CIBERSEGURIDAD EN LA SOCIEDAD DIGITAL

ALBERTO URUEÑA
ANTONIO HIDALGO
Universidad Politécnica de Madrid

La preocupación por la seguridad de la información aumenta año tras año en los hogares españoles. En el segundo semestre de 2016 (Kaspersky Lab, 2017), en España aumentó el número de internautas preocupados por la ciberseguridad, pasando del 28% al 39%. Ante este dato cada vez son más los usuarios de Internet que adoptan medidas de protección contra las ciberamenazas.

Esta investigación comienza analizando los principales informes nacionales e internacionales en materia de ciberseguridad, analizando las principales amenazas y medidas de seguridad, utlizando fuentes de datos secundarias públicas y privadas para, en los epígrafes finales, explicita un conjunto de conclusiones y recomendaciones que puedan resultar de utilidad en materia de seguridad en Internet.

LAS TIC Y LA SEGURIDAD EN LOS HOGARES ESPAÑOLES

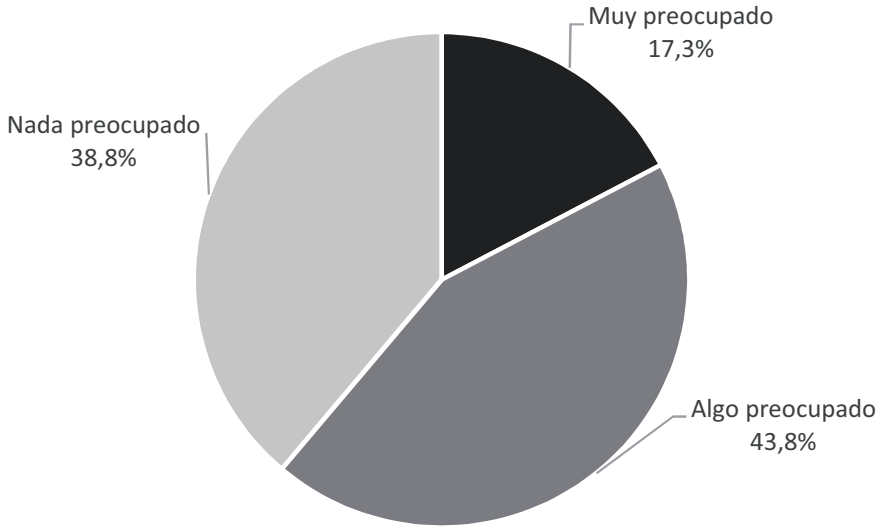
La protección contra las ciberamenazas

El usuario final es uno de los factores clave en la seguridad cibernética. Los expertos en seguridad informática continúan advirtiendo sobre el peligro del uso de ordenadores e Internet si no se siguen unas normas básicas de seguridad. En definitiva, las conductas de riesgo de los usuarios influyen en las amenazas potenciales que afectan a los ordenadores (Herrero *et al*., 2017a). También algunos estudios han apuntado que la combinación de uso intensivo de un *smartphone* (teléfono inteligente) con un bajo nivel de apoyo social se relaciona de manera positiva y significativa con la existencia de *malware* y con niveles más altos de actitudes de riesgo hacia el uso del *smartphone* (Herrero *et al*., 2017b).

En 2016, el 64% de la población de España ya utilizaba algún tipo de *software* de seguridad (anti-virus, *anti-spam*, *firewall*, etc.) con el objetivo de proteger los datos privados y el ordenador personal (Instituto Nacional de Estadística, 2016), cifra que se incrementó en 2,4 puntos porcentuales respecto a 2015. Además, el 71,6% de los ciudadanos españoles que han utilizado Internet durante el último año actualizaron en 2016 sus productos de seguridad informática (antivirus o programas de detección de espías), lo que pone de manifiesto que los españoles están cada vez más preocupados por la seguridad, ya que este indicador también se incrementó en 2,8 puntos porcentuales respecto al año 2015.

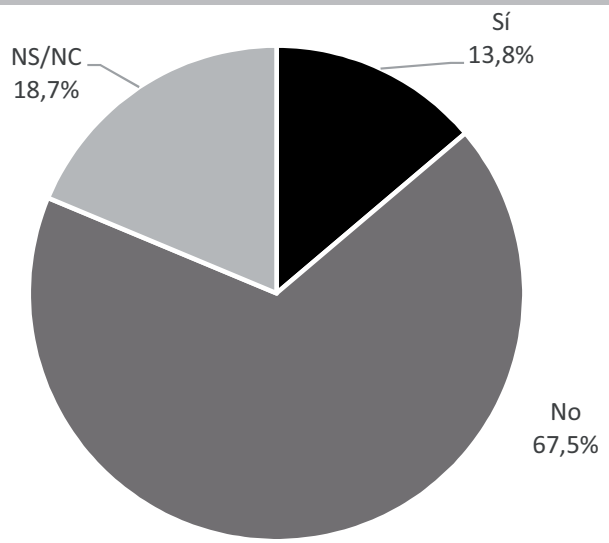
Adicionalmente, el 17,3% de los ciudadanos españoles que se han conectado a Internet en 2016 afirman que están muy preocupados por el hecho de que sus actividades sean monitorizadas. Casi

GRÁFICO 1
INDIVIDUOS QUE HAN USADO INTERNET EN LOS ÚLTIMOS 12 MESES POR GRADO DE PREOCUPACIÓN RESPECTO A QUE SUS ACTIVIDADES *ONLINE* SEAN MONITORIZADAS (%)



Fuente: Elaboración propia con datos INE 2016

GRÁFICO 2
INDIVIDUOS QUE HAN USADO INTERNET EN LOS ÚLTIMOS 12 MESES QUE UTILIZAN UN *SOFTWARE* ANTI-RASTREO (%)

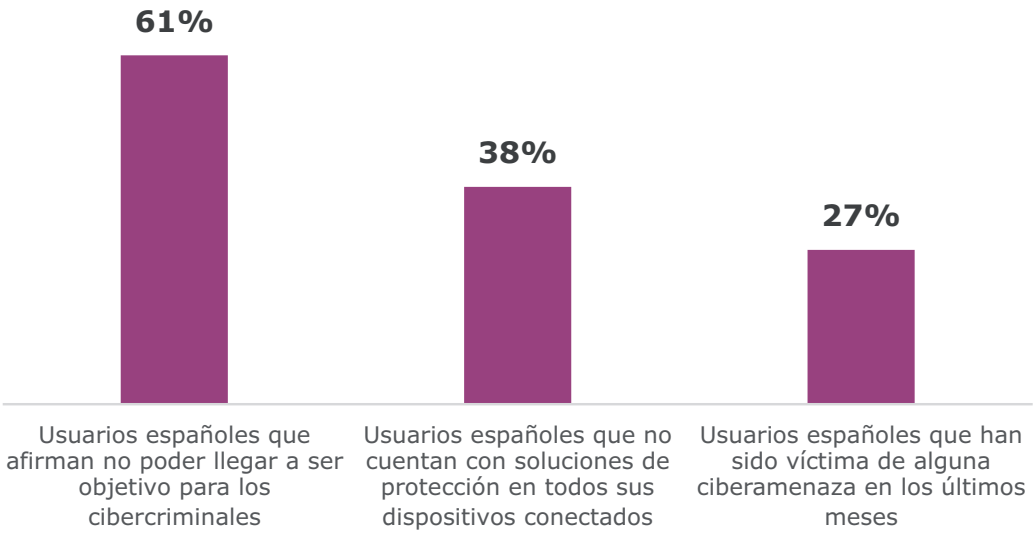


Fuente: Elaboración propia con datos INE 2016

la mitad de los individuos (43,8%) se muestra algo preocupado por ello, mientras que el 38,8% siente indiferencia o muy poca preocupación por que sus actividades en la red sean monitorizadas (Gráfico 1). Sin embargo, y aunque más de la mitad de los españoles está algo o muy preocupado por la seguridad, el 67,5% de los internautas no tiene ningún *software* anti-rastreo. Sólo un 13,8% de los internautas cuenta con uno de estos programas (Gráfico 2).

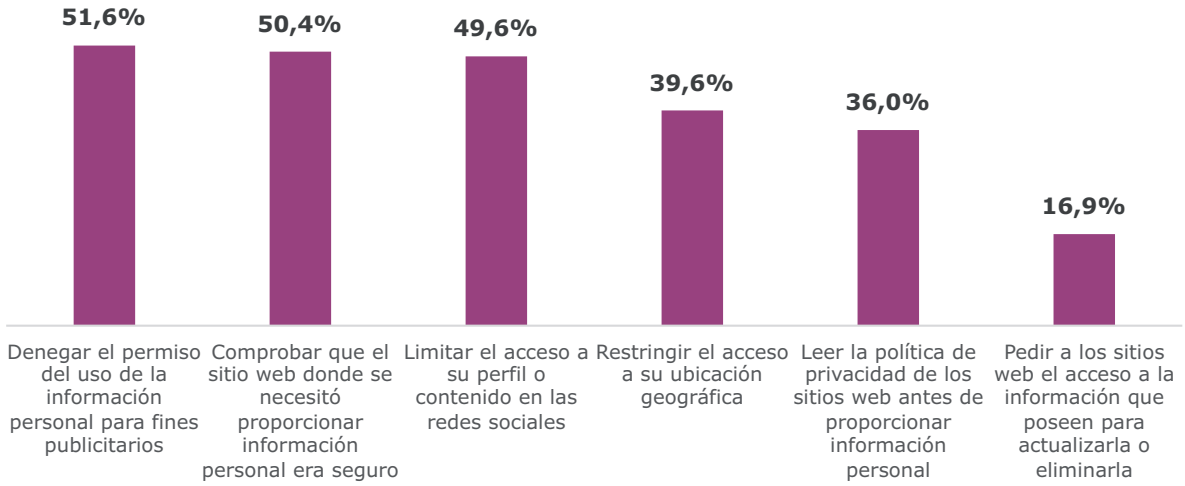
A pesar de la mayor concienciación y del progresivo aumento de medidas de seguridad en los hogares españoles, aún se detectan ciertas carencias. Según el índice Kaspersky Cibersecurity, el 61% de los usuarios españoles afirma que no cree poder llegar a ser objetivo para los cibercriminales, el 38% no cuenta con soluciones de protección en todos los dispositivos conectados, y el 27% reconoce haber sido víctima de alguna ciberamenaza en los últimos meses (Gráfico 3). En cuanto a la tipología de amenazas concretas, destacan el *malware* (18%), las cuentas pirateadas (6%), el *ransomware* (5%), los dispositivos hackeados (4%) y los datos filtrados (3%).

GRÁFICO 3
USUARIOS DESPREOCUPADOS, DESPROTEGIDOS Y DAMNIFICADOS EN ESPAÑA EN EL SEGUNDO SEMESTRE DE 2016 (%)



Fuente: Elaboración propia con datos del índice Kaspersky Cibersecurity 2017

GRÁFICO 4
INDIVIDUOS QUE HAN USADO INTERNET EN LOS ÚLTIMOS 12 MESES POR ACCIONES REALIZADAS PARA GESTIONAR EL ACCESO A LA INFORMACIÓN PERSONAL EN INTERNET (%)



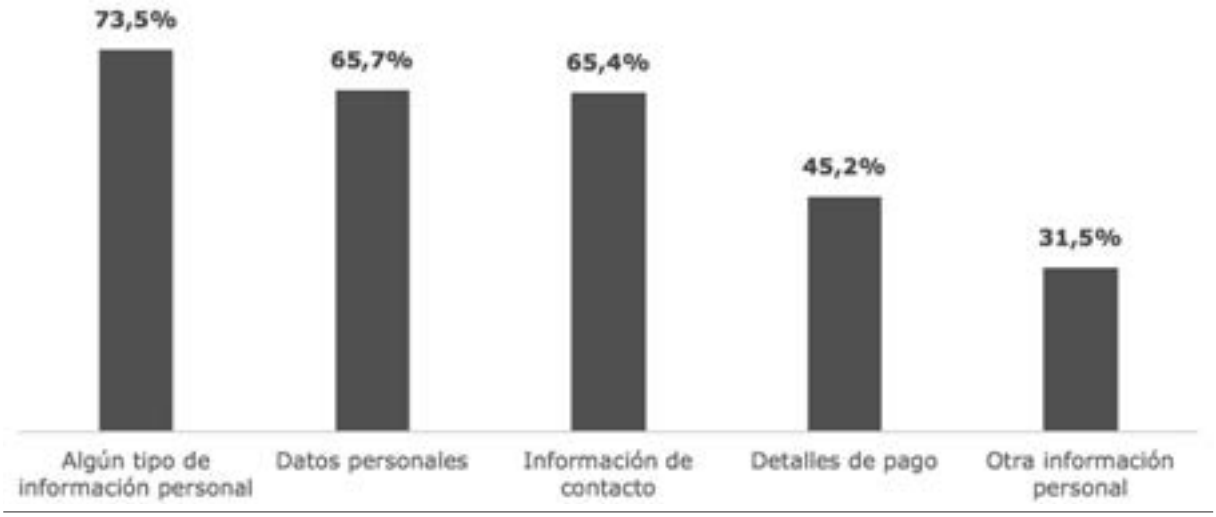
Fuente: Elaboración propia con datos INE 2016

La información personal en Internet

Una de las actividades más habituales para los usuarios españoles es la de facilitar sus datos o cualquier información personal a través de la Red. De entre todas las acciones existentes para gestionar el acceso a la información personal en Internet, denegar el permiso del uso de la información personal para fines publicitarios es realizada por el 51,6% de los internautas. A continuación se sitúan el hecho de comprobar que el sitio *web* donde se necesitó proporcionar información personal era seguro (50,4%) y la acción de limitar el acceso al perfil o contenido en redes sociales (49,6%). Además, el 39,6% de los individuos que usan Internet restringen el acceso a su ubicación geográfica y el 36% lee la política de privacidad de los sitios *web* antes de proporcionar información personal. Finalmente, los usuarios que piden a los sitios *web* el acceso a la información que poseen para actualizarla o eliminarla son solamente el 16,9% (Gráfico 4).

El 73,5% de los internautas han suministrado a través de la Red algún tipo de información personal en los últimos 12 meses. En cuanto al tipo de información personal, destacan los datos personales (nombre, fecha de nacimiento, número del documento de identidad, etc.) con un 65,7% de internautas. Muy cerca se sitúa la información de contacto (dirección, número de

GRÁFICO 5
INDIVIDUOS QUE HAN USADO INTERNET EN LOS ÚLTIMOS 12 MESES POR TIPO DE INFORMACIÓN PERSONAL SUMINISTRADA (%)



Fuente: Elaboración propia con datos INE 2016

teléfono, mail, etc.) con el 65,4%. Del mismo modo, el 45,2% de los usuarios de Internet en España proporciona información relacionada con el detalle del pago (número de tarjeta de crédito o cuenta bancaria). Finalmente, el 31,5% de estos individuos suministra otro tipo de información (fotos personales, ubicación actual, información relativa a la salud, etc.) (Gráfico 5).

Es importante resaltar que los ciudadanos españoles están cada vez más concienciados con el rastro que deja su navegación por Internet y cada vez están más familiarizados con términos como el de «cookies». De hecho, en 2016 el 62,9% de los internautas españoles sabían que las cookies pueden ser usadas para trazar los movimientos de una persona en Internet con el fin de obtener un perfil de cada usuario y proporcionarle publicidad adaptada o personalizada. Este dato aumentó 10,9 puntos porcentuales respecto a 2015. En esta misma línea, el 31% de los internautas españoles han cambiado alguna vez la configuración de su navegador de Internet con el fin de prevenir y limitar la cantidad de cookies en su ordenador.

Incidentes gestionados por el CCN-CERT

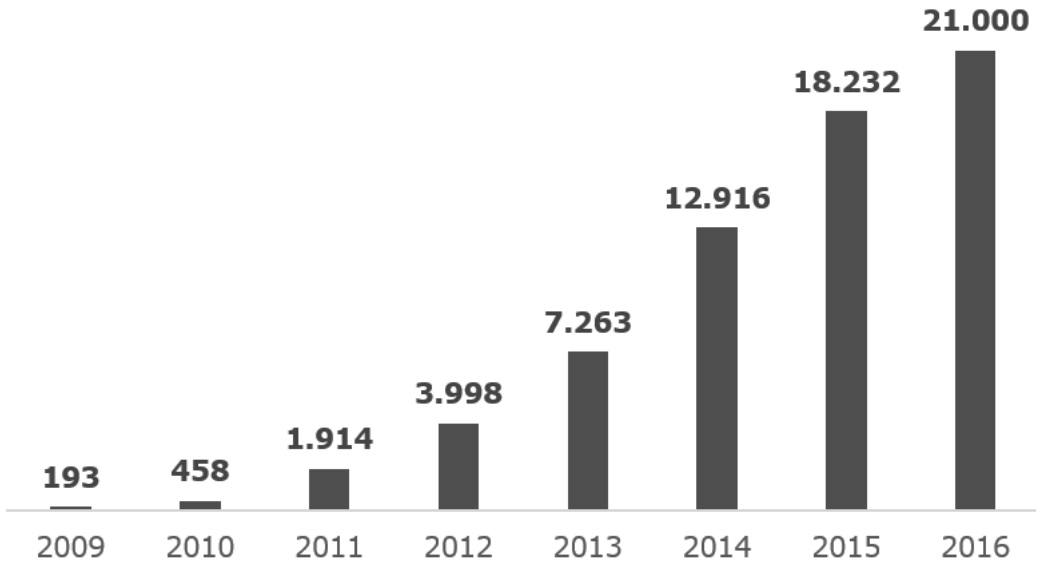
El CCN-CERT es la capacidad de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional. Este servicio se creó a finales del año 2006 como Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés *Computer Emergency Response Team*) gubernamental español y su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (central, autonómica y local).

En España se observa que en 2016 aumentó el número de ataques contra los sistemas de información de las Administraciones Públicas. Entre ellos destacan el incremento constante de las amenazas y ataques, la intrusión en todo tipo de dispositivos, con especial hincapié en los equipos móviles con un grado de protección mucho menor, el robo, el sabotaje o la infección a través de correo electrónico, páginas web o redes sociales. En este sentido, el impacto económico, los perjuicios a la reputación o a la privacidad de empresas, administraciones y ciudadanía, y la extorsión a través de medios tecnológicos siguen siendo un importante vector de afección para gobiernos, empresas y ciudadanos.

Tampoco hay que perder de vista la utilización de la amenaza terrorista que se beneficia de las oportunidades que les brinda el ciberespacio para, por un lado, realizar actividades de propaganda, comunicaciones internas, formación y adoctrinamiento, financiación, reclutamiento y obtención de información y, por otro, para llevar a cabo ataques contra sistemas informáticos de infraestructuras críticas o contra otros sistemas cuya vulneración suponga una alteración del normal funcionamiento de nuestra sociedad. Muchas de estas amenazas hacen uso de la web profunda (*deep web*) y de redes como TOR (*The Onion Router*) que continúan siendo facilitadoras de un amplio abanico de actividades delictivas y están cobrando una enorme importancia como medio donde imperan actividades englobadas en el marco del mercado negro. Así pues, de acuerdo con el gráfico 6, el número de incidentes gestionados por el CCN-CERT ascendió a 21.000 en el año 2016, un 15,2% más respecto a 2015, y 10 veces superior a la registrada en 2011 (1.914 incidentes) (Ministerio de la Presidencia, 2016).

El número de incidentes gestionados por los equipos de respuesta ante incidentes de seguridad de la información (CERT) nacionales en 2016 se muestra en sintonía con la tendencia internacional alcista. Es en el sector de los operadores estratégicos de la industria, incluyendo las infraestructuras críticas, en el que el aumento se

GRÁFICO 6
EVOLUCIÓN DEL NÚMERO DE INCIDENTES GESTIONADOS POR EL CCN-CERT (2009-2016)



Fuente: Elaboración propia a través del Departamento de Seguridad Nacional con datos del Ministerio de la Presidencia y para las Administraciones Territoriales. 2016

muestra más relevante, con cifras que triplican las de años precedentes.

Seguridad en el Internet de las cosas (IoT)

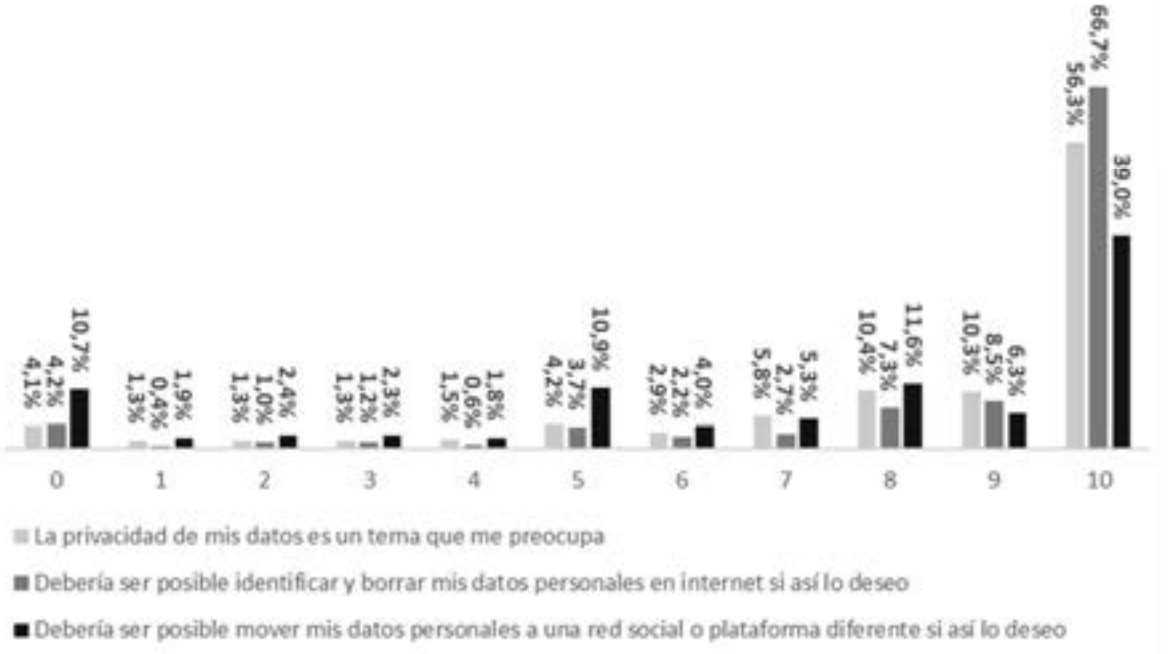
El proceso de digitalización de los servicios y de la economía, en general, implica importantes retos que conciernen a diferentes elementos del ecosistema digital. De entre los usuarios, las empresas suelen tener una mayor capacidad para afrontar estos retos ya que disponen de más recursos y suelen contar con especialistas en tecnologías de la información, motivo por el que el internauta individual se puede considerar la parte más débil de este ecosistema. En esta sección se analiza la percepción de los usuarios ante la seguridad, las amenazas que se presentan hoy y las medidas que los usuarios toman ante esta situación.

Según el estudio realizado por Fundación Telefónica en 2015 para conocer la percepción de los usuarios ante estos aspectos, los usuarios califican en una escala entre 0 y 10 su coincidencia con respecto a diferentes afirmaciones sobre privacidad: el 82,8% reconoce este tema como de gran importancia (valoran este aspecto entre 7 y 10), y más de la mitad, el 56,3%, lo valoran con la nota máxima. También el 10 es la puntuación más común cuando se pregunta a los internautas acerca de si debería ser posible identificar y borrar los datos personales de Internet, si así lo desea, y si debería ser posible mover los datos a otra plataforma o red social, con un 66,7% y un 39%, respectivamente. Ampliando este rango a las calificaciones entre 7 y 10, que indican un sentir muy favorable con respecto al enunciado, se observa que estas cifras suben hasta el 85,2% en el primer caso y al 62,2% en el segundo (Gráfico 7).

La información que los usuarios califican de personal y que no les gustaría que escapara de su control es muy variada, poniéndose de manifiesto que las mujeres dan a la privacidad una mayor importancia. Así, al 71,3% de los hombres y al 83% de las mujeres les preocupa mucho que fotografías y vídeos personales escapen de su control (valoración entre 7 y 10); al 79,6% de los hombres y al 87,2% de las mujeres que se escapen datos personales; al 60,8% de los hombres y al 74,1% de las mujeres que lo haga el historial de búsquedas; y al 58,4% de los hombres y al 71,9% de las mujeres, el historial de navegación (Gráfico 8). En todos los casos hay una diferencia de más de 10 puntos porcentuales para la mayoría de los tipos de información a favor de las mujeres, lo que refleja su mayor preocupación. Este comportamiento también se observa en las familias que tienen hijos pequeños, lo que demuestra que también poseen una sensibilidad especial con todos los aspectos relacionados con la privacidad.

En la actualidad existe un debate sobre la posibilidad de ceder datos personales a cambio de beneficios, ya sean en forma de dinero o mediante ofertas personalizadas de productos. De esta forma, el usuario se puede plantear ceder sus datos a cambio de recibir parte de los beneficios que las empresas consiguen por el uso de dichos datos. No obstante, a pesar de que la idea parece positiva para los intereses de los usuarios (más aún cuando en la actualidad la mayoría cede sus datos sin recibir ningún tipo de compensación por ello), las cifras muestran

GRÁFICO 7
PREOCUPACIÓN ANTE LA SEGURIDAD Y PRIVACIDAD EN INTERNET (% USUARIOS CON VALORACIONES ENTRE 7 Y 10)



Fuente: Elaboración propia. Datos de Fundación Telefónica 2015

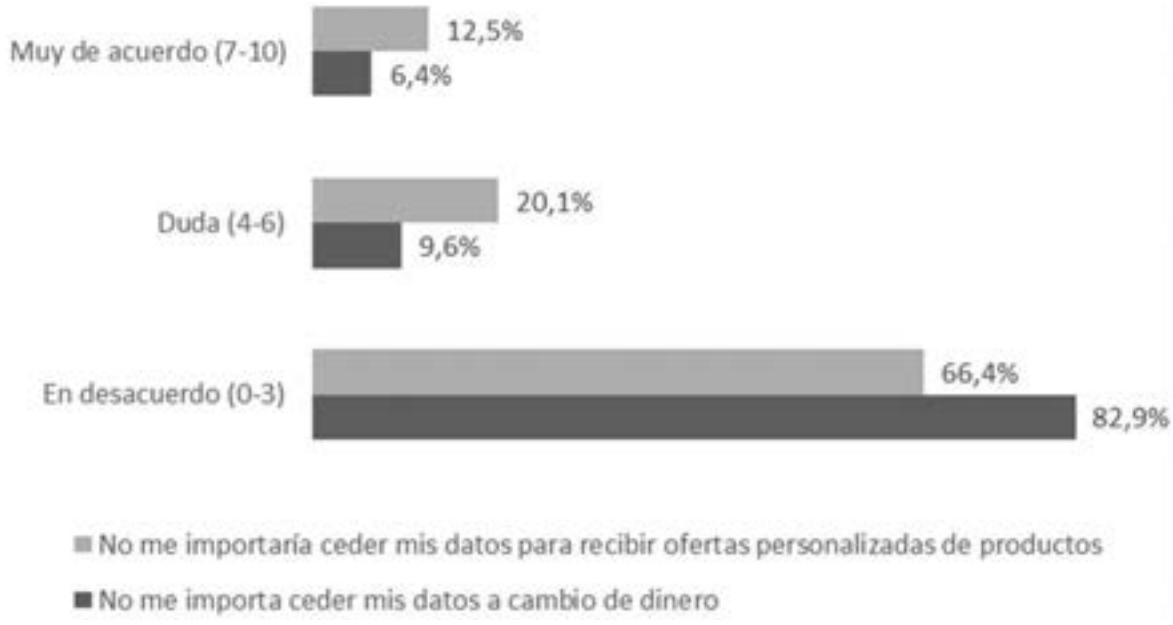
GRÁFICO 8
PREOCUPACIÓN POR LA PRIVACIDAD SEGÚN EL TIPO DE INFORMACIÓN (% USUARIOS QUE VALORAN ENTRE 7 Y 10)

Fuente: Elaboración propia. Datos de Fundación Telefónica 2015

que la mayoría de la población no está de acuerdo con ceder parte de la privacidad a cambio de ofertas personalizadas o dinero. De acuerdo con lo expresado en el gráfico 9, solamente un 12,5% está muy de acuerdo con ceder sus datos a cambio de recibir ofertas personalizadas, un 8,5% en caso de familias con niños pequeños y un 6,4% los cederían por dinero.

Los datos analizados ponen de relieve que los usuarios presentan una actitud de preocupación e interés ante estos temas, aunque en muchas ocasiones no son capaces de identificar cuáles son los peligros y, por tanto, no saben cómo enfrentarse a ellos. Una primera medida en este sentido debe estar orientada a conocer cómo el *malware* llega hasta nuestros sistemas, lo que deberá condicionar nuestro comportamiento;

GRÁFICO 9
INTERÉS POR CEDER DATOS A CAMBIO DE BENEFICIOS (% INTERNAUTAS)



Fuente: Elaboración propia. Datos de Fundación Telefónica 2015

por ejemplo, no seguir cadenas de correos, utilizar software de fuentes seguras, tener cuidado al introducir USB de terceras personas, etc., pues es necesario tener en cuenta que los medios de distribución de software dañino son cada vez más variados.

A esta situación ha de añadirse que la naturaleza y los objetivos de los ataques cibernéticos han ido cambiando con el tiempo. Por ejemplo, la mayoría de los usuarios piensa que los atacantes buscan información sobre ellos, ya sea personal o relativa a claves de acceso. No obstante, en muchas ocasiones el objetivo de los atacantes es acceder a los recursos del usuario, como aprovechar el poder de procesamiento para realizar tareas que requieran gran poder de computación, o realizar minería de criptomonedas (*bitcoin mining*). Otro ejemplo sería acceder a su ancho de banda para que su sistema actúe como un zombi dentro de una «botnet» y poder realizar ataques masivos.

Es posible también que el usuario considere que no tiene ninguna información relevante que pueda ser utilizada por delincuentes, lo que suele ser una percepción falsa, ya que los atacantes pueden querer acceder a las libretas de contactos para realizar spam masivo personalizado y atacar a terceras personas, o bloquear el ordenador y pedir un rescate por recuperar la información, pues aunque la información no sea de valor para terceras personas, sí lo es para el propio usuario.

Los robos más importantes de información pueden afectar a tres tipos de aspectos:

- Económico: si roban las contraseñas o tienen acceso a sistemas *online* (bancos, PayPal, bitcoins, etc.).
- Lúdico: pérdida de fotografías, acceso a información sensible como repositorios en la nube, etc.
- De imagen: robo de cuentas de redes sociales, pudiendo llegar a suplantar la identidad y dañarla.

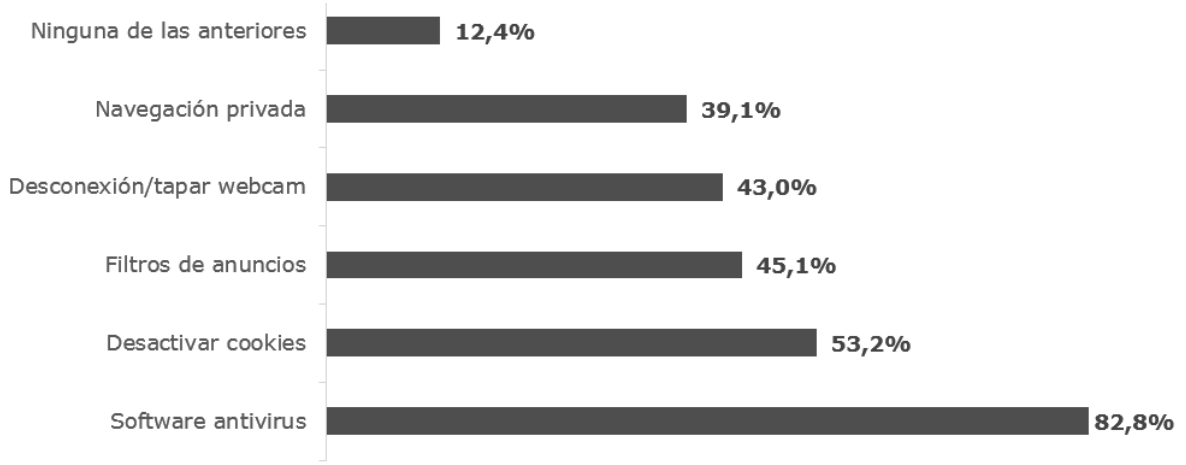
Es necesario que los usuarios sean conscientes de las nuevas normas de juego que imponen Internet y las nuevas tecnologías, y conozcan tanto los mecanismos más importantes que utilizan los atacantes como cuáles de nuestras identidades pueden ser interesantes para ellos.

Medidas relacionadas con privacidad y seguridad adoptadas por los usuarios

La situación analizada muestra cómo el número y las características de las amenazas han ido evolucionando con respecto a hace unos años, cuando Internet no era tan habitual y, además, no existían tecnologías como la computación en la nube o los *smartphones*. Se observa que el entorno tecnológico ha cambiado sustancialmente en los últimos años, la digitalización ha llegado a prácticamente todos los servicios y se ha pasado de una comunicación esporádica a estar continuamente conectados con el entorno.

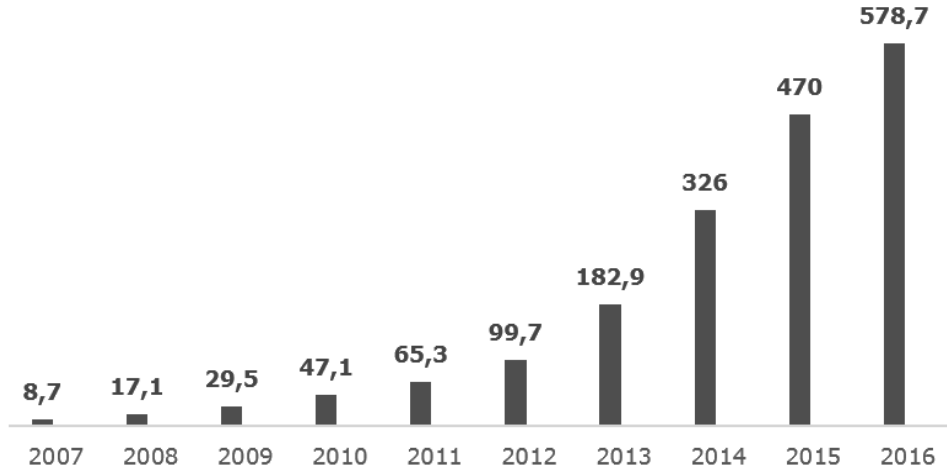
Se trata pues de una situación completamente diferente a la que existía hace unos años, y que debería suponer una transformación completa de las medidas y actitudes que los usuarios adoptaran en referencia a la privacidad y seguridad en su mundo digital. No obstante, según se desprende de la encuesta

GRÁFICO 10
MEDIDAS PARA PROTEGER LA PRIVACIDAD ADOPTADAS POR LOS INTERNAUTAS (% USUARIOS)



Fuente: Elaboración propia. Datos de Fundación Telefónica 2015

GRÁFICO 11
EVOLUCIÓN DE LOS *MALWARE* EN LOS ÚLTIMOS 10 AÑOS (Nº DE *MALWARES* EXISTENTES)



Fuente: Elaboración propia con datos The Independent IT-Security Institute

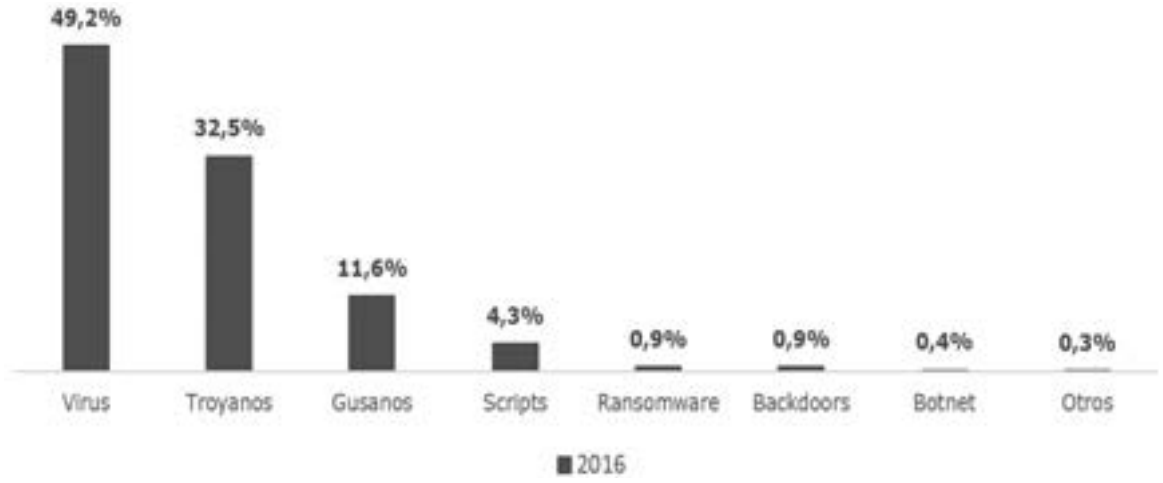
de hábitos realizada por Fundación Telefónica, estas nuevas circunstancias no están siendo interiorizadas por los usuarios, que en su mayoría siguen confiando en los antivirus como fórmula preferida para proteger su privacidad.

En el gráfico 10 se observa que la mayoría de estas medidas delegan la protección de su privacidad en poseer software especializado, como antivirus o filtros de anuncios, en lugar de medidas activas como cambios en los hábitos. La excepción más reseñable de comportamiento activo con respecto a la seguridad es desconectar o tapar la webcam, hábito que llega al 43% de los internautas, y alcanza al 45,7% en el caso de las mujeres y el 54,4% entre los jóvenes entre 20 y 24 años. También se deduce que existe una cierta inercia en los comportamientos con respecto a la seguridad y que todavía la mayoría de la población internauta mantiene los hábitos que tenía en la época en que la conexión a Internet era más puntual y las tecnologías estaban más restringidas a actividades muy concretas. Se hace imprescindible, por tanto, una actividad de concienciación y formación sobre los peligros que se plantean y qué comportamientos podrían evitarlos.

EL *MALWARE* A NIVEL MUNDIAL

El *malware* es un tipo de software que tienen como principal objetivo infiltrarse en un sistema de información sin el permiso del propietario con la intención de dañarlo. La evolución de los diferentes *malware* existentes ha sido exponencial en los últimos años, como pone de relieve el gráfico 11 que muestra que en 2007 apenas existían 8,7 millones

GRÁFICO 12
TIPOS DE *MALWARE* (%)



Fuente: Elaboración propia con datos The Independent IT-Security Institute

de *malware*. En cambio, dicha cifra ha crecido hasta los 578,7 millones en casi 10 años, lo que representa una enorme progresión (IT Security Report, 2016).

Entre todos los tipos de *malware* existentes, los virus son los más frecuentes representando casi la mitad de todos los *malware* (49,2%). Este tipo de *malware* tiene dos características particulares: actúa de forma transparente al usuario y tiene la capacidad de reproducirse así mismo. Los virus pueden introducirse en un ordenador a través de otro dispositivo infectado, a través de medios extraíbles (CD, DVD, USB, etc.) o través de una red (local o Internet).

El segundo tipo de *malware* más frecuente es el troyano, que abarca el 32,5% de todos los *malware* detectados. El troyano, a diferencia de otros *malware*, no puede reproducirse por sí mismo e infectar archivos. Normalmente se encuentra en forma de archivo ejecutable (.exe o .com) y no suele contener ningún elemento más, a excepción del troyano. Adicionalmente, los gusanos engloban el 11,6% de todos los *malware* localizados. Los gusanos son un *malware* que se reproduce a través de una red y, a diferencia de los virus (que necesitan del archivo infectado para ser copiados y replicarse), el gusano se propaga activamente enviando copias de sí mismo a través de una red local o Internet, a través de la comunicación por correo electrónico o, incluso, aprovechando errores de seguridad del sistema operativo.

Poco a poco otros *malware* como los *scripts* (4,3%) y las *backdoors* (0,9%) van incrementando su presencia. De entre todos ellos destaca el *ransomware* (0,9%), un *malware* novedoso que se encarga de infectar el equipo de un usuario proporcionando al ciberdelincuente la capacidad de bloquearlo desde una ubicación remota y cifrar los archivos escamoteando el control de toda la información y datos almacenados. Para desbloquearlo el *malware* lanza una ventana emergente en la que se solicita el pago de un rescate. El gráfico 12 refleja la distribución de los diferentes tipos de *malware* en 2016.

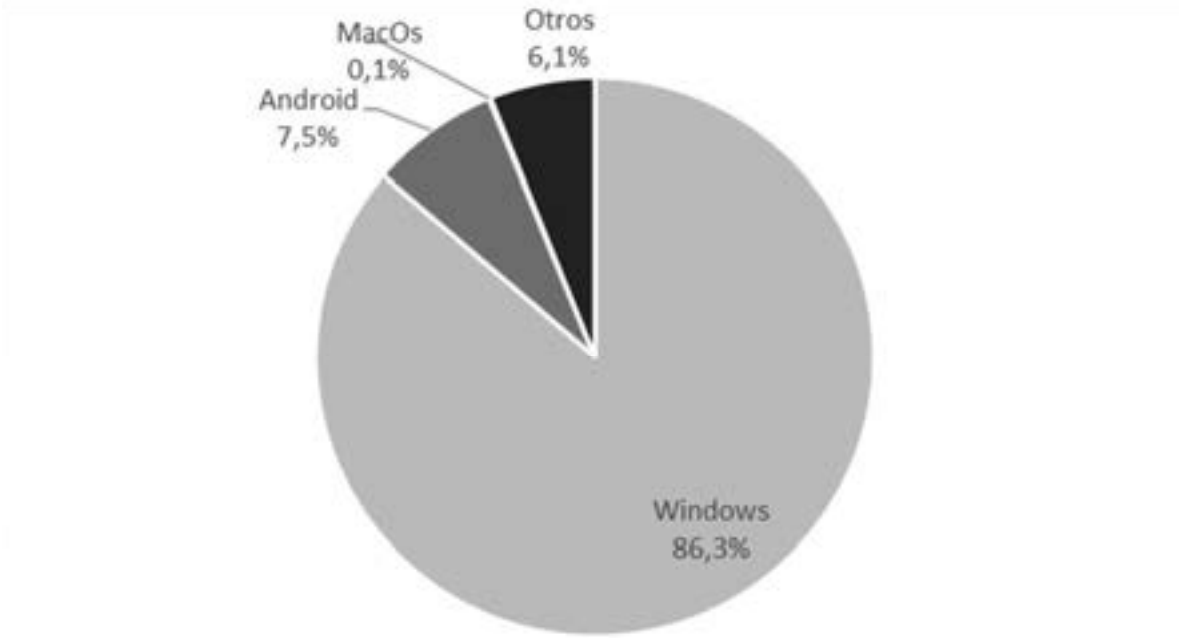
No obstante, de entre todos los *malware* que han aparecido en el primer trimestre de 2016, el 66,8% son troyanos, seguidos de los virus (16%) y los gusanos (11%). El resto de *malware* tiene una incidencia mucho más pequeña, acumulando el 6,2% de los *malware* surgidos en el primer trimestre de 2016 (Informe Pandalabs, 2016).

A nivel de sistemas operativos, el 86,3% de los *malware* detectados se encuentran en el sistema operativo Windows, mientras que Android es el segundo sistema operativo más infectado (7,5%). Tan solo el 0,1% de los *malware* se encuentran en los dispositivos cuyo sistema operativo es MacOS, según se refleja en el gráfico 13 (IT Security Report, 2016).

Si se tiene en cuenta el sector de actividad económica, la mayor parte de los *malware* detectados afectan a dispositivos que tienen relación con el sector servicios (65,6%), seguido del sector comercio (13,6%) y el sector financiero, seguros e inmobiliarias (10,8%). También se encuentran afectados, aunque en menor medida, los sectores de Administración Pública (5,6%), fabricación (2,3%), transporte y servicios públicos (2%), y construcción (1%), según se refleja en el gráfico 14.

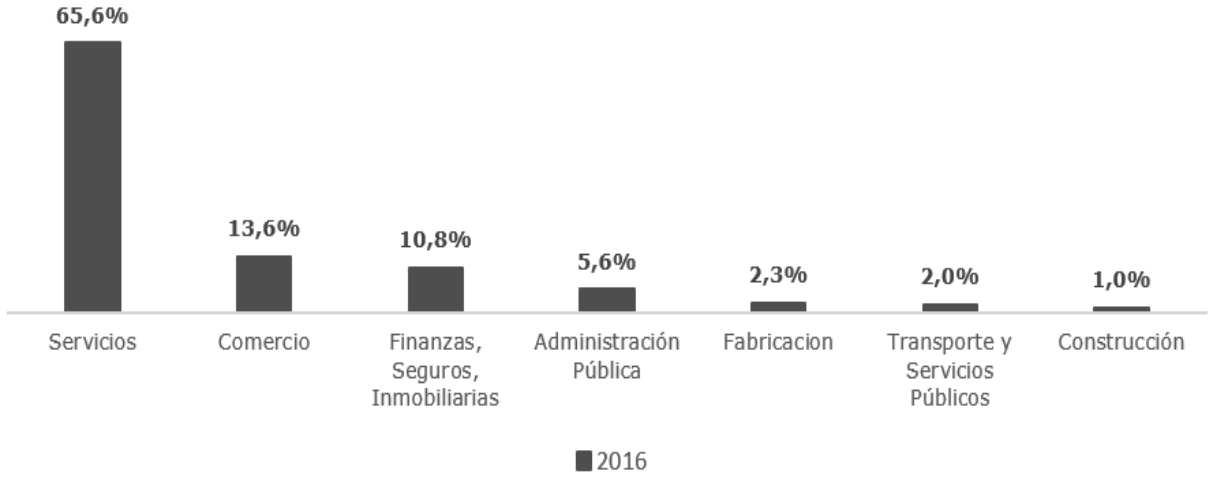
El análisis a nivel global pone de manifiesto que China es el país que ha experimentado más infecciones de cualquier tipo de *malware* durante el primer trimestre de 2016, con un 51,4% de ordenadores infectados, al que siguen Turquía y Taiwán con un 48% y 41,2% de equipos infectados, respectivamente. El resto de países con mayor infección de *malware* en el primer trimestre de 2016 son Ecua-

GRÁFICO 13
SISTEMAS OPERATIVOS INFECTADOS POR *MALWARE* (% SOBRE Nº DE *MALWARES* DETECTADOS)



Fuente: Elaboración propia con datos The Independent IT-Security Institute

GRÁFICO 14
SECTORES INFECTADOS POR *MALWARE* (% SOBRE Nº DE *MALWARES* DETECTADOS)



Fuente: Elaboración propia con datos 2016 Internet Security Threat Report

dor (39,6%), Guatemala (38%), Rusia (38%), México (36,3%), Perú (36%), Polonia (35,6%) y Brasil (34%), con porcentajes similares (Gráfico 15).

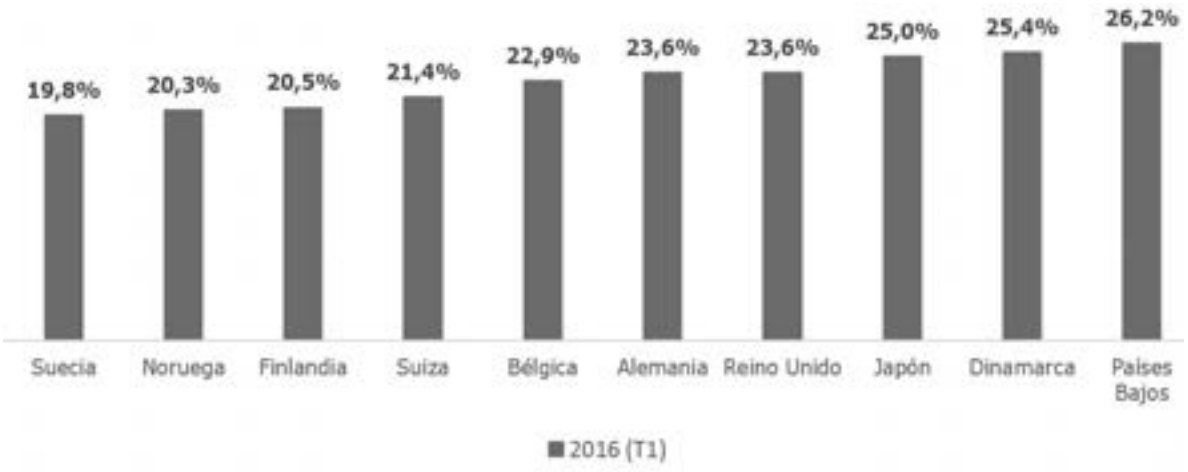
En el polo opuesto, es decir, entre los diez países que presentan un menor índice de infección de *malware* a principios del año 2016, se encuentran principalmente los países europeos. Suecia (19,8%), Noruega (20,3%) y Finlandia (20,5%) registran el menor índice de infección de *malware* a nivel mundial, seguidos de Suiza (21,4%), Bélgica (22,9%), Alemania (23,6%) y Reino Unido (23,6%). Japón es el primer país no europeo que aparece en el ranking con una tasa de infección del 25%. Cierran este grupo de países Dinamarca (25,4%) y Países Bajos (26,2%) (Gráfico 16).

PwC (2016) pone de manifiesto que las ciberamenazas que nos acechan son muy relevantes y cuentan con grandes infraestructuras, métodos y tecnología para sus fines. La mayor parte de la actividad que se desarrolla a nivel de países y ciudadanos se centra en la defensa y protección, pero es necesario ampliar el espectro de actuación, principalmente mediante la anticipación y la prevención del impac-

GRÁFICO 15
PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN DE *MALWARE* EN EL PRIMER TRIMESTRE DE 2016 (%)

Fuente: Elaboración propia con datos de Pandalabs-2016-T1

GRÁFICO 16
PAÍSES CON MENOR ÍNDICE DE INFECCIÓN DE *MALWARE* EN EL PRIMER TRIMESTRE DE 2016 (%)



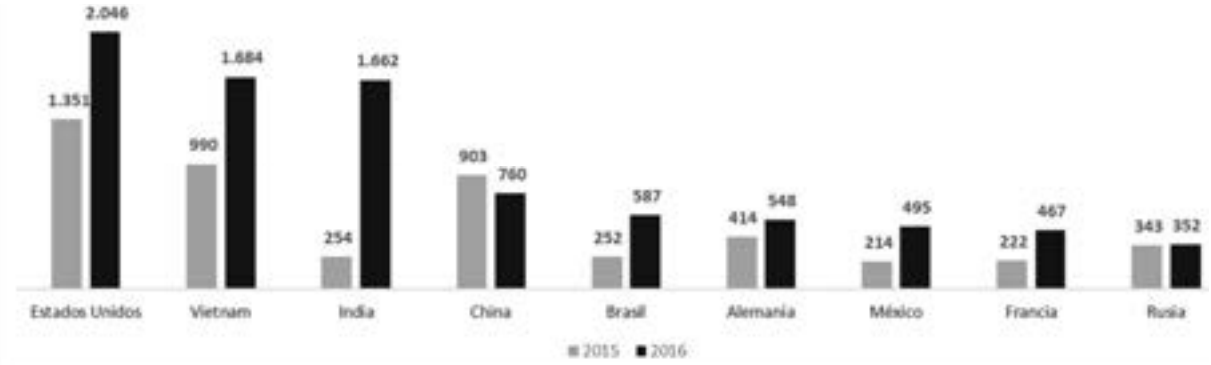
Fuente: Elaboración propia con datos de Pandalabs-2016-T1

to de las ciberamenazas. Para ello se requiere un mayor ámbito de actuación y adoptar un enfoque global en vez de protegerse solamente a nivel local. Pero hay que tener presente que el reconocimiento es un paso fundamental para lanzar un ciberataque y, en esta fase, los adversarios buscan infraestructuras de Internet vulnerables o debilidades en la red que les permitan obtener acceso a los ordenadores de los usuarios y, en última instancia, infiltrarse en las organizaciones.

Los archivos binarios sospechosos de Windows que contienen amenazas, como *spyware* y *adware*, y las aplicaciones potencialmente indeseadas (PUA), como las extensiones maliciosas del navegador, encabezaron la lista de métodos de ataque en la web en 2016 por un margen considerable. A continuación se encuentran las estafas de Facebook, que incluyen ofertas y contenido multimedia falsos, junto con estafas de encuestas. La continua importancia de las estafas de Facebook en las listas anuales y semestrales del *malware* observado con más frecuencia pone de relieve el papel fundamental que tiene la ingeniería social en los ciberataques. Facebook cuenta con casi 1.800 millones de usuarios activos en todo el mundo, por lo que constituye un territorio de actuación lógico para los ciberdelincuentes y otros agentes que buscan engañar a los usuarios.

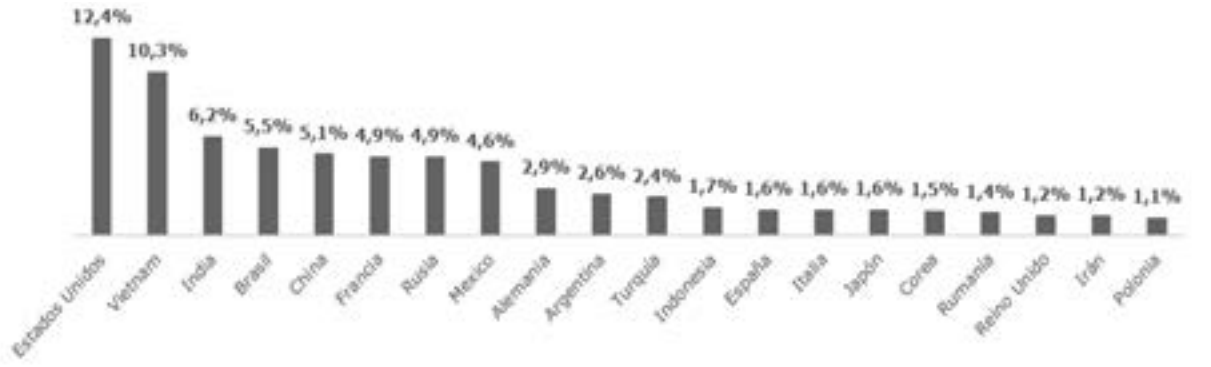
Las infecciones del navegador pueden exponer a los usuarios a publicidad maliciosa (*malvertising*) que se utiliza para configurar el *ransomware* y otras campañas de *malware*. Los investigadores de amenazas de Cisco advierten que el *adware* malicioso, que incluye inyectores de anuncios, secuestradores de las configuraciones del navegador, utilidades y des-

GRÁFICO 17
NÚMERO DE BLOQUEOS DE IP POR PAÍS (12/2015 A 11/2016)



Fuente: Elaboración propia con datos del Grupo de investigación de Seguridad de CISCO

GRÁFICO 18
FUENTES DE SPAM POR PAÍSES EN EL MUNDO EN 2016 (% SOBRE TOTAL DE SPAM)



Fuente: Elaboración propia con datos de Kasperky Lab 2016

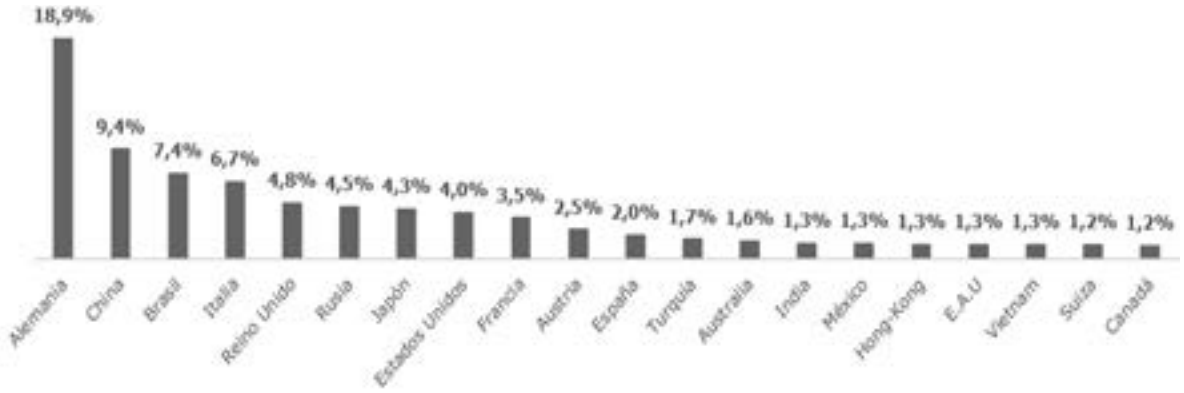
cargadores, es un problema cada vez mayor. De hecho, se han identificado infecciones de *adware* en el 75% de las empresas que se han investigado recientemente (Cisco, 2016).

Otros tipos de *malware*, como el abuso de iFrame y JavaScript en el navegador, también se han diseñado para facilitar las infecciones en los navegadores. Los troyanos (instaladores y descargadores) también aparecen entre los cinco tipos de *malware* principales observados con más frecuencia, lo que indica que siguen siendo herramientas populares para obtener un acceso inicial a los ordenadores de los usuarios y a las redes organizativas. Otra tendencia que se debe vigilar es el alto uso del *malware* que tiene como objetivo a los usuarios de la plataforma operativa Android. Los troyanos de Android han avanzado sin parar en la lista de amenazas de la cola corta durante los últimos dos años.

Cada vez más amenazas buscan específicamente los navegadores y los *plug-ins* o complementos vulnerables. Este cambio se corresponde con una mayor dependencia de los adversarios en el *malware*, ya que cada vez es más difícil abarcar un número de usuarios a través de los vectores de ataque en las webs tradicionales. El mensaje para los usuarios individuales, los profesionales de la seguridad y las empresas está claro para prevenir infecciones por *malware*: asegurarse de que los navegadores estén protegidos y desactivar o eliminar los *plug-ins* de navegador innecesarios. Estas infecciones pueden derivar en ataques más significativos, complejos y costosos, como las campañas de *ransomware*. Estos sencillos pasos pueden reducir considerablemente la exposición a las amenazas basadas en las webs más comunes, así como evitar que los adversarios encuentren espacio operativo para llevar a cabo la siguiente fase de la cadena de ataque: la militarización.

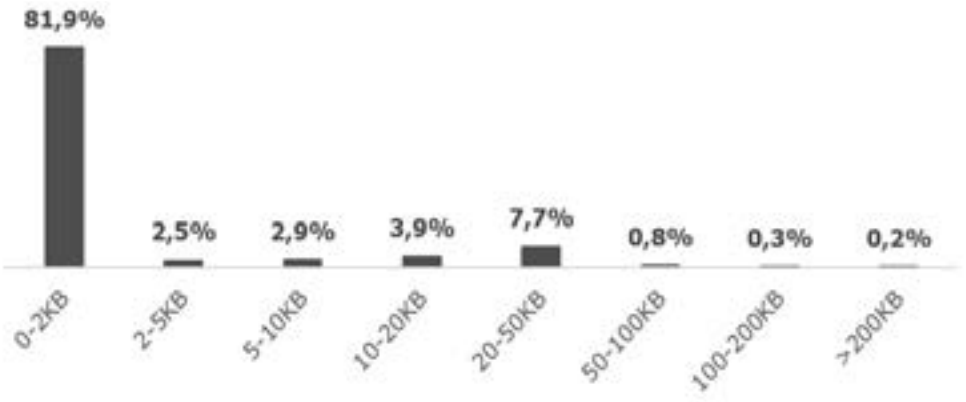
Otro frente de amenazas a nivel global se centra, según Cisco, en el *spam*, que representa aproximadamente dos tercios (65%) del volumen total de correos electrónicos. El volumen global de spam está aumentando, lo que se debe principalmente a las grandes y exitosas *botnets* de envío de spam como *Necurs*. De los datos dispo-

GRÁFICO 19
RECEPTORES DE SPAM POR PAÍSES POR EN EL MUNDO EN 2016 (% SOBRE TOTAL DE SPAM)



Fuente: Elaboración propia con datos de Kasperky Lab 2016

GRÁFICO 20
TAMAÑO DEL SPAM EN EL MUNDO EN 2016 (% SOBRE TOTAL DE SPAM)



Fuente: Elaboración propia con datos de Kasperky Lab 2016

nibles se puede afirmar que aproximadamente entre el 8% y el 10% del spam global observado en 2016 puede categorizarse como malicioso. Este hecho se confirma si se tiene en cuenta que desde diciembre de 2015 a noviembre de 2016 se produjo un aumento significativo en el número de bloqueos de conexiones IP, tal y como se refleja en el gráfico 17.

El gráfico 18 pone de manifiesto que el 12,4% del spam proviene de Estados Unidos, principal generador de spam. En segunda y tercera posición se encuentran Vietnam e India, que generan el 10,3% y 6,2% de spam en el mundo, respectivamente. A continuación se encuentran cinco países que producen un porcentaje similar de spam: Brasil (5,5%), China (5,1%), Rusia (4,9%), Francia (4,9%) y México (4,6%). El resto de países que generan spam lo hacen en una proporción inferior al 3%, rango en el que se encuentra España que se sitúa en decimotercera posición (1,6%), al mismo nivel que Italia, Japón y Corea.

Desde la perspectiva de la recepción de spam, Alemania es el principal país receptor con el 18,9% del total de correos electrónicos, seguido de China (9,4%), Brasil (7,4%), Italia (6,7%), Reino Unido (4,8%), Rusia (4,5%), Japón (4,3%) y Estados Unidos (4%). El resto de países recibe menos del 4% del spam en el mundo, y España se sitúa en undécima posición con el 2% (Gráfico 19).

Por último, es de interés resaltar el análisis de esta amenaza en función del tamaño del fichero. El gráfico 20 pone de manifiesto que la gran mayoría de los mensajes spam (81,9%) tienen un tamaño entre 0 y 2 kb; el 9,3% de los mensajes spam se concentran en un tamaño entre 2 y 20kb; el 7,7% de los mensajes spam tienen un tamaño entre 20 y 50kb; y el 1,3% tienen un tamaño superior a 50kb.

TABLA 1
MARCO CONCEPTUAL DEL ÍNDICE MUNDIAL DE CIBERSEGURIDAD (IMC)

Índice Mundial de Ciberseguridad (IMC)	Medidas jurídicas	Legislación penal
		Reglamento y conformidad
	Medidas técnicas	CERT/CIRST/CSIRT
		Normas
		Certificación
	Medidas organizativas	Política
		Hoja de ruta para la gobernanza
		Organismo responsable
		Evaluación comparativa nacional
	Creación de capacidades	Desarrollo de la normalización
		Desarrollo laboral
		Certificación profesional
		Certificación del organismo
	Cooperación	Cooperacion interestatal
		Cooperación entre organismos
		Asociaciones enre los sectores públicos y privado
		Cooperación internacional

Fuente: Elaboración propia a través del índice Mundial de Ciberseguridad y perfiles de ciberbienestar

ESTUDIOS SOBRE LA CIBERSEGURIDAD POR PAÍSES

Índice Mundial de Ciberseguridad (ABI Research)

Tras varios años de estudio, la ABI Research ha publicado el primer Índice Mundial de Ciberseguridad (IMC) de carácter anual (ABI Research, 2017). El IMC tiene sus orígenes en la Agenda sobre Ciberseguridad Global de la Unión Internacional de Telecomunicaciones (UIT), y considera el nivel de compromiso en cinco ámbitos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional (Tabla 1). El resultado es un índice a nivel estatal y una clasificación mundial de la preparación para la ciberseguridad. Este índice no tiene la intención de determinar la eficacia ni el éxito de una medida en particular, sino de comprobar la existencia de estructuras nacionales para implementar y promover la ciberseguridad.

La tabla 2 refleja los valores del IMC para los 28 países que conforman la Unión Europea en la actualidad. Se observa que Alemania, Estonia y Reino Unido son los países con mayor puntuación (0,71 puntos), mientras que Grecia (0,21 puntos), Irlanda (0,21 puntos) y Eslovenia (0,18 puntos) son los países europeos que ocupan las últimas posiciones. España se sitúa en la undécima posición con 0,59 puntos, igual valoración que Dinamarca y Francia, y por encima de países como Italia, Bélgica y Luxemburgo, entre otros.

Un análisis más detallado del IMC pone de manifiesto que España obtiene la puntuación más alta (1 punto) en el indicador de medidas jurídicas, por delante de países como Holanda, Suecia, Italia y Bélgica. Además, supera los 0,6 puntos en los indicadores relativos a medidas técnicas (0,67 puntos), medidas organizativas (0,63 puntos) y creación de capacidades (0,63 puntos). Sin embargo, presenta una puntuación muy baja en el indicador de cooperación (0,25 puntos), en el que solamente supera a Grecia, Irlanda y Eslovenia.

The Inclusive Internet

The Inclusive Internet es un informe elaborado por *The Economist* que engloba diferentes indicadores relacionados con la sociedad de la información en el mundo a través de 75 países. Este informe está compuesto por cuatro grandes categorías (dispo-

TABLA 2
ÍNDICE MUNDIAL DE CIBERSEGURIDAD UE-28 (IMC)

Nº	País	Medidas jurídicas	Medidas técnicas	Medidas organizativas	Creación de capacidades	Cooperación	IMC
1	**Alemania**	1,00	1,00	0,63	0,63	0,50	**0,71**
1	**Estonia**	1,00	0,67	1,00	0,50	0,50	**0,71**
1	**Reino Unido**	1,00	0,67	0,75	0,75	0,50	**0,71**
4	**Austria**	1,00	0,33	0,88	0,75	0,50	**0,68**
4	**Hungría**	1,00	0,67	0,75	0,63	0,50	**0,68**
4	**Holanda**	0,75	0,50	0,88	0,63	0,63	**0,68**
7	**Letonia**	1,00	0,67	0,75	0,50	0,50	**0,65**
7	**Suecia**	0,75	0,67	0,63	0,63	0,63	**0,65**
9	**Finlandia**	0,50	0,67	0,88	0,50	0,50	**0,62**
10	**Eslovaquia**	1,00	0,67	0,88	0,25	0,50	**0,62**
11	**Dinamarca**	1,00	0,67	0,88	0,50	0,50	**0,59**
11	**España**	**1,00**	**0,67**	**0,63**	**0,63**	**0,25**	**0,59**
11	**Francia**	1,00	0,17	0,50	0,75	0,63	**0,59**
14	**Italia**	0,75	0,33	0,63	0,63	0,50	**0,56**
15	**Polonia**	1,00	0,33	0,63	0,63	0,25	**0,53**
16	**Rep. Checa**	0.75	0,67	0,63	0,38	0,25	**0,50**
17	**Luxemburgo**	0,75	0,33	0,50	0,38	0,25	**0,47**
17	**Rumanía**	0,75	0,33	0,63	0,25	0,50	**0,47**
19	**Bélgica**	0,75	0,50	0,25	0,38	0,50	**0,44**
19	**Bulgaria**	0,75	0,67	0,50	0,38	0,50	**0,44**
19	**Lituania**	1,00	0,33	0,75	0,13	0,25	**0,44**
22	**Croacia**	0,75	0,67	0,25	0,38	0,25	**0,41**
23	**Malta**	0,75	0,50	0,25	0,25	0,25	**0,35**
24	**Chipre**	0,75	0,17	0,38	0,13	0,25	**0,29**
24	**Portugal**	0,75	0,50	0,13	0,13	0,25	**0,29**
26	**Grecia**	0,50	0,33	0,13	0,13	0,13	**0,21**
26	**Irlanda**	0,50	0,17	0,00	0,38	0,13	**0,21**
28	**Eslovenia**	0,50	0,33	0,00	0,13	0,13	**0,18**

Fuente: Elaboración propia a través del índice Mundial de Ciberseguridad y perfiles de ciberbienestar.

nibilidad, competitividad, aplicabilidad y preparación) que, a su vez, se dividen en subcategorías que incluyen diversos indicadores (*The Economist*, 2017).

Una de estas categorías, concretamente la preparación, incluye diversos indicadores relacionados con la seguridad. El primero de ellos hace referencia a la disponibilidad del CERT o del CSIRT (*Computer Security Incident Response*) en los diferentes países. Estas herramientas son sistemas que se encargan de gestionar las diferentes situaciones de emergencia relacionadas con la ciberseguridad. Países como España, Alemania, Francia, Holanda, Italia o Reino Unido, entre otros, disponen de estas herramientas. No obstante, Turquía no posee ninguna herramienta que pueda encargarse de situaciones de emergencia relacionada con la ciberseguridad. De hecho, según datos de los Ministerios de Interior y de Industria de España, a través del Centro de Respuesta a Incidentes Cibernéticos, España ha gestionado más de 105.800 incidentes relacionados con la seguridad en la red durante 2016, de los que 479 afectaron a estructuras críticas de diferente grado, más del doble que en 2015.

El otro indicador que se expone en el informe son las diferentes normas de privacidad que disponen los países analizados. Estas regulaciones hacen referencia a la capacidad que tienen los países en guardar de manera segura todos los datos de personas que se tramitan de manera online. Al igual que en el indicador anterior, España, Alemania, Francia, Holanda, Italia y Reino Unido cuentan con una normativa avanzada en esta materia. En cambio, Turquía no cuenta con una normativa eficaz para evitar ataques de ciberseguridad a los datos personales proporcionados por sus habitantes.

CONCLUSIONES Y RECOMENDACIONES

A nivel general cada usuario de Internet juega un papel en el mantenimiento de la integridad de la Red. Las personas comprometen la seguridad general del sistema al permitir, incluso inadvertidamente, que las fuerzas delictivas accedan a sus cuentas o sus máquinas (Shillair *et al*., 2015). Los usuarios españoles están cada vez más preocupados por la seguridad y año tras año las medidas de protección contra las ciberamenazas se amplían en los hogares españoles. España se encuentra en línea con los países de su entorno a la hora de contar con estructuras a nivel nacional para implementar y promover la ciberseguridad.

Está comprobado que las técnicas de *phishing* se usan a menudo para obtener contraseñas de los empleados y acceder a cuentas para robar fondos (Dhamija, Tygar y Hearst, 2006). El *malware* se instala subrepticiamente en las computadoras de usuarios que no perciben el alto riesgo de descargar archivos o programas sin escanear (Workman, Bommer y Straub, 2008). Las personas cuyas computadoras parecen estar trabajando solo un poco más lento de lo normal no se dan cuenta de que estos dispositivos pueden haberse convertido en *botnets* que pueden ser utilizados por fuerzas externas (Leder, Werner y Martini, 2008). Los responsables políticos encuentran problemático encontrar formas de comunicar la gravedad de las amenazas y qué precauciones deben seguirse.

El *malware* ha crecido de manera exponencial en los últimos años. Con el paso del tiempo las ciberamenazas evolucionan, se transforman y se propagan por los dispositivos de particulares y empresas como si de una enfermedad se tratase. Estos *malware* son cada vez más fuertes y dañinos provocando perjuicios algunas veces hasta irreparables. Es aquí donde la ciberseguridad toma el testigo y adquiere una importancia hasta ahora nunca vista. Por si fuera poco, una oleada de ataques ha sacudido gobiernos, empresas y hogares por igual en los últimos meses. Estos ataques se intensifican cada vez más provocando daños irreparables y una importante pérdida de confianza por parte de los usuarios. Por todo ello, los profesionales de esta rama deben analizar y estudiar como adelantarse a los hackers defendiéndose de todo tipo de *malware* y, sin duda, el sector de la ciberseguridad será un sector al alza que en los próximos años alcanzará una importancia incontestable.

En los próximos tiempos la ciberseguridad deberá incorporar nuevas prácticas y tecnologías que actualmente son tendencia, como son la seguridad en los dispositivos móviles personales con usos profesionales (BYOD), la seguridad en las infraestructuras críticas y la seguridad en el Internet de las Cosas.

La utilización de dispositivos móviles propios para acceder a los datos corporativos es una tendencia ascendente entre los trabajadores denominada *bring your own device* (BYOD). El apogeo del BYOD es muy beneficioso para las empresas debido al ahorro de costes ya que cada empleado utiliza sus propios dispositivos para la realización del trabajo, entre otras cosas. No obstante, el BYOD manifiesta unos riesgos importantes para las empresas debido a la sensibilidad de estos dispositivos ante potenciales ciberataques. Es por ello que las empresas y los trabajadores deberán esforzarse en aumentar las medidas de seguridad en las BYOD con el objetivo de disminuir el número de ataques que se puedan producir.

Las infraestructuras críticas (centrales y redes de energía, transportes, sistema financiero, hospitales, etc.) son elementos esenciales de cualquier sociedad. Estas infraestructuras son controladas por sistemas informáticos, por lo que pueden recibir ciberataques en cualquier momento con consecuencias desastrosas. Por si fuera poco, estos sistemas de control industrial están en el foco de atención por sus continuos problemas de seguridad, debidos a su continua expansión y a la escasa protección del software que los gestiona. Actualmente, el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) es el organismo que vela por la seguridad de dichas infraestructuras.

El concepto de Internet de las Cosas hace referencia a la creciente interconexión de objetos inteligentes (electrodomésticos, sensores, dispositivos) a través de Internet. En su mayoría, este tipo de dispositivos carecen de las medidas de seguridad adecuadas permitiendo que los hackers monitoricen los datos y pongan en peligro la integridad de los productos y servicios. Con el auge de las Ciudades Inteligentes (*Smart Cities*), basadas en Internet, es muy probable que a corto plazo puedan ocasionarse importantes problemas de seguridad en estos dispositivos.

Como consecuencia de todo lo analizado se plantean, a modo de consejos, un conjunto de actuaciones que pueden servir para mejorar la seguridad informática a nivel de usuario:

- Mantener actualizado el software en todo momento. Cuando un desarrollador/fabricante publica un programa informático pueden aparecen fallos de seguridad. Estos fallos de seguridad, denominados vulnerabilidades, son aprovechados por los cibercriminales para tratar de infectar nuestro equipo con software malicioso con el objetivo de robar nuestros datos, usar nuestro equipo para su beneficio, etc. Es, por ello, que resulta fundamental mantener una atención constante sobre las actualizaciones de nuestro sistema operativo, así como de aquellos programas que puedan implicar un agujero de seguridad en caso de ser explotados por un atacante o cualquier tipo de *malware*.
- Tener precaución al usar equipos compartidos. Cuando se utiliza un ordenador compartido conviene tener en cuenta las siguientes recomendaciones:
    - No guardar los datos de acceso. Muchos sitios web (correo online, redes sociales, etc.) nos ofrecen la posibilidad de guardar nues-

tra contraseña para no tener que teclearla cada vez que entramos a una aplicación. Se debe responder siempre «no» a este ofrecimiento, o proceder a desactivar la casilla donde se ofrece dicha opción.

- Usar el modo «privado» siempre que sea posible. Hoy en día los principales navegadores web ofrecen un modo especial de navegación (Incógnito en Chrome o *InPrivate* en Internet Explorer, por ejemplo) con el que se puede visitar páginas web sin dejar rastros, al no guardar historial, cookies, datos de formularios web, etc.

- Comprobar que se usa una conexión segura. La manera más fácil de comprobar que estamos conectando a Internet bajo el amparo de una conexión segura es asegurarnos de que en la barra de direcciones del navegador aparecen las siglas 'https', en lugar del clásico 'http' de las conexiones normales. Se trata de una opción especialmente recomendable si conectamos a Internet mediante redes inalámbricas o teléfonos móviles, ya que nuestras contraseñas o datos bancarios podrían ser descubiertos si no navegamos bajo el paraguas de una conexión segura.

- No utilizar contraseñas poco seguras. La contraseña no debe contener el nombre de usuario de la cuenta o cualquier otra información personal fácil de averiguar (cumpleaños, nombres de hijos, cónyuges...). Tampoco una serie de letras dispuestas adyacentemente en el teclado («qwerty») o siguiendo un orden alfabético o numérico (123456, abcde...). No se deben almacenar las contraseñas apuntadas en un papel en un lugar público y al alcance de los demás, ni compartir las contraseñas en Internet (por correo electrónico), ni por teléfono. Por último, no se debe utilizar la opción de «Guardar contraseña» que en ocasiones se ofrece para evitar reintroducirla en cada conexión.

- Tener cuidado con los correos no solicitados o no deseados (spam). Muchos de los correos no solicitados o no deseados pueden contener *malware*, programas y códigos maliciosos cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario. Se puede reducir en nuestra bandeja de entrada evitando los correos en cadena y no publicando nuestro e-mail completo en páginas web (los enlaces 'mailto' hacen que nuestro correo sea indexado en buscadores y se convierta en una fuente de spam).

- Analizar las descargas con un antivirus. Las descargas de Internet son una fuente de infección ampliamente utilizada por los desarrolladores de *malware*. A través de códigos maliciosos camuflados en ficheros que despiertan interés para el usuario (como, por ejemplo, novedades de software, archivos sobre nuevas producciones cinematográficas o musicales, etc.), los ciberdelincuentes logran el objetivo de infectar el equipo informático de usuarios poco precavidos.

- Realizar copias de seguridad de ficheros y archivos. Por seguridad y protección de toda la información es más que recomendable realizar una copia de respaldo de aquellos archivos que no se quieren perder. La realización de copias de seguridad nos permitirá disponer de la información si nuestros equipos se infectan de *malware* o si somos víctimas de un ataque de ransomware.

BIBLIOGRAFÍA

ABI Research (2017). Índice Mundial de Ciberseguridad (IMC). Extraído de https://www.abiresearch.com/

CISCO (2016). Informe Anual de Seguridad. Extraído de https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems, pp. 581-590.

Fundación Telefónica (2015, 2016). Informe Anual Fundación Telefónica España. Extraído de https://www.fundaciontelefonica.com/conocenos/informe-anual/

Herrero, J., Urueña, A., Torres, A., & Hidalgo, A. (2017a). My computer is infected: the role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm. Journal of Risk Research, 20(11), 1466-1479.

Herrero, J., Urueña, A., Torres, A., & Hidalgo, A. (2017b). Smartphone addiction: psychosocial correlates, risky attitudes, and smartphone harm. Journal of Risk Research. Publicado on-line https://doi.org/10.1080/13669877.2017.1351472

Informe Pandalabs (2016). Primer trimestre 2016. http://www.pandasecurity.com/spain/mediacenter/src/uploads/2016/05/Pandalabs-2016-T1-LR-ES.pdf

Instituto Nacional de Estadística (2016). Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. 2016. Extraído de http://www.ine.es/

IT Security Report (2016). The Independent IT-Security Institute. AV TEST. 2015/2016. Extraído de https://www.av-test.org/es/

Kaspersky Lab (2017). Kaspersky Cybersecurity Index. Extraído de https://index.kaspersky.com/

Leder, F., Werner, T., & Martini, P. (2009). Proactive botnet countermeasures: an offensive approach. The Virtual Battlefield: Perspectives on Cyber Warfare, 3, pp. 211-225.

Ministerio de la Presidencia (2016). Datos del Ministerio de la Presidencia y para las Administraciones Territoriales. Extraído de http://www.seat.mpr.gob.es/portal/index.html

PWC (2016). Informe Temas Candentes de la Ciberseguridad. Extraído de http://www.pwc.es/es/publicaciones/gestion-empresarial/temas-candentes-ciberseguridad.html

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, pp. 199-207.

Symantec (2016). Internet Security Threat Report. Extraído de https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

The Economist (2017). The Inclusive Internet. Extraído de https://theinclusiveinternet.eiu.com/

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24, pp. 2799-2816.