DOI: http://dx.doi.org/10.22267/rus.171902.90

Universidad y Salud
ARTÍCULO ORIGINAL

Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles

Model of assessment of requirements of privacy, security and quality of service for mobile medical applications

Edward Paul Guillen-Pinto[1*] orcid.org/0000-0002-2002-4021
Leonardo Ramírez-López[1] orcid.org/0000-0002-6473-5685
Yuli Paola Cifuentes-Sanabria[1] orcid.org/0000-0001-6722-5448

1 Universidad Militar Nueva Granada. Bogotá, Colombia

Fecha de recepción: Agosto 8 - 2016 Fecha de revisión: Junio 1 - 2017 Fecha de aceptación: Agosto 11 - 2017

Guillen-Pinto EP, Ramírez-López L, Cifuentes-Sanabria YP. Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles. Rev Univ. Salud. 2017;19(2):280-292. DOI: http://dx.doi.org/10.22267/rus.171902.90

Resumen

Introducción: El desarrollo de tecnologías móviles ha facilitado la creación de aplicaciones mHealth, las cuales son consideradas herramientas clave para la atención segura y de calidad a los pacientes de poblaciones apartadas y con carencia de infraestructura para la prestación de servicios de salud. El artículo considera una propuesta de un modelo de evaluación que permite determinar las debilidades y vulnerabilidades a nivel de seguridad y calidad de servicio (QoS) en aplicaciones mHealth. **Objetivo:** Realizar una aproximación de un modelo de análisis que apoye la toma de decisiones referentes al uso y producción de aplicaciones seguras, minimizando el impacto y la probabilidad de ocurrencia de los riesgos de seguridad informática. **Materiales y métodos:** El tipo de investigación aplicada es de tipo descriptivo, debido a que se detallan cada una las características que deben tener las aplicaciones móviles de salud para alcanzar un nivel de seguridad óptimo. La metodología utiliza las normas que regulan las aplicaciones y las mezcla con técnicas de análisis de seguridad, empleando la caracterización de riesgos planteadas por Open Web Application Security Project -OWASP y las exigencias de QoS de la Unión Internacional de Telecomunicaciones -UIT. **Resultados:** Se obtuvo un análisis efectivo en aplicaciones reales actuales, lo que muestra sus debilidades y los aspectos a corregir para cumplir con parámetros de seguridad adecuados. **Conclusiones:** El modelo permite evaluar los requerimientos de seguridad y calidad de servicio (QoS) de aplicaciones móviles para la salud que puede ser empleado para valorar aplicaciones actuales o generar los criterios antes de su despliegue.

Palabras clave: Confidencialidad; sistemas de información en hospital, seguridad computacional. (Fuente: DeCS, Bireme).

Abstract

Introduction: The development of mobile technologies has facilitated the creation of mHealth applications, which are considered key tools for safe and quality care for patients from remote populations and with lack of infrastructure for the provision of health services. The article considers a proposal for an evaluation model that allows to determine weaknesses and vulnerabilities at the security level and quality of service (QoS) in mHealth applications. **Objective:** To carry out an approximation of a model of analysis that supports the decision making, concerning the use and production of safe applications, minimizing the impact and the probability of occurrence of the risks of computer security. **Materials and methods:** The type of applied research is of a descriptive type, because each one details the characteristics that the mobile health applications must have to achieve an optimum level of safety. The methodology uses the rules that regulate applications and mixes them with techniques of security analysis, using the characterization of risks posed by Open Web Application Security Project-OWASP and the QoS

***Autor de correspondencia**
Edward Paul Guillen-Pinto
e-mail: edward.guillen@unimilitar.edu.co

requirements of the International Telecommunication Union-ITU. **Results:** An effective analysis was obtained in actual current applications, which shows their weaknesses and the aspects to be corrected to comply with appropriate security parameters. **Conclusions:** The model allows to evaluate the safety and quality of service (QoS) requirements of mobile health applications that can be used to evaluate current applications or to generate the criteria before deployment.

Keywords: mHealth Apps; data security; Quality of service (QoS); risk assessment and management. (Source: DeCS, Bireme).

Introducción

En el sector de la salud, la adopción y uso de las tecnologías de la información y las comunicaciones –TIC– para la prestación de servicios médicos han tenido una gran aceptación a nivel mundial, a causa de la estrecha relación que tienen estas tecnologías con la eficiencia, la competitividad y la calidad, que proporcionan en las actividades que realizan los profesionales de la salud y de la biomedicina. En el 2005, la organización mundial de la salud, en su reporte mundial *"Connecting for Health: Global Vision, Local Insight"*[1], afirmó que las TIC eran el instrumento clave para alcanzar los objetivos del sistema de salud, ya que su uso en la comunicación, el procesamiento y transmisión de información a través de medios electrónicos, mejora la prestación de los servicios de salud a los usuarios[2]. Con el tiempo este tipo de herramientas tecnológicas han ampliado su alcance y han introducido el concepto "mHealth" o salud móvil, definido por la Organización Mundial de la Salud 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*"[3]. El concepto mHealth pretende eliminar las limitaciones existentes en los sistemas tradicionales de salud, como el acceso en tiempo real a los servicios y a la información médica de un paciente.

Durante la última década, el crecimiento de los dispositivos móviles ha alimentado el interés en utilizar la tecnología móvil, específicamente aplicaciones móviles para la atención médica en poblaciones rurales, donde existen necesidades básicas de salud que no pueden ser cubiertas ya sea por las condiciones geográficas, sociales y/o económicas[4]. En el 2015, el Institute for Healthcare Informatics (IMS), en su informe "Patient Adoption of mHealth", estimó que existían 165.000 mHealth Apps en el mercado mundial, en las plataformas de distribución Apple iOS y Google App, agrupadas principalmente en dos categorías: Bienestar general y gestión de la enfermedad[5]. Aunque se ha presentado un crecimiento significativo desde el 2013 en el número de Apps mHealth disponibles para los consumidores, su adopción ha sido limitada por parte de usuarios, profesionales de la salud y proveedores, que consideran que las Apps tiene falencias como: conectividad limitada y falta de integración con los sistemas de salud, bajos niveles de confidencialidad de datos, privacidad, seguridad e incertidumbres regulatorias y falta de evidencia científica que midan la eficacia de las aplicaciones[5]. En el 2016, la compañía ARXAN, en su informe anual de seguridad de las aplicaciones[6], encontró que la mayoría de las esas contienen vulnerabilidades de seguridad críticas y el 83% de las aplicaciones móviles analizadas y probadas por los órganos reguladores, son tan vulnerables como otras aplicaciones móviles, especialmente por la falta de suficiente protección de la capa de transporte.

No obstante, los principales organismos reguladores en Estados Unidos y la Unión Europea se siguen esforzándose por determinar parámetros de seguridad y privacidad que deben cumplir los fabricantes de aplicaciones mHealth. En el caso de la entidad Food and Drug Administration - FDA, mediante el documento "Mobile medical applications: Guidance for food and drug administration Staff"[7], se definió el concepto de aplicación médica móvil y se estableció los tipos de aplicaciones a reglamentar y supervisar con base a su funcionalidad. En el 2014, la Unión Europea presentó su plan de acción para la salud electrónica 2012-2020, a

través del "Libro verde sobre salud móvil"[8], mediante este material se promovió el desarrollo de mecanismos para garantizar la protección de los datos sanitarios. Los organismos reguladores han determinado que la principal limitación que tienen las mHealth Apps es la falta de convergencia normativa internacional, que permita a todos los desarrolladores, los profesionales sanitarios, las empresas, entre otros actores, evaluar, supervisar y controlar la producción y distribución de estas herramientas.

Bajo el interés de fomentar la producción de mHealth de calidad, investigadores han propuesto recomendaciones que satisfacen la legislación de seguridad y privacidad actual. Martínez *et al.,*[9] presentó algunos requisitos legales que permiten mantener la seguridad y privacidad de la información y que se encuentran organizados en las siguientes categorías: cobertura de la información de los pacientes, requerimientos y métodos utilizados para recoger la información, requisitos de consentimiento, retención de datos, seguridad durante la adquisición, transmisión y almacenamiento de los datos y obligaciones de notificación. Arora *et al.,*[10] analizaron los factores de riesgo en la salud móvil y plantearon posibles soluciones para mitigarlos durante los procesos de identificación, autenticación, trasmisión de la información y control de acceso. Con respecto a los requerimientos de Calidad de Servicio (QoS) Meraz *et al*.,[11] enfatizan en la importancia de evaluar los parámetros QoS durante la transmisión de la información, debido a que si las herramientas y/o plataformas mHealth no proporcionan respuestas rápidas y eficientes en términos de retransmisiones y consumo de ancho de banda, se pueden generar retrasos en la trasmisión, pérdida de información y denegación de servicios. Hechos que podrían poner en riesgo la salud del paciente.

Aunque las recomendaciones proporcionadas por los diferentes investigadores son viables y cubren algunos aspectos de seguridad, se evidencia la falta de un mecanismo que evalúe tanto los requerimientos legales como los funcionales de las aplicaciones. Motivos que justificaron la creación de un método para evaluar los parámetros de seguridad y calidad de servicio QoS de aplicaciones móviles para la salud, de acuerdo a su categorización y funcionalidad presentado en este trabajo.

Inicialmente el modelo categoriza la aplicación móvil en relación a los criterios funcionales, tecnológicos y de diseño. Posteriormente, se evalúa el cumplimiento de los requerimientos de seguridad, que fueron seleccionados previamente bajo el criterio de identificación de los riegos planteados para la seguridad informática de aplicaciones móviles en el proyecto OWASP *(Open Web Application Security Project)*[12]. Luego, se procede a implementar el modelo desarrollado, utilizando tres aplicaciones móviles de telemedicina, que realizan las funciones de monitoreo de frecuencia cardiaca, gasto energético y supervisión remota de sistemas de salud. Los resultados indicaron las deficiencias y vulnerabilidades que presentan las diferentes aplicaciones mHealth en temas de seguridad y calidad de servicio y proporciona posibles acciones correctivas y preventivas a desarrollar, con base a los factores de riesgo determinados.

Materiales y métodos

El tipo de investigación aplicada al modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles, es de tipo descriptivo ya que se detallan cada una las características que deben tener las aplicaciones móviles de salud para garantizar un nivel de seguridad óptimo. En el caso de esta investigación los autores utilizaron las siguientes fases para el desarrollo del modelo: Fase 1. Diseño del modelo de evaluación de requerimientos de seguridad y calidad de servicio. Fase 2. Validación de cada uno de los requerimientos de seguridad y calidad de servicio-QoS. Fase 3. Análisis y gestión de riesgos. Fase 4. Implementación del modelo.

Fase 1. Diseño del modelo de evaluación de requerimientos de seguridad y calidad de servicio-QoS

La elaboración del modelo de evaluación inicia con la categorización de las aplicaciones

mHealth, de acuerdo a su campo de aplicación y funcionalidad determinada por la OMS[13] y presentadas en la Figura 1.

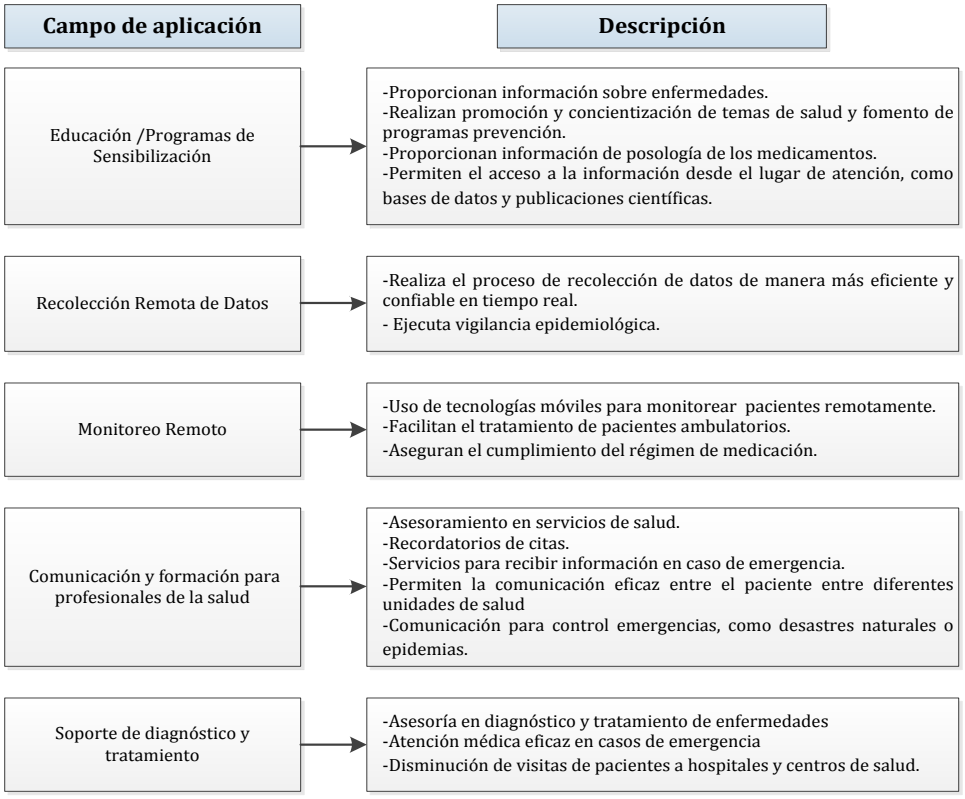

Figura 1. Categorización de aplicaciones mHealth

Fuente: The United Nations Foundation and Vodafone Foundation Technology Partnership

En el proceso de selección de requerimientos de seguridad, los autores tomaron como criterio la categorización de los riegos planteados en el proyecto OWASP. En el caso de los requerimientos de QoS, se seleccionaron los requisitos QoS end-to-end, determinados por la Unidad Internacional de Telecomunicaciones (UIT) para redes IP de telemedicina[14,15]. Los parámetros integrados al modelo son los siguientes:

Autenticación: Permite conocer la identidad de cada uno de los usuarios y dispositivos que pertenecen a una red de información[16]. Su importancia en el campo de las aplicaciones mHealth radica en la necesidad de garantizar que: 1. La monitorización se está realizando al paciente correcto, 2. La información sólo pueda ser accedida por el personal autorizado, iii. Se debe permitir el acceso seguro a cada uno de los equipos que hacen parte de la red de monitoreo[17].

Autorización: La importancia de un mecanismo de autorización, consiste en que los usuarios sólo pueden acceder a la información para la cual están autorizados[16].

Confidencialidad: Mediante este parámetro, se busca garantizar que la información clínica del usuario sólo sea conocida por él y por los usuarios a los cuales él autorice, por ejemplo personal médico o enfermeras[18].

Control de acceso: Este parámetro busca limitar el número de usuarios que acceden a la información, con el objetivo de no afectar la disponibilidad de los servicios prestados, implicando realizar previamente procesos de autenticación y autorización[10].

Integridad: Se enfoca en garantizar la no alteración de la información durante el proceso de transmisión, es decir que la información esté completa y que corresponda a la enviada por el emisor[17].

Disponibilidad: Además de proteger el sistema de un acceso no autorizado y de posibles robos o modificación de la información, se debe prestar igual importancia a la disponibilidad de la información clínica del paciente en caso de una emergencia, la cual deberá ser consultada por el personal médico para prestar un servicio adecuado al usuario y/o para detectar posibles riesgos en contra de su salud[19].

Interoperabilidad: Se refiere a todos los elementos que conforman el sistema, los cuales deben estar regidos bajo una serie de parámetros que permitan la comunicación entre ellos y el uso de protocolos que faciliten la comprensión de la comunicación entre las aplicaciones y el sistema de información[20].

En el proceso de interoperabilidad e intercambio de información, es importante que los sistemas de información cumplan los requerimientos legales para el manejo de información médica. Los parámetros o métricas QoS que se evalúan primordialmente en aplicaciones para la salud se presentan en la Tabla 1[19,21-23].

Tabla 1. Parámetros QoS para aplicaciones mHealth

Tipo de servicio	Medio	Aplicación	Aplicación en tiempo real	Volumen		Tiempo		Precisión		Seguridad	
				Tasa de transmisión de datos (kbps)	Througput	Retardo (ms)	Jitter (ms)	Tasa de pérdida de datos	Requerimiento de ancho de banda	Confiabilidad	Seguridad de tráfico de flujo
Monitoreo Remoto y Recolección de datos	Datos	Telemetría	Sí	<28.8	Bajo	<250	<100	0	2K-52M	Es necesario tener un nivel alto de fiabilidad	La integridad es el principal requisito
Comunicación y formación	Video	Video Broadcasting	Si	4000 -60000	Alto	<150	<100	<0.0001%	-	La fiabilidad es Importante pero no crítica	Autenticación y confidencialidad Son los principales requisitos.
	Audio	Audio Broadcasting (voz)	Si	abr-26	Alto	<150	<100	<0.1%	60-80 Kbps		
	Datos	Email	No	<30.5		<400	N/A	0	> 32 kbps		
	Datos	Web-browsing	No	< 30.5	Alto	< 400	N/A	0	< 30.5 Kbps	La confiabilidad es importante, pero no crítica	Autenticación, integridad y confidencialidad son obligatorios
	Audio	VoIP	Si	500		150 -240 downlink 200 uplink	100–300	0.01%	> 16 kbps	Es necesario el cumplimiento del estándar ITU-T H.323	
Soporte de diagnóstico y tratamiento	Video	Alta calidad de video para diagnóstico	Si	640 - 5000 (MPEG-4)	Alto	<250 E2E	100–300	0,01%	10 kb/s–1 Mb/s	La fiabilidad es Importante pero no critica. Es Recomendable utilizar los estándares UIT-T e ISO / IEC JTC,UIT-T H.262 o MPEG-2,UIT-T H.264	Autenticación y confidencialidad son los principales requisitos
	Audio	Audio para diagnóstico	Si	32-384 (MPEG-1)	Alto	150-400		0,01%			
	Datos	Imagen para diagnóstico	No	<1000		~10000	N/A	0		Es recomendable utilizar los estándares ISO/IEC JTC1,ITU-T T.81,ITU-T T.800 JPEG-2000	
	Datos	FTP	No	16.99	Alto	177.6	100–300	0	64 kbps		
Educación /Programas de Sensibilización	Audio, video	Investigación conversacional y educación	Si			<150 E2E Para audio		<3% PLR audio			
						<250 E2E Para video		<1% PLR Video			
	Datos, Imágenes	Investigación y la educación interactiva	No			<300 ida y vuelta		1% PLR			

La medición y evaluación de los parámetros de QoS en las aplicaciones mHealth está condicionada por diferentes factores. En el caso de las aplicaciones utilizadas para apoyar los servicios de monitoreo remoto y recolección de datos, la evaluación depende de los siguientes componentes: tiempo de aplicación del servicio (puede ser en tiempo real o no), cantidad de transmisión de datos, estado clínico del paciente, contexto de locación y tiempo para la prestación del servicio. Es necesario identificar si el servicio que presta la App se enfoca en cubrir emergencias o no[23].

La determinación de estándares de normalización y vigilancia para aplicaciones mHealth, es uno de los grandes retos que tienen a nivel mundial las instituciones de salud. La integración de las leyes y los estándares es importante en el modelo de selección, por lo que algunos de los más relevantes estándares y leyes de referencia fueron organizadas en la Tabla 2.

Tabla 2. Estándares regulatorios para información médica en medios electrónicos

	Requerimientos de seguridad				
Regulador	**Control de acceso**	**Almacenamiento**	**Conectividad**	**Análisis de vulnerabilidades**	**Interoperabilidad**
HIPAA (Health Insurance Portability and Accountability)	1. Establece sistemas de autenticación e identificación para acceder a la información 2. Exige contraseña o pines de acceso		Determina el uso de cifrado para la información médica mientras es transmitida	Establece protocolos para garantizar la confidencialidad de la información	
COBIT (Control Objectives for Information and Related Technology)	Limita los intentos de acceso	Reglamenta el proceso para realizar copias de seguridad de la información almacenada	Reglamenta la utilización de protocolos de seguridad durante el envío de datos		
CALDICOTT	Determina el uso de privilegios de usuario para acceder a la información médica	Establece el uso y manejo de base de datos para información médica	Establece firma asincrónica durante la transmisión de la información		Interoperabilidad entre sistemas nuevos y sistemas existentes
HL7 (Electronic Health Information Systems)			Establece el uso de formatos EDI y XML para envío de mensajería clínica		
DICOM Digital Imaging and Communications in Medicine por NEMA – National Electrical Manufacturers Association	Describe los mecanismos de autenticidad	Define perfiles de acceso y protección durante el almacenamiento de imágenes	1. Define esquemas de anonimato, cifrado y compresión de datos 2. Establece mecanismos para incluir una firma digital en el conjunto de datos asociado a imágenes	Especifica perfiles y políticas de seguridad, para imágenes	

Finalmente, el modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio QoS, desarrollado en esta investigación y presentado en la Figura 1, establece un proceso sencillo que facilita la evaluación de las aplicaciones mHealth (Figura 2).

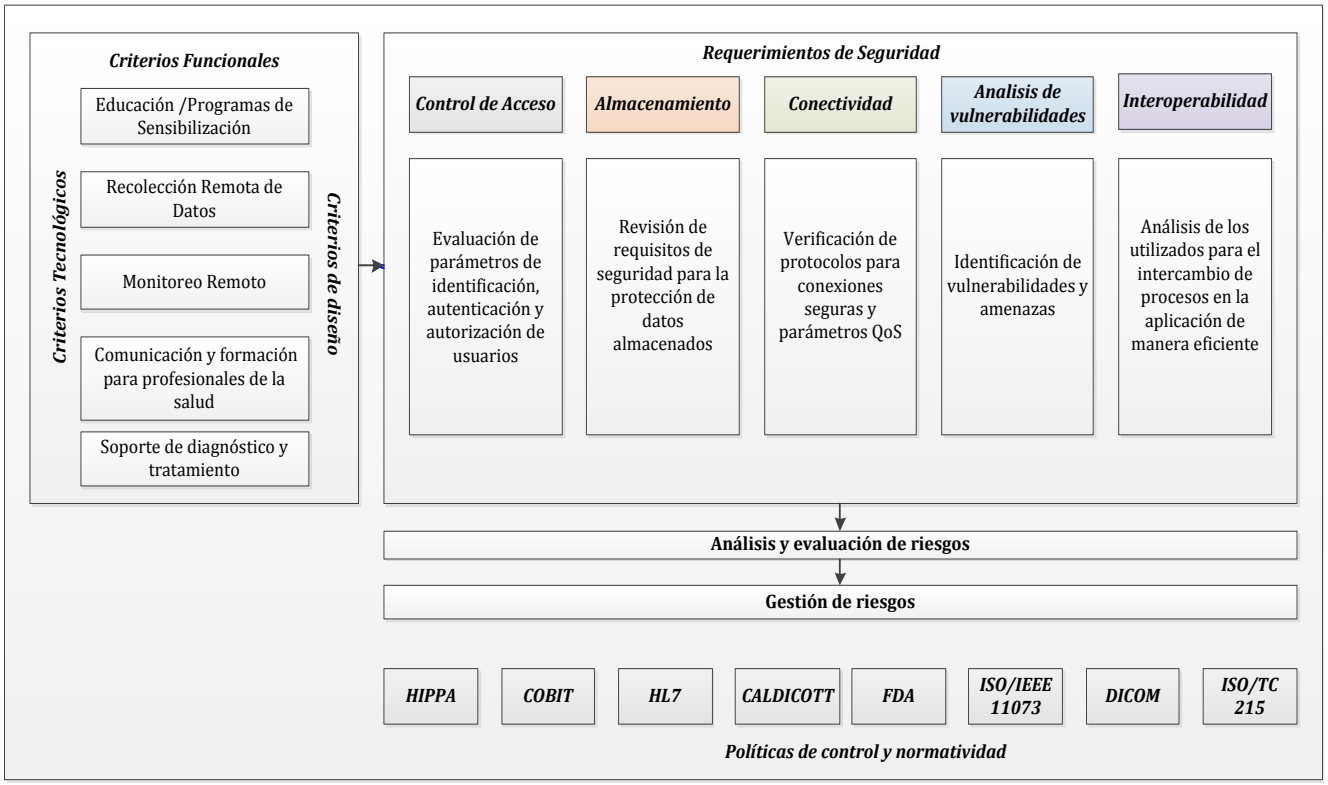

Figura 2. Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio-QoS

Fase 2. Validación de los requerimientos de seguridad en el modelo

Antes de utilizar el modelo propuesto en las aplicaciones móviles para la salud es necesario comprender cada una de las etapas de evaluación de los requerimientos presentados en la Figura 2 y Figura 3, descritas a continuación:

- Control de acceso

El proceso de evaluación de control de acceso inicia con la identificación del tipo de usuario, determinado si es necesario o no autenticación para su ingreso, mediante mecanismos de autenticación como: usuario y contraseña, patrón biométrico, tarjetas inteligentes, certificados electrónicos, token de seguridad, entre otros.

Posteriormente, se procede a validar el usuario examinando si la aplicación utiliza privilegios de usuario que pueden ser globales o individuales. Generalmente los usuarios se clasifican en: invitados, usuarios, usuarios interactivos, usuarios autenticados y administradores.

El proceso de validación de control de acceso termina cuando se comprueba que se emitió una autorización a los usuarios de forma segura. Es importante aclarar que el modelo contempla dos tipos de acceso, acceso básico o acceso privilegiado y seguro, dependiendo de los criterios de funcionalidad, diseño y tecnología de la aplicación.

- Almacenamiento

Los sistemas de almacenamiento que utilizan las aplicaciones móviles se evalúan bajo los criterios de funcionalidad de la aplicación y de la normatividad vigente. El proceso inicia con la identificación del tipo de almacenamiento, en caso que se utilice un almacenamiento local se analiza si este garantiza la disponibilidad de la información. Se verifican los siguientes factores: la conexión de la base de datos - BD con la aplicación, con el objetivo de mantener actualizada la información del paciente y mejorar el rendimiento de las consultas. Luego se analiza los mecanismos de control de acceso a la BD, los mecanismos para la protección de copias de

seguridad y las técnicas o mecanismos de encriptación de los datos durante el desarrollo de las copias de seguridad.

La entidad CALDICOTT[24-27] establece el uso de bases de datos como mecanismo de almacenamiento de información médica para garantizar la disponibilidad de la información y minimizar la pérdida de datos por extravío del dispositivo o desbordamiento de memoria del dispositivo. En el proceso de control de acceso a la base de datos, DICOM recomienda definir perfiles para los usuarios autorizados, estableciendo funciones de restricción en la administración de la base de datos y en la realización de copias de seguridad realización de copias de seguridad según COBIT.

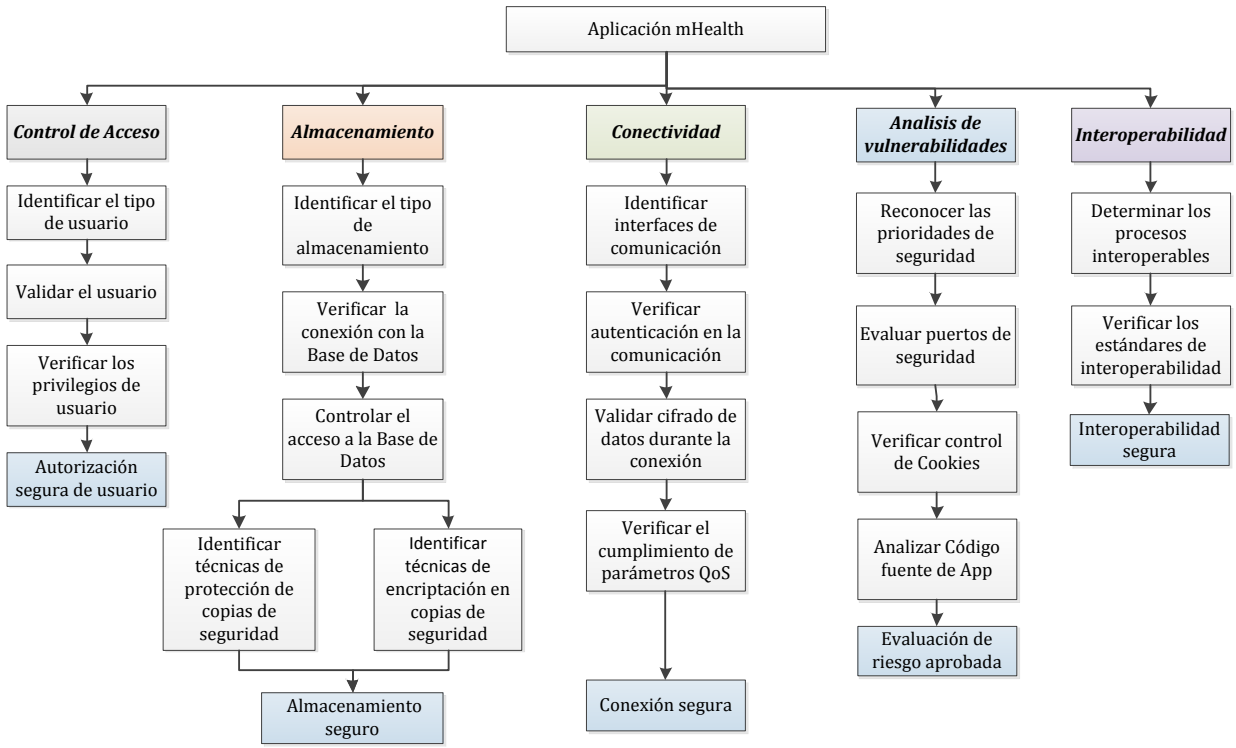

Figura 3. Proceso de evaluación de los requerimientos de seguridad

- Conectividad

Durante el proceso de verificación del cumplimiento de los parámetros de transmisión de la información se evalúa el uso de protocolos de conexión segura y cumplimento de los parámetros QoS, para mantener la confidencialidad e integridad de la información de los usuarios.

Las aplicaciones mHealth utilizan en mayor proporción redes inalámbricas que se caracterizan por presentar un mayor índice de vulnerabilidades durante el proceso de transmisión, en comparación con las redes cableadas, a causa de este riesgo se hace indispensable revisar la autenticación de la conexión en redes privadas y/o públicas. Simultáneamente, se debe evaluar el uso de protocolos criptográficos en la transmisión de información asegurando la protección de la información durante la conexión de las aplicaciones mHealth con la red. Los protocolos de mayor uso son: Secure Sockets Layer –SSL, que proporcionan los certificados digitales durante la comunicaciones segura en internet[28] y el protocolo Transport Layer Security –TLS[29], el cual proporciona la seguridad en la capa de transporte.

- Análisis de vulnerabilidades

El uso de técnicas de prevención de ataques permite proteger la información del usuario contra hackers. Para realizar el análisis de vulnerabilidades, se identifican las prioridades de seguridad que tiene la aplicación posteriormente, se valida utilizando técnicas de prevención como: evaluación de puertos, control de cookies y análisis de código utilizando software especializado para realizar pruebas de penetración y auditorías de seguridad en un entorno controlado.

- Interoperabilidad

La interconexión entre diferentes departamentos de las instituciones de salud, ha creado la necesidad de implementar procesos interoperables para el manejo de sistemas de archivo de imágenes, radiología, laboratorio e historias clínicas electrónicas. La administración de estos procesos requiere el uso de estándares de seguridad informáticos establecidos por las entidades regulatorias como el DICOM, el HL7 entre otras.

Fase 3. Análisis y evaluación de riesgos en el modelo

Para realizar el proceso de análisis y evaluación de riesgos en la seguridad de las aplicaciones mHealth, es necesario cuantificar la gravedad y probabilidad de ocurrencia de los riesgos a través de los valores primarios de calificación de impacto[30,31], como se señalan en la Tabla 3. Después de evaluar los riesgos se requiere tomar acciones y establecer políticas que permitan controlar y mitigar las amenazas detectadas para cada una de las aplicaciones, mediante la gestión de riesgo.

Tabla 3. Evaluación y análisis de riesgos en aplicaciones mHealth

Probabilidad	**Impacto**				
	Grave (5)	Medio alto (4)	Medio bajo (3)	Bajo (2)	Insignificante (1)
Alto (3)	Extremo (15)	Elevado (12)	Moderado (9)	Soportable (6)	Admisible (3)
Medio (2)	Elevado (10)	Moderado (8)	Soportable (6)	Soportable (4)	Admisible (2)
Bajo (1)	Soportable (5)	Soportable (4)	Admisible (3)	Admisible (2)	Admisible (1)

Fuente: Microsoft B. Guía de administración de riesgos de seguridad[31]

En esta fase el evaluador toma acciones preventivas o correctivas de acuerdo al valor de gestión de riesgo obtenido en el proceso anterior. Si el valor de gestión de riesgo se encuentra entre 1-3 se recomienda asumir la vulnerabilidad, entre 4-6 se recomienda reducir la vulnerabilidad a través de mecanismos de protección, entre 7-9 se recomienda asumir, evitar o compartir la vulnerabilidad, entre 10-12 se recomienda evitar la vulnerabilidad y entre 13-15 se recomienda evitar al máximo la vulnerabilidad.

Fase 4. Validación del modelo

Para validar la estructura y la funcionalidad del modelo, los autores utilizaron tres aplicaciones móviles de telemedicina que hacen parte del sistema de información y supervisión en salud de los grupos Gissic-Tigum de la Universidad Militar Nueva Granada.

Resultados

Como resultado de este trabajo de investigación los autores proporcionan un modelo para evaluar los requerimientos de seguridad y calidad de servicio-QoS de aplicaciones móviles para la salud. Este modelo se apoya en el análisis de los estándares y normas de la seguridad de la información emitidas por entidades regulatorias.
En términos del diseño del modelo su principal aporte corresponde a la facilidad de comprensión y la concreta selección de los requerimientos de seguridad y calidad de servicio QoS para cada una de las aplicaciones móviles de acuerdo a los criterios de funcionalidad, tecnológicos y de diseño. Respecto al proceso de validación de requerimientos el modelo presenta una estructura clara que ayuda a identificar los incumplimientos de los requerimientos con base en los factores de riesgo determinados por OWASP. Posteriormente, en la etapa de análisis y evaluación de riesgos el modelo proporciona posibles acciones a realizar en caso que se presenten incumplimientos en los requerimientos y que pongan en riesgo la seguridad de la información que manejan las aplicaciones móviles.

Como resultados específicos, en la fase de implementación del modelo se analizó la seguridad de tres aplicaciones móviles que fueron clasificadas por el modelo en las categorías de: App 1. Monitoreo remoto, App 2. Recolección de datos y App 3. Soporte de diagnóstico y tratamiento. Durante el proceso de validación de los requerimientos de seguridad en las aplicaciones, se encontraron los hallazgos presentados en la Tabla 4 y que se describen a continuación: En la aplicación número 1, se presentó incumplimientos en los requerimientos de control de acceso y almacenamiento. En el caso del requerimiento de control de acceso, este hallazgo representa un impacto con calificación extrema de 15 puntos, debido a que incumple con las normatividad establecida por HIPAA para manejo de información médica a través herramientas tecnológicas. El modelo considera que se debe evitar al máximo este tipo de vulnerabilidad implementando mecanismos de autenticación.

Tabla 4. Validación del modelo utilizando mHealth Apps

Categoría de la aplicación	Requerimientos de Seguridad				
	Control de Acceso	**Almacenamiento**	**Conectividad**	**Análisis de Vulnerabilidades**	**Interoperabilidad**
App 1. Monitoreo remoto	Falta de mecanismos de autenticación (15)	El almacenamiento Local no garantiza la disponibilidad de la información (12)	N/A	N/A	N/A
App 2. Recolección de datos			No implementa autenticación en redes públicas y privadas (6). No utiliza protocolos seguros de transporte (12).	La aplicación no tiene medidas para proteger la información de amenazas (8).	N/A
App 3. Soporte de diagnóstico y tratamiento		La aplicación no realiza copia de seguridad de la BD (10).	No utiliza protocolos seguros de transporte (12). La aplicación no encripta los datos antes de ser enviados (12).	La aplicación no tiene medidas para proteger la información de amenazas (8).	

En caso del almacenamiento local el riesgo es considerado como elevado con una calificación de 12 puntos, ya que este hallazgo que cumple de los pilares de la seguridad de la información y se compromete la información del usuario en caso de una emergencia y/o pérdida del dispositivo. El modelo recomienda evitar esta vulnerabilidad utilizando bases de datos como sistema de almacenamiento de acuerdo a lo estipulado por CALDICOTT[27].

La aplicación número 2, incumple los requerimientos de seguridad de conectividad al no implementar procesos de autenticación en redes públicas y privadas. Este riesgo tiene una calificación soportable de 6 puntos y se sugiere reducir este tipo de vulnerabilidad, para garantizar niveles altos de seguridad en la información durante la conectividad a las redes. Otro hallazgo es la falta de uso de protocolos seguros de transporte, el cual tiene un impacto elevado con una calificación de 12 puntos. La importancia del uso de estos protocolos radica en el aporte de nivel de seguridad durante los procesos de transmisión de la información.

En el caso de la aplicación 2, se presentan falencias en el requerimiento de análisis de vulnerabilidades, debido a que esta aplicación no utiliza mecanismos para evitar amenazas de seguridad. Se considera un riesgo moderado con una calificación de 8 puntos. Se recomienda asumir la vulnerabilidad o evitarla, incluyendo mecanismos que bloquen cualquier tipo de ataque.

Finalmente, la evaluación de la aplicación 3, presentó 3 incumplimientos a los requerimientos de almacenamiento, conectividad y análisis de vulnerabilidades. En el requerimiento de almacenamiento, la aplicación no realiza copia de seguridad de la BD, este hallazgo tiene una calificación de elevado con 10 puntos y se recomienda establecer un procedimiento para realización de copias de seguridad reglamentadas por las políticas de COBIT. El incumplimiento del requerimiento se debe a la falta de protocolos de transporte y mecanismos de encriptación que facilita los ataques XSS, Freak-SSL/TLS, SSL-strippping.

Discusión

Con el objetivo de mejorar la calidad de los servicios de salud con mayor demanda, minimizar errores médicos y disminuir costos innecesarios, los sistemas de salud han adaptado herramientas tecnológicas móviles como dispositivos médicos para adquirir, registrar y controlar variables médicas de un paciente. El auge de las mHealth Apps, en las diferentes plataformas de distribución en la categoría de fitness y salud, ha puesto en duda la calidad de estas Apps en materia de seguridad, contenidos y funcionalidad. Analistas consideran que muchas de las mHealth Apps son de dudosa fiabilidad y la mayoría no se encuentran integradas al sistema sanitario. El crecimiento desordenado de estas herramientas ha conllevado a la elaboración de mecanismos de regulación para garantizar la seguridad del usuario y de la información que estas registran. Aunque su falta de convergencia normativa internacional genera poco uso por parte de los desarrolladores de software. Adicionalmente, no existe una única entidad internacional que avale o certifique la funcionalidad de las aplicaciones y la calidad y seguridad de la información.

Las aproximaciones a la realización de esta función se cumplen por entidades como la FDA, que se encarga de regular algunas aplicaciones médicas móviles, definidas en sus políticas. El instituto IMS Healthcare Informatics, a través de su reporte[5], incluye la evaluación del valor potencial que tienen las Apps en el mercado de la salud. Por su parte, el directorio europeo de aplicaciones de la salud 2012-2013[32] presenta algunas aplicaciones seguras y reguladas por el contorno europeo, que fueron recomendadas por grupos de pacientes o consumidores, no obstante, esta entidad no establece los criterios de selección, ni los parámetros con los que se analizó la seguridad y calidad de estas Apps. En el caso de la Unión Europea, a través del libro verde sobre la salud móvil, analiza las barreras existentes para la implantación móvil, dentro de la que se encuentran la falta de confianza por parte del personal médico, las garantías de seguridad de datos de los usuarios y el adecuado funcionamiento de estas herramientas tecnológicas. España como incentivador de mHealth Apps ha propuesto un distintivo de AppSaludable[33] como estrategia para reconocer la calidad y seguridad de las aplicaciones de salud, este proyecto analiza el diseño, la calidad y seguridad de la información, la prestación del servicio y la confidencialidad y privacidad de la información. Si bien abarca una cantidad de requerimientos de seguridad deja por fuera el análisis de los requerimientos de almacenamiento e interoperabilidad entre la aplicación y el sistema. The App intelligence[34] presenta "las 50 mejores Apps de salud en español", con el objetivo de ser punto de referencia para la selección de Apps que tiene la más alta calidad bajo criterios de selección como: contenido riguroso y de calidad, diseño y experiencia de uso, reconocimiento y premios, utilidad. Estos criterios llegan a ser subjetivos y no proporcionan todos los niveles de seguridad y calidad que requiere la información del usuario.

El enfoque que presenta el modelo propuesto en esta investigación para evaluar la seguridad, privacidad y calidad de servicio de las aplicaciones mHealth, aporta una gran cobertura a todos los aspectos de la seguridad, soportado por un análisis amplio de los estándares y normas internacionales vigentes para la salud móvil, pero el mayor aporte del modelo es ser un facilitador en la evaluación de aplicaciones en desarrollo o terminadas.

Conclusiones

La obtención de un modelo funcional que permita la evaluación de los requerimientos de seguridad y calidad de servicio en aplicaciones mHealth, proporciona estándares de confianza en la inclusión de tecnologías de información en los sistemas de salud y ofrece una guía práctica, que facilita la identificación de posibles factores de riesgo para la confidencialidad, disponibilidad e integridad de información médica de los usuarios.

El modelo desarrollado en esta investigación contempla un escenario general, en el que se definen los requerimientos de seguridad informática, que son susceptibles a los ataques informáticos y que se encuentran en la lista OWASP. Este modelo se caracteriza por incorporar una categorización de las aplicaciones mHealth bajo criterios técnicos, de funcionalidad, diseño, personalizando el análisis y garantizando el cubrimiento de los requisitos indispensables en cada aplicación.

Igualmente, el modelo es una herramienta que apoya a los tomadores de decisión a definir mejoras en la aplicación para garantizar la seguridad del usuario y de su información.

Agradecimientos
Los autores agradecen a la Universidad Militar Nueva Granada, por la financiación del proyecto de investigación INV-ING-2108 y a los grupos de investigación GISSIC y TIGUM por su contribución al desarrollo de modelo propuesto.

Conflicto de intereses: Ninguno declarado.

Referencias

1. Dzenowagis J, Kernen G. Global Vision, Local Insight: Report for the WSIS. Geneve: WHO; 2005;1-41.
2. Bukachi F, Pakenham-Walsh N. Information technology for health in developing countries. Chest. 2007;132(5):1624-30.
3. World Health Organization. New horizons for health through mobile technologies. Geneve: WHO; 2011;3.
4. Engle KL, Plourde KF, Zan T. Evidence-based adaptation and scale-up of a mobile phone health information service. MHelth Journal. 2017;3(3):1-9.
5. Aitken M. Patient Adoption of mHealth. USA: IMS Institute for Healthcare Informatics; 2015.
6. ARXAN. Arxan's 5th Annual State of Application Security Report Reveals Disparity between Mobile App Security Perception and Reality. USA: ARXAN; 2016. p. 2-6. Available from: https://www.arxan.com/2016/01/12/arxans-5th-annual-state-of-application-security-report-reveals-disparity-between-mobile-app-security-perception-and-reality/
7. USA Food Drug Adm. Guidance for Industry and Food and Drug Administration Staff [Internet]. USA: USA Food Drug Adm; 2016. p. 1-44. Available from: https://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf
8. Comisión Europea. Libro Verde: sobre sanidad móvil. Bruselas: CE; 2014.
9. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and Security in Mobile Health Apps : A Review and Recommendations. J Med Syst. 2015;39(1):181.
10. Arora S, Yttri J, Ph D, Nilsen W. Privacy and Security in Mobile Health (mHealth) Research. Alcohol Res. 2014;36(1):143-51.
11. Sanchez M, Leyva A, Gonzalez S. Quality of Service in Wireless Technologies for mHealth Service Providing. Mobile Health. 2015;5:971-89.
12. OSWAP. Top 10 Mobile Risks. United States: OSWAP; 2012.
13. Vital Wave Consulting. MHealth for Development: The Opportunity of Mobile Technology for Healthcare in the Developing World. Washington and Berkshire: Foundation Vodafone, Foundation Partnership; 2009.
14. Unión Internacional de Telecomunicaciones. Recomendación UIT-t p.800: Métodos de determinación subjetiva de la calidad de transmission. Ginebra: UIT; 1996.
15. Unión Internacional de Telecomunicaciones. Recomendación UIT-T G.1010: Categorías de calidad de servicio para los usuarios de extremo de servicios multimedios. Ginebra: UIT; 2001.
16. Islam SMR, Kwak D, Kabir H. The Internet of Things for Health Care : A Comprehensive Survey. IEEE Access. 2015;3:678-708.
17. Kotz D. A threat taxonomy for mHealth privacy. Bangalore: IEEE; 2011. p. 1-6.
18. U.S. Department of Health and Human Services. Recommendations on Privacy and confidentiality, 2006-2008. USA: US Dep Heal Hum Serv; 2009.
19. Goncalves F, Macedo J, Nicolau M, Santos A. Security Architecture for Mobile E-Health Applications in Medication Control. USA: Software, Telecommun Comput Networks (SoftCOM), 2013 21st Int Conf on IEEE; 2013;1-8.
20. Payne J. The State of Standards and Interoperability for mHealth among Low- and Middle-Income Countries. USA: The mHealth Alliance; 2013. p. 48.
21. Skorin-Kapov L, Matijasevic M. Analysis of QoS requirements for e-Health services and mapping to evolved packet system QoS classes. Int J Telemed Appl. 2010;2010:1-19.

22. Alinejad A, Philip N, Istepanian RSH. Mapping of multiple parameter m-health scenarios to mobile WiMAX QoS variables. Proc Annu Int Conf IEEE Eng Med Biol Soc EMBS. 2011;15:32-5.
23. Gállego JR, Hernández-Solana Á, Canales M, Lafuente J, Valdovinos A, Fernández-Navajas J. Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel. IEEE Trans Inf Technol Biomed. 2005;9(1):13-22.
24. Guillen E, Ramirez L, Estupiñan E. Análisis de seguridad para el manejo de la información médica en telemedicina. Cienc E Ing Neogranadina. 2011;21(2):57-89.
25. Gutiérrez-Martínez J, Núñez-Gaona MA, Aguirre-Meneses H, Delgado-Esquerra RE. Implementación de la seguridad en el manejo de las imágenes médicas. Investig en Discapac. 2014;3(4):177-84.
26. H-Dolin R, Alschuler L, Boyer S, Calvin B, M-Behlen F, V-Biron P, et al. Model Formulation: HL7 Clinical Document Architecture, Release 2. JAMIA. 2006;13:30-9.
27. Crook MA. The Caldicott report and patient confidentiality. J Clin Pathol. 2003;56(6):426-8.
28. Freier A, Karlton P, Kocher P. The Secure Sockets Layer (SSL) Protocol Version 30. IETF. 2011;3:1-67.
29. Turner S. Transport layer security. IEEE Internet Comput. 2014;18(6):60-3.
30. Gómez R, Hernán D, Donoso Y, Herrera A. Metodología y gobierno de la gestión de riesgos de tecnologías de la información Methodology and Governance of the IT Risk Management. Rev Ing. 2010;31:109-18.
31. Microsoft. Guía de administración de riesgos de seguridad. USA: Microsoft; 2017. Available from: https://www.microsoft.com/latam/technet/recursos/migracion/srsgch00.mspx#ERC
32. Patient View. European Directory of Health Apps 2012-2013: A review by patient groups and empowered consumers. London: Patient View; 2013. 200 p.
33. Santillán A, Martínez J. Apps de salud: Nuevas herramientas para el cuidado del paciente cardiológico. Enferm Cardiol. 2015;(66):28-34.
34. The App intelligence. Informe 50 mejores Apps de Salud en español [Internet]. Madrid: The App intelligence; 2014. p. 4-8. Available from: http://boletines.prisadigital.com/Informe-TAD-50-Mejores-Apps-de-Salud.pdf