

# Smart Cities, IoT y Salud: Retos de Internet of Medical Things (IoMT)

Jesús Daniel Trigo Vilaseca, Luis Serrano-Arriezu, José Javier Astrain Escola, Francisco Falcone Lanas  
 Instituto de Smart Cities, Universidad Pública de Navarra, E-31006 Pamplona, Navarra, España.

LA INNOVACIÓN TECNOLÓGICA APLICADA AL ÁMBITO DE LA SALUD ESTÁ PERMITIENDO EL RÁPIDO DESARROLLO DE LA INTERNET DE LOS DISPOSITIVOS MÉDICOS, O EN SU VERSIÓN INGLESA MÁS ACEPTADA INTERNET OF MEDICAL THINGS (IOMT). EN ESTE ARTÍCULO SE PRETENDE DAR UNA VISIÓN GENERAL DE LAS POSIBILIDADES Y RETOS DE ESTAS TECNOLOGÍAS, LA CUALES DEBEN IMBRICARSE COMO PILAR FUNDAMENTAL EN EL DESARROLLO DE ESTRATEGIAS LOCALES, REGIONALES Y ESTATALES DE LAS CIUDADES INTELIGENTES O SMART CITIES.

**PALABRAS CLAVE:** *Smart Cities, Internet of Medical Things (IoMT), Salud, Biosensores, Tecnologías de Comunicación, Seguridad y Privacidad, Explotación de Datos*

## INTRODUCCIÓN

Resulta evidente que la innovación tecnológica ha sido, es y será el motor del cambio de nuestra sociedad. La denominada Ley de Moore ha sobrevivido durante más de 50 años y se espera que siga siendo válida durante las próximas décadas a pesar de que le hayan surgido competidores muy serios [1]. El oximoron de más por menos, *Moore for Less*, es decir, más potencia de cálculo por menos consumo o más rápido por menos coste, etc. es de dominio público. Esta innovación tecnológica está presente en todos y cada uno de los sectores de la economía y la sociedad; y la salud no podría ser menos [2].

Por otro lado, con los números en la mano, se puede decir que la urbanización de la población mundial resulta imparable [3]. No solamente crece el número de habitantes en el planeta, sino que dichos habitantes se instalan en las ciudades. En este sentido, desde hace ya unos años, se viene hablando de las *Smart Cities* como una solución para ofrecer una mejor calidad de vida a la ciudadanía. *Smart Cities*, como su nombre indica, supone el desarrollo de una serie de servicios cuyo fin último sea el indicado, la mejora de la calidad de vida en la ciudad;

y la salud es una componente fundamental de ésta [4].

En salud, los retos para aplicar la innovación tecnológica de forma que se procure una mejora de la calidad de vida, basándose en la sostenibilidad, pasa por el despliegue de servicios sanitarios inteligentes. Estos servicios sanitarios, imbricados en las ciudades inteligentes, deben aprovechar el desarrollo tecnológico de los sensores, las tecnologías de comunicación, la implementación de medidas de seguridad y privacidad, así como la explotación de los datos con el objetivo de mejorar la calidad de vida de la ciudadanía.

En este artículo se va a realizar un breve pero completo recorrido por la innovación tecnológica aplicada en salud, y en particular, en el desarrollo de IoMT, para el despliegue de servicios de salud inteligentes, en el ámbito de las *Smart Cities*, para la mejora de la calidad de vida de la ciudadanía. En primer lugar, se revisará el estado del arte en el desarrollo de sensores para la captación de datos de salud. Posteriormente se analizarán las tecnologías de comunicaciones disponibles, así como las estrategias de seguridad y privacidad necesarias para la gestión de dichos datos. A continuación, se expondrán los retos para la integración y explotación de

dichos datos. Por último, se expone una breve conclusión abierta del horizonte que se presenta en el IoMT dentro de las *Smart Cities*.

### BIOSENSORES: EN CONTINUA INNOVACIÓN TECNOLÓGICA

El rápido desarrollo de tecnologías emergentes aplicadas al ámbito de los biosensores está propiciando la aparición de múltiples dispositivos médicos con capacidad de conexión en cualquier lugar y en todo momento, *anywhere at anytime*. Un estudio de *Allied Market Research* [5] predice que el mercado de IoMT alcanzará para el año 2021 la cifra de 136.8 mil millones de dólares, siendo actualmente 3.7 millones la cifra de dispositivos médicos en uso conectados y monitorizando datos médicos.

En una primera aproximación, sería posible distinguir entre biosensores no invasivos e invasivos. Por su inocuidad, los primeros son los preferidos para el desarrollo de la IoMT y, en particular, para el despliegue de servicios de telemonitorización socio-sanitarios. Sin embargo, los últimos también resultan de interés como, por ejemplo, para la adherencia de los pacientes a las prescripciones farmacológicas [6]. En cualquiera de ambos casos, lo que se está considerando actualmente es el desarrollo de dispositivos *wearables* o llevables. Esta necesidad de “llevabilidad” impone una serie de requisitos de diseño, fundamentalmente un tamaño y consumo reducidos (dispositivos *ultra-low power*).

Como demostración del concepto de IoMT, elegiremos la diabetes como enfermedad de referencia. La diabetes es una de las enfermedades crónicas con más prevalencia entre la población y su crecimiento es constante. Nuestros hábitos de vida, alimentación y sedentarismo, actúan como un catalizador de dicho crecimiento. En la actualidad, el control de la glucosa en sangre se realiza mediante un método semi-invasivo: un pinchazo en uno de los dedos de la mano. Como complemento, existe en la actualidad numerosas propuestas de bombas de insulina en lazo cerrado de manera que el control de la glucemia resulta transparente al paciente. Centrándonos, como se ha comentado, en la susti-

tución del método de control semi-invasivo por método no invasivos que puedan ser llevables se han publicado varias propuestas de interés, algunas de ellas ya cercanas al mercado [7]. En numerosos casos, la medida de la glucosa se realiza por medios electroquímicos tanto del líquido intersticial (*Reverse Ionphoresis*, RI) como del sudor mediante el uso de parches, tatuajes permanentes o muñequeras, las cuales están fabricadas, junto con la electrónica necesaria para el procesado de los datos, así como la transmisión de los mismos con tecnologías de tipo *Thin-Film* [8].

### COMUNICACIONES: TECNOLOGÍAS ACTUALES Y DEL MAÑANA

El desarrollo del IoMT se enmarca dentro de la búsqueda de entornos contextuales interactivos, siendo su paradigma las *Smart Cities/Smart Regions*. Uno de los elementos claves en el desarrollo de dichos entornos contextuales son los sistemas de comunicaciones, que sirven de facilitadores tanto para el intercambio de información entre dispositivos, como entre los diferentes usuarios de dichos sistemas. En este sentido, los sistemas de comunicaciones inalámbricos juegan un papel fundamental, debido a su capacidad de proporcionar conectividad con un elevado grado de movilidad y de su reconfigurabilidad. El fuerte auge de los sistemas de comunicaciones móviles, la adopción progresiva de sistemas de comunicación de área personal/corporal y la previsión de un elevado número de dispositivos con capacidad de conexión a Internet prevista en el marco general IoT ha llevado a la definición de redes de comunicaciones inalámbricas de tipo heterogéneo o HetNet, mostrada de manera esquemática en la Figura 1.

De esta manera, se pueden emplear múltiples estándares de comunicaciones en un esquema colaborativo, con el fin de poder optimizar las relaciones cobertura/capacidad de los mismos, ofreciendo niveles adecuados de calidad de servicio, minimizando niveles de interferencia así como de consumo energético. En este esquema de operación cabe mencionar los futuros sistemas de comunicaciones 5G, inte-

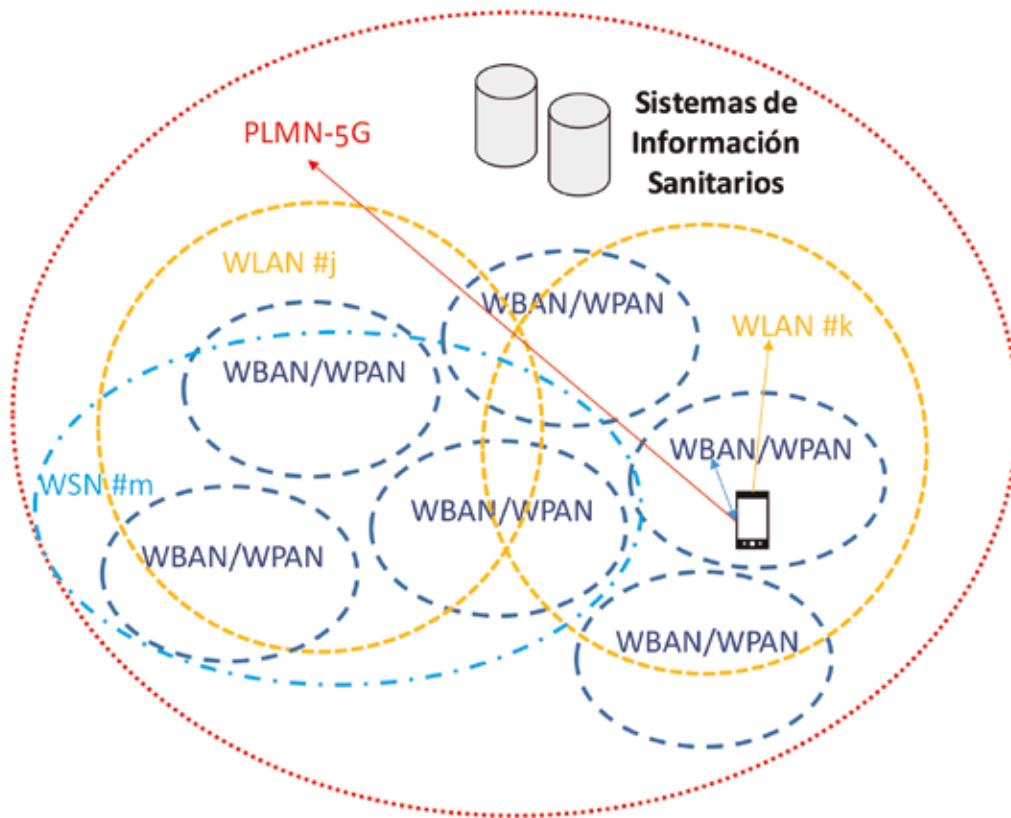


Figura 1: Representación esquemática de redes HetNet

grados dentro de este esquema HetNet y que proporcionan entre otras características comunicaciones de baja latencia y de alta densidad de dispositivos, con *Machine Type Communications* entre dispositivos (Device to Device, D2D). En el ámbito de prestación de servicios socio-sanitarios, el concepto de integración de servicios dentro de las *Smart Cities* ha llevado a la definición del concepto de *Smart Health*, en el que el comportamiento inherentemente contextual de las mismas se traslada al ámbito sanitario [9]. Los sistemas de comunicaciones inalámbricos que conforman la red HetNet se pueden clasificar por su grado de cobertura en relación con el usuario. De esta manera, las redes de área personal y corporal (*Wireless Body Area-WBAN* y *Wireless Personal Area-WPAN networks*) se emplean para la conexión entre sensores portados por los usuarios, tanto para su interconexión como para poder conectarlos con pasarelas externas. Las redes de área local (WLAN) se pueden emplear como medios de conexión de sensores de manera directa a la red, aunque es más habitual su empleo como

pasarelas, debido a su consumo energético más elevado frente a WBAN/WPAN. La conexión de área más extensa se lleva a cabo mediante redes móviles (2G a 4G) y en un futuro, mediante redes 5G. En este marco, cabe destacar el papel de las redes de sensores inalámbricos (*Wireless Sensor Networks*), que ofrecen múltiples estándares de comunicaciones, permitiendo operar en rangos de distancia amplios, con una gran cantidad de dispositivos por red y con un consumo energético reducido. Por ello, su integración puede ser directa (i.e., se pueden emplear directamente como elementos de red WBAN/WPAN) o como elementos indirectos de recolección de datos en redes independientes más extensas (e.g., redes de captación de datos ambientales urbanos).

### INSEGURIDAD EN LA SEGURIDAD DE LOS DATOS DE SALUD: NUEVO OXÍMORON

La seguridad y la privacidad son relevantes en cualquier sistema, pero más aún en un entorno

de IoMT, en el que los datos, que son altamente sensibles, van a viajar desde los sensores hasta los servicios de telemonitorización, parcial o totalmente de manera inalámbrica. Por tanto, es necesario implementar en dichas aplicaciones de IoMT políticas de protección de datos adecuadas para lograr niveles de seguridad y privacidad en línea con las demandas de los usuarios y las regulaciones aplicables. Entre dichas regulaciones encontramos, por ejemplo, la *General Data Protection Regulation* (GDPR) en Europa (que está previsto que entre en vigor en mayo de 2018) o algunas otras reglamentos nacionales, como la Ley Orgánica de Protección de Datos (LOPD). Los objetivos más comunes de estas regulaciones son: garantizar la seguridad de la información, el control del paciente sobre sus propios datos, la prevención y reacción ante las violaciones de la seguridad y privacidad de los datos, así como la responsabilidad y las sanciones a aquellos que no cumplan dichas medidas [10].

A pesar de los innegables beneficios de las plataformas de IoMT, la falta de privacidad y seguridad sigue siendo una de las principales preocupaciones [11-12], especialmente cuando se manejan datos confidenciales. Con respecto a la actitud de los consumidores, el control de las características de seguridad y privacidad de la salud móvil, así como la confianza en los proveedores, se han identificado recientemente como cuestiones clave [13].

Como resultado de este contexto de seguridad y privacidad, las plataformas de salud IoMT que se diseñen a día de hoy en Europa, deberán plantearse en línea con las políticas que marca la GDPR. Para conseguir cumplir estos requisitos, los proyectos tendrán que examinar a fondo las normas y regulaciones actuales que sean de aplicación a la arquitectura propuesta.

Técnicamente, los diseñadores de arquitecturas IoMT tendrán que estudiar modelos y esquemas de seguridad y privacidad adecuados para su inclusión en la plataforma que se proponga. Los esquemas bajo consideración incluirán (pero no se limitarán a), por ejemplo, alternativas recientes basadas en *Blockchain* como otras más asentadas, como los envoltorios criptográficos estandarizados existentes, tales

como *Cryptographic Message Syntax* (CMS) o bien *openPGP* (*open Pretty Good Privacy*). En un nivel inferior, dichos envoltorios soportan un conjunto de algoritmos criptográficos. Por lo tanto, cuando se implemente un envoltorio específico en una plataforma de IoMT, se tendrá que analizar el conjunto existente de algoritmos para seleccionar el más apropiado a fin de crear una capa robusta adicional de seguridad y privacidad. Para una mayor robustez, los algoritmos seleccionados serán, siempre que sea posible, diferentes de y complementarios a los algoritmos ya definidos por los protocolos y estándares situados bajo la capa de aplicación, si es que implementan alguno. En cualquier caso, si alguno de los algoritmos elegidos resultase comprometido, debería ser reemplazado inmediatamente por otro algoritmo existente considerado seguro y adecuado para la plataforma en ese momento.

## SOFTWARE, SOFTWARE Y MÁS SOFTWARE PARA LA INTEGRACIÓN Y EXPLOTACIÓN DE DATOS

La implantación de sistemas IoMT inteligentes de monitorización y su integración en los sistemas de información sanitaria es una tarea ardua no exenta de complicaciones pues implica la interoperabilidad de equipos y sistemas de información heterogéneos con varios formatos y diferentes arquitecturas. Es necesario disponer de mecanismos eficaces de integración de fuentes de datos heterogéneas para adaptarse a la nueva realidad de la red inteligente [14].

A la hora de seleccionar el modelo de negocio es relevante distinguir el modelo de nube que se desea emplear: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) o *Infrastructure as a Service* (IaaS). Sus principales características se describen a continuación.

En el caso de concebir el sistema como una aplicación (SaaS) a la que se accede generalmente desde un entorno web, es muy importante valorar el grado de madurez de la solución. Pocas de las soluciones comerciales poseen un nivel de madurez adecuado, lo que implica que se debe convivir con partes del sistema de información no integradas en la nube. A este condicionante

deben añadirse otros como la dependencia que se establece con el proveedor, no sólo a nivel de software (aplicaciones y servicios) sino a nivel de datos, que dejan de estar en poder de la organización para residir en la infraestructura del proveedor de servicio; la necesidad de programar y planificar con mucho cuidado la migración al nuevo modelo de trabajo para garantizar que la organización maximice los beneficios de la transición. La selección de un modelo SaaS suele deberse a criterios económicos de ahorro de costes en infraestructura, actualizaciones y revisiones de software, y a la oportunidad de rediseñar el proceso de negocio para ganar en eficiencia y reducir los tiempos de duración de los procesos. El peaje a pagar es la dependencia que se establece con el proveedor.

Si se opta por una solución basada en plataforma (PaaS) la institución mantiene el control sobre las aplicaciones, lo que facilita el empleo de aplicaciones personalizadas diseñadas y creadas específicamente por desarrolladores internos o externos para la institución. Esta cuestión es especialmente importante relevante en el ámbito de salud en el que garantizar la interoperabilidad entre aplicaciones y equipos de distintos fabricantes y desarrolladores no suele resultar sencilla ni rápida, y requiere del empleo de buses de servicio. La gran diferencia real entre los modelos SaaS y PaaS es el desarrollo y control de las aplicaciones. En el caso del modelo de plataforma, se garantiza la interoperabilidad de dispositivos y aplicaciones heterogéneas que deben respetar determinados estándares como DICOM o HL7 y se facilita el desarrollo de aplicaciones proveyendo a los desarrolladores kits de desarrollo de software (SDK). PaaS permite disociar las aplicaciones de la infraestructura, o un equipamiento de un determinado proveedor del resto, algo que no resulta trivial en el sector. Este modelo ofrece mayores capacidades de interoperabilidad y menor dependencia tecnológica, pero requiere disponer de un equipo solvente de profesionales TIC.

Finalmente, el modelo de infraestructura como servicio (IaaS) otorga todo el control a la organización, ofreciendo así una mayor flexibilidad y elasticidad ante las necesidades puntuales y futuras de recursos, una mayor facilidad de facturación por servicio prestado, una mayor inde-

pendencia tecnológica, una mayor interoperabilidad que los otros modelos (SaaS, PaaS) pero requiere disponer de un amplio y experimentado equipo de profesionales TIC. En lo referente a los costes, puede ser una buena oportunidad de acceder al último *hardware* sin tener que comprar, instalar o mantener las herramientas en sus propias instalaciones (derivación de pacientes para pruebas diagnósticas).

Una vez que la información sobre el paciente ha sido obtenida, procesada y convenientemente almacenada tiene sentido aplicar técnicas de minería de datos, *Big Data* y *Business Intelligence* (BI) para poder dar valor añadido a la información recopilada. Las autoridades sanitarias necesitan dimensionar y planificar adecuadamente los servicios e infraestructuras para prestar un servicio adecuado al ciudadano y con un coste contenido. Esta necesidad está impulsando marcos de trabajo como BSHSF (*Big data enabled Smart Healthcare System Framework*) [15]. La expansión del *Big Data* y la evolución de la IoT han jugado un papel importante en la viabilidad de las iniciativas de ciudades inteligentes [16].

## DISCUSIÓN Y CONCLUSIONES

En este artículo se ha realizado recorrido por la innovación tecnológica aplicada en salud. Concretamente, se ha fijado el marco en el entorno de la IoMT como recurso para la introducción de servicios de salud inteligentes en el ámbito de las *Smart Cities*. Este proceso nos ha llevado a recorrer las diferentes etapas o características de las plataformas IoMT. En particular, los sensores para la recolección de datos de salud, las tecnologías de comunicaciones, las estrategias de seguridad y privacidad y, finalmente, los retos de integración y explotación de dichos datos. En lo referente a la sensorica, se ha producido un ascenso notable en la variabilidad y disponibilidad de sensores de salud con capacidad de conexión a Internet, bien sea directamente o a través de una pasarela. La tendencia actual de medir todo lo medible conlleva, sin embargo, una gestión más complicada en lo que se refiere a las comunicaciones, y la integración y explotación de datos con seguridad.

Las comunicaciones, principalmente inalámbricas, se vislumbran como un elemento clave para los entornos contextuales interactivos de las *Smart Cities*. En concreto, las redes heterogéneas HetNet permiten crear entornos colaborativos entre diferentes tipos de redes, muy apropiadas para el contexto de *Smart Cities*, si bien su gestión puede ser más complicada que una red homogénea.

En lo referente a la seguridad y privacidad, esta capa adicional ha de implementarse de la manera más transparente posible para el usuario, si bien es cierto que mejorar la seguridad y la privacidad generalmente implica una complejidad adicional para el usuario, por ejemplo, obligándole a efectuar una gestión de claves. Asimismo, la introducción de estrategias de seguridad y privacidad puede comprometer la operatividad, incrementando la latencia y el coste computacional (que redundará en mayor consumo energético).

Finalmente, el despegue de loMT va a producir (está produciendo ya) una ingente cantidad de datos de salud, cuya gestión y apropiada explotación resultan cruciales para conseguir una mejora de la calidad de vida de los ciudadanos. Para la gestión, es relevante seleccionar un modelo de negocio apropiado (SaaS, PaaS o IaaS), con sus ventajas e inconvenientes descritas en este artículo, mientras que para la explotación, la tendencia actual nos lleva a sistemas *Big Data* y *Business Intelligence*, a través de los cuales las plataformas loMT pueden ofrecer un servicio integral a las *Smart Cities*, todo ello sin olvidar, como ya se ha mencionado la seguridad y la privacidad de los ciudadanos.

## BIBLIOGRAFÍA

- [1] M. Waldrop. The chips are down for Moore's law. *Nature*, February 2016. <https://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338>. Último acceso: Abril 2018
- [2] Everis Health. <https://www.ehcos.com>. Último acceso: Abril 2018
- [3] World Urbanization Prospects. <https://esa.un.org/unpd/wup>. Último acceso: Abril 2018
- [4] Smart Cities partnership in Europe. <http://ec.europa.eu/eip/smartcities>. Último acceso: Abril 2018
- [5] Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018. <https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018>. Último acceso: Abril 2018
- [6] H. Hafez, T.L. Robertson, G.D. Moon, Kit-Yee Au-Yeung, M.J. Zdeblick, G.M. Savage. An Ingestible Sensor for Measuring Medication Adherence. *IEEE Transactions on Biomedical Engineering*, 62(1), pp. 99-109. January 2015. doi:10.1109/TBME.2014.2341272.
- [7] J. Kim, A.S. Campbell, J. Wang. Wearable non-invasive epidermal glucose sensors: A review. *Talanta*, 177, pp. 163-70. 2018. doi:10.1016/j.talanta.2017.08.077.
- [8] L. Lipani, B.G.R. Dupont, F. Doungmene, F. Marken, R.M. Tyrrell, R.H. Guy, A. Ilie. Non-invasive, transdermal, path-selective and specific glucose monitoring via a graphene-based platform. *Nature Nanotechnology*, [publicación on-line]. 2018. doi:10.1038/s41565-018-0112-4.
- [9] A. Solanas, C. Patsakis, M. Conti, I.S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P.A. Perez-Martinez, R. Di Pietro, D.N. Perrea, A. Martinez-Balleste. Smart Health: A Context-Aware Health Paradigm within Smart Cities. *IEEE Communication Magazine*, 52(8), pp. 74-81. 2014. doi: 10.1109/MCOM.2014.6871673
- [10] Y. Cherdantseva, J. Hilton, O. Rana, W. Ivins, A multifaceted evaluation of the reference model of information assurance & security, *Computer Security* 63, pp. 45-66. 2016. doi:10.1016/j.cose.2016.09.007.
- [11] M.J. Harvey, M.G. Harvey, Privacy and security issues for mobile health platforms, *Journal of the Association for Information Science and Technology*, 65, pp. 1305-18. 2014. doi:10.1002/asi.23066.
- [12] S. Arora, J. Yttri, W. Nilsen, Privacy and Security in Mobile Health (mHealth) Research, *Alcohol Research: Current Reviews*, 36(1), pp. 143-51. 2014
- [13] A.A. Atienza, C. Zarcadoolas, W. Vaughan, P. Hughes, V. Patel, W.-Y.S. Chou, J. Pritts, Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings From a Mixed-Methods Study. *Journal of Health Communication*. 20, pp. 673-9. 2015. doi:10.1080/10810730.2015.1018560.
- [14] J.I. Guerrero, A. García, E. Personal, J. Luque, C. León. Heterogeneous data source integration for smart grid ecosystems based on metadata mining. *Expert Systems with Applications*, 79, pp. 254-68. 2017. doi:10.1016/j.eswa.2017.03.007.
- [15] I. Pramanik, R.Y.K. Lau, H. Demirkan, A.K. Azad. Smart health: Big data enabled health paradigm within smart cities. *Expert Systems with Applications*, 87, pp. 370-83. 2017. doi:10.1016/j.eswa.2017.06.027.
- [16] I.A.T Hashem, V. Chang, N.B. Anuar, K. Adewole, I. Yaqoob, A. Gani, E. Ahmed, H. Chiroma. The role of big data in smart city. *International Journal of Information Management*. 36(5), pp. 748-58. 2016. doi:10.1016/j.ijinfomgt.2016.05.002.



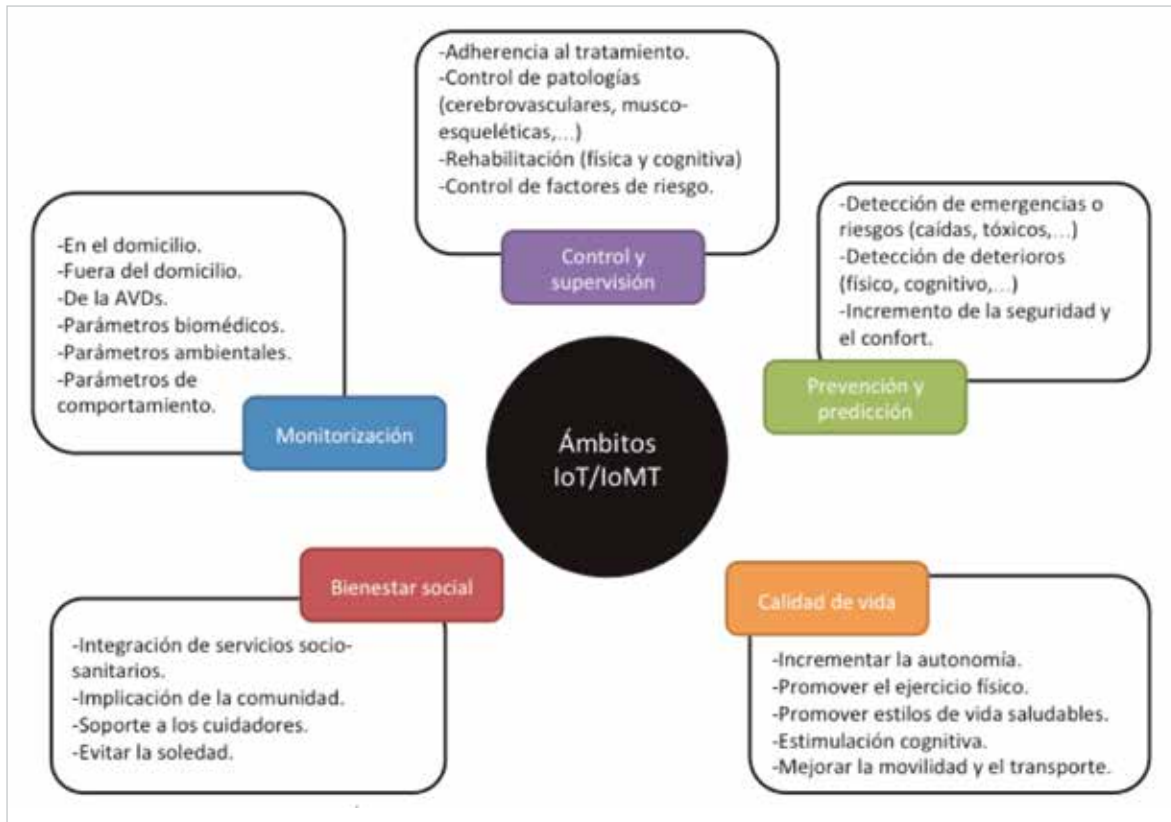


Figura 1. Ámbitos de impacto de IoT/IoMT en Telesalud y AAL

porarán muchas más que tan siquiera somos capaces de imaginar.

La figura 1, sin ser exhaustiva, muestra algunos de los ámbitos de Telesalud y AAL en los que IoT tiene un impacto directo para mejorar y desarrollar nuevos servicios de eSalud:

- **Monitorización:** tanto dentro como fuera del hogar, de parámetros biomédicos, ambientales o de contexto. Monitorización de las Actividades de la Vida Diaria (AVD).
- **Control y Supervisión:** supervisando adherencias al tratamiento, actividades de rehabilitación, determinadas patologías e, incluso, factores de riesgo.
- **Prevención y predicción:** con técnicas de IA permitiendo la detección temprana de posibles complicaciones o situaciones de riesgo, incrementando la seguridad de los pacientes y disminuyendo los ingresos hospitalarios.
- **Calidad de vida:** mejorando la autonomía individual, promoviendo hábitos y estilos de vida saludables.

- **Bienestar social:** posibilitando integraciones entre los entornos sociales y sanitarios, teniendo en cuanto a los cuidadores y facilitándoles su labor en la atención al paciente.

## RETOS

IoT / IoMT en Telesalud y AAL tendrá que hacer frente a retos, no exclusivamente de contexto tecnológico, sino también de predisposición de uso, de normativas existentes y de modelos de negocio y asistenciales que se verán profundamente afectados.

Los retos de contexto tecnológico serán, en muchos casos, compartidos con otros sectores: de hardware (gestión de energía en dispositivos, conectividad), de estándares (integración, interoperabilidad, interacción), de seguridad y privacidad (vulnerabilidad de infraestructura y dispositivos, exposición total involuntaria de nuestros datos, implicaciones legales) y de es-



***IoT / IoMT en Telesalud y AAL tendrá que hacer frente a retos, no exclusivamente de contexto tecnológico, sino también de predisposición de uso, de normativas existentes y de modelos de negocio y asistenciales que se verán profundamente afectados***

calado y rendimiento (por el incremento de dispositivos y datos generados).

Pero son los no tecnológicos, los retos más complicados que tendrá que abordar: legislativos (regulaciones, homologaciones de dispositivos sanitarios, RGPD en salud), cambio de procesos y procedimientos en las organizaciones, integración de la HCE y los datos IoMT, sostenibilidad del sistema, ritmo de adopción de dispositivos y wearables por la ciudadanía... No en vano, IoT se encuentra en el “Pico de expectativas” y queda aún un largo camino para que sea una realidad en el día a día de la Telesalud y AAL.

## CONCLUSIONES

No cabe duda de que IoT / IoMT transformará el sector de la salud al redefinir cómo las aplicaciones, los dispositivos y las personas interactúan y se conectan entre sí para mejorar la calidad de vida de los pacientes-ciudadanos en entornos extra-hospitalarios (incluido AAL) y, por otra parte, conformar un sistema de salud integrado con el objetivo de garantizar que los pacientes reciban un mejor cuidado, optimizar los resultados del tratamiento y lograr la sostenibilidad del sistema.

A pesar de la avalancha de cifras que continuamente los analistas están arrojando sobre IoT, debemos ser cautos; En la adopción de una nueva innovación, es común la existencia de una cierta confusión inicial y la incapacidad de visualizar todo el potencial, con procesos y procedimientos en las organizaciones que a veces son más barreras que facilitadores a la hora de un despliegue y explotación adecuados.

## AGRADECIMIENTOS

Trabajo financiado por el proyecto de investigación PI15CIII/00003 “Plataforma de innovación en Telemedicina y e-Salud: TIC para los retos de I+i en servicios de salud (*Platform for Innovation in Telemedicine and e-Health: ICT for the challenges of I + i in health services*) – PITES-TIiSS”.

## BIBLIOGRAFÍA

- [1] “Gartner says 6.4 billion connected things will be in use in 2016, up 30 percent from 2015”. <http://www.gartner.com/newsroom/id/3165317>
- [2] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., et al. (2015). “The internet of things: Mapping the value beyond the hype”. <http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>
- [3] Gubbia, J., Buyya, R., Marusica, B.S., Palaniswamia, M. (2013). “Internet of things (IoT): a vision, architectural elements, and future directions”. *Future Gener. Comput Syst.* 29 (7), 1645–1660.
- [4] GrowthEnabler, (2017). “Market Pulse Report, Internet of Things (IoT)”. <https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf>
- [5] Panetta K., (2017). “Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017”. Gartner Inc. <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>
- [6] Clayton M.C., Bohmer R., Kenagy J. (2000). “Will Disruptive Innovations cure Health Care?”. *Harvard Business Review*. Septiembre-octubre, pp. 102-12.
- [7] [Clinicaltrials.gov database](https://clinicaltrials.gov/), U.S. National Library of Medicine. <https://clinicaltrials.gov/>
- [8] Cattell J., Chilukuri S., Levy M. (2013). “How big data can revolutionize pharmaceutical R&D”. McKinsey&Company. <https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-big-data-can-revolutionize-pharmaceutical-r-and-d>
- [9] Jain, S.H., Powers, B.W., Hawkins J.B., & Brownstein, J.S. (2015). “The digital phenotype”. *Nature Biotechnology*, 33(5). 462-463 <http://doi.org/10.1038/ntb.3223>
- [10] U.S. Food&Drug Administration FDA, (2018). “Real World Data and Real World Evidence”. <https://www.fda.gov/ScienceResearch/SpecialTopics/RealWorldEvidence/default.htm>
- [11] The IoT European Large-Scale Pilots Programme’s website: <https://european-iot-pilots.eu/>
- [12] ACTIVAGE project’s website: <http://www.activage-project.eu/>