# When eHealth Meets the Internet of Things: Pervasive Security and Privacy Challenges (Cuando eHealth se Encuentra con el Internet de las Cosas: Seguridad Generalizada y Desafíos de Privacidad)

**Abstracto:**

Las tecnologías móviles de eHealth son cada vez más frecuentes tanto en el mundo personal como en el médico, ayudando a los profesionales de la salud a monitorear el progreso y la condición actual de los pacientes. Estos dispositivos a menudo recopilan, transmiten y analizan datos personales. Los datos sanitarios tienen requisitos rígidos de seguridad, confidencialidad y disponibilidad, mientras que la trazabilidad y el control del acceso, y la preservación a largo plazo también son muy deseables, especialmente cuando se exponen a entornos de computación en la nube. Este artículo explora algunos de los desafíos de seguridad y privacidad que enfrentan los dispositivos de salud electrónica actualmente. Se consideran las implicaciones legislativas de las violaciones de datos, así como la responsabilidad del proveedor de servicios. El trabajo también proporciona numerosas recomendaciones de seguridad y privacidad, con el fin de mejorar futuras implementaciones.

**Publicado en:**[2017 Conferencia internacional sobre ciberseguridad y protección de servicios digitales (ciberseguridad)](https://ieeexplore.ieee.org/xpl/conhome/8054574/proceeding)

**Fecha de la conferencia:** 19-20 de junio de 2017

**Fecha añadida a IEEE *Xplore* :** 19 de octubre de 2017

**Información del ISBN:**

**Número de acceso de INSPEC:** 17279309

**DOI:**[10.1109 / CyberSecPODS.2017.8074857](https://doi.org/10.1109/CyberSecPODS.2017.8074857)

**Editorial:**IEEE

**Lugar de la conferencia:** Londres, Reino Unido

**SECCIÓN I.**

## **Introducción**

Con el atractivo paradigma emergente de Internet de las cosas (IoT) y sus numerosas capacidades, IoT está ganando terreno en la industria, desde el seguimiento logístico hasta el dominio médico. Informes recientes de Cisco predicen más de 50 mil millones de dispositivos conectados para 2020, creando innumerables interacciones entre los dominios físicos y cibernéticos [1].

Los principales actores como Samsung, Sony y Apple ya han comenzado el desarrollo de diferentes dispositivos médicos conectados [2]. A través de sus pulseras y relojes inteligentes, estas compañías ya han podido analizar problemas básicos relacionados con la salud, como la cantidad de pasos, la frecuencia cardíaca y las calorías quemadas. Sin embargo, estas empresas también han adoptado el concepto de abordar problemas específicos relacionados con la salud con sensores IoT conectados, como detectores de accidentes cerebrovasculares conectados o servicios de atención médica conectados personalizados [2] [3]. Esta tendencia también ha sido seguida por las nuevas empresas, que en los últimos años han producido una gama de dispositivos inalámbricos de monitoreo conectados, como balanzas conectadas, monitor ECG / EKG, monitores de presión arterial y marcapasos, así como ropa inteligente [4].

A medida que los sensores de red inalámbrica y el IoT en eHealth se han vuelto cada vez más populares, es apropiado que los investigadores de seguridad investiguen su funcionamiento interno e identifiquen los desafíos futuros.

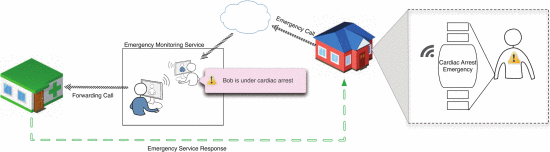
**SECCION II.**

## **Tecnologías de salud electrónica**

Con las nuevas tecnologías emergentes y las capacidades integradas, se han agregado sensores de todo tipo a los objetos cotidianos para hacerlos "inteligentes". Esta tendencia ha sido adoptada por el dominio médico. Los diagnósticos realizados por los médicos se producen a intervalos regulares para evaluar las condiciones del paciente y proponer el tratamiento adecuado. Sin embargo, las condiciones del paciente pueden cambiar rápidamente entre estos intervalos o pueden surgir y retroceder nuevos síntomas antes de que puedan registrarse. El IoT permite que los datos de los pacientes se recopilen continuamente y proporciona a los médicos un historial más completo, ayudándoles a establecer cronogramas y comprender eventos o anomalías. Permite la conectividad ubicua de los registros de salud electrónicos.

La reciente adopción generalizada de dispositivos eHealth IoT se atribuye principalmente a la prevalencia de los teléfonos inteligentes: el aumento de las capacidades de almacenamiento y la potencia de procesamiento permiten utilizar una amplia gama de aplicaciones complejas de forma portátil. Esto permite un monitoreo constante a nivel personal. Como se destaca por Hill et al. El creciente número de dispositivos de eSalud también se debe a la conveniencia: el usuario puede realizar un seguimiento de los posibles cambios en la frecuencia cardíaca, la hidratación, el uso de energía, la temperatura corporal y la fuerza muscular. Además, los datos se pueden procesar en tiempo real, proporcionando al usuario actualizaciones constantes sobre sus desempeños diarios. En su estudio, Hill et al. También destacó el aumento de dispositivos IoT eHealth de 400 millones en 2014 a 600 millones en 2019, así como los dominios donde se utilizan sensores de eHealth, como la autenticación biométrica,[5].

El IoT también permite el potencial de la gamificación en la atención médica, satisfaciendo las demandas de los clientes a través de las interacciones de las redes sociales. Como tal, las compañías de pulseras inteligentes han creado redes sociales en torno a estadísticas de calorías quemadas, número de pasos o entrenamiento colaborativo. Esto alienta a los usuarios a adoptar un mejor estilo de vida y a las empresas a desarrollar un mejor software de análisis que, por lo tanto, puede proporcionar niveles más altos de participación del usuario.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-fig-1-source-large.gif)

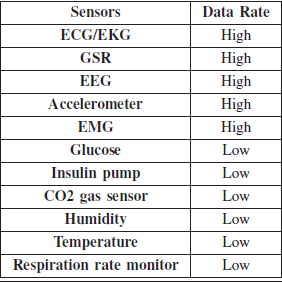
**Figura 1.** Respuesta de emergencia rápida usando iot para la atención médica generalizada

Existe una clara indicación en estudios previos de que involucrar al usuario en la gamificación ayuda a proporcionar mejores sistemas de atención médica y a empoderar a los pacientes [6]. La motivación de los pacientes a menudo se mantiene a través de logros personales y recompensas, así como la competencia [7]. Por lo tanto, es posible definir el campo de eHealth IoT en dos categorías distintas: monitoreo personal y monitoreo profesional.

### A. Monitoreo personal

Con un enfoque centrado en el cliente, el monitoreo del tiempo libre ofrece a los usuarios una gama de servicios, como análisis de datos, redes sociales y logros personales. Este tipo de monitoreo a menudo se ofrece a través de tecnologías portátiles, haciendo uso de la gamificación para impulsar la competencia. Las métricas proporcionadas por el monitoreo del tiempo libre son métricas básicas que permiten a los usuarios mejorar su estilo de vida [8].

**Tabla I** Tipos de sensores

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-1-source-large.gif)

B. Monitoreo profesional

Los dispositivos diseñados por y para profesionales de la salud tienen un enfoque centrado en la condición. Proporcionan a los médicos médicos datos de monitoreo relacionados con una o más afecciones graves. Los datos proporcionados por el monitoreo profesional tienen como objetivo proporcionar a los profesionales datos que salvan vidas, monitorear la condición del paciente y proporcionar métricas precisas. Este tipo de monitoreo se puede usar en un contexto de Monitoreo como servicio (MaaS), vinculando los dispositivos y los usuarios a los servicios de emergencia que brindan a los pacientes atención médica generalizada [9].

**SECCION III.**

## **Comunicación**

Los datos generados por los dispositivos de monitoreo personal a menudo se transmiten de forma inalámbrica a un teléfono inteligente, lo que le permite actuar como un relé entre los servidores de la empresa que brinda los servicios y los dispositivos portátiles. Esto permite además al usuario monitorear el desempeño y procesar los datos generados para un primer análisis. Cuando se transmiten a teléfonos inteligentes, los dispositivos portátiles a menudo usan Bluetooth Low Energy (BLE). Una vez procesados ​​previamente para el usuario, los datos se cargan a través del teléfono inteligente a un servidor distante, lo que permite a la empresa procesar datos a gran escala y proporcionar al usuario más información o mostrar los datos a través de servicios web.

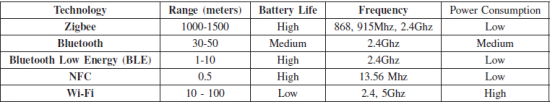
Los datos generados por dispositivos de monitoreo profesionales a menudo están conectados a Wi-Fi, lo que permite que los datos se transmitan como una transmisión. El flujo de datos se procesa y se transmite a los profesionales de la salud. El dispositivo de monitoreo también podría estar procesando datos en el sitio, lo que permite proporcionar al usuario servicios de emergencia como se muestra en la Figura 1. El dispositivo controla la actividad cardíaca de los usuarios; Cuando se detecta una falla, el problema se transmite automáticamente a un centro de llamadas de emergencia, lo que les permite proporcionar primeros auxilios y enviar los detalles a los servicios de emergencia para una respuesta rápida. Esto cambia la práctica sanitaria de un sistema centralizado a un sistema descentralizado [10]

Triantafyllidis et al. [11] propuso una red de sensores inalámbricos abierta y reconfigurable que permite monitorear pacientes, comunicándose con un teléfono inteligente conectado a servicios de emergencia. También se propone un modelo de seguridad similar en [12], sin embargo, el autor recomienda la redundancia de los servicios, utilizando sistemas móviles, así como sistemas basados ​​en satélites.

La Tabla I proporciona una serie de sensores para servicios de salud generalizados y sus velocidades de datos apropiadas [13].

* ECG / EKG proporciona servicios de atención médica con los datos del electrocardiograma del corazón del paciente, lo que les permite controlar la actividad eléctrica del corazón.
* **GSR** proporciona datos sobre el comportamiento galvánico de la piel que permite la correlación de los datos de presión arterial, frecuencia cardíaca y resultados de ECG / EKG.
* **EEG** proporciona datos relacionados con la actividad cerebral del paciente.
* **EMG** proporciona datos relacionados con las actividades eléctricas de los músculos.

**Tabla II**

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-2-source-large.gif)

Los datos proporcionados por todos estos diversos sensores pueden desempeñar un papel importante en el monitoreo de la salud y, a menudo, requieren hardware con capacidades de comunicación de alta velocidad, para registrar todos los eventos que ocurren.

La Tabla II resume las diferentes tecnologías de comunicación adaptadas a las redes inalámbricas de sensores, incluida la duración de la batería, el alcance y el consumo de energía [14].

### A. Monitoreo

Según lo descrito por Yuan et al. [15] El monitoreo de la atención médica a menudo se realiza a través de tecnologías web, lo que permite al usuario tomar el control, validar la información y revisar sus signos vitales en diferentes plataformas. Además, este tipo de diseño permite un fácil acceso remoto y puede estar disponible a través de navegadores web y aplicaciones móviles.

Este enfoque permite a los profesionales de la salud monitorear el progreso del usuario y actuar en caso de emergencia. Lee y col. propuso un enfoque para monitorear los datos de ECG / EKG de personas mayores y enviar los datos a un servidor web para su revisión inmediata por profesionales. Esto proporcionó la capacidad de activar una alarma y actuar en tiempo casi real [16].

Con sensores de salud ubicuos, numerosas tecnologías web están involucradas para mostrar datos al usuario final y proporcionarles resultados analíticos. La Figura 2 muestra un resumen de las diferentes tecnologías disponibles para crear una arquitectura eficiente para sensores de red inalámbrica.

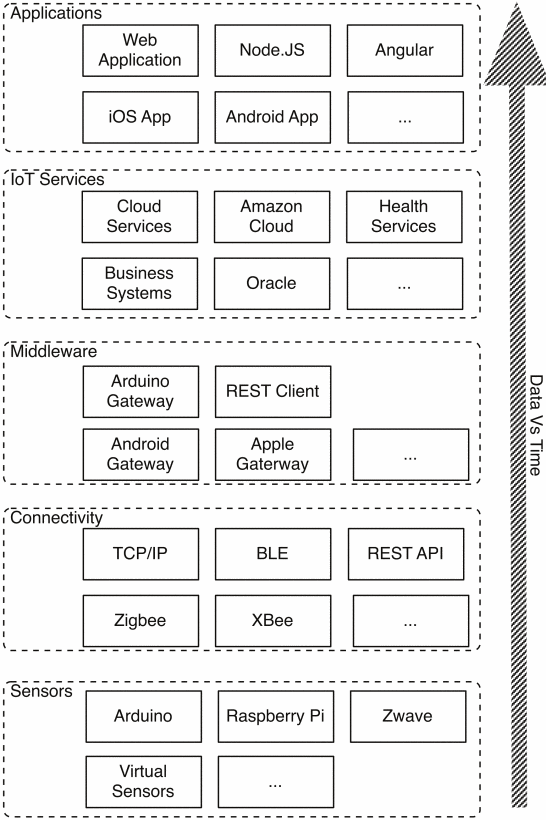
**SECCION IV.**

## **Desafíos de seguridad y privacidad**

Las topologías actuales están sujetas a una serie de limitaciones, como la potencia de procesamiento de los sensores [17] y la seguridad y privacidad de las arquitecturas.

Según lo declarado por Bellekens et al [18] y Adibi et al [14], los sensores actuales a menudo no incorporan mecanismos de seguridad y privacidad necesarios para el cifrado de extremo a extremo, entre los sensores y los servidores */* operadores. Los diferentes sensores utilizados para el monitoreo profesional y personal están diseñados sin tener en cuenta un aspecto de seguridad generalizado, y a menudo se puede considerar que es vulnerable a numerosos tipos de ataques o sujetos a fugas de datos [19].

Aunque se derivan varios beneficios del monitoreo de eHealth, existe la necesidad de un equilibrio entre los beneficios y la seguridad y privacidad del sistema ya que se transmiten datos confidenciales. La mayoría de los sistemas y dispositivos de eHealth disponibles transfieren sus datos a servidores remotos a través de Internet independientemente del medio (redes inalámbricas). Esto puede poner en riesgo los datos confidenciales durante la transferencia. Por ejemplo, ataques como espionaje, rastreo de paquetes y suplantación de identidad son posibles si los datos o el medio de comunicación no están bien protegidos. Una vez que ocurren estos ataques, la confidencialidad y privacidad de los datos se viola automáticamente.



**Figura 2.** Pila de sensores inalámbricos de aplicaciones, servicios, middleware y conectividad

### A. Amenazas y ataques de seguridad

Las redes inalámbricas de sensores pueden ser atacadas en los tres puntos débiles principales del sistema de monitoreo de eHealth; el dispositivo en sí, el enlace de comunicación y el servidor de destino. Diversas amenazas o ataques a la seguridad de la red que se analizarán en detalle en esta subsección, así como técnicas de mitigación.

#### Escuchar a escondidas los datos

Este es un ataque de red común; generalmente ocurre durante la transmisión de datos entre dos entidades de un sistema. El atacante puede interceptar información a medida que se transmite desde los sensores inalámbricos al servidor remoto. Esto se puede hacer suplantando paquetes ARP al enrutador y creando un ataque Man In The Middle (MITM). Una vez que ocurre este ataque, la privacidad del paciente se viola automáticamente.

#### Acceso a los datos

Esto ocurre cuando un atacante o una persona no autorizada accede a los datos médicos mientras se transfieren desde o hacia el servidor remoto. Una vez que obtienen acceso a los datos, pueden modificar, eliminar o incluso falsificar datos que conducen a registros de pacientes incorrectos y falsas alarmas. Esto también puede conducir a eventos de emergencia innecesarios. La modificación de los datos a resultados regulares cuando el paciente está en peligro también podría ocultar situaciones de emergencia, resultando en la muerte o una condición crítica. Además, el acceso a datos también cubre las infracciones de datos o los datos almacenados en carpetas públicas por un usuario legítimo.

#### Negación de servicio

En este caso, un atacante inundará los servidores remotos con solicitudes innecesarias que conducen a la interferencia o sobrecarga del sistema de monitoreo de salud. Una vez que esto ocurre, los datos autorizados del paciente no podrán llegar al servidor y esto puede prevenir o impedir el tratamiento rápido del paciente durante emergencias.

#### Falsificación de identidad de pacientes

Esto puede ocurrir principalmente en el extremo del sistema del paciente, donde otra persona usa los sensores y las lecturas se almacenan en el perfil del paciente autorizado. Esto puede conducir a muchas complicaciones, como datos médicos incorrectos en casos de emergencia. Además, tal ataque podría ocurrir si el "perfil" del paciente puede ser replicado (por ejemplo, ataque de repetición) [20].

#### Localización ilegal y seguimiento de actividad de pacientes

Algunos sistemas de monitoreo remoto de la salud toman diversos datos médicos, como la temperatura, la frecuencia cardíaca, la saturación de oxígeno, etc., así como las coordenadas de ubicación. Cuando un atacante puede acceder a esta información, puede usarla para rastrear la ubicación exacta de la persona y una vez que se conoce la ubicación, el paciente podría ser atacado o dañado físicamente. De acuerdo con Kargl et al. [21] las compañías de seguros médicos pueden abusar de estos datos para restringir los beneficios de salud a los pacientes que se consideran que tienen estilos de vida poco saludables (derivados de sus datos médicos) [18].

### B. Soluciones de seguridad para sistemas de monitoreo de salud

Siguiendo los problemas de seguridad y privacidad del sistema de monitoreo de eHealth discutidos anteriormente, esta sección explica en detalle varios mecanismos y estrategias que pueden adoptarse para prevenir los problemas de seguridad que puede enfrentar el sistema, ayudando a la adopción general de estos sistemas y garantizando la privacidad en sistemas de salud generalizados.

#### Cifrado

Este es un mecanismo de seguridad que se puede utilizar para garantizar la confidencialidad y la privacidad de los datos. El mecanismo ayuda a convertir los datos en información ilegible a medida que se pasa a través de la red. Por lo tanto, si un atacante puede interceptar la comunicación, los datos serán completamente ilegibles, evitando las escuchas. Se pueden implementar varios algoritmos simétricos y asimétricos para proporcionar cifrado en todo el sistema. Un ejemplo es la arquitectura de seguridad de TinySec que puede usarse para proporcionar autenticación a varios sistemas. Este sistema se ha utilizado en el pasado para proporcionar dispositivos médicos con un mecanismo de autenticación ligero pero fuerte [22].

#### Mecanismo de Autenticación

El mecanismo de autenticación puede garantizar que los datos del sensor médico que se registran se recopilan del paciente para el que se creó el perfil médico. Se pueden utilizar numerosos algoritmos, como las firmas digitales y los protocolos de desafío / respuesta, para garantizar que el paciente esté autenticado correctamente. Esto ayudará a prevenir ataques de suplantación de identidad en el sistema y garantizar la integridad de los datos. La autenticación también se puede lograr mediante el uso de la función hash proporcionada por TinySec. Además, los datos como las funciones de frecuencia cardíaca se pueden utilizar para proporcionar un mecanismo de autenticación presentado por Bao et al. [23] ; Esta técnica finalmente permite liberar al usuario de cualquier mecanismo de autenticación intrusivo.

#### Protección de integridad

Los componentes en los nodos del sensor pueden estar expuestos a alteraciones físicas en algunas situaciones. Para mitigar los ataques en un nivel lógico, Kargl et al. [21] proponen el uso de dispositivos resistentes a la manipulación pero describen esta solución como costosa. Otras alternativas, como el cifrado punto a punto, pueden ayudar a preservar la integridad de los datos. El sistema de fondo, por otro lado, debe diseñarse con un enfoque en la seguridad y la privacidad de los datos, incluidos servicios como sistemas de detección de intrusos, controles de acceso y seguridad física.

#### Control de acceso a datos

Controlar las entidades del sistema de monitoreo de salud que tienen acceso a datos médicos es crucial para garantizar la privacidad. Se pueden implementar varios controles de acceso a datos como el acceso basado en roles en el sistema para determinar quién puede modificar qué datos dependiendo del rol que desempeñan dentro del sistema de eHealth. Por ejemplo, no se debe permitir a todas las entidades editar los datos recopilados de los sensores, ya que puede provocar un mal uso de los datos o alteración de los datos, lo que lleva a falsas alarmas o complicaciones dentro del sistema.

#### Cortafuegos

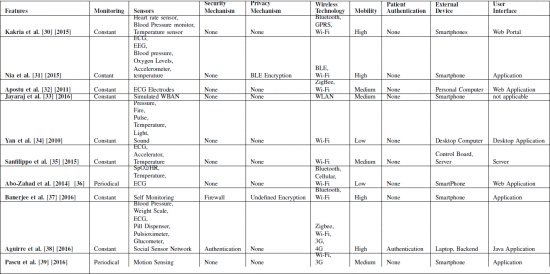
El uso de firewall y listas de control de acceso en los servidores remotos puede ayudar a prevenir muchos ataques, como ataques de denegación de servicio, y puede tener varios otros beneficios de seguridad. El firewall ayudará a monitorear y rastrear todo el tráfico que ingresa a la red. El cortafuegos también restringe a los usuarios malintencionados para obtener acceso al sistema.

**SECCION V.**

## **Requisitos de seguridad**

En los últimos años, la salud se ha convertido en un área prominente de trabajo, tanto para la academia como para la industria. Se han probado y desplegado diferentes tecnologías que proporcionan a los usuarios y al personal médico una gran variedad de datos. La Tabla III muestra el estado del arte. Como se muestra en la Tabla III, las diferentes implementaciones usan diferentes tecnologías para transmitir datos del sensor. Sin embargo, una gran cantidad de estas implementaciones no incluyen mecanismos de seguridad.

**Cuadro III** Estado actual de la técnica

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8054574/8074842/8074857/8074857-table-3-source-large.gif)

**SECCION VI.**

## **Requisitos para regulaciones**

Con el creciente número de aplicaciones de monitoreo de salud y hardware conectado, existe un requisito claro para proporcionar a los usuarios pautas legales. Dichas pautas proporcionarán al usuario una cobertura legal en caso de uso indebido de datos y proporcionarán a los proveedores de hardware / servicio una regulación mejorada para aumentar la seguridad del hardware y software que maneja los datos personales.

### A. Divulgación

En el caso de una violación de datos, los usuarios deben recibir información clara y concisa sobre el evento, así como la acción tomada por el proveedor para mitigar la fuga o el ataque. Además del evento, la compañía debería plantear el problema a las autoridades superiores y colaborar con los equipos de respuesta a emergencias informáticas locales y nacionales como se sugiere en [19]. Algunas leyes ya están cubriendo la divulgación en caso de violaciones de datos, como la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA), la Ley Gramm-Leach-Bliley (GLBA) o la Ley de Derechos Educativos y Privacidad de la Familia (FERPA) en los Estados Unidos [24], o la Directiva 2002/58 sobre privacidad y comunicaciones electrónicas en Europa. Sin embargo, las divulgaciones solo son aplicables en una variedad de casos, que cubren solo ciertos tipos de filtraciones de datos [25], proporcionando una serie de áreas grises para los servicios de salud electrónica y proveedores de hardware dentro de la UE [26].

### B. responsabilidad

Con el fin de proporcionar un alto nivel de privacidad y seguridad, los proveedores de servicios deben ser responsables de la seguridad y privacidad que brinda su plataforma, lo que permite una mayor Transparencia, Garantía, Confianza del usuario, Responsabilidad y cumplimiento de las Políticas, según lo sugerido por Pearson et al. [26].

Además, como se sugiere en [27] - [28] [29], las personas o empresas que brindan servicios o hardware que manejan información confidencial deben ser responsables de garantizar que los servicios brinden un nivel adecuado de seguridad.

**SECCION VII.**

## **Conclusión**

Las tecnologías de eSalud se están volviendo cada vez más comunes y ahora están presentes en la atención primaria y secundaria, así como para fines de monitoreo personal. A pesar del amplio alcance de este trabajo, se han destacado una serie de desafíos fundamentales de seguridad y privacidad en el campo de los sistemas de monitoreo de salud portátiles. Se demostró que la seguridad y la privacidad de los pacientes y sus datos seguirán siendo uno de los mayores desafíos que enfrentará la salud móvil en el futuro cercano. Se demostró que a pesar de las actuales leyes de EE. UU. Y las directivas europeas, los servicios de salud electrónica y los proveedores de hardware no siempre deben proporcionar al usuario información relacionada con las violaciones de datos. Por último, se hicieron una serie de recomendaciones con el objetivo de mejorar las arquitecturas de salud electrónica actuales y futuras, mejorando la confianza entre los servicios prestados y los usuarios.