LA INFLUENCIA DE LA CIBERSEGURIDAD EN EL MUNDO DIGITAL. ESPECIAL REFERENCIA A LA DIRECTIVA (UE) 2016/1148[1]

Mikael Leal Coronado
Estudiante del Máster en Acceso a la Abogacía
Becario de Colaboración Dpto. Derecho Civil -
Universidad de Castilla-La Mancha

Fecha de publicación: 23 de mayo de 2017

1. INTRODUCCIÓN

Cuando navegamos por Internet para realizar todo tipo de operaciones, ya sea adquirir un determinado bien o servicio, consultar la prensa, buscar información o llevar a cabo banca online -por mencionar algunas actividades diarias en constante auge-, estamos expuestos a todo tipo de amenazas en la Red, lo que supone un riesgo para los consumidores y usuarios. Prueba constatable de ello es el ciberataque masivo perpetrado hace unos días en ordenadores a escala global, y que ha puesto en jaque, entre otros, a empresas de comunicación, hospitales y entidades bancarias[2].

En el concreto ámbito de los medios de pago electrónicos, objeto de recurrente análisis por parte de CESCO, este problema se ve acrecentado, convirtiéndose el potencial ciber-riesgo en una barrera para muchas personas a la hora de decidir si comprar o no un producto por Internet, o realizar la mencionada compra de forma física.

Es en este escenario, donde la seguridad ocupa un papel central para el desarrollo y crecimiento, no sólo de los medios de pago electrónicos, sino de los nuevos negocios digitales, los particulares, comerciantes y empresas en general están apostando cada vez más por este nuevo mercado que ofrece infinidad de oportunidades. Es por ello que, a mayor inversión e incremento de la ciberseguridad, se conseguirá un mayor afianzamiento de la e-

[1] Trabajo realizado en el marco del Proyecto "Presente y futuro de los medios de pago en una sociedad de transformación digital" bajo la tutela de la Prof. Mª Nieves Pacheco Jiménez, concedido por Beca de colaboración en el Departamento de Derecho Civil e Internacional Privado de la Facultad de Ciencias Sociales de Cuenca (UCLM) por el Ministerio de Educación, Cultura y Deporte.

[2] *Vid*. http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html y http://www.bbc.com/mundo/noticias-39929920 (Consultados 16/05/2017).

confianza de todos los agentes intervinientes, propiciando así mayores posibilidades de elección y de crecimiento.

En este punto se hace necesaria una adecuada regulación que siente las bases y los objetivos para poder garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea; regulación que viene de la mano de la Directiva 2016/1148, que se analizará a lo largo de este estudio.

Pero es más, a nivel de usuario, es necesario conocer la importancia de disponer de medidas de seguridad y su relación con el *malware,* teniendo en cuenta una serie de aspectos para evitar incidentes de seguridad, con el objeto de sacar el máximo partido posible a los nuevos medios de pago y poder interactuar en un entorno digital con total confianza y seguridad en el mismo.

2. SITUACIÓN ACTUAL DE LA CIBERSEGURIDAD

En un ámbito como el descrito, cuyo progreso está fuertemente marcado por la innovación y los avances tecnológicos, la seguridad y la regulación normativa apropiada determinan su desarrollo presente y futuro. De hecho, la seguridad se ha configurado como el elemento central para el progreso de los medios de pago, estando condicionados la aparición y el óptimo progreso de estos últimos a la necesidad de implementar las medidas de seguridad[3].

En los pagos electrónicos concurren determinados riesgos, pudiendo provenir de alguna modalidad de fraude, que varían de un método de pago a otro, así como del soporte tecnológico o de la solución que se utilice en función de su gravedad y dificultad, por lo que el propósito de disminuir estos riesgos hace preciso establecer requisitos y medidas de seguridad[4]. De ahí que el uso cada vez más extendido de los medios de pago electrónicos por los consumidores necesite de la consolidación de instrumentos jurídicos concretos que consigan incrementar la rapidez de su uso, así como una mayor facilidad y, sobre todo, seguridad. Ello se alcanzará mediante la formación de herramientas técnicamente seguras, clarificando la trascendencia jurídica de las mismas y la obtención de una proporción entre los diferentes intereses que se ponen en juego[5].

Partiendo de esta premisa, a mediados de diciembre de 2014, la Autoridad Bancaria Europea[6] (en lo sucesivo EBA), presentó un elenco de directrices para poner en funcionamiento la

[3] MALDONADO, L. (Coord.) *et al*: "Los medios de pago, un paisaje en movimiento", Informe del Centro del Sector Financiero de PwC e IE Business School, 2015, pp. 54 y 61 (Disponible en: http://www.pwc.es/es/publicaciones/financiero-seguros/assets/medios-pago-paisaje-movimiento.pdf).

[4] MARTÍNEZ GONZÁLEZ, M.: "Mecanismos de seguridad en el pago electrónico", en MATA Y MARTÍN, R. M. (dir.); JAVATO MARTÍN, A. Mª. (coord.) *et al: Los medios electrónicos de pago: problemas jurídicos,* Comares, Granada, 2007, p. 6.

[5] MATA Y MARTÍN, R. M.: *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*, Aranzadi, Cizur Menor, 2007, p. 17.

[6] Autoridad Bancaria Europea o *"European Banking Authority"* (EBA).

seguridad de los consumidores de la Unión Europea en la realización de sus compras a través de Internet con el propósito de combatir el fraude *online* y así incrementar la confianza de los consumidores en los servicios de pago, centrándose estas recomendaciones en el inicio de los pagos y en el acceso a los datos sensibles, que requieren de la protección necesaria mediante una autenticación reforzada de la identidad del cliente-usuario.[7]

Y es que en el sector de los medios de pago móvil hay todavía una parte importante de la población que no considera estos como instrumentos seguros. En el cambio de óptica de este sector poblacional incide la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015[8], sobre servicios de pago en el mercado interior, al establecer un elenco de requisitos de seguridad de carácter reforzado, estando obligados los prestadores de servicios de pago a poner en conocimiento del Banco Central Europeo y de la EBA cualquier incidente grave, ya sea operativo o en relación con la seguridad de la información de sus sistemas operativos, así como de proporcionar información a los clientes, si hubiera un retraso indebido en su operativa o determinado incidente que pueda ocasionar daños en sus intereses financieros[9].

Además de ello, la Comisión Europea pretende revisar antes de septiembre del presente año la estrategia de ciberseguridad de la Unión Europea, así como el mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), con el objetivo de adecuarlo al nuevo contexto de ciberseguridad de la Unión. A ello hay que añadir el constante trabajo planteando una serie de medidas adicionales sobre normas, certificación y etiquetado de ciberseguridad, resultando así más ciberseguros todos los objetos conectados[10].

2.1.Importancia de las medidas de seguridad y su relación con el *malware*

Este panorama tecnológico, en el que confluyen multitud de dispositivos móviles (v. gr., *smartphones*, *tablets*), la nube, el Internet de las Cosas "IoT", etc., ha dado como resultado que los ciberdelincuentes pongan su punto de mira en este tipo de dispositivos,

---

La EBA "es una autoridad independiente de la UE que trabaja para garantizar un nivel efectivo y coherente de regulación y supervisión prudencial en todo el sector bancario europeo. Sus objetivos generales son mantener la estabilidad financiera en la Unión Europea (UE) y velar por la integridad, la eficiencia y el correcto funcionamiento del sector bancario". Su principal función es contribuir a la formación de un código normativo único para el sector bancario, que proporcione la armonización de un conjunto único de normas para las instituciones financieras en toda la UE.
Vid. https://www.eba.europa.eu/languages/home_es (Consultado 03/05/2017).

[7] PACHECO JIMÉNEZ, Mª. N.: "La e-confianza del internauta español: retos de ciberseguridad", en *Centro de Estudios de Consumo* [online], 16 de marzo de 2015, p. 2. (*Vid*. www.uclm.es/centro/cesco)

[8] DOUE núm. 337, de 23 de diciembre de 2015.

[9] Diario La Ley, nº 8825, Sección Tribuna, 16 de Septiembre de 2016, Ref. D-326, Ed. Wolters Kluwer.

[10] *Vid.* http://diariolaley.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAFXMMQqAMAwAwN90TgqiDh1EXZ3cRU0KQWmKxYK_FwcF9-OEyA09AKCta6jQZD6SaHAWsIQCwQQlHrvWnYHYS2B6iPir03W8Ijs_74kNL6rbb5q-QVIT46GZ6V0RrS1vbOISgXsAAAA=WKE **(**Consultado 11/05/2017).

pero sin olvidar a los tradicionales ordenadores y todos aquellos terminales que se encuentren conectados[11]. Por ello, y con el fin de evitar ser una de las víctimas de los ciberdelincuentes, es preciso disponer de medidas de seguridad, entendidas como "programas o acciones utilizadas por el usuario para proteger el ordenador y los datos que se encuentren en este". Estas medidas pueden ser[12]:

- Automatizables: son de carácter pasivo y, en general, no precisan de ninguna acción por parte del usuario, o su configuración permite que se pongan en marcha de forma automática.

- No automatizables: son de carácter activo y, en general, precisan de una actuación concreta por parte del usuario para su buen funcionamiento.

- Proactivas: se utilizan para prevenir y evitar las posibles incidencias de seguridad, minimizando amenazas desconocidas y también conocidas.

- Reactivas: se utilizan para corregir una incidencia de seguridad mediante la eliminación de amenazas conocidas y/o incidencias ocurridas.

Pues bien, con estas medidas lo que se pretende es hacer frente a todas aquellas amenazas provenientes de Internet, como el *malware*, que hace referencia a "todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un PC/portátil o dispositivo móvil (*tablet*, *smartphone*, relojes inteligentes, etc.) sin el consentimiento del propietario". Aunque generalmente los conocemos como virus, en realidad se trata de una expresión más amplia que abarca otros tipos[13].

Merece especial referencia el *ransomware*[14], centrado cada vez más en dispositivos móviles. Su funcionamiento se basa en provocar una infección maliciosa, teniendo la víctima la posibilidad de recuperar los datos que han sido secuestrados a cambio de una contraprestación dineraria. Cabe señalar que el pago de este rescate puede ser una opción desacertada ya que no se sabe con certeza si la información será recuperada[15] o seguirán

---

[11] *Vid.* https://www.osi.es/es/actualidad/blog/2017/02/02/tendencias-en-ciberseguridad-para-2017 (Consultado 03/05/2017).

[12] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ONTSI): "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles", 2017, p. 8. (Disponible en: http://www.ontsi.red.es/ontsi/sites/ontsi/files/Ciberseguridad%20y%20confianza%20en%20los%20hogares%20espa%C3%B1oles%20%28abril%202017%29.pdf)

[13] *Ibídem*, p. 31.

[14] El *ransomware* es la "extorsión que se realiza a través de un software malicioso o *malware* que se introduce en los equipos y que secuestra la información que contienen, impidiendo el acceso a la misma, generalmente cifrándola y solicitando un rescate a cambio de su liberación". *Vid.* https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-recuerda-los-dispositivos-moviles (Consultado 03/05/2017).

[15] Los expertos señalan que la posibilidad de recuperar la información oscila entre un 30% y 40%. *Vid*. http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html (Consultado 16/05/2017)

pidiendo más dinero a cambio, además de estar contribuyendo al lucro de una actividad delictiva. Los expertos señalan que este tipo de extorsión estará a la vanguardia en este año, habiendo crecido en variedad y sofisticación[16]. Así lo hemos podido comprobar en el ciberataque mundial que ha infectado a multitud de sistemas informáticos en diferentes países a través del *ransomware* denominado WanaCrypt0r, que, tras instalarse en el equipo, bloquea el acceso a los ficheros del dispositivo afectado requiriendo un rescate para permitir de nuevo el acceso y recuperar los datos secuestrados[17].

A la vista de las complicaciones descritas, resulta imprescindible contar con una correcta solución de seguridad instalada; aunque es cierto que los ciberdelincuentes actúan de manera rápida y se van reinventando, por lo que es importante tener en cuenta que la mejor protección es utilizar medidas preventivas para impedir que nuestros sistemas se vean amenazados y afectados. De esta manera, el hecho de que una buena parte de los usuarios no empleen medidas de seguridad básicas, la poca supervisión sobre las aplicaciones en los mercados oficiales, y la utilización de enlaces maliciosos en los sistemas de mensajería, pone a los dispositivos electrónicos, y aún más a los *smartphones*, en el punto de mira ideal para los ciberdelincuentes[18].

2.2. Recomendaciones para evitar incidencias en seguridad

Atendiendo a este panorama digital, se prevé que a lo largo del presente año 2017 se sigan ocasionando intentos de micro estafas a través de números de tarificación adicional o por medio de suscripción a SMS Premium, aplicaciones falsas o maliciosas en mercados no oficiales, secuestro de datos a través de *ransomwares* con el fin de obtener un lucro extorsionando a las víctimas, así como ataques de denegación de servicio por *botnets* –tipo de virus capaz de tener el control de un ordenador de modo remoto-[19]. Por ello, cuando usamos el ordenador, *smartphone* o *tablet* vinculados a Internet, debemos informarnos del funcionamiento de los mencionados dispositivos, y de cómo utilizarlos de forma segura y adecuada para hacer frente a las posibles amenazas y riesgos que nos atacan.

De ahí que haya que tener en cuenta una serie de precauciones para proteger nuestros dispositivos electrónicos, como son las ofrecidas por la Oficina de Seguridad del Internauta (OSI)[20]:

---

[16] *Vid.* https://www.osi.es/es/actualidad/blog/2017/02/02/tendencias-en-ciberseguridad-para-2017 (Consultado 03/05/2017)

[17] *Vid.* http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html (Consultado 16/05/2017)

[18] *Vid.* http://www.revistapagos.com//2015/12/predicciones-de-ciberseguridad-para-2016/ (Consultado 03/05/2017).

[19] *Vid.* https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-recuerda-los-dispositivos-moviles (Consultado 04/05/2017).

[20] *Vid.* https://www.osi.es/es/actualidad/blog/2015/12/11/si-queremos-mantener-nuestros-dispositivos-seguros

- Conocer los virus informáticos, para saber cómo se infectan los dispositivos, las consecuencias de los mismos y las medidas de protección aplicables.

- Información sobre actualizaciones de seguridad para conocer su importancia, de dónde provienen y la forma de actuar ante una nueva actualización.

- Saber crear cuentas de usuarios y su relación con la seguridad.

- Conocer la forma de proteger los dispositivos electrónicos, entre ellos el *smartphone* y la *tablet,* para evitar la instalación de aplicaciones peligrosas y ser víctimas de estafas[21], proteger la información almacenada en ellos, evitar las conexiones inseguras, y apreciar los riesgos que podría conllevar que se eliminen las restricciones del fabricante del dispositivo.

Es crucial, por tanto, estar preparados y dotar a nuestros dispositivos de una protección adecuada para prevenir cualquier tipo de amenaza proveniente de Internet, por lo que habrá que disponer de contraseñas robustas, controlar las aplicaciones instaladas en los dispositivos, así como las redes wifi a las que se accede, debiendo estar actualizados (preferentemente a través de las actualizaciones lanzadas por los fabricantes), con el objeto de que nuestros dispositivos no entrañen riesgo alguno evitando potenciales problemas de seguridad[22]. Y ello porque el uso de programas/archivos que provienen de fuentes dudosas puede ocasionar variados incidentes de seguridad así como la instalación en los dispositivos móviles de alguna clase de *malware*[23].

Queda patente que la mayor problemática que encontramos a la hora de navegar por la Red es proteger la privacidad e integridad, es decir, imposibilitar que un tercero que no está autorizado intervenga, y que ninguna persona pueda suplantar nuestra identidad o la del interlocutor. Para ello la criptografía se configura como una forma efectiva para acreditar que los datos se muevan con toda garantía por la Red, consistiendo en transformar un texto en una serie de caracteres inconexos que sólo tendrán sentido para la persona que posea la clave exacta -la cual se genera a través de complejos algoritmos matemáticos-. Existirán comunicaciones en las que el mensaje se cifre y descodifique utilizando una misma clave y otras en las que se use una clave para encriptar y otra para leer, aumentando el nivel de seguridad y siendo necesario que el mensaje vaya

(Consultado 04/05/2017).

[21] A lo largo de la historia la estafa tiene una vinculación respecto a hechos relacionados con el uso ilícito de medios de pago, permitiendo al autor obtener un enriquecimiento injusto. Los estafadores han ido adecuando los medios de comisión práctica a los nuevos contextos y situaciones, buscando a lo largo de los años la manera de alcanzar beneficios que no son legítimos a través de los instrumentos de pago mediante un uso fraudulento. *Vid.* MATA Y MARTÍN, R. M.: *Estafa convencional…, op. cit.*, p. 21.

[22] *Vid.* https://www.osi.es/es/actualidad/blog/2017/02/02/tendencias-en-ciberseguridad-para-2017 (Consultado 04/05/2017).

[23] ONTSI: "Estudio…", *op. cit.,* p. 28.

autentificado, además, con una firma digital, que verifique que el remitente es quien afirma ser[24].

Para un buen número de empresas el cifrado es necesario para la protección de la información de identificación personal, así como de datos de clientes o consumidores; siendo el cifrado en la nube aún más significativo, puesto que las empresas que buscan la eficiencia, optimización y ahorro monetario, mueven gran cantidad de información en un contexto asentado en la citada nube[25].

Por último, reseñar que, además de la criptografía, los sistemas de identificación biométrica -que podrían reconocer la palma de la mano, las características faciales o la voz- incrementan de manera considerable los niveles de seguridad. Si bien es cierto que ningún sistema de seguridad supone una garantía al cien por cien, el uso combinado de firmas, certificados digitales, claves y sistemas de reconocimiento biométrico, como pueden ser los sensores de huella, hará que quien pretenda cometer un fraude o suplantar la identidad se encuentre con muchos obstáculos[26].

3. e-CONFIANZA Y SEGURIDAD EN EL ENTORNO DIGITAL

Parece aceptable que la sensación de inseguridad que supone para el consumidor y usuario tener que introducir su número de tarjeta en Internet es una de las barreras primordiales para el progreso del comercio electrónico[27]. Así, es innegable la estrecha interrelación entre seguridad y e-confianza de los consumidores y usuarios, pues una depende de la otra, resultando favorable el porcentaje de confianza depositado por los consumidores en Internet.

Y si a las cifras nos remitimos, un 4,3% tiene mucha confianza, un 36,9% bastante confianza, un 44,9% suficiente confianza, un 11,7% poca confianza y solamente un 2,2% no tiene ninguna confianza[28]. No obstante, la seguridad constituye una barrera para los usuarios en el uso de nuevos servicios en Internet. Según los datos ofrecidos por el Estudio sobre la Ciberseguridad y Confianza en los hogares españoles, un 47% está de acuerdo en que la falta de información en lo relativo a la seguridad en el uso de las nuevas tecnologías limita el mencionado uso, y un 51,4% está de acuerdo en que emplearía más servicios mediante el uso de Internet si le enseñasen la manera de proteger su ordenador pudiendo tener una navegación segura. Además de ello, una gran parte de los usuarios reconocen que Internet gozaría de mayor seguridad mediante un empleo correcto de los programas (76,8%), y que la proliferación de amenazas a través de Internet tiene que ver principalmente con la poca precaución de los usuarios (65,9%). Sin embargo, un 45,4% de los usuarios consideran que

[24] DORAL, A.: *Seguridad en Internet y medios de pago electrónicos*, Prentice Hall, Madrid, 2002, pp. 22, 44 y 46.
[25] *Vid*. http://diarioti.com/tendencias-ciberseguridad-2016/92929 (Consultado 04/05/2017).
[26] DORAL, A.: *Seguridad en Internet…, op. cit.*, pp. 52 y 53.
[27] *Ibídem*, pp. 3 y 4.
[28] ONTSI: "Estudio…", *op. cit.*, p. 56.

sus acciones *online* acarrean consecuencias en la ciberseguridad y un 44,4% creen que se tienen que tomar ciertos riesgos para un buen disfrute de las experiencias que brinda Internet[29].

Con estos datos en la mano resulta evidente que se debe seguir avanzado e invirtiendo en seguridad, considerándose como un elemento imprescindible en este entorno de Internet y nuevas tecnologías. Y ello porque sin la misma habría un descenso paulatino de la e-confianza de los consumidores y usuarios, dejando a los ciberdelincuentes campar a sus anchas en este escenario tecnológico, en el que aumentan paulatinamente las transacciones y pagos electrónicos, debido al avanzado desarrollo de los mismos y las ventajas que suponen. Pero sin olvidarnos, claro está, de los riesgos que conllevan.

4. LA DIRECTIVA DE CIBERSEGURIDAD (UE) 2016/1148

4.1. Principales consideraciones

En este marco de no retorno y ante las evoluciones producidas, se hace necesaria una regulación a nivel europeo para proteger a todos los actores participantes de los incidentes de seguridad. Así, la Directiva (UE) 2016/1148[30] del Parlamento Europeo y del Consejo, de 6 de julio de 2016, nace con la finalidad de establecer medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, para, a la postre, mejorar el funcionamiento del mercado interior, como se desprende del artículo 1 de la presente Directiva.

Y es que "las redes y sistemas de información desempeñan un papel crucial en la sociedad; su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior" (Considerando 1). De manera que "la seguridad de las redes y sistemas de información es fundamental para el correcto funcionamiento del mercado interior" (Considerando 3), puesto que "la magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información" (Considerando 2).

Ante esto, y según se desprende del Considerando 6, se hace preciso dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información por medio de un planteamiento global en la Unión que integre una serie de requisitos mínimos comunes en materia de:

-Desarrollo de capacidades y planificación.

-Intercambio de información.

[29] ONTSI: "Estudio…", *op. cit.,* pp. 62 y 67.
[30] DOUE núm. 194, de 19 de julio de 2016.

-Cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

Ello no obsta para que los operadores de servicios esenciales y los proveedores de servicios digitales puedan aplicar medidas de seguridad más estrictas que las previstas en la mencionada norma. Atendiendo a ello, "la presente Directiva debe entenderse sin perjuicio de que los Estados miembros puedan adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de su seguridad, preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales" (Considerando 8), siendo necesario que "a fin de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, cada Estado miembro debe disponer de una estrategia nacional de seguridad de las redes y sistemas de información que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar" (Considerando 29).

En cuanto a la exigencia de cooperación y comunicación transfronterizas, y de aplicación efectiva de la Directiva, "es necesario que cada Estado miembro designe, sin perjuicio de las disposiciones normativas sectoriales, un punto de contacto único nacional que se encargue de coordinar las cuestiones relacionadas con la seguridad de las redes y sistemas de información y de la cooperación transfronteriza a escala de la Unión […]; dado que la finalidad de la presente Directiva es mejorar el funcionamiento del mercado interior mediante la creación de un clima de confianza y seguridad, los organismos de los Estados miembros deben poder cooperar eficazmente con los agentes económicos y han de estar estructurados en consecuencia" (Considerando 31).

4.2. Aspectos clave

Con el fin de lograr el objetivo ya mencionado, esto es, lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión, el artículo 1 de la Directiva en su apartado segundo establece una serie de medidas, que son desarrolladas pormenorizadamente a lo largo de todo su articulado; a saber:

- "Establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información".

- "Crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos".

- "Crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, "red de CSIRT", por sus siglas en inglés de *"Computer Security Incident Response Teams"*) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz".

- "Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales".

- "Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información".

Entre todas estas medidas que implanta la Directiva, destacan particularmente los requisitos en materia de seguridad y notificaciones para los operadores de servicios esenciales y para los proveedores de servicios digitales. Respecto a los primeros, y para su plena aplicación, "los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones"; igualmente "velarán por que los operadores de servicios esenciales tomen medidas adecuadas para prevenir y reducir al mínimo los efectos de los incidentes que afecten la seguridad de las redes y sistemas de información utilizados para la prestación de tales servicios esenciales con el objeto de garantizar su continuidad" (*ex* art. 14, apartados 1 y 2). Y en cuanto a los requisitos en materia de seguridad de las redes y sistemas de información de los proveedores de servicios digitales, al igual que los proveedores de servicios esenciales, tendrán que adoptar medidas técnicas y organizativas adecuadas y proporcionadas en el marco de la oferta de servicios en la Unión a que hace referencia el anexo III de la Directiva, de conformidad con el art. 16.1, que además continua estableciendo que, "habida cuenta de los avances técnicos, dichas medidas garantizarán un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado, y tendrán en cuenta lo siguiente:

-La seguridad de los sistemas e instalaciones.

-La gestión de incidentes.

-La gestión de la continuidad de las actividades.

-La supervisión, auditorías y pruebas.

-El cumplimiento de las normas internacionales".

Para dar cumplimiento a estas y todas las medidas instituidas en el texto de la Directiva, los Estados miembros tendrán que adoptar y publicar, como muy tarde el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas que sean necesarias, con el fin de dar cumplimiento a lo establecido en la Directiva 2016/1148, pues así se establece en su artículo 25.

5. CONSIDERACIONES FINALES

Es innegable que la ciberseguridad se configura como el elemento central para el desarrollo de multitud de negocios digitales, expuestos a múltiples, variados y sofisticados riesgos, por

lo que se hace necesario disponer de adecuadas medidas de seguridad, así como conocer las precauciones básicas para proteger nuestros dispositivos de incidentes de seguridad o amenazas provenientes de Internet. En el continuo avance de la implementación de elementos de seguridad, la criptografía se configura como una buena manera de acreditar que los datos y el dinero se mueven por la red con toda garantía; sin olvidar que los sistemas de identificación biométrica van ganando terreno en el ecosistema de los medios de pago.

Es constatable la relación que existe entre seguridad y e-confianza de los consumidores y usuarios, puesto que la falta de seguridad de un determinado medio de pago tiene como resultado una pérdida de confianza en el mismo, generando un efecto negativo en el crecimiento de los medios de pago electrónicos, y, por consiguiente, en el comercio electrónico. Si bien ningún sistema de seguridad es lo suficientemente seguro para estar totalmente protegidos, lo cierto es que es imprescindible estar prevenidos y tomar conciencia de los riesgos a los que nos exponemos, pues, como ya se ha podido comprobar, los ciberdelincuentes actúan a pasos agigantados, reinventando los esquemas para cometer una actividad delictiva, lo que implica la necesidad de estar preparados y no esperar a instalar una concreta solución de seguridad demasiado tarde.

En definitiva, para aumentar el nivel de e-confianza y fomentar un entorno digital seguro, es necesario establecer importantes medidas que garanticen un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea; objetivo que pretende conseguir la Directiva 2016/1148, pero cuya transposición a nuestro país no tendrá lugar hasta mayo de 2018. Aunque, quizás para esa fecha, y dadas las previsiones tecnológicas, ya se hayan producido nuevos y cada vez más sofisticados incidentes de seguridad. De ahí que sea imprescindible una rápida actuación por parte de todos los agentes implicados para frenar los mismos.

6. BIBLIOGRAFÍA

Diario La Ley, nº 8825, Sección Tribuna, 16 de Septiembre de 2016, Ref. D-326, Ed. Wolters Kluwer.

DORAL, A.: *Seguridad en Internet y medios de pago electrónicos*, Prentice Hall, Madrid, 2002.

MALDONADO, L. (Coord.) *et al*: "Los medios de pago, un paisaje en movimiento", Informe del Centro del Sector Financiero de PwC e IE Business School, 2015.

MATA Y MARTÍN, R. M. (dir.); JAVATO MARTÍN, A. Mª. (coord.) *et al: Los medios electrónicos de pago: problemas jurídicos*, Comares, Granada, 2007.

MATA Y MARTÍN, R. M.: *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*, Aranzadi, Cizur Menor, 2007.

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN (ONTSI): "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles", 2017.

PACHECO JIMÉNEZ, Mª. N.: "La e-confianza del internauta español: retos de ciberseguridad", en *Centro de Estudios de Consumo* [online], 16 de marzo de 2015.

Páginas web consultadas

https://www.eba.europa.eu/languages/home_es (Consultado 03/05/2017)

https://www.osi.es/es/actualidad/blog/2017/02/02/tendencias-en-ciberseguridad-para-2017 (Consultado 03 y 04/05/2017).

https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-recuerda-los-dispositivos-moviles (Consultado 03 y 04/05/2017).

http://www.revistapagos.com//2015/12/predicciones-de-ciberseguridad-para-2016/

(Consultado 03/05/2017).

https://www.osi.es/es/actualidad/blog/2015/12/11/si-queremos-mantener-nuestros-dispositivos-seguros (Consultado 04/05/2017).

http://diarioti.com/tendencias-ciberseguridad-2016/92929 (Consultado 04/05/2017).

http://diariolaley.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAFXMMQqAMAwAwN90TgqiDh1EXZ3cRU0KQWmKxYK_FwcF9-OEyA09AKCta6jQZD6SaHAWsIQCwQQlHrvWnYHYS2B6iPir03W8Ijs_74kNL6rbb5q-QVIT46GZ6V0RrS1vbOISgXsAAAA=WKE **(**Consultado 11/05/2017).

http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html (Consultado 16/05/2017).

http://www.bbc.com/mundo/noticias-39929920 (Consultado 16/05/2017).

http://www.pwc.es/es/publicaciones/financiero-seguros/assets/medios-pago-paisaje-movimiento.pdf

www.uclm.es/centro/cesco

http://www.ontsi.red.es/ontsi/sites/ontsi/files/Ciberseguridad%20y%20confianza%20en%20los%20hogares%20espa%C3%B1oles%20%28abril%202017%29.pdf