Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

EL INTERNET DE LAS COSAS Y SU VINCULACIÓN CON LA INGENIERÍA INDUSTRIAL

Danino, Carlos Ignacio; Rouillon, Esteban José

Facultad de Ciencias Exactas, Ingeniería y Agrimensura, Universidad Nacional de Rosario
FCEIA.CID@gmail.com; EstebanJRouillon@gmail.com

RESUMEN

El Internet de las Cosas (IoT) actualmente juega un papel preponderante y cada vez más creciente dentro de la Ingeniería Industrial. Son muchas las empresas o áreas de trabajo que han implementado el IoT como parte de su solución tecnológica; por ello, es de primordial importancia la colaboración entre la Ingeniería Industrial y el IoT para enfrentar los retos tecnológicos y éticos del futuro, asegurando así un impacto positivo en la sociedad.

Como objetivo de la presente investigación, se busca comunicar la efectividad del IoT en la optimización de los procesos productivos, analizados en distintas áreas de implementación. Además, se indagará acerca de los riesgos a la privacidad de los datos que acompañan a la implementación de la presente herramienta.

A tal fin, se persigue una metodología de investigación, recopilando datos mediante búsquedas y observaciones. Posteriormente, se interpretarán los mismos haciendo hincapié en los beneficios asociados a la Ingeniería Industrial y el riesgo vinculado a la privacidad de los datos.

A modo de conclusión, se espera encontrar que existe una actual necesidad por parte de las empresas de contar con un Ingeniero Industrial capacitado en la implementación del Internet de las Cosas; de igual manera, se entiende que será de imperiosa necesidad la creación de un conjunto de políticas éticas de uso.

Palabras Claves: Internet; Cosas; Implementación; Ejemplos; Privacidad.

ABSTRACT

Internet of Things (IoT) is currently playing an increasingly important role in Industrial Engineering. Many companies or work areas have already implemented IoT as part of their technological solution; therefore, collaboration between Industrial Engineering and IoT is essential in order to face, in the future, technological and ethical challenges, thus ensuring a positive impact on society.

The objective of this research is to communicate the effectiveness of IoT in optimizing production processes, while analyzing different areas of implementation. In addition, it will investigate the data privacy risk that comes with the implementation of this tool.

To this end, a research methodology is pursued, collecting information through searches and observations. Then, information will be analized while emphasizing the benefits associated with Industrial Engineering and the risk linked to data privacy.

In conclusion, the data thus collected is expected to determine that there is a current need for enterprises to have an Industrial Engineer with experience in the implementation of the Internet of Things; moreover, it will be absolutely necessary to create a set of ethical policies for the use of IoT.

Keywords: Internet; Things; Implement; Examples; Privacy

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

1. INTRODUCCIÓN

La película “El Golpe” (*The Sting*, 1973), protagonizada por Paul Newman y Robert Redford, ganó 7 premios Oscar incluyendo mejor película, director y guión, tras obtener 10 nominaciones en total. Ambientada en 1936, la película se basaba en una estafa que hacía uso de una técnica de apuestas en carreras de caballos denominada “apuesta tardía”, por la cual estaba permitido realizar la apuesta hasta el momento exacto en que comenzaran a llegar los resultados. En esos tiempos, la empresa *Western Union* transmitía por teletipo los resultados de una carrera *recién minutos después de haber terminado la misma*. Por tal motivo, de poder retrasar el envío de los datos, los estafadores podían usar un teletipo paralelo o un teléfono para informarse antes y así apostar al caballo ganador.

En la actualidad, los autos de Fórmula 1 están equipados con una unidad de control electrónico (ECU) que recoge datos de más de 300 sensores y, mediante un sistema de telemetría, los envía al *pit* donde los ingenieros toman decisiones cruciales en tiempo real. Un claro ejemplo tuvo lugar en el Gran Premio de Países Bajos el 27 de agosto pasado, donde la diferencia entre llamar al *box* al piloto para cambiar las cubiertas en la vuelta actual o en la siguiente llegó a costar hasta 10 posiciones.

A lo largo de los años, la capacidad de transmisión de los datos se ha ido incrementando a pasos agigantados, de hecho, las grandes potencias ya se encuentran desarrollando la tecnología de comunicación 6G, siendo que existen muchos países que aún no cuentan con 5G. Es precisamente esta evolución lo que ha dado lugar a lo que hoy conocemos como Internet de las Cosas.

En el presente trabajo nos centraremos en la productividad del Internet de las Cosas como parte de un sistema de información, demostrando los beneficios de su aplicación y la generación de valor tanto para empresas de producción (Industria, Agricultura) como para empresas de servicio (Medicina) y sus clientes. Además, en base a la experiencia laboral de los autores, comentaremos las falencias y los riesgos asociados a la privacidad en cada una de las mencionadas áreas.

2. MARCO TEÓRICO

Se define como Internet de las Cosas (*Internet of Things – IoT*) a la interconexión de dispositivos físicos, a través de una tecnología de comunicación, mediante sensores y software específicos. Dicha definición ofrece la posibilidad de analizar los distintos elementos que forman parte del IoT:

- *los dispositivos físicos*, entendiéndose a los mismos como las “Cosas” de uso;

- *la tecnología de comunicación*, necesaria como medio de transmisión de los datos; si bien “Internet” es la más popular, los dispositivos conocidos como IoT también se conectan a través de *Bluetooth*, redes 4G y 5G, *transponders* satelitales o redes *ZigBee*, por mencionar algunas tecnologías;

- *los sensores*, siendo dichos elementos los responsables de la captación de los datos del entorno; a modo de ejemplo, se pueden mencionar sensores de movimiento, de presión, de temperatura, de sonido, de luminosidad, de caída, sensores táctiles y biométricos;

- *el software específico*, tanto para su funcionamiento como para el procesamiento de los datos mediante una interfaz de usuario; ambos impactan en la vulnerabilidad de los dispositivos.

Es importante aclarar que el software específico puede dividirse en dos grandes rubros: el *firmware* del dispositivo es un software de bajo nivel que hace referencia a su funcionamiento básico, es un código cerrado y escrito por el fabricante, inherente al hardware, que le permite al dispositivo realizar tareas de encendido, de control de funcionamiento, de conexión a otros dispositivos u otro software y de apagado; por otro lado, el *software de interfaz de usuario* es a menudo conocido como *App* (principalmente en usos hogareños), y es el encargado de proporcionar al usuario una forma de interactuar con el dispositivo, permitiendo analizar los datos recabados y tomando acción al respecto.

2.1. Matriz de aplicación del Internet de las Cosas

En forma general, se pueden describir 4 áreas de uso del IoT, tal como muestra la siguiente Figura 1:

Figura 1: Matriz de aplicación de IoT.

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

El área de **Seguridad** hace referencia al objetivo principal del dispositivo, siendo el mismo detectar una amenaza con el fin de informar a un ser humano responsable para que este último tome acción.

A tal fin, estos dispositivos IoT están equipados con cámaras de reconocimiento facial, sensores biométricos, de detección de movimiento o temperatura y, en algunos casos más avanzados, están dotados de movimiento autónomo dando lugar a la robótica en seguridad.

Un detalle importante es que, en todos los casos, el dispositivo IoT de seguridad no toma acción por sí solo: ya sea que estemos hablando de un robot *Knightscope K5* (Figura 2) dotado con reconocimiento facial y la habilidad de leer las patentes de vehículos próximos, como de un sistema de alarma *ZeroVision* que llena de humo denso la habitación de una casa, la capacidad del dispositivo IoT está limitada a informar a un ser humano con poder de decisión, cuya acción podrá ser la de dar aviso a las fuerzas de seguridad y/o activar medidas de seguridad pasivas, no dañinas.

Figura 2: Robot de seguridad Knightscope K5 equipado con IoT.

El área de **Confort** hace referencia a la automatización del hogar, mediante dispositivos domésticos que buscan mejorar la calidad de vida. Su objetivo primordial es otorgar mayor comodidad al usuario y una mayor eficiencia, por rapidez o economía, en la ejecución de las tareas hogareñas.

Los sensores de los dispositivos IoT captan variables del entorno e informan al usuario para que tome acción al respecto. Un ejemplo son los lavarropas inteligentes, los cuales poseen cámaras que identifican el tipo de tela, el color y hasta el nivel de suciedad, conjuntamente con sensores de carga que les permiten determinar el peso de la ropa; posteriormente, determinan la cantidad y tipo de detergente, temperatura del agua y tiempo de lavado, sugiriendo al usuario dicha información.

Los dispositivos IoT hogareños también tienen la capacidad de tomar acción en forma directa si el usuario lo requiere. Es posible que el aire acondicionado se encienda solo si considera que la temperatura del ambiente no es agradable o que la aspiradora inteligente reconozca a la mascota de la casa y emita una señal sonora o la rocíe con agua para lograr que la misma se aleje (Figura 3).

Figura 3: Robot aspiradora reconoce a mascota.

El área de **Big Data** se nutre del resto de las áreas de aplicación de IoT: Seguridad, Confort y Productividad. El objetivo de las empresas es recabar los datos de los propios dispositivos, conjuntamente con los datos de los usuarios y formas de uso, con el fin de identificar tendencias, patrones, gustos, preferencias y así retroalimentar y mejorar las funciones de los dispositivos IoT.

Esta información representa en la actualidad un activo de vital importancia para las empresas. Por tal motivo, a medida que las tecnologías de comunicación avanzan, se favorece el armado de un Big Data a partir de su vinculación con los dispositivos IoT.

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

3. PRODUCTIVIDAD BASADA EN LA INTERNET DE LAS COSAS

El área de **Productividad**, último eslabón de la matriz de aplicación de IoT, comprende el uso de dispositivos IoT con la finalidad de optimizar la producción, reducir los costos y aumentar la eficiencia de procesos y servicios; además, ayudan a comprender mejor las necesidades y comportamientos de los clientes, mejorando la satisfacción de los mismos. Dentro de esta área existen diversas clasificaciones según su rubro, tales como "*Internet de las Cosas de la Construcción*" (IoCT), abocado exclusivamente a empresas constructoras; "*Internet de las Cosas del Transporte*" (TIoT), utilizado para el seguimiento de vehículos y su logística; "*Internet de las Cosas en Ciudades Inteligentes*" (SCIoT), denominado así porque conecta infraestructuras, edificios y servicios públicos.

Sin embargo, las tres clasificaciones más comunes abarcan a la medicina, la industria y la agricultura.

3.1. Internet de las Cosas Médicas (*Internet of Medical Things - IoMT*)

En los últimos años, gracias al avance de la tecnología, la medicina ha conseguido mejorar los procedimientos, los dispositivos y los medicamentos que se están implementando día a día.

Existen diferentes términos específicos como el "*Internet de Cosas Médicas*" (IoMT), el "*Internet de las Cosas para el Cuidado de la Salud*" (IoHcT), "*e-Salud*", "*Telemedicina*", entre otros. Este trabajo se centrará únicamente en IoMT debido a que es el término más amplio y abarcador de los restantes.

El IoMT comprende un sistema interconectado de dispositivos y aplicaciones que permiten aprovechar el IoT dentro de la medicina, con el fin de generar soluciones personalizadas a las necesidades de un paciente, independientemente de donde se encuentre el mismo o los especialistas médicos o los centros de salud. El flujo de información se puede apreciar en la Figura 4.

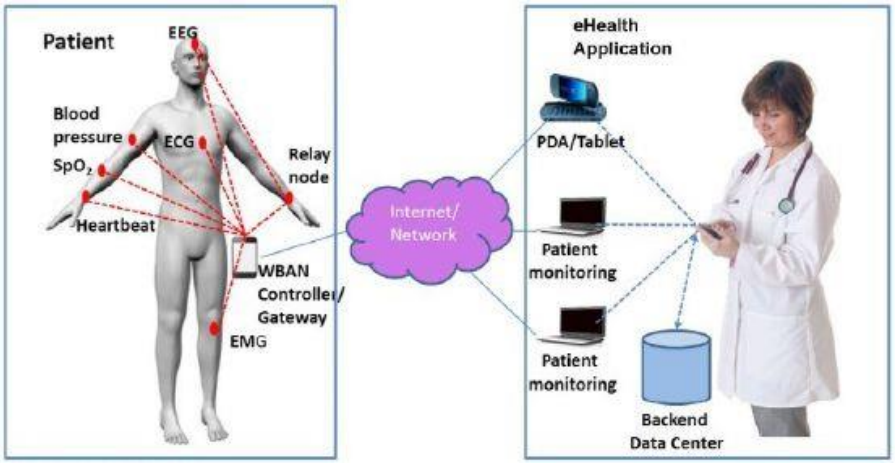

Figura 4: Dispositivos IoMT y el flujo de la información Paciente-Médico.

Las aplicaciones del IoMT son variadas y están ampliamente diversificadas dentro del sector de la medicina, desde la prevención de enfermedades y la promoción de la actividad física hasta la intervención remota en situaciones de emergencia. A continuación se describirán variadas formas de implementación del IoMT con ejemplos asociados.

3.1.1. Manejo de enfermedades crónicas, con o sin intervención remota

Los dispositivos conectados al IoMT ofrecen alternativas prometedoras en cuanto al manejo de enfermedades crónicas como la hipertensión, la falla cardiaca y la diabetes. Estos dispositivos se utilizan para monitorear diversos parámetros como la presión sanguínea, la conducción eléctrica del corazón y el nivel de azúcar en sangre, entre otros. Los dispositivos IoMT monitorean al paciente en tiempo real, es decir, los datos obtenidos pueden ser procesados y utilizados al instante, ya sea para implementar futuros tratamientos o para predecir los avances de la enfermedad.

En algunos casos, los datos de los sensores se combinan con parámetros de respuesta automáticos, que en casos de emergencia permiten intervenciones remotas. Tales intervenciones oportunas ofrecen asistencia médica de alta tecnología, llegando a salvar la vida del paciente.

Un claro ejemplo es el chip debajo de la piel que posee el futbolista Sergio "*Kun*" Agüero. Dicho chip mide la conducción eléctrica del corazón para detectar si hay arritmias o cuadros de síncope. Los sensores envían información al celular del futbolista y al del propio médico; de hecho, durante el

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

partido entre Argentina y Países Bajos (Qatar 2022), el "*Kun*" Agüero debió contactarse varias veces con su médico pues su frecuencia cardíaca superaba los 100 latidos por minuto. El chip implantado es exclusivamente de monitoreo, pero existen versiones que además son en sí cardiodesfibriladores, de tal forma que si se presenta una arritmia grave, provocan una descarga eléctrica al corazón.(Costa, J, marzo 2023, La Nación)

3.1.2. Logística de medicamentos y asistencia de medicación a distancia

Las etiquetas de RFID (identificación por radiofrecuencia) basadas en IoMT gestionan los problemas de disponibilidad de medicamentos y el costo de su suministro. Algunas directrices dadas por la FDA (Administración de Alimentos y Medicamentos de los Estados Unidos) incluyen la adición de las etiquetas inteligentes en los envases de medicamentos, las cuales permiten a los fabricantes mitigar los riesgos y las pérdidas durante la cadena de suministro y la administración.

Por otro lado, también se han desarrollado pastillas inteligentes que, una vez ingeridas, ayudan a monitorear las dosis de medicamentos y la farmacodinamia del paciente. Mediante las mismas, se recopilan datos específicos del paciente y posibilitan al profesional médico analizar los mismos en tiempo real, comparando con registros pasados, decidiendo el curso futuro de la medicación y corrigiendo tratamientos en forma inmediata. En relación al paciente, mejoran su calidad de vida, logrando que se sienta protegido en todo momento, recibiendo una atención personalizada y reduciendo el tiempo de atención al reducir la necesidad de acudir y esperar en un centro de salud.

3.1.3. Bienestar y cuidado preventivo (asesoramiento en el estilo de vida)

Los dispositivos conectados a IoMT facilitan la supervisión mediante sistemas que monitorean la dieta, la actividad física y la calidad de vida del paciente. Día a día, éstos son más innovadores, desde implantes de chips hasta sensores que están incluidos en la ropa deportiva; ambos brindan información sobre el porcentaje de grasa corporal y/o visceral, índice de masa muscular, porcentaje de hidratación, etc. lo que le permite al paciente accionar de acuerdo al estilo de vida deseado.

Durante la pandemia de 2020, una de las medidas preventivas recomendadas por médicos clínicos fue la adopción de los dispositivos IoT conocidos como *smart-bands*, siempre que pudieran registrar el nivel de oxígeno en sangre. La inflamación pulmonar, que podía presentarse como dificultad para respirar o sensación de ahogo, era uno de los primeros síntomas conocidos; por otro lado, se buscaba evitar que las personas asistieran a los centros de salud salvo que fuera realmente necesario. La recomendación era que, aún con cierto grado de inexactitud, si la *smart-band* indicaba un nivel de oxígeno del 93% o menos, el paciente solicitara un turno en la guardia médica.

3.1.4. Riesgos y limitaciones éticas asociadas al Internet de las Cosas Médicas

Actualmente los bancos y financieras requieren cada vez menos personal en sus sucursales debido al uso del *Homebanking*, a través de una PC o del celular. En los centros de salud ocurre lo opuesto: el acceso a los dispositivos IoMT es costoso para muchas personas y, aún accediendo a los mismos gracias a la ayuda del estado, puede ser inviable para aquellos que no tienen acceso a internet.

Además, aún cuando los pacientes tengan acceso, será necesario contar con un centro de datos acorde y con especialistas expertos en el manejo de la información; siendo necesaria una erogación monetaria tanto en los centros privados como en los estatales. Inclusive, en caso de lograr un acceso de datos fluido, no hay que dar por descontado que el médico sea capaz de interpretar correctamente los datos recopilados por los dispositivos IoMT; la falta de estándares de medición, el volumen de datos y los errores propios en la toma de los mismos a distancia, podría llegar a confundir al profesional médico, lo cual conduciría a diagnósticos y/o tratamientos incorrectos.

Es en relación a la salud, donde la privacidad y seguridad de la información se vuelve crítica. Los dispositivos IoMT, al estar conectados a internet, pueden ser objeto de un ataque informático… ¿Qué sucedería si un hacker lograra conectarse a un marcapasos inteligente? De igual manera, los datos recabados también pueden ser objeto de un ataque informático. Si se filtrara una base de datos de aspirantes laborales, con sus problemas de salud preexistentes… ¿Qué impediría a un empleador discriminar a un candidato en base a dicho informe? Finalmente, y considerando que muchos datos recabados son usados por los fabricantes de dispositivos IoMT para mejorar sus productos, o por las empresas farmacéuticas para mejorar sus medicamentos… ¿Dónde se traza la línea entre la privacidad de un paciente y la necesidad de la mejora continua para el bien de la comunidad?

Por estas razones, los sistemas de información que usen dispositivos IoMT deben garantizar un gran nivel de seguridad en cuanto a la integridad, protección y encriptación de sus comunicaciones, como

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

también al propio acceso a los componentes del sistema. Asimismo, es imprescindible desarrollar estándares de privacidad y políticas de uso empresarial vinculadas al Internet de las Cosas Médicas.

3.2. Internet de las Cosas Industriales (*Industrial Internet of Things - IIoT*)

El concepto de "*Industria 4.0"* se originó en un proyecto de estrategia de alta tecnología del gobierno de Alemania y fue mencionado por primera vez en la Feria de Hannover en 2011. A través del "*4.0"* se pretendió establecer el origen de la cuarta revolución industrial, marcada por el avance de las tecnologías de comunicación y la consecuente capacidad de obtener, almacenar, transmitir, compartir, filtrar y procesar los datos en las industrias. La combinación del Internet de las Cosas y del concepto de "*Industrial 4.0"* da lugar al Internet de las Cosas Industriales (IIoT).

En la revisión bibliográfica se han hallado numerosas definiciones del IIoT, algunas hacen referencia a la estrecha integración de los objetos físicos propios de la industria con internet, a fin de detectar, monitorizar y controlar los procesos, promoviendo el progreso de los negocios y la fabricación. Otras definiciones simplemente hacen referencia al IoT vinculado al proceso de fabricación en sí mismo.

Teniendo en cuenta lo anterior, en el presente trabajo se define IIoT como una red de dispositivos fabriles que se pueden conectar y transferir datos entre sí en tiempo real, implementando sistemas de red con el objetivo de monitorizar, controlar y analizar grandes volúmenes de datos, permitiendo la reducción de costos, el aumento de la productividad y una mejorada toma de decisión en la industria.

Cada día más empresas usan el IIoT debidos a la gran cantidad de beneficios que se obtienen en el proceso productivo; entre los usos más significativos se pueden encontrar los siguientes:

3.2.1. Gestión remota y conexión digital

A través de una Intranet empresarial, las máquinas equipadas con dispositivos IIoT se conectan a los distintos partícipes: otros dispositivos IIoT, gerentes, personal capacitado y operarios de campo.

Sin importar su ubicación física, los gerentes pueden identificar las áreas críticas y establecer o modificar los objetivos de producción y/o de abastecimiento de insumos; luego el personal capacitado define las métricas de operación en concordancia con los informes generados por otras máquinas (que también forman parte del IIoT) y, finalmente, los operarios de campo controlan el correcto andar operativo. Esto otorga mayor flexibilidad y versatilidad, en especial en líneas de producción.

3.2.2. Supervisión autónoma (P2D)

El Procesamiento en el Dispositivo (P2D) es una tecnología que permite procesar datos en el dispositivo en tiempo real. La combinación entre un dispositivo IIoT y un dispositivo P2D posibilita a la máquina tomar decisión en forma autónoma y en tiempo real: gracias a los sensores IIoT una máquina captura al instante los datos de otras máquinas, en flujo ascendente y/o descendente, que impactan en su rendimiento; luego, gracias al dispositivo P2D, también posee la capacidad de procesar esos datos y tomar decisiones en forma autónoma, buscando cumplir el objetivo predefinido.

A modo de ejemplo, en una cadena de suministro, los parámetros y objetivos podrían ser maximizar el tiempo si hubiera insumos ociosos, reducir el costo de energía si hubiera una demora en el flujo productivo (Figura 5), nivelar la carga a fin de eliminar un efecto látigo, u otra decisión gerencial.

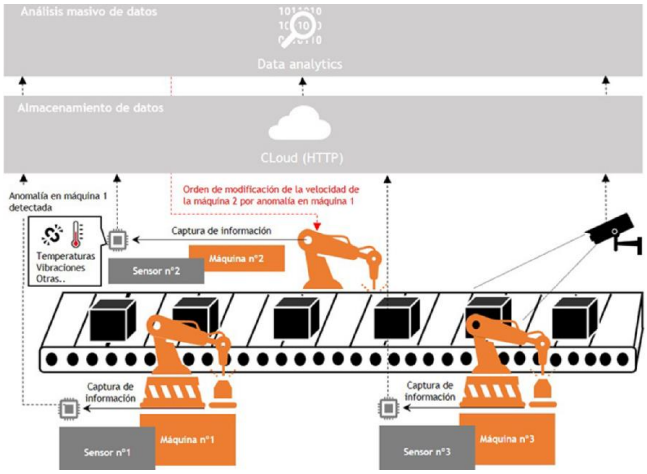

Figura 5: Ejemplo de Supervisión Autónoma, combinando IIoT con P2D.

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

3.2.3. Mantenimiento preventivo y predictivo

La aplicación de sensores IoT en máquinas de fabricación posibilita emitir alertas de reparación y mantenimiento basadas en condiciones previamente establecidas. Cuando los parámetros se cumplen (horas de trabajo, por ejemplo), los dispositivos IIoT inherentes a las máquinas pueden simplemente emitir un alerta o bien disminuir la carga de trabajo, incluso deteniendo la máquina. Esto permite que las empresas puedan evitar roturas con los consecuentes costos de parada asociados.

En forma predictiva, la evaluación continua del funcionamiento de la máquina, utilizando los datos en tiempo real, facilita predecir cuándo la misma podría fallar, ayudando a determinar cronogramas de mantenimiento y garantizando una producción sin inconvenientes.

3.2.4. Logística de transporte e inventario

Bajo IIoT, se plantea el concepto de "*visibilidad total en tiempo real*". Dicho concepto abarca el monitoreo de vehículos, rutas y entregas en cualquier fase dentro del proceso, debido a que los vehículos pueden ser equipados con sensores vinculados al GPS para actualizar continuamente su ubicación. De esta manera, hasta el mismo cliente (si es que se le brinda acceso) puede conocer el trayecto que está haciendo su producto y el tiempo estimado de arribo.

Internamente, facilita la medición del consumo de combustible, mejora la rentabilidad encontrando las mejores rutas de entrega, calcula de antemano el costo de peajes y estacionamiento e inclusive puede sugerir al conductor rutas alternativas ante la detección de exceso de tránsito.

No sólo los vehículos pueden contar con dispositivos IIoT. La empresa *MAERSK* combina IIoT bajo *Blockchain* en todos sus contenedores, creando una extranet llamada *TradeLens*. La misma es una plataforma industrial, abierta y neutral, que se usa para intercambiar información sobre la documentación de los contenedores, validar su contenido y controlar los mismos online.

En referencia a la logística interna, el IIoT permite localizar en tiempo real productos y objetos en las instalaciones de almacén: contenedores, pallets, cajas y productos intermedios. Esto promueve la implementación de gestiones rápidas de entrada y salida en los almacenes, facilita el trabajo en las tareas de recogida de pedidos y en las tareas de gestión interna del stock. Además, previene el almacenamiento erróneo de mercancías, detectando instantáneamente irregularidades y fallos, lo que ayuda a ahorrar tiempo y a aumentar la productividad.

Amazon hace uso del IIoT aplicado a la logística interna en sus depósitos: en vez de colocar todos los productos iguales o del mismo tipo en un mismo sector, el almacenamiento sigue un orden aleatorio, donde la única regla es *la velocidad en colocar o retirar un producto de la estantería* (ver Figura 6). Un empleado coloca siempre un producto en el estante más próximo; luego, el sensor IIoT de cada estante escanea dicho producto y manda una señal a la computadora principal informándole dónde ha quedado almacenado. Posteriormente, cuando un producto sea requerido, a fin de retirar el mismo lo más rápidamente posible, el sistema buscará todos los producto iguales almacenados y le informará al operario cuál es la ruta más rápida al producto en cuestión. (Rubin, B., diciembre2015, CNET).

Figura 6: Almacenamiento "caótico" en el depósito de Amazon Prime.

3.2.5. Seguridad en la planta

Los dispositivos fabriles no necesariamente son máquinas. Los dispositivos portátiles, como los chalecos de protección inteligentes, pueden recopilar datos sobre la ubicación y el comportamiento de

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

los trabajadores. Dichos datos se conectan a su vez con otros dispositivos IIoT y se pueden utilizar para determinar zonas prohibidas o identificar situaciones peligrosas.

Los autores Singh y Kaushik brindan el siguiente ejemplo: *"Si un sensor detecta a un trabajador en una zona de peligro, el sistema de IIoT puede generar una alerta para que la máquina se detenga o para que el trabajador se aleje de la máquina."* (Singh & Kaushik, 2022, p. 157).

Los empleados con dispositivos portátiles y/o sensores incorporados en su ropa de trabajo, informarán de forma automática datos como la frecuencia cardíaca, el ritmo respiratorio y la temperatura corporal. Los mismos pueden ser utilizados para identificar a los trabajadores que están fatigados o en situaciones límites, sugiriendo tiempos de descanso y evitando errores o accidentes.

3.2.6. Control de calidad

El IIoT permite realizar una inspección del producto final utilizando cámaras y/o sensores 3D, ultrasonido o incluso rayos X. Tras analizar los materiales del producto final, su composición, el peso, sus medidas y tolerancias, automáticamente es posible determinar no sólo si el producto es defectuoso sino también en qué lugar del proceso productivo se originó el defecto.

Este análisis, si bien es costoso, puede efectuarse con una máquina IIoT en cualquier parte del proceso, permitiendo determinar falencias en productos intermedios o semi-elaborados.

3.2.7. Inconvenientes y riesgos vinculados al uso del Internet de las Cosas Industriales

El principal inconveniente está vinculado a la seguridad industrial, entendiéndose por ello la inexistencia de soluciones integrales de seguridad cibernética en empresas de gran escala.

La gran cantidad de dispositivos IIoT y sistemas dependientes hacen de la organización un blanco fácil para ataques cibernéticos; si bien principalmente las Extranet son las más afectadas por su exposición global, también las Intranet y los dispositivos IIoT están sujetos a amenazas externas e internas. Un ataque a una máquina IIoT podría paralizar la misma, o lo que es mucho peor, configurar sus operaciones con parámetros incorrectos, ocasionando así pérdidas en insumos, fallas en el flujo descendente, gastos de energía y la obligación de subsanar los problemas ocasionados.

En segundo lugar, nuevamente la privacidad de los datos es un elemento a evaluar. Los cibercriminales muchas veces buscan información de los clientes tales como sus datos personales, productos adquiridos, fechas de adquisición y de entrega para llevar a cabo sus propias estafas. A través de la ingeniería social, buscan contactarse con el cliente en forma virtual o telefónica y, mediante engaños, obtener acceso a las cuentas bancarias o números de tarjeta de crédito.

No hay que dejar de lado la privacidad de los datos de las propias compañías. Conocer información acerca de la capacidad de producción, stock, empleados, direcciones de entrega, trayectos, fechas de recepción de insumos puede ser muy redituable tanto para su uso como para su venta.

En tercer lugar, teniendo en cuenta la variedad de dispositivos, máquinas y tecnologías, la falta de compatibilidad entre los mismos debido a la ausencia de estándares universales puede dificultar la interoperabilidad entre ellos. Inclusive, es frecuente que la actualización de las tecnologías de información, o bien la aparición de otra, implique tener que renovar todo un sistema debido a que los dispositivos IIoT pierden la habilidad de conectarse efectivamente y sincronizarse entre ellos.

En cuarto lugar, encontramos el entorno. En muchas oportunidades, se producen problemas en las máquinas con dispositivos IIoT como resultado de cortes de servicio de Internet o de energía, con la consecuente interrupción en el flujo de información. Inclusive, al renovar el servicio, también es posible que surjan inconvenientes en la sincronización entre los dispositivos IIoT. Si bien este problema se puede resolver en forma general mediante una doble acometida, no todas las empresas poseen dicha alternativa en todas sus dependencias.

Adicionalmente, pueden existir zonas donde no haya una señal de red suficiente para comunicarse correctamente, afectando así la solución tecnológica en la terminal del empleado de campo.

En quinto y último lugar, algunos autores mencionan el costo asociado en implementar y mantener los dispositivos IIoT, el hardware y el software operativo, la conectividad misma y la gestión de datos; además del costo de los profesionales IT y de capacitación a los distintos participantes del proceso. Sin embargo, con el aumento de productividad asociado, quizás sea mejor hablar de "inversión".

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

3.3. Internet de las Cosas en la Agricultura (*Internet of Things in Farming - IoTF*)

Si bien la agricultura no ha sido pionera en aplicar Internet de las Cosas, en los últimos años ha tenido un franco crecimiento en su aplicación, especialmente después del año 2017, cuando la Organización de las Naciones Unidas para la Alimentación y la Agricultura (*Food and Agriculture Organization - FAO*) emitió un informe donde hizo hincapié en que la mecanización agrícola era idónea para aumentar la productividad aún en explotaciones de pequeña escala. (FAO, 2017)

Actualmente, el Internet de las Cosas en la Agricultura (IoTF) o "*agricultura inteligente*" está presente en dispositivos IoTF clavados en el suelo, en drones sobrevolando los campos, en grandes invernaderos inteligentes, todo conectado a los dispositivos móviles de los agricultores, ingenieros y operarios a cargo. A continuación se desarrollan las aplicaciones del IoTF más comunes.

3.3.1. Gestión de recursos hídricos con dispositivos IoTF

En el sistema de riego tradicional, hasta el 50% del agua se desperdicia debido al exceso de riego causado por ineficiencias en los métodos; inclusive, muchas veces se producen faltantes de riego sin que hubiera faltantes de agua. A fin de optimizar los recursos hídricos, los dispositivos IoTF se clavan en el suelo cerca de las raíces de las plantas, con la finalidad de detectar la humedad y temperatura y así determinar el momento exacto en que la planta necesita agua.

Posteriormente, se comunican con otros dispositivos IoTF que están ubicados en los tanques de agua, a fin de consultar que existan los recursos necesarios. Estos datos se envían a una computadora central que crea modelos de riego. Finalmente, es el ingeniero quien toma la decisión de permitir que el sistema de riego se active solo siguiendo los parámetros predeterminados por la computadora central, o bien, de decidir modificar alguno de los mismos e iniciar manualmente el riego. Diferentes cultivos requieren diferentes estrategias de riego y el uso de datos en tiempo real posibilita al agricultor aumentar el rendimiento de un cultivo específico.

3.3.2. Control del cultivo mediante drones

El uso de drones para el control de cultivos permite analizar la salud de los mismos, tomando acciones preventivas y/o correctivas sobre la cosecha. Además, son una importante herramienta de ahorro debido a que trabajan solamente en el sector del campo que lo requiere, ahorrando insumos y tiempo. Los usos más comunes son la fertilización del suelo, el control de plagas y la siembra.

3.3.2.1. Fertilización del suelo

Los dispositivos IoTF ubicados en el suelo también sirven para recabar datos sobre la salud de las plantas. Una vez obtenidos los mismos, se envían drones (inclusive de forma autónoma) a los lugares donde están ubicados los sensores de suelo. Los drones están dotados de un receptáculo con el fertilizante, el cual es distribuido en todos los sentidos mediante el uso de un disco de rotación. La velocidad de rotación del mismo, conjuntamente con la velocidad del dron (ambas modificadas por el ingeniero), determinan la cantidad de fertilizante suministrado (Figura 7).

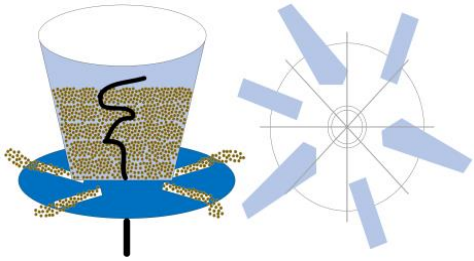

Figura 7: Receptáculo con fertilizante y disco de rotación.

La fertilización con drones incrementa su utilidad en grandes campos, pues los drones cubren las grandes áreas en forma rápida y con mayor precisión que los métodos tradicionales de fertilización.

3.3.2.2. Control de plagas

Los drones están equipados con cámaras ópticas y térmicas; al volar a baja altura y con una velocidad adecuada, captan con precisión imágenes de las plantas. Las mismas se transmiten a una computadora donde un ingeniero hace uso de un software específico de análisis, generalmente basado en redes convolucionales. El objetivo es detectar manchas, decoloraciones o cambios en la forma de las hojas, síntomas propios de la existencia de una plaga (insectos, maleza, hongos, etc.).

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás
AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

Además de poseer la capacidad de detectar con mayor precisión y velocidad una plaga que con los métodos tradicionales de inspección, los drones también aplican pesticidas a las plantas infectadas. Los modelos más avanzados fumigan áreas de 5.000 m^2 en 10 minutos, es decir, casi 50 veces más rápido que los métodos manuales de uso tradicional, protegiendo así los cultivos y aumentando la productividad del campo. La siguiente Figura 8 muestra un dron en acción.

Figura 8: Dron fumigando un campo.

3.3.2.3. Siembra

El proceso de "*siembra de precisión"* es una combinación de los dos procedimientos anteriores: en primer lugar, los dispositivos IoTF evalúan que las condiciones del entorno sean aptas para la siembra. Luego, informan a la computadora central, la cual es gestionada por un ingeniero que decide el tipo de semilla, cantidad y lugar exacto de siembra. Finalmente, mediante un receptáculo que soporta alrededor de 80 Kg. de semillas, los drones esparcen la misma en los lugares indicados. Todo el proceso es monitoreado a través de las mismas cámaras de los drones.

Gracias al Internet de las Cosas en la Agricultura, los nuevos métodos de siembra reducen el desperdicio de semillas, acortan los tiempos de operación, permiten plantar en lugares de acceso remoto con mayor facilidad y optimizan la producción de alimento y la calidad del cultivo.

3.3.3. Invernaderos inteligentes (*Smart Greenhouses*)

Existe una variedad de plantas que son difíciles de cultivar al aire libre, debido a las condiciones específicas de entorno que requieren: frutos rojos (arándanos, frambuesas, moras), frutos tropicales (mango, papaya, piña), flores (tulipanes). Otras plantas simplemente tienen la capacidad de crecer en interiores sin problemas: tomates, pimientos, lechuga; aprovechando dicha capacidad, los agricultores cultivan las mismas en invernaderos a fin de protegerlas de las plagas y eventos meteorológicos.

Los invernaderos inteligentes se denominan así porque hacen uso del Internet de las Cosas para mejorar la productividad de sus cultivos. Cuentan con dispositivos IoTF de suelo para capturar datos de humedad, lámparas inteligentes con sensores de luminosidad, sensores de temperatura e inclusive dispositivos destinados a detectar la calidad del aire. Como es costumbre, la información es enviada por los dispositivos IoTF a una computadora central cuyo software determina la mejor combinación para aumentar el rendimiento de los cultivos.

Además, los invernaderos también cuentan con dispositivos P2D similares a los mencionados anteriormente en el presente trabajo. Esta combinación le confiere al invernadero la capacidad de automatizar el riego según la necesidad de las plantas, controlar la cantidad de luz artificial para optimizar el crecimiento, modificar la temperatura del invernadero para corregir variaciones externas e inclusive reducir los niveles de dióxido de carbono. Sin embargo, si bien los invernaderos inteligentes son capaces de automatizar todo el proceso, es un ingeniero o personal capacitado quien debe tomar la decisión final, así sea la misma la de "ceder" el control a las máquinas IoTF.

3.4. Limitaciones vinculadas al uso del Internet de las Cosas en la Agricultura

La agricultura, al ser un eslabón inicial de la cadena productiva, generalmente posee una política de venta a empresas (B2B), en consecuencia, la privacidad de los datos personales está menos comprometida que en los ámbitos de industria o medicina. De cualquier manera, sigue existiendo un riesgo empresarial en cuanto a resguardar la información sensible tal como las áreas sembradas, áreas con problemas de crecimiento, áreas con plagas, la estimación de cultivos sanos y los insumos.

La principal limitación está dada por la falta de interoperabilidad o integración entre los distintos dispositivos IoTF. Por un lado, es un sector que tardíamente empezó a aplicar el Internet de las Cosas; por otro lado, ha tenido un muy rápido crecimiento de los últimos 6 años.

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

Estos dos factores han traído como consecuencia que las soluciones tecnológicas no sean compatibles entre sí, es decir, una cierta marca de dispositivos IoTF opera solamente con otros dispositivos de su misma marca, con su propio software específico para el procesamiento de los datos y su propia interfaz de usuario. Esta situación obliga al agricultor a quedar “atrapado” con un proveedor, invirtiendo mucho tiempo y dinero en caso de querer cambiar por otro. Con la llegada de los tractores y cosechadoras inteligentes, la situación tiende a agravarse aún más.

La conectividad en el entorno rural conlleva otra limitación. La baja densidad de población rural vuelve poco rentable para las empresas de telecomunicaciones extender su infraestructura hacia estas zonas, dependiendo del gobierno o de una asociación de agricultores para subsanar este problema.

4. CONCLUSIONES

El presente trabajo tuvo por objetivo comunicar la efectividad del Internet de las Cosas en la optimización de los procesos productivos. Para ello se analizaron tres áreas muy diferentes entre sí donde se implementa el IoT en forma masiva: la medicina, la industria y la agricultura.

Dentro del área de la medicina se detallaron los beneficios, principalmente para el usuario final del servicio: el paciente. Se observaron que las ventajas de la atención a distancia y el seguimiento continuo del estado del individuo, no sólo mejoran la calidad de vida del paciente, sino que incluso pueden llegar a salvarle la vida. Sin embargo, también se notaron los grandes riesgos que trae aparejada la vulnerabilidad de los dispositivos IoMT, en especial, cuando se trató la privacidad del historial clínico. Un profesional como el ingeniero industrial deberá ser capaz de gerenciar un sistema de información seguro y confiable, además de fijar políticas de acción para proteger la información crítica y confidencial de los pacientes, manteniendo la productividad y eficiencia del servicio.

En cuanto al área industrial, el uso del IIoT está ampliamente diversificado, como se hace observó en la gran cantidad de aplicaciones mencionadas e inherentes a la producción: logística, transporte, mantenimiento, automatización, control de calidad, gestión remota y seguridad, por nombrar las más importantes. Las posibilidades de optimización para un ingeniero industrial son muy variadas y sólo están limitadas por la inversión deseada. Su desafío en esta área nuevamente será la de desarrollar la seguridad para con los dispositivos IIoT, con el agravante de no contar siempre con una compatibilidad entre los mismos; y sin descuidar la privacidad de la información propia de la empresa.

Finalmente, comprobamos un crecimiento muy veloz en la asimilación del Internet de las Cosas en la Agricultura. A pesar de contar con una menor cantidad de años de desarrollo que las áreas anteriores, se observó que la agricultura ya hace uso de todo tipo de sensores IoTF, en combinación con novedosas herramientas tecnológicas como son los drones y los invernaderos autónomos, para optimizar los procesos más importantes de siembra y crecimiento de los cultivos. Un ingeniero industrial deberá ser capaz de sortear las limitaciones de compatibilidad, muy comunes en toda la maquinaria agrícola, para lograr y preservar un flujo constante y necesario de la información.

El elemento limitante del crecimiento del IoT siempre han sido las tecnologías de comunicación. A medida que las mismas sigan desarrollándose, mayor provecho sacará la Ingeniería Industrial.

5. REFERENCIAS

Alonso Cascallana, T. (2020, Marzo). *IOMT: la importancia del internet de las cosas médicas en contextos como el actual.* Orange. https://hablemosdeempresas.com/empresa/iomt/

Banco Mundial. (2018, Julio). *El Internet de las cosas: una promesa para el desarrollo.* https://www.bancomundial.org/es/news/feature/2018/07/03/el-internet-de-las-cosas-una-promesa-para-el-desarrollo

Berhanu, Y., Abie, H. y Hamdi, M. (2013). *Proceedings of the International Workshop on Adaptive Security: A testbed for adaptive security for IoT in eHealth.* Editorial ACM.

Chowdhury, A. y Haque, M. (2022). *Internet of Things (IoT) for Worker Safety in Industrial Environments: A Review*. IEEE. https://ieeexplore.ieee.org/document/9713496

Collins, B. (2023, agosto). *The Strategist: Rain, red flags and confusion – how do the teams plan for a race like Sunday's Dutch GP?.* Formula One Digital Media Limited. https://www.formula1.com/en/latest/article.the-strategist-rain-red-flags-and-confusion-how-do-the-teams-plan-for-a-race.3eqV2nbYoydVL0Z9CHwDrD.html

Universidad Tecnológica Nacional
XVI COINI 2023 1, 2 Y 3 de noviembre de 2023
Facultad Regional San Nicolás

AJEA –Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes del congreso DOI: https://doi.org/10.33414/ajea.1316.2023
Publicación en AJEA https://rtyc.utn.edu.ar/index.php/ajea/article/view/1450

Costa, J. (2023, marzo). *El dolor del Kun Agüero: expertos explican los tipos de arritmia y la función de un desfibrilador*. La Nación. https://www.lanacion.com.ar/sociedad/el-dolor-del-kun-aguero-expertos-explican-los-tipos-de-arritmia-y-la-funcion-de-un-desfibrilador-nid30032023/

Danel Ruas, O. (2020). *Internet de las cosas y su aplicación en el sector de la salud*. ORCID Org. https://orcid.org/0000-0001-5247-1101

Danino, C. (5 de octubre de 2022). *Innovación Tecnológica en la Justicia: IoT.* [Discurso principal]. Centro de Capacitación Judicial, Poder Judicial de la Prov. de Santa Fe, Argentina.

DelVecchio, A. (2017, febrero). *Internet de las cosas médicas (IoMT).* Computer Weekly. *https://www.computerweekly.com/es/definicion/Internet-de-las-cosas-medicas-IoMT-o-IoT-de-la-salud*

Faludi, R. (2021, marzo). *¿Cómo se comunican los dispositivos de IoT?.* DIGI. https://es.digi.com/blog/post/how-do-iot-devices-communicate

Food and Agriculture Organization of the United Nations. (2017). *El Estado Mundial De La Agricultura Y La Alimentacion: www.fao.org/3/a-I7658s.pdf*

IMDb. (2023). *The Sting*. https://www.imdb.com/title/tt0070735/

Jimenez Nieto, M. (2017, noviembre). *Internet de las Cosas Médicas*. Revista virtual U-GOB, 016, 42-46. https://736737d3e7.nxcli.net/tienda/revista-individual/u-gob-016/

Juan, J. (2022, noviembre). *Aplicaciones del IoT en medicina*. Invox Medical. https://invoxmedical.com/blog/iot-medicina/

Kaur, V. y Kaur, R. (2019, febrero). *Role of IoT in agricultura.* Journal of Pharmacognosy and Phytochemistry, 2019, SP1, 422-425. https://www.phytojournal.com/special-issue/2019.v8.i1S

La Nación. (2022, diciembre). *Kun Agüero contó que durante Argentina vs. Países Bajos le escribió al cardiólogo porque "se sentía raro"*. https://www.lanacion.com.ar/deportes/canchallena/kun-aguero-conto-que-durante-argentina-vs-paises-bajos-le-escribio-al-cardiologo-porque-se-sentia-nid10122022/

Lu, Y., Liu, M., Li, C., Liu, X., Cao, C., Li, X. y Kan, Z. (2022) *Precision Fertilization and Irrigation: Progress and Applications.* AgriEngineering. https://doi.org/10.3390/agriengineering4030041

McFarlane, D. (2018, octubre). *Industrial Internet of Things: Applying IoT in the Industrial Context*. Connected Everything. https://connectedeverything.ac.uk/industrial-internet-of-things/

Moreno, S. (2018, octubre). *Internet De Las Cosas Como Base De La Industria 4.0.* BDO Auditores. https://www.bdo.es/es-es/blogs-es/blog-coordenadas-bdo/octubre-2018/internet-de-las-cosas-como-base-de-la-industria-4-0

Nowak, S. (2023). *Smart cities: el IoT en las ciudades inteligentes*. Nuclio Digital School. https://nuclio.school/smart-cities-el-iot-en-las-ciudades-inteligentes/

Orcutt, M. (2016, diciembre). *Security Experts Warn Congress That the Internet of Things Could Kill People*. MIT Technology Review. https://www.technologyreview.com/2016/12/05/155664/security-experts-warn-congress-that-the-internet-of-things-could-kill-people/

Passett, A. (2023, junio). *Knights in Shining IoT Armor: Knightscope Secures New Contracts for its New Autonomous Security Robots*. IoT Evolution. https://www.iotevolutionworld.com/autonomous-vehicles/articles/456072-knights-shining-iot-armor-knightscope-secures-new-contracts.htm

RoboCleaners. (2023). *Trifo Ironpie m6+.* https://www.robocleaners.com/en/trifo-ironpie-m6.html

Rubin, B. (2015, diciembre). *Amazon Prime Now: A peek inside the Manhattan warehouse.* CNET. https://www.cnet.com/pictures/amazon-prime-now-a-peek-inside-the-manhattan-warehouse/

Senthil Kumar, A. e Iyer, E. (2019, abril). *An Industrial Iot In Engineering And Manufacturing Industries – Benefits And Challenges*. International Journal of Mechanical and Production Engineering Research and Development, Vol. 9, Issue 2, Apr 2019, 151-160. http://dx.doi.org/10.24247/ijmperdapr201914

Shelke, Y. y Sharma, A. (2016). *Internet Of Medical Things.* Aranca. https://www.aranca.com/assets/uploads/resources/special-reports/Internet-of-Medical-Things-IoMT_Aranca-Special-Report.pdf

Singh, K., y Kaushik, A. (2022). *Internet of Things (IoT) and Quality Control*. Editorial Springer.

TelcoAgro. (2023). *Fumigación con Drones.* https://telcoagro.com/fumigacion-con-drones/