20/04/16

Nota de Actualidad 11 / 2016

Apple, el FBI y la encriptación digital

Centro de Análisis y Prospectiva
Gabinete Técnico de la Guardia Civil

Apple, el FBI y la encriptación digital:

la lucha contra el terrorismo vs la privacidad de los consumidores

Desencadenante: atentado de San Bernardino

El pasado 2 de diciembre de 2015, una pareja de origen pakistaní establecida en Estados Unidos inició un tiroteo masivo en un centro de servicios sociales de San Bernardino, California. El episodio finalizó con la muerte de catorce personas y más de veinte heridos. Los autores del atentado fueron abatidos por la policía durante la persecución posterior. El tiroteo fue considerado un acto terrorista perpetrado por terroristas locales inspirados en grupos extranjeros[1] y desencadenó una batalla legal entre el FBI y Apple a raíz de la petición por parte del FBI de obtener acceso a la información contenida en el iPhone del terrorista Syed Rizwan Farook.

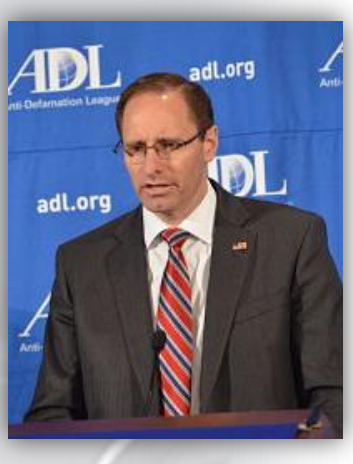
Encriptación y puertas traseras

Tras los atentados del 11-S, Estados Unidos eliminó aquellas leyes relacionadas con el derecho a la intimidad o a la privacidad de datos personales tal y como se entienden y acatan en Europa, de manera que los cuerpos policiales y las agencias de inteligencia accedían a datos sin necesidad de orden judicial –fuesen información bancaria, llamadas por teléfono, mensajería instantánea o cualquier otro tipo de datos recogidos en Internet dentro de un servidor situado en Estados Unidos o de una compañía estadounidense[2].

[1] Ortiz, E. (2015). *San Bernardino Shooting: Timeline of How the Rampage Unfolded*. **NBC News**. Obtenido de http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernardino-shooting-timeline-how-rampage-unfolded-n473501

[2] Hidalgo, C. (2016). *El Gobierno de EEUU empieza a encontrar resistencia al acceso a los datos de los ciudadanos*. **BEZ**. Obtenido de http://www.bez.es/966085299/El-Gobierno-de-EEUU-empieza-a-encontrar-resistencia-al-acceso-a-los-datos-de-los-ciudadanos.html

15 años después, las fuerzas de seguridad americanas y sus servicios de inteligencia –siendo lo más destacados el FBI, la NSA y la CIA–, han optado por reforzar y ampliar la política de puertas traseras o *backdoors* en vez de replanteársela ante las numerosas críticas recibidas a raíz de los acontecimientos. Michael C. Steinbach, director adjunto para el Contraterrorismo del FBI, declaró en el Congreso hace unos meses que las compañías tecnológicas tienen la obligación de ayudarles a prevenir la encriptación «por encima de todas las cosas», puesto que el mismo Dáesh utiliza mensajes encriptados en herramientas de mensajería (ibíd.)



Las puertas traseras son un método que permite saltarse las medidas de seguridad impuestas por las empresas a sus propios productos y suelen insertarse en un programa o algoritmo. Por lo tanto, si Apple, Google o Microsoft creasen puertas traseras para los datos encriptados de sus dispositivos informáticos, las fuerzas de la ley y el Gobierno podrían intervenirlos siempre que quisieran[3]. La encriptación nunca vuelve a ser tan segura como antes una vez que se han instalado las puertas traseras. Continuamente hay actores estatales violando las defensas de los departamentos informáticos corporativos y es factible, por ejemplo, que el gobierno de China sea capaz de elaborar un dossier con los hábitos de consumo de cada ciudadano estadounidense (ibíd.).

Por otro lado, la encriptación se ha convertido en un fenómeno mundial cuyo número de seguidores aumenta todos los días. Según el estudio más reciente de este año, hay al menos 865 productos de hardware o software que incorporan sistemas de cifrado de 55 países diferentes, muchos de ellos son paraísos fiscales[4]. La encriptación se define como el proceso de codificación y descodificación de mensajes en el cual solo los agentes

[3] Nims, C. (2016). *Ciberseguridad: ¿hacen falta las puertas traseras?* **Expansión: Economía Digital**. Obtenido de http://www.expansion.com/economia-digital/innovacion/2016/01/24/569fb6c8268e3eb3358b4594.html

[4] Peirano, M. (2016). *Imponer puertas traseras no detendrá el cifrado de datos (ni el terrorismo)*. **El Diario**. Obtenido de http://www.eldiario.es/cultura/tecnologia/privacidad/Imponer-puertas-traseras-detendra-cifrado_0_483652441.html

autorizados pueden descifrar el contenido[5]. A la hora de que los gobiernos exijan la descodificación de los mensajes encriptados, sin estar ellos autorizados, las empresas tecnológicas tienen pocas opciones: o abandonar el país donde operan o proveer a sus clientes con una versión de sus servicios mucho más vulnerable[6].

Operación Blockbuster

El ciberataque que sufrió la productora Sony en 2014 es uno de los más recientes y de importancia en cuanto a impacto y respuesta. El grupo atacante fue clasificado dentro de la categoría Amenaza Permanente Avanzada (APT por sus siglas en inglés), lo cual quiere decir que se trataba de una organización con abundancia de recursos técnicos y humanos, técnicas de espionaje y gran cantidad de información acerca de los puntos vulnerables del target[7]. En una gran mayoría de los casos no se trata solo de intereses privados, sino de actores estatales que operan según los intereses militares, políticos y económicos del gobierno en cuestión.

La Operación Blockbuster se puso en marcha como respuesta al caso Sony, tratándose de la primera gran alianza privada contra las APT. De lo que se trata es de poner en común bases de datos sobre las amenazas potenciales o existentes para que las empresas puedan protegerse unas a otras en vez de competir mutuamente. Por regla general se procede con cuidado al atribuir el ataque a un Estado específico o a una iniciativa privada de atacantes a sueldo (ibíd.) En este caso, existen grandes posibilidades de que Corea del Norte fuese el generador del ataque lo que, de todas formas, demuestra que hay Estados y actores gubernamentales interesados en acceder a información de empresa privadas y que, en ocasiones, las alegaciones sobre crimen y terrorismo encubren otro tipo de objetivos que busca el Estado y que no se corresponden únicamente con la seguridad del ciudadano.

---

[5] Wu, T. et al. *The ethics or not of massive government surveillance*. Obtenido de https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html

[6] Peterson A. (2016). *The debate over government 'backdoors' into encryption isn't just happening in the U.S.* **The Washington Post**. Obtenido de https://www.washingtonpost.com/news/the-switch/wp/2016/01/11/the-debate-over-government-backdoors-into-encryption-isnt-just-happening-in-the-u-s/

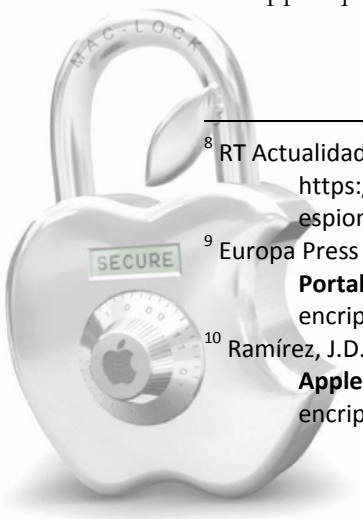
[7] Hidalgo, C. (2016). *Las empresas se alían contra el ciberespionaje económico*. **BEZ**. Obtenido de http://www.bez.es/617447150/Identificado-el-grupo-responsable-del-ataque-y-la-crisis-de-Sony-Pictures.html

El caso FBI vs Apple

El FBI se opone a las medidas de seguridad de datos de los gigantes tecnológicos Google y Apple. Para ellos, la encriptación no supone una característica tecnológica cualquiera, sino una caja fuerte indestructible, en palabras del director del FBI James Comey, lo cual les impide realizar investigaciones penales como corresponde[8]. Se ha llegado incluso a afirmar que las tecnologías de encriptación facilitan las actividades terroristas a la hora de captar, radicalizar y planear ataques, y que además los gigantes tecnológicos construyen su negocio en torno a la encriptación para poseer la exclusividad de los datos y así venderlos a anunciantes y gobiernos en sus intentos de hackearlos[9]. El FBI y la CIA demandan por tanto la creación de leyes acordes a la nueva era de avance tecnológico y formas de comunicación sofisticadas.

Apple ha recibido, no obstante, el apoyo de Google y Facebook, mientras que, por su parte, el exdirector de la CIA, Michael Hayden, justificó que Apple no haya querido colaborar en el descifrado del iPhone 5S de uno de los terroristas de San Bernardino para no crear puertas traseras en sus dispositivos[10]. Tras el atentado, el FBI protestó ante el Senado alegando que se encontraba en posesión del teléfono móvil del terrorista pero que era incapaz de acceder a los datos por culpa de la encriptación de Apple.

El iOS 8, en concreto, presenta una nueva característica por la cual resulta prácticamente imposible desencriptar el contenido de los usuarios. Mientras, Google está haciendo algo similar en Android. En el caso de Apple, la empresa ni siquiera posee puertas traseras para sus propios dispositivos: simplemente los encripta por defecto. A su vez, el FBI demanda de Apple que instale en ese terminal una versión de su sistema operativo que tenga una



[8] RT Actualidad (2014). *FBI: Si Google y Apple no descodifican información, les forzaremos*. Obtenido de https://actualidad.rt.com/actualidad/view/143903-eeuu-fbi-google-apple-encriptacion-espionaje

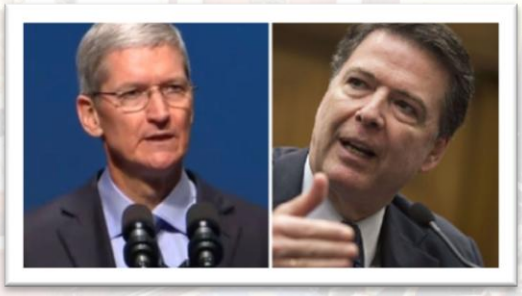
[9] Europa Press (2015). *El FBI afirma que la encriptación de Whatsapp y Apple ayuda a los terroristas*. **Portaltic**. Obtenido de http://www.europapress.es/portaltic/sector/noticia-fbi-afirma-encriptacion-whatsapp-apple-ayuda-terroristas-20150605154738.html

[10] Ramírez, J.D. (2016). *Apple vs FBI: Michael Hayden, exdirector de la CIA y la NSA opina al respecto*. **Applesencia**. Obtenido de http://applesencia.com/2016/02/apple-vs-fbi-michael-hayden-encriptacion

puerta trasera permanente. Esto es algo a lo que Apple se ha negado con rotundidad y a lo que el FBI quiere obligarles a cumplir invocando una ley de 1789[11].

No hay término medio

Recientemente, Apple y las agencias de seguridad acudieron al Congreso para dirimir la disputa, que había quedado estancada en el plano judicial. Apple se niega a dejar que el FBI debilite sus productos, que quedarían por entero desprotegidos ante los hackers[12]. El debate sigue centrado en torno a la misma cuestión: la primera de las prioridades, ¿es la seguridad colectiva o la privacidad del usuario?



En una carta reciente de Tim Cook (CEO) a los usuarios de Apple, el director ejecutivo advierte de los peligros que entrañaría ceder ante las peticiones de las entidades policiales y de inteligencia. Entre ellos, destaca la posibilidad de que toda nuestra información personal (financiera, sanitaria, conversaciones privadas, fotos y vídeos, contactos y correos) caiga en manos de hackers y criminales[13]. La encriptación, resalta en la carta, es por tanto el único método eficaz para combatir las amenazas externas y por ello Apple no puede acceder a la petición del FBI acerca de crear una puerta trasera para el iPhone o de entregar sus claves de encriptación (puesto que ni siquiera Apple tiene la capacidad de hacerlo una vez que ha externalizado el proceso).

Además, la creación de una llave para entrar en el sistema encriptado del iPhone supondría, en el mundo digital, la entrada de una llave maestra capaz de abrir y descodificar cualquier sistema mediante ramificaciones que persigan una técnica similar. Apple cuenta con el apoyo de la ONU, cuyo Alto Comisionado para los Derechos Humanos, Zeid Ra'ad Al Hussein, presentó su respaldo a la negativa de Apple a desencriptar el iPhone del autor del

[11] Hidalgo, C. (2016). *El Gobierno de EEUU empieza a encontrar resistencia*…

[12] Diario Libre (2016). *Pelea entre Apple y el FBI por encriptación va al Congreso*. Obtenido de http://www.diariolibre.com/ciencia-y-tecnologia/tecnologia/pelea-entre-apple-y-el-fbi-por-encriptacion-va-al-congreso-KM2925297

[13] Cook, T. (2016). *A message to our customers*. **Apple**. Obtenido de http://www.apple.com/customer-letter/

atentado en California. Al Hussein considera que se pondría en peligro la seguridad de miles de activistas humanitarios, disidentes y periodistas que necesitan la privacidad garantizada por el dispositivo para denunciar violaciones y abusos en todo el mundo[14].

Últimas actualizaciones: hackers de sombrero gris

Apple ha ganado finalmente la batalla legal, gracias a que el FBI ha encontrado una forma alternativa de acceder al iPhone del terrorista sin necesidad de recurrir a la colaboración de la empresa, contradiciendo su afirmación anterior en la cual declaró ante los medios que era imposible descifrar el dispositivo sin la cooperación de Apple[15]. La multinacional, no obstante, considera que el caso merece una mayor profundización y que debe continuarse el debate nacional sobre las libertades civiles, la seguridad colectiva y la privacidad.

En cuanto a los métodos utilizados para desbloquear el iPhone, el Washington Post anunció el 12 de abril que el FBI había pagado a un grupo de hackers para que eliminaran el sistema de autodestrucción (al décimo intento de desbloqueo, un iPhone borra todo su contenido) y encontraran la combinación correcta para desbloquear el dispositivo[16]. El agujero de seguridad habría sido detectado por hackers de sombrero gris, esto es, individuos que venden sus servicios a distintos gobiernos, servicios de inteligencia o militares y policía. En este caso, es probable que los hackers se lanzaran a buscar agujeros en el teléfono nada más conocer la noticia y luego esperaron a poder comerciar con el gobierno, a sabiendas de que nadie más podía acceder a los datos del iPhone (ibíd.). Cabe mencionar que los hackers grises se distinguen de los blancos –quienes cumplen un servicio público y son recompensados por las empresas tras localizar fallos en la seguridad– y los negros, que directamente comercian con información robada: datos, contraseñas, tarjetas de crédito, etc. A esta última categoría pertenece el caso de la ciudad rumana Râmnicu

[14] Europa Press (2016). *La ONU respalda a Apple en su negativa a desencriptar un iPhone para el FBI*. **BEZ**. Obtenido de http://www.bez.es/924647862/La-ONU-respalda-a-Apple-en-su-negativa-a-desencriptar-un-iPhone-para-el-FBI.html

[15] Hern, A. (March 29, 2016). *Apples declares victory in battle with FBI but the war continues*. **The Guardian**. Obtenido de https://www.theguardian.com/technology/2016/mar/29/apple-victory-battle-fbi-but-war-continues-san-bernardino-iphone

[16] Sarabia, D. (14 de abril de 2016). *Los hackers llevan sombrero blanco, gris y negro*. **El Diario**. Obtenido de http://www.eldiario.es/cultura/tecnologia/privacidad/hackers-llevan-sombrero-blanco-negro_0_505349668.html

Vâlcea, con un alto índice de hackers per cápita que afirman que un 80% de los sistemas presentan vulnerabilidades. Algunos habitantes de esta ciudad han llegado a hackear a la familia Bush, al Pentágono, a Hilary Clinton y a la NASA, entre otras entidades de importancia similar[17].

Lo que está por verse es si el FBI decide compartir con Apple la información sobre el agujero en el software del iOS 9. En ese caso, sería un grupo dirigido por la Casa Blanca quien llevara a cabo la notificación. Pero, de todas formas, el FBI ha comunicado sus reservas puesto que, si desvelan la información, Apple modificará el software y el FBI se encontrará otra vez al comienzo de la investigación y habiendo perdido las ventajas que ahora posee[18].

Internet profunda en España

En España, el gobierno se ha visto obligado a adaptarse a las nuevas formas digitales bajo las que se esconden las amenazas criminales, con la consiguiente actualización de la Ley de Enjuiciamiento Criminal acerca de la figura del agente 2.0, al que se le permite asumir una identidad falsa y participar en los foros de encuentro de los cibercriminales[19].

De esta forma, el agente de policía judicial, con previa autorización de un juez, atraviesa las capas de ocultación adicional para llegar a las páginas web ocultas y, una vez allí, intercambia archivos ilícitos en foros públicos o de invitación, haciéndose pasar por un ciberdelincuente (ibíd.) Así, el agente actúa como un investigador capaz de sumergirse en el gran sistema descentralizado del crimen informático, donde todos los actores se caracterizan por su capacidad de adaptación y su estructura flexible.

---

[17] Norton (17 de junio de 2015). *In Search of The Most Dangerous Town On the Internet - Episode 1*. **YouTube**. Obtenido de https://www.youtube.com/watch?v=un_XI4MM6QI

[18] Nakashima, E. and Goldman, A. (12 de abril de 2016). *FBI paid professional hackers one-time fee to crack San Bernardino iPhone*. **The Washington Post**. Obtenido de: https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

[19] Hidalgo, C. (2016). *Policías y guardias civiles patrullan de incógnito la Internet profunda*. **BEZ**. Obtenido de http://www.bez.es/189108365/Policias-y-Guardias-Civiles-tambien-patrullan-de-incognito-la-Internet-profunda.html

Las fuerzas de seguridad y los servicios de inteligencia en España también sufren las consecuencias de la encriptación digital en dispositivos y redes. Javier Zaragoza, jefe fiscal de la Audiencia Nacional española, y sus homólogos en Manhattan, París y Londres publicaron un editorial de protesta contra la nueva opción de cifrado que Apple y Google han introducido por defecto en los sistemas operativos de smartphones IOS 8 y Android Lollipop. Al parecer, habían encontrado dos teléfonos en el bolsillo de la víctima de un asesinato y habían sido incapaces de acceder a la información porque estaban cifrados. Tras llamar a los fabricantes del sistema operativo y pedir la llave, tanto Apple como Google anunciaron que no podían compartirla puesto que no la tenían[20].

Según el jefe de ciberseguridad del Centro Criptológico Nacional (CCN) Javier Candau, los ciberataques constituyen una amenaza crítica para España, que con frecuencia es víctima de atacantes que buscan información de elevado valor como, por ejemplo, datos referentes a la seguridad española, I+D, mercados, clientes, sistemas financieros y propiedad intelectual[21]. En 2014 se registraron unos 13.000 incidentes cibernéticos con un aumento del 80% respecto al número de casos el año anterior. Los campos en los que prima el aumento son los de mayor importancia estratégica: el de defensa, energético, aeroespacial, farmacéutico y químico (ibíd.).

En cualquier caso, ha habido determinados países europeos que se han mostrado en desacuerdo con la política de instalación de puertas traseras. El gobierno holandés ha sido uno de los primeros en dar su apoyo a las empresas tecnológicas como Apple y Blackberry mientras que otros, como Reino Unido, han protestado ante las tecnologías comerciales que dificultan el trabajo policial y de inteligencia a la hora de vigilar las comunicaciones, sobre todo tras los dobles atentados de París en 2015[22].

---

[20] Peirano, M. (2016). *Imponer puertas traseras no detendrá el cifrado de datos (ni el terrorismo)*. **El Diario**. Obtenido de http://www.eldiario.es/cultura/tecnologia/privacidad/Imponer-puertas-traseras-detendra-cifrado_0_483652441.html

[21] Candau, J. (2015). *"El ciberespionaje persigue información de altísimo valor y debe considerarse una amenaza crítica"*. **Red Seguridad**. Obtenido de https://www.ccn-cert.cni.es/pdf/articulos-y-reportajes/937-el-ciberespionaje-persigue-informacion-de-altisimo-valor-y-debe-considerarse-una-amenaza-critica/file.html

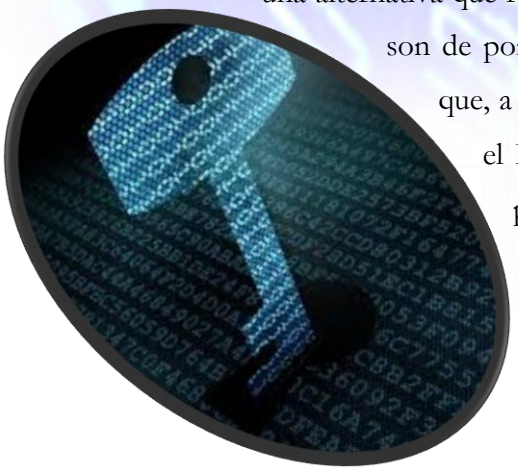
[22] Eressea Solutions (2016). *Varios países europeos en contra de las puertas traseras para espiar datos*. **Eressea Solutions**. Obtenido de http://www.eresseasolutions.com/noticias/actualidad/varios-paises-europeos-en-contra-de-las-puertas-traseras-para-espiar-datos/

Conclusión

La encriptación es una tecnología matemática que ha existido desde tiempos del Imperio romano y puede adaptar múltiples formas y códigos, por lo que nunca podrá prohibirse o eliminarse en su totalidad. A su vez, en el caso de que se colocaran puertas traseras en dispositivos y redes de las grandes empresas tecnológicas, tanto criminales como terroristas podrían buscar vías paralelas a su alcance y encontrar con éxito otros medios de comunicación encriptada que las autoridades no puedan descifrar. Si un criminal quisiera mantener una conversación secreta o mandar correos cifrados podría encontrar otras plataformas y dispositivos que burlen la vigilancia policial y de inteligencia sin grandes dificultades.

En cualquier caso, las puertas traseras son una amenaza a largo plazo para la ciberseguridad y vulneran la protección asegurada de los ciudadanos al tiempo que facilitan la proliferación del crimen y de los ataques por parte de hackers. Por último, las consecuencias económicas para las empresas tecnológicas y los negocios estadounidenses podrían traducirse en pérdidas de miles de millones de dólares. ¿Deberíamos sacrificar la privacidad en aras de la seguridad o es que al hacerlo estamos en realidad desatando una serie de consecuencias desastrosas para la seguridad de las siguientes generaciones?

La mejor opción se encuentra, sin duda, en establecer un equilibrio entre ambos extremos, como afirma Christopher Nims (2016). El autor sugiere la herramienta del pirateo legal, una alternativa que reconoce el hecho de que nuestros ordenadores y dispositivos son de por sí poco seguros y presentan vulnerabilidades en el sistema que, a su vez, pueden ser explotadas por las agencias de seguridad y el Estado sin necesidad de añadir nuevas debilidades como las puertas traseras. En resumen, deben buscarse herramientas distintas, como el análisis de los metadatos en los mensajes, que también proporciona información valiosa y no compromete la seguridad online a gran escala.



Referencias

Candau, J. (2015). *"El ciberespionaje persigue información de altísimo valor y debe considerarse una amenaza crítica"*. **Red Seguridad**. Obtenido de https://www.ccn-cert.cni.es/pdf/articulos-y-reportajes/937-el-ciberespionaje-persigue-informacion-de-altisimo-valor-y-debe-considerarse-una-amenaza-critica/file.html

Cook, T. (2016). *A message to our customers*. **Apple**. Obtenido de http://www.apple.com/customer-letter/

Diario Libre (2016). *Pelea entre Apple y el FBI por encriptación va al Congreso*. **Diario Libre**. Obtenido de http://www.diariolibre.com/ciencia-y-tecnologia/tecnologia/pelea-entre-apple-y-el-fbi-por-encriptacion-va-al-congreso-KM2925297

Eressea Solutions (2016). *Varios países europeos en contra de las puertas traseras para espiar datos*. **Eressea Solutions**. Obtenido de http://www.eresseasolutions.com/noticias/actualidad/varios-paises-europeos-en-contra-de-las-puertas-traseras-para-espiar-datos/

Europa Press (2015). *El FBI afirma que la encriptación de Whatsapp y Apple ayuda a los terroristas*. **Portaltic**. Obtenido de http://www.europapress.es/portaltic/sector/noticia-fbi-afirma-encriptacion-whatsapp-apple-ayuda-terroristas-20150605154738.html

Europa Press (2016). *La ONU respalda a Apple en su negativa a desencriptar un iPhone para el FBI*. **BEZ**. Obtenido de http://www.bez.es/924647862/La-ONU-respalda-a-Apple-en-su-negativa-a-desencriptar-un-iPhone-para-el-FBI.html

Hidalgo, C. (2016). *El Gobierno de EEUU empieza a encontrar resistencia al acceso a los datos de los ciudadanos*. **BEZ**. Obtenido de http://www.bez.es/966085299/El-Gobierno-de-EEUU-empieza-a-encontrar-resistencia-al-acceso-a-los-datos-de-los-ciudadanos.html

Hidalgo, C. (2016). *Las empresas se alían contra el ciberespionaje económico*. **BEZ**. Obtenido de http://www.bez.es/617447150/Identificado-el-grupo-responsable-del-ataque-y-la-crisis-de-Sony-Pictures.html

Hidalgo, C. (2016). *Policías y guardias civiles patrullan de incógnito la Internet profunda*. **BEZ**. Obtenido de http://www.bez.es/189108365/Policias-y-Guardias-Civiles-tambien-patrullan-de-incognito-la-Internet-profunda.html

Hern, A. (29 de marzo de 2016). *Apples declares victory in battle with FBI but the war continues*. **The Guardian**. Obtenido de https://www.theguardian.com/technology/2016/mar/29/apple-victory-battle-fbi-but-war-continues-san-bernardino-iphone

Nakashima, E. and Goldman, A. (12 de abril de 2016). FBI paid professional hackers one-time fee to crack San Bernardino iPhone. The Washington Post. Obtenido de:

https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

Nims, C. (2016). *Ciberseguridad: ¿hacen falta las puertas traseras?* **Expansión: Economía Digital**. Obtenido de http://www.expansion.com/economia-digital/innovacion/2016/01/24/569fb6c8268e3eb3358b4594.html

Norton (17 de junio de 2015). *In Search of The Most Dangerous Town On the Internet - Episode 1*. **YouTube**. Obtenido de https://www.youtube.com/watch?v=un_XI4MM6QI

Peirano, M. (2016). *Imponer puertas traseras no detendrá el cifrado de datos (ni el terrorismo)*. **El Diario**. Obtenido de http://www.eldiario.es/cultura/tecnologia/privacidad/Imponer-puertas-traseras-detendra-cifrado_0_483652441.html

Peterson A. (2016). *The debate over government 'backdoors' into encryption isn't just happening in the U.S*. **The Washington Post**. Obtenido de https://www.washingtonpost.com/news/the-switch/wp/2016/01/11/the-debate-over-government-backdoors-into-encryption-isnt-just-happening-in-the-u-s/

Ramírez, J.D. (2016). *Apple vs FBI: Michael Hayden, exdirector de la CIA y la NSA opina al respecto*. **Applesencia**. Obtenido de http://applesencia.com/2016/02/apple-vs-fbi-michael-hayden-encriptacion

RT Actualidad (2014). *FBI: Si Google y Apple no descodifican información, les forzaremos*. **RT**. Obtenido de https://actualidad.rt.com/actualidad/view/143903-eeuu-fbi-google-apple-encriptacion-espionaje

Sarabia, D. (14 de abril de 2016). *Los hackers llevan sombrero blanco, gris y negro*. **El Diario**. Obtenido de http://www.eldiario.es/cultura/tecnologia/privacidad/hackers-llevan-sombrero-blanco-negro_0_505349668.html

Wu, T. et al. *The ethics or not of massive government surveillance*. Obtenido de https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html

Laura Revuelta Guerrero

Estudiante en prácticas de la Universidad Pontificia de Comillas