Las ciberamenazas en los dispositivos y redes del internet de las cosas médicas

Mtro. Flores Montaño Luis Alberto
Ex Alumno de Maestría en Informática SEPI UPIICSA

Lic. Aline Militzin Rojas Perea
Estudiante de Maestría en Doncencia ALIAT

Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática SEPI UPIICSA

Resumen
En los años recientes, el Internet de las cosas ha tenido un crecimiento considerable, debido al número de dispositivos que están conectados a la internet actualmente, dichos dispositivos usan controladores basados en microprocesadores con aplicaciones, obteniendo utensilios "inteligentes", que pueden ser desde tostadoras hasta transportes complejos como aviones, logrando notar su importancia en diversas áreas de la industria. Sin embargo, esta investigación se enfoca únicamente a un sector salud de la industria, ya que esta última ha sido la más lenta en adoptar las tecnologías del internet de las cosas, en comparación con otras industrias; esta tecnología utilizada en el sector salud lleva por nombre el Internet de las Cosas Médicas (en inglés "Internet of Medical Things" IoMT), la cual se encarga de vincular dispositivos "inteligentes" para el monitoreo de pacientes que deben de estar en constante observación. Esta última tecnología está preparada para transformar la forma en que mantiene a las personas seguras y saludables. Cabe mencionar que el Internet de las cosas médicas puede ayudar a monitorear, notificar e informar, no sólo a los médicos o las personas encargadas del cuidado del paciente, sino también a los proveedores de atenciones médicas, con datos reales para identificar los problemas antes de que se vuelvan críticos o para anticipar una intervención. Cabe mencionar, que esta industria no solo ha sido lenta para adoptar esta tecnología del Internet de las cosas, también ha mostrado deficiencia en la seguridad en la información obtenida mediante sus dispositivos, esto debido a que varias firmas dedicadas a la fabricación de estos dispositivos han dado pocas o ninguna medida de seguridad. Dicho lo anterior, esta investigación da a conocer algunos de los puntos de la importancia del Internet de las cosas médicas, así como las consecuencias debido a la falta de seguridad en este sector.

Palabras clave
Internet de las cosas médicas, Ciberseguridad, Riesgo, Farmacéutica.

Summary
In recent years, the Internet of Things has had considerable growth, due to the number of devices that are currently connected to the internet; these devices use microprocessor-based controllers with applications, obtaining "smart" utensils, which can be from toasters to complex transports such as airplanes, managing to notice its importance in various areas of the industry. However, this research focuses only on the health sector of the industry, since it has been the slowest in adopting the internet of things technologies, compared to other industries. This technology used in the health sector is called the Internet of Medical Things (IoMT), which is responsible for linking "smart" devices for monitoring patients who must be in constant observation. This technology is prepared to transform the way you keep people safe and healthy. It is worth mentioning that the Internet of Medical Things can help monitor, notify and inform, not only doctors or caregivers, but also medical care providers, with real data to identify problems before they become critical, or to anticipate an intervention. It is worth mentioning that this industry has not only been slow to adopt the technology of the Internet of Things, it has also shown a deficiency in the security of the information obtained through its devices, this because several firms dedicated to the manufacture of these devices have given few to no security measures. That said, this research reveals some of the points of the importance of the Internet of Medical Things, as well as the consequences due to the lack of security in this sector.

Keywords
Internet of medical of things, Cybersecurity, Risk, pharmacist

I Introducción

Actualmente, el Internet de las cosas (en inglés Internet of Things-IoT) es omnipresente, teniendo un gran potencial en gran parte de los sectores de la sociedad; sin embargo, en este gran avance se presentan problemas de seguridad de la información obtenida desde los dispositivos que censan la actividad humana. Los dispositivos en esta tecnología son conocidos como el Internet de las Cosas Médicas (en inglés Internet of Medical Things-IoMT); es importante mencionar que estos dispositivos carecen de seguridad debido a que los proveedores de esta tecnología no implementan protocolos de seguridad en la obtención de información, añadiendo un uso inadecuado [4].

Es importante mencionar que hoy en día se cuentan con diversos dispositivos del internet de las cosas médicas, como es el caso de refrigeradores que almacenan productos químicos, microscopios, bombas de infusión, camas y marcapasos "inteligentes" y hasta equipos farmacéuticos, todos estos conectados a la red de un hospital o centro de salud, bajo una arquitectura compleja de información [3]. De esta manera los datos que se comparten están conectados a la misma red, de modo que el equipo de tratamiento puede tener una visión compartida de los eventos; es importante mencionar que esta tecnología es muy reciente ya que hace 10 años era imposible realizar este tipo tareas [5].

Las funciones más importantes que se pueden encontrar en estos dispositivos, además de la asistencia sanitaria, es el de recopilar datos, monitorear sistemas y controlar el tejido que mantiene unidos al funcionamiento interno; por ejemplo, las farmacias de los hospitales requieren el mismo nivel de control que se utiliza en las refinerías, así como las instalaciones que generan algún tipo de energía e incluso los almacenes que llevan control de ciertos productos, donde los sensores evalúan los procesos con precisión y ajustes en tiempo real acorde con las necesidades del sector [1].

Debido al costo y la necesidad de monitorear los sistemas en diversas empresas dedicadas a la salud, muchos de estos dispositivos se han agregado a redes corporativas primarias; sin embargo, se debe recalcar que estas redes no fueron diseñadas para considerar riesgos en la seguridad de la información, todo esto debido al mal diseño de la planificación de las redes [3].

Existen organizaciones dedicadas al tratamiento en materia salud, las cuales tienen la necesidad de proteger datos confidenciales de los ataques cibernéticos, especialmente porque hay vidas en juego; lamentablemente, las soluciones prácticas son difíciles de implementar a estos dispositivos [1]. Teniendo esta problemática, en esta investigación, se incluyen algunas medidas que se pueden aplicar a los dispositivos del internet de las cosas médicas.

II Contenido del artículo

Empezando desde sensores pequeños hasta sistemas completos en hospitales, el internet de las cosas médicas ha ayudado a salvar muchas vidas y cambiar la modalidad de la práctica en la medicina [5]. Capturando de forma remota los datos médicos, facilita el suministro de medicamentos y habilita las aplicaciones de salud de manera digital, ofreciendo de esta manera funcionalidad y comodidad a los médicos y a su vez a los pacientes, considerando los siguientes aspectos:

- Crean productos farmacéuticos personalizados, para determinar pautas de atención basadas en los sistemas biológicos únicos de un paciente en particular, por lo que el internet de las cosas médicas ayuda a

que la atención médica en un paciente sea más personalizada.

- Garantizan el cumplimiento de las órdenes de los médicos; hay que tener en cuenta que el internet de las cosas médicas no pretende sustituir a los proveedores de atención médica, más bien esta tecnología ayuda a recolectar los datos de los dispositivos, con el propósito de tener un mejor diagnóstico y planes de tratamiento, reduciendo de esta manera las ineficiencias y el uso inadecuado de sistemas de atención médica.

- Soportan al monitoreo de la actividad y el comportamiento del paciente fuera de la clínica o consultorio, por lo que el proveedor obtendrá los datos reales para cumplir con las recomendaciones de terapia del paciente y lo que posteriormente sucede al abandonar el centro de salud.

Con el aumento del número de los dispositivos conectados, se debe de determinar cómo manejar la carga de datos de forma segura. Con el propósito de que los dispositivos del internet de las cosas médicas sean realmente elementos que transforman las organizaciones en las atenciones médicas, se debe de atender el cómo obtener los datos en los que se recopila la información [6]. El impulso de esta transformación está aumentando, por lo que se requiere que los administradores de un hospital o centro de salud, los proveedores y fabricantes deban trabajar coordinados para impulsar la metamorfosis cultural del cuidado de la salud.

Anteriormente se mencionó que el desarrollo medidas de seguridad puede ayudar a las compañías de la tecnología que producen productos del internet de las cosas médicas, con componentes y software relacionado a atenuar los riesgos [2]. A continuación, se mencionan algunas medidas de seguridad para que este tipo de dispositivos y los riesgos que pueden producir estos:

1. Lesiones corporales.

Si existe un mal funcionamiento en algún dispositivo del internet de las cosas médicas, pueden ser responsables de las lesiones resultantes, o incluso la muerte, de un paciente. Por ejemplo, si un médico receta una pastilla con un chip para verificar y monitorear a un paciente con un problema de memoria, teniendo una falla podría evitar que el transistor envié los datos de monitoreo al médico, provocando que el médico no reciba las alertas de que el paciente no esté tomando la medicación adecuada. En la figura 1 se muestra un paciente con lesiones corporales debido al mal funcionamiento de un dispositivo del internet de las cosas médicas.

Figura 1: Lesiones corporales por mal funcionamiento de un dispositivo del internet de las cosas médicas

2. Errores y omisiones de tecnología.

Un error común que se encuentra en esta tecnología es que los dispositivos pueden de dejar de funcionar debido a un acto negligente en el diseño, ocasionando pérdidas económicas o interrupción del negocio a un posible comprador. Por ejemplo, si una aseguradora de salud ofrece un incentivo a los clientes para que usen un rastreador de actividad física, y este genera un error en el conteo de los pasos, mandado datos con un conteo más alto de lo normal al software, la compañía podría otorgar

más descuentos de los que debería otorgar a sus clientes, provocando así pérdidas financieras.

Figura 2: Errores y Omisiones en la IoMT

3. Los riesgos cibernéticos.

Los hackers o ciberdelincuentes pueden considerar a la información médica protegida como un objetivo atractivo para los ataques cibernéticos, infiltrándose en las bases de datos que generan los dispositivos. De tal manera que, si se llegarán a exponer estos datos, la empresa podría presentar grandes pérdidas financieras, además de demandas y daños a la reputación de empresa.

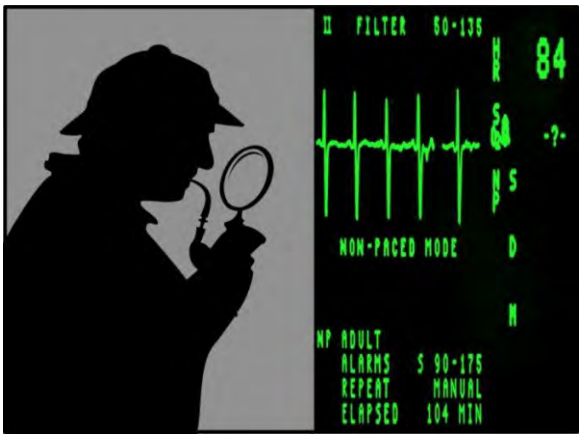

Figura 3: Ciberdelincuencia en las IoMT

Por ejemplo, una compañía que fabrica monitores cardíacos portátiles puede tener lecturas médicas cargadas en una nube, por lo que los ingenieros serían los responsables de la seguridad de esta, sin embargo, si no configuran correctamente un parche de seguridad, podría crear una vulnerabilidad, dando paso a que los "hackers" obtengan el acceso a dicha información, y vendan los datos de salud confidenciales de un paciente con fines lucrativos y de daño a la salud de este.

Las vulnerabilidades que abordan las médicas plantean un daño potencial a los pacientes [1]. Scott Erven (director asociado de Protiviti) menciona lo siguiente acerca de las vulnerabilidades en dispositivos de atención médica:

> "No tenemos evidencia de que la vulnerabilidad en los dispositivos, o un problema de ciberseguridad en un dispositivo médico, haya causado un problema directo de seguridad del paciente. Pero debido a que estos dispositivos carecen de capacidad de captura de evidencia y de registro forense, me gusta decir que tenemos poca seguridad de que algo no ha sucedido ".

Así como en los últimos años han surgido nuevas aplicaciones y dispositivos para el Internet de las cosas Médicas, también han estado surgiendo nuevos riesgos para este tipo de tecnología. Tomando en cuenta dichos riesgos, se ha vuelto notable que la comunidad médica ha ido aceptando cada vez más el uso de dispositivos de cosas del internet médicas; ya que las empresas del cuidado de la salud han optado cada vez más por el uso de está tecnología; sin embargo, es importante mencionar que dichas empresas son responsables de la poca seguridad en la recopilación de datos, así como las pérdidas económicas y las lesiones corporales que estos puedan ocasionar [5].

Teniendo en cuenta lo anterior, las empresas de la salud deben considerar a empresas

tecnológicas que pueden ayudar a contrarrestar los riesgos mencionados anteriormente.

Algunas medidas que se pueden considerar para evitar percances en la seguridad en la información de estos son las siguientes:

- Analizar las coberturas de responsabilidades del producto, civiles y cibernéticas, así como los errores y las omisiones, y la cobertura, que ayudan a proteger contra la responsabilidad potencial.

- Construir una infraestructura de seguridad cibernética adecuada.

- Realizar una evaluación de vulnerabilidad en cada dispositivo conectado, con el propósito de que los riesgos estén administrados y documentados.

- Asignar un tipo de riesgo a un propietario para la responsabilidad de este y mitigar el riesgo.

- Revisar los riesgos trimestralmente, tomando en consideración cualquier cambio en el programa debe escalarse a la gerencia ejecutiva.

- Evaluar e implementar sistemas adecuados de gestión de calidad y riesgo.

- Evaluar las prácticas contractuales de la empresa.

- Realizar un inventario de todos los dispositivos y aplicaciones, para la creación de un "diccionario de datos"; es importante mencionar que tener un inventario de aplicaciones no resuelve el problema, sin adicionalmente tener un directorio de datos. Es decir, se necesita tener un directorio dónde residen todos los datos, de dónde se origina, se usan, así como las capacidades de transmisión.

- Identificar todos los dispositivos IoT en la red, independientemente del tiempo que lleva el dispositivo funcionando.

- Cifrar y la realizar un arranque seguro en los dispositivos, con el propósito de que cuando se encienda un dispositivo, se verifique que ninguna de sus configuraciones se haya modificado.

III. Conclusiones

En esta investigación se vieron diversas ventajas que se tienen hoy en día con el uso de los dispositivos del internet de las cosas enfocadas a la industria de la salud, tales como el uso de un diagnostico adecuado no solo dentro de los centros de salud u hospitales, si no también fuera de ellos y monitorear al paciente de una manera adecuada y remota; sin embargo, como se llegó a notar, todos estos avances tecnológicos llevan un proceso en cuanto a la dedicación y responsabilidad en el control de estos dispositivos.

Para llevar a cabo todo esto se necesita llevar una minuciosa inspección acerca de estos, en especial en la parte de la seguridad, con la finalidad de no ser pirateados, o tener fugas de información para propósitos delictivos.

Con motivo de tales riesgos, se proporcionan diversos métodos para ayudar a incrementar la seguridad y evitar la fuga de datos. Este tipo de métodos no solo están enfocados a las empresas dedicadas a la creación de estos dispositivos, si no también en los usuarios que los utilizan, como sería el caso del personal en los hospitales o centros de salud.

Referencia y Recursos Electrónicos

1. Clyde, H., “The Risks of IoT in Medicine and Healthcare”, Recuperado de: https://www.securitymagazine.com/articles/88

811-exploring-the-wide-ranging-iot-risks-in-healthcare, 2018

2. Lee. K., "Healthcare IoT security issues: Risks and what to do about them" Recuperado de: https://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-the, 2015

3. López, M., "Emerging Services as New Revenue Streams" Recuperado de: https://www.channelfutures.com/industry-perspectives/emerging-services-new-revenue-streams, 2017

4. Marr, B.,"Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018" Recuperado de: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#2a90e34e4a3c, 2018

5. O'Connor, M., "A Wearable That Listens for Troubling Coughs," Recuperado de: http://www.iotjournal.com/articles/view?14687, 2016

6. Yu, L.; Lu, Y.; Zhu X; Tecnologías civiles disruptivas, Seis Tecnologías con Potencial de Impacto en los intereses de Estados Unidos hasta el 2025; Consejo Nacional de Inteligencia-NIC, Washington D.C, Estados Unidos, 2008.