Seguridad y ciberseguridad en los dispositivos médicos

DOI: 10.29236/sistemas.n149a7

Conceptos y retos

Resumen
En el contexto de una convergencia tecnológica y de disciplinas científicas como la biología, la informática, la electrónica y la medicina, en las que se habilitan cada vez más nuevos sistemas ciberfísicos, entre ellos los dispositivos médicos, es necesario actualizar las reflexiones sobre la seguridad y la ciberseguridad, como quiera que la explotación de una vulnerabilidad, no sólo afectará la funcionalidad de los mencionados dispositivos, sino la salud de las personas. En este sentido, este artículo desarrolla una reflexión conceptual sobre los retos de seguridad y control en los dispositivos médicos, algunas de las prácticas y estándares más relevantes, así como los desafíos emergentes que generan tensiones en el diálogo interdisciplinar y abre nuevas visiones desde una óptica más sistémica para recorrer el camino de la confianza digital.

Palabras clave
Dispositivos médicos, sistemas ciberfísicos, ciberseguridad, seguridad, vulnerabilidades

Jeimy J. Cano M.

Introducción

En un contexto digitalmente modificado, cada vez más los objetos del mundo físico incrementan su densidad digital (Zamora, 2017), habilitando flujos de información que son

utilizados para concretar nuevas funcionalidades y desplegar nuevas experiencias en los clientes. Esta nueva realidad expande el concepto de sociedad informacional (Castells, 2001) para dar paso a una sociedad digital y tecnológicamente modificada, que establece nuevas fronteras del conocimiento desde la lectura de un entorno volátil, incierto, complejo y ambiguo.

Por tanto, los objetos físicos adquieren la connotación de inteligentes, lo que en palabras de Porter y Heppelman (2014), significa que las nuevas características de inteligencia amplifican las capacidades y el valor de los componentes físicos, mientras que la conectividad incrementa las capacidades y el valor de los componentes inteligentes, motivando un resultado que lleva a un círculo virtuoso de mejora de valor. Luego, la realidad física estará cada vez más afectada por las condiciones tecnológicas, creando un espacio inexistente de convergencia donde las implicaciones y riesgos del mundo informático, tendrán efectos en el mundo tangible.

En consecuencia con lo anterior, los dispositivos médicos (tecnológicamente modificados) configuran un escenario novedoso, en el que la biología, la tecnología y la conectividad se encuentran para promover nuevas oportunidades y experiencias, tanto para los pacientes como para los prestadores de los servicios de salud, demandando de los proveedores de estos dispositivos, el mayor compromiso de calidad y conformidad de producto, que genere la suficiente confianza digital en sus usuarios, para su adecuado uso y mejoramiento de su calidad de vida.

Así las cosas, esta convergencia tecnológica en el ámbito de la salud, debe motivar reflexiones sobre la seguridad y control de esta nueva generación de objetos digitalmente modificados, con el fin de avanzar rápidamente frente a la inevitabilidad de la falla, inherente a cualquier elemento de tecnología, con el fin de no sólo anticiparla, sino preparar tanto a pacientes como a entidades prestadoras de salud, para que entiendan y actúen frente a los retos y connotaciones tanto informáticas, como físicas y humanas que una vulnerabilidad o brecha de seguridad puede causar en un entorno como este.

Si comprendemos que ahora en una entidad de salud, -institución hospitalaria- estamos pasando de una cama que funcionaba aislada en un cuarto, a tener entre 10 a 15 dispositivos en una habitación conectados a la red del hospital (Coventry & Branley, 2018), sin contar con los objetos digitales personales (tabletas, teléfonos y relojes inteligentes, entre otros) que también pueden estar haciendo uso de dicha red, se abre un nuevo espectro de gestión y gobierno de riesgos emergentes frente a la ciberseguridad que exige un entendimiento

tanto de la seguridad del paciente, como de la misma infraestructura de la entidad, para brindar un ambiente confiable de operaciones que capitalice la nueva promesa de valor.

Por consiguiente, este breve artículo, entendiendo la ciberseguridad como una capacidad que deben desarrollar las organizaciones, que demanda un ejercicio de carácter interdisciplinar socio-técnico (Craigen, Diakun-Thibault & Purse, 2014), desarrolla algunas reflexiones sobre la gestión de la seguridad y ciberseguridad de los dispositivos médicos, como una forma para comprender los desafíos que esta realidad implica en la práctica de la medicina actual, así como algunas recomendaciones para movilizar un necesario despertar tanto de pacientes, como de médicos, proveedores e instituciones de salud frente a una realidad que ya no es ciencia ficción, sino un hecho real.

Dispositivos médicos, conceptos básicos

De acuerdo con la norma *ISO 14971:2007 Aplicación de la gestión del riesgo a los dispositivos médicos y reactivos de diagnóstico in vitro*, un dispositivo médico se define como:

"Cualquier instrumento, aparato, dispositivo, equipo, implante, reactivo o calibrador para diagnóstico in vitro, programa informático, material u otro similar o relacionado, utilizado sólo o en combinación, destinado por el fabricante a ser utilizado en seres humanos con fines de:

- diagnóstico, prevención, control, tratamiento o alivio de una enfermedad;
- diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia;
- investigación, sustitución o modificación de la anatomía o de un proceso fisiológico;
- mantenimiento o prolongación de la vida;
- regulación de la concepción;
- desinfección de dispositivos médicos;
- proporcionar información para fines médicos mediante análisis in vitro de muestras derivadas del cuerpo humano,

Y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios".

Esta definición establece una visión convergente, desde el mundo médico como del informático. Cualquier dispositivo con estas características es susceptible de ser usado de forma externa e interna en los pacientes, con el fin de materializar algunas de las características antes mencionadas. Hoy muchas personas en el mundo usan dispositivos médicos (con componentes electrónicos e informáticos) tales como bombas de insulina, marca-

pasos, neuroestimuladores, entre otros, que permiten un tratamiento eficiente y focalizado sobre los pacientes, mejorando su condición de salud y aumentando la capacidad de monitorización y seguimiento por parte de los médicos.

En este contexto, es necesario establecer un conjunto base de buenas prácticas sobre la operación del dispositivo las cuales, por lo general, vienen dadas por parte del proveedor y con frecuencia no incluyen temáticas relacionadas con la seguridad o ciberseguridad del mismo, como quiera que estos aspectos no existían previamente como exigencias concretas o atributos de calidad para su fabricación, distribución y uso.

En la actualidad los dispositivos médicos cuentan con referencias internacionales sobre la necesidad de su aseguramiento desde su fabricación, de tal forma que las consideraciones de seguridad y privacidad se incorporen desde su diseño, habida cuenta que son los datos del paciente, su seguridad y su condición de salud, las que están en juego (Perakslis, 2014). Ya no es suficiente que las verificaciones de funcionalidad y calidad habituales de estos objetos digitalmente modificados pasen en el mundo médico, sino que es necesario exponerlos a pruebas de mal uso para ver su comportamiento en situaciones no previstas y así establecer los procedimientos alternos para su atención.

En razón de lo anterior y considerando que el sector salud se ha convertido en objetivo de los ciberatacantes, dada su poca madurez en el aseguramiento de este tipo dispositivos, así como de su infraestructura de operaciones (Martin, Martin, Hakin, Darzi & Kinross, 2017), se requiere aumentar la concienciación y sensibilización de cada uno de sus actores, para crear un lenguaje común frente a los riesgos cibernéticos (Eling & Schnell, 2016), en el que se configure una red extendida de protección en el diseño del dispositivo y se concrete en su administración y configuración, para que el paciente sea consciente y mantenga una monitorización clara y efectiva en el uso de estos dispositivos.

El reto de la inseguridad en los dispositivos electrónicos cardíacos

Comprender el reto de la seguridad, la privacidad y la ciberseguridad de un dispositivo médico implantado es trazar un diálogo interdisciplinar entre la medicina, la ingeniería y la tecnología, con el fin de establecer las relaciones y las implicaciones en el mejoramiento de las condiciones de salud de una persona, a través del aumento de la densidad digital de artefactos físicos diseñados para tal fin. En este sentido, los implantes cardíacos, como los marcapasos, ilustran las bondades y retos de tiene habilitar nuevas funcionalidades que asistan al médico en su labor de prevención y monitorización, así como

al paciente en su uso y apoyo de su condición de salud.

A la luz de la literatura especializada, un marcapasos se considera como un tipo de sistema ciberfísico, con componentes electrónicos que son implantados en el cuerpo humano como soporte en la monitorización permanente, detección y pronóstico de condiciones específicas, así como en la administración de terapias particulares (estimulación neuronal, administración de farmacéuticos, entre otros) (Altawy & Youssef, 2016). De igual forma estos sistemas se encuentran conectados a redes de telemetría (radio frecuencia y redes inalámbricas) que reciben sus señales, las cuales fluyen hacia sistemas de información integrados para un seguimiento y validación permanentes de la condición médica del paciente, como factor clave para una intervención oportuna frente a situaciones de excepción.

En este contexto, un marcapasos es susceptible, como sistema ciberfísico, de ciberamenazas y riesgos emergentes, que no sólo pueden comprometer al dispositivo, sino la condición específica de una persona. Sobre este particular, investigaciones recientes establecen un marco general de amenazas que se pueden materializar (Baranchuk, A., Refaat, Patton, Chung, Krishnan, Kutyifa, Upadhyay, Fisher, & Lakkireddy, 2018) y para enfrentarlas se requiere el concurso y comprensión de tres actores claves como son los proveedores, los prestadores de servicios (clínicas, hospitales, centros de salud) y los pacientes, para lograr un ejercicio integral donde se construya la confianza digital (Lewrén, Murdoch, & Johnson, 2014) en este escenario digitalmente modificado.

De acuerdo con la propuesta de Camara, Peris y Tapiador (2015), quienes siguiendo la metodología STRIDE (acrónimo en inglés que hace referencia a: *Spoofing (Suplantación), Tampering (Alteración), Repudiation (Repudio), Information disclosure (Revelación de información), Denial of service (Negación del servicio), y Elevation of privilege (Elevación de privilegios)*) establecen un conjunto base de condiciones en las cuales puede verse afectado un dispositivo médico implantado (DMI) y muestran cómo afecta los servicios propios de la seguridad de la información.

Considerando lo planteado en la Tabla 1 es necesario que, como parte de la relación entre la entidad prestadora del servicio de salud y el paciente, se actualice el protocolo de entrega, seguimiento y monitorización del DMI, para tener en cuenta al menos los siguientes puntos:

- Consecuencias potenciales si se explota una vulnerabilidad en el DMI.
- Opciones para mitigar el riesgo de vulnerabilidad asociada con la ciberseguridad.

Tabla 1
Metodología STRIDE aplicada a un DMI

Característica de seguridad	Amenazas	Riesgo
Autenticación	• Suplantación del programador • Suplantación del dispositivo	Suplantación
Integridad	• Alteración de los datos del paciente • Entradas de datos maliciosas • Modificación de los canales de comunicación	Alteración
No repudio	• Borrado de los registros de auditoría • Intentos repetidos de acceso	Repudio
Confidencialidad	• Revelación de información médica • Determinar el tipo de dispositivo implantado • Revelar la existencia del dispositivo en una persona • Seguimiento del dispositivo	Revelación de información
Disponibilidad	• Drenaje de la batería del dispositivo • Interferencias hacia el dispositivo • Inundación de datos hacia el dispositivo	Negación del servicio
Autorización	• Reprogramación del DMI • Actualización de la terapia del paciente • Apagar del DMI	Elevación de privilegios

Nota: Traducción libre de: Camara, Peris, & Tapiador, 2015, p.277

- Riesgos asociados con una actualización del software/firmware del DMI.

- Viabilidad técnica para explotar la vulnerabilidad de ciberseguridad del DMI.

- Solución a largo plazo a la vulnerabilidad de ciberseguridad identificada.

- Beneficios del DMI frente al riesgo de una vulnerabilidad de ciberseguridad. (Slotwiner, Deering, Fu, Russo, Walsh, & Van Hare, 2018)

De esta forma, no sólo se protegen las condiciones propias del dispositivo, sino aumenta la confianza del paciente, sabiendo que está informado sobre los riesgos inherentes en el uso del DMI y las acciones que el prestador tiene previstas ante cualquier eventualidad con el dispositivo.

Seguridad, ciberseguridad y privacidad en los dispositivos médicos

Frente al panorama anterior, es necesario establecer un marco de estándares y buenas prácticas para vincular a los proveedores, las clínicas y los pacientes, de tal forma que aumenten las garantías de manufactura y calidad de producto, la atención y el seguimiento por parte de los médicos, además de la concienciación y apropiación de las exigencias de seguridad y control por parte de los individuos portadores de DMI.

Muchas de las normas y buenas prácticas sobre este tema se han establecido en los Estados Unidos de Norteamérica (EUA), y otras en Europa, con el fin de aumentar la protección y responsabilidad de los diferentes interesados en los DMI. En este sentido, nombres como HIPAA (*US Health Insurance Portability and Accountability Act*), HITRUST (*Health Information Trust Alliance*), COBIT 5.0, CIS Critical Security Controls (*Center for Internet Security*), ISO 27002, NIST Cybersecurity Framework, GDPR (*General Data Protection Regulation*) revelan la nutrida participación de estándares y marcos de control disponibles a la fecha, sin perjuicio de las indicaciones de protección y aseguramiento que viene haciendo la FDA (*Food & Drug Administration*) de EUA frente a la ciberseguridad de los DMI, y a las exigencias claves para proveedores y prestadores de servicios de salud.

En particular la FDA establece un programa de recomendaciones antes y después de la comercialización del DMI. Así mismo, en su fase previa invita a los proveedores a considerar las posibles vulnerabilidades de los dispositivos durante su diseño y desarrollo, con el fin de aumentar las exigencias de conformidad y calidad de producto.

De igual forma, demanda de los fabricantes adelantar las acciones necesarias para mitigar las fallas identificadas, y mantener un conjunto de controles validados y ase-

gurados durante el ciclo de vida del DMI (Webb & Dayal, 2017).

En su fase posventa, la FDA sugiere que los proveedores adopten el estándar de ciberseguridad del NIST, el cual incorpora estrategias claves en cada uno de los elementos del modelo como "identificar, proteger, detectar, responder y recuperar", el cual, en pocas palabras, implica seguimiento y verificación permanentes de sus productos y servicios, con el fin de aumentar la resistencia de los DMI a las vulnerabilidades y en el caso de que se presenten, responder y acompañar a los prestadores del servicio de salud, para atender el incidente y apoyar de forma inmediata al paciente en esta condición adversa (Webb & Dayal, 2017).

En concreto y de manera general la FDA recomienda:

- Identificar activos, amenazas y vulnerabilidades, y evaluar su impacto en la funcionalidad de los dispositivos y en los usuarios/pacientes finales.

- Evaluar la probabilidad de que una amenaza y una vulnerabilidad sean explotadas. esto puede lograrse utilizando herramientas de evaluación de vulnerabilidad de ciberseguridad.

- Determinar los niveles de riesgo y las estrategias de mitigación adecuadas; por ejemplo, la FDA recomienda que los fabricantes determinen el "nivel de alerta" apropiado para el software (es decir, una estimación de la gravedad de las lesiones que un dispositivo podría permitir o infligir, directa o indirectamente, a un paciente u operador, como resultado de fallos del dispositivo, defectos de diseño, o empleando el dispositivo para su propósito previsto). Los niveles de preocupación varían desde Mayor (riesgo grave de muerte o lesión), Moderado (lesión menor) o Menor (improbable que cause lesión).

- Evaluar el riesgo residual en función de criterios adecuados de aceptación del riesgo.
  Limitar el acceso a los dispositivos a usuarios de confianza mediante el uso de programas de autenticación, tiempos de espera, privilegios de autorización por capas (por ejemplo, proveedor, administrador del sistema) y cierres de sesión.

- Restringir las actualizaciones de software o *firmware* basado en código autenticado y asegurar que los datos puedan transferirse de forma segura desde y hacia el dispositivo médico, por ejemplo, mediante cifrado. (Webb & Dayal, 2017, p.561)

De otra parte, y de forma complementaria, la TGA (s.f.) (*Australian Therapeutic Goods Administration*) de Australia, establece un conjunto de principios esenciales para la fabricación,

uso y comercialización de dispositivos médicos, que brindan tanto a los proveedores como a las clínicas, un marco de responsabilidad demostrada y cumplimiento respecto de los retos de seguridad y control, los cuales se desarrollan en una extensa lista de chequeo encabezada por los siguientes fundamentos básicos:

- El uso de los dispositivos médicos (implantados o no) no debe comprometer la salud ni la seguridad del paciente ni del operador.

- El diseño y construcción de dispositivos médicos debe hacerse de acuerdo con los principios de seguridad en el ámbito físico y lógico.

- Los dispositivos deben ser desarrollados para el uso previsto.

- La seguridad (física y lógica) del dispositivo debe ser una característica de largo plazo.

- Los dispositivos médicos no deben verse afectados negativamente por el transporte o el almacenamiento.

- Los beneficios del uso de los dispositivos médicos deben compensar cualquier efecto indeseable.

Como se puede observar, a la fecha se cuentan con marcos de trabajo que demandan el entendimiento de los riesgos emergentes propio de la convergencia tecnológica en el sector salud. Por tanto, se hace necesario reconocer esta nueva realidad y ajustar las prácticas actuales del sector en mención, para generar un contexto de operación y aplicación de las nuevas tecnologías con un marco de responsabilidad demostrada en un escenario digitalmente modificado.

Reflexiones finales

Si bien son claras las posibles implicaciones de la explotación de una vulnerabilidad en un dispositivo médico (una falla técnica, producir una alteración orgánica o incluso la muerte) (Hansen & Hansen, 2010), también lo es, que el ejercicio de aseguramiento de éstos es una responsabilidad compartida (Webb & Dayal, 2017). Lo anterior implica comprender su contexto de operación (Williams & Woodward, 2015), los flujos de información (Krawiec, Nadler, Tye, & Jarbo, 2015), sus capacidades inteligentes (monitorización, control, optimización, autonomía) (Porter & Heppelmann, 2014) y sus retos en el contexto organizacional (Jalali & Kaiser, 2018).

En consecuencia y de acuerdo con los resultados de la más reciente encuesta organizada por la HIMSS (*Healthcare Information and Management Systems Society*) (HIMSS, 2018) en los EUA, las entidades del sector salud continúan experimentando incidentes de seguridad que, por lo general, tienen como vector de ataque correos electrónicos ma-

liciosos, *phishing*, lo cual combinado con la baja sensibilización del personal médico sobre las temáticas de ciberseguridad, configura un fértil caldo de cultivo para que la inseguridad de la información se manifieste de diferentes formas y con retos inesperados que terminen afectando no sólo la operación de una clínica u hospital, sino comprometiendo la salud de un paciente.

Sin perjuicio de lo anterior, se abren nuevos retos para el sector salud con ocasión de la convergencia tecnológica y la incorporación de nuevas propuestas basadas en algoritmos de inteligencia artificial. La aparición de la *ciberbioseguridad* (Peccoud, Gallegos, Murch, Buchholz, & Raman, 2018; Murch, So, Buchholz, Raman, & Peccoud, 2018), como la "*comprensión de las amenazas derivadas del espionaje, las intrusiones y las amenazas maliciosas y perjudiciales que pueden tener lugar dentro o en las interfaces de las ciencias médicas y de la vida combinadas, los sistemas ciberfísicos, la cadena de suministro y los sistemas de soporte a la infraestructura, con el fin de diseñar medidas para prevenir, proteger, mitigar, investigar y atribuir dichas amenazas en la medida en que sean pertinentes a la seguridad, la competitividad y la resiliencia*" (Murch et al, 2018, p.1), hace evidente una frontera inexplorada que exige una visión interdisciplinar que comienza en una lectura de referencia en el mundo de la biología y la medicina, y se configura en una realidad física asistida y construida con componentes electrónicos e informáticos.

Una lectura de la ciberbioseguridad, se advierte en las impresoras 3D utilizadas en la actualidad, quienes serán las primeras en estar sometidas a este nuevo reto de seguridad cuando se empiecen a imprimir de manera masiva órganos, huesos o material biológico fruto de investigaciones que trascienden los límites de los desarrollos disponibles a la fecha.

Los recientes diagnósticos médicos asistidos por algoritmos de inteligencia artificial, los brazos robóticos para adelantar cirugías de alta precisión, implantes cocleares inteligentes, entre otros adelantos, confirman retadores campos de aplicación de tecnología para beneficio de la humanidad, que generan una esperanza para encontrar soluciones a muchas de las enfermedades conocidas a la fecha y posiblemente anticipar la aparición de nuevas. Sin embargo, la confiabilidad de la información, los archivos de base, la conectividad y los algoritmos de inteligencia artificial no se pueden asegurar, como quiera que éstos "son tan buenos como los datos con los que se nutren, el entrenamiento y el contexto que proporcione un experto humano" (Dunbar, Buffomante, Bell, & Justice, 2017).

Por tanto, los nuevos sistemas ciberfísicos propios del mundo médi-

co y los avances que se verán habida cuenta del avance de la cuarta revolución industrial, serán el escenario privilegiado para que el diálogo interdisciplinar que se abre entre diferentes disciplinas (biología, electrónica, informática y medicina), motive una visión sistémica de la seguridad y control que habilite la configuración y materialización de una confianza digital, orientada a crear la condiciones para avanzar en soluciones confiables, prácticas y efectivas, para las organizaciones y las personas, en un mundo digital y tecnológicamente modificado.

Agradecimientos

El autor agradece al Dr. Javier González Rodríguez, Profesor Asociado de la Escuela de Administración de la Universidad del Rosario, por su valiosos y acertados comentarios que permitieron afinar las reflexiones de este artículo.

Referencias

Altawy, R. & Youssef, A. M. (2016) Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access*. 4. 959-979. Doi: https://doi.org/10.1109/ACCESS.2016.2521727

Baranchuk, A., Refaat, M., Patton, K., Chung, M., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. & Lakkireddy, D. (2018) Cybersecurity for Cardiac Implantable Electronic Devices. What Should You Know? *Journal of the American College of Cardiology*. 71(11). 1284-1288. Doi: https://doi.org/10.1016/J.JACC.2018.01.023

Camara, C., Peris, P. & Tapiador, J. (2015) Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*. 55. 272-289. https://doi.org/10.1016/j.jbi.2015.04.007

Castells, M. (2001) Internet y la sociedad red. *Lección inaugural*. Recuperado de: http://www.uoc.edu/web/cat/articles/castells/print.html

Coventry, L. & Branley, D. (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113. 48-52. Doi: https://doi.org/10.1016/j.maturitas.2018.04.008

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13-21. http://doi.org/10.22215/timreview/835

Dunbar, K., Buffomante, T., Bell, G. & Justice, C. (2017) Se busca nueva estrategia de ciberseguridad. Razón: inteligencia artificial. *Harvard Business Review*. Recuperado de: https://hbr.es/tecnolog/616/se-busca-nueva-estrategia-de-ciber seguridad-raz-n-inteligencia-artificial

Eling, M. & Schnell, W. (2016) What do we know about cyber risk and cyber risk insurance? *The Journal of Risk*

Finance. 17(5). 474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122

Hansen, J. & Hansen, N. (2010) A Taxonomy of Vulnerabilities in Implantable Medical Devices. *Proceedings of the second anual workshop on Security and privacy in medical and home-care systems (SPIMACS '10)*, 13-20. Doi: 10.1145/1866914.1866917

Healthcare Information and Management Systems Society – HIMSS (2018) 2018 HIMSS Cybersecurity Survey. *Survey Report*. Recuperado de: http://www.himss.org/2018-himss-cybersecurity-survey

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5), e10059. http://doi.org/10.2196/10059

Krawiec, R., Nadler, J., Tye, E., & Jarbo, J. (2015) No appointment necessary: How the IoT and patient-generated data can unlock health care value. *Deloitte Insights*. August. Recuperado de: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-health-care-industry.html

Lewrén, M., Murdoch, R. & Johnson, P. (2014) The four keys to digital trust. Don't be left behind. *Accenture*. Recuperado de: https://www.accenture.com/t20150527T203143__w__/usen/_acnmedia/Accenture/ConversionAssets/Microsites/Documents14/Accenture-Four-Keys-Digital-Trust.pdf

Martin, G., Martin, P., Hakin, C., Darzi, A. & Kinross, J. (2017) Cybersecurity and healthcare: how safe are we? *British Medical Journal*, 358(7). Doi: 10.1136/bmj.j3179

Murch, R., So, W., Buchholz, W., Raman, S. & Peccoud, J. (2018) Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Trends in Biotechnology*, 36(1). 4-6. Doi: http://dx.doi.org/10.1016/j.tibtech.2017.10.012

Peccoud, J., Gallegos, J., Murch, R., Buchholz, W. & Raman, S. (2018) Cyberbiosecurity: from naive trust to risk awareness. *Frontiers in Bioengineering and Biotechnology*, 6(39). 1-6. Doi: 10.3389/fbioe.2018.00039.

Perakslis, E. (2014) Cybersecurity in health care. *The New England Journal of Medicine*, 371, 395-397. Doi: 10.1056/NEJMp1404358

Porter, M. & Heppelmann, J. (2014) How smart connected products are transforming competition. *Harvard Business Review*. November. 1-23

Slotwiner, D., Deering, T., Fu, K., Russo, Andrea M., Walsh, M. & Van Hare, G. (2018) Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians. *Proceedings of the Heart Rhythm Society's Leadership Summit*. Heart Rhythm 2018.15:e61–e67. Doi: https://doi.org/10.1016/j.hrthm.2018.05.001

TGA (s.f.) Medical Devices Essential Principles Checklist. Recuperado de: https://www.tga.gov.au/node/3285

Webb, T. & Dayal, S. (2017) Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review*. 33(4). 559-563. Doi: https://doi.org/10.1016/j.clsr.2017.05.004

Williams, P. & Woodward, A. (2015) Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problema. *Medical devices: Evidence and Research*, 8, 305-316. Doi: 10.2147/MDER.S50048

Zamora, J. (2017) ¿Es posible programar modelos de negocio? *IESE Insight*. 33. II Trimestre. 23-30. Doi: 10.15581/002.ART-3013

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D in Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*