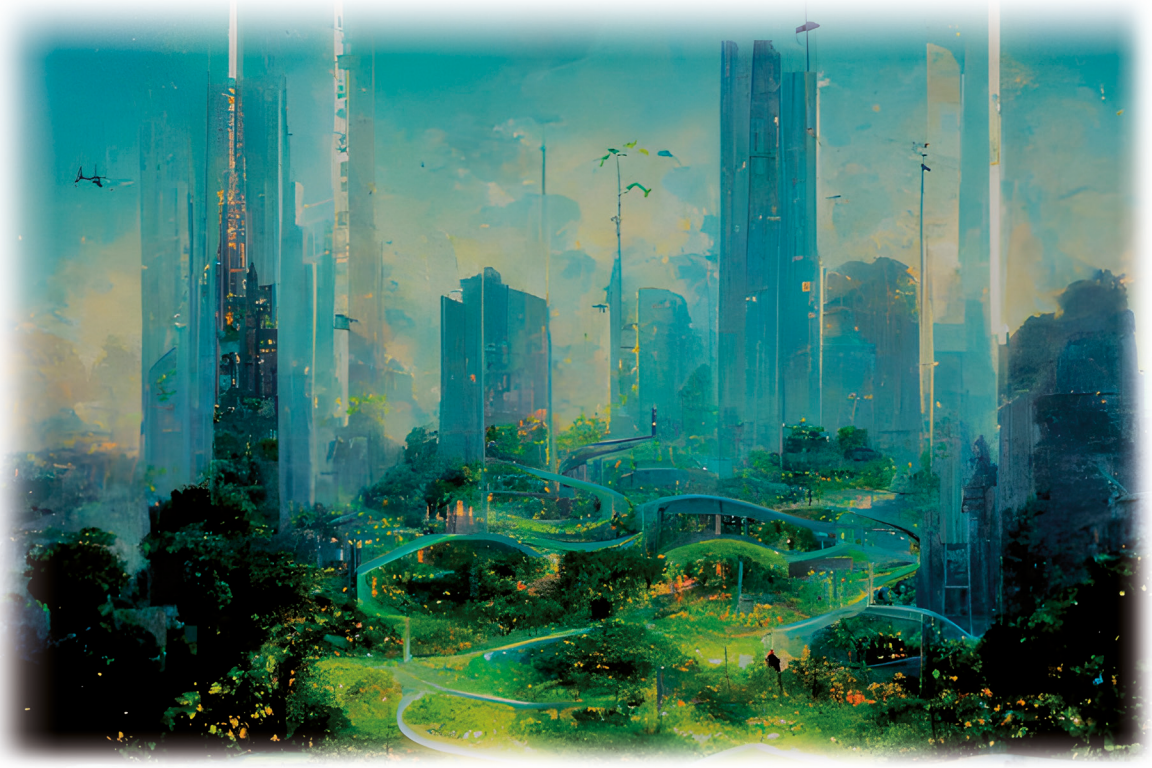
Ciberseguridad IoT y su aplicación en Ciudades Inteligentes



Enrique Villa Crespo
Ismael Morales Alonso

Ra-Ma®
Ediciones de la U

Ciberseguridad IoT y su aplicación en ciudades inteligentes

Enrique Villa Crespo
Ismael Morales Alonso

Ra-Ma®
edU
Conocimiento a su alcance

Villa Crespo, Enrique, *et. al.*

Ciberseguridad IoT y su aplicación en ciudades inteligentes / Enrique Villa Crespo e Ismael Morales Alonso --. Bogotá: Ediciones de la U, 2023
298 p. ; 24 cm
ISBN 978-958-792-583-8 e-ISBN 978-958-792-584-5
1. Informática 2. Tecnologías IoT 3. Digitalización de ciudades 4. Software de gestión IoT 5. Ciberseguridad para smart cities I. Tít.
621.39 ed.

Edición original publicada por © Editorial Ra-ma (España)
Edición autorizada a Ediciones de la U para Colombia

Área: Sistemas e informática
Primera edición: Bogotá, Colombia, septiembre de 2023
ISBN. 978-958-792-583-8

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Adriana Gutiérrez M.
Carátula: Ediciones de la U
Impresión: DGP Editores SAS
Calle 63 #70D-34, Pbx (+57) 601 7217756

Impreso y hecho en Colombia
Printed and made in Colombia

A mi familia:
mi mujer y mis hijas por las fuerzas
y la alegría que me dan,
y a mis padres y mi hermano
por su apoyo constante

Enrique Villa Crespo

A mis niñas

Ismael Morales Alonso

ÍNDICE

AUTORES

ENRIQUE VILLA CRESPO

Ingeniero de Telecomunicaciones por la Universidad de Sevilla. Profesor del Máster de Ciberseguridad de la Universidad de Sevilla. SCCISP por IoTSI Institute y Cisco CCNP/CCDP. CEO de IRIS Sentinel y CTO de Wellness Techgroup. Ha trabajado en el ciclo de vida completo del negocio de desarrollo e implantación de productos de IoT para *Smart Cities*, y en proyectos de Ciberseguridad IT/OT/IoT nacionales e internacionales en el sector público y privado.

ISMAEL MORALES ALONSO

Ingeniero Técnico en Informática de Sistemas, Ingeniero en Informática y Máster de Investigación en Ingeniería de Sistemas y de la Computación por la Universidad de Cádiz. Auditor Jefe y Especialista Implantador de ISO 27001 por AENOR, CISSP por ISC², CSX por ISACA y SCCISP por IoTSI Institute. CTO de IRIS Sentinel y Cybersecurity Manager de Wellness TechGroup. Ha trabajado para numerosos proyectos de ciberseguridad para el sector público y privado, centrándose en los últimos años a la ciberseguridad en el entorno de las *Smart Cities*.

PRÓLOGO

”En el mundo de la inmediatez, un profuso libro sobre tecnología podría sonar a contradicción. Sin embargo, es más necesario que nunca. Detenerse a estructurar las ideas, desarrollarlas, organizarlas e intentar explicarlas es un ejercicio tan necesario como escaso en la actualidad, donde se ha convenido que la atención fragmentada y superficial es más rentable que la reflexión profunda. ¿Pero rentable para quién? ¿Para los que monetizan y distribuyen esas distracciones o para sus consumidores? Un libro debe apostar por la concentración frente a la cultura de la distracción. Y como ejercicio de reflexión profundo, a largo plazo, es una inversión y un ahorro de tiempo para el lector, que podrá localizar en un solo punto toda la información condensada relativa a una disciplina y, además, disponer de esos datos en futuras consultas. Y por eso debemos celebrar estas obras que, tras un enorme esfuerzo por parte de los autores, nos ofrecen visiones desarrolladas y esquemáticas sobre una tecnología tan relevante (más de lo que pensamos) como el IoT en ciudades inteligentes.

“Ciberseguridad IoT y su aplicación en Ciudades Inteligentes” ofrece una visión global de un mundo tan heterogéneo como interesante. Ordena y estructura las ideas de forma que no solo podrá leerse en orden sino consultado en el futuro como una valiosa referencia. Desde la base de las tecnologías IoT, hasta su aplicación en Smart Cities siempre con la ciberseguridad como vertebrador del discurso. El estado del arte de las amenazas, descripción de los protocolos, incidentes más destacados Una lectura que aglutina y a su vez establece un punto de partida para ahondar en otros muchos aspectos gracias a sus profusas referencias a investigaciones recientes y clásicas. Se convierte este libro así en un trabajo tanto de síntesis de conocimiento como, además, de proyección perfectamente documentado para quien quiera ir más allá.

Por si fuera poco, el libro realiza una propuesta de *framework* de ciberseguridad para Ciudades Inteligentes que esperamos se estandarice y ponga orden para facilitar su implantación en un sistema tan heterogéneo. Y esto me parece especialmente importante porque considero que la implementación de ciudades inteligentes será uno de los elementos imprescindibles para la adaptación de los seres humanos al inminente escenario de superpoblación (como se indica en la obra, en 2030 habrá 43 megaciudades frente a las 31 actuales). O abrazamos nuevos modelos o resultará muy difícil una habitabilidad de las ciudades compatible con la sostenibilidad del planeta. Y para ello, el uso inteligente de la tecnología me parece la herramienta clave. Porque si el IoT en Smart Cities tiene sentido y resulta relevante, es para mejorar nuestros desplazamientos, consumo, actividades urbanas y calidad de vida. Al fin y al cabo, creo que lo práctico es recopilar y usar los datos necesarios que nos permitan convivir de forma óptima. Esto es, ser eficientes en todos los aspectos: social, turístico, económico, transporte, ecológico, turístico, etc. que se entrelazan en una ciudad. Como en toda tecnología, hay que aplicar transversalmente la ciberseguridad, por supuesto.

Agradezco a Enrique e Ismael la oportunidad de escribir este prólogo y les deseo la mejor de las suertes con el proyecto. También les agradezco apostar, en un mundo donde la suma de distracciones no equivale a la concentración, por la recopilación de información sobre una disciplina que requiere una reflexión profunda. Estas apuestas por allanar el camino del conocimiento de estas tecnologías son importantes para alcanzar un mundo inteligente de verdad y, en consecuencia, sostenible para todos.

Sergio de los Santos
Enero 2023

PREFACIO

Hoy en día, nos encontramos con infraestructuras y servicios cada vez más conectados, a través de los denominados Servicios Inteligentes o *Smart*. Estos servicios, se ofrecen a través de Territorios Inteligentes o *Smart Territories*, como pueden ser las Ciudades Inteligentes o *Smart Cities*) o Puertos Inteligentes o *Smart Ports*. Estos Territorios Inteligentes, de la mano del Internet de las cosas o IoT (*Internet of Things*), permiten la consecución y la evolución de las estrategias de digitalización, pero, también, los transforman en escenarios con objetivos de ataque altamente vulnerables, con exposición a nuevas ciberamenazas. Todo ello, unido a la necesidad de preservar la privacidad de los datos de los usuarios y ciudadanos, crean un ecosistema que necesita protegerse a través de una estrategia/marco de ciberseguridad específica *Smart*.

En el caso de las *Smart Cities*, nos encontramos con una evolución en las infraestructuras y digitalización de las ciudades, con todos los beneficios que esta evolución aporta, pasando por la digitalización de la administración electrónica hasta las infraestructuras y servicios *Smart*. Esta evolución, además de ofrecer beneficios a los ciudadanos, también presenta mayores riesgos cibernéticos que impactan directamente en el mundo físico.

La implementación actual de las iniciativas *Smart* se suele vertebrar a través de plataformas horizontales multipropósito, que generalmente carecen de un enfoque holístico de ciberseguridad. Existe, por tanto, una fuerte necesidad de contar con soluciones capaces de monitorizar toda la información, encontrar anomalías de ciberseguridad y ofrecer planes de acción y soluciones a corto, medio y largo plazo en los proyectos *Smart*.

Además de la monitorización, no existe actualmente un marco de buenas prácticas o *framework* de ciberseguridad estándar que cubra las áreas técnicas, social

y de cumplimiento. La existencia de un *framework* con tales características permitiría que los Servicios Smart disminuyeran su superficie de exposición, contaran con menor riesgo de materialización de las ciberamenazas y no quedaran riesgos latentes sin identificar.

De esta manera, las personas, instalaciones, sistemas, comunicaciones y tecnologías de la información que dan soporte a los servicios de los Territorios Inteligentes serían administrados y operados con las medidas adecuadas para proteger a las personas y a los sistemas de información. Esta protección, se realizaría frente a daños accidentales o amenazas deliberadas de rápida evolución con potencial para incidir en la confidencialidad, integridad y disponibilidad de la información tratada y de los servicios prestados.

Por todo lo anterior, el presente libro ofrece una visión de las tecnologías IoT y su aplicación en las *Smart Cities*, su evolución en lo que respecta a la digitalización junto a los servicios ofrecidos y su relación dentro de lo que conocemos como modelo IoT. También se ahonda en la ciberseguridad de los entornos *Smart*, indicando el estado del arte en lo que respecta a las amenazas y la fragmentación actual con respecto a las normativas y buenas prácticas existentes. Por último, en el libro se realiza una propuesta de *framework* de ciberseguridad adaptado para *Smart Cities* para terminar con un apartado de evolución futura y conclusiones.

Se persiguen los siguientes objetivos en este libro:

- Aunar todo el conocimiento de ciberseguridad en IoT y su aplicabilidad en las *Smart Cities* para que sea fácilmente consultable en caso de necesitarse por parte de todos los interesados.
- Conseguir *Smart Cities* seguras, que detecten y den respuesta las ciberamenazas a las que están expuestas, aumentando su nivel de ciberseguridad.
- Creación de un marco de buenas prácticas en ciberseguridad en *Smart Cities*.
- Mejorar la confianza en las *Smart Cities* por parte de la ciudadanía y los turistas.

Contenido

La obra consta de 5 capítulos. En el Capítulo 1 introducimos el concepto de las tecnologías IoT, empezando por un repaso de su historia y continuando con las aplicaciones de estas tecnologías en distintos sectores o ámbitos. Posteriormente,

presentamos la evolución de las ciudades o municipios en relación con su digitalización. Por último, aterrizamos en los servicios IoT que se ofrecen en las *Smart Cities* y sobre el concepto de *Smart City* como Infraestructura Crítica.

En el Capítulo 2 describimos el modelo IoT, profundizando en los componentes principales: dispositivos, comunicaciones y plataformas software, terminando el capítulo describiendo la convergencia de los entornos IoT con los entornos IT o Tecnologías de la Información y OT o Tecnologías de la Operación.

El Capítulo 3 está orientado a describir la ciberseguridad en los entornos *Smart*. Para ello, introducimos el capítulo describiendo las distintas amenazas que encontramos en estos entornos, describiendo previamente las amenazas presentes en los entornos IT u OT. Luego, presentamos una taxonomía de amenazas propuesta para estos entornos. Finalmente, detallamos la normativa y buenas prácticas existente en los entornos IoT y *Smart Cities*, haciendo un repaso de la fragmentación tan extensa que existe actualmente, pero enfocándonos a las prácticas de seguridad aplicables, concretamente, a los entornos IoT y *Smart Cities*.

En el Capítulo 4 proponemos un *framework* de ciberseguridad para *Smart Cities*, aplicable internacionalmente. Como hemos comentado anteriormente, no existe un consenso de cómo abordar la ciberseguridad en las *Smart Cities* concretamente, más allá de normativa o guías aplicables de manera parcial. Por ello, con toda la información especificada en los anteriores capítulos, proponemos el *framework* detallando la elección del mismo, la personalización en el ámbito de las *Smart Cities*, y una guía de implementación para cada uno de los controles propuestos.

En el Capítulo 5 y último aportamos las conclusiones y reflexionamos sobre dónde pensamos que evolucionarán las *Smart Cities* y, con ello, la ciberseguridad.

Orientación a los lectores

Hasta hace pocos años, los proyectos de las *Smart Cities* no pasaban de algunos demostradores de servicios con proyección a futuro. Esto quiere decir que la ciberseguridad prácticamente no se ha tenido en cuenta, ya que el impacto que podría haber causado en servicios de unos dispositivos que no son críticos eran mínimos, además de la dificultad de aplicar medidas de ciberseguridad en estos entornos, que no está estandarizada, entre otros motivos.

Hoy en día, se realizan proyectos que involucran miles de dispositivos, grandes exigencias en las comunicaciones en áreas de difícil cobertura y plataformas software que necesitan ingestar, procesar y analizar miles de eventos en cortos

periodos de tiempo. Estos proyectos sí que tratan activos críticos y el impacto de un ciberataque puede llegar a causar daños físicos.

Encontrándonos en este punto, y por nuestra experiencia y conocimiento en el sector, el principal propósito de elaborar este libro ha sido la realización de un compendio de la ciberseguridad para las *Smart Cities* y facilitar a todas las personas involucradas en estos proyectos que la ciberseguridad sea tenida en cuenta cumpliendo unos mínimos para que la madurez en ciberseguridad aumente, y que esto ocurra en el máximo de ciudades posibles.

Agradecimientos

En primer lugar, queremos dar las gracias a Sergio de los Santos, por haber aceptado escribir el prólogo del libro.

Queremos también agradecer a Juan Boubeta-Puig, Javier Tallón Guerri y David Romero Santos por haber revisado y poder aportar su experiencia en algunos capítulos del libro.

También agradecer al equipo de IRIS Sentinel por haber ayudado a hacer realidad la ciberseguridad en los entornos *Smart* y al equipo de Wellness TechGroup por su apoyo y soporte.

Por último, agradecer también a la editorial Ra-Ma, especialmente a Julio Santoro por su apuesta en la temática propuesta y por la facilidad en la comunicación durante el desarrollo del libro.

Enrique Villa Crespo
Ismael Morales Alonso
Sevilla, Enero 2023.

1

INTRODUCCIÓN A LAS TECNOLOGÍAS IOT

En la actualidad vivimos una etapa de progreso tecnológico sin parangón en la historia de la humanidad. Los grandes avances en los campos de la electrónica y las comunicaciones de las últimas décadas, con el desarrollo de Internet a la cabeza y seguido por las mejoras en tecnologías de sensores y sistemas energéticos, la creación de nuevos protocolos de comunicación y algoritmos de análisis de datos, y los aumentos de capacidades de procesamiento, almacenamiento y anchos de banda disponibles, entre otros, han permitido que una gran variedad de escenarios hayan sido digitalizados, automatizados e interconectados mediante Internet.

De esta forma, Internet se ha convertido en un medio no solo para la comunicación entre personas, si no entre dispositivos, permitiendo su acceso y control remoto. Estos dispositivos han pasado de ser únicamente ordenadores y sistemas de servidores en CPDs (Centros de Procesamiento de Datos) a teléfonos móviles, contadores de energía, pulseras que miden las constantes vitales o dispositivos industriales con sensores embebidos en cadenas de fabricación.

En 2022 se calcula que hay más de 14.000 millones de dispositivos conectados[1] y se prevé una evolución hasta los casi 30.000 millones para 2030[2]. En la Figura 1 puede observarse esta proyección.

---

1 https://iot-analytics.com/number-connected-iot-devices/

2 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

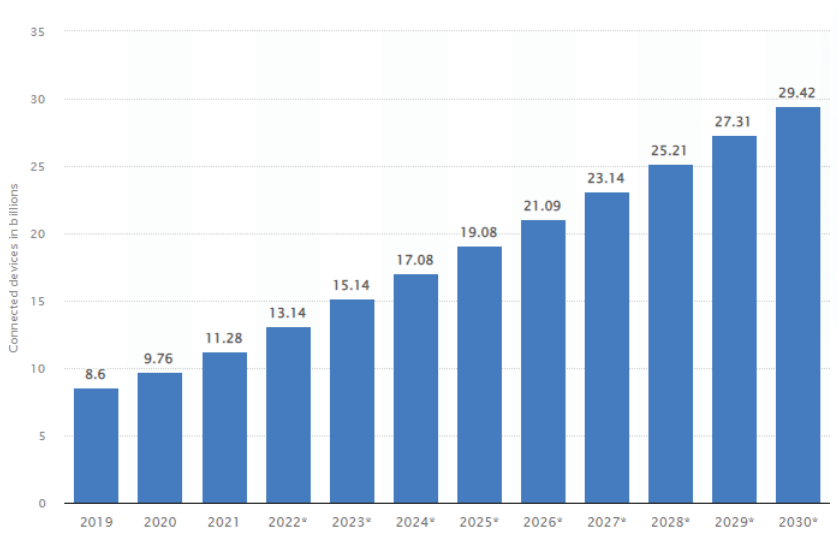


Figura 1: Proyección de dispositivos conectados

En términos económicos, algunos estudios[3] prevén un impacto de entre 3.9 a 11 billones de dólares al año a partir de 2025, entre un 5% y un 10% de la economía mundial global[4].

Todo esto ha significado que, a día de hoy, el concepto de Internet de las Cosas o IoT (*Internet of Things*) se haya convertido en una de las principales tendencias tecnológicas, propiciando el desarrollo dentro del sector de las TIC (Tecnologías de Información y Comunicación) o IT (*Information Technology*), así como de otros campos que han encontrado en las tecnologías IoT un escenario con muchas posibilidades como fuente de innovación y generación de nuevos modelos de negocio.

¿Pero cuál es la definición del concepto de IoT? La realidad es que nos encontramos con que el IoT es un paradigma con varias visiones diferentes, y sus correspondientes definiciones.

Las dos visiones primarias vienen directamente del término IoT. Una visión desde las "*Things*" o "Cosas", que está centrada en los dispositivos y objetos y sus

3 https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact

4 https://www.reuters.com/business/world-economy-top-100-trillion-2022-first-time-report-2021-12-26/

capacidades integradas en un marco de trabajo común, y la otra basada en "Internet", con un planteamiento más orientado a un concepto de IoT orientado a las redes de comunicación más importantes.

Una definición directa de estas dos visiones combinadas del término IoT sería "una red mundial de objetos interconectados con direcciones únicas, basada en protocolos de comunicación estándar"[5]. Pero las direcciones únicas y el contexto, la coherencia, la representación y almacenamiento de los datos intercambiados presentan un desafío que nos lleva a la tercera visión: una perspectiva del IoT desde el punto de vista semántico. Las tecnologías semánticas (utilizadas para conectar datos, darles significado y crear un contexto) juegan un papel clave en la explotación de la información que nos proporcionan los dispositivos, y en la escalabilidad de las soluciones, uno de los puntos disruptivos que nos promete el IoT.

Por tanto, teniendo en cuenta estas 3 visiones vamos a definir el IoT como "Una **red abierta** y **completa** de **objetos inteligentes** que tienen la capacidad de **auto-organizarse**, **compartir información, datos y recursos, reaccionar y actuar** ante situaciones y cambios en el entorno"[6].

La implementación a gran escala de la tecnología IoT promete transformar muchos aspectos del modo en que vivimos. Para los consumidores finales, productos como electrodomésticos inteligentes o aplicaciones de control de la energía doméstica, o que permiten la automatización los lugares de residencia, nos llevan a la realización de las casas inteligentes (*Smart Homes*), enfocadas a la sostenibilidad energética y medioambiental, así como a mejorar la calidad de vida de sus ocupantes. Otros productos que utilizan la tecnología IoT que se han integrado en el día a día de las personas, como los *wearables* orientados a la salud, los dispositivos de monitorización de constantes vitales remotos, o los dispositivos médicos conectados en tiempo real, están evolucionando el panorama de los servicios de salud.

Otros sistemas IoT como los vehículos conectados, los sistemas de optimización energética para edificios o alumbrado público, los sistemas de transporte inteligente y los sensores embebidos en infraestructuras como carreteras y puentes nos han llevado al concepto de Ciudades Inteligentes o *Smart Cities* con el objetivo de mejorar la calidad de vida de los residentes y optimizar los costes energéticos y de mantenimiento.

---

5 INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in cooperation with the Working Group RFID of the ETP EPOSS, "Internet of Things in 2020, Roadmap for the Future", Version 1.1 - 27 May 2008

6 Madakam, S. (2015). Internet of Things: Smart Things. International Journal of Future Computer and Communication, 4(4), 250–253. https://doi.org/10.7763/IJFCC.2015.V4.395

También, la aplicación de tecnologías IoT está transformando los sectores agrícolas, industriales y de generación y distribución de energía (agua, gas, electricidad, renovables, nucleares), usando sensores conectados que aumentan la visibilidad y la eficiencia en los procesos a lo largo toda la cadena de valor de la producción.

No obstante, hay que tener en cuenta que las tecnologías IoT aún se están consolidando en el mercado, y que las siglas IoT son un paraguas para multitud de tecnologías e interrelación entre las mismas. Este campo tecnológico se mueve muy deprisa, y a día de hoy presenta una serie de desafíos que aún no están resueltos. Los más importantes a nuestro juicio están relacionados con los siguientes.

La **Energía** y su gestión, ya que los dispositivos y aplicaciones IoT consumen energía de la red eléctrica o mediante baterías, y con la explosión de despliegue de dispositivos que se prevé para los próximos años, es necesario que se desarrollen sistemas de almacenamiento de mayor confiabilidad, que sean sostenibles y que permitan aumentar la autonomía de operación de los dispositivos actuales, así como sistemas *hardware* y protocolos de comunicación que tengan menores demandas energéticas.

La **Estandarización**, que aún está dando sus primeros pasos, con avances desiguales dependiendo del sector de aplicación. Para que la visión del IoT como tecnología de futuro presente en todos los lugares donde se necesita sea viable y verdaderamente interoperable es esencial una estandarización a diferentes niveles (técnico, normativo, alcance geográfico), para que la industria y el mercado puedan producir soluciones que aseguren el funcionamiento de ecosistemas IoT heterogéneos.

La **Ciberseguridad,** en todos sus ámbitos (personas, procesos y tecnología) y a través de toda la cadena de valor que compone el IoT (*software*, *hardware*, protocolos de comunicaciones, seguridad física), es una asignatura pendiente de la tecnología IoT. El carácter transversal del IoT y la novedad de sus aplicaciones ha influido en que no exista aún una visión homogénea de los mecanismos de seguridad y marcos de trabajo que, si están presentes en la TIC como conjunto, ya que son tecnologías con mayor recorrido en el tiempo. A nuestro modo de ver, urge que haya un modelo de ciberseguridad para IoT regulado, con participación de los principales actores (gobiernos, fabricantes, entidades certificadoras, consumidores) que forman el mercado.

1.1 BREVE HISTORIA DEL IOT

Como toda tecnología o grupo de tecnologías, el IoT tiene su propia historia que cuenta como hemos llegado a las capacidades de hoy en día. Vamos a aprovechar para repasar los hitos más importantes y/o curiosos que forman parte de la historia del desarrollo del IoT.

Cuando hablamos del "Internet de las Cosas" estamos refiriendo de una forma u otra a la generación y envío de información entre máquinas a través de un medio de comunicación masivo, Internet.

Las máquinas o dispositivos empezaron a soportar las comunicaciones de datos directas desde que el telégrafo (la primera línea de comunicación por cable) se desarrolló entre 1830 y 1850. Las primeras transmisiones de radio, descritas como "telegrafía sin hilos", ocurrieron en las décadas de 1880-1890. No fue hasta 1900 cuando se transmitió voz humana por primera vez.

Unas décadas más tarde, en pleno siglo XX, en la década de 1950, comenzó el desarrollo en masa de ordenadores. La propia Internet, otro de los componentes más significativos del concepto IoT, comenzó como un proyecto de la Agencia del Departamento de Defensa estadounidense DARPA (*Defense Advanced Research Projects Agency*) en 1962, y evolucionó hacia ARPANET (*Advanced Research Projects Agency Network*) en 1969.

En la década de 1980, los proveedores de servicios comerciales comenzaron a proporcionar acceso público a ARPANET, evolucionando así hasta nuestra Internet moderna.

Los satélites de posicionamiento global o GPS (*Global Positioning System*) se convirtieron en una realidad en 1993, cuando de nuevo el Departamento de Defensa estadounidense lanzó la primera red de 24 satélites estables, a los que se sumaron satélites privados comerciales con el paso de los años.

En esta década (1990) se acuñó el concepto original de *Internet of Things*, exactamente en 1999. Pero tenemos ejemplos anteriores de "proto-IoT" que son interesantes destacar.

Uno de los primeros ejemplos relacionados con el IoT es de 1989, con una máquina de Coca Cola en la universidad Carnegie Mellon. Los estudiantes de programación se conectaban a través de ARPANET a la máquina refrigeradora para comprobar si tenía bebidas disponibles y si estaban lo suficientemente frías antes de darse el paseo hasta la máquina.

El primer ejemplo de dispositivo controlado a través de Internet se produjo en 1991, cuando John Romkey y Simon Hackett crearon una tostadora de pan automática[7] (con un brazo mecánico para meter y sacar las tostadas incluido) que podía ser encendida y apagada en remoto. Este experimento sirvió entre otras cosas para que las primeras dudas acerca de la seguridad de dispositivos conectados se plantearan. ¿Para quién es visible el dispositivo a través de Internet? ¿Alguien podría tomar el control del dispositivo ilegítimamente y usarlo para provocar un fuego?

La primera "cámara web", creada para monitorizar cuanto café quedaba en una cafetera, se conectó a la red en Cambridge en 1993[8]. Poco después, en 1994 Steve Mann inventó la *WearCam*[9], una cámara web conectada a unas gafas para mandar imágenes en directo, con un rendimiento casi en tiempo real usando un sistema de 64 procesadores. De esta forma, estos primeros ejemplos de dispositivos IoT fueron pioneros también en aspectos que luego han aparecido en forma de las redes sociales, los teléfonos inteligentes e incluso el *streaming*.

Paul Saffo publicó la primera descripción acerca de sensores[10] y su futuro en 1997, donde vaticina que "…los sensores, baratos, ubicuos y de alto rendimiento, van a dar forma a la siguiente década".

Como decíamos al principio, en 1999 se nombró por primera vez el término de IoT. Fue utilizado por Kevin Ashton, Director Ejecutivo de los Laboratorios Auo-ID del MIT (*Massachusetts Institute of Technology*), que empezó a explorar la idea de cosas conectadas mientras trabajaba para Procter & Gamble. Implantó la tecnología RFID (*Radio Frecuency ID*) para fines de rastreo de activos logísticos en cosmética ese mismo año[11]. Kevin Ashton exponía que RFID era un prerrequisito necesario para el IoT, específicamente para habilitar la monitorización automatizada de inventarios remotos, y que, si todos los activos se encontrasen "etiquetados", podríamos desarrollar *software* para monitorizarlas, gestionarlas e inventariarlas. A día de hoy, además del RFID, nos encontramos con que tecnologías como los códigos QR (*Quick Response*), las marcas de agua digitales o los códigos de barras han permitido y habilitado que esta idea de las "etiquetas" electrónicas sea algo común en nuestro día a día.

---

7 https://romkey.com/

8 https://www.cl.cam.ac.uk/coffee/coffee.html

9 http://wearcam.org/myview.html

10 https://www.saffo.com/essays/sensors-the-next-wave-of-infotech-innovation/

11 http://www.rfidjournal.com/articles/view?4986

En el año 2000, LG anunció la primera nevera inteligente conectada, que podía determinar automáticamente si necesitaba reabastecerse.[12]

En 2002-2003, Walmart y el Departamento de Defensa norteamericano fueron las primeras grandes organizaciones que implementaron monitorización y rastreo de activos por RFID, con un modelo como el que había propuesto Kevin Ashton.

En 2007 se lanzó el primer IPhone, precursor de los teléfonos inteligentes. En 2008 un grupo de compañías lanzaron la *IPSO Alliance*[13] para promover el uso del protocolo IP en redes de "objetos inteligentes". Además, en Estados Unidos la FCC (*Federal Communications Commision*) aprobó el uso sin licencia[14] del espectro blanco o *white space spectrum*, bandas de frecuencia de UHF (*Ultra High Frequency*) y VHF (*Very High Frequency*). En 2008 el número de dispositivos conectados superó por primera vez a la de humanos en el planeta, aunque tendríamos que esperar a 2017 para que ese número fuera de dispositivos estrictamente IoT (excluyendo teléfonos móviles, ordenadores personales, etc.).

En 2009, Google empezó a hacer pruebas con coches sin conductor. En 2011, Nest[15], un termostato inteligente conectado, llegó al mercado, permitiendo gestionar el control remoto de calefacciones centralizadas. También se desarrolló en este mismo año, 2011, el primer timbre inteligente, *Ring*[16].

Por esta época, IPv6 empezó a convertirse en una realidad ya que en 2012 los proveedores de servicios más grandes acordaron incrementar el espacio de direcciones públicas de Internet global, habilitando IPv6 en sus productos y servicios[17]. Esto permitió asegurar que el crecimiento del IoT podía ser todo lo masivo que se necesitara, ya que solucionaba a priori el problema que existía con IPv4 y el número limitado de direcciones IP públicas.

En paralelo, en estos primeros años de la década de 2010, los entornos IoT como tales comenzaron a aparecer de forma más o menos regular. Así, como veremos más adelante, se empezaron a crear casos de uso específicos para Ciudades

12 https://www.ryt9.com/en/prg/23392

13 http://www.ipso-alliance.org/

14 https://docs.fcc.gov/public/attachments/FCC-08-260A1.pdf

15 https://support.google.com/googlenest/answer/7029281?hl=es

16 https://ring.com/doorbell-cameras

17 https://www.worldipv6launch.org/

Inteligentes o *Smart Cities*, un escenario que no ha parado de crecer y que ocupará buena parte de esta obra.

El IIoT (*Industrial Internet of Things*) o Internet de las Cosas Industrial, que agrupa las mejoras que introduce IoT aplicado a procesos industriales y de fabricación, empezó a tomar forma también durante estos años, con varias compañías que desarrollaron sus propios sistemas. General Electrics (GE) acuñó el término IIoT en 2012.

Para 2013, el IoT se había convertido en un sistema que usaba múltiples tecnologías, desde la comunicación a través de Internet a la comunicación inalámbrica local, y desde los sistemas micro-electromecánicos (MEMS) a los sistemas embebidos.

Nuevos entornos IoT empezaron a desplegarse a partir de esta época, primero como pilotos, y luego de forma más masiva. Se empezaron a implantar aplicaciones Verticales de *Smart City*, como Telegestión de alumbrado Inteligente, *Smart Parking* o *Smart Waste*, y aplicaciones IoT destinadas a la agricultura, la logística y el transporte, etc., mientras aparecían nuevos protocolos de comunicación IoT, de almacenamiento de datos y de securización de los mismos. La industria de la salud también comenzó a aplicar tecnologías IoT monitorizando remotamente pacientes a través de dispositivos IoT.

En paralelo, los teléfonos inteligentes se convirtieron también en una parte muy importante del llamado IoT del consumidor final. Este IoT está más centrado en dispositivos domésticos, gestionables remotamente a través de aplicaciones móviles, así como *wearables*, dispositivos personales (como auriculares, bicicletas estáticas, cepillos de dientes…) que monitorizan constantes vitales, localización y otros parámetros. Esta parte del IoT incide directamente con la privacidad de los datos personales, y este concepto de "sensor humano" voluntario o involuntario que han permitido crear los teléfonos inteligentes y la tecnología *wearable* es algo recurrente en relación con la privacidad y la seguridad de los individuos que desde entonces sigue estando sin resolver completamente, como comentaremos más a fondo más adelante.

Hoy en día, la siguiente revolución donde el IoT está muy presente es en la conducción autónoma de vehículos, que implica la conceptualización del vehículo como plataforma de dispositivos IoT que intercambia datos con otros dispositivos y vehículos sobre redes inalámbricas. Y para terminar, el futuro del IoT está conformándose con la aplicación de técnicas de IA (Inteligencia Artificial) a casos de uso donde el IoT está presente, que está revolucionando las capacidades de automatización, orquestación y operación autónoma.

1.2 APLICACIONES DE LAS TECNOLOGÍAS IOT

Como hemos comentado, las aplicaciones de las tecnologías IoT han dado paso al impulso y la creación de casos de uso sectorizados de IoT, escenarios IoT o entornos IoT. Estos términos se pueden utilizar indistintamente, y aparecerán en esta obra en muchas ocasiones.

Las tecnologías IoT han permitido que cualquier objeto sea susceptible de conectarse a Internet, y esto abre muchas puertas a nuevas aplicaciones que se han desarrollado en los últimos años y en las que se están desarrollando en la actualidad.

Esta versatilidad que ofrece IoT como habilitador tecnológico se define en varios entornos de aplicaciones IoT. Estas aplicaciones se definen por la capacidad de monitorizar y controlar dispositivos físicos, y de aprender de los datos que se generan de la operación. De esta forma son entornos que se caracterizan por el avance en las capacidades de gestión activa, en contraposición con la gestión reactiva, habilitando mecanismos de optimización y de alertas y mantenimientos predictivos.

En el resto del capítulo vamos a ver diferentes ejemplos de los entornos donde más ha avanzado el IoT, donde, entre otros, se enclava el entorno de *Smart Cities*.

1.2.1 Energía Inteligente

Uno de los sectores donde el uso del IoT ha destacado en los últimos tiempos es, sin duda, en el de la energía. Nos enfrentamos a un futuro energético incierto y las medidas de ahorro y optimización energéticas son uno de los focos más importantes tanto del sector público como del sector privado. La Agencia Internacional de la Energía (IAE) ha pronosticado un aumento del consumo de energía global de aproximadamente el 37% para 2040[18].

La aplicación de IoT en el dominio de la energía permite un uso de la energía más eficiente, que a su vez ayuda a decrementar los requerimientos de energía totales de los sistemas donde se aplique. Como en otros sectores, los dispositivos IoT y la analítica de datos asociada se han venido desplegando desde incluso antes de que el término se acuñara. Las necesidades de telecontrol remoto siempre han estado ahí, y IoT ha acelerado la implementación de casos de uso relacionados con la energía de manera masiva.

---

18 https://www.iea.org/reports/world-energy-outlook-2018

Estos casos de uso, donde el IoT y sus aplicaciones están presentes, incluyen la planificación de uso energético residencial, optimización y ahorro de energía para empresas productoras y distribuidoras, monitorización de los consumos energéticos en tiempo real de forma remota y estandarizada, ahorros energéticos en edificios inteligentes que veíamos en el entorno de Ciudad Inteligente, el telecontrol remoto del alumbrado público, la monitorización y control de puntos de recarga de vehículos eléctricos, la optimización energética en procesos industriales, la implantación de redes inteligentes de energía o *Smart grids,* etc.

Otro aspecto relacionado donde el IoT ha servido de catalizador es la planificación estratégica de la gestión energética, para entidades productoras, distribuidoras o comercializadoras. Estos planes ayudan a estos actores a reducir sus costes de operación y planificar mejor la demanda pico máxima esperada. La predicción de necesidades energéticas de los usuarios, y del mercado, es un aspecto crítico y esencial para hacer un uso más inteligente y sostenible de la energía y sus fuentes.

Por tanto, el IoT es una herramienta crucial para evolucionar en la gestión activa y eficiente de las fuentes energéticas. A continuación, veremos algunos casos de uso relacionados.

1.2.1.1 GENERACIÓN ENERGÉTICA Y CONTROL DE LA RED

Los avances que el IoT ha permitido en el control y monitorización de la generación energética y las redes de transporte y distribución tienen un impacto directo en la mejora de la eficiencia energética, reducción del impacto medioambiental y uso de tecnologías renovables de generación.

Estos avances están fuertemente ligados a la sensorización del equipamiento a niveles de generación, distribución y transporte, así como a la monitorización de las *Smart Grids* (protección de la red, balanceo de cargas, control de los voltajes, configuración y mantenimiento, información y alertas en tiempo real, etc.).

También a los contadores inteligentes, que monitorizan y optimizan la infraestructura de abonados a la red energética en tiempo real, para detectar fugas y caídas de potencia, automatizar la facturación y activar/desactivar servicios remotamente.

1.2.1.2 PREVISIÓN DE LA DEMANDA Y GESTIÓN DE PRECIOS

Como hemos comentado anteriormente, la previsión de la demanda es uno de los campos con más posibilidades dentro de las aplicaciones IoT en el mundo de

la energía. Los proveedores de servicios están implementando tecnologías (como IoT, analítica de datos y búsqueda de anomalías, algoritmos optimizados mediante ML (*Machine Learning*) o DL (*Deep Learning*), etc.) que les permiten optimizar la precisión con la que actualizan sus modelos de previsión, y, por tanto, de los precios de la energía en el sistema.

Estos modelos correlacionan variables de diferente índole, como el consumo de la energía con la temperatura exterior o la época del año, patrones nocturnos y diurnos, capacidades de las redes, costes de producción y otros, para determinar patrones y tendencias en una región determinada. Usando estos datos se puede desarrollar una previsión más acertada que ayuda a tomar decisiones, por parte de los productores y los consumidores, de forma anticipada para poder satisfacer la demanda optimizando el coste de producción y de consumo.

La monitorización del clima a través de dispositivos IoT distribuidos no solo ayuda a predecir la demanda, también a maximizar la estabilidad de la red energética.

1.2.1.3 ALMACENAMIENTO DE ENERGÍA

El almacenamiento eficiente de Energía es otro de los grandes retos a los que se enfrenta la industria energética en su conjunto. Uno de los focos de las aplicaciones IoT en el sector energético son las energías renovables, que tienen un carácter intrínsicamente intermitente en su producción.

El desafío que tiene este caso de uso es ayudar en el diseño y construcción de almacenamiento energético, con una densidad energética elevada.

1.2.2 IoT Industrial

La aplicación del IoT a la industria ha permitido la recolección y análisis de grandes cantidades de datos, que pueden ser usados para mejorar el rendimiento general de los sistemas industriales y reducir el coste de operación, a través de varios tipos de casos de uso que se han desarrollado en última década.

El IIoT es un entorno de IoT que requiere niveles altos de seguridad física, lógica y comunicaciones confiables, sin la posibilidad de introducir ninguna disrupción en las operaciones industriales en tiempo real, debido a las características críticas que poseen los entornos industriales y de fabricación. El foco de la IIoT es la gestión eficiente de los activos industriales y las operaciones, conjuntamente con el mantenimiento predictivo.

Se han acuñado varios términos que describen la implicación del IoT en la industria, como Industria 4.0, IoT Industrial, Fabricación Inteligente, etc. Uno de los pioneros en definirlo, en 2011, fue el gobierno alemán cuando introdujo una iniciativa que llamó *Industrie 4.0*[19] (que conocemos como Industria 4.0), que pretendía mejorar la eficiencia de la fabricación en la industria, apuntando a la recolección e intercambio de información de los activos durante todo el ciclo de vida de fabricación de un producto.

El concepto común detrás de estos términos es el uso de tecnologías y aplicaciones avanzadas (e. g. IoT, Computación en la nube/*Edge*, ML/DL) optimizadas específicamente para soportar casos de uso de procesos industriales.

La optimización de procesos y el mantenimiento predictivo han sido los primeros beneficios que ha traído el IIoT en el sector industrial y de fabricación. Estas nuevas capacidades han dado lugar a la investigación, diseño y puesta en marcha de múltiples casos de usos verticales de aplicación del IoT en la industria. A continuación, vamos a comentar algunos de estos casos que ya se han implementado hoy en día, y que beneficios aportan.

1.2.2.1 MONITORIZACIÓN Y RASTREO DE ACTIVOS EN LA CADENA DE SUMINISTRO

Se centra en la supervisión de los componentes de la cadena de suministro (materiales en bruto, contenedores, productos elaborados…) para optimización de la logística, mantenimiento de inventarios y detección de anomalías. También se utiliza para aumentar la seguridad de los trabajadores y reducir pagos de seguros. En general está focalizado a reducir costes y riesgos.

1.2.2.2 MANTENIMIENTO PREDICTIVO

Este campo fue uno de los pioneros en la aplicación del IoT en los procesos industriales. Permite implementar capacidades de monitorización avanzadas del estado del equipamiento industrial/de fabricación y de campo (e. g. componentes individuales del equipamiento) para la recolección y análisis de datos de operación. Esta analítica de datos avanzada, mediante algoritmos específicos y/o el uso de ML/DL, habilita el establecimiento de mecanismos de mantenimiento predictivo del equipamiento.

---

19 https://ati.ec.europa.eu/reports/policy-briefs/germany-industry-40