Centro de Estudios de Consumo

www.uclm.es/centro/cesco

# LA e-CONFIANZA DEL INTERNAUTA ESPAÑOL: RETOS DE CIBERSEGURIDAD

***Mª Nieves Pacheco Jiménez***
*Prof. Contratada Doctora*
*Centro de Estudios de Consumo*
*Universidad de Castilla-La Mancha*

*Fecha de publicación: 16 de marzo de 2015*

## I. INTRODUCCIÓN

Este trabajo se gesta a raíz de la publicación en prensa hace unas semanas del artículo titulado "La venta *online* es la forma más habitual de fraude por Internet"[1]. Esta afirmación se fundamenta en el Estudio sobre la ciberseguridad y confianza de los hogares españoles[2], elaborado por el Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información (ONTSI)[3] y el Instituto Nacional de Ciberseguridad (INCIBE)[4], publicado en febrero de 2015.

Lo expuesto enlaza con el artículo publicado en CESCO el pasado mes de enero sobre las Directrices de seguridad en los pagos por Internet dadas por la Autoridad Bancaria Europea[5]. En él se analiza la encuesta de opinión pública "Especial Eurobarómetro" sobre "seguridad cibernética"[6] en los países de la UE27 y Croacia, que examina la frecuencia y el tipo de uso que los ciudadanos de la UE realizan de Internet[7], su confianza en las transacciones *online*[8],

[1] http://politica.elpais.com/politica/2015/02/16/actualidad/1424102293_530364.html
[2] http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares espa%C3%B1oles-febrero-2015
[3] http://www.ontsi.red.es/ontsi/
[4] https://www.incibe.es
[5] PACHECO JIMÉNEZ, Mª N.: "Pagos por Internet: ¿riesgos a raya con las Directrices de Seguridad publicadas por la Autoridad Bancaria Europea?", en *Blog CESCO*, enero 2015.
[6] Special Eurobarometer 404 – Cyber security, publicado en noviembre de 2013.
*Vid*. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
[7] Alrededor de la mitad de los usuarios de Internet en la UE dicen visitar redes sociales (55%), comprar productos o servicios *online* (50%) o realizar Banca *online* (48%), mientras que el 18% vender bienes o servicios.
[8] Cuando el uso de Internet se dirige a banca o compras *online*, las preocupaciones más comunes de los usuarios son que alguien pueda coger o usar inadecuadamente sus datos personales (37%) y la seguridad de los pagos (35%).

su experiencia en ciberdelitos[9] y el nivel de concienciación que tienen acerca de este tipo de delitos. Dicho Estudio pone de manifiesto los riesgos que presenta Internet para el usuario, repercutiendo consecuentemente en la confianza de éste en el denominado *e-comercio* (concretamente en la venta al por menor y en el sector bancario).

En base a estos resultados, los usuarios de Internet han variado su comportamiento en lo relativo a la seguridad. Así, un 46% ha instalado un antivirus, un 40% no abre los *e-mails* de remitentes desconocidos, un 34% no da información personal en los sitios web, un 32% únicamente visita los sitios web que conoce y en los que confía, un 26% sólo usa su propio ordenador, un 24% emplea diferentes contraseñas para diferentes sitios web, y un 6% afirma haber cancelado una compra *online* por sospechar del vendedor o del sitio web[10].

Es evidente que este escenario requiere un mecanismo para reducir los riesgos en ciberseguridad, siendo uno de los ámbitos más complejos el sistema de pagos realizados vía Internet. Así, la Autoridad Bancaria Europea (EBA[11]) presentó a mediados de diciembre de 2014 una serie de directrices para implementar la seguridad de los consumidores de la UE en sus compras por Internet con el objetivo de luchar contra el fraude *online* y aumentar la confianza de aquellos en los servicios de pago. El acento de estas recomendaciones se pone en el inicio de los pagos –bien a través de servicios de Banca *online* bien mediante el uso de tarjetas- y en el acceso a datos sensibles, que deben protegerse a través de una fuerte autenticación de la identidad del cliente-usuario[12].

## II. ASPECTOS CLAVE DEL ESTUDIO DE LA CIBERSEGURIDAD Y CONFIANZA EN LOS HOGARES ESPAÑOLES

El Estudio de la ciberseguridad y confianza en los hogares españoles, diseñado y promovido por el Instituto Nacional de Ciberseguridad (INCIBE) y el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es, se llevó a cabo de abril a junio de 2014 entre usuarios españoles de Internet mayores de 15 años con acceso

[9] Un 10% de los usuarios de Internet en toda la UE ha experimentado fraude *online*, y un 6% robos de identidad. Un 12% no ha podido tener acceso a servicios *online* debido a ataques cibernéticos, y un 12% ha tenido una cuenta de correo electrónico hackeada. Por último, un 7% ha sido víctima de fraude de tarjeta de crédito o de Banca *online*.

[10] *Vid*. tabla QC6 del "Especial Eurobarómetro".

[11] European Banking Authority: Autoridad independiente de la UE establecida el 1 de enero de 2011, que trabaja para garantizar una regulación eficaz y coherente, así como la supervisión del sector bancario europeo. Sus objetivos generales son: mantener la estabilidad financiera en la UE y salvaguardar la integridad, la eficiencia y el correcto funcionamiento del sector bancario. Su principal tarea es contribuir a la creación de un único código normativo europeo en Banca, cuya finalidad es proporcionar un conjunto único de normas armonizadas para las instituciones financieras en toda la UE. Además, desempeña un papel importante en la promoción de la convergencia de las prácticas supervisoras, debiendo evaluar los riesgos y vulnerabilidades en el sector bancario de la UE. *Vid*. www.eba.europa.eu

[12] *Vid*. PACHECO JIMÉNEZ, Mª N., *op. cit*., p. 3.

frecuente desde el hogar (al menos una vez al mes) en el ámbito de la Península, Baleares y Canarias, siendo el tamaño muestral de 3097 hogares encuestados y, de ellos, 2131 equipos escaneados[13].

Como el propio Estudio indica, su objetivo general es "hacer un análisis del estado real de la ciberseguridad y confianza digital entre los usuarios españoles de Internet y, al mismo tiempo, contrastar el nivel real de incidentes que sufren los equipos con las percepciones de los usuarios y mostrar la evolución temporal de estos indicadores. Además se trata de impulsar el conocimiento especializado y útil en materia de ciberseguridad y privacidad, para mejorar la implantación de medidas por parte de los usuarios. Asimismo, se pretende reforzar la adopción de políticas y medidas por parte de la Administración, orientando iniciativas y políticas públicas tanto en la generación de confianza en la Sociedad de la Información, como en la mejora individual de la seguridad, sustentadas en una percepción realista de los beneficios y riesgos de las mismas".

Por la clara conexión que tiene el referido Estudio con los ítems "ciberseguridad" y "fraude" expuestos anteriormente, este trabajo pretende poner de relieve los resultados más relevantes arrojados por aquél.

## II.1. *MALWARE* Y MEDIDAS DE SEGURIDAD

Se denomina *malware* a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del usuario (v. gr., troyanos; *adware* o *software* publicitario; herramientas de intrusión; virus; archivos sospechosos; *spyware*; gusano; *scripts*, *lockers*)[14]. Aunque comúnmente se conocen como virus, la realidad es que se trata de un término mucho más amplio que engloba otras tipologías. Y son las descargas de Internet las que constituyen una fuente de infección ampliamente utilizadas por los desarrolladores de *malware*.

Antes estas amenazas, se fomenta el empleo de medidas de seguridad adecuadas, entendidas como programas o acciones utilizadas por el usuario para proteger el ordenador y los datos

[13] Los datos presentados en este informe han sido extraídos siguiendo diferentes metodologías:
Dato declarado: Obtenido de las encuestas *online* realizadas a la totalidad hogares que han conformado la muestra del estudio.
Dato real: Para ello se utiliza el software iScan desarrollado por INCIBE, que analiza los sistemas y la presencia de *malware* en los equipos gracias a la utilización conjunta de 50 motores antivirus.

[14] El Estudio señala que el *malware* con mayor presencia en los equipos informáticos es aquel cuyo cometido es lograr un beneficio económico. Así el troyano se encontró en el 37,9% de los ordenadores escaneados y el *adware* publicitario fue detectado en más de un tercio (35,1%). Es más, prácticamente el 60% de los equipos analizados con iScan se encuentran infectados con al menos una muestra de *malware* conocida. De estos, casi dos de cada tres (63,4%) presentan un nivel de riesgo alto debido al potencial peligro que suponen los archivos maliciosos encontrados en ellos.

que se encuentren en él. Estas medidas se clasifican en:
- Automatizables: de carácter pasivo que, por lo general, no requieren de ninguna acción por parte del usuario, o cuya configuración permite una puesta en marcha automática (v. gr. cortafuegos o *firewall*)[15].
- No automatizables: de carácter activo que, por lo general, sí requieren una acción específica por parte del usuario para su correcto funcionamiento (v. gr., contraseñas, copias de seguridad de archivos, partición del disco duro, certificados digitales de firma electrónica, utilización habitual de permisos reducidos, DNI electrónico, cifrado de documentos o datos).
- Preactivas: utilizadas para prevenir y evitar la ocurrencia de incidencias de seguridad y minimizar las posibles amenazas desconocidas y conocidas (v. gr., cortafuegos o *firewall*, programa antivirus, actualizaciones del sistema operativo y programas, actualizaciones del antivirus).
- Reactivas: utilizadas para subsanar una incidencia de seguridad, eliminando amenazas conocidas y/o incidencias ocurridas (v. gr., programa antivirus, actualizaciones del sistema operativo y programas, actualizaciones del antivirus, *plugins* para navegador, programas de bloqueo de ventanas emergentes, programas anti*spam*, programas antifraude, eliminación de archivos temporales o *cookies*).

## II.2. HÁBITOS DE USO DE *SMARTPHONES*

Según estudios especializados en el sector de los *smartphones*, el uso de estos dispositivos aumenta progresivamente[16]. Es más, sus aplicaciones van más allá de los tradicionales usos (efectuar y recibir llamadas, escribir mensajes, jugar), pudiendo realizar vídeollamadas,

[15] Destacan como principales medidas de seguridad automatizables el *software* antivirus (81,7%) y sus actualizaciones (80,5%). Por su parte, en el ámbito de medidas no automatizables, casi el 60% de los usuarios declaran utilizar contraseñas para proteger su equipo y/o documentos, y más de la mitad (52,9%) se preocupan por eliminar los archivos temporales y *cookies* generados durante la navegación a través de la Red.
Resultan curiosos dos datos aportados por el Estudio:
- Un 12,5% de los usuarios deja su red inalámbrica Wi-Fi desprotegida y/o desconoce su estado. Para solucionarlo, facilita un enlace para configurar la red Wi-Fi de modo seguro: http://www.osi.es/protege-tu-wifi
- Únicamente un 8,2% declara utilizar *software* de cifrado en su terminal móvil para evitar que la información que contienen sea accesible por terceros en caso de pérdida o robo. Para solucionarlo, facilita un enlace para proteger y/o conservar la información almacenada en los dispositivos móviles: http://www.osi.es/smartphone-y-tablet

[16] Según iZettle, el proveedor líder europeo de servicios y aplicaciones de pago a través del móvil, habrá 2500 millones de usuarios de smartphones en 2015.
(*Vid*. http://www.marketingdirecto.com/especiales/mobile-marketing-blog/4-previsiones-para-los-pagos-moviles-en-2015-segun-izettle/)
Es más, para 2015 se prevé un crecimiento de los pagos por móvil del 60,8 por ciento.
(*Vid*. http://ecommerce-news.es/servicios/metodos-de-pago/el-volumen-de-s-pagos-moviles-crecera-un-608-en-2015-18476.html)
Y se espera que el 2015 sea el año del despegue definitivo de la industria de los pagos móviles.
(*Vid*. https://www.momopocket.com/tendencias-en-el-sector-de-los-pagos-moviles-para-el-2015/)
Según el Estudio de la ciberseguridad y confianza en los hogares españoles, el 88,1% de los internautas con acceso frecuente a Internet posee un *smartphone* o teléfono móvil "inteligente".

ejecutar pagos[17], comprar *online*, realizar Banca en línea, etc[18].

Los usuarios de *smartphones* muestran su preocupación por la seguridad, constatando el Estudio de la ciberseguridad y confianza en los hogares españoles que la principal incidencia en dispositivos móviles declarada por los usuarios que tuvieron problemas de seguridad es el *spam* (76,6%). La segunda incidencia con mayor ocurrencia es el fraude, sufrido por un 16,3% de los encuestados.

De la interrelación de las incidencias de seguridad (v. gr., extravío, robo, virus o *malware*, suplantación de identidad, intrusión externa, *spam*, fraude) en dispositivos móviles y sus consecuencias (v. gr. robo de datos, pérdida de datos, suplantación de identidad, sustracción de datos *online*, perjuicio económico, suscripción a servicios no solicitados), se desprenden los siguientes resultados[19]: un 54,6% ha experimentado fraude y perjuicio económico; un 45,5%, intrusión externa y robo de datos; un 45,4%, fraude y suscripción a servicios no solicitados; un 44%, extravío y pérdida de datos; un 24,3% suplantación de identidad; un 13,6%, robo y sustracción de datos *online*.

## II.3. BANCA EN LÍNEA Y COMERCIO ELECTRÓNICO

Retomando lo señalado al principio de este trabajo acerca del "Especial Eurobarómetro" sobre seguridad cibernética, en las actividades realizadas *online* los usuarios españoles se distribuyen del siguiente modo[20]: 85% para leer sus *e-mails*, 60% para leer noticias *online*, 58% para redes sociales, 33% para Banca *online*, 29% para comprar productos o servicios, 18% para juegos *online*, 11% para ver televisión, 5% para vender productos y servicios.

[17] Lo último es el *smartphone ticketing*: sistema por el que se puede pagar el transporte público a través del móvil. Por el momento está pensado para funcionar con la descarga de una aplicación al móvil desde la que adquirir uno o varios billetes, así como paquetes de un día, semanales o mensuales, que se pagarán por métodos como PayPal o mediante transacción bancaria a una tarjeta de crédito previamente establecida. Estas *apps* son desarrolladas por las entidades de transporte de cada ciudad y dispuestas para su descarga al *smartphone*, de modo que, a partir de su compra ya sea posible utilizarlas una vez configurados los datos de usuario y cuenta. Eso sí, la validación del billete siempre se deberá realizar frente a un lector y usando el teléfono mediante varios sistemas: uno de los más extendidos es el envío de los billetes o bonos por tiempo determinado al móvil, ya sea a través de un SMS o un correo electrónico (en ambos casos lo que se envía es un enlace a una página web que se abre con el navegador del teléfono y contiene un código bidimensional que se muestra frente a la máquina de validación de billetes, que es un lector de códigos QR); otro sistema consiste en el envío de los billetes en un formato electrónico y sin aspecto gráfico (son señales de radio) que se almacenan en los chips NFC del *smartphone* (el chip recibe la información del billete o bono desde la aplicación que con anterioridad el usuario se instala y, después, la muestra a un lector que valida el billete en el autobús, metro o tren). (*Vid*. http://n-economia.com/noticias/sectores/paga-con-tu-smartphone-smartphone-ticketing-en-el-transporte-publico/)

[18] Según un reciente estudio, en menos de dos años el *smartphone* puede convertirse en nuestro único ordenador. (*Vid*. http://www.wired.com/2015/02/smartphone-only-computer/)

[19] Estudio de la ciberseguridad y confianza en los hogares españoles, p. 41.

[20] *Vid*. tabla QC3 del "Especial Eurobarómetro".

Atendiendo a estos datos, es patente que la Banca *online* y el comercio electrónico se configuran como dos actividades frecuentemente realizadas por los internautas españoles. Del Estudio de la ciberseguridad y confianza en los hogares españoles se colige que los usuarios de estos servicios a través de Internet mantienen buenos hábitos de comportamiento (un porcentaje superior al 73% sigue buenas prácticas), como pueden ser los siguientes: que el dispositivo esté a salvo de *malware*, no dejar el dispositivo desatendido durante el uso de Banca electrónica, no grabar contraseñas importantes en el navegador, utilizar un programa seguro de gestor de contraseñas, monitorizar habitualmente los gastos para asegurar que nadie ha realizado un uso fraudulento de la tarjeta de crédito, emplear tarjetas monedero/prepago ("wallet"), etc.

A la hora de evitar posibles fraudes, el Estudio recuerda que las entidades bancarias nunca solicitan datos y contraseñas de usuario, siendo esta información confidencial[21].

## II.4. FRAUDE *ONLINE*

Las actividades de Banca *online* y comercio electrónico son objeto de potenciales fraudes. El "Especial Eurobarómetro" pone de manifiesto que un 10% de los usuarios de Internet en toda la UE ha experimentado fraude *online*; un 6% ha sufrido robos de identidad; un 12% no ha podido tener acceso a servicios *online* debido a ataques cibernéticos; un 12% ha tenido una cuenta de correo electrónico *hackeada*; y un 7% ha sido víctima de fraude de tarjeta de crédito o de Banca *online*.

Centrándonos en los usuarios españoles y en el Estudio de la ciberseguridad y confianza en los hogares españoles, un 48% de la muestra ha sufrido alguna situación de fraude[22]. Como buenas prácticas por parte del usuario se indica comprar en sitios fiables y desconfiar de gangas; y para los portales se recomienda fomentar la prevención del fraude y la protección de sus usuarios a través de mecanismos de denuncia apropiados, controles sobre la autenticidad, etc.[23]

El mencionado Estudio refleja los intentos de fraude *online* más habituales[24]. A saber:

- Invitación a visitar alguna página web sospechosa: 57,3%.
- Recepción de e-mail ofertando un servicio no solicitado: 50,1%.
- Recepción de una oferta de trabajo que pudiera ser falsa o sospechosa: 44,7%.
- Recepción de productos desde páginas de comercio que pudieran ser falsas: 35,1%.

[21] Se facilita un enlace para detectar correso electrónicos falsos de Banca en línea: http://www.osi.es/es/banca-electronica
[22] Estudio de la ciberseguridad y confianza en los hogares españoles, p. 43.
[23] Indica un enlace al respecto: http://www.osi.es/fraude-online
[24] Estudio de la ciberseguridad y confianza en los hogares españoles, p. 43.

- Recepción de e-mail solicitando claves de usuario: 20,4%.
- Acceso a páginas web falsas de entidades bancarias, comercio o Administraciones: 10,8%.

Asimismo, señala las formas más comúnmente adoptadas por el remitente de la comunicación sospechosa de ser fraudulenta: la imagen de páginas de "comercio electrónico" (26,9%) y de "loterías, casinos y juegos *online*" (26,8%); seguidas por las de "Banco" (24,5%), "operadores de Telecomunicaciones" (21,7%) y "entidades de medios de pago" (13,6%)[25].

Es interesante reseñar que el *phishing* es la estafa más utilizada en Internet. Esta técnica consiste en la creación y distribución de una página web similar a la de una entidad bancaria con la finalidad de obtener las claves de usuario. Y ello está en estrecha conexión con el dato que arroja el Estudio sobre que la principal forma adoptada por el remitente es la entidad bancaria cuando pretente solicitar claves de usuario (54,3%).

En este tipo de estafas cobra especial importancia el *malware*, concretamente los "troyanos bancarios", robando información confidencial a los clientes de Banca y/o de plataformas de pago *online*, reflejándose en la recepción de peticiones de acceso a páginas web falsas de entidades bancarias y/o comercio electrónico, o de e-mails solicitando claves de usuario. De ahí la importancia de realizar un cambio de hábitos tras producirse un incidente de este tipo. Pero el Estudio refleja que sólo el 30,5% ha realizado alguna modificación en sus costumbres, básicamente con las siguientes actuaciones: cambiar las contraseñas (30,5%), actualizar las herramientas de seguridad ya instaladas (19%)[26].

En lo que respecta a los hábitos seguidos por el usuario en los ámbitos de servicios de Banca *online* y de comercio electrónico, ante el intento de fraude, el Estudio indica que un 17,2% utiliza las medidas de seguridad de su entidad bancaria, un 4,8% limita el uso de Banca electrónica, un 5,5% reduce el uso de Banca electrónica, un 13,1% reduce el uso de comercio electrónico, y un 9,2% ha modificado la forma de pago[27].

Si bien es cierto que, a pesar de este escenario, únicamente un pequeño porcentaje de los intentos de fraude acaban suponiendo un perjuicio económico para la víctima (7-8%), no ascendiendo la cuantía a más de 100 euros[28].

Ante este contexto de problemas de seguridad, el 42,3% de los internautas españoles declaran ser capaces de solucionarlos ellos mismos, y casi el 30% solicita ayuda a un familiar o amigo.

[25] *Ibídem*, p. 44.
[26] *Ibídem*, pp. 48 y 49.
[27] *Ibídem*, pp. 51 y 52.
[28] *Ibídem*, p. 46.

Es significativo que menos del 10% de la población española acuda al servicio técnico profesional para estas situaciones[29].

## II.5. e-CONFIANZA Y LIMITACIONES EN LA SOCIEDAD DE LA INFORMACIÓN

La denominada "e-confianza" es el pilar fundamental que sustenta la sociedad de la información y el comercio electrónico, permitiendo a los consumidores o usuarios establecer relaciones seguras con las empresas que comercializan productos o servicios en Internet.

El Estudio de la ciberseguridad y confianza expone el nivel de confianza en Internet de los usuarios españoles, siendo el resultado bastante positivo: un 5,5% confía mucho, un 39,8% bastante, un 42% suficiente, y sólo un 12,7% poco o nada[30]. Es más, un 46,2% de los internautas españoles perciben Internet cada día como más seguro[31].

En lo que respecta a los hábitos en operaciones de compraventa *online* que mayor confianza suponen para el usuario, el pago con PayPal y servicios afines se consolida como la opción preferida. No obstante, se sigue depositando mayor confianza en el trato con otra persona en la entidad bancaria[32] o en el pago con tarjeta de crédito/débito en establecimiento público[33]. Atendiendo a estos últimos supuestos, los usuarios encuestados señalan que no utilizan los servicios de Banca *online* y el comercio electrónico básicamente por su falta de necesidad y/o interés (un 34,2% para el caso de Banca *online* y un 46,8% para el caso de comercio electrónico); el segundo motivo se fundamenta en la falta de confianza en estos servicios (el 32,9% para el caso de Banca *online* y 24,9% para el caso de comercio electrónico).[34] Y todo ello por la percepción que el usuario tiene de los riesgos que entraña la navegación por Internet[35].

Es innegable la interrelación entre la e-confianza y la seguridad en las nuevas tecnologías, configurándose esta última como factor limitante para el usuario en el manejo de nuevos

[29] *Ibídem*, p. 53.
[30] *Ibídem*, p. 55.
[31] No obstante, y atendiendo a la tabla QC4 del "Especial Eurobarómetro", sobre el grado de confianza en la Banca *online* o compra de productos o servicios, la media europea se encuentra en un 70%.
[32] Un 56% prefiere realizar operaciones bancarias en la sucursal y un 38,2% confían en efectuarlas *online*.
[33] Estudio de la ciberseguridad y confianza en los hogares españoles, p. 57.
[34] *Ibídem*, p. 61.
[35] Un 43% percibe el robo y uso de información personal (fotografías, nombre, dirección) sin consentimiento como el principal riesgo; un 37,8% el perjuicio económico (fraude en cuentas bancarias *online*, tarjetas de crédito, compras) derivado de un fraude; el 19,2% restante obedecería a daños en los componentes del ordenador (hardware) o en los programas que utilizan (software). (*Vid*. Estudio, p. 63).
Resulta curioso el test que realiza la Oficina de Seguridad del Internauta (OSI) sobre los conocimientos generales acerca de posibles situaciones de riesgo que pueden plantearse en Internet (*Vid*. https://www.osi.es/es/cuanto-sabes).

servicios[36]. Concretamente, un 48,3% de los usuarios encuestados afirma estar de acuerdo con que la falta de información referente a la seguridad limita su uso de Internet. Asimismo, un 52,3% de los encuestados afirma que emplearía más servicios a través de Internet (v. gr., Banca, comercio electrónico, redes sociales) si le enseñasen a proteger su ordenador y hacer una navegación segura[37].

Por último, una amplia mayoría de los internautas considera que Internet sería más seguro si se empleasen correctamente los programas (77,2%), entendiendo que la propagación de amenazas a través de la Red se debe principalmente a la poca cautela de los usuarios (65,9%). Sin embargo, un 43,6% creen que sus acciones *onlin*e tienen consecuencias en la ciberseguridad, y otro 42,1% opinan que se deben asumir riesgos para disfrutar de las experiencias que ofrece Internet[38].

## III. CONSIDERACIONES FINALES

Aprovechando la celebración en Barcelona hace unos días del *Mobile World Congress*, se pueden destacar varios datos en lo que respecta al uso de *smartphones* en nuestro país. Así, los españoles están a la vanguardia del uso de estos dispositivos y de aplicaciones como la mensajería instantánea, situándose España entre los países con mayor penetración de la banda ancha móvil[39].

Este significativo aumento no debe hacernos olvidar los peligros que entraña la navegación por Internet, sobre todo en lo que concierne a Banca *online* y comercio electrónico. En estos últimos días se ha puesto de manifiesto que el innovador sistema de pago con móvil Apple Pay[40] ha sufrido una oleada de operaciones fraudulentas (cuyo número y valor total no ha

[36] Según el Estudio, la limitación se puede clasificar en: limitación alta (7-10), afectando a un 34,9% de los usuarios; limitación media (4-6), afectando a un 45,1% de los usuarios; limitación baja (0-3), afectando a un 19,9% de los usuarios. (*Vid*. Estudio, p. 60).

[37] *Ibídem.*

[38] *Ibídem*, p. 66.

[39] Informe de Organización para la Cooperación y el Desarrollo Económicos (OCDE), que agrupa a 34 países de los más avanzados. En el mismo se atestigua que España se ha situado en el decimocuarto puesto con mayor penetración de Internet móvil, con 73,3 suscripciones por cada 100 habitantes.

[40] Este sistema funcionará con los nuevos iPhone 6 y el iPhone 6 Plus por NFC, y gracias a la inclusión de un chip específico llamado *Secure Element*. El funcionamiento será el siguiente: en primer lugar habrá que configurar una cuenta y los usuarios podrán transferir los datos de su tarjeta de crédito o débito (American Express, MasterCard y Visa) de su cuenta de la iTunes Store, creando el monedero móvil. Así, cuando el usuario añada una tarjeta de crédito o débito, los números de dicha tarjeta no se almacenarán en el dispositivo ni en los servidores de Apple, sino que se le asignará un número de cuenta, que se cifrará y se almacenará de forma segura en el dispositivo. Posteriormente, cada transacción se autorizará para el referido número de cuenta del dispositivo pero con un número único de un solo uso. No requerirá el número de seguridad de tres cifras que aparece en el reverso de las tarjetas ya que se creará un código de seguridad dinámico para validar el pago de forma segura. Eso sí, las operaciones no serán del todo gratis ya que Apple ha anunciado que cobrará una comisión a las entidades bancarias por cada pago que los usuarios de sus dispositivos realicen con Apple Pay.

trascendido) a consecuencia de piratas informáticos[41]. Éstos introdujeron en el sistema datos de tarjetas de crédito robadas y realizaron compras de gran valor. En sentido estricto la plataforma en sí no ha sufrido el pirateo y, como defienden sus responsables "Apple Pay está diseñado para ser extremadamente seguro y para proteger la información personal de los usuarios"[42].

Concluyendo, si el progresivo incremento de la utilización de Internet (sobre todo a través de dispositivos móviles) para Banca *online* y comercio electrónico no va asociado a una mayor seguridad en la navegación y, fundamentalmente, en los sistemas de autenticación, no sólo nos encontraremos ante un caldo de cultivo idóneo para potenciales y heterogéneos fraudes (y sus consiguientes perjuicios económicos), sino ante un descenso de la e-confianza por parte del usuario, repercutiendo negativamente en el tráfico *online* de actividades que suponen un movimiento considerable en la Red, como son la Banca en línea y el e-comercio.

(*Vid*. http://www.abc.es/tecnologia/informatica-software/20140910/abci-apple-pay-iphone-6-iphone-6-plus-como-funciona-caracteristicas-keynote-201409101443.html).
De hecho, el grupo hotelero *Marriot* ha sido el primero en aceptar el pago a través de Apple Pay, pudiendo los clientes abonar su estancia en algunos hoteles estadounidenses del grupo a partir del próximo verano (al igual que los clientes que tengan el Apple Watch, "wearable" que, a través de una *app*, permitirá a los clientes no sólo pagar la habitación del hotel, sino también abrir y cerrar la puerta de su habitación).
(*Vid*. http://cincodias.com/cincodias/2015/03/11/empresas/1426101225_232235.html)

[41] *Vid*. http://economia.elpais.com/economia/2015/03/06/actualidad/1425635567_610620.html

[42] Es cierto que la responsabilidad de verificar la identidad del titular de la tarjeta antes de ser utilizada para abonar una compra con el móvil recae sobre los Bancos.