UNIVERSIDAD DE  VALLADOLID

E.T.S.I. TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA DE TECNOLOGÍAS ESPECÍFICAS DE TELECOMUNICACIÓN. MENCIÓN EN INGENIERÍA DE SISTEMAS DE TELECOMUNICACIÓN

Estudio de Soluciones de Seguridad para Apps Móviles en Sanidad

Autor:

Enrique Pérez Morera

Tutor:

Isabel de la Torre Díez

Valladolid, 15 de Abril de 2016

TÍTULO:	Estudio de Soluciones de Seguridad para Apps Móviles en Sanidad
AUTOR:	Enrique Pérez Morera
TUTORES:	Isabel de la Torre Díez
DEPARTAMENTO:	Teoría de la Señal, Comunicaciones e Ingeniería Telemática

TRIBUNAL

PRESIDENTE:	Miguel López-Coronado Sánchez-Fortún
VOCAL:	Isabel de la Torre Díez
SECRETARIO:	Beatriz Sainz de Abajo
SUPLENTE:	Carlos Gómez Peña
SUPLENTE:	Salvador Dueñas Carazo

FECHA:	15 de Abril de 2016
CALIFICACIÓN:	

RESUMEN

Las *apps* de *mHealth* están cambiando el modelo sanitario siendo la tercera categoría de mayor crecimiento, por detrás de los juegos y utilidades, y es que la medicina de hoy pasa por los datos que éstas recopilan y su análisis, conocido como *Big Data*. Sin embargo, la mayoría de las *apps* cuentan con una seguridad insuficiente a la hora de recoger y tratar la información, convirtiéndose en un problema significativo. En este Trabajo Fin de Grado se presenta una guía sobre soluciones de seguridad de gran utilidad para los desarrolladores de *apps* de *mHealth*.

Durante agosto de 2015 se llevó a cabo la búsqueda de aplicaciones móviles de salud existentes en las distintas tiendas virtuales como *Google Play* de *Android*, *iTunes App Store* de *Apple*, etc. con el fin de hacer una clasificación de las mismas según su utilidad. Después de esta búsqueda se revisaron las vulnerabilidades más extendidas en el campo de la seguridad en el desarrollo de *apps* móviles, basándose en diferentes fuentes como el *OWASP Mobile Security Project*, la iniciativa lanzada recientemente por la *OCR* (Oficina de Derechos Civiles) y otros artículos de interés científico.

Finalmente se ha creado una guía elemental, de carácter informativo para el desarrollo de *mHealth apps*. En esta guía se dan a conocer los elementos de seguridad y su implementación por niveles, de los tipos de *apps* móviles de salud basándonos en los datos que manipula cada una de ellas, el cálculo del riesgo asociado fruto de la probabilidad de ocurrencia y el nivel de impacto de las amenazas derivadas de las vulnerabilidades. Nivel alto (*apps* de monitoreo, diagnosis, tratamiento y asistenciales) de 6≤9, nivel medio (calculadora, localizadores y alarma) de 3≤6 y nivel bajo (*apps* informativas y educacionales) de 0≤3.

La guía propuesta facilita y garantiza que se tomen medidas de seguridad en los desarrollos de aplicaciones móviles de salud por parte de programadores ajenos al campo de las *TIC* y profesionales sanitarios.

ABSTRACT

Being the third fastest-growing app category behind games and utilities, *mHealth apps* are changing the healthcare model, as medicine today involves the data they compile and analyse, information known as *Big Data*. However, the majority of apps are lacking in security when gathering and dealing with the information, which becomes a serious problem. This article presents a guide regarding security solution, intended to be of great use for developers of *mHealth apps*.

In August 2015 current mobile health apps were sought out in virtual stores such as *Android Google Play*, *Apple iTunes App Store* etc., in order to classify them in terms of usefulness. After this search, the most widespread weaknesses in the field of security in the development of these mobile *apps* were examined, based on sources such as the *"OWASP Mobile Security Project"*, the initiative recently launched by the *Office of Civil Rights (OCR)*, and other articles of scientific interest.

An informative, elemental guide has been created for the development of *mHealth apps*. It includes information about elements of security and its implementation on different levels for all types of mobile health *apps* based on the data that each *app* manipulates, the associated calculated risk as a result of the likelihood of occurrence and the threat level resulting from its vulnerabilities - high level (*apps* for monitoring, diagnosis, treatment and care) from 6≤9, medium level (calculator, localizer and alarm) from 3≤6 and low level (informative and educational *apps*) from 0≤3.

The guide aims to guarantee and facilitate security measures in the development of mobile health applications by programmers unconnected to the *ITC* and professional health areas.

PALABRAS CLAVE: apps, guía para desarrolladores, mHeatlh, mSalud, seguridad.

Agradecimientos

Me gustaría agradecer en primer lugar a mis padres, José Vicente y Julita, poder brindarme una educación, así como su enorme e incondicional apoyo a lo largo de toda mi vida en todo lo que he hecho, permitiéndome llegar a ser quien soy. Han sido unos cuantos años. Han sido muchos los momentos duros y muchos los felices. A veces gateando, a veces andando, a veces esprintando, pero siempre hacia adelante, sin rendirme y luchando hasta el final, tal y como he aprendido de ellos, en especial de mi madre, una gran mujer, enérgica, sacrificada y cariñosa, a la que no hay nada que la pueda hacer caer, aunque la tiren a dar. Gracias a ellos he llegado al menos hasta aquí. Gracias.

Gracias también a mi hermano Daniel, en breves Graduado en Comercio, por estos años de convivencia, a pesar de sus temporales y tempestades, porque aunque a Daniel lo echen a la cueva de los leones, éstos no se lo comen. Daniel se come a los leones. Gracias.

Gracias a mi ciudadrealeña, Paloma, de naturaleza despistada y libre, fruto de una inteligencia y sensibilidad admirable, por ser mi compañera de remo capaz de evitar que vaya a la deriva en los momentos difíciles dándome cariño, risas, ánimos y comprensión, convirtiéndose en la arquitecta de mi corazón. Gracias por disfrutar a tu lado. *Grazie mille mi piccola ragazza.*

Estos años, han sido mucho de aprendizaje personal gracias a mis amigos de toda la vida y a los de la carrera, de técnica y grado, como David Marcos, Juan Diego, David "Kace", Manu Pérez, Ismael Sanz, Diego Velayos, Jorge Jiménez, Jorge Cerro, etc. y en particular a Francisco Camazón, cigaleño de gran buqué, amigo de enorme luz interior y fiel escudero de batalla ante los molinos de viento de Teleco. Gracias socio por estar presente en los buenos y malos momentos. Gracias chicos. La unión hace la fuerza y de todos ellos me llevo un buen saco de recuerdos y de experiencias, tantas como horas he pasado en la academia OCHO con Pablo Martínez y José Jacinto, buenrollistas y virtuosos maestros capaces de hacer fácil lo difícil ayudándome a encontrar el camino hacia el mar. Gracias.

Agradecer especialmente a mi tutora, Isabel de la Torre, la dedicación y confianza que ha puesto en mi, haciendo posible este TFG y el Articulo de Investigación. Demuestra cada día su profesionalidad, vocación docente y lo más importante, su pasión y calidad humana conectando con los alumnos, cosas, que aunque no relucen, bien podrían valer mucho más que el propio oro.

Finalmente dar gracias al resto de familiares y de personas que han pasado por mi vida, los que están y los que no, como mi abuelo materno, Pablo Morera. Un hombre cariñoso y de gran carácter que se sentía fascinado por la tecnología. De su mano viví muy buenos momentos, me inculcó su pasión por la poesía, el arte y lo más importante, me enseño que "caminante no hay camino, se hace camino al andar".

Acabo con una sensación de agradecimiento infinito. Es lo que cuenta. Gracias por ayudarme a ser mi propio ídolo. Gracias por ser fuerza e inspiración. A todos vosotros, gracias de todo corazón.

Índice

Índice de Imágenes

Índice de Tablas

Índice de Figuras

"El hecho de poner en peligro la seguridad de nuestra información personal puede acabar poniendo en peligro nuestra seguridad personal"

Tim Cook (*CEO* de *Apple Inc.*), 2016

CAPÍTULO 1

INTRODUCCIÓN

CAPÍTULO 1. INTRODUCCIÓN

1.1 Sociedad Conectada

El 9 de enero de 2007 [1], en la *Imagen 1.1*, el difunto cofundador de Apple, Steve Jobs, daba a conocer *"un producto revolucionario que lo cambiaría todo". "Lo vamos a llamar iPhone",* apostilló Jobs, siendo el *smartphone* que marcaría un antes y un después en el rumbo de la telefonía móvil, convirtiéndose en el *"invento del año"* según la revista *Time* en 2009 [2]. Llegaría al mercado meses más tarde, en junio de ese año, sin teclado físico, con una pantalla táctil y lo más importante, acompañado de su sistema operativo *iOS (iPhone OS)*, el cual te ofrecía servicios de Internet como leer correo electrónico y cargar páginas *Web* gracias a la conectividad 2G *(GSM, Global System for Mobile).*

Imagen 1.1. Steve Jobs presentando el *iPhone* de 1º generación en 2007. Fuente: [1]

Una vez abierta la caja de Pandora, un año más tarde, junto a la presentación de la segunda iteración de *iPhone* y su tienda de aplicaciones móviles *App Store*, en octubre de 2008 [3] se pondría a la venta el *T-Mobile G1* o *HTC Dream*. El primer teléfono inteligente con otro sistema operativo acreditado por *Google*, llamado *Android (Android Apple Pie 1.0)*, de plataforma libre y código abierto, que a día de hoy, es el más famoso del mundo. En octubre de ese mismo año, se pondría en marcha *Android Market*, la tienda de aplicaciones de *Google* que más tarde pasaría a llamarse *Google Play*.

Pronto, estos dispositivos junto con sus tiendas de aplicaciones, se convertirían en la navaja suiza del siglo XXI ya que aprovecharían todas las ventajas de la tercera generación (3G) de transmisión de voz y datos a través de telefonía móvil mediante *UMTS (Universal Mobile Telecommunications System o Servicio Universal de Telecomunicaciones Móviles).* Según los últimos datos de la

ITU (Unión Internacional de las Telecomunicaciones) [4], la evolución de la banda ancha móvil es la más dinámica, aumentando el número de suscriptores activos a un 47% en 2015, 12 veces más que en el año 2007. En 2015, se ofrece cobertura de banda ancha móvil 3G al 69% de la población mundial, cuando en el año 2011 esta cobertura se ofrecía solo al 45%. Es muy notable la expansión de la banda ancha móvil 3G en zonas rurales. La *ITU* estimó que a finales de 2015 el 29% de la población que reside en zonas rurales tendrían cobertura en banda ancha móvil 3G, es decir, unos 986 millones de personas.

A día de hoy, contamos con multitud de fabricantes de *smartphones* así como con 2,5 millones de aplicaciones [5] aproximadamente entre *Google Play (Google)* y *App Store (Apple)*, capaces de aprovechar las ventajas de las redes de telefonía móvil. Los fabricantes chinos [6], liderados por *Huawei*, *Lenovo* y *Xiaomi*, escalan posiciones en el mercado mundial de *smartphones* que lideran *Samsung* y *Apple*, con un 37% de cuota en el tercer trimestre de 2015. En la actualidad, prácticamente seis de cada diez móviles inteligentes que se venden en el mundo son de marcas chinas, según datos de *Strategy Analytics*, haciendo que [7] *Android* con su 82.2% de cuota de mercado se posicione como el sistema operativo móvil más usado a pesar de que *iOS* haya tenido un crecimiento de 0.6% respecto a 2014, situándose en un 14.6%. Las ventas totales de teléfonos inteligentes en 2015 [8] ascienden a 1433 millones con *Android* e *iOS* controlando el 97,8% del mercado de *smartphones*. El reciente estudio de la *GSMA* (*Groupe Speciale Mobile Association)* [9] pronostica que para 2020, como se ve en la *Figura 1.1*, la cifra de *smartphones* conectados podría ser de 6.000 millones, gracias a países emergentes como India, China, Indonesia o Brasil.

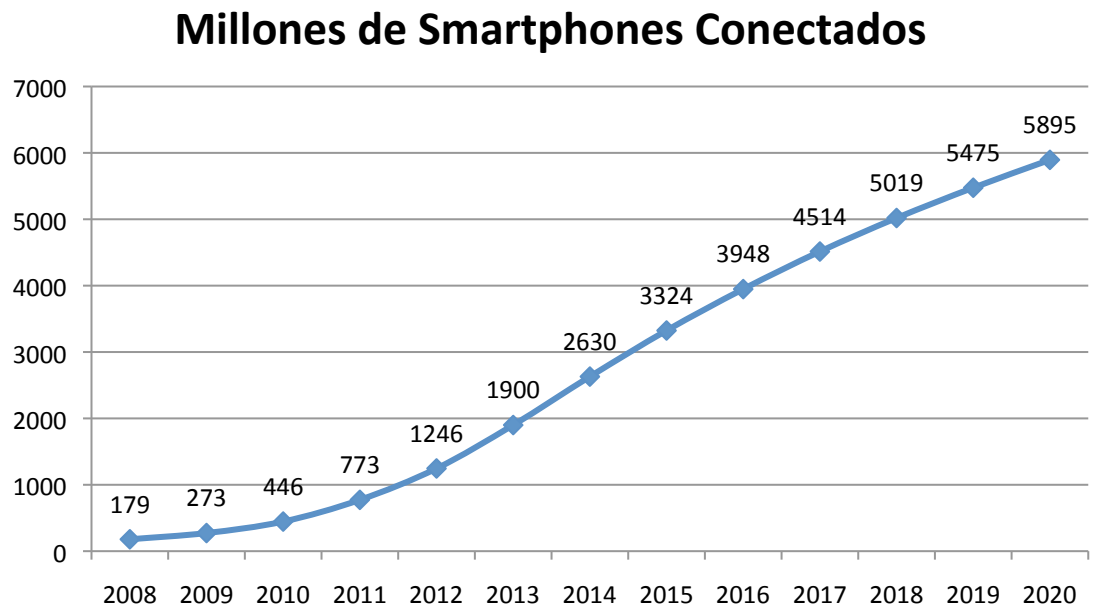


Figura 1.1. Millones de *Smartphones* conectados entre los años 2008 y 2020. Fuente: [9]

Todos estos datos nos muestran, que la tecnología móvil es un mercado en crecimiento y que vivimos en una época marcada por una tremenda revolución tecnológica. Hoy en día, el alcance del móvil es mayor que nunca, y su continua adopción está condicionando tanto el comportamiento de los consumidores como las estrategias de negocio en sectores como la banca o la salud. España se ha convertido en uno de los países de Europa en el que la telefonía móvil tiene mayor grado de aceptación. Los teléfonos móviles son omnipresentes y, de hecho, desde marzo de 2006, en nuestro país hay oficialmente más líneas de teléfono móvil que habitantes, situándose la tasa de penetración de la telefonía móvil en 108,5% en abril de 2015, según datos de la *CMT* [10].

Todos somos conscientes de que para mucha gente, hoy podría decirse que para la mayoría de los ciudadanos, el *smartphone* se ha convertido en una parte fundamental de su vida. A día de hoy, un mayor número de consumidores utilizan su *smartphone* para tareas que antes sólo estaban disponibles a través del *PC*. Chequear los saldos bancarios o realizar compras online a través del teléfono, por ejemplo, son prácticas que se están extendiendo (41% y 22% de los encuestados, respectivamente, confirman realizar estas actividades según el informe "*Consumo Móvil en España 2014"* de *Deloitte*) [11].

Los *smartphones* se han convertido en elementos esenciales en nuestras vidas, por lo que muchos de nosotros nos hemos hechos adictos a ellos. Parecemos incapaces de separarnos de nuestros teléfonos. Alrededor de uno de cada cuatro adultos que tiene un *smartphone* mira su teléfono más de 50 veces al día [11]. Casi la mitad de estos mismos adultos mira su teléfono en los cinco minutos después de levantarse, y de ellos, un 13% lo hace inmediatamente (aumentando este porcentaje hasta el 31% en el caso de los jóvenes entre los 18 y 24 años).

Para la mayoría de los propietarios de *smartphones*, comprobar quién se ha puesto en contacto con ellos ha pasado a formar parte de su rutina al levantarse. La primera aplicación utilizada por la mañana [11] en opinión de los encuestados es la mensajería instantánea (primera en acceder por el 36%), seguida por el correo electrónico (con el 21%) y las redes sociales (con el 13%). Queda claro que la conectividad es el punto de partida para nuevas formas de innovar, colaborar y convivir. Esto significa libertad, autonomía y la oportunidad de transformar sectores de la economía y la sociedad como un todo, dando lugar a una revolución tecnológica, por medio de las Tecnologías de la Información y la Comunicación, las *TICs*, facilitando, en gran medida, la tendencia de los usuarios a evolucionar de un modelo basado en la posesión de los contenidos a otro basado en la descarga en el momento que se quieren consumir.

Las *TICs*, mediante la digitalización y con el *smartphone* como eje central de todo, están propiciado avances con el fin de integrarse en nuestra vida de forma natural, aspirando abarcar todos los campos posibles, desde el hogar hasta el vehículo pasando por la salud, con el objetivo de aportar mayor calidad de vida y es que el acceso móvil es un servicio al alcance de todos, independientemente

de la renta de la población, de su dispersión geográfica o del nivel sociocultural. La universalidad de los dispositivos móviles es una novedad radical en la adopción de cualquier tecnología, y una gran diferencia con el resto de las *TICs*, ya que ha supuesto un gran revulsivo en el fortalecimiento del uso de Internet, así como la consolidación del mercado de aplicaciones para dispositivos móviles. Cualquier necesidad que se nos plantee es muy probable que, por ejemplo, ya tenga una *app* asociada para que podamos solventarla. Simplemente tenemos que estar conectados a Internet y descargarla en nuestro *smartphone*.

1.2 Aplicaciones. Wearables & mHealth

La apuesta por el acceso en movilidad ha hecho de España el líder europeo de penetración del *smartphone*. Nada menos que cuatro de cada cinco teléfonos móviles en España son inteligentes. En sólo dos años, han pasado de representar el 63% al 81% de los teléfonos móviles en España. Ello no debe ensombrecer el importante crecimiento del 68% de la venta de *tablets* el pasado año. [12]

En septiembre de 2014 se presentó el "*V informe sobre el estado de las Apps en España*" [13] elaborado por *The App Date* utilizando fuentes informativas y estudios tales como los del *INE (Instituto Nacional de Estadística)*, *Fundación Telefónica*, *Fundación Orange*, *IAB Spain*, *The Cocktail Analysis*, *Kantar Worldpanel*, *IDC's Worldwide Quarterly Tablet Tracker*, *ONTSI* y *ComScore* entre otros. Según este informe, los españoles hacen un uso exhaustivo tanto de las tabletas como de los *smartphones*, como lo prueba el alto número de descargas de aplicaciones para ambos dispositivos. En España existen 23 millones de usuarios activos de *apps* que realizan 3,8 millones de descargas diarias de aplicaciones, y esto es el reflejo de una tendencia similar de carácter planetario. De media, cada usuario tiene instaladas 39 aplicaciones, por 33 de los usuarios de *tablets*, y es que las *apps* proporcionan soluciones a diversas necesidades de los usuarios, pensadas y adaptadas para cada tipo de dispositivo, y por lo tanto son aplicables a prácticamente a todos los ámbitos de la economía y de la sociedad. [12]

Estos datos nos dan muchas razones para seguir con el desarrollo de aplicaciones móviles *(apps)* en 2016, ya que en 2015 el uso de *apps* móviles ha continuado su racha de crecimiento, apoyado en tendencias que ya hemos visto aparecer en años precedentes. Según un informe de *KPCB* [14], habrá nada menos de 1.600 millones de *smartphones* en el mundo entre 2015 y la primera parte de 2016. Por otra parte, los ingresos generados en las diferentes tiendas de aplicaciones estaban previstos en 45.400 millones de dólares para 2015, y esa cifra sería de 76.520 millones para 2017 como se puede ver en la *Figura 1.2*, según previsiones de *Statista* [15]. Esto va unido a las previsiones de descargas de *apps*, estimadas en 167.050 millones para 2015 y en 211.310 millones para 2016, también según *Statista*. A nadie le impresiona ya estas cifras, si bien hay que tener en cuenta que las descargas, e ingresos, cada vez están más concentradas en un porcentaje de desarrolladores y *publishers* muy reducido. A pesar de esto, muchas empresas siguen muy ilusionadas con el desarrollo de aplicaciones móviles.

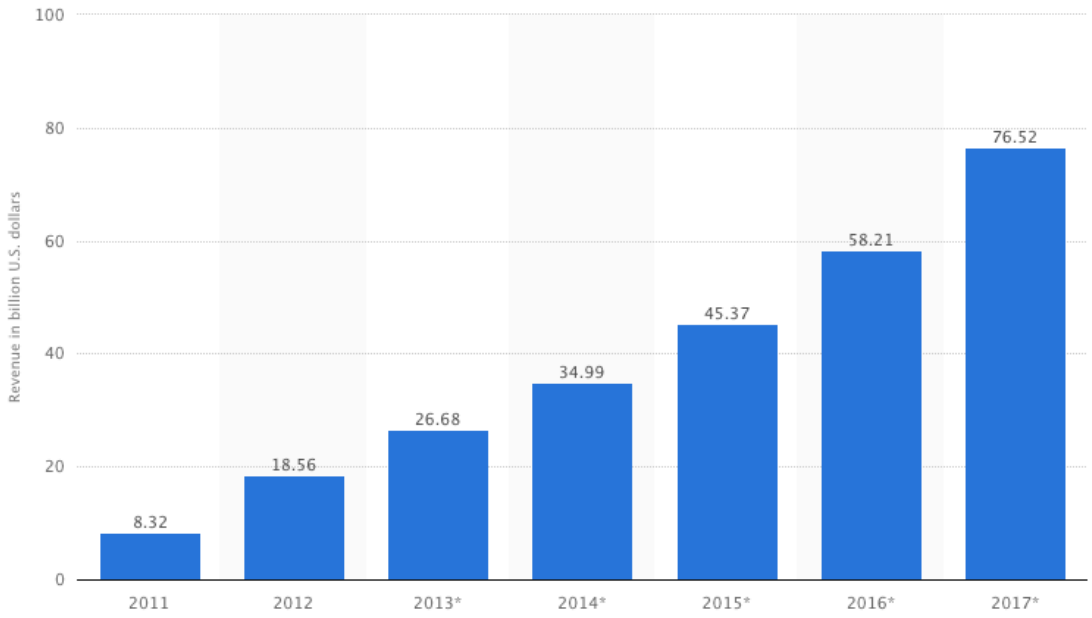


Figura 1.2. Ingresos generados en la diferentes tiendas de aplicaciones móviles (2011 - 2017). Fuente: [15]

Estos indicadores ponen de manifiesto el importante negocio detrás de las aplicaciones móviles, y el mundo de la salud no se ha mantenido al margen, siendo las *apps* de salud la tercera categoría de mayor crecimiento, por detrás de los juegos y utilidades. En el mes de Mayo de 2015 se ha publicado el informe "*mHealth App Developper Economy 2015*" [16] elaborado por *Research2Guidance*, en el cual se presenta un estudio con el ranking de los países europeos con mejor mercado para aplicaciones móviles relacionadas con la salud. España es el cuarto mejor país de Europa para emprender un negocio de *mHealth* y es que las aplicaciones móviles de salud o *mHealth*, según el primer "*Informe de las 50 mejores apps de salud en español*", elaborado por *The App Date* han generado en 2015 [17] un volumen de negocio de 4.000 millones de euros en España, debido a que un tercio de los usuarios de *smartphones* tiene instalada, al menos, una de estas aplicaciones. Además, se estima que su presencia anual crecerá un 23% en los próximos cinco años y que en cuatro años los ingresos aumentarán un 511%.

El éxito de estas aplicaciones radica en que si algo pueden hacer los dispositivos móviles de hoy en día es facilitar la tarea de recogida de datos de pacientes en ensayos clínicos y otros, incluso, pueden ayudar a detectar de forma temprana brotes de enfermedades relacionadas con exposiciones ambientales o agentes infecciosos gracias sus numerosos sensores. También facilitan la comunicación con los profesionales de la salud dando lugar a una nueva forma de relación entre el médico y el paciente ofreciendo múltiples beneficios para ambas partes, desde la optimización del tiempo en consulta hasta la mejora de la adherencia terapéutica y la monitorización de pacientes crónicos.

Otra de las razones de éxito de *mHealth* es la apuesta indiscutible por estas aplicaciones por parte de los profesionales de la salud, industria farmacéutica y administración, tal y como ha señalado el director del *Observatorio Zeltia*, Fernando Mugarza [18], puesto que *"Estamos cambiando el modelo sanitario a través de Internet y gracias a estas herramientas que, además de mejorar la calidad asistencial, juegan un papel muy relevante en la seguridad del paciente y un ahorro en el consumo de los recursos sanitarios",* y es que un informe de *PwC* [19], revela que el *mHealth* podría suponer un ahorro del 50% en los costes de servicios sanitarios hasta 2017. Dicho de otro modo, en España, se podrían ahorrar hasta 10.000 millones de euros en los próximos cuatro años gracias a un modelo de servicios interconectados.

A todo lo anterior tenemos que sumar las tendencias tecnológicas vistas en el *CES (Consumer Electronic Show)* 2015 y 2016 [20] con un claro predominio del mercado de los *wearables/smartwatches* o también conocidos como dispositivos electrónicos o biosensores de carácter inalámbrico con sensores que podemos vestir o llevar puestos, para recabar y mostrar información de constantes vitales y actividad física. Estos *devices* mediante una *app* móvil están altamente ligados al cuidado de la salud ya que pueden medir pulsaciones, ritmo cardiaco, ritmo respiratorio, presión arterial, nivel de glucosa, saturación de oxígeno en sangre, temperatura, sudoración, etc.

Durante los próximos años, el mercado de los *wearables* será uno de los más prolíferos y rentables. La explosión de estos dispositivos conectados puede hacer que se pase de los 130 millones *wearables* de *fitness* conectados hoy en día a los 1.300 millones que se prevén para 2025, según *McKinsey&Company* [21]. Ésta tecnología inteligente será clave y usual en el funcionamiento óptimo de la sociedad del futuro no muy lejano, sobre todo cuando se trate de la salud ya que sólo en Europa, la completa digitalización en todo el sistema sanitario podría suponer un ahorro de 99.000 millones de euros.

La industria de la salud y el bienestar, es consciente del enorme potencial de crecimiento económico que suponen las más de 100.000 [22] aplicaciones de salud móvil *(mHealth)* que hay actualmente asociadas a los *wearables* y *smartphones*, y es que, tal y como afirma el doctor John W. Denniger en el *IOT Solutions World Congress* de 2015 [23], la medicina de hoy en dia pasa por el análisis de la información *(Big Data)* que recogen *smatphones* y *wearables* en diversas *apps* dado su enorme potencial, mejorando la medicina y nuestro bienestar, ya que éstos a diferencia de los pacientes, no mienten. Tu médico sabrá a qué hora te has levantado, si has tomado la medicación, si has seguido tus rutinas o incluso si has sufrido una caída y no puedes levantarte. Es por ello que toda esta innovadora tecnología necesita una regulación y homologación para que se certifique si son ciertamente seguras brindando protección a la información sensible con la que se trabaja, como son los datos del paciente. Esto plantea un desafío importante en el entorno de las aplicaciones móviles de salud para que las *apps* y los dispositivos asociados dejen de ser elementos vulnerables a ataques informáticos y nos aseguren la intimidad de la información registrada.

1.3 Objetivo. Seguridad y Privacidad de la Información

El tráfico mundial de datos móviles alcanzó aproximadamente 52 millones de *terabytes* (TB) en 2015, un aumento del 59% desde 2014, según un estudio de *Gartner*. El rápido crecimiento va a continuar hasta 2018 [24], año en que se triplicará respecto a este, debido al creciente número de teléfonos inteligentes y otros dispositivos como por ejemplo, *tablets* o *wearables* que hacen uso de aplicaciones que consumen un gran volumen de datos como refleja la *Figura 1.3*.

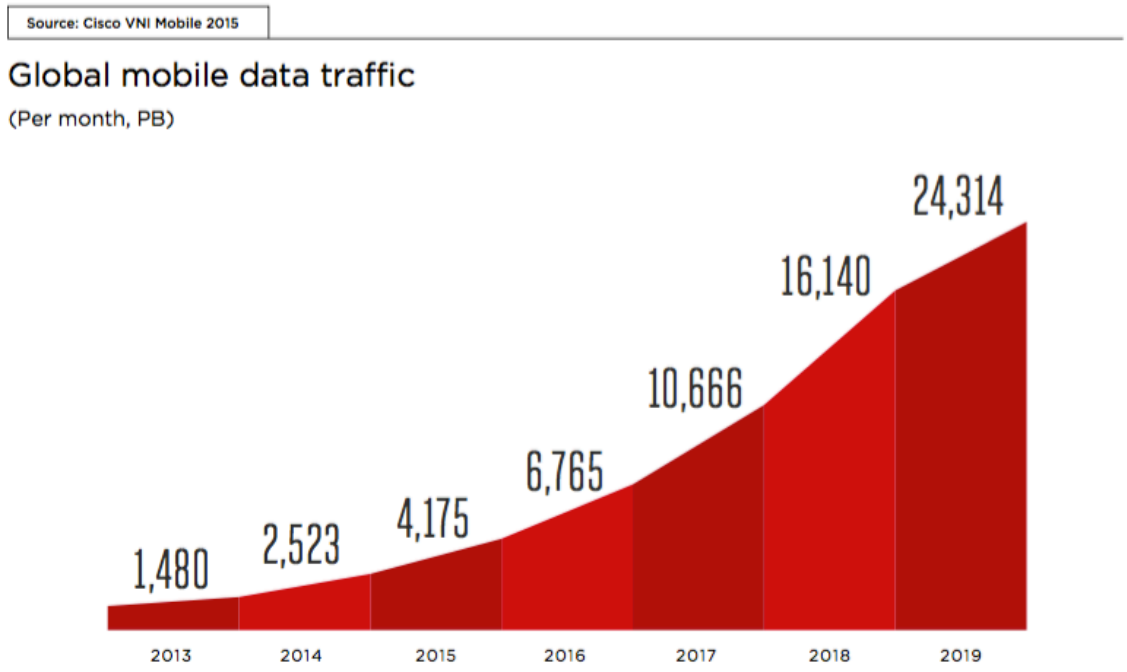


Figura 1.3. Tráfico de datos móviles generado a nivel mundial (2013 – 2019). Fuente: [9]

En diciembre de 2013 se produjo una de las mayores brechas de seguridad con la filtración de información personal de más de 70 millones de clientes de la empresa norteamericana *Target*, incidente que motivó la movilización inmediata de recursos en ciberseguridad por valor de cinco millones de dólares. A partir de ese momento, las empresas son cada vez más conscientes de que necesitan proteger sus activos pero, pesar de ello, el año 2015 ha estado marcado por una gran cantidad de brechas de seguridad (unas 250) con casi 220 millones de credenciales filtradas, que ha supuesto una amenaza tanto para sus usuarios como para otras empresas. [25]

"No se trata solo de la privacidad de los datos o de la seguridad de nuestras identidades digitales", explica Chema Alonso [26], *CEO* de *ElevenPaths*, la filial de ciberseguridad de *Telefónica*. *"En los próximos años viviremos rodeados de dispositivos conectados a Internet que digitalizarán cada paso que demos, convertirán nuestra actividad diaria en información, distribuirán cualquier interacción por la red e interactuarán con nosotros en función de esta información. Nunca antes nuestro día a día había estado tan cerca del mundo digital. La difusa línea entre el mundo digital y el mundo real es precisamente el espacio donde se materializan los cambios introducidos por el Internet*

de las Cosas. Comprendamos el problema antes de que sea demasiado tarde y garanticemos que estamos en condiciones de ofrecer un plan de protección completo, aprovechando todos los conocimientos que se han generado en otros ámbitos".

Y es que, de entre la inmensa cantidad de datos que se manejan diariamente, los datos médicos son un negocio más que jugoso para los cibercriminales ya que pueden ganar hasta 10 veces más dinero en el mercado negro que los datos de las tarjetas de crédito, según ha avisado el ingeniero Guillermo Fernández de *WatchGuard Iberia* y *PALOPs*, quien ha advertido de que son una "*realidad*" los riesgos que tienen los dispositivos sanitarios que cuentan con información de pacientes [27]. Prueba de ello es el informe [29] *"2016 Healthcare Breach Report"*, elaborado por *Bitglass*, el cual asegura que solo en EE.UU. 111 millones de individuos sufrieron *hackeos* que tenían por objetivo datos relacionados con la salud. El aumento en un 80% de las violaciones de datos mediante *hackeos* pone de manifiesto el enorme interés de los datos médicos por parte de lo ciberdelincuentes debido a su gran valor en el mercado negro, así como poder acceder a atención médica haciéndose pasar por la víctima o realizar extorsión a las empresas. El coste promedio pagado por cada registro perdido o robado que contiene información sanitaria sensible y confidencial aumentó de 145 dólares en 2014 a 154 dólares en el estudio de este año elaborado por el *Ponemon Institute* [30]. Dicho coste global promedio llega hasta los 363 dólares si se trata de la perdida o robo de datos sanitarios por parte de una organización sanitaria.

Guillermo Fernández asegura que "*han puesto sus ojos*" en la industria sanitaria, por que es un sector que, a su juicio, cuenta con una seguridad "*insuficiente*" para tratar los ataques modernos, debido a la "*dependencia*" de las soluciones de protección anteriores. *"El equipamiento sanitario también evoluciona hacia el mundo digital, incrementando así las conexiones 'on line' y exponiéndose a una gran cantidad de nuevos ataques, por lo que su seguridad, a menudo, va por detrás de su tecnología"*, ha explicado Fernández. Por ello, ha destacado la necesidad de examinar los dispositivos médicos, tanto los nuevos como los antiguos, para ver si tienen defectos de seguridad y, por ende, utilizar la misma como parte del desarrollo del ciclo de vida para mitigar futuros riesgos.

La firma *Veracode* [28] ha publicado un estudio dónde se extraen varias conclusiones acerca de las vulnerabilidades en el software. La más impactante es que más del 80% de aplicaciones móviles para *iOS* tienen fallos en el cifrado. La fuente de información utilizada para la generación del reporte ha sido una plataforma que la firma tiene en la nube, la cual ha analizado más de 1,5 billones de líneas de código fuente. Tras el análisis de este código han podido llevar a cabo un diagnóstico y detección de ciertas carencias en el *software*. Los resultados del informe van más allá de las vulnerabilidades criptográficas, pero si nos centramos en lo que se puede encontrar en el informe sobre el tema es sorprendente ya que *"por cada empresa madura que está abordando la seguridad de aplicaciones móviles, surgen un montón de nuevas pequeñas empresas de software con programadores noveles que no lo abordan"*, dijo Chris Wysopal, experto en seguridad de *Veracode*. Esto muestra que existe una alta prevalencia de

problemas criptográficos en *iOS* y *Android* y los resultados de dichos problemas hacen reflejar que algo no se está haciendo bien por parte de los desarrolladores y que se debe mejorar.

Por ello, el objetivo principal de este Trabajo de Fin de Grado es desarrollar una guía completa en el campo de la seguridad de aplicaciones móviles de salud o *mHealth*, tratando de conocer el estado actual de las aplicaciones móviles de salud, en el marco de la *mHealth*, para dar como resultado una clasificación de los tipos de aplicaciones de salud existentes así como un estudio de seguridad y privacidad en aplicaciones móviles en base al análisis de sus funcionalidades, temáticas y aportaciones al sector de la salud.

Para ello primero ha sido necesario hacer un estudio del estado del arte de la *mHealth* o aplicaciones móviles de salud, así como la enorme transformación, desarrollo y crecimiento de la salud hacia entornos digitales, de manera que sirva como base para identificar los tipos de aplicaciones móviles de salud en función de las enfermedades más mortales a día de hoy según la *OMS*, mediante la presentación de un ejemplo de cada una de ellas.

Este estudio de seguridad, contempla las vulnerabilidades más extendidas en el campo del desarrollo de aplicaciones móviles y su importancia a la hora de manejar datos sensibles de usuarios. Está claro que estas aplicaciones, que nacen con el objetivo de mejorar el nivel de vida de sus usuarios, generan inquietud sobre la seguridad y nivel de protección de estos datos personales tan sensibles ante la posible divulgación o uso inadecuado y plantea dudas sobre si la normativa actual está obsoleta. Frente a esta situación, son muchas las voces que solicitan la creación de una regulación para mejorar la seguridad frente a un posible robo o *hackeo*, siendo necesario incluir una revisión del estado de la privacidad en el entorno digital, dando una visión global de aspectos legales, presentes y futuros, así como unos aspectos comunes extraídos de ellas que deberían cumplir cualquier ley actual sobre el tratamiento de datos personales.

El *TFG* facilitará, así como intentará mejorar o complementar, estándares de seguridad como el de *OWASP (Open Web Application Security Project)* mediante la elaboración de una guía específica para cada tipo de *app* de salud en función de la cantidad de datos que manipula cada una, proporcionando unas pautas de ayuda para desarrolladores de aplicaciones en dicho campo. Por supuesto, este estudio de seguridad en aplicaciones móviles de salud tendrá un fin informativo, ya que el desarrollador de la *app* podrá interpretar y adecuar su contenido en base al tipo de aplicación que desarrolle.

CAPÍTULO 2
MHEALTH

CAPÍTULO 2. MHEALTH

2.1 ¿Qué es mHealth? Desarrollo y nacimiento

El termino *mSalud (mHealth)* o mercado de aplicaciones móviles de salud es parte fundamental de algo más grande llamado *eSalud*, heredado de la *Telemedicina*, cuya primera referencia en la literatura médica aparecido en 1950 [31]. El artículo describe la transmisión, a partir de 1948, de las imágenes radiológicas por teléfono entre West Chester y Philadelphia, Pennsylvania, una distancia de 24 millas. Sobre la base de este primer trabajo, radiólogos canadienses del Hospital Jean-Talon de Montreal crearon un sistema de teleradiología en la década de 1950.

Desde entonces, en la intersección de muchos esfuerzos de médicos, investigadores de servicios de salud, e ingenieros en el uso de servicios de comunicación y tecnologías de la información para mejorar la atención de la salud, se encuentra la *Telemedicina* como combinación de tecnologías ya establecidas e innovación, que se define como "*el uso de tecnologías de la información electrónica y de las comunicaciones para proporcionar y apoyar la atención de la salud cuando la distancia separa a los participantes"* [31]

Históricamente, el impulso para desarrollar la *Telemedicina* vino de la mano de las primeras aplicaciones centradas en poblaciones remotas esparcidas por zonas montañosas, islas, llanuras y las regiones árticas, donde no era fácil que llegaran especialistas médicos y profesionales de la atención primaria. La mayoría de los proyectos de telemedicina de la década de 1960 hasta principios de 1980 falló. Los costes de las telecomunicaciones eran altos, y las tecnologías difíciles de usar. Pocos proyectos parecían estar guiados por un plan de negocios y los resultados necesarios para hacer de ello un proyecto sostenible. Recientemente, una nueva ola de interés en este campo ha llevado a una serie de nuevas actividades. Los costes se han reducido para muchas de las tecnologías de la información y comunicación que apoyan la telemedicina, y el desarrollo de las infraestructuras está haciendo estas tecnologías más comunes y mas fáciles de usar, dando lugar a un nuevo concepto.

Es en el séptimo *Congreso Internacional de Telemedicina y Teleasistencia* en Londres de 1999 [32] donde surge el nuevo concepto de *Telemedicina,* ahora llamado *eSalud.* John Mitchell de Sidney, Australia, se refirió a un estudio del gobierno nacional definiendo este concepto como el *"uso integrado de las telecomunicaciones y tecnologías de la información en el sector de la salud"*, más concretamente como *"el uso combinado de las tecnologías de la comunicación y la información electrónica en el sector de la salud mediante datos digitales - transmitidos, almacenados y recuperados electrónicamente - con fines clínicos, educativos y administrativos, tanto en el sitio local como a distancia".*

Es a partir de entonces cuando se usa el termino amplio y prometedor de *eSalud*, dejando de lado la *Telemedicina* puesto que tienen matices diferenciados, pasando a ser el nombre común para todos los campos tecnológicos vinculados a la salud orientada a la prestación de servicios, siendo éste el *"equivalente de comercio electrónico de la industria de la salud"*, englobando un conjunto dinámico de tecnologías, aplicaciones y procesos comerciales que enlaza tanto empresas, consumidores y a comunidades a través de un intercambio electrónico de productos, servicios, transacciones e información. – *Oracle* [32].

Por el contrario, la *Telemedicina* se usa para poder acceder a servicios médicos desde lugares alejados donde no llega cobertura médica especializada, usos tan comunes que a menudo se pasan por alto, como las llamadas de emergencia al 911 usando teléfonos ordinarios o simplemente el modelo tradicional de venta de equipos médicos.

Otra diferencia significativa es que la *Telemedicina* permanece vinculada a profesionales de la medicina, mientras que la *eSalud* es impulsada por los no profesionales, es decir, los pacientes o consumidores que con su interés conducen a nuevos servicios, incluso en el campo del cuidado de la salud sobre todo para su fortalecimiento a través del acceso a la información y el conocimiento.

La *eSalud* abarca una variedad de aplicaciones en la atención al paciente, la educación, la investigación, la administración y la salud pública, por que ya no solamente estamos preocupados por nuestra salud cuando sentimos algún dolor o tenemos alguna anomalía en nuestro cuerpo. Nos gusta cuidarnos y llevar una vida lo mas saludable posible, buscando en Internet información de salud o descargando alguna *app* relacionada con algún área de la medicina en particular.

Es en este contexto donde surge la *mSalud* como un componente de la salud electrónica *(eSalud)*. Hasta la fecha, no se ha establecido ninguna definición estandarizada de *mHealth*, pero según un informe de la *OMS (Organización Mundial de la Salud)* [33] llevado a cabo por el Observatorio Mundial para la eSalud *(GOe)*, se define la salud móvil como la práctica médica y de salud pública con el apoyo de los dispositivos móviles, tales como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes digitales personales *(PDA)*, y otros dispositivos inalámbricos. La *mSalud* es una parte de la *eHealth* y abarca el uso y capitalización en la utilidad principal de un teléfono móvil como son los servicios de voz y de mensajes cortos *(SMS)*, así como el uso de las funcionalidades más complejas y aplicaciones de un teléfono inteligente, incluyendo el servicio general de paquetes vía radio *(GPRS)*, la tercera y cuarta generación de telefonía móvil (sistemas 3G y 4G), sistema de posicionamiento global *(GPS)*, y la tecnología *Bluetooth*.

mHealth es la intersección entre salud electrónica y la tecnología de los teléfonos inteligentes [34]. La salud móvil abarca la adquisición, manipulación, clasificación y transmisión de información relacionada con la salud. El enlace de extremo a extremo, es usado normalmente para transmitir datos relacionados con la salud, captados por lo general con un sensor biomédico que esta en

contacto con el cuerpo del usuario o paciente. En los escenarios típicos, la información sensorial se recoge mediante dispositivos portátiles con un gran número de aplicaciones corriendo en ellos como es el caso de los *smartphones*. La información en forma de bits es transmitida a través de las señales inalámbricas como es el *Wifi* o redes móviles 3G o 4G almacenándose en servidores. Finalmente los administradores de estos servidores como puedan ser médicos, laboratorios, empresas o instituciones hospitalarias son los que gestionan dicha información en busca de su análisis e interpretación.

Neelie Kroes [35], vicepresidenta de la Comisión Europea, responsable de la Agenda Digital para Europa ha declarado: *"mHealth es sólo uno de los beneficios de un "continente conectado" –ayudar a los pacientes, médicos y cuidadores a tomar el control, estén donde estén. Desde aplicaciones sencillas que ayudan a cumplir con su régimen de ejercicio hasta herramientas de monitoreo para pacientes con diálisis renal."*

En un primer momento, las experiencias de *mHealth* se caracterizaron por su orientación informativa o de consulta. La capacidad del móvil para consultar información en cualquier momento y desde cualquier lugar, atrajo rápidamente iniciativas que trataban de resolver una duda médica o de llevar un control de nuestra salud a través de una *app*, de manera inmediata, pero cada día que pasa, los teléfonos móviles cobran cada vez más importancia en la supervisión y entrega de las intervenciones sanitarias. Son considerados como ordenadores de bolsillo, debido a sus potentes *CPUs* y *GPUs*, sistemas operativos estables y diversas capacidades técnicas. Sus sofisticados sensores y aplicaciones complejas de software hacen de las aplicaciones basadas en la salud algo viable e innovador. En una serie de escenarios de facilidad de uso, la conveniencia y la eficacia de estos sistemas han sido reconocidos por los pacientes, así como profesionales de la salud. La *mSalud* emplea conceptos y técnicas avanzadas de los campos multidisciplinarios de ingeniería eléctrica, ciencias de la computación, ingeniería biomédica y la medicina que se benefician de las innovaciones de estos campos hacia los sistemas de salud.

Con el catálogo disponible en las tiendas de aplicaciones, un usuario o usuaria estándar puede hacer un seguimiento de su presión arterial, su calendario menstrual o de un embarazo, marcar las tomas de un medicamento, consultar los hitos de crecimiento de un bebé o localizar las farmacias de guardia más cercanas, todo ello desde su móvil. Si hablamos de una patología en concreto, la utilidad de las aplicaciones adquiere mayor relevancia aún para el usuario. Es el caso de los enfermos de diabetes, que necesitan un especial cuidado para ajustar las dosis de insulina a los niveles de azúcar en sangre. En cuanto a la gestión remota de la salud, el control médico es el máximo estandarte. A través de las aplicaciones móviles se puede transmitir información en tiempo real, con datos que los dispositivos conectados permiten generar procesando la información generada durante la actividad física o simplemente como resultado de la rutina diaria y su muestra en forma de gráficas y datos que el usuario puede consultar desde el móvil. Pueden ayudar también a resolver a distancia una situación de riesgo, además de ofrecer información médica muy valiosa, que se puede almacenar en el historial del paciente.

El crecimiento protagonizado por las *apps* en la categoría de medicina ha demostrado que los dispositivos móviles no son un mero instrumento de entretenimiento. El volumen de aplicaciones disponibles relacionadas con la salud, son una clara muestra de su consolidación en un mercado distinguido por una voraz competencia. Es precisamente esa competencia la que, de la mano de los avances tecnológicos, están animando la renovación de la *mSalud*. La tendencia actual la marcan, sin duda, los dispositivos conectados. Esta claro que las aplicaciones móviles son desde hace unos años un gran aliado para la salud, pero es la consolidación de los dispositivos conectados la que está permitiendo una interacción más completa, partiendo de la actividad que generan los propios usuarios. Más que nada ofrecen la posibilidad de que sea el usuario quien tome el control y, al mismo tiempo, apoyan la evolución hacia un mejor estado de salud.

2.2 Impacto de las Enfermedades en la Sociedad

El mercado de las aplicaciones móviles de salud, o *mHealth*, se esta desarrollando en tres fases diferentes. Actualmente, los actores han conseguido salir de la fase inicial de pruebas y entrar en la fase de comercialización en el mercado. Esta fase se puede caracterizar por un incremento masivo de las soluciones ofrecidas, de la creación de nuevos modelos de negocio, y la concentración de gente interesada en la salud, como pacientes y corporaciones como grandes grupos objetivos [36].

Hoy en día hay más de 100.000 *apps* de salud en varios catálogos de aplicaciones. La mayoría de estas tratan de herramientas de ayuda que facilitan a miembros individuales el seguimiento de ciertos parámetros de la salud, además de proveerles de información variada de salud [36]. Cabe destacar que el número de aplicaciones crece día a día, debido a la disposición de los programadores de herramientas y a las *APIs (Application Programming Interface)* necesarias para hacer posible cualquier aplicación inimaginable. Además, las denominadas "tiendas de aplicaciones" facilitan la tarea tanto a programadores para que su producto sea visible, como a clientes en la búsqueda de aplicaciones relacionadas. Por ello, hay que determinar en qué punto acotar la búsqueda de *apps* de salud, y para ello se acude a estudios sobre el impacto de las enfermedades en la sociedad.

Según estimaciones de la *OMS* [37], en el año 2012 se produjeron 56 millones de muertes en el mundo. Las enfermedades no transmisibles causaron más de 68% de las muertes en el mundo, lo que representa un aumento por comparación con el 60% registrado en el año 2000. Como muestra la *Figura 2.1* y la *Figura 2.2*, las cuatro entidades nosológicas principales de este grupo son las enfermedades cardiovasculares, el cáncer, la diabetes y las neumopatías crónicas. Las enfermedades transmisibles, maternas, perinatales y relacionadas con la nutrición causaron en conjunto una 23% de las muertes en el mundo, y los traumatismos, un 9%.

Las enfermedades cardiovasculares son la causa número uno de muerte en el mundo con 17,5 millones de muertes en 2012; es decir, 3 de cada 10. De estas, 7,4 millones se atribuyeron a la

cardiopatía isquémica (13,2% de las muertes), y 6,7 millones, a los accidentes cerebrovasculares (11,9%). Seguidamente, encontramos la enfermedad pulmonar obstructiva crónica ó *COPD* (5,6%) e infecciones respiratorias bajas (5,5%) [37].

Si nos fijamos en la *Figura 2.3*, el número de muertes causadas por las enfermedades crónicas aumenta sin cesar en todo el mundo. El cáncer pulmonar (junto con el de la tráquea y el de los bronquios) causó 1,6 millones de defunciones (2,9%) en 2012, por comparación con 1,2 millones (2,2%) en 2000.

El número de defunciones debidas al *VIH* se redujo levemente, de 1,7 millones (3,2%) en 2000, a 1,5 millones (2,7%) en 2012. La diarrea ya no figura entre las cinco principales causas de defunción, pero aún está entre las diez primeras, y en 2012 se cobró las vidas de 1,5 millones de personas (2,7%). De modo parecido, la diabetes causó 1,5 millones de defunciones (2,7%) en 2012, por comparación con 1,0 millones (1,9%) en 2000. Por último, nos encontramos los accidentes de tráfico con un 2,2% de las muertes totales y la cardiopatía hipertensiva con un 2%.

Figura 2.1. Las diez principales causas de defunción en el mundo en porcentaje (2012). Fuente: [37]

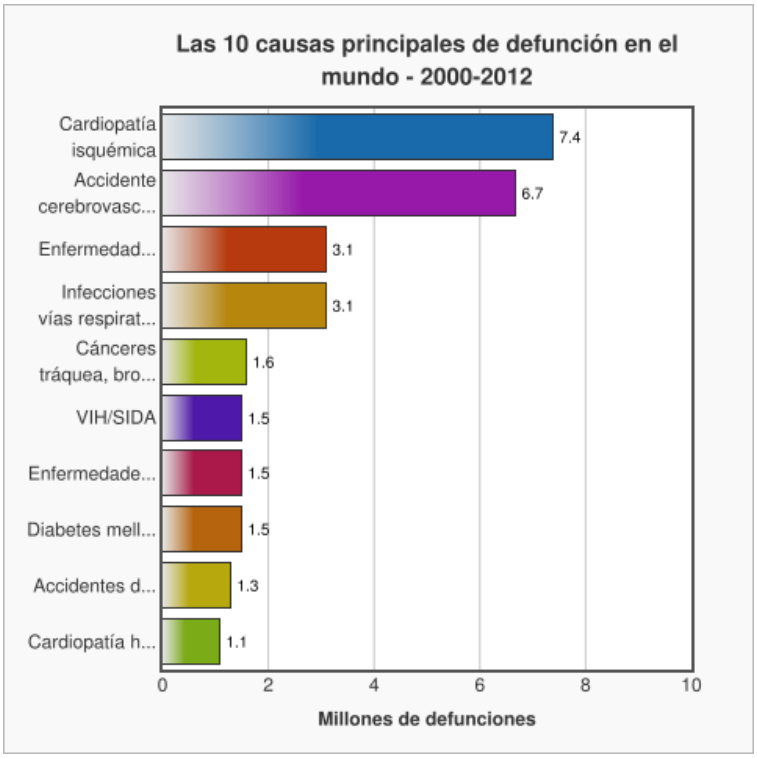


Figura 2.2. Las diez principales causas de defunción en el mundo (2000 – 2012). Fuente: [37]

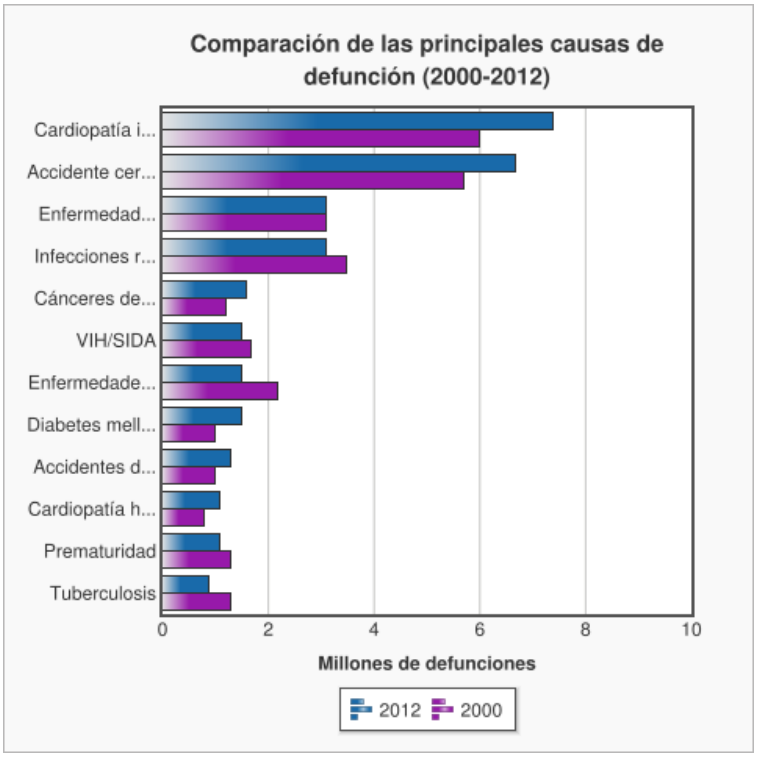


Figura 2.3. Comparación de las principales causas de defunción (2000 – 2012). Fuente: [37]

Se analiza además el *Global Burden of Disease (GBD)* de 2004 [38], que muestra las dolencias que generan un mayor número de nuevos casos de personas enfermas en el mundo, así como las enfermedades más predominantes para años venideros.

Las dolencias que generan un mayor número de casos aportan nuevas enfermedades al estudio, como la malaria (causante de 198 millones de nuevos casos), el sarampión (27,1 millones) o la tos ferina (18,4 millones).

Las enfermedades más predominantes tienen en cuenta aquellas dolencias cuyos síntomas no se presentan de manera continuada. Se estudian las diez primeras causas por millones de personas afectadas: anemia (1159 millones), pérdida de audición (636,5 millones), migrañas (324,1 millones), pérdidas de visión (272,4 millones), malnutrición (238,9 millones), asma (234,9 millones), diabetes (220,5 millones), osteoartritis (151,4 millones), trastornos depresivos unipolares (151,2 millones), fuertes infecciones intestinales (150,9 millones) y trastornos vinculados al uso del alcohol (125 millones) [38].

El objetivo principal es poner sobre la mesa la cantidad de *apps* móviles disponibles para cada una de las enfermedades y dolencias citadas, detectando los puntos fuertes y débiles de cada sección, para generar como punto de partida, una clasificación según el tipo de aplicación que nos permita trabajar en el desarrollo de la seguridad a implementar en cada uno de los tipos, paliando las carencias identificadas y mejorando las funcionalidades ya existentes.

A continuación, en el apartado de tipos de *apps* móviles de salud, se aborda la manera de proceder con la búsqueda de aplicaciones, presentando tanto las tiendas donde buscar, los criterios de selección y la forma de presentación de los datos obtenidos. También se mostrarán los resultados divididos en dos partes, por un lado las conclusiones generales del conjunto de dolencias estudiadas, y por otro el porcentaje de aplicaciones de cada clase.

2.3 Tipos de Aplicaciones Móviles de Salud

La búsqueda de aplicaciones se centra en aquellas aplicaciones comerciales dispuestas al público en general en las distintas tiendas de aplicaciones de las plataformas más importantes a fecha de agosto de 2015 [7,39], que son –en orden descendente de cuota de mercado- *Google Play* de *Android* [40], *iTunes App Store* de *Apple* [41], *Windows Phone Apps+games* de *Microsoft* [42], *BlackBerry World* de *BlackBerry* [43] (antiguo *RIM* o *Research In Motion*) y otros como *Ovi Store* de *Nokia* [44].

Haciendo una recopilación de todas las tiendas de aplicaciones móviles, ya hay más de [45] 165.000 *app*s relacionadas con la salud y la medicina, siendo la tercera categoría con mayor crecimiento solo por detrás de juegos y utilidades, según afirma el informe *"Patient Adoption of mHealth"* publicado por el *IMS*. Partiendo de esta premisa y basándonos en el "Análisis y evolución de las aplicaciones móviles en el campo de la salud" publicado en el "I+S Informática y Salud" de Diciembre de 2014 [47], las directrices que se siguen a la hora de discriminar entre los resultados de las búsquedas llevadas a cabo son, descartar aquellas *apps* que no estén disponibles en inglés o castellano, aceptándose sólo como válidas las *apps* encuadradas en "medicina" y "salud o bienestar"

("salud y forma física"), ya que [45] el 65% de las *app*s de salud van dirigidas al público en general, siendo estas las relacionadas con el ejercicio físico y el bienestar, mientras que el 35% restante están dirigidas hacia el sector de los profesionales sanitarios y sus pacientes. La funcionalidad más común que ofrecen las aplicaciones relacionadas con la salud es la de aportar información, lo que representa más de dos tercios de todas las aplicaciones de *mHealth*, y el principal uso de las mismas está relacionado con la prevención o estilos de vida.

Como excepciones de las aplicaciones mencionadas anteriormente están los localizadores de enfermos de alzhéimer o las *apps* relacionadas con trastornos depresivos que permiten interactuar con otros usuarios a modo de "red social". Para la inclusión de las *apps* en los listados de aplicaciones, en aquellas búsquedas donde los resultados sean elevados, se opta por incluir una muestra variada de las opciones disponibles, teniendo en cuenta el número de descargas y las valoraciones de los usuarios. Cuando los resultados sean mínimos, se opta por incluir todas las *apps* disponibles, así como otras que tengan un mínimo de relación con la palabra clave empleada para su búsqueda.

Para ello, lo primero ha sido elegir la palabra calve relacionada con la dolencia o enfermedad correspondiente y se ha llevado a cabo la búsqueda. La no obtención de resultados lleva a variar dichas palabras clave. En caso afirmativo, se analiza cada aplicación individualmente, para comprobar si cumple los requisitos o parte de éstos y listarla por enfermedad y plataforma. Una vez finalizada la búsqueda, el resultado se centrará en las plataformas *iOS (Apple)* y *Android (Google)*, concediéndoles la importancia que el propio mercado les otorga por si mismo.

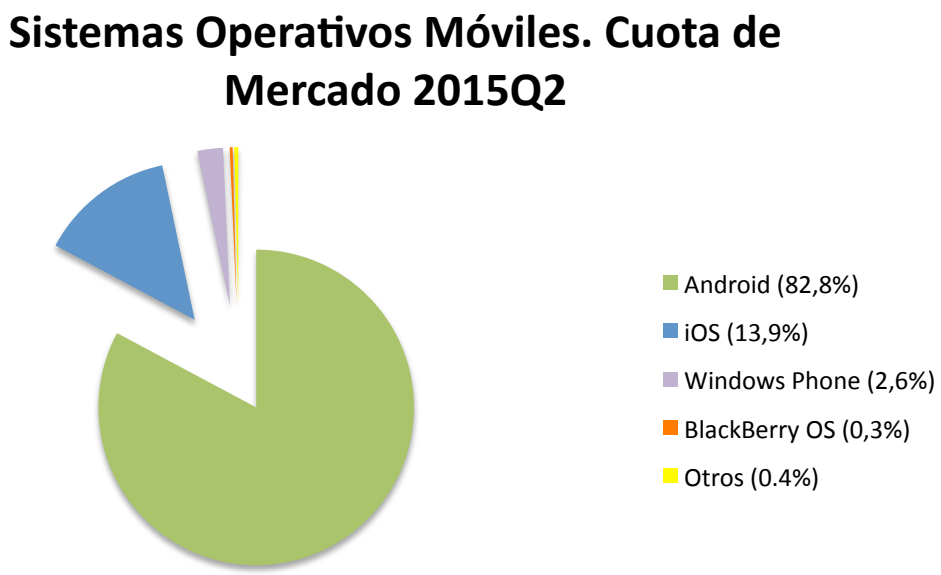
Las enfermedades isquémicas del corazón son buscadas dentro de una palabra clave que engloba toda una especialidad como es cardiología. La sección de fuertes infecciones intestinales no muestra resultados, aquellos que podrían incluirse por afinidad ya lo han sido en la sección de enfermedades diarreicas. Accidentes de tráfico y trastornos vinculados al uso del alcohol sólo muestran alcoholímetros que estiman el alcohol en sangre; al poseer baja fiabilidad no se listan. Tampoco se obtienen resultados para tos ferina y malnutrición.

La búsqueda de aplicaciones comerciales llevada a cabo para un total de 26 enfermedades muestra que a fecha de 2013 (último año del que se disponen datos) había 2.837 aplicaciones válidas en las diferentes plataformas móviles y que a día de hoy, ha sufrido un aumento del 70%, lo cual da como resultado una estimación aproximada de 4.823 aplicaciones de salud para dichas enfermedades.

Google Play presenta el mayor número de resultados, seguida de cerca por la *App Store* de *Apple* [46], que ha crecido un 106% desde 2013 pasando de tener 43.689 *apps* a tener un catalogo 90.088 aplicaciones relacionadas con la salud. Esto nos da una idea respecto al dinamismo, evolución y constante crecimiento del mercado de aplicaciones móviles que sufren las principales tiendas de aplicaciones, por lo que es probable que en lo que a volumen de aplicaciones médicas se refiere, puedan alternarse la primera posición cada cierto tiempo. Sin embargo, el resto de plataformas no

presentan unos datos tan positivos. *Apps+Games* de *Microsoft* se sitúa como la tercera plataforma, un peldaño por debajo nos encontraríamos a *BlackBerry World*. Totalmente olvidada queda *Ovi Store* de *Nokia*.

En cuanto al sistema operativo utilizado, es muy notable el predominio *Android*, como se muestra en la *Figura 2.4*. En los *smartphone*s, en 2015Q2 [39], el sistema operativo *Android* está presente en un 82,8% de ellos, seguido por el sistema operativo *iOS*, con una presencia del 13,9%. Sin embargo, respecto a las *tablet*s [46], *Android* está presente en un 66% de ellas, mientras que *iOS* lo hace en un 25,5%.



Periodo	Android	iOS	Windows Phone	BlackBerry OS	Otros
2015Q2	82,8%	13,9%	2,6%	0,3%	0,4%

Figura 2.4. Sistemas Operativos Móviles. Cuota de Mercado 2015Q2. Fuente: [39]

Por dolencias o enfermedades, quien acumula un mayor número de aplicaciones relacionadas es la diabetes [47]. En segundo lugar lo ocupa la sección denominada como cardiología. Muy por debajo se sitúan el resto, divididas en tres bloques por cantidad de aplicaciones. Alzheimer, *VIH*, asma, cáncer de tráquea, bronquios y pulmón y enfermedades cerebrovasculares forman el primer bloque. Un segundo grupo está formado por cáncer de mama, osteoartritis, enfermedades diarreicas, pérdida de visión, infecciones de las vías respiratorias bajas, perdida de audición y *COPD*. El último grupo incluye tanto las secciones con pocas o ninguna aplicación disponible, como anemia, malaria, cáncer de colon y recto, tuberculosis, sarampión, parto prematuro y accidentes de tráfico, infecciones

intestinales, malnutrición, tos ferina y trastornos derivados del uso de alcohol que no aportan ninguna aplicación.

Las dolencias de sarampión, tuberculosis y anemia son las secciones donde existe un mayor número de aplicaciones *Android*, frente al cáncer de colon y recto, *COPD* y cardiología donde *iOS* presenta más número de aplicaciones.

Teniendo en cuenta todo lo mencionado hasta ahora y extrapolando los datos, se obtiene el porcentaje de aplicaciones según su utilidad como se muestra en la *Figura 2.5*. Debido a que no se necesita implementar ninguna característica especial, las aplicaciones más abundantes de manera muy destacada son las informativas y suponen [47] casi cuatro de cada diez *apps* (37,48%). En segundo lugar las *apps* con carácter educacional (17,30%). En esencia estas dos secciones son la misma, pero cambia la manera de enfocar y enseñar la información al usuario. Juntando las dos como una sola, se obtiene que un 54,78% de las *apps* son de este tipo. Es decir, 1 de cada 2 aplicaciones ofrece contenidos de información al usuario o contenido más científico dirigidas fundamentalmente a profesionales de la salud. Las herramientas de monitorización de parámetros físicos y ayuda al diagnóstico son las dos siguientes en orden de importancia rondando ambas el 14%, con amplio contenido médico, pero concebidas para servir de apoyo a pacientes y familiares/cuidadores en el proceso de una enfermedad o problema médico. El resto de clases no son tan visibles, siendo las que disponen de contenido más generalista ya que facilitan la labor de la prevención, atención primaria y el cuidado de la salud, dirigidas a la sociedad en general: las que ayudan en el seguimiento del Tratamiento (7,65%), Calculadoras (5,57%), Asistenciales (2,78%), Localizadores (1,74%) y Alarmas (0,17%). Estas dos últimas clases de *apps* se dan en alzhéimer y enfermedades cerebrovasculares respectivamente.

Muchas de las *apps* necesitan hacer uso de la Internet para funcionar, a través de redes móviles mediante 3G/4G o *Wifi*, o para disponer de alguna de sus funcionalidades. Algunas de éstas lo necesitan de manera continuada para acceder a algunas particularidades incluidas, como opiniones de otros usuarios, videos explicativos, etc. En un punto medio se encuentran aquellas que necesitan actualizar la información mostrada cada cierto tiempo -como servidores de noticias-, o descargar paquetes de información -enciclopedias y guías médicas-. Sin embargo, la experiencia tras este estudio muestra que la gran mayoría de aplicaciones sólo necesitan Internet para enviar información acerca de resultados obtenidos por el usuario, ya sea por correo electrónico, redes sociales, o a través de las propias funcionalidades implementadas en cada aplicación en particular, pudiendo ser los receptores de dicha información tanto profesionales sanitarios (médicos y enfermeros), industria, asociaciones de pacientes, sociedades científicas, organismos públicos, así como empresas del sector sanitario, tecnológico y otros usuarios.

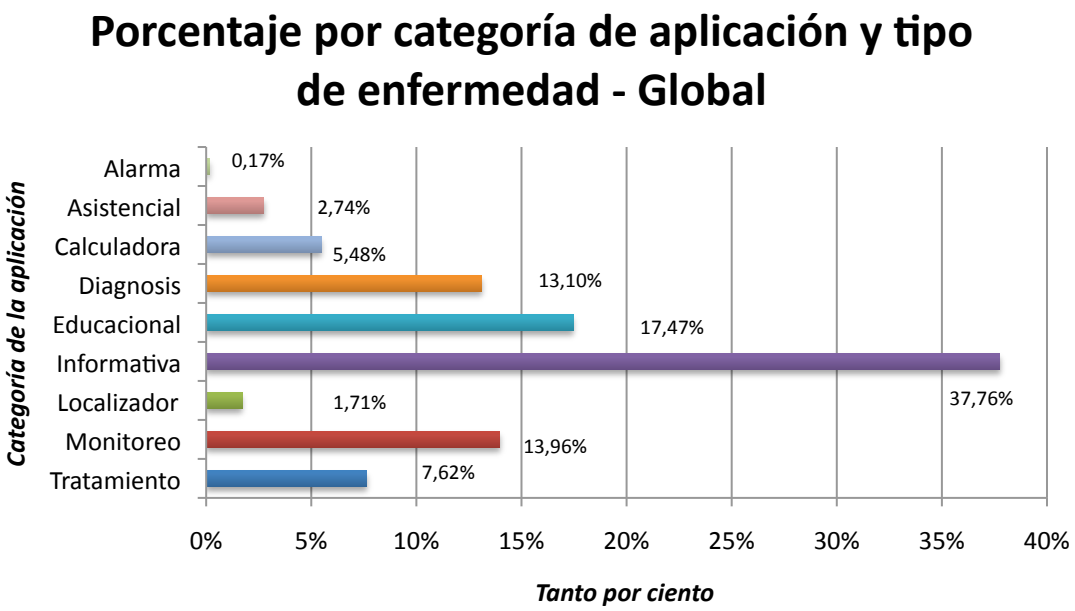


Figura 2.5. Porcentaje por utilidad de *app* y tipo de enfermedad - Global. Fuente: Propia

El proceso de categorización ha entrañado ciertas dificultades, ya que no existe, por el momento, una clasificación consensuada de categorías y cada informe usa la que considera más adecuada. En nuestro caso hemos establecido nueve categorías intentando abarcar grandes áreas de estudio y funcionalidad de las aplicaciones, de forma que todas puedan verse representada por alguna de las mismas mediante un ejemplo.

1. **Informativa & Educacional.** Tienen como principal función aportar información completa y detallada sobre alguna patología determinada o área de especialización médica, ya sea en formato texto, imagen o vídeo, así como aportar información actualizada sobre alguna enfermedad facilitando la educación activa por parte del paciente o público al que va dirigida [17]. En este apartado nos encontramos con aplicaciones como:

   - ***Heart Pro III* (Informativa):** La *Imagen 2.1* muestra un atlas del corazón muy completo que ayuda a explicar las distintas afecciones y enfermedades del corazón. Tiene diferentes funcionalidades: animaciones, cuestionarios y locuciones con nombres de diferentes partes del corazón. La *app* está avalada por la facultad de medicina de la Universidad de Stanford [41].
   - ***Kids Beating Asthma* (Educacional):** Tal y como muestra la *Imagen 2.2*, su objetivo es educar al paciente infantil ofreciéndole claves sobre el asma, explicando en que consiste, su origen y cómo convivir con dicha patología. Incluye actividades lúdicas que ayudan a reforzar la comprensión del mensaje educativo. Está avalada por "Incubadora de Ideas" del Instituto de Investigación Sanitaria del Hospital Clínico San Carlos. [41]

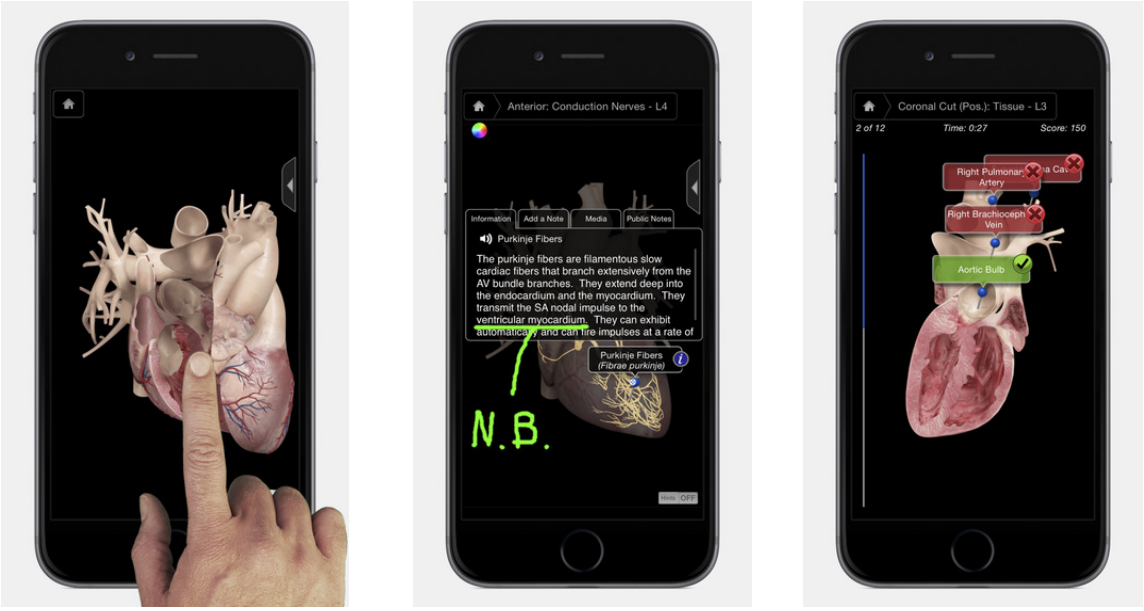


Imagen 2.1. Interfaz de la *app Heart Pro III* (Informativa). Fuente: [41]

Imagen 2.2. Interfaz de la *app Kids Beating Asthma* (Educacional). Fuente: [41]

2. **Monitoreo.** Las aplicaciones de monitoreo, miden todos nuestros parámetros físicos permitiéndonos tomar el control sobre nuestra salud y nuestro bienestar [17].

   - ***Endomondo:*** Tiene como objetivo promover un estilo de vida saludable a través de la actividad física. A modo de entrenador personal, registra rutas, consumo de calorías, frecuencia cardiaca y otros parámetros físicos tal y como se ve en la *Imagen 2.3*, motivando a los usuarios a mantenerse activos. Fomenta además el ejercicio social, planteando retos con amigos y compartiendo la actividad a través de las redes sociales [41].

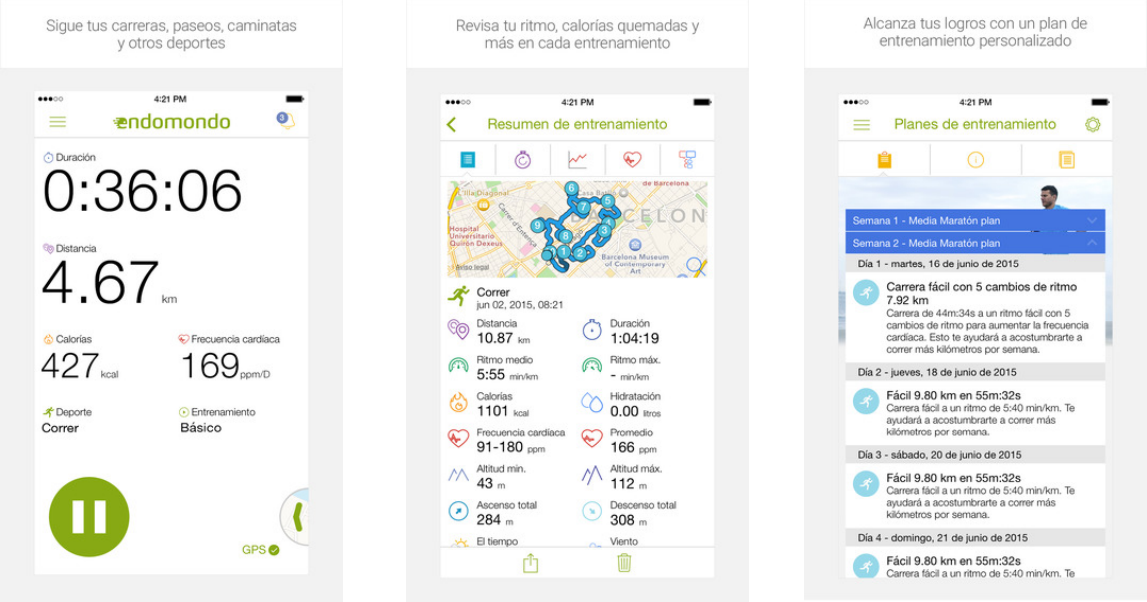


Imagen 2.3. Interfaz de la *app Endomondo* (Monitoreo). Fuente: [41]

3. **Diagnosis.** Este tipo de aplicaciones facilitan el proceso de identificación de una determinada enfermedad o alteración médica, aportando datos de valor para el profesional sanitario [17].

- ***Mobile MIM:*** Se dirige a profesionales y permite la visualización, intercambio y registro de imágenes *SPECT, PET, CT, MRI,* radiografías y ultrasonidos. Como se aprecia en la *Imagen 2.4*, se puede utilizar para revisar las imágenes, los contornos, el *DVH* y las curvas de isodosis de los planes de tratamiento de radiación [41].

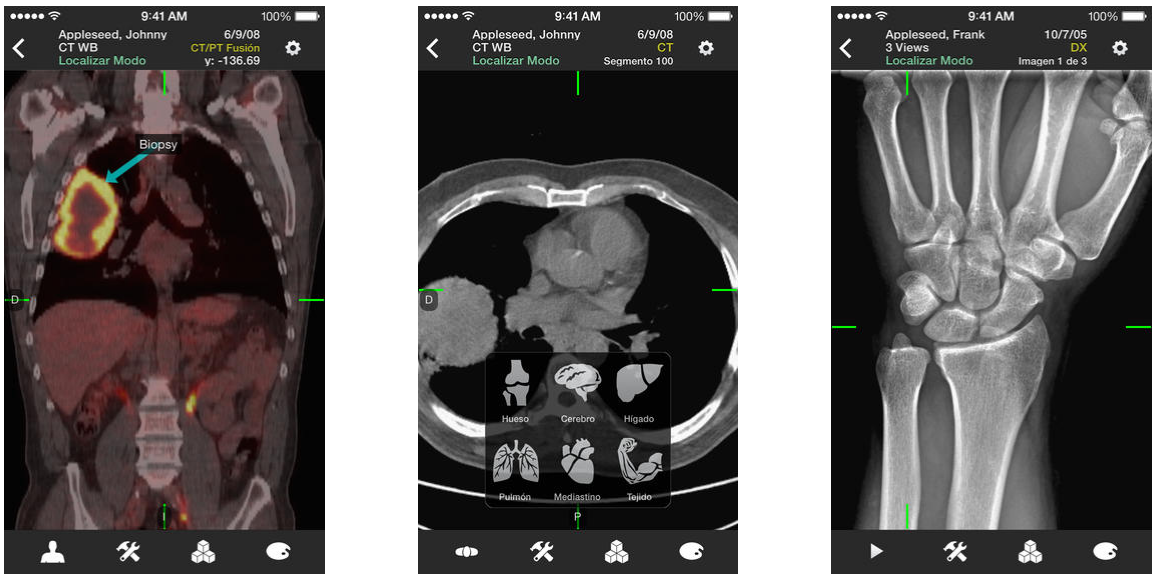


Imagen 2.4. Interfaz de la *app Mobile MIM* (Diagnosis). Fuente: [41]

4. **Tratamiento**. Este tipo de aplicaciones ayudan al control y tratamiento de enfermedades, permitiendo al paciente llevar un control de sus hábitos saludables, sobre medicamentos y su adherencia al tratamiento, y permiten una atención continuada e inmediata, más allá de la consulta tradicional [17].

- ***MediSafe:*** Se trata de una aplicación, como podemos ver en la *Imagen 2.5*, que ayuda a recordar la toma de medicamentos mediante el envío de notificaciones. Es especialmente útil para seguir el tratamiento de enfermedades crónicas. Permite gestionar gran número de afecciones y se puede sincronizar con los pastilleros de familiares para controlar su medicación [41].

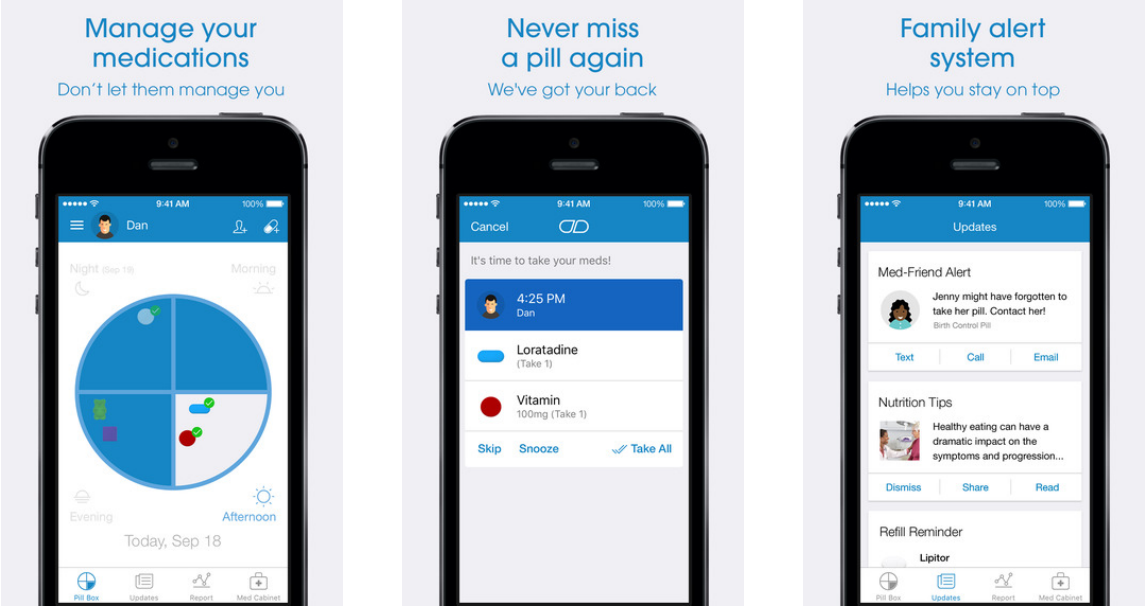


Imagen 2.5. Interfaz de la *app MediSafe* (Tratamiento). Fuente: [41]

5. **Calculadoras.** Este tipo de aplicaciones móviles de salud permiten calcular el índice de masa corporal, la tasa metabólica basal, la frecuencia cardíaca máxima, el contenido de alcohol en la sangre, la dosis de antitérmico recomendada en función del peso del niño, etc.

- ***FitCalculator***: Es una aplicación para hacer de manera sencilla un seguimiento de la salud y el estado físico mediante el cálculo del el Índice de Masa Corporal *(IMC)*, Tasa Metabólica Basal *(TMB)*, Porcentaje de Grasa Corporal *(PGC)*, Masa Corporal Magra *(MCM)* y peso ideal. Sugiere dietas saludables, tal y como nos muestra la *Imagen 2.6* [41].

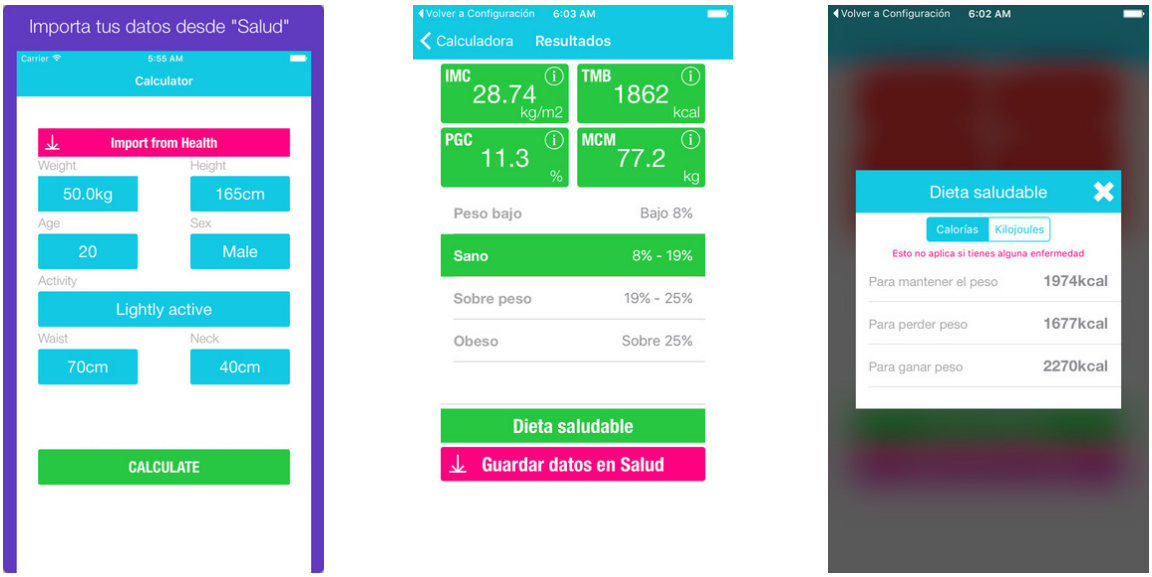


Imagen 2.6. Interfaz de la *app FitCalculator* (Calculadora). Fuente: [41]

6. **Asistenciales.** Este tipo de aplicaciones permiten mejorar la gestión asistencial de los pacientes proporcionando inmediatez en derivaciones de tratamientos y seguimiento clínico de pacientes, conociendo exhaustivamente que sucede con ellos en todo momento.

   - ***Click Doctors:*** En la *Imagen 2.7* vemos como esta aplicación nos permite llevar un registro gratuito de distintas variables de salud, monitorizar constantes vitales y que éstas sean controladas por un equipo médico proporcionando asistencia médica 24 horas los 365 días del año en caso de ver alguna anomalía, así como recibir asistencia farmacéutica personalizada [40].

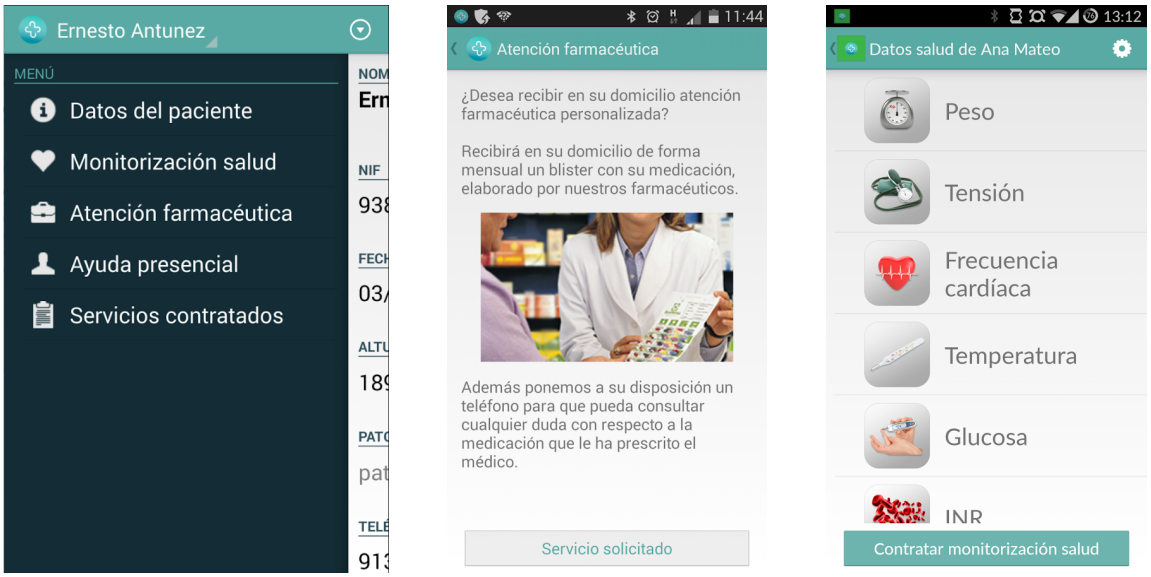


Imagen 2.7. Interfaz de la *app Click Doctors* (Asistencial). Fuente: [40]

7. **Localizadoras.** Permiten pedir ayuda u orientarte de manera rápida y efectiva mediante localización *GPS*, tal y como se puede ver en la *Imagen 2.8*.

- ***Tweri:*** Permite que las personas con alzhéimer estén localizadas, siendo útil tanto para pacientes como para sus familiares y cuidadores. En su desarrollo ha participado la Asociación de Familiares de Enfermos de Alzheimer *AFAL* Getafe [40].

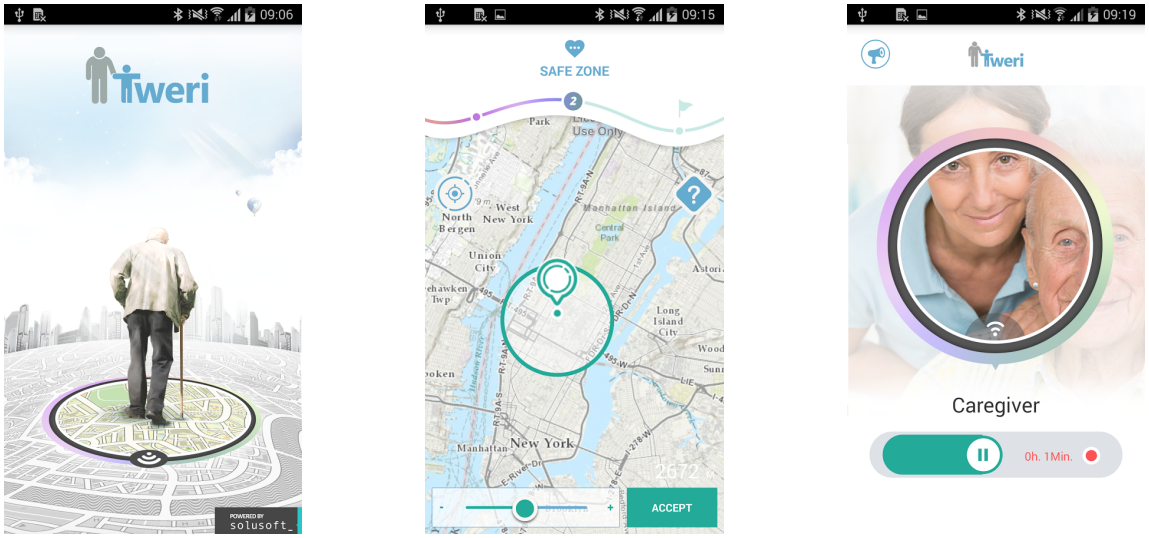


Imagen 2.8. Interfaz de la *app Tweri* (Localizadora). Fuente: [40]

8. **Alarma.** Son aplicaciones móviles que pretenden avisarte mediante una alarma sobre algún acontecimiento importante relacionado con tu salud. La *Imagen 2.9*, muestra un ejemplo.

- ***Pocket Cylce:*** Permite llevar un mejor control y seguimiento de la menstruación y la fertilidad. Da la opción de crear recordatorios personales y alarmas para la toma de la píldora anticonceptiva, entre otros [41].

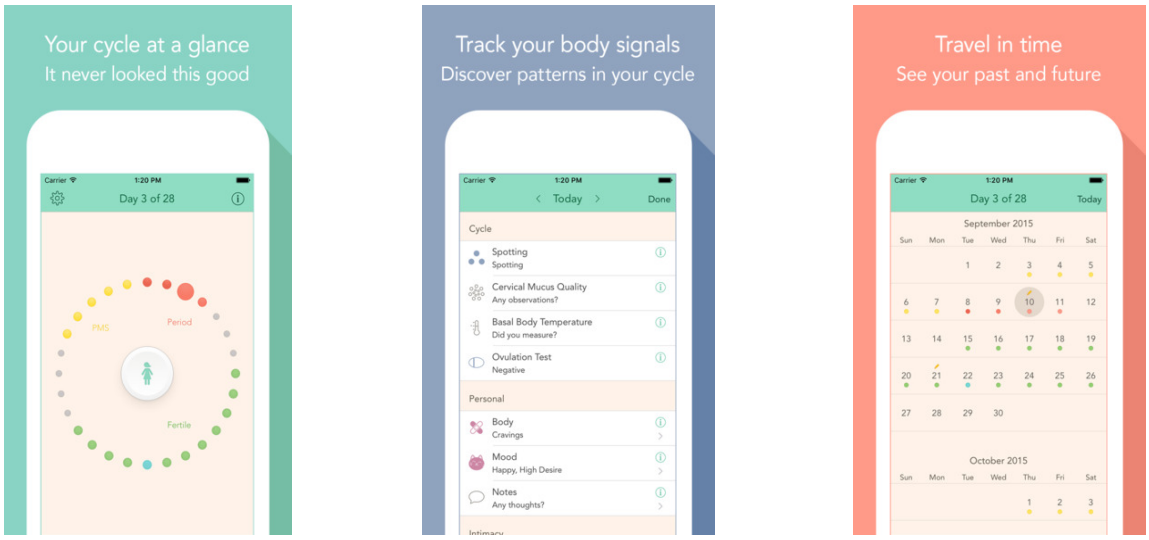


Imagen 2.9. Interfaz de la *app Pocket Cycle* (Alarma). Fuente: [41]

Después de este repaso por los tipos de aplicaciones móviles de salud mediante el uso de ejemplos, hay que resaltar una cuestión bastante importante, que es saber que tipo de seguridad implementar a cada uno de lo tipos de aplicaciones vistos anteriormente, según sus características, como herramientas de apoyo por parte de especialistas, estudiantes o público en general. Por ello, en el siguiente bloque, trataremos el tema de la importancia en la privacidad y seguridad en aplicaciones móviles que tratan información sensible de los usuarios.

CAPÍTULO 3

SEGURIDAD & PRIVACIDAD

CAPÍTULO 3. SEGURIDAD Y PRIVACIDAD

3.1 Importancia de la Seguridad y Privacidad en Aplicaciones Móviles

En los últimos 15 años, los avances significativos en el campo de las telecomunicaciones y la informática han propiciado un increíble impulso de las comunicaciones móviles y redes inalámbricas [48-55], así como la expansión de los teléfonos móviles y su extenso uso, especialmente teléfonos inteligentes con nuevas características capaces de aprovechar las nuevas redes 3G y 4G [56-58] gracias a la combinación de tecnologías como el escalado de transistores, gráficos de alta calidad mediante potentes *GPUs* y el uso de diseños compactos [59-62]. Por lo tanto, los últimos datos publicados por la *ITU* (Unión Internacional de Telecomunicaciones) estiman que en la actualidad hay más de 7.000 millones de líneas móviles a fecha de mayo de 2015 [4] y un estudio realizado por los analistas de *Gartner* mostraba como las ventas de teléfonos inteligentes han sobrepasado el billón de unidades en 2014 representando las dos terceras partes del mercado global de teléfonos [63], sufriendo un aumento del 28,4% respecto a 2013, y los números siguen aumentando continuamente.

El mercado de teléfonos inteligentes ha creado una nueva industria del *software* basada en la creación de aplicaciones para *smartphones*, lo que conlleva a ingentes oportunidades de desarrollo socioeconómico. Esta industria se ha expandido exponencialmente y está continuamente en progreso, de hecho el número de desarrolles activos de *Google Play* ha crecido casi hasta las 400.000 personas a lo largo de estos tres últimos años [64], ganando por mucho al resto de tiendas de aplicaciones. Como se puede ver en la *Figura 3.1*, 2014 ha sido un año destacado para los dispositivos móviles, ya que por primera vez la *Play Store* de *Google* ha superado a la *App Store* de *Apple* en número de aplicaciones dando como resultado entre las dos, más de dos millones aplicaciones creadas para los dos sistemas operativos de *smartphones* más importantes, *Apple iOS* y *Google Android* [64], donde secciones como la de los videojuegos son las grandes beneficiarias experimentado una mayor subida, aunque se cuelen aplicaciones de estilo de vida pertenecientes a las 165.000 *apps* que están orientadas a la salud como se ha comentado en líneas pasadas.

Teniendo en cuenta sólo esos sistemas operativos mencionados anteriormente, la tienda de aplicaciones de *Apple* [45,41] tiene más 90.000 aplicaciones para *iOS*, relacionadas con la medicina, la salud y la forma física mientras que *Google Play* para *Android* [40], cuenta con más de 74.000 aplicaciones médicas y cuidado de la salud [45]. Todas estas aplicaciones están incluidas en lo que se conoce como *mHealth* o la salud móvil, definido por la *OMS* (Organización Mundial de la Salud) como: *"la práctica de la medicina y la salud pública soportada por dispositivos móviles como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes personales digitales y otros dispositivos inalámbricos"* [33].

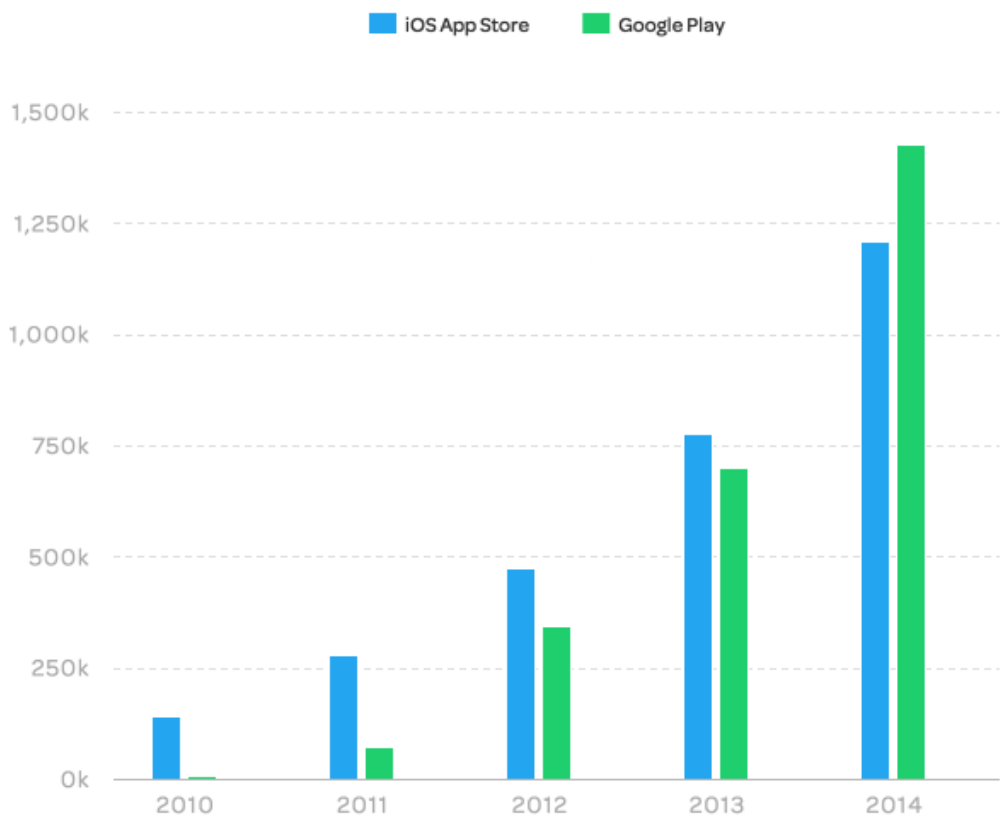


Figura 3.1. Comparación entre el número de aplicaciones de *iOS* y *Android* (2014). Fuente: Propia

Sin embargo, en esta carrera por ser el primero en el desarrollo y realización de una nueva aplicación, algunos aspectos no se han considerado adecuadamente. Entre ellos, la privacidad y la seguridad, tienen una importancia singular, especialmente en aquellas aplicaciones que tienen que ver con los datos personales y no transferibles, como las aplicaciones de salud que almacenan un registro electrónico de la salud de los pacientes o varios datos relativos a su estado de salud. De acuerdo con las definiciones adoptadas por el *NCVHS* (Comité Nacional de Estadísticas Vitales y de Salud) del departamento de Salud y Servicios Humanos [65], *"la privacidad de información sobre la salud es el derecho del individuo para controlar la adquisición, utilización, o divulgación de sus datos de salud. La confidencialidad, que está estrechamente relacionada, se refiere a las obligaciones de los que reciben información de respetar el interés de privacidad de aquellos a los que se refieren los datos. La seguridad es totalmente diferente. Se refiere a las garantías o las herramientas físicas, tecnológicas o administrativas que se utilizan para proteger los datos de salud identificables de su acceso o divulgación indebida".*

Una de las conclusiones del estudio realizado por *IBM* y *Ponemon Institute* [66] en más de 400 grandes organizaciones de todo el mundo demuestra que el 50% de las grandes empresas desarrolladoras de aplicaciones móviles no destina ningún presupuesto a la seguridad y casi el 40% de ellas no están tomando las precauciones pertinentes para proteger las aplicaciones móviles que desarrollan para sus clientes. El estudio demuestra que el número de ciberataques que tienen que ver con la seguridad de los dispositivos móviles sigue creciendo y actualmente los ataques afectan a más

de 11,6 millones de dispositivos móviles. Hoy en día, los cibercriminales están aprovechando la popularidad de las aplicaciones móviles inseguras y de las redes *Wifi* públicas para acceder a información importante que a menudo se almacena en dispositivos móviles.

El estudio también ha encontrado importantes fallos de seguridad en el modo en que la mayoría de las organizaciones desarrolla e implanta las aplicaciones móviles para sus clientes. Un 33% de las compañías nunca prueba sus aplicaciones. Cada una de ellas se gasta una media de 34 millones de dólares anuales en desarrollar aplicaciones para el móvil pero solo el 5,5% de este presupuesto se asigna a garantizar que sean seguras frente a ciberataques antes de estar disponibles para los usuarios.

Además, los médicos y los pacientes están adoptando las tecnologías móviles más rápido de lo que los proveedores pueden proteger la seguridad y la privacidad de éstas, convirtiéndolo en un problema significativo, es por ello que las empresas dan prioridad al plazo de salida al mercado y a la experiencia del usuario, descuidando la seguridad, con lo que abren vías de acceso a información confidencial de negocio y personal para ciberdelincuentes. Sólo en 2014 se pusieron en peligro más de 1.000 millones de registros de información personal como consecuencia de ataques cibernéticos. Durante el desarrollo de las aplicaciones móviles, aspectos como la utilidad para el usuario final está por encima de la seguridad y la privacidad. De acuerdo con el estudio, el 65% de las organizaciones afirma que la seguridad se ve a menudo comprometida por las demandas del cliente y el 77% menciona "las prisas por el lanzamiento" como la razón principal por la que las aplicaciones contienen un código vulnerable. De las empresas que en la actualidad analizan vulnerabilidades antes de lanzar aplicaciones en el mercado, solo el 15% las prueba con la frecuencia necesaria para comprobar que sean seguras y efectivas.

El fenómeno *BYOD* (*Bring Your Own Device*) [66] se está popularizando e incluso, en muchos casos, se está convirtiendo en una necesidad para las compañías y las organizaciones de atención de la salud que han aceptado fácilmente este enfoque debido a la comodidad y el ahorro potencial de costes por permitir a los empleados llevar sus propios dispositivos para trabajar, aun suponiendo un riesgo. [67,68] Según una encuesta reciente de la *HIMSS* (*Healthcare Information and Management Systems Society* o Salud de la Información y Sistemas de Gestión de la Sociedad) [69], el uso clínico de la tecnología móvil para recopilar datos se elevó al 67%, por encima del 45% del año pasado, y el 93% de los médicos ya utilizan su *smartphone* personal para acceder al *HCE* (Historial Clínico Electrónico), pero sólo el 57% lo hizo bajo una política móvil formal.

El problema surge cuando médicos y estudiantes de medicina se conectan a redes no seguras o descargan aplicaciones inseguras de fuentes que no son de confianza, lo que hace que el dispositivo sea altamente vulnerable. Aunque la mayoría de los empleados hace un "uso intensivo de las aplicaciones", [66] más de la mitad (un 55%) afirma que su organización no cuenta con una política que defina cómo debería ser su uso en el móvil en el lugar de trabajo, y una gran mayoría de las

compañías (67%) les permiten descargar aplicaciones que no han sido revisadas en sus dispositivos de uso profesional. Asimismo, el 55% de las organizaciones dice que los empleados están autorizados a utilizar y descargar aplicaciones empresariales en los dispositivos personales.

Larry Ponemon, fundador del *Ponemon Institute* dijo que este estudio *"Es sólo un indicador de que tenemos un problema, un riesgo que no se está atendiendo, o al menos no en relación a entrenamiento y concientización"*, y la realidad es que los médicos y estudiantes de medicina no son conscientes de los aspectos de seguridad y privacidad de las aplicaciones móviles que utilizan en su actividad diaria, como muestra otro estudio realizado por Whipple et al. (2012). Dicho estudio concluye que algún tipo de educación en estos temas es necesario porque el conocimiento sobre ellos es muy bajo [70].

Además, en el campo de la salud móvil se necesita trabajar intensamente con el fin de superar las diferencias legales y culturales sobre la privacidad entre las naciones y regiones del mundo. En este campo donde están convergiendo dos tipos de campos -médicos y de telecomunicaciones- los reguladores están luchando para mantenerse al día, ya que hay varios gobiernos y organismos internacionales que se han dado cuenta de que hay un problema que resolver, y se han trasladado a abordar los desafíos de la seguridad personal y la privacidad en la era de los teléfonos inteligentes y aplicaciones móviles [71].

Aunque hay algunos investigadores que hablan acerca de la privacidad y la seguridad en *mHealth* en general [72-74], estos documentos no profundizan en la complejidad y el problema mundial que estos aspectos implican. Además, hay pocas investigaciones respecto a la privacidad y las leyes de seguridad para la salud móvil [75-76], pero muchas sobre las técnicas específicas de privacidad o de seguridad en este campo [77-81].

Por lo tanto, el objetivo de este *TFG* (Trabajo Fin de Grado) es evaluar el estado actual de estas características y hacer una guía a seguir por los diseñadores al crear una aplicación con una/s determinada/s funcionalidad/es, para satisfacer los requisitos necesarios de seguridad. Para ello, en primer lugar, se realiza una revisión de la seguridad, privacidad y las leyes de seguridad y privacidad en *mHealth* en los países desarrollados, centrándose en la Unión Europea y los Estados Unidos con el fin de conocer los aspectos principales para ser tenidos en cuenta por los diseñadores de aplicaciones. En segundo lugar, se desarrolla una revisión acerca de las preocupaciones y los problemas que se encuentran sobre la privacidad y la seguridad en las aplicaciones móviles de salud, para ver las líneas de investigación abiertas. Por último, con el conocimiento obtenido a partir de los apartados anteriores, serán redactadas unas pautas base con respecto a los aspectos de seguridad y privacidad para cada tipo de aplicación de *mHealth*, con el fin de convertirse en un estándar en seguridad básica para la industria de desarrolladores de aplicaciones, capaz de satisfacer los requisitos establecidos por las leyes consideradas.

3.2 Revisión sobre las Leyes de Seguridad y Privacidad

El objetivo final de este *TFG* es establecer una guía básica de seguridad mediante una serie de recomendaciones técnicas de seguridad y privacidad para diseñadores de aplicaciones *mHealth*, realizada a través de los resultados obtenidos del estudio de las leyes específicas que las aplicaciones deben obedecer, así como las técnicas y tecnologías utilizadas para estos aspectos de seguridad y privacidad. Para ello nos apoyamos en la revisión de las leyes de seguridad y privacidad en *mHealth* en la Unión Europea y Estados Unidos, debido a la dificultad de cubrir otros continentes, donde las leyes pueden ser diferentes o más restrictivas como es el caso del continente asiático, siendo necesario separarlas en diferentes estudios.

Otra razón de centrarse sólo en la Unión Europea y los Estados Unidos es por ser probablemente las zonas más representativas de los países occidentales desarrollados y dos mercados que son el objetivo de un importante número de diseñadores de aplicaciones, tal y como muestra la *Figura 3.2* basada en un informe realizado en 2014 por [82] *Vision Mobile* en Londres, donde se estima que hay 2,3 millones, y aumentando, de personas que trabajan en el desarrollado de aplicaciones móviles en todo el mundo. De esta población, Asia es el continente con el mayor número de desarrolladores de aplicaciones, que se calcula en 760.000 personas, o el 32,9 por ciento del total. Europa ocupa el segundo lugar, con aproximadamente 680 mil desarrolladores de aplicaciones (específicamente se ha estimado un número de 330.000 desarrolladores de aplicaciones trabajando en la Unión Europea en concreto) siendo el 29,7 por ciento del total. Norteamérica está en un cercano tercer lugar, también con 680.000 desarrolladores, o lo que es lo mismo, el 29,4% de la población global de desarrolladores.

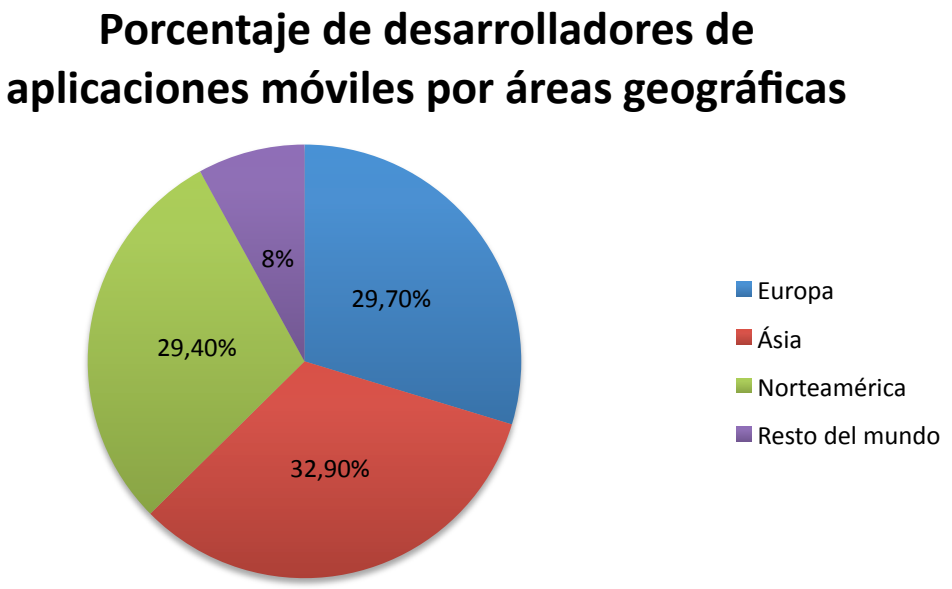


Figura 3.2. Porcentaje de desarrolladores de aplicaciones móviles por áreas geográficas (2014). Fuente: [82]

En el estudio de las leyes de seguridad y privacidad, el director de la Agencia Vasca de Protección de Datos, Iñaki Pariente de la Prada [83], afirma que: *"El paciente es dueño de sus datos. Su consentimiento tiene que regir cualquier actuación con sus datos. No hay otro camino"* y aunque no haya una regulación especial sobre la información de pacientes y usuarios de aplicaciones móviles en el campo de la salud, el paciente es el que tiene que tener la última palabra cuando se utilizan sus datos sanitarios. Y detalla: *"pese a no haber una ley se prevé la obligación a las administraciones y empresas de todo el mundo que hagan tratamiento masivos de datos, de redactar un texto denominado 'evaluación de impacto' que tiene que elaborarse antes de la recogida de datos o tratamientos masivos e información. En dónde se analice si se va a respetar o no la normativa de privacidad y como se va hacer"*.

Para Pariente de la Prada hay que respetar la ley tanto en la recogida, como en el tratamiento y en la cancelación de los datos personales. Aunque no exista una ley específica para datos de salud, si existe [83] "La Ley General de Protección de Datos" del año 1999 (transpone una directiva del 95) y engloba la protección de datos en general y no regula sectorialmente cada campo de actuación. Una ley que se hizo cuando unos pocos estaban familiarizados con Internet y la manipulación de grandes cantidades de datos en el campo de las *TIC* ni existía. El director de la Agencia Vasca de Protección de Datos explica: *"Hay dos principios esenciales en la recogida de datos sanitarios: información y consentimiento. Supuestamente una persona cuando da sus datos a otra tiene que haber sido informada previamente de para que se van a recoger -la finalidad- , cómo se van a utilizar, donde se van a utilizar, en qué ficheros se van a guardar y la seguridad que van a tener. Teóricamente una vez informado de todo esto, la persona consiente o no dar esa información. Específicamente en los datos de salud siempre tiene que existir un consentimiento expreso y por escrito. Y si recojo datos en una página Web gracias a una casilla, el sistema tiene que permitir guardar esa casilla para acreditar que se dio el consentimiento. A efectos de prueba"*. Pariente de Prada remacha: *"Siempre que se recojan datos de salud el esquema es este: información y consentimiento y esto último agravado pues son datos especialmente protegidos"*.

Está claro que cuando un paciente va a un hospital a tratarse existe un consentimiento tácito. Sus datos los puede ver todo el equipo médico pues la finalidad es curativa, paliativa -sanitaria- y existe el secreto profesional. Otro de los casos en que no se pide consentimiento es cando se estudian millones de datos. Si es imposible contactar con los pacientes uno a uno, esa información se puede anonimizar para ser utilizada, por ejemplo, en investigaciones médicas o en la gestión de recursos sanitarios. El problema, señala otro experto en datos [40], Ramón Miralles, es si esa información –en principio segura- nunca va a desvelar la identidad de los pacientes. *"Al igual que las técnicas de anonimización han ido evolucionando, las técnicas para cruzar bases de datos han evolucionado también. Y esos procesos pueden, en ciertas circunstancias, llegar a asociar esa información anonimizada con alguien. La tecnología no para y al cruzar información y utilizar muchas bases de datos perderemos el control de a quien cedemos los datos"*. Pariente de Prada comparte la misma opinión: *"Es un acto de fe. Te dicen que técnicamente hay garantía de que no puede ser 'reanonimizado' pero realmente no sabes, aunque en ese momento sea cierto, si mañana la tecnología va a evolucionar. Pasa a ser un problema técnico"*.

Europa ya ha tomado cartas en el asunto con una ley sobre seguridad y privacidad en *mHealth*: "La Directiva en Protección de Datos de la Unión Europea 95/46/CE" de 1995 [84]. Se trata de un grupo de trabajo que reúne a todas las autoridades de protección de datos de los países miembros y establece los principios sobre los que los estados miembros de la Unión Europea deben aplicar en sus leyes. Ese grupo de expertos, que inicialmente se reunía de forma esporádica, ha cobrado importancia y emite cerca de cuatro dictámenes al año. A principios de 2012, la Unión Europea ha aprobado un proyecto, el "Reglamento General de Protección de Datos Europea" [85], que sustituirá a la directiva anterior en 2016, si tiene éxito. No habrá necesidad de aplicar esta normativa en las leyes de los Estados miembros, ya que se aplicará en general, sobre todos ellos. Con esta nueva regulación, todos los Estados miembros estarán en el mismo escenario de la seguridad y protección de datos. El de abril de 2014 [83] fue sobre *"técnicas de anonimización"* y estableció los criterios técnicos para anonimizar los datos. *"Es un dictamen que marca las pautas que hay que seguir. De alguna forma es como si actualizase la ley. Trata cosas que la norma no contempló cuando nació y que hay que ir interpretando. La ley no cambia pero con estos dictámenes se actualiza, son muy importantes"*, explica el experto vasco Iñaki Pariente de la Prada.

Uno de los puntos de mira de este grupo de expertos europeos son las empresas de tecnología que, con sus *wearables*, controlan hasta el último latido de un paciente sano y que también están detrás de los dispositivos de control que se instalan en las viviendas de pacientes crónicos. Como señala el director de la Agencia Vasca [83]: *"Los sanos que se ponen pulseras con aplicaciones en el móvil están registrando millones de datos de salud que una empresa está guardando. Hoy por hoy con una finalidad indeterminada pues todavía no tienen claro para qué los van utilizar. Son empresas que están en Estados Unidos, que no están sujetas al derecho español, y por ello si tengo un problema no voy a poder acudir a que me tutelen o ayuden las instituciones estatales. También hay cada vez más modelos mixtos: médicos de la sanidad pública que pueden acceder a perfiles que se está generando en la empresa privada"*. La gran incógnita es como gestionar toda esa información y cuál es su utilidad final, y para ello César Rubio, coordinador del sector de *eHealth* de la Federación Española de Empresas de Tecnología Sanitaria *(Fenin)* señala que esos datos *"sirven para obtener información y transformarla en valor. Y se supone que su uso va ser bueno"*.

Ramón Miralles también refleja la misma idea y explica que los pacientes ceden en algún momento sus datos porque confían en la sanidad y que, aunque puedan ser utilizados por terceras personas, *"hay que poner en una balanza si ese riesgo compensa"*. *"Los datos pueden pasar de ser seguros a inseguros y escapar de nuestro control. El riesgo está presente pero también es verdad que esa información que se cede puede ser vital en la investigación médica. Hay que hacer un equilibrio entre el riesgo que representa y los beneficios que nos puede aportar ceder nuestros datos, nadie puede decir que estos datos seguirán siendo anónimos dentro de cinco años"*.

Aparte de la anonimización, en los mecanismos para salvaguardar la privacidad del paciente *"se aplica una lógica que ya existía y que ya estaba en la ley de historia clínica –en la ley 41/2002- y que dice que el paciente es dueño de sus datos, señala Pariente de la Prada. La historia clínica es del paciente. Puede pedir, puede ver, y*

eso se ha plasmado en la generalización de las tarjetas sanitarias con las que puede consultar parte de la historia clínica y la puede gestionar. Los datos son cada vez más del paciente. Y por ello si se utilizan con otra finalidad que no se la curativa, sólo se puede conseguir con consentimiento. O tirar por la anonimización. No hay un camino intermedio", concluye.

La última decisión europea en octubre de 2015 lanza un rotundo mensaje a Estados Unidos en materia de protección de datos, donde se ofrecen varias leyes relativas a la privacidad y la seguridad en *mHealth*. La principal ley que se aplica a cuestiones *mHealth* es la "Ley de Transferencia y Responsabilidad de Seguro Médico" *(HIPAA)* de 1996 [86]. Esta ley protege la privacidad de la información de salud digital. Otra ley importante es la sección 5 del Acta de la Comisión Federal de Comercio *(FTC)* [87]. Recientemente, esta ley recoge aspectos de privacidad *mHealth* en el informe *Mobile Privacy Disclosures: Building Trust Through Transparency* [88]. Hay otra ley significativa que sólo se aplica a los niños menores de 13 años, la "Ley de Protección de la Privacidad Infantil en Línea" *(COPPA)* de 1998 [89], que prohíbe la recolección de información personal de estos niños sin el consentimiento expreso de sus padres o un tutor legal. Una sentencia del Tribunal de Justicia de la Unión Europea [83] sobre la que no cabe recurso señala que cualquier estado miembro podrá a partir de ahora bloquear el envío de datos personales a los Estados Unidos. El fallo habilita las agencias nacionales de protección para que frenen las transferencias de datos de ciudadanos europeos a terceros países (incluido los Estados Unidos) si consideran que la empresa o el país no es de fiar. Con este dictamen, el criterio de las agencias prevalecerá sobre el de la Comisión Europea y, por ello, las empresas americanas con sede en Europa tendrán que legitimar la transferencia de datos hacia los Estados Unidos recabando la voluntad inequívoca del usuario que debe ser informado y consentirlo.

A continuación se recoge un resumen, extraído del artículo [90] titulado "*Privacy and Security in Mobile Health Apps: A Review and Recommendations",* de los puntos más restrictivos de las leyes mencionadas, ordenados por los diferentes requisitos en base a un estudio realizado por Thompson Reuters [91]. Esto es, cuando una ley es más restrictiva que las otras con respecto a un requisito específico, se muestra la información de esta ley en dicho resumen. Si las leyes son muy similares con respecto a un requisito, entonces el resumen muestra los aspectos comunes extraídos de ellos.

- **Encubrimiento de Datos:** Los datos que deben ser encubiertos son respecto a la información que se puede utilizar para identificar a una persona. Incluye números de identificación, físicos, fisiológicos, factores mentales, económicos, genéticos, sociales, médicos y culturales respecto el pasado, presente o futuro del paciente.
- **Requisitos de Información:** Antes de proporcionar su información de salud personal *(PHI)*, los usuarios deben ser informados de la identidad de la persona o entidad que utilizará la información de salud personal *(PHI)*, los efectos de la recolección, las prácticas de privacidad de la entidad, si la disposición de la información es obligatoria o voluntaria, los derechos que tienes sobre acceder o modificar los datos y método de contacto para obtener más información o

quejas. Esta información se debe dar directamente a un padre o tutor legal en caso de los niños sean menores de 13 años.

- **Requisitos de Consentimiento:** El usuario o el consentimiento del paciente para la recogida de datos deben ser obtenidos por la entidad, cuando está recogida no pueda ser justificada por un motivo legal. La entidad se ha mejorado para obtener este consentimiento por escrito. En el caso de los niños menores de 13 años, no pueden consentir su obtención de datos, siendo sus padres o tutores legales los que lo autoricen.
- **Retención de Datos:** En general, la información personal de salud debe mantenerse sólo el tiempo necesario para los fines que se obtuvieron y debe ser borrado una vez alcanzado el objetivo. Las entidades también deben incluir una política de retención de datos clara como parte de sus procedimientos de seguridad.
- **Seguridad:** Las entidades están obligadas a implementar y mantener las medidas de seguridad técnicas, administrativas, físicas y organizativas adecuadas para proteger la información personal de salud de la posible pérdida accidental o ilícita y el acceso no autorizado o divulgación de información. Dado que los datos de salud son muy sensibles, la seguridad debe ser mayor.
- **Incumplir Notificaciones Obligatorias:** En caso de una violación de los datos personales, las entidades deberán notificar a la autoridad competente, así como al usuario cuyos datos se han visto comprometidos y sin demora injustificada, sobre todo cuando la infracción puede haber afectado negativamente al usuario. En casos de violaciones masivas, los medios de comunicación deben ser también notificados.
- **Transferencias de Datos:** Las entidades necesitan el consentimiento de los usuarios para transferir sus datos personales a otra entidad o de un tercero, incluso cuando es necesaria esta transferencia para completar uno de los propósitos de la recogida de datos, a menos que la transferencia esté permitida por la ley.

3.3 El desafío de la Seguridad y Privacidad en Aplicaciones de Salud

La privacidad es un aspecto que se puede ver comprometido derivado de la seguridad ya que se pone en riesgo la información protegida de la salud de los consumidores. Los datos confidenciales recogidos por aplicaciones móviles de salud pueden ser accesibles por los pacientes, médicos, familiares o investigadores científicos, pero también pueden ser compartidos con terceros, como anunciantes [92], poniendo la confidencialidad de la información de los consumidores en entredicho.

Dado el creciente uso de Registros Electrónicos de Salud (*HCE* o en inglés *EHR*) y cuidado de la salud electrónica *(eHealth)*, la confidencialidad, integridad y disponibilidad de los datos de consumo son los principales problemas de hoy en día para los proveedores de servicios de salud en términos de seguridad y privacidad de los datos [93].

Según Luciano Saez Ayerra [83], Presidente de la Sociedad Española de Informática de la Salud, *"Lo más importante es tomar conciencia de que el tratamiento masivo de datos de salud, además de entrañar grandes beneficios para la investigación y la asistencia y gestión sanitaria, supone una serie de riesgos para la privacidad y la intimidad de los pacientes"*, por ello es importante que los datos sean seguros, evitando riesgos que puedan afectar a la privacidad de las personas y al uso malicioso que se podría hacer de estos datos. Esto plantea un reto tecnológico, ya que supone redefinir la arquitectura de las redes de comunicación, las infraestructuras tecnológicas, todo ello no solo para garantizar los servicios actuales y en implantación, sino por lo que pueda venir en un futuro inmediato.

Este apartado pretende presentar una serie de temas de seguridad y privacidad en aplicaciones móviles de salud como son: el desafío de la seguridad y la privacidad, datos de consumo mal protegidos, las brechas de seguridad de datos, la falta de normas y directrices en aplicaciones y el almacenamiento en la nube, que pretenden introducir al lector al Proyecto Abierto de Seguridad de Aplicaciones Web *(WOASP)* [94] que aglutina en una lista los diez fallos de seguridad más comúnmente explotados en aplicaciones móviles y que pretende crear conciencia acerca de la seguridad, identificando dichos riesgos, para así poder hacerles frente en el siguiente bloque de este *TFG* (Trabajo Fin de Grado).

La seguridad de los datos y la privacidad son las principales preocupaciones para los registros personales de salud de acuerdo con Kharrazi, Chisholm, VanNasdale y Thompson [95]. La falta de temas de normalización y de seguridad involucrados en aplicaciones de *mHealth* es una gran barrera para su uso generalizado. En particular, los autores se centraron en la limitación de la seguridad de la información en un dispositivo móvil. Los consumidores pueden perder sus dispositivos o no pueden utilizar cualquier autenticación de seguridad para proteger los datos. Por tanto, es responsabilidad del consumidor, para asegurar su propia información, usar contraseñas en el dispositivo y las contraseñas dentro de las aplicaciones para proteger su información privada. Los autores también hicieron hincapié en que para reducir los riesgos de seguridad de aplicaciones de salud, se requiere un proceso de verificación a fondo por parte de las tiendas de aplicaciones para poder detectar *malware* en aplicaciones.

Kane [92] declaró que algunas aplicaciones de salud hacen uso de Internet conectando de forma inalámbrica sensores como por ejemplo *wearables* o integrados dentro del propio *smartphone* que hacen un seguimiento o miden el estado de salud de un paciente o de las actividades de un consumidor. El seguimiento de la salud del paciente puede ocurrir en tiempo real, con o sin la participación del paciente o la aprobación en cada instante. El autor se centró en los datos recogidos por las aplicaciones de salud que acceden al paciente y al mismo tiempo comparten datos con otros. Los datos recogidos por tales aplicaciones de salud no sólo contienen información detallada acerca de la salud de una persona, sino también sobre sus hábitos, la ubicación y movimientos, que

posiblemente pone información sensible de la persona en riesgo, si dicha información se da a conocer.

McCarthy [96] puso de relieve una de las principales preocupaciones en relación con los datos del consumidor, que generalmente están mal protegidos en aplicaciones de salud. En un estudio de 43 aplicaciones de salud y *fitness*, sólo el 74% de las aplicaciones gratuitas y el 60% de las aplicaciones de pago tenían una política de privacidad, disponible ya sea en la aplicación o en el sitio *Web* del desarrollador. Sin embargo, sólo el 25% de las aplicaciones gratuitas y el 48% de las aplicaciones de pago informan a los consumidores sobre la política de privacidad. Por otra parte, ninguna de las aplicaciones gratuitas y sólo unas pocas de las aplicaciones de pago encriptan los datos de los consumidores que introdujeron al usar la aplicación. La encriptación o cifrado es la conversión de los datos en una forma que no puede ser fácilmente entendida por personas no autorizadas. Por lo tanto, las aplicaciones de salud que no encriptan la información de los consumidores pueden suponer una amenaza para la privacidad de los datos.

Nasiri [97] también informó de los riesgos sobre la privacidad de los datos en aplicaciones de salud. Encontró muchos consumidores que usan aplicaciones de salud para interactuar con sus proveedores de atención médica, así como realizar un seguimiento para gestionar los síntomas y otra información. Nasiri encontró que la información compartida con otros puede llevar a riesgos de privacidad. Nasiri informó que los investigadores, llevaron a cabo una encuesta sobre 20 de las 23 aplicaciones de salud gratuitas más populares y encontraron que el 50% de ellas envía datos a anunciantes de terceros y el 39% envía datos a partes no identificadas y sin ningún tipo de encriptación. Afirmó que las aplicaciones de pago son un poco más seguras en comparación con aplicaciones de salud gratis. Muchas aplicaciones de salud gratuitas para teléfonos móviles envían datos, conectándose a sitios de terceros, utilizan conexiones sin cifrar, permiten la recopilación de datos por parte de terceros así como almacenan datos externamente y la mayoría de las veces esto sucedió sin ser notificado a los usuarios.

Las brechas de seguridad de datos en la asistencia sanitaria se han vuelto comunes según Figg y Kam [98], con muchos proveedores de *mHealth* en línea, incluidos los médicos y los investigadores científicos, capaces de ver los historiales clínicos de los pacientes sin el conocimiento de los pacientes. Los autores también señalaron que las violaciones de la seguridad de datos en la asistencia sanitaria son una amenaza a la privacidad que pueden conducir al robo de identidad médica. El Foro Mundial de Privacidad [99] describe el robo de identidad médica como un suceso en el que una persona utiliza la identidad de otra persona, como el nombre de una persona o el número de *Medicare* (cobertura de seguridad social administrado por el gobierno de Estados Unidos), sin el conocimiento y consentimiento de la persona, lo que afectaría la seguridad de muchos consumidores [99]. De acuerdo con la *FTC* (Comisión Federal de Comercio) había cerca de 18.000 casos de robo de identidad médica entre 2005 y 2011, dando lugar a ciertos beneficios por parte del delincuente. El

delincuente puede robar registros y venderlos en el mercado negro, o pueden alterar los registros de los pacientes por pura diversión como por ejemplo, añadir entradas falsas en relación con el diagnóstico, el tipo de sangre, alergias a medicamentos y otra información de salud. Las víctimas que tienen sus expedientes médicos alterados por los delincuentes pueden recibir un tratamiento médico falso que puedan provocar consecuencias desastrosas para su salud, dando lugar a posibles muertes.

Los problemas de seguridad en aplicaciones móviles de salud están aumentando debido a la falta de directrices o un estándar en el desarrollo de aplicaciones [95]. Una ocurrencia común, tales como la pérdida o robo de un dispositivo móvil con los datos de una persona sin encriptar, incluyendo números de tarjetas de crédito, podría dar lugar a un fallo de seguridad con consecuencias de gran alcance. El fraude y el robo de identidad causados por roturas de seguridad también podría conducir a la desconfianza entre los consumidores y los proveedores de salud. Sin embargo, un entorno seguro de *mHealth* que genere confianza entre los consumidores y los proveedores de servicios de salud tendría que adoptar una norma o estándar para aumentar la seguridad y proteger de cualquier ataque no autorizado [100].

Sin embargo, el almacenamiento en la nube de información trae un conjunto de nuevos retos, sobre todo cuando se trata de la disponibilidad de los servicios, la seguridad y privacidad de los consumidores [101]. Los problemas de seguridad son críticos cuando un proveedor de atención médica tiene previsto desplegar un sistema de gestión de *HCEs* basado en la nube, porque mover los datos del paciente a la nube significa que los archivos de los pacientes acabarán alojados en los servidores del proveedor de servicio [102]. De acuerdo con Zhang y Liu [103], al mover los datos del paciente a la nube, los proveedores de salud están exponiendo información a varias amenazas externas, porque los datos están disponibles a través de Internet. Tanto los proveedores de servicios en la nube y proveedores de salud deben entender las consecuencias en relación con los riesgos para la privacidad de los datos sensibles de los consumidores: el profesional de la salud debe garantizar la seguridad de los datos del paciente, asegurando que la plataforma en la nube cuenta con los mecanismos de seguridad necesarios [104] y es responsabilidad del proveedor de la nube proteger la seguridad y privacidad de la información al proporcionar la seguridad necesaria para evitar ataques externos para robar o incluso borrar la información. La falta de privacidad de datos de los usuarios y la falta de regulación y directrices para el desarrollo de aplicaciones de *mHealth* deben tenerse en cuenta para la mejora de las aplicaciones de *mHealth*.

Todo esto provoca que los cibercriminales generen constantemente ataques que buscan explotar tanto la inexperiencia y credulidad de los usuarios como los fallos de seguridad del propio sistema y aplicaciones. Entendiendo que las vulnerabilidades y fallos de seguridad propios de las plataformas escapan al control de los desarrolladores de aplicaciones para dispositivos móviles, hay otros aspectos, como es el caso de la seguridad de las propias aplicaciones que éstos desarrollan, cuya responsabilidad sí que recae sobre ellos. Existen diferentes metodologías cuya máxima es el *"security by*

design" y que permiten evaluar la seguridad de las aplicaciones, como es el caso de *OWASP* [94], que tiene como objetivo identificar los peligros correspondientes a la seguridad de dispositivos móviles y proporcionar los controles necesarios en el desarrollo para reducir su impacto y la probabilidad de explotación de los mismos. Estas metodologías, son independientes de la plataforma para la que se desarrolla la aplicación y es igualmente recomendable seguir las pautas y tener en cuenta los controles que indican a la hora de desarrollar para cualquier otra plataforma y más si cabe, si se está desarrollando alguna aplicación que maneje información sensible como son datos de salud.

A continuación, se pueden ver en la *Figura 3.3*. los aspectos más relevantes de *"OWASP Mobile Security Project"* de 2014 al ser la que tiene un uso más extendido. *OWASP* [94], referenciado por muchos estándares, libros, herramientas, y organizaciones, incluyendo *MITRE*, *PCI DSS (Payment Card Industry Data Security Standard), DISA (Defense Information Systems Agency)*, *FCT (Federal Trade Commission)*, y muchos más, identifica los siguientes riesgos en el desarrollo de *apps* móviles:

Figura 3.3. Los Diez Riesgos de Seguridad en Aplicaciones Móviles más importantes. Fuente: [94]

1. **Controles Débiles en el Servidor:** Corresponde a las inyecciones de código malicioso en un servidor para poder explotarlos. Las fallas de inyección, tales como *SQL (Structured Query Language)* y *LDAP (Lightweight Directory Access Protocol),* ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder a datos no autorizados.
2. **Almacenamiento Inseguro de Datos:** Se trata mayormente de dispositivos móviles perdidos y/o robados, aunque también está la posibilidad de acceder a dichos dispositivos sin la necesidad de tenerlos físicamente a través de *exploits in-the wild* y/o distintos códigos maliciosos, así como el uso de cualquier *jailbreak* o *rooting* ya que eluden cualquier cifrado de la información. Algunos ejemplos de información robada puede ser nombres de usuario, *tokens* de autenticación, contraseñas, *cookies*, datos de localización, *UDID (Unique Device Identifier)/IMEI (International*

Mobile Station Equipment Identity), nombre del dispositivo, datos personales: fecha de nacimiento, dirección, razón social, tarjeta de crédito, datos de la aplicación, registros de la aplicación almacenados, información de depuración, mensajes de la aplicación en caché, historial de transacciones, etc.

3. **Protección Insuficiente en la Capa de Transporte:** Cuando se desarrolla una aplicación normalmente los datos son intercambiados entre un cliente y un servidor. Las aplicaciones móviles con frecuencia no protegen el tráfico de red. Pueden utilizar *SSL (Secure Sockets Layer)/TLS(Transport Layer Security)* durante la autenticación, pero si la codificación es débil existen diversas técnicas para visualizar datos sensibles mientras viajan entre el cliente y el servidor como por ejemplo el monitoreo del tráfico de una red *wifi* de un establecimiento público como es una cafetería o un aeropuerto. También se expone a sufrir ataques *MITM (Man-In-The-Middle)* y de *phising*.
4. **Fuga de Datos no Deseada:** Las aplicaciones móviles tienen que interactuar con sistemas operativos, infraestructuras digitales, *hardware* nuevos, etc. que no son propiedad de los desarrolladores, por lo que no pueden controlar cambios y/o fallas que estén fuera de sus aplicaciones. En este sentido, es posible que se pierdan datos si no se realizan evaluaciones para entender cómo las aplicaciones interactúan con todos los elementos de los dispositivos.
5. **Autorización y Autenticación Pobres o Débiles:** Existen patrones de autenticación considerados inseguros y que deben ser evitados. A diferencia de las aplicaciones *Web* tradicionales, las aplicaciones móviles no esperan a que el usuario este en todo momento en línea para autenticarse mediante un servidor *backend*, sino que lo hacen de modo *off-line* pudiendo sufrir ataques binarios eludiendo a la aplicación de la autenticación en línea. Las funciones de la aplicación relacionadas con la autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, *tokens* de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios. Algunos ejemplos son: *"*Recuérdame*"* (cuando existe la opción de que la aplicación guarde la contraseña de forma automática), la falta de *tokens* de seguridad, etc.
6. **Criptografía Rota/ Errores de Cifrado:** En algunas ocasiones, los métodos de encriptación de datos se vuelve una práctica casi obsoleta. Crear y utilizar tu propio algoritmo de encriptación y utilizar algoritmos desfasados son ejemplos de malas prácticas. Hay dos maneras fundamentales de que los errores de cifrado se manifiesten dentro de las aplicaciones móviles. En primer lugar, la aplicación móvil puede utilizar un proceso de encriptación o desencriptación en segundo plano erróneo a través del sistema operativo y puede ser aprovechado por el ciberdelincuente para descifrar los datos con herramientas como *ClutchMod* o *GBD*. En segundo lugar, la aplicación móvil puede aplicar o aprovechar un algoritmo de cifrado/descifrado que es débil por naturaleza y pueden ser descifrados directamente por el ciberdelincuente con herramientas como *IDA pro* o *Hopper*. Muchos algoritmos y protocolos criptográficos no deben utilizarse porque se ha

demostrado que tienen debilidades significativas o que son insuficientes para las necesidades de seguridad modernos. Éstas incluyen: *RC2, MD4, MD5, SHA1*.

7. **Inyección del Lado del Cliente:** Siempre y cuando exista la posibilidad de que usuarios externos, internos y la aplicación misma puedan enviar datos no confiables al sistema, un atacante podría inyectar *exploits* sencillos (basados en texto) como *SQL Injection* a las aplicaciones móviles, lo que causa un potencial riesgo de robo de información.
8. **Acciones de Seguridad Vía Entradas Inseguras:** Para entender mejor este caso, tenemos que entender el concepto de *IPC (Inter-Process Communication* o Comunicación entre Procesos*)*. Los procesos entre aplicaciones y sistemas operativos comparten espacios de memoria para permitir la comunicación y sincronización entre los mismos. Para minimizar los riesgos de ataque, la aplicación móvil debería permitir solamente comunicación con otras aplicaciones confiables, las acciones sensibles deberían requerir la interacción del usuario, la información sensible no debería ser enviada a través de *IPC*, etc.
9. **Manejo de Sesión Incorrecto:** El manejo incorrecto de la información es muy similar a la autenticación débil del **punto 5**. Las aplicaciones móviles utilizan *tokens* de sesión para mantener el estado de la sesión a través de protocolos como *HTTP (Hypertext Transfer Protocol)* o *SOAP (Simple Object Access Protocol)*. Para ello, la aplicación móvil debe primero autenticar al usuario a través del *backend*. En respuesta a la autenticación exitosa, el servidor emite una *cookie* de sesión para la aplicación móvil. La aplicación móvil añade esta *cookie* a todas las transacciones futuras de servicios entre la aplicación móvil y el servidor. Esto permite al servidor cumplir convenientemente la autenticación y autorización de las solicitudes de servicio emitidas por la aplicación móvil. El manejo de sesión incorrecto se produce cuando el *token* de sesión se comparte involuntariamente con el ciberdelincuente durante una transacción posterior entre la aplicación móvil y los servidores *backend*. Por esta razón, es tan importante manejar bien la sesión una vez abierta. Si no se aplican sencillos cuidados pero importantes que veremos en el siguiente capitulo, puede que terceros no autorizados con acceso al tráfico *HTTP/S* de la aplicación o a datos de *cookies*, intercepten información de otros usuarios.
10. **Falta de Protección a Nivel Binario:** La falta de protección a nivel binario facilita el ataque a través de ingeniería inversa. Si un programador no es creador del código de su programa a nivel binario y no lo tiene protegido, un atacante puede fácilmente buscar fallos en el código, copiarlo, hacer cambios menores y revender una aplicación móvil nueva como si fuese suya.

CAPÍTULO 4

SOLUCIÓN & RESULTADO

CAPÍTULO 4. SOLUCIÓN Y RESULTADO

4.1 Elementos de Seguridad a Implementar

Después de la revisión llevada a cabo hasta ahora, podemos establecer algunas medidas que deben cumplir los desarrolladores de aplicaciones con el fin de garantizar la seguridad y privacidad de la información personal de los usuarios, complementando las normas existentes en materia de seguridad y privacidad, tales como *ISO/IEC 27001/2013* sobre la gestión de seguridad de la información [107], redactada por los mejores especialistas del mundo en el tema y proporcionando una metodología para implementar la gestión de la seguridad de la información en una empresa.

Apoyándonos en el *"OWASP Mobile Security Project"* [94] de 2014, el artículo "*Privacy and Security in Mobile Health Apps: A Review and Recommendations"* [90] y la iniciativa lanzada recientemente por la *OCR* (Oficina de Derechos Civiles) [105], tal y como se muestra en la *Figura 4.1*, vamos a identificar diez bloques esenciales que agrupan la totalidad de las pautas a tener en cuenta para que la información sea segura al usar dispositivos móviles como *smartphones*, ya que la *OCR* informó que cada año se producen un número significativo de violaciones de datos privados fruto de móviles perdidos o robados.

Figura 4.1. Diez bloques de seguridad para aplicaciones móviles de salud. Fuente: Propia

1. **Control de Acceso.** El control de acceso a la información médica protegida debe estar centrada en el paciente. También hay que entender cómo las aplicaciones interactúan con todos los elementos de los dispositivos.
   - Los dispositivos móviles pueden ser configurados para requerir contraseñas, números de identificación personal *(PIN)*, códigos de acceso, o patrones para tener acceso al terminal móvil.

- La contraseña utilizada debe ser compleja y robusta, con al menos siete caracteres fruto de la combinación de letras y números, incluyendo una letra mayúscula y un carácter especial.
- La contraseña, *PIN* o código de acceso se pueden enmascarar para evitar que la gente lo visualice.
- Se recomienda el uso de técnicas como *Pin Scramble* que cambie el orden del patrón de acceso a la aplicación.
- Comprobar la entropía de las contraseñas.
- Los usuarios deben ser capaces de permitir o prohibir el acceso a su información en cualquier momento, cambiando los permisos que tiene la aplicación sobre los recursos e información a la que necesita acceder para funcionar correctamente y así evitar la fuga de datos no deseada.
- Crear un acceso basado en administradores, dando posibilidades de lectura para algunos y gestionar las limitaciones de otros.
- Recomendar el uso de un cortafuegos *(firewall)* ya que puede proteger contra las conexiones no autorizadas mediante la interceptación de los intentos de conexión entrantes y salientes y bloquear o permitir la conexión basándose en un conjunto de reglas predeterminadas.
- Es importante que la aplicación no almacene *cookies*, ocultar el *buffer* donde se almacena el contenido que se copia y se pega, no permita el uso de la aplicación en segundo plano, evité el envío de datos analíticos de uso a terceros, etc.

2. **Mantenimiento de la Seguridad en el Servidor**. El programador *backend* es aquel que se encuentra del lado del servidor encargándose de interactuar con bases de datos y verificar manejos de sesiones de usuarios, es decir, de la manipulación de los datos que generé la aplicación móvil de salud, por eso debe protegerse de todo tipo de inyecciones que se puedan hacer al servidor para que no sea vulnerable.
   - Se debe analizar periódicamente el *backend* en busca de vulnerabilidades.
   - Mantener el servidor completamente actualizado.
   - Establecer los mecanismos necesarios para que en el caso de que el servidor se vea afectado por un incidente, se pueda llevar a cabo un análisis forense.
   - Utilizar medidas para prevenir ataques de denegación de servicio *(DoS)*.
   - Asegurarse de que el servidor rechaza todas las peticiones no cifradas.
   - Durante la tramitación de la solicitud de servicio de la aplicación al servidor, el código del servidor debe comprobar que la solicitud entrante está asociada a un usuario conocido.
   - El código de fondo que procesa la solicitud de servicio de la aplicación móvil al servidor tiene que verificar que la identidad asociada con la petición tiene derecho a ejecutar el servicio. Por lo tanto, los ciberdelincuentes no serian capaces de realizar acciones remotas contra el servidor utilizando cuentas de usuario con privilegios bajos.

3. **Autorización, Autenticación y Manejo de Sesiones**. Este es un conjunto de controles que se utilizan para verificar la identidad de un usuario, u otra entidad, la interacción con el software, y también para asegurar que las aplicaciones manejan la gestión de las contraseñas de una manera segura.
    - La aplicación no debería usar un *PIN*, pero en los casos en que la aplicación móvil requiera que un usuario cree una contraseña o necesite introducir un *PIN*, exija una contraseña que cumpla con una política de contraseñas seguras. Ver punto de **Control de Acceso**.
    - No se deben usar patrones de seguridad *(Pin Scramble)* en sustitución de contraseñas, que no sean tanto o más seguros que éstas y que sean fácilmente vulnerables mediante *Smudge Attack* (detección de las manchas aceitosas dejadas por los dedos del usuario durante el uso del dispositivo a través de sencillas cámaras y software de procesamiento de imágenes).
    - En escenarios donde se necesita el acceso sin conexión a los datos mediante contraseña, llevar a cabo un bloqueo/borrado de cuentas/aplicación y/o datos de la aplicación después de 10 intentos no válidos.
    - Integrar una solución *CAPTCHA* cuando se quiera mejorar la funcionalidad/seguridad de la aplicación, sin restar en la experiencia del usuario (por ejemplo, durante registro de nuevos usuarios, publicación de comentarios de usuarios, encuestas en línea, contactar con los desarrolladores, etc.).
    - La autenticación se debe hacer con un identificador único y una contraseña que sólo conozca el usuario. Este *ID* se puede vincular a una *PKI* (Infraestructura de Clave Pública), el sistema preferible *RSA* (*Rivest, Shamir y Adleman*) y/o una clave simétrica utilizada para la encriptación.
    - Medir el riesgo mediante la correlación de los factores tales como la dirección *IP* en el que resultaría muy sospechoso el acceso a la misma cuenta desde dos lugares que están muy separados durante un corto período de tiempo.
    - Establecer controles de seguridad adicionales a la hora de acceder a información sensible empleando la autenticación de múltiples factores para complementar el *ID* más contraseña de identificación cuando sea posible: el uso de un elemento que el usuario posee *(smart key)* o una característica biométrica, como la huella digital.
    - Se recomienda usar la autenticación en dos pasos médiate *TOTP (Time-based One Time Password).*
    - Si es posible utilizar *tokens*, como *OAuth*, en vez de contraseñas y hacer que éstos expiren.
    - Deben implementar herramientas que detecten cualquier cambio del código no autorizado, como puedan ser los ataques binarios.
    - Para manejar sesiones correctamente, hay que asegurarse de que el código de la aplicación móvil crea, mantiene y destruye *tokens* de sesión correctamente sobre el ciclo de vida de la sesión de la aplicación móvil de un usuario.

- Todos los eventos de la invalidación de la sesión se tienen que ejecutar en el servidor y no sólo en la aplicación móvil.
- El tiempo de espera de la sesión será de 15 minutos para aplicaciones de alta seguridad, 30 minutos para aplicaciones de seguridad media y 1 hora para aplicaciones de baja seguridad, con el fin de evitar el riesgo de robo de sesión.
- Obligar al usuario a autenticarse utilizando un estándar *Web* o *API* de inicio de sesión a través de *HTTPS* así como garantizar los tiempos de espera de la sesión.
- Es fundamental que las sesiones se destruyen en el lado del servidor y que las *cookies* de sesiones anteriores no sean aceptadas. Idealmente, la aplicación podría notificar el uso de dichas *cookies* para inicios de sesión no voluntarios.
- Los *tokens* deben ser lo suficientemente largos, complejos y pseudoaleatorios de manera que sean resistentes a los ataques de anticipación y adivinación.

4. **Uso de Librerías y Código de Terceros.** Se trata de un conjunto de prácticas para asegurar que la aplicación se integra con seguridad en el código producido a partir de terceros.
   - Verificar la seguridad/autenticidad de cualquier código/librerías de terceros utilizadas en tu aplicación móvil (por ejemplo, asegurándose de que provienen de una fuente fiable, seguirá teniendo soporte técnico, no contiene puertas traseras).
   - Realizar un seguimiento de todos los *Frameworks/API* de terceros utilizados en la aplicación móvil reciben actualizaciones para los parches de seguridad a medida que se liberan.
   - Prestar especial atención en validar todas las entradas y salidas de datos a aplicaciones de terceros que no son de confianza (por ejemplo, software de publicidad móvil) antes de incorporar su uso en una aplicación.

5. **Integridad de Datos y Ofuscación de Código.** Así como puede ser posible leer información sensible, también es posible realizar cambios o incluso borrar esta información, suplantar identidad y alterar datos existentes inyectando *exploits* sencillos (basados en texto) como *SQL Injection* a las aplicaciones móviles. Por otro lado, la ofuscación trata de un conjunto de controles que se utilizan para prevenir la ingeniería inversa del código, lo que aumenta el nivel de habilidad y el tiempo necesario para atacar a la aplicación.
   - Evitar la Inyección *SQL*, el desbordamiento de *buffer* permitiendo la ejecución de código malicioso mediante *Cross-Application Scripting Attacks* y las modificaciones *HTML* locales a través de *malware* u otras aplicaciones resultado de la ejecución de código *JavaScript* malicioso en la capa de presentación de la aplicación, también conocido como *Cross-Site Script Attacks.*
   - Manejar de forma segura las credenciales del usuario, instalando y habilitando el cifrado en dispositivos móviles que hace inutilizable, ilegibles, e indescifrables la información a personas no autorizadas, preservando la integridad de los datos.

- Utilizar *Advanced Encryption Standard* (*AES*) para cifrar los *PHI*. La clave criptográfica utilizada debe tener al menos 128 *bits* (mejor de 192 o 256 *bits*). Este método ofrece mejores tiempos de cifrado que otras técnicas [106].
- Revisar cuidadosamente cualquier código de error en la ejecución utilizando analizadores estáticos de código y "*fuzzers*" para buscar fallos de seguridad.
- En los casos en que los requisitos de seguridad son muy altos alrededor de cifrado, el desarrollador debe considerar seriamente el uso de la criptografía *whitebox*.
- Muchos algoritmos y protocolos criptográficos no deben utilizarse porque han demostrado tener debilidades significativas o que son insuficientes para las necesidades de seguridad modernos. Éstos son: *RC2, MD4, MD5, SHA1*.
- Se debe utilizar un código de autenticación basada en clave simétrica, por ejemplo *AES (Advanced Encryption Standard).*
- Se prefiere una firma digital pública basada en claves. En ningún caso, los métodos de marca de agua se deben utilizar con imágenes médicas, ya que pueden deteriorar su calidad e incluso provocar el mal diagnóstico.
- El desarrollador de la aplicación debe prevenir adecuadamente que un ciberdelincuente analice y haga ingeniería inversa de la aplicación utilizando técnicas de análisis estático o dinámico. Se recomienda "ofuscar" el código para que sea inteligible y ocultar así su funcionalidad.
- La aplicación debe ser capaz de reaccionar adecuadamente en tiempo de ejecución a una violación de integridad del código.
- Para las aplicaciones que contienen datos sensibles, aplicar técnicas antidepuración.
- Asegurarse de que el registro está deshabilitado puesto que los registros pueden ser interrogados por otras aplicaciones con permisos de lectura de registros.

6. **Informar a los Pacientes.** Según una iniciativa de la Red Global de Vigilancia de la Privacidad *(Global Privacy Enforcement Network)* [108] se debe incluir enlaces a las políticas de privacidad, antes de realizar la respectiva descarga de la aplicación. Otras pautas son:
   - Antes de la recolección y uso de la *PHI*, la aplicación debe presentar una política de privacidad informando a los pacientes sobre la identidad de la entidad que va a utilizar los datos, la finalidad de la recogida de datos, los métodos de privacidad utilizados, los derechos que tienen y un método de contacto.
   - Si los usuarios aceptan esta política dan su consentimiento a la recopilación de datos. Debe incluir una sección para menores de edad, que requiere la aprobación de un tutor legal.
   - La política debe ser fácil de entender, concisa y clara, ya que a los usuarios no les gusta leer documentos legales en una aplicación.
   - Se recomienda dejar la política accesible en un apartado de la aplicación para que el usuario en cualquier momento pueda revisarla.

7. **Comunicaciones Seguras.** El intercambio de archivos está diseñado para permitir a los usuarios conectarse a Internet y compartir archivos. El uso compartido de archivos podría proporcionar permiso de acceso de un dispositivo móvil a los usuarios no autorizados sin el conocimiento del usuario. Es importante asumir que el medio a través del cual se transmite la información no es seguro así como evitar enviar o recibir información a Internet mediante una red *Wifi* pública, ya que hay riesgo de que se intercepten las comunicaciones. Es por ello que es fundamental asegurar que los datos sensibles son protegidos al transmitirlos.
   - Establecer algún canal de comunicación segura como SSL/TLS *(Transport Layer Security)* con métodos de cifrado de 128 *bits* o 256 *bits*, asegurando de este modo la confidencialidad y la integridad de la información.
   - Se deben utilizar algoritmos de cifrado de una contrastada robustez, y utilizar certificados firmados por autoridades certificadoras confiables, manteniendo en todo momento la cadena de validación.
   - También es posible utilizar redes privadas virtuales (*VPN*) e inicios de sesión a través de *HTTPS*.
   - Mostrar un icono en la aplicación que notifique la transferencia de datos o que se esta haciendo uso del *GPS* del *smartphone* para geolocalización.
   - Alertar a los usuarios a través de la interfaz de usuario si la aplicación móvil detecta un certificado no válido.
   - Auditar los mecanismos de comunicación en busca de posibles fugas de información.

   En el caso de comunicaciones *BAN (Wireless Body Area Network)*, red formada por dispositivos (sensores) de baja potencia implantados en el cuerpo, que controlan los parámetros vitales del cuerpo y movimientos, comunicándose a través de tecnologías inalámbricas y transmitiendo datos desde el cuerpo a una estación base, donde los datos pueden ser remitidos a un hospital, Clínica o a otro lugar, en tiempo real, se debe:
   - Utilizar métodos criptográficos en la obtención de los *BSNs* para la autenticación y distribución de claves. El dispositivo móvil (*smartphone*) puede ser identificado y autenticado por su *IMEI* o su *SIM*.
   - Usar patrones de usuario Biométricos para cifrar y descifrar la clave simétrica, lo que puede facilitar la conexión de los *BSNs* al dispositivo móvil.

8. **Almacenamiento de Datos.** Prestar atención específica al consentimiento para la recogida y utilización de información de los usuarios. Se trata de un conjunto de controles para ayudar a asegurar que el software maneja el almacenamiento y manejo de la información de una manera segura. Dado que los dispositivos móviles son móviles, tienen una mayor probabilidad de pérdida o robo que debe ser tenido en cuenta aquí.

- Crear una política de privacidad que cubra la utilización de información personal. La política de retención de datos debe ser incluida en la política de privacidad para informar a los pacientes.
- Nunca almacenar las contraseñas en texto plano.
- Establecer restricciones de acceso a la información sensible en base a diferentes aspectos como la geolocalización.
- Es preferible almacenar la información sensible en el lado del servidor, al ser los dispositivos móviles elementos susceptibles de ser sustraídos o extraviados y que los datos grabados en el dispositivo se pueden recuperar.
- Cuando se logra el propósito, el *PHI* debe ser borrado y el usuario debe ser notificado. La entidad debe proporcionar un mecanismo para que el usuario compruebe que se han suprimido sus datos.
- Evitar que las credenciales sean visibles en la caché o en los *logs*.
- No almacenar ninguna contraseña *hardcodeada* en el código.
- Los datos deben almacenarse sólo el tiempo necesario para el propósito inicial.
- Tener en cuenta que la normativa para la recolección de información puede ser distinta, dependiendo del país.
- Cifrar los datos sensibles al ser almacenados o al almacenarlos en la memoria caché (no volátil) utilizando un estándar de cifrado aprobado como *AES* 256.
- Los datos sensibles (tales como claves de cifrado, contraseñas, datos sanitarios, etc.) deben permanecer en la memoria *RAM* durante el menor tiempo posible.
- Las claves de cifrado no deben permanecer en la memoria *RAM* durante el ciclo de vida de la sesión de la aplicación. En lugar de ello, las claves deben ser generadas en tiempo real para el cifrado/descifrado, según sea necesario y descartadas una vez se hayan usado.
- No almacenar datos sensibles en el llavero de los dispositivos *iOS*, debido a vulnerabilidades en sus mecanismos criptográficos.
- Activar limpieza remota y/o desactivación remota. Esto permite a un individuo borrar permanentemente todos los datos almacenados en un dispositivo móvil de forma remota, en caso de ser robado.
- Evitar capturas de pantalla de la aplicación en *iOS* ya que este puede guardarlas en memoria caché como imágenes cuando se borra una aplicación.
- Recomendar eliminar o borrar todos los datos almacenados en un dispositivo móvil antes de deshacerse del dispositivo.
- En el caso de teléfonos *Android* que usen la tarjeta de almacenamiento *SD*, si se puede evitar almacenar datos sensibles en estas y sino, se puede logar cierta seguridad a través de la biblioteca *'javax.crypto'* para cifrar los datos de texto plano con una contraseña maestra y *AES* 128.

9. **Distribución y Testeo de *Apps*.** Conjunto de controles para asegurar que la *app* es probada y distribuida libre de vulnerabilidades proporcionando mecanismos para informar de nuevos problemas de seguridad si se encuentran, y también que la *app* ha sido diseñada para aceptar parches con el fin de abordar la seguridad.
    - Diseñar y distribuir aplicaciones para permitir actualizaciones de seguridad mediante parches.
    - Proporcionar canales de retroalimentación para que los usuarios reportan problemas de seguridad con aplicaciones (como una dirección de correo electrónico).
    - Asegurar que las versiones de aplicaciones anteriores ya no son compatibles y son retiradas de las tiendas de aplicaciones y repositorios de *APIs*.
    - Firmar digitalmente las aplicaciones que utilizan un certificado de firma en el código, obtenido a través de una entidad emisora de certificados (*CA*).
    - Asegúrese de que la aplicación esta lo suficientemente ofuscada antes de su liberación, mediante la realización de pruebas que tratan de aplicar ingeniería inversa a la aplicación.
    - Validar todas las entradas de información.
    - Minimizar las líneas de código y su complejidad.
    - Utilizar funciones seguras con el fin de prevenir desbordamientos de *buffer*, etc.
    - Ejecutar las aplicaciones con el mínimo nivel de privilegios.

10. **Notificación de Incumplimiento.** Las aplicaciones están diseñadas para ofrecer servicios, pero muchas no invierten en la privacidad y seguridad de los usuarios. En este punto se indican las siguientes pautas a seguir:
    - En caso de que se produzca una violación de la información del *PHI* de un usuario, la autoridad competente, así como el usuario afectado deben ser notificados tan pronto como sea posible (1-3 días).
    - La entidad debe ayudar al usuario con el fin de aliviar las consecuencias de la infracción que se puedan haber causado.
    - Es importante compensar el usuario afectado con el fin de restaurar el posible daño causado.
    - En los casos de violaciones que afecten a un número significativo de usuarios, los medios de comunicación deben ser notificados para informar sobre el problema.

Además de los requisitos indicados, se recomienda realizar revisiones periódicas, preferiblemente ejecutadas por empresas externas, de la política de seguridad y privacidad llevado a cabo por la entidad (los diseñadores). De esta manera, los diseñadores pueden certificar que sus políticas cumplan los requisitos legales de privacidad y seguridad.

4.2 Implementación de Seguridad en Apps mHealth por Tipo

En esta sección efectuamos una evaluación de seguridad mediante el riesgo real de sufrir una amenaza fruto de una vulnerabilidad. *OWASP Risk Rating Methodology* [113] recomienda el uso de una metodología general para descomponer los hallazgos de seguridad y evaluar los riesgos con el objetivo de priorizarlos y gestionarlos. El primer paso es identificar un riesgo de seguridad que necesita ser tratado. Para identificar un riesgo de seguridad que necesite ser valorado, se necesita recopilar información sobre los agentes que causan la amenaza, el ataque que utilizan, la vulnerabilidad involucrada, y el impacto de una explotación con éxito en tu *app*.

Cuando se identifican los riesgos, debe estimarse la probabilidad de que una vulnerabilidad en particular sea descubierta y explotada. Inicialmente es recomendable definir parámetros de calificación cualitativos para estimar la probabilidad. Para un cálculo con mayor certeza es recomendable el cálculo cuantitativo.

Una vez has identificado un riesgo potencial, para averiguar lo serio que es, el primer paso es estimar la "probabilidad de ocurrencia" global y técnica. Generalmente, es suficiente con identificar si la probabilidad de ocurrencia es baja, media o alta. Para determinar la severidad del riesgo, se debe trabajar con la probabilidad de ocurrencia de la amenaza y el impacto generado sobre la aplicación, tal y como se muestra en la *Tabla 4.1*.

Probabilidad de ocurrencia y niveles de impacto		
6 ≤ 9	Alto	Vulnerabilidad que si es explotada comprometería en su totalidad los datos de usuario. Debe solucionarse de inmediato.
3 ≤ 6	Medio	Vulnerabilidad que si es explotada tendría un impacto leve sobre el usuario. Puede solucionarse en un tiempo prudente.
0 ≤ 3	Bajo	Vulnerabilidad que si es explotada no ocasionaría mayores inconvenientes. Su solución no necesariamente será inmediata.

Tabla 4.1. Niveles de impacto en función de la prob. de ocurrencia de cada vulnerabilidad. Fuente: Propia

Existen varios factores que pueden ayudarnos a realizar esta estimación. El primer grupo de factores, mostrados en la *Tabla 4.2*, están relacionados con los agentes que causan la amenaza involucrada. El objetivo es estimar la probabilidad de ocurrencia de un ataque con éxito por parte de un grupo de posibles atacantes. Podría haber múltiples agentes que exploten una vulnerabilidad en concreto, vistos en la *Tabla 4.3*, así que generalmente es mejor ponerse en el peor de los casos. Cada factor tiene un conjunto de opciones, y cada opción tiene asociada una valoración de 0 a 9 a su probabilidad de ocurrencia. Emplearemos estas cifras más tarde para estimar la probabilidad de ocurrencia global y técnica que nos da el nivel alto, medio o bajo de seguridad a implementar.

Agentes Causantes de la Amenaza			
Habilidades Técnicas	Motivación	Oportunidad	Tamaño
Sin conocimientos (1) Algún conocimiento (3) Usuario Avanzado (4) Redes/Programación (6) Hacker (9)	Ningún interés (1) Algo de interés (4) Mucho interés (9)	Ningún acceso (0) Acceso limitado (4) Acceso especial (7) Acceso total (9)	Desarrolladores (2) Admin. de sistemas (2) Usuarios internos (4) Socios de negocio (5) Usuarios autenticados (6) Usuarios anónimos (9)

Tabla 4.2. Agentes causantes de la amenaza. Fuente: Propia

Factores Causantes de la Vulnerabilidad			
Facilidad de Descubrimiento	Facilidad de Explotación	Conocimiento	Detección de Intrusión
Casi imposible (1) Difícil (3) Fácil (7) Herramientas automatizadas disponibles (9)	Complejo (1) Dificultad media (3) Sencilla (5) Herramientas automatizadas disponibles (9)	Desconocida (0) Oculta (4) Obvia (7) Publico (9)	Activa en la *app* (1) Autenticado y monitoreado (3) Autenticado sin monitoreo (8) No autenticado (9)

Tabla 4.3. Factores causantes de la vulnerabilidad. Fuente: Propia

Cuando una amenaza se materializa, debe considerarse el impacto técnico, como se puede ver en la *Tabla 4.4*.

Factores de Impacto Técnico			
Confidencialidad	Integridad	Perdida de Disponibilidad	Responsabilidad
Revelación mínima de datos no sensibles (2) Revelación mínima de datos sensibles (6) Amplia revelación de datos no sensibles (6) Amplia revelación de datos sensibles (9)	Datos ligeramente corruptos (1) Pocos datos seriamente dañados (3) Muchos datos ligeramente dañados (5) Muchos datos bastante dañados (9)	Mínima (servicios no críticos) (1) Mínimo (servicios críticos) (5) Considerable (servicios no críticos) (5) Considerable (servicios críticos) (7) Todos los servicios perdidos (9)	Algo auditable (1) Auditable (7) Anónima (9)

Tabla 4.4. Factores de impacto técnico. Fuente: Propia

Se debe considerar los factores e identificar aquellos que son clave, ya que están condicionando el resultado. Es posible que la impresión inicial fuera incorrecta al considerar

aspectos de riesgo que no eran obvios. Existe bastante incertidumbre en estas estimaciones, pero esos factores tienen por objetivo ayudar a alcanzar un resultado razonable. El primer paso es seleccionar una de las opciones asociadas con cada factor, después simplemente calcular la media de las puntuaciones para cada uno de lo factores dando como resultado la probabilidad de ocurrencia global y la técnica. Para este proceso se pueden utilizar herramientas automatizadas que facilitan los cálculos. De nuevo, menos que 3 se considera bajo, de 3 a 6 medio, y de 6 a 9 alto.

Finalmente esto da como resultado tres niveles de seguridad (alto, medio y bajo) para cada tipo de *app* vista en los capítulos anteriores, como se indica en la *Tabla 4.5*, en base al tipo de aplicación móvil de salud según su funcionalidad (Informativa, Educacional, Monitoreo, Diagnosis, Tratamiento, Calculadoras, Asistenciales, Localizadores y Alarma), los datos de usuario que manipulan cada una de ellas, el lugar donde dicha información es tratada y del riesgo asociado, fruto de la probabilidad de ocurrencia y el nivel de impacto, de que una posible amenaza surgida de una vulnerabilidad llegue a cumplirse.

Tipo	Datos de usuario	Lugar	Seguridad	Probabilidad
Informativa	No	-	Baja	0 ≤ 3
Educacional	No	-	Baja	0 ≤ 3
Monitoreo	Si	*App* y Servidor	Alta	6 ≤ 9
Diagnosis	Si	*App* y Servidor	Alta	6 ≤ 9
Tratamiento	Si	*App* y Servidor	Alta	6 ≤ 9
Calculadoras	Si	Principalmente *App*	Media	3 ≤ 6
Asistenciales	Si	*App* y Servidor	Alta	6 ≤ 9
Localizadoras	Si	*App*/*GPS*	Media	3 ≤ 6
Alarma	Si	Principalmente *App*	Media	3 ≤ 6

Tabla 4.5. Tabla con los niveles de seguridad según el tipo de aplicación móvil de salud. Fuente: Propia

Dentro de cada nivel de seguridad (bajo, medio y alto), se pretende acercar al lector una serie de pautas de seguridad claras y específicas, de manera visual, en forma de pila de recomendaciones básicas que puedan tener en cuenta tanto personal médico como desarrolladores de aplicaciones amateurs, que hasta hora descuidaban este aspecto por desconocimiento.

Como punto de partida tomaremos de referencia la *Figura 4.2* donde se muestra de manera visual e icónica las partes esenciales a tener en cuenta en la comunicación entre el dispositivo móvil (*smartphone* o *tablet*) donde ejecutamos la aplicación móvil de salud y el servidor (nube o *backend*) donde normalmente se almacenan los datos del usuario que han recopilado dichas *apps*. Entre medias podemos ver que el canal de transmisión en el caso de las tecnologías móviles, no es un cable, sino que es el aire quien transporta la información mediante ondas electromagnéticas haciendo uso de las redes de telefonía móvil o *Wifi*.

Figura 4.2. Esquema con los elementos esenciales en la comunicación entre dispositivos. Fuente: Propia

En el caso de que la aplicación sea de carácter Informativo o Educacional, tal y como muestra la *Tabla 4.6*, la información que la aplicación usa del usuario es prácticamente nula (salvo excepciones), siendo ésta un mero portal donde visualizar el contenido informativo o educacional que esta contenido en la *app* o en su defecto se descarga de un servidor mediante conexión a Internet.

Nivel de Seguridad Bajo: Aplicaciones Informativas & Educacionales
Aplicación *(App/Frontend)*
Control de acceso a la Información (Contactos, Cámara, Localización…) mediante permisos
Recomendar el uso de Cortafuegos (*Firewall*) tanto en *iOS* como en *Android* desde la *app*
La *app* no debe almacenar *Cookies*
Ocultar el *buffer* donde se almacena el contenido que se copia y pega de la *App*
Permitir desactivar el uso de la aplicación en segundo plano
Evitar que se pueda realizar ingeniería inversa de la aplicación "ofuscando" el código de la *app*
Reaccionar ante una violación de integridad de código evitando que sea modificado
Programar la aplicación con librerías de terceros fiables
Distribuir las aplicaciones en repositorios seguros *(App Store, Google Play…)*
Validar todas las entradas y salidas de información a la *app* evitando casos como *QR Code Leaks*
Usar funciones seguras con el fin de prevenir desbordamientos de *buffer*
Testear las aplicaciones ejecutándolas con el mínimo nivel de privilegios
Usar analizadores estáticos de código y *fuzzers* a la hora de desarrollar la *app*
Hacer actualizaciones de seguridad con regularidad mediante parches
Proporcionar canales *(email)* para reportar problemas con la aplicación
Canal
Establecer un canal de comunicación seguro como *SSL/TLS* con cifrado de 128 *bits*
Servidor *(Backend)*
Analizar el servidor con periodicidad y mantenerlo actualizado

Tabla 4.6. Medidas de seguridad para un nivel de seguridad bajo. Fuente: Propia

El siguiente nivel, mostrado en la *Tabla 4.7*, esta compuesto de *apps* del tipo Calculadora, Localizadoras y de Alarma, cuyo requisitos de seguridad son intermedios, dado que tratan una cantidad menor de información del usuario e incluso de menor relevancia y salvo excepciones, como es el uso del *GPS* para el caso de las Localizadoras, la mayor parte de esa información es tratada en el la propia aplicación desde el dispositivo móvil.

Nivel de Seguridad Medio: Aplicaciones de Calculadora, Localizadoras y Alarma

Aplicación *(App/Frontend)*
Control de acceso a la Información (Contactos, Cámara, Localización…) mediante permisos
Recomendar el uso de Cortafuegos (*Firewall*) tanto en *iOS* como en *Android* desde la *app*
La *app* no debe almacenar *Cookies*
Permitir desactivar el uso de la aplicación en segundo plano (evitar la geolocalización permanente)
Uso de Contraseñas de Acceso, *Pin Scramble* o huella dactilar verificando la identidad del usuario
Ocultar el buffer donde se almacena el contenido que se copia y pega de la *app*
No enviar datos a terceros y en su defecto notificarlo
La sesión debe expirar en 30 minutos como máximo en caso de conectarse a un servidor
Evitar que se pueda realizar ingeniería inversa de la aplicación "ofuscando" el código de la *app*
Reaccionar ante una violación de integridad de código evitando que sea modificado
Encriptar el código. Las *apps* tiene que ser cifradas y firmadas por fuentes confiables
Evitar que las credenciales (datos personales) sean visibles en la caché o en el código
Evitar la *exploits* sencillos como es la inyección *SQL*
Evitar *Cross-Site Script Attacks* (modificaciones *HTML* a través de *malware*)
Evitar *Cross-Application Scripting Attacks*
Usar analizadores estáticos de código y *fuzzers* a la hora de desarrollar la *app*
Incluir políticas de privacidad fáciles de leer y entender por parte del usuario
Incluir sección para menores de edad con el requerimiento de la aprobación del tutor legal
Dejar la política accesible en un apartado de la aplicación de fácil acceso
Los datos recogidos deben ser de carácter temporal. Ser borrados tras lograr el objetivo de la *App*
Programar la aplicación con librerías de terceros fiables
Distribuir las aplicaciones en repositorios seguros (*App Store, Google Play*…)
Hacer actualizaciones de seguridad con regularidad mediante parches
Validar todas las entradas y salidas de información a la *App* evitando casos como *QR Code Leaks*
Usar funciones seguras con el fin de prevenir desbordamientos de *buffer*
Testear las aplicaciones ejecutándolas con el mínimo nivel de privilegios
Icono de localización en la *App* que notifique al usuario el uso de la ubicación
Borrado de datos de la aplicación después de 10 intentos no válidos de la contraseña
Para las aplicaciones que contienen datos sensibles, aplicar técnicas antidepuración
No almacenar datos sensibles en el llavero de los dispositivos *iOS*
Evitar capturas de pantalla de la aplicación en *iOS* ya que se guardan en memoria caché
Proporcionar canales *(email)* para reportar problemas de seguridad con aplicaciones
Canal
Uso de métodos criptográficos en la obtención de los *BSNs* en el caso de pulseras cuantificadoras
Establecer un canal de comunicación seguro como *SSL/TLS* con cifrado de 128 *bits*

Usar algoritmos de cifrado robustos, certificados firmados y confiables
Servidor *(Backend)*
Preferiblemente almacenar la información en el servidor (*backend*) y no en la *app*
Analizar el servidor con periodicidad y mantenerlo actualizado
Destruir la sesión iniciada por el usuario en el lado del servidor y no aceptar *cookies* anteriores
Evitar inyecciones en el servidor y ataques binarios (*DoS*)

Tabla 4.7. Medidas de seguridad para un nivel de seguridad medio. Fuente: Propia

Por último, nos encontramos aplicaciones del tipo Monitoreo, Diagnosis, Tratamiento o Asistenciales, las cuales se encuentran en el nivel más alto de seguridad, tal y como vemos en la *Tabla 4.8*, ya que la información que la aplicación móvil de salud manipula del usuario es total. La información o datos de usuario se encuentran tanto en el dispositivo móvil mediante la aplicación como en el servidor, transfiriéndose los datos en ambos sentidos *(Full-duplex)* a través de Internet gracias a una infraestructura de antenas de telefonía móvil 3G/4G o redes *Wifi* cuyo principal medio de transmisión o canal es el aire. En este caso, hay que extremar las precauciones focalizando nuestra atención tanto en la *app*, como en el canal y finalmente, el servidor.

Nivel de Seguridad Alto: Aplicaciones de Monitoreo, Diagnosis, Tratamiento y Asistenciales

Aplicación *(App/Frontend)*
Control de acceso a la Información (Contactos, Cámara, Localización…) mediante permisos
Recomendar el uso de Cortafuegos (*Firewall*) tanto en *iOS* como en *Android* desde la *app*
La *app* no debe almacenar *Cookies*
Uso de Contraseñas de Acceso (7 Caracteres: alfanumérica con algún carácter) o *Pin Scramble*
Ocultar el buffer donde se almacena el contenido que se copia y pega de la *app*
No almacenar contraseñas en texto plano y comprobar su entropía
Permitir desactivar el uso de la aplicación en segundo plano
No enviar datos a terceros y en su defecto notificarlo
Verificar la identidad del usuario mediante algún sistema de Autenticación o parámetro biométrico
Autenticación con un *ID* único vinculado a una *PKI, RSA* o clave simétrica y contraseña
Se recomienda usar la Autenticación en dos pasos médiate *TOTP*
Autenticarse a través de una *API* de inicio de sesión a través de *HTTPS*
Crear, mantener y destruir *Tokens* (largos, complejos y pseudoaleatorios) de sesión mediante *OAuth*
Evitar que se pueda realizar ingeniería inversa de la aplicación "ofuscando" el código de la app
Reaccionar ante una violación de integridad de código evitando que sea modificado
Habilitar el cifrado en dispositivos móviles mediante *whitebox*
Encriptar el código. Las *apps* tiene que ser cifradas y firmadas por fuentes confiables
No almacenar contraseñas *hardcodeadas* en el código
Evitar que las credenciales (Datos Personales) sean visibles en la caché o en el código/*logs*
Usar AES (*Advanced Encryption Standard*) de al menos 192 bits para cifrar los *PHI*
Evitar la *exploits* sencillos como es la inyección *SQL*

Evitar *Cross-Site Script Attacks* (modificaciones *HTML* a través de *malware*)
Evitar *Cross-Application Scripting Attacks*
Usar analizadores estáticos de código y *fuzzers* a la hora de desarrollar la *app*
Usar Firma Digital Pública basada en claves
Incluir políticas de privacidad fáciles de leer y entender por parte del usuario
Incluir sección para menores de edad con el requerimiento de la aprobación del tutor legal
La sesión debe expirar en 15 minutos como máximo
Tener una política de retención de datos clara y en un apartado de la aplicación de fácil acceso
Permitir la limpieza o desactivación remota de la aplicación y su contenido
Uso de la biblioteca *javax.crypto* para cifrar datos de texto plano en móviles con tarjeta SD
Notificar las violaciones de seguridad (de la información) a usuarios y medios de comunicación
Programar la aplicación con librerías de terceros fiables
Distribuir las aplicaciones en repositorios seguros (*App Store, Google Play*…)
Hacer actualizaciones de seguridad con regularidad mediante parches
Validar todas las entradas y salidas de información a la *app* evitando casos como *QR Code Leaks*
Usar funciones seguras con el fin de prevenir desbordamientos de *buffer*
Testear las aplicaciones ejecutándolas con el mínimo nivel de privilegios
Icono en la *app* que notifique la transferencia de datos
Icono de localización en la *app* que notifique al usuario el uso de la ubicación
Borrado de datos de la aplicación después de 10 intentos no válidos de la contraseña
Integrar una solución *CAPTCHA* para mejorar la funcionalidad/seguridad de la *app*
Para las aplicaciones que contienen datos sensibles, aplicar técnicas antidepuración
No almacenar datos sensibles en el llavero de los dispositivos *iOS*
Evitar capturas de pantalla de la aplicación en *iOS* ya que se guardan en memoria caché
No Publicar tus Certificados Digitales en la *App*
Proporcionar canales *(email)* para reportar problemas de seguridad con aplicaciones
Los datos recogidos deben ser de carácter temporal. Ser borrados tras lograr el objetivo de la *App*
Canal
Uso de métodos criptográficos en la obtención de los *BSNs* en el caso de *wearables*
Establecer un canal de comunicación seguro como *SSL/TLS* con cifrado de 128 *bits*
Usar algoritmos de cifrado robustos, certificados firmados y confiables
Usar *VPN* (Redes Virtuales Privadas) o inicios de sesión *HTTPS*
Auditar los mecanismos de comunicación en busca de posibles fugas de información
Los eventos de la invalidación de la sesión se tienen que ejecutar en el servidor
Servidor *(Backend)*
Eliminar el *PHI* del servidor una vez logrado el propósito de la aplicación y notificarlo
Preferiblemente almacenar la información en el servidor (*backend*) y no en la *app*
Analizar el servidor con periodicidad y mantenerlo actualizado
Tomar medidas para evitar ataques de denegación de servicio (*Ataques Binarios - DoS*)
Evitar inyecciones en el servidor
Verificar la identidad del usuario antes de ejecutar el servicio que ofrece la aplicación
Destruir la sesión iniciada por el usuario en el lado del servidor
Las *cookies* de sesiones anteriores no sean aceptadas
Asegurarse de que el servidor rechaza todas las peticiones no cifradas
Medir el riesgo mediante la correlación de los factores tales como la dirección *IP*

Tabla 4.8. Medidas de seguridad para un nivel de seguridad alto. Fuente: Propia

La implementación de la seguridad es de carácter orientativo, dado que las funcionalidades de las aplicaciones pueden variar en sus diferentes iteraciones añadiendo o quitando prestaciones que requieran tener en cuenta medidas de seguridad de otro nivel cuando a priori resultaron ser de uno más bajo o más alto. En cualquier caso, las medidas de seguridad al completo y de carácter general se muestran en el **Punto 4.1**, dando vía libre de escoger al programador o diseñador de la aplicación móvil cuantas medidas resulten necesarias o crea convenientes en el desarrollo de su aplicación en base al servicio y utilidades que quiera prestar con su aplicación móvil de salud.

4.3 Discusión

Una de las partes más importantes dentro del desarrollo de cualquier proyecto tecnológico como es el desarrollo de una aplicación móvil de salud, en campo de la ingeniería, es la responsabilidad social. Ser responsable con la sociedad es pensar en la seguridad, salud y bienestar de las personas a las cuales afecta directa o indirectamente el uso de una aplicación móvil de salud después de su ejecución. Es decir, ser consciente del verdadero alcance de nuestras acciones tratando siempre de proteger los derechos de los individuos, puesto que están depositando su confianza en nuestra *app*, garantizando su seguridad y su privacidad.

Sin embargo, si nos paramos a preguntar cuantos desarrolladores primerizos o personas ajenas al campo de las *TIC* son conscientes y están tomando las medidas necesarias para cumplir con una serie de estándares en relación al campo de la seguridad en sus *apps*, muchos te dirán rápidamente que ninguna. Este apartado explora ese campo tan importante dentro del desarrollo de aplicaciones móviles de salud.

Es increíble como, incluso antes de que se surjan vulnerabilidades dentro de una *app*, un atacante puede obtener una copia de una aplicación mediante técnicas de ingeniería inversa. Las aplicaciones más populares son pirateadas con código malicioso y puestas nuevamente en las principales tiendas de aplicaciones para atraer y engañar a los usuarios que confiados instalan dichas *apps* y acaban corrompiendo sus dispositivos y lo más valioso de ellos, su información privada.

Los desarrollos de aplicaciones por y para el ámbito empresarial ponen a disposición de los desarrolladores herramientas para detectar vulnerabilidades de seguridad y así luego fortificar sus aplicaciones contra la ingeniería inversa y la manipulación de estas. Sin embargo, la mayoría de las "aplicaciones de consumo" que usamos todos en nuestro día a día, todavía representan una amenaza, ya que no pueden someterse al mismo proceso que el de las empresas, puesto que los desarrolladores particulares muchas veces no cuentan con el conocimiento, ni los medios suficientes para ello.

La seguridad de una aplicación pasa por la seguridad del dispositivo donde se instala y se usa. Dispositivos con *jailbreak* (en el caso de *iphone* con *iOS* de *Apple*) o *rooteados (smartphones Android)*

presentan más posibilidades de contener aplicaciones falsas que puedan representar un riesgo de la información que manipulan. Los desarrolladores de *apps* deben conocer los entresijos de dichos sistemas operativos para poder buscar formas de medir de forma dinámica la seguridad del dispositivo móvil al que va destinada su aplicación. Para ello, en primer lugar, el sistema operativo donde se realiza el testeo de la aplicación móvil debe estar intacto. El *jailbreak* o acceso *root* del dispositivo rompe la seguridad subyacente, y es muy recomendable que el desarrollador restrinja el uso de sus aplicaciones únicamente a dispositivos limpios que no hayan sido corrompidos. El *jailbreak* está evolucionando rápidamente para evadir su detección por parte de las aplicaciones y hacer frente a estos mecanismos, subiendo las aplicaciones a repositorios seguros, donde cada vez las políticas de seguridad son más restrictivas es primordial y esencial para mantener a raya estas amenazas, otorgando mayor confianza a los usuarios que se las descargan.

Dado que las aplicaciones móviles permiten a los usuarios realizar transacciones de información (datos personales) con servicios hospitalarios, el nivel de riesgo variará según el tipo de aplicación y que uso hace de la información. Por ejemplo, la lectura de contenidos médicos puramente informativos o educacionales, puede ser considerada de bajo riesgo en comparación con la transferencia de nuestro *PHI* a un nuestro médico, típico de una *app* de diagnostico. Los desarrolladores deben adaptar sus aplicaciones según el uso que hagan de la información, siendo conscientes de los riesgos y restringiendo sus funcionalidades mediante políticas que tengan en cuenta los factores de riesgo como la seguridad del dispositivo, la ubicación del usuario y la seguridad de la conexión de red, entre otros.

El nivel bajo de seguridad, mostrado en la *Tabla 4.9*, está destinado a *apps* de carácter Informativo o Educacional. Éstas apenas hacen uso de datos de usuario ya que tienen como principal función aportar información completa y detallada sobre alguna patología determinada o área de especialización médica, ya sea en formato texto, imagen o vídeo, así como aportar información actualizada sobre alguna enfermedad, que bien se encuentra en la propia aplicación o se descarga de un servidor mediante conexión a Internet, facilitando la educación activa por parte del paciente o público al que va dirigido.

Nivel	**Bajo**
Riesgo	$0 \leq 3$
Aplicación(es)	Informativas y Educacionales
Datos de Usuario	No
Directrices para el Desarrollo de *Apps* de Salud Seguras	Control de Acceso Mantenimiento de la Seguridad en el Servidor Comunicaciones Seguras Distribución y Testeo de *Apps*

Tabla 4.9. Elementos para el desarrollo de *apps* seguras de nivel bajo. Fuente: Propia

Estás aplicaciones no necesitan hacer uso continuo de Internet para funcionar o disponer de alguna de sus funcionalidades, a través de redes móviles o *Wifi*. En el caso de que la información esté alojada en algún servidor, como servidores de noticias o descarga paquetes de información -enciclopedias y guías médicas-, ésta se actualiza cada cierto tiempo, por lo que es fundamental analizar el servidor con periodicidad y mantenerlo actualizado así como establecer un canal de comunicación seguro mediante *SSL/TLS* con cifrado de 128 *bits*.

En cuanto a la aplicación, deberá permitir desactivar el uso de la aplicación en segundo plano y tendrá un control de acceso a la información (Contactos, Cámara, Localización…) mediante permisos que evite proporcionar a las aplicaciones maliciosas y pirateadas el acceso a los servicios básicos (por ejemplo, *SMS*) tan utilizados para cometer actividades fraudulentas.

El nivel medio de seguridad, mostrado en la *Tabla 4.10*, esta destinado a *apps* con funciones de Calculadora, Localizadoras y Alarma. Éste tipo de aplicaciones móviles de salud permiten calcular el índice de masa corporal, la tasa metabólica basal, la frecuencia cardíaca máxima, el contenido de alcohol en la sangre, la dosis de antitérmico recomendada en función del peso del niño, etc. También permiten pedir ayuda u orientarte de manera rápida y efectiva mediante localización *GPS* o avisarte mediante una alarma sobre algún acontecimiento importante relacionado con tu salud. Solo de manera muy puntual hacen uso de Internet salvo las del tipo Localizadoras, las cuales lo necesitan de manera continuada para acceder al servicio de *GPS*, función que se debe restringir y notificar mediante un icono en pantalla solo cuando se este usando la aplicación protegiendo así la seguridad y privacidad del usuario.

Nivel	**Medio**
Riesgo	3 ≤ 6
Aplicación(es)	Calculadoras, Alarma y Localizadoras
Datos de Usuario	Si (Principalmente en la *App*)
Directrices para el Desarrollo de *Apps* de Salud Seguras	Control de Acceso Mantenimiento de la Seguridad en el Servidor Autorización, Autenticación y Manejo de Sesiones Integridad de los Datos y Ofuscación de Código Comunicaciones Seguras Almacenamiento de Datos Seguro y Protegidos Distribución y Testeo de *Apps*

Tabla 4.10. Elementos para el desarrollo de *apps* seguras de nivel medio. Fuente: Propia

El nivel medio de seguridad se caracteriza porque hace un mayor uso de información del usuario o bien introducido de manera manual por el usuario u obtenido de algún *wearable* capaz de cuantificar parámetros de salud por ello es fundamental usar métodos criptográficos, algoritmos de

cifrado robustos y certificados firmados y confiables tanto en la transmisión de la información como en la propia aplicación. Los datos recogidos bien por un *wearable* o introducidos por un usuario y las conexiones establecidas con un servidor o *wearable* deben ser de carácter temporal, siendo borrado cualquier rastro tras lograr el objetivo de la *App*. Finalmente se recomienda que el acceso a la *app* este respaldado mediante el uso de Contraseñas de Acceso, *Pin Scramble* o huella dactilar verificando la identidad del usuario.

El nivel alto de seguridad, mostrado en la *Tabla 4.11*, corresponde a las aplicaciones de monitoreo, diagnosis, tratamiento y asistenciales. Éstas nos permiten tomar el control de nuestro bienestar mediante la cuantificación de todos nuestros parámetros físicos, facilitando el proceso de identificación de una determinada enfermedad o alteración médica y aportando datos de valor para el profesional sanitario. También ayudan al control y tratamiento de enfermedades, permitiendo al paciente llevar un mejor seguimiento del tratamiento y la toma de medicamentos, y permiten una atención continuada e inmediata, más allá de la consulta tradicional, pudiendo mejorar la gestión asistencial de los pacientes proporcionando inmediatez en derivaciones de tratamientos y seguimiento clínico de pacientes, conociendo exhaustivamente que sucede con ellos en todo momento. En definitiva, la experiencia tras este estudio demuestra que este tipo de aplicaciones hacen uso de Internet para funcionar ya que envían información acerca de resultados obtenidos por el usuario siendo receptores de dicha información tanto médicos como otros usuarios. Es por todo ello que hay que tener una seguridad alta tanto en el lado del servidor, como de la aplicación sin olvidar el medio de comunicación.

Nivel	**Alto**
Riesgo	6 ≤ 9
Aplicación(es)	Monitoreo, Diagnosis, Tratamiento y Asistenciales
Datos de Usuario	Si (*App* y Servidor)
Directrices para el Desarrollo de *Apps* de Salud Seguras	Control de Acceso Mantenimiento de la Seguridad en el Servidor Autorización, Autenticación y Manejo de Sesiones Uso de Librerías y Código de Terceros Integridad de los Datos y Ofuscación de Código Informar a los Pacientes Comunicaciones Seguras Almacenamiento de Datos Seguro y Protegidos Distribución y Testeo de *Apps* Notificación de Incumplimiento

Tabla 4.11. Elementos para el desarrollo de *apps* seguras de nivel alto. Fuente: Propia

En el nivel medio y especialmente en el nivel alto, las aplicaciones móviles acceden a datos personales, empresariales e información que se almacena en el dispositivo y el riesgo ante el robo de datos se ve en aumento en cuanto el dispositivo se pierde o cuando los datos se comparten entre aplicaciones. Es fundamental que los desarrolladores implementen en sus *apps* la capacidad de "borrado remoto" para hacer frente a los dispositivos robados o perdidos. Además, se debe cifrar y controlar los datos a los que tienen acceso las aplicaciones móviles, para asegurar los datos contra el *malware* y otras formas de acceso. Cuando se permiten transferencias de información desde la *app* móvil de salud, éstas pueden aprovechar a medir el riesgo mediante la correlación de los factores tales como la dirección *IP (Internet Protocol)* en el que resultaría muy sospechoso el acceso a la misma cuenta desde dos lugares que están muy separados durante un corto período de tiempo. Otros factores a tener en cuenta serían los patrones de acceso de usuario y el acceso constante a los datos del perfil de usuario. Este enfoque hay que hacerlo extensible a la *app* para que sea capaz de detectar y responder a los ataques complejos que pueden abarcar múltiples canales de interacción y eventos de seguridad aparentemente no relacionados.

Por otro lado, es importante tener en cuenta que las contraseñas hay que erradicarlas poco a poco dado que es un secreto compartido, ya que no te identifican realmente. Cada vez menos, va a ser una cadena de caracteres la que nos va a otorgar o verificar el derecho a acceder a los contenidos de la aplicación, sistemas que se usan para verificar que usted es quien dice ser gracias a que la contraseña dice que si eres tú. La autenticación de usuario, a día de hoy, pasa por confiar en algún parámetro físico o externo del usuario de carácter biométrico. Los dispositivos, actualmente, gracias al avance de la tecnología, están equipados con más sensores que nunca y no es descabellado pensar que van a estar equipados con más escáneres (sensores) en los próximos años siendo capaces de verificar nuestras identidades.

Un sistema de identificación robusto debe basarse en dos de tres factores: algo que conoces (una contraseña), algo que tienes (un teléfono móvil a través de la *SIM*) y algo que eres (la biometría mediante huella digital, la verificación del iris o las exploraciones capilares mirando a los vasos sanguíneos debajo de la piel). La banca online ya usa "autenticación de factores múltiples" gracias a una contraseña y una validación por el teléfono móvil. Se trata de introducir en la *app* un segundo código único enviado al móvil mediante un *SMS (Short Message Service)* que da al usuario el consentimiento de acceso a los servicios de la *app*. El motivo de usar un segundo factor de autenticación es que por ejemplo la biometría (huella dactilar) tiene el problema que una vez que te copian la huella, no puedes cambiarla de tu dedo, por eso siempre hay que usar dos de los tres factores. La alternativa para acceder a los servicios de la *app* es *OAuth*, un protocolo distinto para acceder a tus cuentas que consiste en dar permiso a cada aplicación. De esta forma, no tienes que preocuparte ni por contraseñas ni por códigos de autenticación protegiendo tus credenciales de tu cuenta.

CAPÍTULO 5

CONCLUSIONES & LÍNEAS FUTURAS

CAPÍTULO 5. CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Finalizado el desarrollo de este *TFG* (Trabajo de Fin de Grado), se obtienen varios aspectos a reflejar en este apartado de conclusiones, sobre todo aquellas conclusiones relacionadas con el estado del arte de la industria de los dispositivos móviles inteligentes, su crecimiento y adopción gracias a los *smartphones* y al desarrollo de las redes de telefonía móvil, dando lugar a un enorme mercado de aplicaciones para dispositivos móviles, en este caso sanitarias, que están condicionando los hábitos de nuestro día a día y por ende la seguridad y la privacidad de los datos e información que manejan.

En primer lugar hay que resaltar la importante revolución tecnológica que estamos viviendo y como toda revolución que se precie, tiene tres características comunes. Es imparable ya que no importa lo que hagas, la revolución va a seguir su camino. Es transformacional, pues la forma de hacer las cosas va a ser radicalmente distinta después de la revolución y finalmente, tiene ganadores y perdedores. Aplicando estas características a la revolución tecnológica que vivimos, podemos concluir que los primeros en aceptar lo inevitable y tomar las acciones necesarias para adaptarse, tal y como profesaba Darwin, serán los ganadores, por ello la industria de la salud no se está quedando atrás.

La industria de la salud y el bienestar, es consciente del enorme potencial de crecimiento que tiene el mercado de los *smartphones* y *wearables* en la sociedad actual debido a las ingentes oportunidades de desarrollo socioeconómico que ofrecen y con ello el grado de penetración de las aplicaciones móviles en el día a día de cualquier persona tanto a nivel profesional como personal en cualquier campo (ocio, banca, salud, etc.).

Destacar la enorme importancia que están adquiriendo las aplicaciones móviles relacionadas con la *mHealth*, siendo la tercera categoría con mayor crecimiento, sólo después de juegos y utilidades. Cada vez más las personas se preocupan por su salud y por su bienestar, y las aplicaciones móviles juegan un papel fundamental. Hemos establecido nueve categorías intentando abarcar grandes áreas de estudio y funcionalidades de las *apps*, de forma que todas puedan verse representadas. Informativas, educacionales, monitoreo, diagnosis, tratamiento, calculadoras, asistenciales, localizadoras y de alarma, todas ellas en base a las diez enfermedades con mayor impacto en la sociedad según la *OMS*. Los estudios y análisis de mercado que se han realizado hasta la fecha destacan el rol que desempeñan dichas aplicaciones actualmente y auguran un futuro muy próspero tanto a nivel de implantación y de buenos resultados así como a nivel económico.

El éxito de estas aplicaciones radica en que si algo pueden hacer los dispositivos móviles de hoy en día es facilitar la tarea de recogida de datos de pacientes en ensayos clínicos y otros, incluso, pueden ayudar a detectar de forma temprana brotes de enfermedades relacionadas con exposiciones ambientales o agentes infecciosos gracias sus numerosos sensores. También facilitan la comunicación con los profesionales de la salud dando lugar a una nueva forma de relación entre el médico y el paciente ofreciendo múltiples beneficios para ambas partes, desde la optimización del tiempo en consulta hasta la mejora de la adherencia terapéutica y la monitorización de pacientes crónicos.

Sin embargo, en esta carrera por conquistar la categoría de la salud y sumarse a la revolución digital de la sanidad, las prisas no son buenas y ser el primero en el desarrollo y realización de una nueva aplicación conlleva a no considerar adecuadamente algunos aspectos. Entre ellos, la privacidad y la seguridad ya que tienen una importancia singular, especialmente en aquellas aplicaciones que tienen que ver con los datos personales y no transferibles, como las aplicaciones de salud que almacenan un registro electrónico de la salud de los pacientes *(PHI)* o varios datos relativos a su estado de salud.

Y es que, de entre la inmensa cantidad de datos que se manejan diariamente, los datos médicos son un negocio más que jugoso para los cibercriminales ya que pueden ganar hasta diez veces más dinero en el mercado negro que los datos de las tarjetas de crédito. Si a esto sumamos que los médicos y los pacientes están adoptando las tecnologías móviles más rápido de lo que los proveedores pueden proteger la seguridad y la privacidad de éstas, la seguridad acaba por convertirse en un problema significativo. Las empresas/desarrolladores dan prioridad al plazo de salida al mercado y a la experiencia del usuario, descuidando la seguridad y las nuevas pequeñas empresas de software con programadores noveles directamente no lo abordan.

Por todos los motivos que se acaban de comentar, tiene lugar pensar que el *TFG* que aquí se ha llevado a cabo puede tener cabida en el mundo de los desarrolladores de *apps* móviles de salud, mercado competitivo, fuerte y en constante evolución, estableciendo una revisión de la seguridad contemplando las vulnerabilidades más extendidas en el campo del desarrollo de aplicaciones móviles y su importancia a la hora de manejar datos sensibles de usuarios. Por otro lado se presentan unas recomendaciones de seguridad de carácter informativo, en el diseño y desarrollo de las mismas que siente las bases para futuros desarrollos de *apps* que sigan la línea de acción de este trabajo.

Finalmente, comentar que este Trabajo Fin de Grado ha sido muy enriquecedor, ya que abarca dos elementos tan importantes como es la salud y la seguridad de la información, realizando un gran trabajo de investigación que da lugar al nacimiento de un artículo de investigación que sirva como referente en el desarrollo de *mHealth*, haciendo de éste, un mundo más sano y seguro.

5.2 Líneas Futuras

Tras haber finalizado el desarrollo de este *TFG*, vienen a la mente dos aspectos esenciales que pueden servir como futuras líneas de investigación. La gran transformación digital que está sufriendo la sociedad, más concretamente el sector de la sanidad y las enormes medidas de seguridad que hay que implementar si queremos preservar la seguridad y privacidad de todos los datos médicos que dicha revolución, en constante crecimiento, va a generar dando lugar al *Big Data* y *Cloud Computing*.

Nuestra privacidad en el futuro va a estar comprometida. Como decía Mark Zuckerberg, creador de *Facebook* [109], la omnipresencia de las redes sociales en nuestra vida cotidiana ha convertido al mundo en una "aldea social" donde el hecho de que las personas a nuestro alrededor no sepan qué estamos haciendo deja de tener sentido.

Ahora, además de verter información en dichas redes de manera proactiva, lo hacemos también de forma involuntaria. Elementos como los *wearables* presentan un posible futuro en el que, empresas como *Facebook*, podrán saberlo todo sobre nosotros. Gracias a los datos sobre nuestra salud que una pulsera puede transmitir, unido a nuestra edad, la de nuestros padres, y a un análisis de nuestros comentarios a través del procesamiento natural del lenguaje, podríamos tener incluso una aproximación a la fecha de nuestra muerte. ¿Podría llegar el caso en el que un banco no nos concediera una hipoteca debido a las predicciones que ha realizado sobre nuestro futuro?

Por otra parte, en otro futuro hipotético, una persona podría pasear por la calle recopilando multitud de datos biométricos de todas las personas a su alrededor y enviarlos a un servidor. Un *datamining* de nuestras vidas, con información que cualquier empresa pueda analizar para saber todo sobre nosotros.

Toda esta información es muy golosa para los ataques de ciberdelincuentes, por ello la seguridad de nuestros datos es un pilar fundamental a la par que difícil de implementar ya que el crecimiento de estas tecnologías crece día a día fruto de la inmediatez que demanda el mercado y los usuarios y todas ellas cuentan con vulnerabilidades de seguridad importantes.

Por ello, recientemente, una nueva herramienta de autentificación del ciudadano llamada *Mobile Connect* [110] ha sido presentada en el *MWC* 2016 *(Mobile World Congress)*, posicionando a Europa un paso por delante en temas de seguridad. Un servicio completamente seguro y sencillo, en el que el usuario valida su identidad a través del móvil tecleando el pin después de haber introducido en un portal digital los datos personales requeridos, sin que en ningún caso se comparta información personal sin autorización y permitiéndole el acceso a servicios digitales. Este estándar cumple los requisitos del reglamento europeo [116] *eIDAS (Electronic Identification and Signature)*, relativo a la identificación y transacciones electrónicas en Europa.

Se podrá hacer frente a posibles robos de contraseñas con un innovador mecanismo de seguridad patentado actualmente por *Amazon* [114] para los pagos móviles [115]. Los usuarios se identificarán en la *app* con un selfi de su rostro y para aceptar la transmisión de información deberán lanzar un guiño a su cámara del *smatphone* o *tablet*.

Por otra parte, la ingente cantidad de datos que recopilan las *apps* móviles de salud y *wearables*, que dan lugar al *Big Data* permiten que empresas de ciberseguridad puedan predecir los ataques. Mediante el análisis de una infinita cantidad de muestras maliciosas es posible anticiparse a los ciberdelincuentes y predecir cómo, cuándo y dónde se producirá el próximo ataque. Se hace referencia a esto como "lagos de datos", en los que se puede bucear para comprobar qué indicadores han sido comprometidos con el objetivo de anticiparse a futuras amenazas.

Como añadido, el *Big Data* es fundamental para el desarrollo de un aprendizaje autónomo por parte de los dispositivos móviles y sistemas operativos. Ya se está trabajando para que sea el propio sistema el que aprenda y alerte cuando detecte algún elemento sospechoso, basándose en todo lo visto anteriormente y es que *"El hecho de poner en peligro la seguridad de nuestra información personal puede acabar poniendo en peligro nuestra seguridad personal."* - Tim Cook (*CEO* de *Apple*) [111]

5.2.1 La Sanidad Digital del Futuro

Este apartado, apoyado en el documento *World Economic Forum* [112], pretende reflejar mediante un breve análisis el impacto que la transformación digital tendrá en la salud y en las organizaciones sanitarias, ya que como es evidente, la revolución digital que vivimos actualmente está transformando todas las industrias y en especial el ámbito *Health*.

Es especialmente relevante la afirmación de que, la introducción de los "servicios digitales" será el mayor vector de cambio de la sanidad en la próxima década. Sin embargo, aunque pocos sectores como el de la salud tienen tal potencial de cambio, no debemos subestimar las enormes barreras regulatorias y económicas que encontrarán aquellos que quieran ser pioneros en este proceso de cambio.

La sanidad del futuro estará centrada en la persona de manera efectiva, asignando a los pacientes y a sus familiares una mayor responsabilidad en la gestión de su salud. Dos grandes cambios operarán en este sentido, la "localización de los cuidados" del hospital al hogar, y la "tipología de cuidados" del tratamiento a la prevención.

Las organizaciones sanitarias del futuro pondrán, por tanto, menos énfasis en la construcción de centros y ampliación de camas hospitalarias y se orientarán al diseño de nuevos servicios digitales, de mayor calidad, más humanos, accesibles y eficientes.

¿Será esta la transformación que necesitamos para hacer sostenible nuestro sistema sanitario?, desde luego, lejos de lo que algunos esperábamos, la crisis no provocó el inicio de ese cambio esencial para mantener a medio plazo uno de nuestros más preciados "tesoros".

Se identifican en el estudio cuatro elementos del mundo digital que dirigirán este cambio:

1. **Salud Inteligente:** Que mejorará la calidad de la atención a un menor coste mediante el uso de medicina de precisión y basada en la evidencia.
2. **Salud Ubicua:** La casa y la consulta conectada y la salud virtual mediante citaciones abiertas, video consulta, etc., acercarán los servicios clínicos y sociales al hogar produciéndose la real integración de lo social y lo sanitario con foco en la persona.
3. **Paciente Experto**: Los nuevos modelos de atención basados en *service design* harán que el paciente sea mucho más conocedor de su enfermedad y le facilitará los medios para gestionar su salud y su enfermedad mediante aplicaciones móviles de salud más avanzadas.
4. **Organizaciones Sanitarias basadas en el Conocimiento**: Extracción del valor de la información que atesoran para mejorar los tratamientos, las decisiones y el soporte en tiempo real a las necesidades y su propia gestión mediante el *Big Data.*

La sanidad digital se orientará a aportar valor apoyada en cinco tecnologías que, estando hoy ya disponibles, habilitarán con seguridad el cambio. Éstas son la analítica e inteligencia artificial, el Internet de las cosas y la medicina conectada, en las técnicas de marketing digital y en el diseño de nuevos servicios digitales.

1. ***Internet of Me:*** El 50% de los pacientes a nivel global llevan habitualmente tecnología que podría medir estilos de vida y signos vitales como son *smartphones* o *wearables*. La utilización de esta información habilitará nuevas formas de atención preventiva y terapéutica.
2. **El Internet de las Cosas** *(IoT)* aplicado al mundo hospitalario permitirá que los edificios sean capaces de identificar la presencia y ubicación del paciente y profesionales, se podrá informar de forma desatendida de las demoras de consulta, guiar al paciente por el centro e integrar servicios clínicos heterogéneos y distantes, de manera virtual, orientándolos a la resolución de procesos complejos.
3. ***Big Data*** **y nuevas Técnicas Analíticas:** el procesamiento inteligente de los datos suministrados en los anteriores puntos, desencadenará alertas y respuestas automatizadas basadas en tecnología cognitiva. Cada año el volumen de datos disponible en un hospital, se duplica, generando una "mina" para el avance de la ciencia. La evidencia científica, se basaba, hasta hoy, en un análisis documental/semimanual de miles de casos (en papel y con un soporte informático básico). Hoy, con estas tecnologías, disponemos de millones de datos de pacientes de forma integrada y procedentes de fuentes muy heterogéneas (*big data*), de capacidades exponenciales de procesamiento de datos, de la automatización del proceso de anonimización,

de sistemas de análisis inteligente de información no estructurada (la que se encuentra en las anotaciones clínicas de la Historia Clínica Electrónica o *PHI)* y potentísimas técnicas de analítica predictiva.

4. **Plataformas de Medicina Conectada**: Las nuevas generaciones de software de gestión hospitalaria e Historia Clínica Electrónica *(PHI)* cuentan con tecnología de interoperabilidad para la integración de centros y para proporcionar conexión coordinada a pacientes y cuidadores. Hoy, el 54% de los pacientes que utilizan aplicaciones móviles lo hacen en el ámbito de la salud.
5. **Doctor Digital**: El médico del futuro se comunicará electrónicamente con sus pacientes de forma rutinaria, citará las visitas presenciales y virtuales mediante el canal Web, derivará y recibirá notificaciones de interacciones de su paciente con otras organizaciones, dispondrá de alertas automatizadas y herramientas avanzadas de soporte a la decisión y guías clínicas inteligentes. El 45% de los directivos de la sanidad están convencidos de que, en 3 años dedicarán especial énfasis en "adiestrar sistemas de soporte".

Está claro, que el futuro de la industria médica tiene que tender a una mayor digitalización casi por inercia ya que una maquina tiene menos probabilidades de equivocarse que una persona. Sin embargo, el mayor desafío al que se tiene que enfrentar esta industria es a un cambio de mentalidad en los pacientes que tienen que depositar su confianza en una máquina y eso sólo sucederá cuando realmente existan altas medidas de seguridad.

CAPÍTULO 6
BIBLIOGRAFÍA

CAPÍTULO 6. BIBLIOGRAFÍA

[1] Isaacson, W. *Steve Jobs. La biografía.* 2011. Debate. Washington DC, USA.

[2] TIME. *Invention Of the Year: The iPhone*. [Consulta: enero de 2016]. Disponible en: http://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html

[3] Szymanczyk, O. *Historia de las telecomunicaciones mundiales.* 2013. Editorial Dunken. Buenos Aires, Argentina.

[4] ITU, International Telecommunication Union. *ICT Facts and Figures – The World in 2015*. 2015. [Consulta: enero de 2016]. Disponible en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

[5] Appfigures Blog. *App Stores Growth Accelerates in 2014*. 2015. [Consulta: enero de 2016]. Disponible en: http://blog.appfigures.com/app-stores-growth-accelerates-in-2014/

[6] Expansión. *Los fabricantes chinos invaden el mercado de "smartphones"*. [Consulta: enero de 2016]. 2016. Disponible en: http://www.expansion.com/economia-digital/companias/2015/10/30/5633a49c268e3e16498b45ef.html

[7] Gartner. *Gartner Says Worldwide Smartphone Sales Recorded Slowest Growth Rate Since 2013*. 2015. [Consulta: enero de 2016]. Disponible en: http://www.gartner.com/newsroom/id/3115517

[8] Mercado Financiero, Europa Press. *Las ventas mundiales de smartphones suben un 10,1% en 2015, hasta la cifra record 1.433 millones*. 2016. [Consulta: enero de 2016]. Disponible en: http://www.europapress.es/economia/noticia-ventas-mundiales-smartphones-suben-101-2015-cifra-record-1433-millones-20160128161652.html

[9] GSMA. *The Mobile Economy 2015*. 2015. [Consulta: enero de 2016]. Disponible en: http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf

[10] Ontsi. *Evolución del número de clientes de telefonía móvil en España*. [Consulta: enero de 2016]. Disponible en: http://www.ontsi.red.es/ontsi/es/indicador/evolución-del-número-de-clientes-de-telefon%C3%ADa-móvil-en-españa

[11] Deloitte. *Consumo Móvil en España 2014*. 2015. [Consulta: enero de 2016]. Disponible en: http://www2.deloitte.com/es/es/pages/technology-media-and-telecommunications/articles/consumo-medios-espana.html

[12] ABC Tecnología. *España, líder europeo en penetración de «smartphones»*. 2015. [Consulta: enero de 2016]. Disponible en: http://www.abc.es/tecnologia/moviles/20150121/abci-estudio-sociedad-informacion-espana-smartphones-tablets-moviles-habitos-usuarios-fundacion-telefonica-datos-201501211605.html

[13] The App Date. *V informe sobre el estado de las apps en España*. 2014. [Consulta: enero de 2016]. Disponible en: http://www.theappdate.es/v-informe-estado-apps-espana/

[14] KPBC. *Internet Trends 2015 – Code Conference*. 2015. [Consulta: febrero de 2016]. Disponible en: http://www.kpcb.com/internet-trends

[15] Statista. *Worldwide mobile app revenues from 2011 to 2017.* [Consulta: febrero de 2016]. Disponible en: http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/

[16] Mobile Health Economics by Reasearch2guidance. *EU Countries' mHealth App Market Ranking 2015*. 2015. [Consulta: febrero de 2016]. Disponible en: http://mhealtheconomics.com/eu-countries-mhealth-app-market-ranking-2015/

[17] The App Date. *Informe 50 mejores app en salud en español*. 2014. [Consulta: febrero de 2016]. Disponible en: http://www.theappdate.es/static/media/uploads/2014/03/Informe-TAD-50-Mejores-Apps-de-Salud.pdf

[18] El Mundo. *Las aplicaciones móviles de salud generarán en 2015 un negocio de 4.000 millones de euros en España.* 2014. [Consulta: febrero de 2016]. Disponible en: http://www.elmundo.es/salud/2014/03/19/5329df6f22601dff5e8b457b.html

[19] PWC. *La mHealth como eje asistencial puede reducir los costes en un 50%*. 2013. [Consulta: febrero de 2016]. Disponible en: http://www.pwc.es/es/sala-prensa/notas-prensa/2013/jornada-mhealth.html

[20] CES, Consumer Technology Association. *CES in the News.* [Consulta: febrero de 2016]. Disponible en: https://www.cesweb.org

[21] MGI, McKinsey Global Institute. *The Internet Of Things: Mapping the Value Beyond the Hype.* [Consulta: febrero de 2016]. Disponible en: http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

[22] Expansión. *¿Hay que regular las "apps" que hacen uso de los datos sanitarios?*. 2016. [Consulta: febrero de 2016]. Disponible en: http://www.expansion.com/juridico/actualidad-tendencias/2016/01/21/56a12926268e3ec0728b458d.html

[23] IOT Solutions World Congress. *The Future of Healthcare Wearables - Innovation - IOTSWC15*. 2015. [Consulta: febrero de 2016]. Disponible en: https://www.youtube.com/watch?v=VR7LPXYYaC0

[24] El País. *Siempre móviles y conectados*. [Consulta: febrero de 2016]. Disponible en: http://economia.elpais.com/economia/2015/10/20/actualidad/1445350108_355232.html

[25] Eleven Paths. *Informe: 2015, el año de las fugas de información.* [Consulta: febrero de 2016]. Disponible en: http://blog.elevenpaths.com/2016/01/informe-2015-el-ano-de-las-fugas-de.html?m=1

[26] Byte TI. *Internet de las Cosas genera riesgos de seguridad de largo alcance para personas, organizaciones y Estados.* [Consulta: febrero de 2016]. Disponible en: http://www.revistabyte.es/actualidad-byte/internet-de-las-cosas-iot-genera-riesgos-de-seguridad-de-largo-alcance62634/

[27] Expansión, Economía Digital. *Datos médicos, un negocio más que jugoso para los hackers.* [Consulta: febrero de 2016]. Disponible en: http://www.expansion.com/tecnologia/2016/01/02/5687958be2704eaa188b4613.html

[28] VERACODE. *State of Software Security Report. Supplement to Vol 6, Fall 2015: Application Development Landscape.* [Consulta: febrero de 2016]. Disponible en: http://www.veracode.com/resources/state-of-software-security

[29] Bitglass. *Healthcare Breach Report 2016.* 2016. 2015 [Consulta: febrero de 2016]. Disponible en: http://pages.bitglass.com/rs/418-ZAL-815/images/BR_Healthcare_Breach_Report_2016.pdf

[30] Ponemon Institute. *2015 Cost of Data Breach Study: Global Analysis.* [Consulta: febrero de 2016]. Disponible en: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF

[31] Field MJ. Editor; Committee on Evaluating Clinical Applications of Telemedicine. *Telemedicine: A Guide to Assessing Telecommunications in Health Care*. Institute of Medicine, 1996 The National Academies press, Washington DC, USA.

[32] Vincenzo Della Mea. *What is e-Health (2): The death of telemedicine?* J. Med Internet Res 2001. [Consulta: noviembre de 2015]. Disponible en: http://www.jmir.org/2001/2/e22/

[33] World Health Organization. *mHealth: New horizons for health through mobile technologies*. 2011. [Consulta: noviembre de 2015]. Disponible en: http://www.who.int/goe/publications/goe_mhealth_web.pdf?ua=1

[34] Adibi, Sasan (Ed.). *Mobile Health. A Technology Road Map*. Srpinger International Pubishing.

[35] European Commision. *What mHealth can do for you.* [Consulta: noviembre de 2015]. Disponible en: http://europa.eu/rapid/press-release_MEMO-14-266_en.htm?locale=EN

[36] Research2guidance. *Mobile Health Market Report 2013-2017*. [Consulta: noviembre de 2015]. Disponible en: http://research2guidance.com/wp-content/uploads/2015/08/Mobile-Health-Market-Report-2013-2017-Preview.pdf

[37] World Health Organization. *Disease and injury regional estimates, cause-specific mortality: regional estimates for 2012.* [Consulta: noviembre de 2015]. Disponible en: http://www.who.int/mediacentre/factsheets/fs310/es/

[38] World Health Organization. *Global Burden of Disease: 2004 Update 2008*. [Consulta: noviembre de 2015]. Disponible en: http://www.who.int/healthinfo/global_burden_disease/2004_report_update/en/

[39] IDC. *Smartphone OS Market Share, 2015 Q2.* [Consulta: noviembre de 2015]. Disponible en: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[40] Google. *Google Play.* [Consulta: noviembre de 2015]. Disponible en: http://play.google.com/store

[41] Apple. *iTunes*. [Consulta: noviembre de 2015]. Disponible en: http://www.apple.com/itunes/

[42] Microsoft. *Windows Phone Apps+Games.* [Consulta: noviembre de 2015]. Disponible en: http://www.windowsphone.com/es-es/store

[43] BlackBerry. *BlackBerry World.* [Consulta: noviembre de 2015]. Disponible en: http://www.appworld.blackberry.com/webstore/product/1/

[44] Nokia. *Ovi Store.* [Consulta: noviembre de 2015]. Disponible en: http://store.ovi.com/

[45] IMS Institute for Healthcare Informatics. *Patient Adoption of mHealth*. EE.UU. 2015. [Consulta: noviembre de 2015]. Disponible en: http://www.imshealth.com

[46] IDC. *Worldwide Tablet Shipments Expected to Decline -8.0% in 2015 While 2-in-1 Devices Pick Up Momentum, Growing 86.5%, According to IDC.* [Consulta: noviembre de 2015]. Disponible en: http://www.idc.com/getdoc.jsp?containerId=prUS25867215

[47] Calvo-González, D.; De la Torre-Díez, I.; López-Coronado, M., *Análisis y evolución de aplicaciones móviles en el campo de la salud*. I+S Informática y Salud: Sociedad Española de Informática y Salud, nº 108. Diciembre de 2014, p. 63 - 70.

[48] El Khaddar, M.A., Harroud, h., Boulmalf, M., and Elkoutbi, M., Habbani A (2012) *Emerging wireless technologies in e-health Trends, challenges, and framework design issues.* International Conference on Multimedia Computing and Systems (ICMCS)

[49] Lin, C. F., *Mobile telemedicine: a survey study*. J Med Syst , 2012.

[50] Martinez-Pérez, B., de la Torre-Díez, I., and López-Coronado, M., *Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis.* J Med Internet Res, 2013.

[51] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., et al., *A comprehensive survey of Wireless Body Area Networks.* J Med Syst, 2012.

[52] Kumar, B., Singh, S. P., and Mohan, A., *Emerging mobile communication technologies for health.* International Conference on Computer and Communication Technology, 2010. Allahabad.

[53] Gupta, R., and Mitra, M., *Wireless electrocardiogram transmission in ISM band: an approach towards telecardiology*. J Med Syst, 2014.

[54] Yan, H., Huo, H., Xu, Y., and Gidlund, M., *Wireless sensor network based E-health system - implementation and experimental results.* IEEE Transactions on Consumer Electronics, 2012.

[55] Sinha, A., And Couderc, P., *A framework for interacting smart objects.* Lecture Notes in Computer Science, 2013.

[56] Touati, F., And Tabish, R., *u-Healthcare system: state-of-the-art re- view and challenges*. J Med Syst, 2013.

[57] Coleman, N., *Mapping subscribers for better mobile networks*. GEO: *connexion*. 2013.

[58] Bert, F., Giacometti, M., Gualano, M. R., and Siliquini, R., *Smartphones and health promotion: a review of the evidence.* J Med Syst, 2014.

[59] Xiao, Z., and Camino, F. E., *The fabrication of carbon nanotube field-effect transistors with semiconductors as the source and drain contact materials.* Nanotechnology, 2009.

[60] Nakatani, K., *New technology trends in touch panel sensing. Proceedings of the International Display Workshops, 2012.*

[61] Benfdila, A., Abbas, S., Izquierdo, R., Talmat, R., and Vaseashta, A.*, On the drain current saturation in carbon nanotube field effect transistors.* Nano, 2010.

[62] Bremer, M., Kirsch, P., Klasen-Memmer, M., and Tarumi, K., *The TV in your pocket: Development of liquid-crystal materials for the new millennium.* Angew Chem Int Ed Engl, 2013.

[63] Gartner. *Gartner Says Smartphone Sales Surpassed One Billion Units in 2014.* 2015. [Consulta: diciembre de 2015]. Disponible en: http://www.gartner.com/newsroom/id/2996817

[64] AppFigures Blog. *App Stores Growth Accelerates in 2014.* [Consulta: diciembre de 2015]. Disponible en: http://blog.appfigures.com/app-stores-growth-accelerates-in-2014/

[65] Cohn SP, National Committee on Vital and Health Statistics. *Privacy and confidentiality in the nationwide health information network.* 2006. [Consulta: diciembre de 2015]. Disponible en: http://www.ncvhs.hhs.gov/060622lt.htm

[66] Ponemon Institute. *The State of Mobile Application Insecurity (Sponsored by IBM)*. 2015. [Consulta: diciembre de 2015]. Disponible en: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGL03074USEN&attachment=WGL03074USEN.PDF

[67] The Wall Street Journal – Deloitte. *Security and Privacy in Mobile Health*. EE.UU. 2013. [Consulta: diciembre de 2015]. Disponible en: http://deloitte.wsj.com/cio/2013/08/06/security-and-privacy-in-mobile-health/

[68] Lindy Benton. *Marrying the BYOD phenomenon to HIPAA compliance. HIMMS.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://www.himss.org/ResourceLibrary/GenResourceDetail.aspx?ItemNumber=18909

[69] HIMMS Analytics. *2015 Mobile Technology Survey | Executive summary.* 2015. [Consulta: diciembre de 2015]. Disponible en: http://www.himss.org/ResourceLibrary/genResourceDetailPDF.aspx?ItemNumber=41510

[70] Whipple, E. C., Allgood, K. L., and Larue, E. M., *Third-year medical students' knowledge of privacy and security issues concerning mobile devices*. Med Teach, 2012.

[71] Vodafone Global Enterprise. *Evaluating mHealth Adoption Barriers: Privacy and Regulation–Protecting your patients' privacy in a mobile world.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf

[72] Hsu, C. L., Lee, M. R., and Su, C. H., *The role of privacy protection in healthcare information systems adoption.* J Med Sys, 2013.

[73] Rosenbaum, B. P., *Radio frequency identification (RFID) in health care: privacy and security concerns limiting adoption.* J Med Syst, 2014.

[74] Green, H., *Strategies for safeguarding security of mobile computing.* Healthc Financ Manage, 2013.

[75] Gardazi SU, Shahid AA, Salimbene C. *HIPAA and QMS based architectural requirements to cope with the OCR audit program.* Proceedings of 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC) 2012.

[76] Luxton, D. D., Kayl, R. A., and Mishkind, M. C., *mHealth data security: the need for HIPAA-compliant standardization.* Telemedicine journal and e-health: the official journal of the American Telemedicine Association, 2012.

[77] Yeh, C. K., Chen, H. M. B., and Lo, J. W., *An authentication protocol for ubiquitous health monitoring systems.* Journal of Medical and Biological Engineering, 2013.

[78] Ren, J., Wu, G., and Yao, L., *A sensitive data aggregation scheme for body sensor networks based on data hiding.* Personal and Ubiquitous Computing, 2013.

[79] Li, X., Wen, Q., Li, W., Zhang, H., and Jin, Z., *Secure privacy-preserving biometric authentication scheme for telecare medicine information systems.* J Med Syst, 2014.

[80] Chen CL, Yang TT, Chiang ML, Shih TF. *A privacy authentication scheme based on cloud for medical environment.* J Med Syst, 2014.

[81] Kim, J. T., *Enhanced secure authentication for mobile RFID healthcare system in wireless sensor networks.* Communications in Computer and Information Science, 2012.

[82] Vision Mobile. *Developer Economics Q1 2014: State of the Developer Nation.* 2014. [Consulta: diciembre de 2015]. Disponible en: http://www.visionmobile.com/product/developer-economics-q1-2014-state-developer-nation/

[83] Prodigioso Volcan, Planner Media, Roche Farma y Siemens. *Big data y Salud.* 2015. [Consulta: diciembre de 2015]. Disponible en: http://www.plannermedia.com/downloads/informebigdataysalud.pdf

[84] Official Journal L (1995) DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995

[85] European Commission (2012) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[86] Pub. L (1996) Health Insurance Portability and Accountability Act of 1996. No. 104–191, 110 Stat. 1936 (1996).

[87] Federal Trade Commission Act. 15 U.S.C

[88] FTC Staff Report. *Mobile Privacy Disclosures: Building Trust Through Transparency.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://www.ftc.gov/sites/default/files/ documents/reports/mobile-privacy-disclosures-building-trust- through-transparency-federal-trade-commission-staff-report/ 130201mobileprivacyreport.pdf

[89] Pub.L (1998) *Children's Online Privacy Protection Act of 1998 (COPPA)*. No. 105–277, 112 Stat. 1998.

[90] Martinez-Pérez, B., de la Torre-Díez, I., and Lopez-Coronado, M., *Privacy and Security in Mobile Health Apps: A Review and Recommendations.* J Med Internet Res (2015)

[91] Thomson Reuters Foundation. *Patient Privacy in a Mobile World. A Framework to Adress Privacy Law Issues in Mobile Health.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://www.mhealthalliance.org/images/content/trustlaw_connect_ report.pdf

[92] Group, V. *Evaluating Mhealth Adoption Barriers: Privacy and Regulation.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf

[93] Wang, J., Zhang, Z., Xu, K., Yin, Y., and Guo, P. *A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System.* Int.l Journal of Security & Its Applications, 2013.

[94] OWASP. *OWASP Mobile Security Project.* 2015. [Consulta: enero de 2015]. Disponible en: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

[95] Kharrazi, H., Chisholm, R., VanNasdale, D., and Thompson, B. *Mobile Personal Health Records: An Evaluation of Features and Functionality.* Int.l Journal of Medical Informatics, 2012.

[96] McCarthy, M. *Experts Warn on Data Security in Health and Fitness Apps.* 2013.

[97] HealthCareBusinessTech. *Mobile Health Apps Create Privacy Risk, Study Says*. 2014. [Consulta: diciembre de 2015]. Disponible en: http://www.healthcarebusinesstech.com/mobile-health-apps-privacy/

[98] Figg, W.C., Ph.D, and Kam, H.J., M.S. *Medical Information Security.* International journal of Security (IJS), 2011.

[99] Dixon, P. *Medical Identity Theft: The Information Crime That Can Kill You.* The world privacy forum, 2006.

[100] Faudree, B., and Ford, M. *Security and Privacy in Mobile Health.* CIO Journal, 2013.

[101] Gu, Q., And Guirguis, M. *Secure Mobile Cloud Computing and Security Issues,* in High Performance Cloud Auditing and Applications. Springer, 2014.

[102] Piette, J.D., Mendoza-Avelares, M.O., Ganser, M., Mohamed, M., Marinec, N., and Krishnan, S. *A Preliminary Study of a Cloud-Computing Model for Chronic Illness Self-Care Support in an Underdeveloped Country.* American journal of preventive medicine, 2011.

[103] Rui, Z., and Ling, L. *Security Models and Requirements for Healthcare Application Clouds.* Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010.

[104] Research, J.o.M.I. *Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems.* 2013. [Consulta: diciembre de 2015]. Disponible en: http://www.jmir.org/2013/8/e186/

[105] HealthIt. *Your Mobile Device and Health Information Privacy and Security.* 2014. [Consulta: enero de 2015]. Disponible en: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health- information-privacy-and-security

[106] Fife, E., and Orjuela, J., *The privacy calculus: Mobile apps and user perceptions of privacy and security*. International Journal of Engineering Business Management.

[107] ISO (2013) ISO/IEC 27001:2013 Information technology - Security techniques - Information security management Systems - Requirements. http://www.iso27001security.com/html/27001.html

[108] Office of the Privacy Commissioner of Canada. *Results of the 2014 Global Privacy Enforcement Network Sweep*. [Consulta: marzo de 2016]. Disponible en: https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp

[109] Blog Think Big –Telefonica. *Hacia un uso más seguro de Internet de las Cosas*. 2016. [Consulta: febrero de 2016]. Disponible en: http://blogthinkbig.com/hacia-un-uso-mas-seguro-de-internet-de-las-cosas/

[110] Mobile Connect. *Mobile Connect*. 2016. [Consulta: marzo 2016]. Disponible en: https://mobileconnect.io

[111] El País. *Tim Cook. Un mensaje a nuestros clientes*. 2016. [Consulta: febrero de 2016]. Disponible en: http://internacional.elpais.com/internacional/2016/02/17/actualidad/1455742775_465869.html

[112] Health World Economic Forum - Accentur. *Digital Transformation of Industries*. 2015. [Consulta: febrero de 2016]. Disponible en: https://drive.google.com/file/d/0ByX_C7o0ryiCQk02bWk4azJteTg/view

[113] OWASP. *OWASP Risk Rating Methodology*. 2016. [Consulta: marzo 2016]. Disponible en: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[114] Amazon. *Amazon.com*. 2016. [Consulta: marzo 2016]. Disponible en: http://www.amazon.com

[115] US Patent & Trademark Office. United States Patent Application: 0160071111. 2016. [Consulta: marzo 2016]. Disponible en: http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=20160071111.PGNR.&OS=&RS=

[116] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. [Consulta: marzo 2016]. Disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.