicas, televisiones inteligentes, relojes inteligentes y, poco a poco, muchos objetos cotidianos interconectados a Internet creando así el nuevo concepto de Internet de las cosas (*Internet of Things,* IoT*),* que nos proporciona un contacto permanente con lo que pasa en el mundo y con las personas con las que convivimos y nos relacionamos. Ya en el año 2015 había mayor número de suscripciones de teléfono móvil que ciudadanos en la Unión Europea (ONTSI, 2016).

La velocidad con la que se están produciendo los avances tecnológicos crece año a año, pero también lo hace la velocidad con la que aceptamos e integramos estos avances en nuestras vidas. Solo hace falta mirar atrás y ver los orígenes de Internet. Los primeros pasos hacia lo que conocemos hoy como Internet se empezaron a dar en los años sesenta del siglo pasado, cuando la antigua agencia estadounidense ARPA (Advanced Research Projects Agency), actualmente DARPA (Defense Advanced Research Projects Agency), desarrolló la red ARPANet (Advanced Research Projects Agency Network) con el objetivo de conectar ordenadores de diferentes centros de investigación para intercambiar datos e información sobre investigaciones. La posibilidad de conectividad e intercambio de información que esta red introducía supuso el embrión de lo que conocemos hoy como Internet. No obstante, no fue hasta principios de los años noventa, con el desarrollo de la World Wide Web (www) y su puesta a disposición para su uso de forma gratuita, así como la mejora de la red ARPANet y el levantamiento de la prohibición para su uso comercial, cuando podemos decir que comienza lo que hoy conocemos como Internet.

En tan solo un cuarto de siglo, Internet y todas las aplicaciones que sobre ella se han desarrollado han crecido de forma exponencial. A día de hoy hay más de 3.700 millones de internautas en el mundo y más de 37.000.000 en España (WAS, 2017). Aplicaciones y redes sociales como Facebook, desarrollada en el año 2004, YouTube en 2005, Twitter en 2006 o WhatsApp en 2009, forman parte de nuestra vida diaria y de la forma en que interactuamos. La tecnología, desarrollada por el hombre, está cambiando nuestras formas de actuar y relacionarnos con los demás.

Las ventajas que las tecnologías de la información y las comunicaciones (TIC) aportan son múltiples y diversas: pensemos por ejemplo en las relacionadas con la mejora en el diagnóstico sanitario, el análisis masivo de datos en diferentes tipos de investigaciones, la automatización en la producción alimentaria e industrial, el transporte, las comunicaciones, etc.

No obstante, la tecnología lleva irremediablemente unida el concepto de «vulnerabilidad». Si consultamos a la Real Academia Española, «vulnerabilidad» se define como: «cualidad de vulnerable», entendiendo por «vulnerable»: «Que puede ser herido o recibir lesión, física o moralmente». Y es aquí donde, quizá hasta la reciente crisis de *WannaCry*, no hemos sido lo suficientemente conscientes de que las tecnologías que utilizamos diariamente, en nuestro trabajo y en nuestra casa, presentan vulnerabilidades y por lo tanto pueden producirnos un daño si no las utilizamos y protegemos correctamente.

2. Historia de la ciberseguridad: de *Creeper* a *WannaCrypt*

Aunque el concepto de virus informático aparece a principios de los años ochenta del pasado siglo, el considerado primer virus informático de la historia se remonta a hace más de 40 años, en concreto, al año 1971. *Creeper*, un programa informático desarrollado por el ingeniero Robert H. Thomas, que trabajaba en la empresa BBN Technologies en Massachusetts, EE UU, se movía entre los ordenadores de la red ARPANet mostrando el mensaje: *I'm the creeper, catch me if you can!* Si bien no producía ningún efecto nocivo en los ordenadores que «infectaba» más allá de mostrar dicho mensaje y, por lo tanto, no constituía un código

malicioso como son los virus, su funcionamiento es considerado el origen de los actuales virus informáticos.

Desde la aparición de *Creeper* hasta la crisis de *WannaCry* han aparecido multitud de virus informáticos y miles de ciberataques han tenido lugar en el mundo, algunos de ellos incluso han ocupado grandes titulares en los medios de comunicación, pero quizá la crisis de *WannaCry*, debido a su impacto mediático, es la que ha supuesto un antes y un después en la conciencia general de que la ciberseguridad es un asunto que nos concierne a todos.

En estos más de 40 años que han transcurrido desde *Creeper* a *WannaCry* numerosos países, Administraciones Públicas, empresas de todo tipo y naturaleza y ciudadanos han sufrido miles de ciberataques con diferentes motivaciones. El ciberespacio, o Internet, presenta una serie de características que lo hacen muy interesante para cometer este tipo de actos:

- Es un espacio global en el que no hay fronteras y que llega a prácticamente todos los rincones del mundo: las redes y sistemas de nuestras empresas, nuestros teléfonos móviles, relojes inteligentes o televisiones inteligentes, entre otros, forman parte del ciberespacio y están permanentemente conectados a él.
- El coste de acceso es muy bajo. Pensemos por ejemplo en el precio del teléfono móvil más barato del mercado con el que nos podemos conectar a Internet.
- La velocidad de acceso se mide en milésimas de segundo. La consulta a una página web ubicada en un servidor a miles de kilómetros de distancia o el envío de un mensaje de WhatsApp a un amigo en otro país son cuestión de milisegundos.
- Es un espacio en el que la atribución de las acciones que en él se realizan no siempre es posible, por lo que proporciona un grado de anonimato que lo hace muy atractivo como medio para la realización de actividades delictivas de todo tipo. Las diferentes legislaciones de cada país, sus condiciones políticas, sus intereses estratégicos, e incluso las diferencias culturales e históricas, hacen que la armonización de normas internacionales que regulen las actividades en el ciberespacio y que mejoren su ciberseguridad sea lenta y compleja.

Un claro ejemplo son las leyes que regulan en cada país la llamada conservación de datos, por las que existe una obligatoriedad por parte de los proveedores de servicios de Internet o ISP (*Internet Service Provider*) de conservar ciertos datos de nuestras conexiones a Internet, como puede ser la relación dirección IP (*Internet Protocol*) —datos del cliente que ha hecho uso de ella— y momento en el que lo hizo, y que permite a las fuerzas y cuerpos de seguridad, bajo solicitud judicial, avanzar en las investigaciones relacionadas con delitos que tuvieron en algún momento una actividad en el ciberespacio. La conclusión que se produzca en la sociedad ante el debate entre privacidad y seguridad y que en muchos casos viene condicionado por los aspectos culturales, históricos y políticos del país, va a afectar de forma determinante que en un país exista una ley de conservación de datos y la especificación de tiempo para el mantenimiento de estos. Es por ello que la situación a nivel mundial es heterogénea, lo que dificulta enormemente la persecución de ciberdelitos, si tenemos en cuenta además que este es global y los ciberataques se pueden estar lanzando a miles de kilómetros de distancia e infectando en el camino a numerosos sistemas de diferentes países.

- Es un espacio vulnerable. Todas las tecnologías, ya estén formadas por *software* (SW), *hardware* (HW) o una combinación de ambas, pueden contener errores en su diseño o incluirlos en el proceso de su desarrollo. Estas vulnerabilidades una vez que han sido descubiertas pueden ser explotadas para la realización de acciones no autorizadas, como pueden ser entre otras el robo de información o la disrupción del sistema. Solo en lo que llevamos del presente año se han publicado más de 13.200 vulnerabilidades sobre productos TIC a nivel mundial (NIST, 2017).
- Estas características del ciberespacio contribuyen además a que éste presente asimetría, es decir, que acciones diseñadas y desarrolladas con muy bajo coste y en poco tiempo puedan producir potencialmente

altos impactos. Los ciberataques a Estonia en el año 2007 o más recientemente el apagón eléctrico que se produjo en diciembre de 2015 en Ucrania son ejemplos de ello.

Todas estas características se han mantenido constantes a lo largo del desarrollo y evolución de Internet, lo que ha sido aprovechado por países, organizaciones criminales y delincuentes para realizar acciones que hasta el momento se venían haciendo en el mundo físico y que en el ciberespacio pueden desarrollarse de forma más rápida, barata y con menos riesgo a ser identificado.

Las amenazas que afectan al entorno físico tradicional pueden aplicarse igualmente a este nuevo dominio que es el ciberespacio. Así, el espionaje que usa el ciberespacio como medio o como fin pasa a llamarse ciberespionaje, la guerra o el conflicto que puede materializarse en el ciberespacio pasan a llamarse ciberguerra y ciberconflicto respectivamente, y así podríamos seguir con el resto de amenazas que pueden utilizar Internet como medio para cometer una acción o como fin en sí mismo.

Solo en el año 2016 las Fuerzas y Cuerpos de Seguridad tuvieron constancia de 66.586 delitos informáticos en España, un 10,7 por 100 más que en el año 2015, siendo el 68,9 por 100 correspondiente a fraudes informáticos y el 17,2 por 100 a amenazas y coacciones (Ministerio del Interior, 2017).

Hasta las recientes crisis de *WannaCrypt* y *Petya*, que han tenido un impacto mediático a nivel mundial, son muchos los ciberataques que han tenido lugar y que han generado un impacto importante tanto en ciudadanos, empresas, Administraciones Públicas e incluso a nivel de país. Los ciberataques a Sony, el robo de información de los clientes de la red de contactos extramatrimoniales Ashley Madison, el robo masivo de información de clientes en grandes almacenes incluyendo los datos de tarjetas de crédito, el código malicioso *Stuxnet* que supuestamente pudo ralentizar el programa de enriquecimiento de uranio en Irán y la *botnet* Mirai que, por primera vez en la historia, utilizó dispositivos IoT vulnerables para realizar un ciberataque, son ejemplos de ciberataques con una repercusión internacional y que, con motivaciones diferentes, produjeron graves situaciones.

No obstante, hay uno de ellos que destaca por ser la primera vez en la historia que una serie de ciberataques impacta seriamente a nivel país: los ciberataques a Estonia en el año 2007.

El 26 de abril del año 2007, coincidiendo con los trabajos preparatorios para el traslado de la estatua conocida como el «soldado de bronce», en la capital Tallin, estatua considerada por la comunidad estonia de origen ruso como un símbolo a los soldados soviéticos caídos durante la Segunda Guerra Mundial, Estonia comienza a sufrir una serie de ciberataques que afectan gravemente al país durante varias semanas.

Si bien hasta mayo de 2006 la situación en torno a la estatua era de normalidad y la comunidad de origen ruso utilizaba la plaza y el monumento como un lugar de celebración, es a partir de esa fecha, a raíz de un incidente entre simpatizantes extremistas de grupos prosoviéticos y proestonios cuando la situación se crispa y empiezan a surgir manifestaciones nacionalistas con posiciones enfrentadas.

Coincidiendo con estos trabajos preparatorios de traslado, se organizó por la mañana una manifestación pacífica de protesta en la plaza del soldado de bronce que según avanzó el día se tornó en numerosos actos violentos que se alargaron por la noche y parte de la mañana del día 27.

El día 27 de abril de 2007, mientras continuaban los disturbios en las calles, Estonia comenzaba a sufrir ciberataques contra sistemas informáticos del ámbito público, privado y medios de comunicación. Los objetivos de estos ciberataques eran varios: desde la disrupción y bloqueo de sistemas informáticos y sitios webs del Gobierno, del Parlamento y diferentes Administraciones Públicas, hasta los sistemas de banca electrónica de los principales bancos nacionales y la modificación de páginas webs oficiales, incluyendo propaganda prorrusa y en lengua rusa.

Los ciberataques se prolongaron hasta el 18 de mayo y fueron evolucionando en cuanto a complejidad, bloqueando el funcionamiento de muchos servicios importantes del país. Estonia, país miembro de la Organización del Tratado del Atlántico Norte (OTAN), era ya entonces un país con una alta dependencia tecnológica en el que, por ejemplo, alrededor del 90 por 100 de las transacciones bancarias que se realizaban se hacían de forma electrónica (Néstor, 2011).

Este ciberataque propició una reflexión en el seno de la OTAN en torno al principio de defensa colectiva, el cual es una de las piedras angulares del tratado fundacional de la OTAN, uniendo a sus miembros y estableciendo un espíritu de solidaridad colectiva.

El artículo 5 de la OTAN establece que: «Las Partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte.

Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán, inmediatamente, en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales» (NATO, 2017).

Lo que estaba sufriendo Estonia era un ataque al país a través de un ciberataque a sus sistemas informáticos, con un impacto importante en el funcionamiento de las instituciones y en la propia vida de los ciudadanos. Las discusiones que en el seno de la OTAN se desarrollaron pusieron de nuevo de relieve las terribles consecuencias que un ciberataque podría tener en la seguridad global y, por lo tanto, la posibilidad de considerarse un «ataque armado», tal como contempla el artículo 5. No obstante, a diferencia de un ataque armado en el mundo físico, la atribución de un ciberataque no siempre es posible, lo que podría impedir desarrollar una respuesta.

3. Ciberseguridad en España

Desde la incorporación de las TIC en nuestras administraciones, empresas y en general en nuestra vida diaria, la preocupación por la ciberseguridad siempre ha estado presente de un modo u otro en nuestro país y, tanto desde el ámbito público como el privado, se han llevado a cabo numerosas acciones para proteger las redes y sistemas contra ataques externos e internos.

Entre las de carácter normativo o legal y a modo de ejemplo, ya la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y posteriormente el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN), asignan al CCN, entre otras misiones, la de garantizar la seguridad de las tecnologías de la información en el ámbito de la Administración. En el ámbito de la protección de la infraestructuras críticas, la creación en el año 2007 del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) del Ministerio del Interior y más adelante la aprobación de la Ley 8/2011, de 28 de abril, de Protección de Infraestructuras Críticas, permite a nuestro país disponer de las estrategias y estructuras adecuadas para dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, incluyendo los aspectos de ciberseguridad.

No obstante, no es hasta diciembre de 2013 cuando, promovida por el Consejo de Seguridad Nacional, se produce la aprobación de la Estrategia de Ciberseguridad Nacional. Con una visión integral de la ciberseguridad, esta establece formalmente los principios rectores de la ciberseguridad en nuestro país así como los objetivos

y líneas de acción necesarios para desarrollar las previsiones que, en materia de protección, establece la Estrategia de Seguridad Nacional.

En línea con las estrategias de ciberseguridad de países de nuestro entorno y que tienen también una alta dependencia tecnológica, la Estrategia de Ciberseguridad Nacional incide en la necesidad de conocer las amenazas a las que está sometido el ciberespacio, la necesidad de gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta.

El liderazgo nacional y coordinación de esfuerzos, la responsabilidad compartida, la proporcionalidad, racionalidad y eficacia, así como la cooperación internacional, son los principios rectores de una estrategia que está sirviendo de modelo a seguir para otros países que están inmersos en el proceso de desarrollo de sus estrategias nacionales y que además España está apoyando intensamente ya que, como se establece en uno de sus objetivos, es necesario trabajar en la mejora de la ciberseguridad en el ámbito internacional.

La ampliación y mejora de los centros de respuesta ante incidentes de ciberseguridad informáticos o CERT (*Computer Emergency Response Teams*), que juegan un papel fundamental en la ciberseguridad nacional permitiendo la alerta temprana y la detección proactiva de incidentes, es uno de los objetivos de esta Estrategia. Así, el papel del CERT de las Administraciones Públicas (CCN-CERT), el del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) en la protección de las redes militares y del Ministerio de Defensa y el del CERT de Seguridad e Industria (CERTSI), operado por INCIBE bajo la coordinación del propio INCIBE y el CNPIC, en la protección de los ciudadanos y sector privado, son una prioridad y aspecto fundamental en la ciberseguridad nacional.

Desde el CERTSI se han gestionado miles de incidentes de ciberseguridad en los últimos años que han afectado a numerosos ciudadanos y empresas. Así, desde el CERTSI se gestionaron cerca de 18.000 incidentes en el año 2014, casi 50.000 en el año 2015 y más de 115.000 en el año 2016, siendo los relativos a operadores críticos 62, 134 y 479 respectivamente (Gráfico 1).

En lo que llevamos de año, desde el CERTSI se han gestionado más de 100.000 incidentes de ciberseguridad, lo que, de continuar con la tendencia en lo que queda de año, 2017 será el año que más incidentes de ciberseguridad se habrán gestionado en España en lo que se refiere a ciudadanos y sector privado.

Este incremento en el número de incidentes responde fundamentalmente a tres factores:

- El primero de ellos, a una mejora considerable de las capacidades de detección de las que dispone el centro. Las inversiones realizadas en los últimos años han permitido mejorar la tasa de detección, manteniendo inalterable un aspecto fundamental: la privacidad de nuestros ciudadanos y empresas. Esta detección se realiza sin la monitorización de la actividad de los usuarios en Internet, recurriendo por tanto a la potenciación del intercambio de información en el marco de acuerdos internacionales y el trabajo con las empresas de ciberseguridad.
- En segundo lugar, el aumento del conocimiento y confianza que los ciudadanos y sector privado tienen en relación a los servicios del CERTSI. Si bien en los primeros años de operación del CERTSI más del 90 por 100 de los incidentes gestionados fueron detectados por el centro y menos del 10 por 100 fue comunicado por el afectado, esta diferencia se va reduciendo poco a poco.
- Por último, es un hecho que el número de ciberataques que se está produciendo a nivel mundial se está incrementando año a año. Las características que el ciberespacio presenta, y de las que hemos hablado anteriormente, hace que este sea un dominio muy interesante para cometer delitos de toda índole.

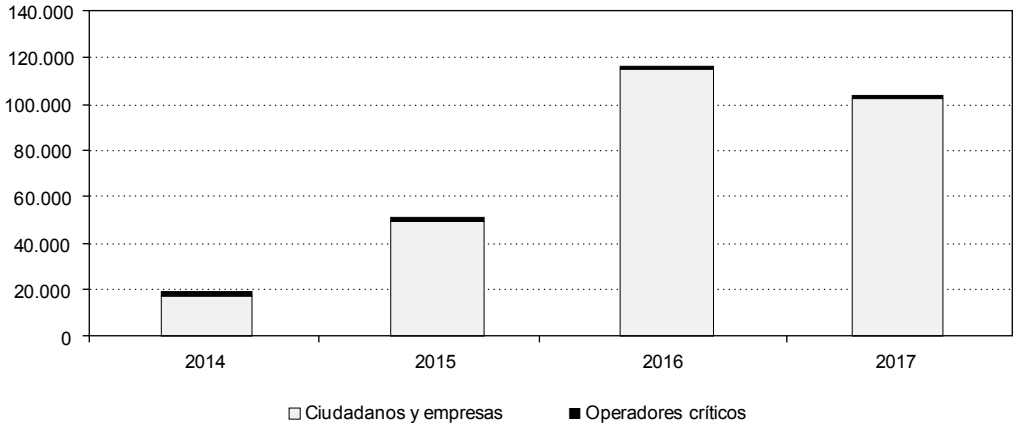
En cuanto a las motivaciones que hay detrás de cada uno de estos incidentes, los análisis del CERTSI indican que estas son variadas, pero predominan las de carácter económico (Gráfico 2).

En nuestro país y a nivel de ciudadanos y sector privado nos encontramos con tres situaciones mayoritarias:

— Incidentes relacionados con fraude, con una clara motivación económica y utilizando multitud de técnicas,

GRÁFICO 1

INCIDENTES DE CIBERSEGURIDAD EN CIUDADANOS Y EMPRESAS GESTIONADOS POR CERTSI, 2014-2017



FUENTE: CERTSI, INCIBE.

algunas de ellas técnicamente poco sofisticadas, pero que producen un gran impacto en cuanto a número de empresas o personas a las que se les sustrae dinero. Entre ellas nos encontramos por ejemplo con:

● Ciberataques que mediante el envío de correos electrónicos, suplantando la imagen de nuestro banco (técnica denominada *phishing*), nos solicitan que nos conectemos a su página web pinchando el enlace que se incluye en el correo, con la excusa de que debemos confirmar algún dato de nuestra cuenta. El enlace no corresponde en realidad a la página del banco sino a otra con la misma imagen pero controlada por los atacantes y que persigue el hacerse con nuestros datos de usuario, contraseña y tarjeta de coordenadas para posteriormente sustraernos dinero de nuestra cuenta.

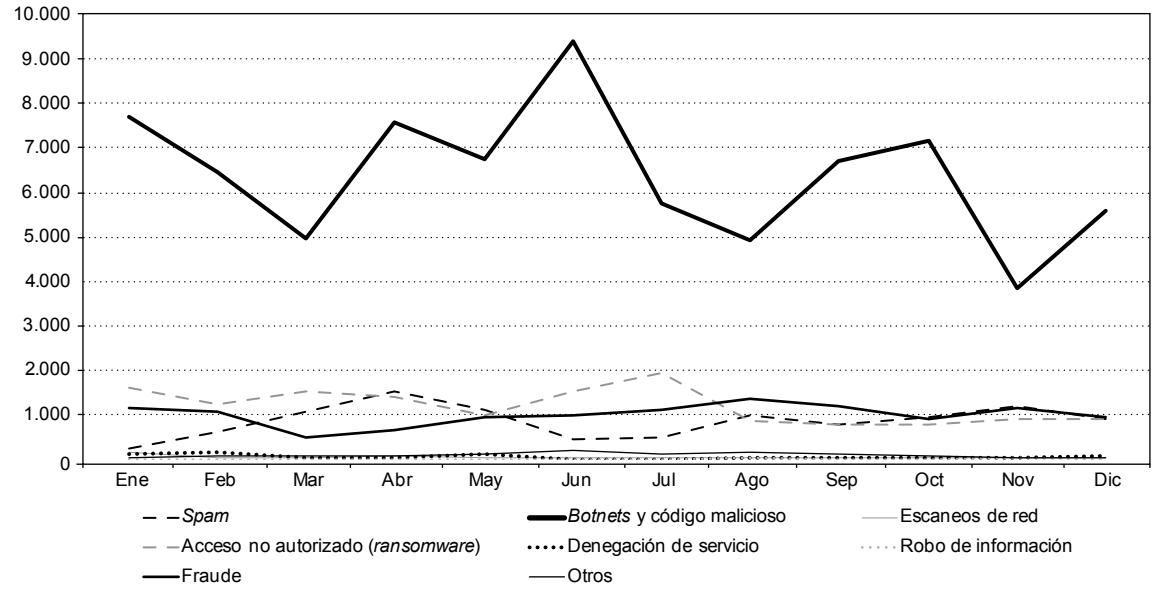
● Incidentes conocidos como «fraude del CEO» (*Chief Executive Officer*) y que en el último año está teniendo cierto impacto en España. En este ciberataque el responsable financiero de una determinada empresa recibe un correo electrónico suplantando al Director General, CEO o Consejero Delegado de la misma, pidiendo que se haga una transferencia internacional con carácter de urgencia aduciendo un asunto importante. La confianza en el origen del correo, unido a la urgencia del mismo, hace que en muchos casos el empleado que recibe el correo realice la transferencia sin hacer comprobaciones adicionales.

● Todo tipo de estafas en alquileres anunciados por Internet, falsas ofertas de trabajo que al final del proceso llevan a pedirnos dinero por alguna razón, prestamistas falsos, etc., son otros ejemplos de acciones fraudulentas que tienen incidencia en España.

— Incidentes relacionados con redes de *botnets*, un tipo de código malicioso cuyo *modus operandi* consiste en la infección de miles de ordenadores, denominados a partir de ese momento *bots* o zombis y que son controlados por el atacante a través de un panel remoto denominado de mando y control o C2 (*Command & Control*), que intenta pasar desapercibido y no ser detectado durante el mayor tiempo posible y así poder realizar numerosas

GRÁFICO 2

INCIDENTES POR TIPO GESTIONADO POR CERTSI, 2016



FUENTE: CERTSI, INCIBE.

acciones no autorizadas como: el robo de información privada, infección de otros ordenadores, lanzamiento de ataques de denegación de servicio distribuido o DDoS (*Distributed Denial of Service*) a otros sistemas, uso de la capacidad de proceso para la generación de criptomonedas, etc.

El CERTSI viene comprobando en los últimos años que las *botnets* con mayor número de ordenadores infectados en España corresponden a códigos maliciosos desarrollados hace tiempo, en algunos casos incluso hace más de diez años, y para los que existe solución y medidas de protección, lo que nos indica que el nivel de concienciación, en general, aún es bajo.

— Incidentes relacionados con *ransomware*, como ha sido *WannaCrypt* o *Petya*. Estos ciberataques tienen también una motivación económica clara utilizando la extorsión para conseguir dinero. Generalmente, mediante la recepción de un correo electrónico suplantando a nuestro banco, proveedor de energía eléctrica, operadora de telecomunicaciones, alguna Administración Pública, etc., nos lleva a hacer clic en un enlace y descargar y ejecutar un fichero, lo que produce el cifrado de todos los ficheros de nuestro ordenador y, en muchos casos, de toda la Red, solicitando un rescate mediante el pago con criptomonedas, por ejemplo *bitcoin,* para descifrarlo. El denominado «virus de la policía» o la denominada *«c*ampaña de Endesa*»* son dos ejemplos de incidentes masivos que han tenido lugar en España y que afectaron a muchos de nuestros ciudadanos y empresas.

De forma general, el éxito de los ciberataques a nivel de ciudadano y empresa tiene más que ver con el bajo conocimiento y concienciación de estos en materia de ciberseguridad que con la sofisticación de los mismos.

El nivel de desconfianza que aplicamos en el conjunto de nuestras acciones profesionales y relaciones personales en el mundo físico disminuye considerablemente cuando estas tienen lugar en el ciberespacio o Internet. La falsa sensación de seguridad que podemos tener cuando estamos sentados en nuestra casa o en nuestro puesto de trabajo es un factor clave a la hora de bajar ese nivel de alerta y desconfianza cuando estamos conectados en el ciberespacio.

Ante el incremento y sofisticación de las ciberamenazas, y en contra de lo que pudiese parecer, las normas básicas de ciberseguridad se han mantenido casi inalterables. Hacer un uso responsable de la tecnología, desconfiar de todas aquellas personas que no conocemos, mantener actualizado el *software* tanto del sistema operativo como de las aplicaciones que tenemos instaladas, seleccionar contraseñas robustas y cambiarlas cada cierto tiempo y no compartirlas, tener un antivirus instalado y conservar una copia de seguridad en caso de incidente, son un ejemplo de medidas básicas que siguen siendo válidas y podrían evitar un porcentaje muy elevado de los incidentes de ciberseguridad que están afectando a nuestros ciudadanos y empresas.

La concienciación, por tanto, es un aspecto fundamental a la hora de prevenir y mejorar el nivel de ciberseguridad. Es importante destacar que para que la concienciación sea efectiva tiene que pasar por al menos tres fases:

- Conocimiento. Es necesario conocer la existencia de las ciberamenazas y necesario realizar un trabajo para protegerse frente a ellas. En este punto, quizá la reciente crisis de *WannaCrypt* ha mejorado sustancialmente el nivel de conciencia colectiva acerca de que los problemas de ciberseguridad son una realidad.
- Comprensión. Es necesario que el problema, además de conocerlo, se entienda. La ciberseguridad ha sido generalmente entendida como una rama técnica restringida a los profesionales que en ella trabajan. Recordemos la imagen extendida, a veces incluso romántica, de un *hacker* adolescente trabajando en su casa sin salir de la habitación, desarrollando cosas incomprensibles para los demás. Sin embargo, la realidad es bien distinta: todos utilizamos tecnología y todos tenemos que conocer y entender sus riesgos para afrontarlos y hacer un uso seguro de ella.
- Interiorización. Incluso si ya hemos pasado por los estados anteriores y pensamos que conocemos y entendemos los riesgos y lo que hay que hacer para protegerse, la pregunta entonces es: ¿hemos interiorizado lo que debemos hacer y lo hacemos de forma automática? Son muchas las personas que reconocen que no. Abrocharse el cinturón de seguridad en un vehículo antes de empezar a circular es una acción que ejecutamos de forma casi automática por motivos de seguridad; sin embargo, en el uso de las tecnologías aún no hemos adoptado de forma general ciertos hábitos de ciberseguridad necesarios.

4. El mercado de la ciberseguridad en cifras

La ciberseguridad no solo presenta un problema para las sociedades y sus economías, sino que supone una gran oportunidad de desarrollo. El sector de la ciberseguridad está teniendo en los últimos años un crecimiento anual que supera el 10 por 100 a nivel mundial y que, de acuerdo con los datos de la compañía Gartner Inc., podrá alcanzar en el año 2018 una facturación anual de 79.292 millones de euros.

En el caso de España, de acuerdo con los estudios realizados por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), la previsión del crecimiento en el gasto a tres años será del 22 por 100, siendo la facturación estimada para el año 2018 de 956.000.000 de euros.

En cuanto al número de empleos que el sector de la ciberseguridad proporciona a día de hoy, existe a nivel mundial una mayor demanda de profesionales que de oferta. De acuerdo con el estudio del Center for Strategic and International Studies (CSIS), en el año 2019 existirán entre 1.000.000 y 2.000.000 de puestos de trabajo no cubiertos a nivel mundial. Solo

en EE UU y en el año 2015, 209.000 puestos de trabajo relacionados con la ciberseguridad se quedaron sin cubrir.

En el caso de España, en el año 2014 se contabilizaban un total de 5.808 empleos en un total de 533 empresas *pure players* de ciberseguridad y empresas TIC que también prestaban servicios y/o productos de ciberseguridad (ONTSI, 2015). Solo en el año 2016, de acuerdo con el informe del mercado laboral en España elaborado por InfoJobs y ESADE, hubo 1.270 vacantes de especialistas de ciberseguridad con una media de 20 candidatos por puesto. En el foro de formación y empleo del evento CyberCamp organizado por INCIBE en la ciudad de León en diciembre de 2016, se publicitaron más de 2.200 ofertas formativas y de trabajo, para las que se recibieron menos de 900 *curriculum vitae*, lo que pone de relieve que esta brecha está también teniendo lugar en nuestro país.

Datos como estos indican que el sector de la ciberseguridad constituye una verdadera oportunidad para la creación de nuevas empresas, el desarrollo de las existentes y, en definitiva, para la generación de empleo.

El sector de la ciberseguridad es sin duda un nuevo sector profesional puesto que, si bien el perfil profesional en el ámbito de la ciberseguridad siempre se ha asociado con un perfil técnico, la demanda de profesionales de otras áreas de conocimiento con formación adicional o específica en ciberseguridad está aumentando día a día. Psicólogos que ayuden a las víctimas de agresiones o extorsiones en Internet, como puede ser el caso de los menores, pedagogos que ayuden a trasladar y hacer entendibles las recomendaciones de protección y uso seguro de las tecnologías, directores de comunicación que trasladen los mensajes adecuados para que sean comprensibles ante una crisis de ciberseguridad como pudimos ver en el caso de *WannaCrypt*, periodistas que informen y transmitan de forma clara a los ciudadanos qué está pasando cuando se está produciendo una crisis por un ciberataque, son ejemplos de perfiles profesionales que ya a día de hoy se están requiriendo en el mercado.

5. Tendencias en ciberseguridad

Conocer las nuevas necesidades y próximos avances tecnológicos, así como las amenazas asociadas, es fundamental a la hora de asegurar a medio y largo plazo los niveles mínimos de protección necesarios para nuestra sociedad.

De acuerdo con el estudio desarrollado por INCIBE en el año 2016: *Tendencias en el mercado de la ciberseguridad*, se han identificado 20 tendencias de ciberseguridad con una alta probabilidad de implantación en España.

- En el ámbito industrial, se prevé que se desarrollarán soluciones y servicios orientados a la protección de las *smart grids*, que mejoren la capacidad de resistir y recuperarse ante un ciberataque (ciberresiliencia) de las infraestructuras críticas, así como que protejan los sistemas de control industrial y SCADA (*Supervisory Control and Data Acquisition*).
- En el ámbito de la movilidad, aumentará la necesidad de protección de las comunicaciones y los transportes, fundamentalmente el aéreo y terrestre.
- En el sector financiero y de seguros y ante la digitalización de sus servicios, como puede ser la banca *online*, se desarrollarán soluciones que aprovechen las ventajas que la generación masiva de datos presenta y que permitan una mejora de la detección del fraude y la protección de los sistemas.
- En el ámbito sanitario, los avances en la ciberseguridad irán orientados a la protección de los dispositivos médicos conectados, la protección de la información sensible de los pacientes, así como las patentes que se están desarrollando y cuya divulgación produciría grandes pérdidas económicas.
- La formación será también un campo de desarrollo y de oportunidad para la creación de empresas especializadas, puesto que deberá cubrir tanto la formación básica como aquella especializada que permita abarcar la gran demanda de profesionales expertos en ciberseguridad. El desarrollo de capacidades de adiestramiento mediante ciberejercicios constituye

otra tendencia que ya a día de hoy numerosas organizaciones están demandando.

- El avance en las capacidades de ciberinteligencia que permitan mejorar la alerta temprana, unida al avance en los métodos de cifrado en tiempo real, ciberseguridad en dispositivos IoT y la ciberseguridad en los servicios en la nube son otras tendencias que a día de hoy ya empiezan a ser una realidad.

Estas tendencias de ciberseguridad darán respuesta a las necesidades de protección que el desarrollo tecnológico y el auge de grandes ciudades autosuficientes, sedes de talento, inversión y de creación de riqueza y crecimiento económico, requerirán en los próximos años.

La incorporación de tecnología dotará de inteligencia a estas ciudades, las cuales estarán hiperconectadas, permitiendo además exportar los avances que allí se produzcan a otras zonas del mundo. Los avances tecnológicos permitirán además la mejora de la calidad de vida y el aumento de la longevidad e incluso la mejora del coeficiente intelectual y la capacidad de aprendizaje o recuperación de la audición y la visión. Si bien la economía se sustenta en un número reducido de multinacionales y un gran grupo de pequeñas y medianas empresas, en el ámbito TIC y de ciberseguridad las pequeñas empresas podrán jugar un papel importante, dado que un aspecto intrínseco al desarrollo TIC y de la ciberseguridad es la innovación disruptiva. Solo echemos un vistazo atrás y podremos comprobar entonces que compañías como WhatsApp, Amazon, Facebook o Twitter, entre otras, nacieron hace muy pocos años basándose en una idea innovadora y a día de hoy son grandes multinacionales que lideran el proceso de transformación tecnológico y de la sociedad en su conjunto. El desarrollo de nuevos métodos de pago que la sociedad demanda, el despliegue de servicios en la nube y la total incorporación de la tecnología en los procesos productivos en el ámbito industrial o Industria 4.0, estarán igualmente condicionados a la existencia de unos niveles adecuados de ciberseguridad.

Referencias bibliográficas

[1] BOLETÍN OFICIAL DEL ESTADO (2017). *Código de Derecho de la Ciberseguridad. Edición actualizada a 9 de marzo de 2017. Disponible en http://www.boe.es/legislacion/codigos/*

[2] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (2016*). Hacking the Skills Shortage. A Study of the International Shortage in Cybersecurity Skills*, Washington, DC.

[3] DEPARTAMENTO DE SEGURIDAD NACIONAL, PRESIDENCIA DEL GOBIERNO (2013). *Estrategia de Ciberseguridad Nacional, España.*

[4] GANUZA ARTILES, N. (2011). «La situación de la ciberseguridad en el ámbito internacional y en la OTAN. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio». *Cuadernos de estrategia*, nº 149, pp. 165-214, Madrid.

[5] INFOJOBS y ESADE (2017). *Estado del mercado laboral en España.*

[6] INSTITUTO NACIONAL DE CIBERSEGURIDAD (2016). *Tendencias en el mercado de la ciberseguridad*, León.

[7] INTERNATIONAL TELECOMMUNICATION UNION (2017). *ICT Facts and Figures 2017.*

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2017). *National Vulnerability Database*. NIST. Recuperado el 10 de septiembre de 2017 de *https://nvd.nist.gov/*

[9] NORTH ATLANTIC TREATY ORGANIZATION (2017). Collective Defence – Artículo 5. NATO. Recuperado el 10 de septiembre de 2017 de *http://nato.int/cps/en/natohq/topics_110496.htm?selectedLocale=en*

[10] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (2016). *Caracterización del subsector y el mercado de la ciberseguridad 2015*, Madrid. ONTSI.

[11] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (2016). *La sociedad en red 2015.* Informe anual. Edición de 2016, Madrid. ONTSI.

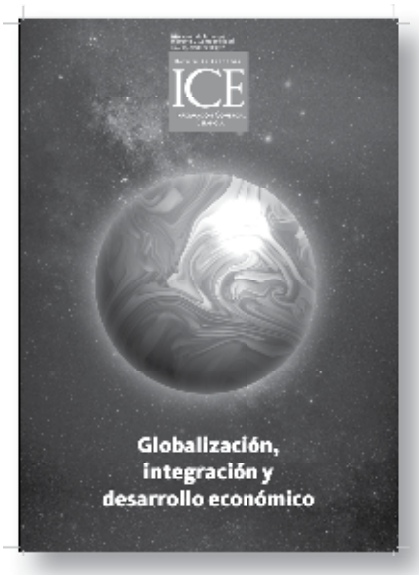
[12] SECRETARÍA DE ESTADO DE SEGURIDAD, MINISTERIO DEL INTERIOR (2016). *Estudio sobre la cibercriminalidad en España*.

[13] WE ARE SOCIAL (2017). 2017 *Digital YearBook: Digital Data for Every Country in the World, Londres. WAS. Disponible en https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview*

ICE

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD **INFORMACIÓN COMERCIAL ESPAÑOLA** *Secretaría de Estado de Comercio*

Últimos números publicados



www.revistasice.com
Librería virtual, suscripción y venta: www.mineco.gob.es
Pº de la Castellana, 162. 28046 Madrid.
Telf. 91 603.79.97/93
distribucionPublicaciones@mineco.es