

Ciberseguridad IoT y su aplicación en Ciudades Inteligentes

Ciberseguridad IoT y su aplicación en Ciudades Inteligentes

Enrique Villa Crespo

Ismael Morales Alonso





Ciberseguridad IoT y su aplicación en Ciudades Inteligentes

Materia: UTN Seguridad de redes

© Enrique Villa Crespo, Ismael Morales Alonso

© De la edición: Ra-Ma 2023

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. RA-MA ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

RA-MA es marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, RA-MA Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente, ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de RA-MA; su contenido está protegido por la ley vigente, que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeran o plagiaran, en todo o en parte, una obra literaria, artística o científica.

Editado por:

RA-MA Editorial

Calle Jarama, 3A, Polígono Industrial Igarsa

28860 PARACUELLOS DE JARAMA, Madrid

Teléfono: 91 658 42 80

Fax: 91 662 81 39

Correo electrónico: editorial@ra-ma.com

Internet: www.ra-ma.es y www.ra-ma.com

ISBN impreso: 978-84-19444-73-8

ISBN ePub: 978-84-19444-74-5

Depósito legal: M-5103-2023

Maquetación: Antonio García Tomé

Diseño de portada: Antonio García Tomé

Filmación e impresión: Safekat

Impreso en España en marzo de 2023

*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	11
PRÓLOGO	13
PREFACIO	15
CAPÍTULO 1. INTRODUCCIÓN A LAS TECNOLOGÍAS IOT	19
1.1 BREVE HISTORIA DEL IOT	23
1.2 APLICACIONES DE LAS TECNOLOGÍAS IOT	27
1.2.1 Energía Inteligente	27
1.2.2 IoT Industrial	29
1.2.3 Transporte Inteligente	32
1.2.4 Agricultura Inteligente	33
1.2.5 Salud Inteligente	35
1.2.6 IoT Doméstico	36
1.2.7 Ciudades Inteligentes	38
1.3 EVOLUCIÓN DE LA DIGITALIZACIÓN DE LAS CIUDADES	39
1.3.1 Primeros pasos y evolución histórica	39
1.3.2 El salto tecnológico	44
1.4 LA ERA DE LAS SMART CITIES	48
1.4.1 Definición y Características de una Smart City	49
1.4.2 El impulso de la Administración a las Smart Cities	54
1.4.3 El futuro de las Smart Cities	56
1.5 SERVICIOS IOT EN SMART CITIES	60
1.5.1 Movilidad Inteligente	60
1.5.2 Alumbrado Inteligente	63
1.5.3 Recogida de Residuos Inteligente	64
1.5.4 Edificios Inteligentes	65
1.5.5 Turismo Inteligente	67
1.5.6 Seguridad Pública Inteligente	68

1.6	SMART CITY, ¿INFRAESTRUCTURA CRÍTICA DIGITALIZADA?	71
1.6.1	Infraestructuras Críticas	71
1.6.2	Normativa en Infraestructuras Críticas	74
1.6.3	Ciberamenazas en las Infraestructuras Críticas	74
1.6.4	Relación de Smart City con Infraestructuras Críticas	80
1.6.5	Conclusiones	83
CAPÍTULO 2. EL MODELO IOT		85
2.1	DESCRIPCIÓN DEL MODELO IOT	85
2.1.1	Modelo de 3 capas	86
2.1.2	Modelo de 5 capas	88
2.1.3	Conclusiones del modelo por capas	89
2.1.4	Conceptos y Definiciones	91
2.2	COMPONENTES DEL MODELO IOT	93
2.2.1	Dispositivos	93
2.2.2	Comunicaciones	95
2.2.3	Control y toma de decisiones inteligente	96
2.3	DISPOSITIVOS IOT	96
2.3.1	Arquitecturas hardware	98
2.3.2	Dispositivos IoT de consumo	101
2.3.3	Dispositivos IoT en industria	103
2.3.4	Dispositivos IoT en Salud	105
2.3.5	Dispositivos IoT en Smart Cities	105
2.4	COMUNICACIONES IOT	106
2.4.1	LoRaWAN	107
2.4.2	Sigfox	116
2.4.3	Tecnologías celulares LPWAN	120
2.4.4	Otras tecnologías de comunicaciones IoT	130
2.5	ENTIDADES SOFTWARE DE GESTIÓN IOT	136
2.5.1	Plataformas Software IoT	137
2.5.2	Implementación y despliegue	154
2.5.3	Protocolos de datos IoT	154
2.6	CONVERGENCIA IT/OT/IOT	166
2.6.1	IT	166
2.6.2	OT	167
2.6.3	IoT	168
2.6.4	Convergencia	169
CAPÍTULO 3. CIBERSEGURIDAD EN ENTORNOS SMART		173
3.1	MISMAS AMENAZAS, NUEVOS ESCENARIOS	174
3.1.1	Tendencias	178
3.1.2	Catálogo de amenazas	184
3.1.3	Catálogo de amenazas en entornos Smart	186
3.1.4	Estado de la privacidad y protección de datos	195

3.2	NORMATIVA Y BUENAS PRÁCTICAS.....	197
3.2.1	Relaciones entre distintas normativas y personalización de medidas de seguridad	198
3.2.2	Iniciativas gubernamentales	200
3.2.3	Estándares.....	206
3.2.4	Guías de buenas prácticas	216
3.2.5	Smart City	230
CAPÍTULO 4. FRAMEWORK DE CIBERSEGURIDAD PARA SMART CITIES .		239
4.1	ELECCIÓN DE <i>FRAMEWORK</i>	240
4.2	PERFIL ESPECÍFICO PARA SMART CITIES	242
4.3	ALINEAMIENTO DE CONTROLES PARA CUMPLIR LOS OBJETIVOS DE LAS SMART CITIES	244
4.4	CATEGORIZACIÓN.....	248
4.5	GUÍA DE IMPLEMENTACIÓN.....	252
4.5.1	Conceptos fundamentales de seguridad	252
4.5.2	Controles transversales.....	254
4.5.3	Seguridad ciudadana	277
4.5.4	Protección de la privacidad	283
4.5.5	Ciudad limpia y sostenible	287
4.5.6	Gestión óptima de tráfico	287
4.5.7	Monitorización, detección y respuestas ante anomalías.....	288
CAPÍTULO 5. EVOLUCIÓN FUTURA Y CONCLUSIONES.....		293
5.1	CIBERSEGURIDAD Y ESTANDARIZACIÓN	294
5.2	EVOLUCIÓN DEL IOT Y EL ENTORNO DE LAS SMART CITIES.....	295



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.

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 conectados¹ y se prevé una evolución hasta los casi 30.000 millones para 2030². 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/>

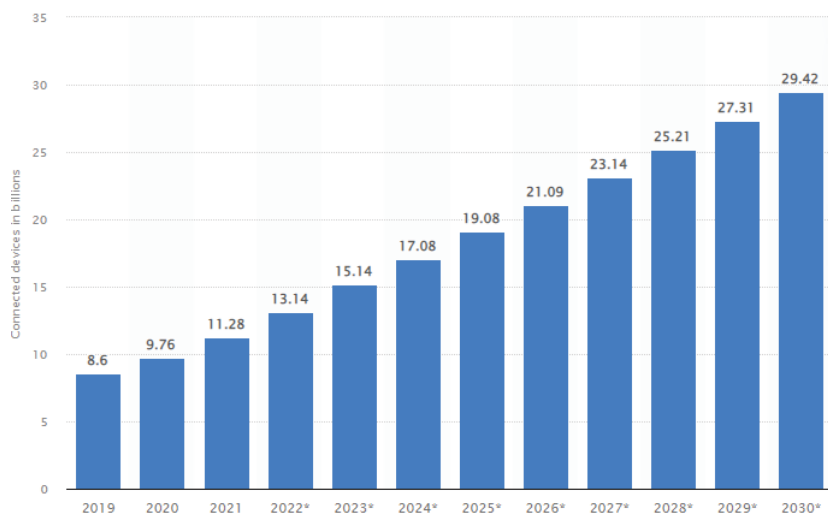


Figura 1: Proyección de dispositivos conectados

En términos económicos, algunos estudios³ 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 global⁴.

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 automática⁷ (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 1993⁸. 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 sensores¹⁰ 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 Auto-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 Frequency ID*) para fines de rastreo de activos logísticos en cosmética ese mismo año¹¹. Kevin Ashton exponía que RFID era un prerequisite 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 Commission*) aprobó el uso sin licencia¹⁴ 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, Nest¹⁵, 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 servicios¹⁷. 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 Electric (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 2040¹⁸.

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 intrínsecamente 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>

Este avance ayuda a incrementar la utilización de la maquinaria (que es un factor clave en el aumento del rendimiento total) y a la reducción de costes en infraestructura.

1.2.2.3 CONTROL DE LA PRODUCCIÓN EN REMOTO

Su foco está en la supervisión de equipamiento de producción de forma centralizada. Esto incluye la monitorización de parámetros relevantes para la producción local o de factorías remotas. Sus beneficios están relacionados con la seguridad física en el proceso de producción, control en tiempo real de maquinaria en remoto, monitorización de trabajadores y su localización (e. g. sitios de acceso remoto como explotaciones mineras), ayudando a la reducción de costes y la seguridad y localización del personal y sus activos de producción.

1.2.2.4 CONTROL DE CALIDAD

Se centra en la monitorización de equipamiento en tiempo real para mejorar dos puntos clave en la industria como son el cumplimiento técnico/legal y la seguridad de las operaciones desde el punto de vista normativo. Es una de las palancas de reducción y gestión de riesgos de negocio asociados a la producción industrial.

1.2.2.5 OPERACIONES EN CAMPO

Esta aplicación del IoT va de la mano con otras tecnologías como VR/AR (*Virtual Reality/Augmented Reality*) para crear un entorno de trabajo más seguro donde las interacciones con el mundo físico (equipamiento o infraestructura) se monitoricen y se guíen de forma automática. Ayuda a mejorar la experiencia de los trabajadores, reduce los riesgos de seguridad y el coste asociado a las operaciones en campo.

1.2.2.6 GEMELOS DIGITALES

El campo de los Gemelos Digitales o *Digital Twins* ha tenido un crecimiento notable dentro de las aplicaciones IoT industriales. Básicamente, los Gemelos Digitales permiten trabajar con réplicas digitales de maquinaria y equipamiento industrial y de fabricación, para predecir problemas y cuellos de botella potenciales antes de entrar en fase de producción. Sus aplicaciones están orientadas a la monitorización y testeo de nuevo equipamiento en un ambiente virtual antes de su paso al mercado real, o la simulación del ciclo completo de la vida de una máquina o dispositivo, y ayudan a reducir costes de mantenimiento y/o reemplazo, así como los costes de diseños iniciales, e incrementar la eficiencia y el rendimiento.

1.2.3 Transporte Inteligente

La industria del transporte y la logística son uno de los catalizadores de aplicación del IoT. Entre otras cosas, ha influido en la definición y desarrollo de conceptos como V2V y V2I (*Vehicle-to-Vehicle* y *Vehicle-to-Infrastructure*) que tiene la capacidad para transformar la industria de forma disruptiva, en el entorno de Vehículos Inteligentes y conectados.

También ha permitido grandes avances en otros servicios como el rastreo de flotas y de activos en almacenes. Sin olvidarnos de los avances en la vertiente de transporte público, a través de la capacidad de adquirir datos de uso y de ocupación en tiempo real, las densidades de peatones dependiendo de la zona geográfica, el conteo y clasificación de vehículos o la identificación automática de daños en las calzadas, por nombrar algunos casos de los más implementados.

El IoT en este sector tiene un futuro muy interesante por delante. Veamos con algo más de detalle algunos casos de uso.

1.2.3.1 GESTIÓN DE FLOTAS, CADENA DE SUMINISTRO Y MONITORIZACIÓN DE ACTIVOS

La capacidad de obtener datos de la flota de vehículos en tiempo real fue una de las primeras palancas de aplicación del IoT en el sector logístico. La monitorización de variables intrínsecas a la flota, como la posición, valores de rendimiento y utilización de diferentes partes del vehículo como el kilometraje parcial/total, la carga total o la presión de los neumáticos se ha engranado con la monitorización de parámetros extrínsecos, como la carga del vehículo. Por ejemplo, en el control de la cadena de frío de alimentos perecederos, o en la trazabilidad completa de las mercancías. También es reseñable la influencia del IoT en las aplicaciones de control de conducción y comportamiento del conducto.

Los beneficios que aporta el IoT en este entorno están enfocados a la disminución de costes en mantenimiento o combustible, mejora del cumplimiento de la regulación legal y optimización de puntos únicos de fallo en el vehículo o el tipo de carga.

1.2.3.2 MICROMOVILIDAD

El campo de la micromovilidad está relacionado con la gestión y la operación de las flotas de vehículos unipersonales (bicicletas, motocicletas, patinetes, etc.) como servicio. El IoT aplicado a este sector permite la monitorización remota (niveles de batería, localización precisa, alertas de intentos de modificación del vehículo) y la

optimización de la flota y su mantenimiento. A medida que las diferentes soluciones de micromovilidad van iterando tecnológicamente, el IoT tiene mayor presencia en su conjunto para la optimización de los costes y la mejora de la experiencia del usuario.

1.2.3.3 GESTIÓN DE INVENTARIOS INTELIGENTE

Este concepto aglutina todas las aplicaciones de optimización de inventarios físicos en centros de almacenaje. La obtención de información en tiempo real de la localización de un elemento del inventario y la maximización de espacios físicos son dos de las aplicaciones más inmediatas que inciden en la reducción de los costes y otros aspectos como el mantenimiento predictivo y el análisis de tendencias. Un componente muy importante del beneficio de este caso de uso es la minimización de errores de inventario.

1.2.3.4 APLICACIONES V2X

El mundo del transporte ha evolucionado en la última década gracias a la implementación de los sistemas inteligentes o ITS (*Intelligent Transportation Systems*). Uno de los grandes focos de atención está puesto en las comunicaciones entre vehículos (V2V), de vehículos con la infraestructura (V2I) y por abstracción del concepto, de vehículos con todo (V2X). Esta tendencia tiene como objetivo principal aumentar la seguridad en las carreteras, intentando anticipar las circunstancias donde puede haber un posible peligro.

Los sistemas resultantes necesitan cumplir con unos requisitos en cuanto a capacidades de comunicaciones, con herramientas como 802.11p (*Wireless Access in Vehicular Environments*) o comunicaciones celulares, latencias máximas y procesamiento híbrido de datos entre el vehículo y la nube. Es un campo específico dentro del IoT que va a suponer una revolución en el futuro, pero que necesita de un camino de inversiones en infraestructuras y estandarizaciones tecnológicas que ya se está construyendo²⁰.

1.2.4 Agricultura Inteligente

La Agricultura Inteligente es un término amplio en el que entran todas las iniciativas de la producción agrícola que utilizan IoT, *Big Data* o analítica avanzada. Los avances en términos de IoT se enmarcan en la integración de sensores, actuadores

20 <https://www.autosinnovate.org/V2X>

y analítica de datos en los procesos tradicionales de la agricultura. El despliegue de redes de dispositivos IoT en este escenario ayuda a la optimización de recursos tales como el agua, productos químicos como plaguicidas o fertilizantes, o la duración de las cosechas y los periodos de floración, aumentando el rendimiento de las instalaciones agropecuarias y disminuyendo su coste.

Las principales aplicaciones IoT específicas de este entorno son la agricultura y la ganadería de precisión. La capacidad de monitorizar ganado, cultivos individuales, vehículos, hacer observaciones de campo de forma remota, o la digitalización de los inventarios y la logística aumenta la “precisión” y el control sobre las producciones agrícolas. No es un concepto nuevo, ya que se desarrolló en la década de 1980²¹, pero sí ha evolucionado, especialmente con la incorporación de la digitalización y las aplicaciones IoT.

Alrededor de la agricultura de precisión podemos encontrar aplicaciones IoT dentro de los entornos que vamos a ver a continuación.

1.2.4.1 SISTEMAS DE SENSORES Y ACTUADORES EN CAMPO

Monitorización de parámetros básicos y avanzados de las explotaciones agropecuarias, como cultivos, humedad y nutrientes del terreno, rastreo de ganado, capacidad de almacenamiento físico, así como actuación (irrigación inteligente, mantenimiento de la alimentación del ganado automatizado)

1.2.4.2 INFRAESTRUCTURAS CONECTADAS

Agricultura de precisión monitorizada en entornos específicos como invernaderos o granjas hidropónicas (donde se sustituye la tierra de cultivo por una solución de agua con nutrientes) inteligentes. El nivel sensorización que permite el IoT da una visibilidad mejor a la hora de entender el ciclo de vida de un cultivo en estos entornos.

1.2.4.3 GESTIÓN, VISUALIZACIÓN Y ANALÍTICA DE DATOS AGRÍCOLA

El campo de la interpretación de los datos obtenidos a través de aplicaciones IoT está creciendo en los últimos años. La correlación de datos tradicionales con los datos obtenidos en campo, con otro tipo de fuentes como imágenes satelitales, unido a la creación de algoritmos específicos y capacidades de ML/DL, es una tendencia

21 «Site-specific nutrient management: objectives, current status and future research needs». https://www.researchgate.net/publication/282610086_Site-specific_nutrient_management_objectives_current_status_and_future_research_needs

iniciada a principios del siglo XXI que evoluciona a pasos agigantados a medida que el sector desarrolla los beneficios que aporta la tecnología, y en especial el IoT, en su negocio.

El fin último de la agricultura de precisión es analizar datos proporcionados por las diferentes fuentes disponibles, de forma digitalizada, y responder de la forma más apropiada a las conclusiones que se extraen de esos datos.

1.2.5 Salud Inteligente

La tendencia que ha marcado la tecnología y la digitalización en el tratamiento de la salud se ha complementado en los últimos años con la aplicación del IoT. Esto ha permitido aplicar capacidades y ángulos diferentes de tratamiento de los pacientes que antes no existían o tenían un coste demasiado elevado para poder llevarlas a la práctica de manera masiva.

Con el envejecimiento general de las poblaciones del mundo occidental, los beneficios que trae la aplicación de IoT para la salud hacen de este campo uno de los más prometedores en términos de impacto y mejora en el bienestar personal. La capacidad de poder hacer seguimientos en tiempo real de la salud de las personas y las capacidades de prevención de enfermedades con mayor antelación están orientando hacia una medicina con capacidades cada vez más proactivas.

Podemos reseñar algunos de los casos de uso actuales del IoT en el tratamiento de la salud, con impulsores comunes alrededor de la mejora de la experiencia del paciente, la mejora de capacidades médicas, y la optimización de costes:

1.2.5.1 MONITORIZACIÓN DE PACIENTES Y ENFERMEDADES CRÓNICAS

La aparición de *wearables* y el aumento de dispositivos médicos conectados ha permitido la monitorización de la salud y de la actividad de enfermedades crónicas de forma menos invasiva. Esta rama de la medicina se conoce como Sistemas de Salud en tiempo real o RTHS (*Real-Time Health Systems*), o IoMT (*Internet of Medical Things*)²², donde las tecnologías habilitantes son el *cloud computing* o el IoT. Es reseñable que estos entornos IoT han tenido un avance cualitativo y cuantitativo durante y después de la crisis provocada por el COVID-19.

22 Bigini, G., Freschi, V., & Lattanzi, E. (2020). A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision. *Future Internet* 2020, Vol. 12, Page 208, 12(12), 208. <https://doi.org/10.3390/FI12120208>

1.2.5.2 AUTONOMÍA VITAL Y GESTIÓN DE TRATAMIENTOS EN REMOTO

Otro de los casos de uso habituales es la monitorización de personas ancianas/impedidas, conjugando la autonomía personal sin la necesidad de estar ingresado en un centro hospitalario con la monitorización remota de los parámetros más importantes en cada caso. Estas aplicaciones de la tecnología ya existían antes de la implantación del IoT, pero esto ha permitido acelerar y homogeneizar aplicaciones de gestión remota de la salud/constantes vitales, así como añadir capacidades como la unificación de sensórica en el paciente, sensores de movimiento o GPS, o gestión automatizada de dispensadores personales de medicinas y cantidad de medicación relacionadas con un tratamiento.

1.2.5.3 MONITORIZACIÓN Y OPERACIÓN REMOTA DE INFRAESTRUCTURA MÉDICAS

La monitorización y operación remota de equipamiento médico ha influido de forma determinante en dos capacidades específicas. Por un lado, la monitorización de equipamiento médico de forma desatendida para que, al igual que en la industria 4.0, poder implementar un mantenimiento predictivo que ayude a bajar los costes de operación y a incrementar la utilización del equipamiento.

Por otro lado, las intervenciones remotas, donde un equipo médico puede ejecutar una intervención en un paciente sin estar presente en el mismo quirófano, son una realidad. Este campo tiene mucho recorrido por delante, y permite mejorar la calidad de vida de los pacientes y de los equipos médicos.

1.2.6 IoT Doméstico

En la última década, las aplicaciones de IoT domésticas han evolucionado el concepto de Casas Inteligentes o *Smart Homes* y se han integrado cada vez más en nuestro día a día.

El concepto de Casa Inteligente con capacidades de control remoto comenzó en 1975 con el desarrollo del protocolo de comunicaciones X10, que usaba el cableado eléctrico de una vivienda para permitir la comunicación entre los dispositivos compatibles y los módulos de control instalados. Fue avanzado para su tiempo, siendo utilizado hasta muchos años más tarde, pero era costoso, necesitaba instalación profesional, no tenía ninguna característica de seguridad de los datos y además no era muy rápido. Sin embargo, cimentó el campo tecnológico de automatización en las casas particulares, también llamado Domótica.

A principios de los 2000, con protocolos inalámbricos como Z-Wave y Zigbee se empezó a dar forma al concepto de Casa Inteligente inalámbrica. En 2011

apareció Nest, un termostato inteligente controlado remotamente a través de internet, que supuso una revolución en las posibilidades que podían tener los dispositivos domésticos.

A día de hoy, hay protocolos como Matter²³ de la CSA (*Connectivity Standards Alliance*) que están respaldados por una gran parte de la industria IoT doméstica y que intentan ayudar a cubrir la fragmentación de *hardware*, *software* y aplicaciones de control de las Casas Inteligentes. También se avanza en el procesamiento del lenguaje natural o NLP (*Natural Language Processing*) para permitir asistentes domésticos más avanzados. Por otro lado, este entorno del IoT es uno de los más inseguros ya que implica dispositivos con comunicación a Internet de muy bajo coste, con funcionalidades muy limitadas de seguridad o de actualización de *firmware*.

Hay muchos tipos de dispositivos para IoT doméstica que permiten por ejemplo controlar la calefacción o el aire acondicionado remotamente, o que reaccione automáticamente según el aprendizaje de nuestras costumbres personales, recibir datos de sensores específicos de ruido, humedad o concentraciones de dióxido de carbono, control del uso de la energía, el agua o el gas en tiempo real, etc.

De esta manera en vez de focalizarnos en los casos de uso, vamos a analizar de forma resumida los objetivos más comunes de las aplicaciones de IoT doméstico.

1.2.6.1 MONITORIZACIÓN Y CONTROL

La monitorización y el control remoto de dispositivos y equipamiento doméstico es quizás el rasgo común de las Casas Inteligentes. Más allá de las funcionalidades específicas de cada dispositivo, estos sistemas se caracterizan por proveer de datos en tiempo real, como la energía usada o el porcentaje de humedad en una estancia, así como datos históricos que permiten discernir tendencias.

Con la inclusión de la inteligencia y la analítica de datos, las posibilidades del control remoto se automatizan mediante algoritmos y/o técnicas de ML/DL. Esta es una tendencia actual de estos entornos que sigue avanzando.

1.2.6.2 OPTIMIZACIÓN DEL GASTO Y REDUCCIÓN DEL IMPACTO MEDIOAMBIENTAL

La capacidad de monitorizar los usos de energía se traduce en una visibilidad de los puntos de sobrecarga del sistema doméstico, tanto en energía eléctrica, como tendencias en el uso del agua o el gas.

23 <https://csa-iot.org/all-solutions/matter/>

Aplicaciones como la Iluminación Inteligente permiten optimizar el consumo eléctrico de iluminación, con el uso de sensores de presencia y movimiento interconectados.

Esta optimización se traduce en una huella de carbono menor por habitante de la vivienda, que unido a otras aplicaciones como los *microgrids* (redes inteligentes de energía a pequeña escala) o las energías renovables, como los paneles solares, tienen un impacto mucho mayor.

1.2.6.3 SEGURIDAD DOMÉSTICA

Este campo de la tecnología está tradicionalmente asociado a los sensores de presencia y cámaras de seguridad con video en tiempo real, para aumentar la seguridad física de las residencias domésticas.

Pero el IoT ha ayudado a evolucionar estas soluciones, como las cámaras de video con analítica de datos (reconocimiento facial, alerta ante peligros o anomalías), pero también a implementar nuevas soluciones de seguridad física y general. Un ejemplo de ellas serían las cerraduras inteligentes, o los sensores de fugas de agua o gas, o de contaminación ambiental. Este tipo de aplicaciones de IoT aumentan el nivel de seguridad de las viviendas y de sus ocupantes, con capacidades que antes no existían o eran muy costosas de implementar.

1.2.7 Ciudades Inteligentes

Los centros urbanos a nivel global están incrementando su población, y por tanto la complejidad de la su gestión. Según las estimaciones²⁴, cerca del 70% de la población vivirá en una ciudad para 2050. A esto se le une el cálculo²⁵ de que para 2030 en el mundo tendremos 43 megaciudades (ciudades con más de 10 millones de habitantes), incrementando las 31 que existen a día de hoy.

En respuesta a esto, las ciudades y sus gobernantes están buscando herramientas e implementándolas con el objetivo de poder evolucionarlas de una manera eficiente y sostenible. Una de esas herramientas son las tecnologías de la información o IT, como arco que engloba otras aplicaciones como las tecnologías de las operaciones u OT (*Operational Technology*) y las tecnologías de sensores y datos que conforman el IoT, y que resumen la aplicación de tecnologías digitales en diferentes ámbitos de la ciudad para proporcionar acceso a la información.

24 <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>

25 <https://www.un.org/en/desa/around-25-billion-more-people-will-be-living-cities-2050-projects-new-un-report>

Con el desarrollo y el uso masivo en el siglo XXI de las tecnologías de la información, grandes corporaciones y ciudadanos digitales se han unido a los esfuerzos gubernamentales para mejorar la calidad de vida en los centros urbanos, que alcanza temáticas como la mejora de los sistemas de transporte, medioambiente saludable y sostenible, crecimiento económico, bienestar social, aumento de la eficacia de los órganos de gobierno de las ciudades, entre otros. El uso de las tecnologías de la información y sus derivadas para ayudar a solucionar problemas urbanos, gestionar ciudades, y mejorar la calidad de vida se asocia estrechamente con el concepto de las *Smart Cities*, aunque la definición de *Smart City* todavía no está del todo clara.

En los próximos puntos de este capítulo recorreremos el desarrollo de este escenario IoT desde sus orígenes a su situación actual, la definición de una *Smart City* y sus casos de uso más importantes.

1.3 EVOLUCIÓN DE LA DIGITALIZACIÓN DE LAS CIUDADES

Una vez hemos visto la importancia del IoT y los escenarios que habilita, vamos a profundizar en el escenario de las *Smart Cities*. Hemos planteado su papel como habilitador que ayuda a las ciudades a abordar determinados aspectos como el cambio climático, la gestión eficiente de la energía y el transporte o la mejora de la calidad del aire. Todo esto además reforzado por la evolución de las personas a un estilo de vida mucho más digitalizado.

Pero ¿cuál es la historia de las *Smart Cities*? ¿Y cómo han evolucionado desde su concepción? ¿Y qué papel juega el IoT en todo esto? Para responder a estas preguntas vamos a hacer un pequeño recorrido por la historia de las últimas décadas para entender mejor de dónde venimos, y a dónde vamos, antes de centrarnos en la definición actual de *Smart City*.

1.3.1 Primeros pasos y evolución histórica

El viaje a los orígenes de las Ciudades Inteligentes comienza realmente desde que se empiezan a aplicar máquinas de cálculo, sistemas computacionales y tecnologías de la información a los servicios de gestión municipales, como el censo, los impuestos, registros etc. Esto nos lleva a finales del siglo XIX, cuando se empezaron a introducir máquinas tabuladoras y mecanismos de conteo para sustituir a los humanos en las labores de elaborar un censo, por ejemplo. A mediados del siglo XX, empresas como IBM introdujeron los sistemas computacionales que sustituyeron a las máquinas de cálculo que se habían utilizado hasta entonces.

Si avanzamos un poco en el tiempo, nos encontramos con la aplicación de técnicas y herramientas apoyadas por computador para modelar problemas y contexto de una ciudad. Específicamente, de Los Ángeles (EE. UU.) en 1974, donde la ciudad, a través de la agencia pública CAB (*Community Analysis Bureau*), empezó a usar bases de datos digitales, analítica de datos y fotografía aérea infrarroja para recolectar datos y producir informes demográficos y de calidad de las viviendas por barriada, con el objetivo de tener mejores herramientas de decisión para luchar contra la pobreza. Se puede considerar esta iniciativa “*A Cluster Analysis of Los Angeles*”, utilizando tecnología puntera para la época, como la primera “Ciudad Digitalizada” en la historia.

Más tarde, en 1981, encontramos otro ejemplo significativo en Singapur. El gobierno creó la agencia NCB (*National Computer Board*) con la misión de conducir a la ciudad a través de la evolución que estaban creando las tecnologías digitales para mejorar la competitividad económica y la calidad de vida de sus residentes, aprovechando las ventajas que proporcionaban las tecnologías de la información, nacientes aún. En los años siguientes se cableó mediante fibra óptica buena parte de la ciudad, lo que permitió aplicar la tecnología a problemas como la congestión del centro urbano, utilizando modelos como el teletrabajo de forma masiva.

A principios de la década de 1990 las tecnologías de la información empezaron a ser potencialmente disruptivas con la expansión de Internet. En 1994, Ámsterdam creó una ciudad virtual digital²⁶, DDS (*De Digital Stad*) para promocionar el uso de Internet, pudiéndose considerar el primer prototipo de *Digital City*, término antecesor al de *Smart City*.

Como resultado de estos avances, a finales de esa década y a principios de la década de los 2000, varias ciudades como Bangalore (India), San Diego (EE. UU.), Ottawa (Canadá), Southampton (Reino Unido), Brisbane (Australia) y otras, comenzaron a usar la IT y sus derivados para solucionar problemas urbanos.

Mientras tanto, IBM, que fue una pieza fundamental en la primera digitalización de muchos municipios en el siglo anterior, fue pionera en 2008-2009 con iniciativas como *IBM Smarter Planet* sobre la investigación aplicada en sensores, redes de comunicación y análisis de datos aplicada sobre problemas urbanos, que se complementó con otra iniciativa de marketing sobre *Smart Cities*²⁷ de 50 millones de dólares²⁸. Esta iniciativa se desarrollaba alrededor del concepto de las “*Smarter Cities*” y la utilización de la tecnología para mejorar la sostenibilidad de las ciudades y la calidad de vida de sus ciudadanos, planteando capacidades como el IoT o el *Big Data* que todavía estaban consolidándose. Otros gigantes tecnológicos como

26 <https://waag.org/en/project/digital-city-dds/>

27 <https://www.ibm.com/downloads/cas/2JYLM4ZA>

28 <https://www.ibm.com/ibm/be/en/responsibility-smarter-cities-challenge.html>

Siemens, Cisco Systems o General Electric también lanzaron iniciativas similares de servicios tecnológicos para mejorar la gestión de los municipios, con un modelo planteado desde las corporaciones tecnológicas hacia las ciudades.

De estas iniciativas, entre 2008 y 2010 emergieron proyectos de ciudades demostradoras como San Francisco, Ámsterdam y Seúl²⁹, con pilotos de tecnologías que involucraban al IoT, para probar las capacidades y el potencial en los casos de uso aplicados a los centros urbanos.

En paralelo, desde el sector público también se avanzó en la legislación para empujar la digitalización de servicios de los consumidores finales. En 2009, las Directivas de electricidad y gas, 2009/72/EC y 2009/73/EC respectivamente, plantean a los estados miembros un despliegue de contadores inteligentes (*Smart Meters*) marcando un mínimo de cobertura a los consumidores de un 80% para 2020. También en 2009, en EE. UU., la iniciativa gubernamental ARRA (*American Recovery and Reinvestment Act*) proporcionó financiación económica³⁰ (9.500 millones de dólares entre financiación pública y privada) para proyectos americanos de *Smart Grid* o Red Eléctrica Inteligente.

A la vez, para ese periodo entre 2008-2010, la civilización a nivel global había evolucionado social y tecnológicamente proporcionando, entre otras muchas capacidades, unas condiciones que sirvieron como catalizador para el desarrollo de aplicaciones para *Smart Cities* con un modelo planteado desde los usuarios finales, en contraste, y complementando el modelo que, como hemos visto, se estaba planteando desde los proveedores de tecnología hacia las ciudades. Estas condiciones se pueden resumir en 3:

1. Por primera vez en la historia, la población de las ciudades igualó a la población rural en el mundo³¹.
2. El número de usuarios de las líneas celulares (móviles)³² superó por primera vez al número de usuarios de líneas fijas (xDSL, Fibra óptica, HFC).
3. El Internet de las Personas, que se había desarrollado en los últimos 20 años, permitió plantear el Internet de la Cosas, con un foco claro en las comunicaciones M2M.

29 <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2009/m03/cisco-and-metropolis-collaborate-to-develop-sustainable-intelligent-cities.html>

30 <https://www.energy.gov/oe/recovery-act-reports-and-other-materials-smart-grid-investment-grant-sgig>

31 <https://www.statista.com/statistics/1262483/global-urban-rural-population/>

32 <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2011.pdf>

Además de estos macro factores, en esa época había otros elementos clave que ayudaron a evolucionar las aplicaciones y los casos de uso en *Smart Cities*. El carácter masivo que estaban adquiriendo la web 2.0 y las redes sociales, la llegada de los teléfonos inteligentes que permitió la difusión e implementación de aplicaciones en el contexto de un dispositivo móvil, el desarrollo del IoT como campo específico en la tecnología, o los ejercicios de transparencia de los gobiernos y municipios para compartir datos de fuentes propias, forman parte de esos elementos clave que permitieron la creación de lo que hoy conocemos como *Smart Cities*.

A partir de esas fechas, el concepto de uso de tecnologías como el IoT para optimizar y mejorar servicios municipales se consolidó y empezó a existir un mercado más maduro de soluciones y proveedores tecnológicos. En 2011 se celebró el primer congreso internacional *Smart City Expo World Congress* en Barcelona³³, con 50 países representados y 6.000 visitantes, que se convirtió en un referente global de soluciones, proveedores y clientes del sector público hasta el día de hoy.

En la última década (2012-2022) hemos asistido a la explosión del concepto de *Smart City*, con grandes urbes poniendo en acción planes en este sentido para hacer frente a los grandes desafíos a los que se enfrentan en las próximas décadas. Al comienzo de 2013 había aproximadamente 143 proyectos en implantación o en producción que se autodenominaban *Smart Cities*³⁴, con 35 en Norte América, 47 en Europa, 50 en Asia, 10 en América del Sur y 10 en Oriente Medio y África.

A día de hoy encontramos decenas de casos de uso y cientos de proyectos urbanos que se apoyan en la tecnología y el IoT para construir su camino “*Smart*” hacia la sostenibilidad, la calidad de vida y la diferenciación. En la Figura 2 se ilustra el ranking de 2022 según DCI (*Digital Cities Index*) de las ciudades con mayores capacidades digitales o inteligentes.

33 <https://www.smartcityexpo.com/>

34 J.H. Lee, M.G. Hancock, and M. Hu, Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco, *Technological Forecasting and Social Change*, in press, 2014.

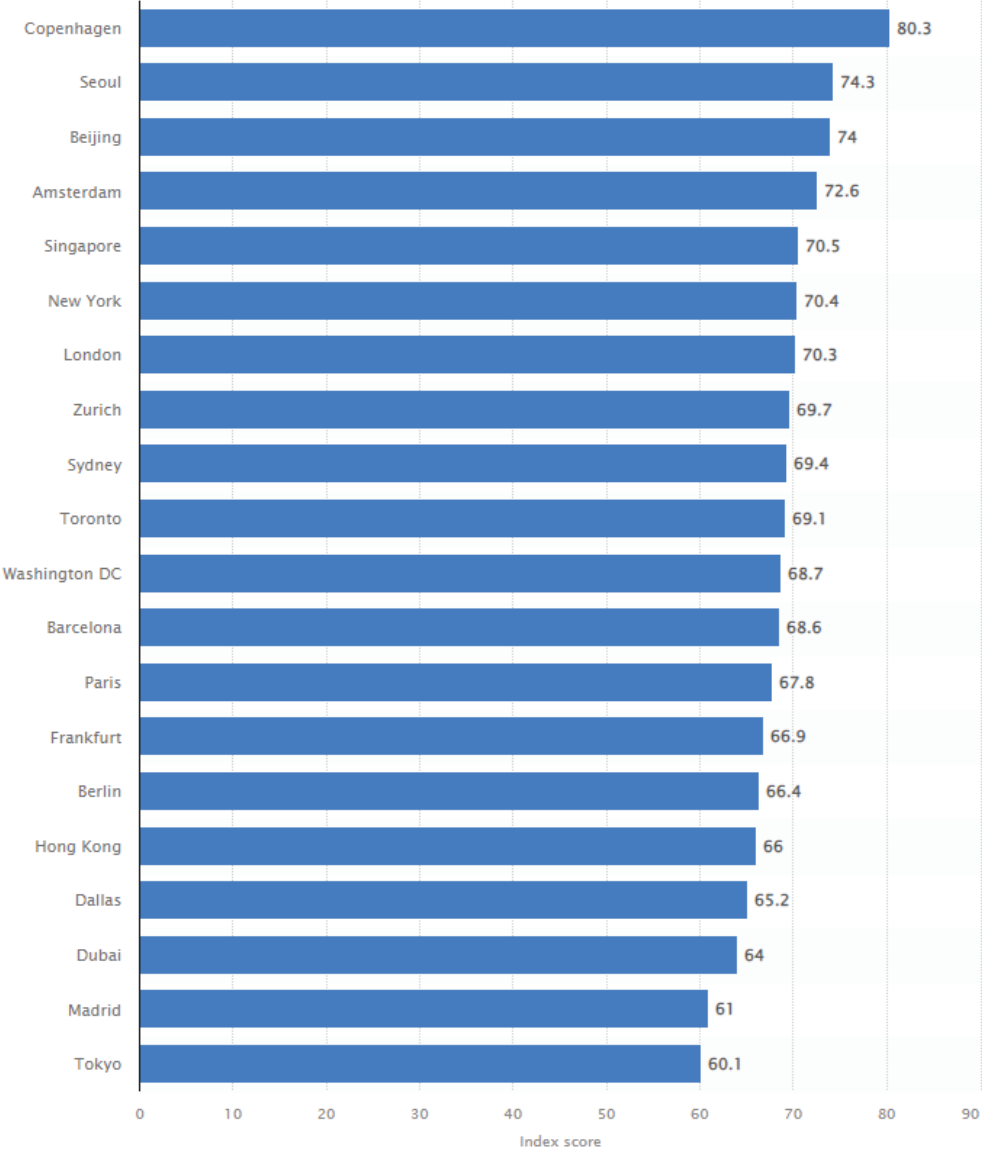


Figura 2: Ranking de Ciudades Digitales en 2022

1.3.2 El salto tecnológico

Como hemos visto, las bases para la digitalización de los centros urbanos y municipios se plantearon en la primera década del siglo XX. A grandes rasgos, podemos plantear 3 fases de evolución en la digitalización de los servicios en las ciudades, como puede observarse en la Figura 3.



Figura 3: Evolución de la digitalización en las ciudades

Así, comenzamos con ciudades con un bajo nivel de digitalización, donde los servicios públicos dependen de interacciones manuales, y se le sigue dando protagonismo a los documentos físicos en papel. En la segunda fase, la administración electrónica ya está implantada completamente, con procesos automatizados para la interacción con los residentes en cuanto a censos, impuestos, tributos e información y servicios telemáticos, y se están explorando otros casos de uso con la ayuda de la tecnología. Es en la tercera fase donde se digitalizan el resto de servicios y se hace uso del IoT y la automatización de las comunicaciones M2M de manera intensiva, y es donde el concepto de *Smart City* se consolida, como veremos más adelante.

Un elemento que ha sido crucial a la hora de poder estimular esa evolución y cambios de fase ha sido la tecnología, y en particular los usos de las tecnologías de la información (IT) y del IoT. Estos avances y nuevas aplicaciones han permitido

hacer realidad las infraestructuras digitalizadas de las ciudades como las conocemos a día de hoy.

La evolución y el desarrollo que han tenido las *Smart Cities* en la última década no hubiera sido posible sin el apoyo de diferentes tecnologías. Entre ellas, podemos nombrar al IoT, el *Big Data* y la analítica de datos y la computación en la nube como las más importantes.

El modelo IoT lo veremos en profundidad en el siguiente capítulo, pero vamos a resumir los aportes más importantes de las otras dos tecnologías y sus derivados.

1.3.2.1 BIG DATA

Una de las circunstancias que nos encontramos cuando aplicamos el modelo IoT en una *Smart City* es el volumen y la tipología de los datos adquiridos a través de las diferentes aplicaciones. Estos datos son una mezcla de datos estructurados, semi estructurados o no estructurados, dependiendo de los servicios IoT implementados.

El análisis de estos datos, llamado BDA (*Big Data Analytics* o analítica del *Big Data*), ayuda a extraer información y correlaciones del conjunto de datos explotados por la *Smart City*, para poder tomar decisiones informadas.

El BDA es una pieza indispensable para poder habilitar las Decisiones basadas en Datos (DDD o *Data-driven Decision making*). DDD refiere a la práctica de basar las decisiones en el análisis de los datos disponibles, en vez de utilizar la intuición.

Se utilizan varias tecnologías, desde el ML (*Machine Learning*), la minería de datos o el DL (*Deep Learning*). Comparados con los métodos tradicionales estadísticos del análisis de datos, BDA permite gestionar flujos de datos estructurados (como bases de datos relacionales como SQL) y no estructurados (como MongoDB) y extraer indicadores cuantitativos y cualitativos de los mismos.

Por ello, la aplicación de técnicas BDA en los servicios IoT de una *Smart City* es indispensable para poder explotar adecuadamente el volumen y el flujo de datos adquiridos, y refinar la toma de decisión y el valor que nos aportan estos datos.

1.3.2.2 COMPUTACIÓN EN LA NUBE

La computación en la nube ha servido herramienta de construcción de servicios digitales y ha catalizado los desarrollos de las aplicaciones IoT para *Smart*

Cities proporcionando capacidades de procesamiento y almacenamiento de datos escalables en tiempo real, y servicios avanzados de *software*.

Su uso en este campo ha estado ligado a las plataformas centralizada de gestión y control utilizadas para ejecutar las aplicaciones de la *Smart City*, ya sean aplicaciones verticalizadas o casos de uso específicos, o plataformas horizontales que homogeneizan las aplicaciones verticales presentando un punto central de normalización y gestión. De esta forma, se centraliza la recolección, procesamiento, almacenamiento de los datos y toma de decisiones. Hablaremos más a fondo sobre estas plataformas en el siguiente capítulo.

La recolección y adquisición de datos de estas aplicaciones IoT puede ser masiva, dependiendo del caso de uso, el número de activos monitorizados y la frecuencia de las actualizaciones, entre otras cosas. La computación en la nube permite acomodar este volumen de datos para poder almacenarlo y procesarlo con las técnicas de *Big Data* del punto anterior.

1.3.2.3 COMPUTACIÓN EN LA NIEBLA/DISPOSITIVO

Como hemos visto, la computación en la nube proporciona servicios avanzados que benefician a las aplicaciones IoT y hacen posible el despliegue de estas soluciones.

Pero hay determinadas aplicaciones donde la computación en la nube no cumple los requisitos indispensables para que sean viables. Concretando algunos ejemplos, tenemos las necesidades de datos en tiempo real continuo, de movilidad, de latencias bajas y de sincronización y coordinación, que no son cubiertas satisfactoriamente con el modelo tradicional en la nube.

Uno de los problemas más difíciles de resolver a día de hoy es la latencia de transmisión de datos entre los dispositivos IoT (o dispositivos *Edge* según nomenclatura anglosajona) y la nube, pública o privada. Para ello se introdujo la arquitectura de computación en la niebla (*Fog Computing*) o en los dispositivos IoT (*Edge Computing*), para ofrecer servicios IoT más localizados, con preprocesamiento de datos en local y por tanto con latencias bajas. Esta arquitectura permite mover algunas funcionalidades de procesamiento desde la nube a los propios dispositivos, o a elementos intermedios (como *gateways*, o servidores locales) que están localizados geográficamente para dar soporte a grupos de dispositivos IoT. En la Figura 4 podemos ver representada las capas de Fog y Edge Computing en una arquitectura IoT.

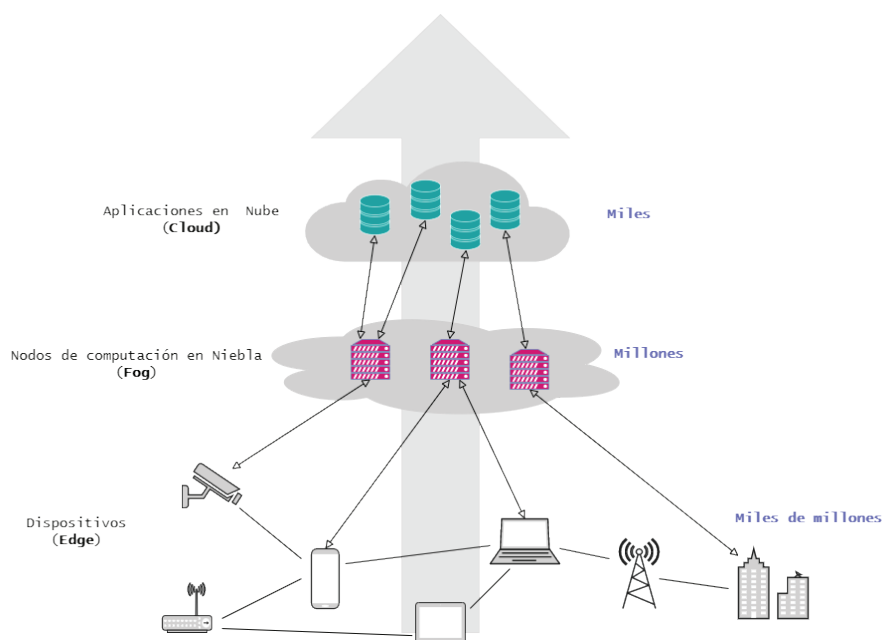


Figura 4: Arquitectura IoT con Cloud, Fog y Edge Computing con escala de magnitud de unidades

Tanto el *Fog* como el *Edge Computing* ayuda a descentralizar las infraestructuras de procesamiento de datos, dividiéndolo entre los dispositivos y elementos intermedios y la nube de forma eficiente para cada aplicación. De esta forma se reduce el volumen de datos que se transmiten a la nube. Además, se pueden aprovechar estas capacidades de preprocesamiento para aportar características de ciberseguridad y privacidad, como anonimizar datos en origen antes de transmitirlos a la nube, o marcar determinados flujos de información para que se circunscriban a una localización determinada, como por ejemplo los datos de pacientes recogidos en un hospital.

Esta tecnología complementa a la computación en la nube, y permite capacidades como analítica de datos a corto plazo en los dispositivos mientras que utilizamos la nube para las proyecciones a medio/largo plazo que utilizan más recursos, además de como repositorio histórico. En la Figura 4 se puede observar la arquitectura IoT con *Cloud*, *Fog* y *Edge Computing*.

A medida que el procesamiento de los datos está más cerca de, o en los mismos dispositivos donde se genera, las aplicaciones y posibilidades para desarrollar inteligencia distribuida e interacciones automatizadas en M2M (sensores, actuadores o dispositivos finales en general) siguen evolucionando y es uno de los caminos claves de las aplicaciones IoT para *Smart Cities* en el futuro.

1.4 LA ERA DE LAS SMART CITIES

Una vez hemos repasado la evolución histórica y los habilitadores tecnológicos, corporativos y sociales que han desembocado en lo que hoy conocemos como *Smart Cities*, estamos en condiciones de poder definir el término un poco más.

De las definiciones que podemos encontrar, y las tendencias que hemos visto en los últimos años, podemos deducir que lo que hace a una ciudad “*Smart*” es la utilización de tecnologías de la información (IT) y sus derivados. Podemos resumirlo en la utilización de nuevas tecnologías, que permiten optimizar la eficiencia y efectividad de servicios, actividades y procesos municipales. Esta optimización se alcanza normalmente haciendo que elementos y actores diversos interactúen en un sistema inteligente, más o menos interactivo.

En este sentido, podemos ver el concepto de *Smart City* como el reconocimiento de la importancia y criticidad de las nuevas tecnologías, especialmente el IoT, para la mejora de la competitividad de la ciudad, así como proporcionar un camino más sostenible para el futuro, de una forma transversal a las personas, negocios, infraestructuras, energía, espacios y en definitiva los principales actores y activos de los centros urbanos. Y así, podemos articularlo sobre algunas ideas esenciales:

- Agenda medioambiental y energética de la ciudad.
- Comunicación fluida entre los actores del tejido urbano: ciudadanía, empresas, instituciones. Participación activa de los usuarios de los bienes y servicios de la ciudad en su concepción y desarrollo.
- Sinergias e interoperabilidad entre dominios y sistemas transversales (e. g. transporte, energía, educación, salud, servicios públicos esenciales, etc.)
- Integración de las nuevas tecnologías de la información y de la comunicación en las aplicaciones y servicios de la ciudad, y el cambio de comportamiento y uso por parte de los ciudadanos.

Así que, aunque las nuevas tecnologías son un elemento crucial para el concepto de *Smart City*, no son suficientes para definirlo por sí solas. Las *Smart Cities* no se crean únicamente desplegando sensores, redes y analítica de datos intentando mejorar la eficiencia. Si no hay un marco de trabajo en el que estén representados los actores del tejido urbano, y una visión del contexto de la ciudad y su evolución y objetivos a largo plazo, no sabemos para qué, ni cuanto tenemos que mejorar esa eficiencia de una forma que sea sostenible en el tiempo.

1.4.1 Definición y Características de una Smart City

Existen varias definiciones de la *Smart City*, dependiendo de los autores y el momento temporal en que nos fijemos de las últimas dos décadas, pero ninguna universalmente aceptada aún.

Veamos algunos ejemplos, provenientes de definiciones académicas y de agencias gubernamentales para dejar fuera el sesgo que pueda haber en definiciones de grandes corporaciones tecnológicas.

Para empezar, tenemos definiciones que ahondan en el aspecto tecnológico:

“Las iniciativas de Ciudades Inteligentes intentan mejorar el rendimiento urbano mediante el uso de datos, información y tecnologías de la información (TI) para proporcionar servicios más eficientes a los ciudadanos, para monitorizar y optimizar la infraestructura existente, para aumentar la colaboración entre diferentes actores económicos y para fomentar modelos de negocio innovadores tanto en el sector privado como en el sector público”³⁵

“El uso de tecnologías de Computación Inteligente para hacer que los componentes y servicios de la infraestructura crítica de una ciudad, que incluyen administración de la ciudad, educación, salud, seguridad pública, bienes raíces, transporte y servicios públicos, sean más inteligentes, interconectados y eficientes”³⁶

Otro modo de abordarlo es desde el aspecto más humano, social y educativo:

“Las Ciudades Inteligentes tienen alta productividad ya que tienen una participación relativamente alta de personas altamente educadas, trabajos intensivos en conocimiento, sistemas de planificación orientados al rendimiento, actividades creativas e iniciativas orientadas a la sostenibilidad”³⁷

“Una Ciudad Inteligente, según ICLEI³⁸, es una ciudad que está preparada para proporcionar las condiciones para una comunidad sana y feliz bajo las exigentes

35 M.L. Marsal-Llacuna, J. Colomer-Llina's, and J. Meléndez-Frigola, “Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative, Technological Forecasting and Social Change” (2014)

36 <https://www.forrester.com/report/Helping-CIOs-Understand-Smart-City-Initiatives/RES55590>

37 K. Kourtis, P. Nijkamp, and D. Arribas, “Smart Cities in Perspective – A Comparative European Study by Means of Self-organizing Maps,” *Innovation: The European Journal of Social Science Research* 25: 2 (2012) 229–246

38 Gobiernos Locales por la Sostenibilidad <https://iclei.org/>

condiciones que pueden traer las tendencias globales, ambientales, económicas y sociales”³⁹

Y también hay definiciones que aúnan ambas visiones:

“Ciudad inteligente como una ciudad de alta tecnología intensiva y avanzada que conecta personas, información y elementos de la ciudad utilizando nuevas tecnologías para crear una ciudad sostenible, más verde, competitiva e innovadora, y una mayor calidad de vida”⁴⁰

“Una Ciudad Inteligente o *Smart City* es un sistema interconectado que aplica las nuevas tecnologías para gestionar de forma más eficiente los servicios públicos de las ciudades, asociado a múltiples interesados dentro del ecosistema urbano.”⁴¹

Desde nuestra opinión, esta perspectiva de complementar ambas visiones es la mejor forma en la que podemos definir el concepto, y vamos a adherirnos a la definición que propone la UNE en su norma UNE 178201:2016⁴². Podemos entonces definir las *Smart Cities* de la siguiente manera:

“Una **Ciudad Inteligente** (*Smart City*) es una ciudad justa y equitativa **centrada en el ciudadano**, que mejora continuamente su **sostenibilidad y resiliencia**, aprovechando el conocimiento y los recursos disponibles, especialmente **las Tecnologías de la Información y Comunicación (TIC)**, para mejorar **la calidad de vida, la eficiencia de los servicios urbanos, la innovación y la competitividad**, sin comprometer las necesidades futuras en aspectos **económicos, de gobernanza, sociales y medioambientales**.”

La definición, los atributos y los requisitos de una *Smart City* son útiles no solamente para la definición del concepto en sí, sino también como base de una semántica común y elemento de relación entre las infraestructuras tecnológicas, métricas e indicadores y políticas de las *Smart Cities*.

Pero ¿cómo decidimos si una ciudad entra dentro de la categoría de *Smart City*? Aquí podemos encontrar múltiples criterios que se ajusten a nuestra definición.

39 L. Guan, “Smart Steps To A Battery City,” Government News 32: 2 (2012) 24–27

40 Bakıcı, T., Almirall, E., & Wareham, J. (2013). A Smart City Initiative: The Case of Barcelona. Journal of the Knowledge Economy, 4(2), 135–148. <https://doi.org/10.1007/S13132-012-0084-9>

41 [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET\(2014\)507480_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf)

42 <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0056504>

Por ello, para responder a esta pregunta se definen una serie de características que consideramos intrínsecas de una *Smart City*. De esta forma, podemos plantear que una *Smart City* debe tener una o varias de estas características o ámbitos para ser considerada como tal.

Pese a que no hay un consenso en relación a los ámbitos mínimos que deben cumplir una *Smart City*, diversos organismos e instituciones han tratado de homogeneizarlo. El Parlamento Europeo presentó, en 2014, un modelo específico para describir los distintas características o ámbitos de aplicación de las *Smart Cities*. Posteriormente, estos ámbitos han sido definidos como atributos en la norma española UNE 178201:2016, la misma que plantea la definición que hemos adoptado.

Así, podemos definir 6 ámbitos o características que caracterizan a una *Smart City*, que podemos ver representados en la Figura 5.

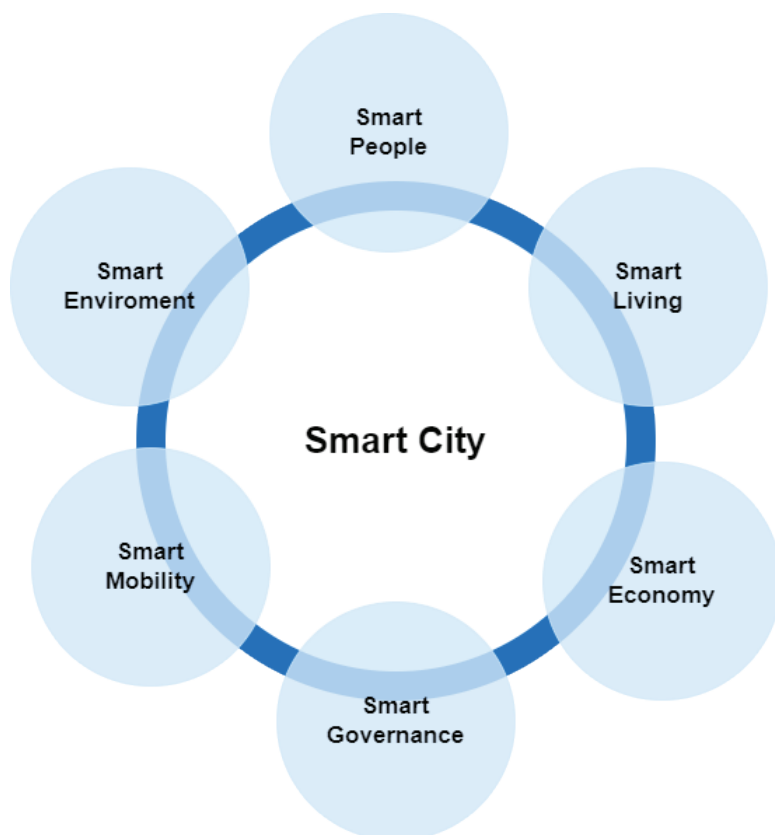


Figura 5: Características de una Smart City

Estos ámbitos de la Smart City se definen como:

Energía y Medio Ambiente Inteligentes (*Smart Environment*), que incluye la utilización de energías renovables y redes de energía telegestionadas, la gestión de la energía en edificios y afecta a servicios urbanos como el alumbrado público, la recogida de residuos, el suministro de agua potable y recogida de aguas fecales, entre otros. Su principal objetivo es asegurar la sostenibilidad medioambiental, realizando una gestión eficiente del ciclo del agua, reduciendo el consumo de energía (electricidad, gas, etc.) a través de la aplicación de distintas medidas de eficiencia energética y mejorando la gestión de residuos y los indicadores ambientales a través de la reducción de las emisiones contaminantes.

Gobierno Inteligente (*Smart Governance*), que incluye el gobierno del municipio y para el municipio, con servicios e interacciones que integran los diferentes intereses del marco urbano, públicos, privados y ciudadanos, mediante herramientas tecnológicas, procesos eficientes, interoperabilidad y con decisiones basadas en datos. Aquí se agrupan todos aquellos servicios destinados a modernizar la administración, optimizar los recursos públicos, aumentar la transparencia de la gestión y de los datos de gobiernos, y facilitar la administración electrónica, para hacer que sea más eficiente para los ciudadanos. Como factor transversal, este ámbito puede integrar y orquestar el resto de ámbitos, o algunos de ellos.

Bienestar Inteligente (*Smart Living*), que está ligado a conceptos como la cohesión y el capital sociales de las ciudades. Su objetivo es desarrollar servicios que mejoran la calidad de vida de los ciudadanos y su estilo de vida. Dentro de este ámbito se engloban aspectos como la salud, la gestión de la demanda asistencial, la teleasistencia, la asistencia a colectivos vulnerables, gestión de emergencias sanitarias, y la seguridad, tanto personal como material, con aspectos como la ciberseguridad, la videovigilancia urbana, la gestión de contingencias o la seguridad en el transporte.

Movilidad Inteligente (*Smart Mobility*), que incluye todos los atributos relativos al transporte y los sistemas de logística. Su objetivo es utilizar la tecnología para reducir el tráfico urbano, la contaminación urbana y los tiempos de los desplazamientos en la ciudad, con ejemplos como el desarrollo de sistemas de información en tiempo real sobre el estado del tráfico o el estado de las plazas de aparcamiento o de sistemas integrados para promover el transporte urbano sostenible, combinando el transporte privado (automóvil, motocicletas, bicicletas, etc.) con el transporte público (tren, metro, tranvía y autobuses urbanos). Estos sistemas pueden utilizarse para permitir a los usuarios proporcionar su propia información en tiempo real y contribuir a la planificación de la movilidad a medio-largo plazo.

Sociedad Inteligente (*Smart People*), que proporciona un entorno adecuado para la mejora de la creatividad y el impulso a la innovación, englobando todos los ámbitos relacionados con el capital humano de la sociedad urbana, educación, colaboración ciudadana y aspectos de inclusión social.

Economía Inteligente (*Smart Economy*), que aborda aspectos relacionados con la economía y negocios urbanos, empleo, marketing personalizado o fomento del turismo, con un aporte tecnológico como catalizador.

Como hemos comentado, al no haber una definición universalmente aceptada de estas características podemos encontrar otros puntos de vista sobre el número y la naturaleza de ámbitos Smart que definen a una *Smart City*. Pero un consenso común es que uno de los puntos clave para estimar como de “*Smart*” es una ciudad que se basa en las interrelaciones e intercambios de información entre los diferentes ámbitos. Intuitivamente, esto se consigue a través de la implementación de las nuevas tecnologías que hemos introducido anteriormente. Por tanto, independientemente de cuales sean los ámbitos específicos a considerar, el rol de la tecnología como aglutinante es uno de los conceptos fundacionales que define una *Smart City*.

En la Figura 6 podemos encontrar una representación de la interrelación entre los niveles de una Smart City extraída del NIST 1900-206⁴³.

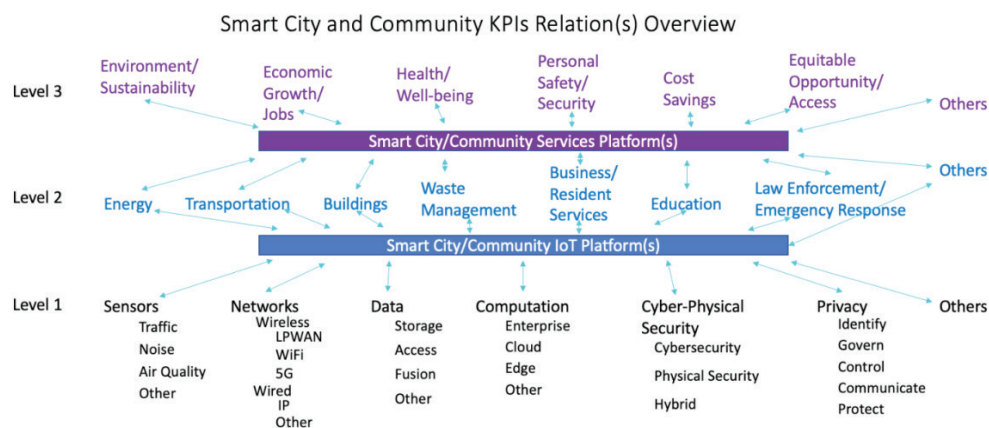


Figura 6: Relaciones entre los niveles de una Smart City

43 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-206.pdf>

1.4.2 El impulso de la Administración a las Smart Cities

Alrededor de esta definición y estas características de Smart City, en la última década se han desarrollado planes estratégicos desde los gobiernos, a escala mundial, en los ámbitos locales, estatales o incluso paneuropeos. España ha sido uno de los países pioneros en la estandarización de normas para *Smart Cities*.

El Comité Técnico de Normalización sobre Ciudades Inteligentes (AEN/CTN 178), promovido por la SETSI (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información) fue creado por AENOR en diciembre de 2012, para llevar a cabo la tarea de normalización en el área de interés de las ciudades inteligentes.

Posteriormente, El Ministerio de Energía, Turismo y Agenda Digital (MINETAD), con el respaldo del sector industrial, las redes de ciudades (RECI (Red Española de Ciudades Inteligentes) y FEMP (Federación Española de Municipios y Provincias)) y la UNE (Asociación Española de Normalización), desarrolló el Plan Nacional de Ciudades Inteligentes⁴⁴, publicado en 2015 y vigente hasta 2017. A continuación, y como evolución del mismo, se desarrolló el Plan Nacional de Territorios Inteligentes⁴⁵, que extiende el alcance más allá de las ciudades, como podemos ver en la Figura 7.



Figura 7: Plan Nacional de Territorios Inteligentes, 2017

44 <https://plantl.mineco.gob.es/planes-actuaciones/Paginas/plan-nacional-ciudades-inteligentes.aspx>

45 https://advancedigital.mineco.gob.es/es-es/Novedades/Documents/Plan_Nacional_Territorios_Inteligentes.pdf

En otros países y regiones también ha habido un impulso específico a la creación y financiación de actuaciones que podemos enmarcar en las *Smart Cities*. Podemos encontrar múltiples ejemplos, como China⁴⁶, EE. UU.⁴⁷, la UE⁴⁸ o Australia⁴⁹, que han creado diversos planes e iniciativas para homogeneizar el concepto y las prestaciones que ofrece una *Smart City* en sus territorios. En el punto 3.2.5 veremos más en profundidad la normativa local e internacional y los marcos de trabajo y estandarización que se han desarrollado en los últimos años.

En definitiva, podemos ver que la planificación estratégica y la evolución de las *Smart Cities* y su estandarización son aspectos que atraen un gran interés y están desarrollándose y creciendo. Pero hay al menos un aspecto que, hasta ahora, no se ha tenido suficientemente en cuenta para la estandarización ni para la consecución de unas buenas prácticas mínimas en el sector. Este aspecto no es otro que la Ciberseguridad, que tiene un gran impacto dado el apoyo en las nuevas tecnologías que hemos visto que tiene el concepto de *Smart City*. Aspectos como la privacidad de los datos de los ciudadanos, el cumplimiento normativo, la regulación de dispositivos *hardware* y *software* con mecanismos básicos de ciberseguridad, etc., han adquirido una importancia considerable dado que los casos de uso de aplicación de tecnologías IoT en las ciudades tienen aspectos que pueden considerarse críticos, como veremos más adelante en el punto 1.6.

Algunos autores del mundo urbanístico introducen el concepto “transdisciplinar”⁵⁰ para describir posibles enfoques de soluciones compuestas de diferentes disciplinas para dar respuesta a la problemática compleja de las ciudades. Podemos decir que la ciberseguridad y la privacidad tienen que imbuirse de este carácter transdisciplinar para poder responder a las necesidades que nos plantean las *Smart Cities*. A partir del capítulo 3 entraremos de lleno en el aspecto de ciberseguridad y la importancia que tiene en un escenario *Smart* y las amenazas y mitigaciones actuales, y describiremos un marco de trabajo ciberseguro en el capítulo 4 que pueda complementar los planes estratégicos que se están desarrollando.

46 https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf

47 <https://www.dhs.gov/science-and-technology/smart-cities>

48 <https://www.europarl.europa.eu/factsheets/es/sheet/95/el-fondo-europeo-de-desarrollo-regional-feder->

49 <https://www.infrastructure.gov.au/territories-regions-cities/cities/smart-cities-suburbs/smart-cities-plan>

50 Ledesma de la Rosa, C. (2017). Gestión de proyectos de regeneración integrada de barriadas residenciales obsoletas. Desde el enfoque transdisciplinar y a través de la metodología PMBOK. Tesis Doctoral, Universidad de Sevilla

En el punto 1.5 vamos a profundizar en los servicios y aplicaciones IoT que podemos encontrar en las *Smart Cities* actuales, y que están alineados con uno o más ámbitos de los que hemos descrito.

1.4.3 El futuro de las Smart Cities

Como hemos visto hasta ahora, el concepto de *Smart City* está plenamente vigente y evolucionando globalmente, mientras las aplicaciones de la tecnología IoT están permitiendo a las ciudades digitalizar y optimizar servicios e interacciones de una forma ágil y orientada a los desafíos que afrontan en el siglo XXI.

Además, la necesidad de replantear nuestro modo de vida urbano es más urgente que décadas atrás. Y una de las principales soluciones por las que se está apostando es por los planes estratégicos para las *Smart Cities*, en las que el compromiso medioambiental es uno de sus principales pilares, alineado con los Objetivos de Desarrollo Sostenible (ODS)⁵¹ que plantea la ONU (Organización de las Naciones Unidas) para en el año 2030.

Para terminar, vamos a enumerar los desafíos y las tecnologías van a ser previsiblemente importantes para la evolución del modelo de *Smart City* en el futuro cercano.

1.4.3.1 DESAFÍOS

Por lo expuesto en anteriores apartados, parece claro que las *Smart Cities* han llegado en la última década para quedarse. Pero para poder seguir evolucionando hay que tener en cuenta algunos desafíos que todavía están por resolver.

Por ejemplo, desde el **ámbito del gobierno** de la *Smart City*, no existe aún una homogeneización de quién debe liderar este tipo de proyectos en las ciudades. Al ser soluciones transversales que afectan a varios centros de decisión (TIC, Operación y Mantenimiento de servicios públicos, Innovación, etc.) todavía estamos en una fase en la que se está produciendo la adaptación de cómo y quién tiene que planificar, impulsar y mantener las soluciones que forman parte de los servicios *Smart* de la ciudad. Esto es normal desde el punto de vista de que la implantación de aplicaciones IoT está todavía en sus primeras fases de adopción y explotación, pero que, si no se estandariza, puede ser un factor que impida la implantación de estrategias de sostenibilidad y resiliencia mediante el uso de la tecnología y el cambio de paradigma social.

51 <https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/>

Por otro lado, el **marco estratégico** que han planteado los diferentes gobiernos y mercados sobre **estandarización, interoperabilidad y planes de financiación** de este tipo de proyectos en ciudades tiene que continuar para estimular la adopción y la evolución de las diferentes soluciones, para que se pueda acelerar la madurez de la que no gozan todas las aplicaciones IoT en *Smart Cities* a día de hoy, por la disparidad temporal de en qué momento se han empezado a implementar. Estos planes estratégicos de financiación actúan como catalizadores y la aceleración de iniciativas que ayuden a reducir indicadores necesarios para el futuro es algo necesario para aspirar a los objetivos ODS.

Por último, el planteamiento de **ciberseguridad** para *Smart Cities* va por detrás de la implementación de las tecnologías y los servicios IoT en las ciudades. Aspectos como la resiliencia de los servicios digitalizados o la privacidad de los ciudadanos son críticos para que el concepto de *Smart City* madure de una forma sostenible. Dedicaremos el capítulo 3 y 4 a hablar de este concepto, que es uno de los desafíos más claros a los que se enfrentan las *Smart Cities* de ahora en adelante.

1.4.3.2 TECNOLOGÍAS PARA EL FUTURO DE LAS SMART CITIES

Hasta hoy, la evolución de la tecnología ha sido uno de los habilitadores principales del modelo de las *Smart Cities*, con IoT en una posición muy prominente. Por tanto, es interesante plantear un breve análisis de que otras tecnologías se están empezando a utilizar, o se prevé que utilicen en el futuro, en este ámbito.

1.4.3.2.1 Inteligencia Artificial

Dada la naturaleza orientada a los datos que ha traído la digitalización y aplicación de tecnologías IoT en las ciudades, el volumen de datos que se maneja es cada vez mayor. Es necesario utilizar técnicas de IA para poder utilizar estos datos de manera eficiente, y permitir la evolución de las decisiones basadas en datos.

En las *Smart Cities* del futuro la analítica de datos mediante IA se prevé como una constante. Las tecnologías específicas donde se está avanzando son:

Machine Learning (ML) o Aprendizaje Automático es una rama de la IA que estudia la automatización de tareas mediante el entrenamiento de un modelo con datos específicos, pero con la característica de que es un modelo capaz de adaptarse con mínima intervención humana. Tiene muchas aplicaciones en las *Smart Cities*, desde los sistemas de transporte inteligente, la ciberseguridad, los sistemas de energía inteligente, etc.

Deep Learning (DL) o Aprendizaje Profundo es un subconjunto del *Machine Learning* que estudia las redes neuronales artificiales para imitar el proceso de aprendizaje del cerebro humano. Las redes neuronales están compuestas por múltiples capas y están optimizadas para tareas de clasificación y predicción. Al igual que ML, DL tiene múltiples usos en las aplicaciones y servicios de una *Smart City*, desde la detección de anomalías de ciberseguridad en IoT a la ayuda al modelado de situaciones en cualquier escenario IoT/IT de los que hemos visto hasta ahora para las ciudades.

Uno de los desafíos más importantes para las técnicas de ML/DL es la capacidad de usarlas correctamente para analizar datos y sacar conclusiones efectivas que nos permitan tomar decisiones. A día de hoy, dependiendo del campo de aplicación en la *Smart City*, estas soluciones están más o menos avanzadas, pero todavía queda un gran recorrido para que puedan convertirse en la parte principal de la analítica avanzada de las aplicaciones de *Smart Cities* y el volumen de datos que adquieren. El uso de la computación en la niebla/dispositivo es uno de los catalizadores del avance de estas técnicas de IA en el IoT, permitiendo que se procesen los datos adquiridos de forma distribuida lo más cerca posible de la fuente.

La **Visión por computador** es una aproximación multidisciplinar que permite adquirir, procesar, analizar y entender las imágenes con un contexto definido. Es uno de las verticales de aplicación de las tecnologías ML/DL más avanzada, ya que el modelo de reconocimiento de patrones y decisión se implementa con ellas. Por otro lado, tecnologías de campos diferentes como PNL (Programación Neurolingüística) se están aplicando la Visión por computador⁵², permitiendo desarrollar aplicaciones con mayores capacidades, como el piloto automático FSD (*Full Self-Driving*) de los automóviles eléctricos Tesla y su *Language of Lanes*⁵³. En una *Smart City* tiene roles cada vez más importantes, donde la monitorización y el reconocimiento de patrones de video se está volviendo ubicua.

1.4.3.2.2 Internet of NanoThings

El Internet de las Nanocosas o IoNT (*Internet of NanosThings*) es un punto de convergencia donde la nanotecnología, el IoT y la industria 4.0 se encuentran. Básicamente es la misma premisa que en las tecnologías IoT, pero a una escala mucho más pequeña: un sistema de nano cosas conectadas que poseen identificadores únicos para transferir datos a través de una red de comunicación hacia un repositorio

52 Wiriyathamabhum, Peratham & Summers Stay, Douglas & Fermüller, Cornelia & Aloimonos, Yiannis. (2016). Computer Vision and Natural Language Processing: Recent Approaches in Multimedia and Robotics. ACM Computing Surveys. 49. 1-44. 10.1145/3009906.

53 <https://www.tesla.com/support/autopilotDone>

en la nube. Involucra un gran número de nanosensores que se pueden utilizar para dar información más precisa y detallada de un objeto o infraestructura en particular.

Las aplicaciones de esta tecnología son inmensas, y aumentarán en el futuro las capacidades de los casos de uso y aplicaciones del IoT tradicional en las *Smart Cities*.

1.4.3.2.3 Nuevos protocolos de comunicación celular

La comunicación 5G entró en servicio comercialmente alrededor de 2020. Aunque aún no está completamente desplegada ni evolucionada, como veremos en el capítulo 2, ofrece potencialmente unos anchos de banda y requerimientos de conectividad alineados con las aplicaciones actuales y del futuro cercano.

Pero la explosión de volumen de datos, necesidad de latencias bajas y número de dispositivos conectados que se prevé con la madurez de las tecnologías IoT/IT/OT hacen necesarias plantear las alternativas más allá del 5G. Aplicaciones multimedia enriquecidas, soluciones de monitorización de la ciudad con audio/video en tiempo real, video de muy alta resolución (4K, 8K) y el aumento del número de suscriptores de la red hacen que la previsión actual sea de 5 Zeta-bytes al mes hasta 2030⁵⁴.

Por ello, es necesaria la investigación de nuevos estándares y tecnologías que se conviertan en la sexta generación de comunicación celular, el 6G.

1.4.3.2.4 Blockchain

Blockchain es una forma de Bitácora Distribuida o DL (*Distributed Ledger*) donde los datos se almacenan usando múltiples nodos, eliminando la posibilidad de un único punto de fallo.

Debido a su naturaleza descentralizada, ofrece inmutabilidad, trazabilidad y un registro a prueba de manipulaciones de almacenamiento de datos. La integración de *blockchain* mejora la interoperabilidad al permitir una interconexión segura y el intercambio de datos entre varios sistemas.

Aunque la tecnología *blockchain* ofrece beneficios teóricos para las aplicaciones IoT en términos de seguridad, hay una serie de barreras para su adopción generalizada. La principal reside en el propio concepto de dispositivo IoT. Dado que muchas redes IoT están compuestas por dispositivos alimentados por baterías con capacidades de computación limitadas, una de esas barreras de adopción es el propio nodo final de IoT.

54 <https://www.itu.int/dms pub/itu-r/opb/rep/R-REP-M.2370-2015-PDF-E.pdf>