

ANÁLISIS EXPLORATORIO DE
COMERCIALIZACIÓN DE
SERVICIOS DE
**CONECTIVIDAD PARA EL
IOT EN MÉXICO**

El Estatuto Orgánico del IFT establece que la Dirección General Adjunta de Prospectiva y Análisis de Impacto Económico (DGAPAIE) tiene la atribución de “Realizar análisis exploratorio de datos para determinar si existen patrones o tendencias a fin de hacer recomendaciones de diseño de políticas regulatorias” y de “Diseñar y realizar encuestas para la elaboración de estudios y análisis de prospectiva regulatoria o de impacto económico en el ámbito de su competencia”¹.

Este informe fue elaborado con información obtenida mediante metodologías y técnicas de ciencia de datos como el análisis exploratorio, la automatización de consultas a sitios web para la sistematización y la elaboración de bases de datos que permiten identificar patrones de comercialización entre los proveedores de servicios de Internet de las Cosas (IoT, por sus siglas en inglés). Utilizando metodologías como la *Knowledge Discovery in Databases* y herramientas de *Web Scraping* programadas y diseñadas por la DGAPAIE, bajo los estándares de seguridad y ética cibernética internacionalmente aceptados, generando una base de datos con los perfiles de las empresas que comercializan servicios de IoT en México.

Este informe se complementa con los resultados de la encuesta realizada a empresas que ofrecen servicios IoT en México, aplicada desde el 3 de octubre al 11 de noviembre de 2022, y que tiene como objetivo generar información cualitativa que profundice sobre la experiencia de las empresas que ofrecen servicios de IoT en México, así como la evolución, retos, logros y expectativas de este modelo de negocio en México.

En resumen, este documento es producto del análisis realizado a partir de fuentes públicas de información, metodologías y técnicas de ciencia de datos, sin prejuzgar sobre la opinión del Pleno del Instituto, de las áreas sustantivas adscritas del Instituto o de cualquier otra autoridad sobre el tema en particular. En este sentido, el documento pretende proporcionar indicios sobre los patrones de comercialización de los servicios asociados al IoT en México, con base en la información disponible y apegado a las metodologías más robustas y confiables disponibles para el análisis de datos.

Estudio elaborado por:

| **Maricarmen Cosío Trujillo**, Analista de Bases de Datos de Telecomunicaciones y Ecosistema Digital

| **Tomas Solache Ramos**, Jefe de Departamento de Modelos Econométricos

| **Raúl Esqueda Martínez**, Subdirector de Modelos Econométricos

| **Jorge Eduardo Ponce Leyva**, Director de Prospectiva

| **Rodrigo Guarneros Gutiérrez**, Director General Adjunto de Prospectiva y Análisis de Impacto Económico

| **Pedro Javier Terrazas Briones**, Coordinador General de Planeación Estratégica

¹ Artículo 74, fracción XV y XVII, Estatuto Orgánico del IFT.

Índice

Introducción	4
1. Perspectivas y evolución del mercado de IoT	8
Tendencias en el desarrollo y aplicaciones de IoT	12
Usuarios de los servicios de Telecomunicaciones y su conocimiento sobre IoT	13
Expectativas sobre el desarrollo de IoT y oportunidades para los operadores de telecomunicaciones	14
2. Acciones regulatorias para Internet de las Cosas (IoT).	17
Arabia Saudita	19
Argentina	21
Brasil	23
Canadá	25
China	28
Colombia	30
Corea del Sur	33
Emiratos Árabes Unidos	34
Estados Unidos	35
India	40
Japón	42
Malasia	44
México	46
Reino Unido	49
Singapur	50
Unión Europea	51
3. Análisis exploratorio de datos de IoT en México	57
Metodología y aplicación de herramientas de Ciencia de Datos	57
Proyectos IoT en México	60
Comercialización de los servicios de IoT en México	65
Análisis de Clúster	75
4. Encuesta a las empresas que ofrecen servicios IoT en México	79
Conclusiones	92
Anexo 1. Metodología de Web Scraping.	94
¿Qué es Web Scraping?	94
Herramientas utilizadas y generación de algoritmo	95
Procesamiento de la información	97
Clasificación de las páginas web	97
Conformación de la base de datos	97
Limitantes y dificultades	97
Código para R Studio	98
Anexo 2. Metodología de Ciencia de Datos utilizadas	101
Metodología Knowledge Discovery in Data Bases (KDD).	101
Pasos de la metodología KDD.	101
Anexo 3: Análisis de Clúster	103
Metodología para el análisis de clúster	103
Algoritmo utilizado en R Studio	105

Introducción

Este documento constituye un paso natural en el análisis del ecosistema IoT y la confirmación de las tendencias identificadas en el documento seminal realizado por el IFT previamente y denominado "Análisis exploratorio de la comercialización de servicios de conectividad para IoT"². Se trata de una segunda fase, donde se busca confirmar cuáles son las tendencias comerciales de conectividad para IoT en México y si éstas son similares a las encontradas en el reporte previo a nivel internacional.

Para el propósito del presente documento, se parte de elementos de análisis que en conjunto proporcionan información fundamental sobre el ecosistema de IoT en México:

- La cadena de valor de la industria de IoT –descrita a detalle en el reporte previo y retomada brevemente para su pronta referencia en este documento–;

- Técnicas de ciencia de datos que van desde el análisis exploratorio de los datos hasta el *Web Scraping* para la búsqueda de las empresas que ofertan servicios de IoT en México a través de búsquedas automatizadas en Internet;

- La metodología *Knowledge Discovery in Databases* (KDD) para identificar patrones importantes, útiles y entendibles en los datos recabados, y que implica utilizar técnicas de *data mining* acorde a la información con la que se cuenta, optando por un análisis para encontrar patrones o grupos (*clusters*) dentro de un conjunto de observaciones a través de la técnica de *K-means clustering* a efectos de realizar las agrupaciones correspondientes.

- Encuesta de tendencia de negocio aplicada a empresas de la industria de IoT en México.

En la narrativa que aquí se propone, se hace énfasis en la información sobre los principales rubros de inversión, tendencias, aplicaciones de IoT, el conocimiento por parte de los usuarios de Telecomunicaciones sobre el IoT y las oportunidades de negocio para los operadores de Telecomunicaciones, tomando en cuenta el crecimiento experimentado en esta industria donde se estima que cada minuto se están conectando 4,800 dispositivos nuevos en las plataformas de IoT alrededor del mundo³.

El presente estudio se divide en cuatro secciones, en la primera sección se presenta una breve descripción de la evolución del IoT desde una perspectiva global, partiendo de los primeros desarrollos de IoT en 1999, la tecnología alrededor de las redes 2G y 3G, la tecnología 4G LTE y el impulso a partir de las necesidades derivadas de la nueva normalidad provocada por el COVID-19. Incluye, además, los servicios integrados basados en la nube para IoT.

² El análisis realizado en 2020 se encuentra disponible en: <http://www.ift.org.mx/estadisticas/analisis-exploratorio-de-datos>

³ Forbes (2016). 152,000 *Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things*. Disponible en: <https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/?sh=35df59344b63>

La segunda sección de este documento se refiere a las tendencias internacionales en materia de acciones regulatorias y estandarización de IoT, además, se incluyen casos de uso de IoT a nivel mundial. En la tercera sección se presenta la metodología y resultados del análisis exploratorio de datos de IoT, en el que se incluye información sobre los proyectos identificados que utilizan IoT en el país, el análisis de la comercialización de los servicios en México y un análisis de clúster de las empresas de IoT. Por último, se presentan los resultados de la encuesta que fue aplicada a las empresas que ofrecen servicios de IoT en México.

En cuanto al contexto internacional, se presenta un análisis comparativo de las principales tendencias en 16 países, incluido México, con particular atención a las iniciativas que buscan fomentar el uso de IoT en cada economía. En este sentido, se incluyen iniciativas de los gobiernos centrales de cada país, así como de los reguladores sectoriales, incluidos algunos reguladores del sector de Telecomunicaciones. La experiencia internacional indica, por ejemplo, que únicamente el 44% de los países analizados cuentan con algún estándar técnico en materia de IoT que, por lo general, son expedidos por los gobiernos centrales.

Como se señaló en el reporte anterior elaborado por el IFT, **el IoT se define como una infraestructura global para la sociedad de la información, permitiendo servicios avanzados mediante la interconexión (física y virtual) de cosas basada en tecnologías de información y comunicación interoperables, existentes y en evolución** (recomendación ITU-T Y.2060)⁴. Infraestructura que permite recolectar volúmenes de información masivos que pueden procesarse para generar información útil a los interesados en el uso de esta tecnología y la optimización de los procesos que integran.

En México se identifican algunas iniciativas gubernamentales entorno al desarrollo de IoT, su estandarización, su uso en diversos proyectos y comercialización en diversos sectores de la economía. Entre los patrones identificados en el ecosistema de IoT mexicano, se identifica que los proyectos donde el IoT juega un papel preponderante se han duplicado pasando de 14 en 2020 a 34 en 2021. Lo que implica un promedio de 3 proyectos nuevos al año en el horizonte comprendido entre 2012 y 2021.

El proyecto más grande identificado y documentado en México, en cuanto al número de dispositivos conectados tiene como objetivo el seguimiento y monitoreo de 125,000 vehículos. Por otra parte, más del 60% de los proyectos documentados (21 de 34 en 2021) implican la conexión de menos de 100 dispositivos, sin embargo, no se identifica una tecnología de conexión universal para el uso de la tecnología de IoT. Respecto a los proyectos grandes (más de 10,000 dispositivos), representan menos del 4% del total de proyectos y en general presentan una asociación intensa y positiva con las tecnologías de conexión de largo alcance y baja potencia (LPWA)⁵.

Conforme a las tendencias a nivel internacional, la oferta de servicios en el ecosistema de IoT está fragmentada, es decir, son pocas las empresas que ofrecen el servicio de IoT punto a punto (v.gr. desde el diseño y producción de dispositivos, la conectividad, la creación de *software* para la gestión de los dispositivos, hasta la explotación de los datos generados por los objetos conectados).

⁴ ITU (2012), *Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Overview of the Internet of Things*. Pág. (2). Disponible en: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>

⁵ IFT (2020), *Análisis exploratorio de la comercialización de los servicios de conectividad para IoT*. Disponible en: <http://www.ift.org.mx/sites/default/files/contenido-general/estadisticas/analisis-exploratorio-iot.pdf>

Por ejemplo, el 26.7% de las empresas dedicadas a algún punto en la cadena de valor de IoT ofrecen sólo servicios de *Software*, mientras que, el 13.6% se especializa en otros mercados laterales tales como la analítica de datos y ciberseguridad. De acuerdo con los resultados del análisis solo el 2.8% ofrecen servicios de extremo a extremo, el 4.0% se dedica al *Hardware* únicamente y un 2.8% se dedican exclusivamente a proveer conectividad para IoT, lo que suma el 50% del total de las ofertas comerciales identificadas en México.



Las ofertas comerciales en México se enfocan principalmente a los sectores de servicios y de producción de bienes, con énfasis en los servicios asociados con la Industria Manufacturera y de Transporte. En segundo lugar, destaca el control de dispositivos, los servicios dedicados a Ciudades Inteligentes y la Telemática. Así mismo, se puede observar un patrón en cuanto a la demanda por parte de las empresas, principalmente los clientes están relacionados con servicios de administración de plataformas, control y manejo de la información, seguido de consultores de sistemas y servicios profesionales para el desarrollo de *Software* y *Hardware*.

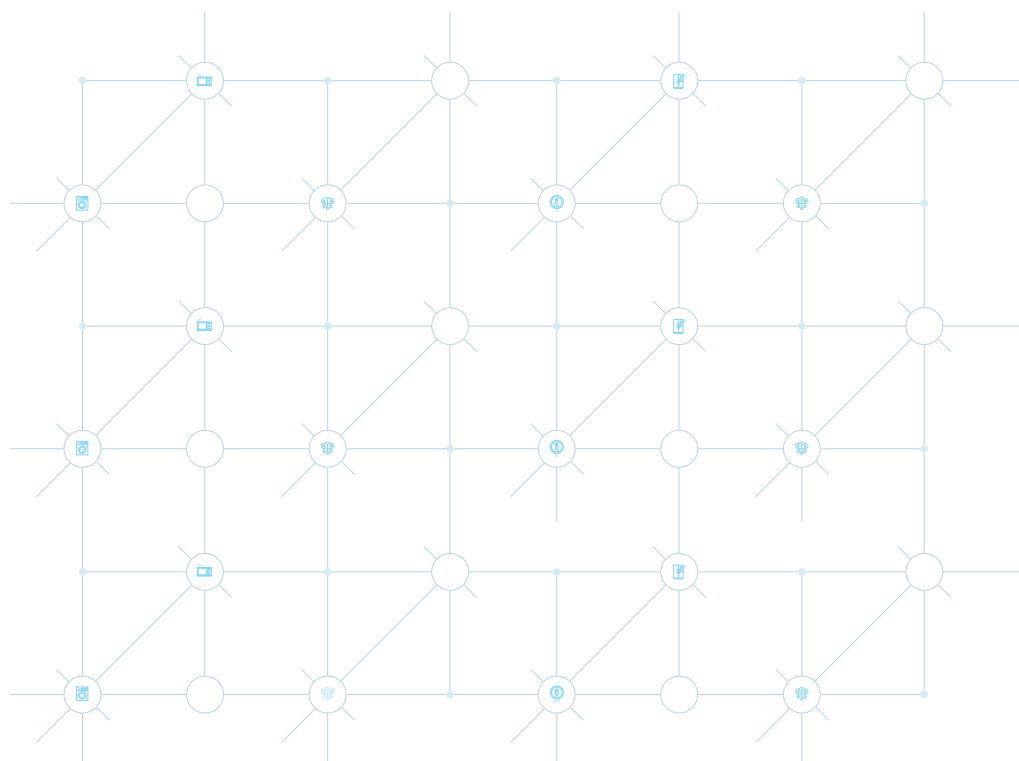
La búsqueda, mediante *Web Scraping*, de las empresas que ofrecen servicios de IoT en México a través de Internet permitió generar un conjunto de datos con información de 176 empresas que ofrecen sus servicios de IoT en México, con presencia en 21 estados del país, principalmente en la Ciudad de México (38.9%), Jalisco (15.2%), Nuevo León (11.9%) y el Estado de México (8.5%), seguidos por Querétaro (4.8%) y Chihuahua (3.7%).

El análisis de clúster identifica 4 grupos que por aproximación están compuestos de la siguiente forma: La Ciudad de México, por la cantidad de empresas que se localizan aquí, es un clúster con su propio centroide, seguido por el clúster formado por Jalisco y Nuevo León, en otro clúster se encuentran las entidades de Chihuahua, Estado de México, Puebla y Querétaro, mientras que, en el último clúster, se agrupan el resto de los estados donde se encuentran las empresas que ofrecen servicios de IoT en México.

En el análisis de la contribución del valor agregado de cada estado se pueden observar indicios de que las empresas que ofrecen servicios de IoT en nuestro país tienen una predilección por las entidades con mayor actividad económica.

Consistentemente con los resultados del análisis de 2020, donde se analizó empíricamente la comercialización de IoT a partir de herramientas de Ciencia de Datos, las ofertas de IoT en México están altamente atomizadas y se distinguen hasta 22 tipos diferentes de ofertas, concentradas principalmente en sectores productivos y de servicios críticos. Este documento toma como base los resultados y conclusiones del documento publicado en 2020 que presentó una visión ordenada y sistemática sobre el IoT partiendo de un marco teórico de economía de redes, para profundizar el análisis para el caso mexicano.

En tanto, los resultados de la encuesta muestran que las empresas que ofrecen servicios de IoT en México en su mayoría se consideran Micro, Pequeñas y Medianas empresas, donde la gran mayoría de las empresas conocen acerca de las Normas mexicanas de IoT. En cuanto a la tecnología utilizada por las empresas, estas prefieren las tecnologías celulares (3G, 4G y 5G) y las de mediano alcance (Wi-Fi, EnOcean, *etc.*), en sus proyectos conectan en promedio 100 dispositivos y señalan como oportunidades de crecimiento para el negocio de IoT proyectos enfocados a la industria y manufactura inteligente, seguridad y vigilancia, así como la administración de dispositivos.



1

Perspectivas y evolución del mercado de IoT

Esta sección presenta la evolución de la industria IoT tanto en términos económicos como de desarrollo tecnológico, con base en reportes especializados y fuentes de datos, en el que se incluye la experiencia de los usuarios de IoT en México y las expectativas de crecimiento de esta industria.

El concepto de Internet de las cosas (IoT) se mencionó por primera vez en 1999 para explicar los potenciales beneficios de la identificación por radiofrecuencia (RFID, por sus siglas en inglés), aunque existe evidencia de su uso en diversas aplicaciones desde 1982⁶.

Antes del inicio de la pandemia, en 2019, la conectividad mediante las redes 2G y 3G permitió el desarrollo de diversas aplicaciones de IoT, dada la complementariedad entre estas tecnologías, muchos proveedores implementaron ambas tecnologías. De acuerdo con datos del *Ericsson Mobility Report*⁷, de los 114 proveedores de servicios identificados en ese año, cerca del 25% daba servicios de IoT con ambas tecnologías, promoviendo el uso 2G y 3G hasta ese momento.

Con el despliegue de las redes móviles de nueva generación (4G y 5G), muchas redes 2G dejaron de operar; sin embargo, al tratarse de redes aún empleadas por una gran cantidad de dispositivos conectados, se consideró en algunos países la opción de reaprovechar la tecnología 2G y utilizarla para servicios tales como *Narrowband IoT* (NB-IoT) y la Categoría M1 (Cat-M1)⁸, debido principalmente a su bajo costo y a la disponibilidad de una amplia cobertura⁹.

De acuerdo con los datos de Ericsson, se estimaba que las conexiones de IoT representarían 10,800 millones a nivel mundial en 2019 y que alcanzarían las 24,900 millones de conexiones en 2025 con una tasa de crecimiento anual ponderada (CARG, por sus siglas en inglés) de 15%¹⁰.

La pandemia de COVID-19 aceleró la innovación, adopción y difusión de distintas aplicaciones en diferentes sectores e industrias, lo que ha favorecido el desarrollo del ecosistema de IoT. Durante 2020, con el inicio de las restricciones de movilidad, el uso de IoT se implementó en diversos sectores; principalmente en el sector salud (*v.gr.* Salud a distancia, control de pacientes, la información del estatus de la pandemia en tiempo real, los servicios médicos disponibles, el aislamiento de las personas infectadas y el rastreo de posibles contactos); todas estas aplicaciones fueron fundamentales para disminuir la propagación del virus.

⁶ Avast (2021), *¿Qué es el Internet de las cosas (IoT)?* Disponible en: <https://www.avast.com/es-es/c-what-is-the-internet-of-things>

⁷ Ericsson (2019), *Ericsson Mobility Report*. Pág. (17). Disponible en: <https://www.ericsson.com/4acd7e/assets/local/reports-papers/mobility-report/documents/2019/emr-november-2019.pdf>

⁸ Cat-M1 opera con un ancho de banda de 1.4 MHz con una mayor complejidad y costo de dispositivo que NB-IoT, pero el ancho de banda permite que Cat-M1 logre mayores velocidades de datos (hasta 1 Mbps), menor latencia y capacidades de posicionamiento de dispositivos más precisas, además, admite llamadas de voz. Para más información visite: <https://www.ericsson.com/en/blog/2019/2/difference-between-nb-iot-cat-m1>

⁹ NAE (2019), *Qué sucede con el apagado de redes 2G/3G*. Disponible en: <https://nae.global/es/que-sucede-con-el-apagado-de-redes-2g-3g/>

¹⁰ Ericsson (2019), *Ericsson Mobility Report*. Pág. (17). Disponible en: <https://www.ericsson.com/4acd7e/assets/local/reports-papers/mobility-report/documents/2019/emr-november-2019.pdf>

Los dispositivos tecnológicos interconectados, como los termómetros inteligentes que pueden medir la temperatura de un paciente, se utilizaron para crear conjuntos de datos para un análisis y diagnóstico más preciso. En algunos países se utilizaron los teléfonos móviles de los pacientes u otros dispositivos portátiles conectados para garantizar el cumplimiento de las reglas de cuarentena y establecer patrones de comportamiento a través de métodos de seguimiento y localización¹¹.

Durante 2021, se esperaba que hubiese una disminución de los casos de COVID-19 debido a la vacunación; sin embargo, las restricciones de movilidad permanecieron durante ese año, en este escenario las empresas tuvieron que adaptar sus actividades y acelerar sus iniciativas de digitalización. **En este contexto, Ericsson estimó que el número de conexiones de IoT era de 14,600 millones en 2021 y se ubicaría en 30,200 millones al cierre de 2027; es decir, un aumento de 15,600 millones de conexiones en seis años, lo que equivale a 2,600 millones de dispositivos al año y 217 millones de dispositivos nuevos conectados al mes o 296,804 dispositivos nuevos por hora**, lo que se traduce en una tasa de crecimiento anual ponderada a dos dígitos (13%)¹².

A principios de 2021, la empresa *Inmarsat* realizó una encuesta a 450 empresas de diferentes sectores (*v.gr. verticals*), dirigida esencialmente a las personas que son responsables de implementar las iniciativas de IoT en sus empresas. Lo anterior, con el objetivo de recabar información sobre la adopción y madurez de IoT en la industria global durante la pandemia de COVID-19.

Dentro de los resultados de la encuesta destaca la aceleración en la adopción de IoT a partir del COVID-19. De acuerdo con esta encuesta, el 77% de las empresas encuestadas han concluido el despliegue de al menos un proyecto de IoT entre 2020 y 2021, de los cuales el 41% fueron desplegados en menos de 12 meses. Mientras que el 23% restante señala estar en fase de prueba de implementación o planean implementarlo en los próximos 12 o 18 meses¹³.

En el ámbito global, las empresas continúan invirtiendo y utilizando cada vez más IoT, según el informe de *IoT Analytics*, la seguridad IoT, la agricultura vertical, el seguimiento de productores, el IoT de consumo, los semiconductores y la conectividad son las principales categorías en las que se invirtió más durante 2021 (Ver Tabla 1.1), y se prevé que la inversión continúe en dichos rubros para 2022¹⁴.

¹¹ Elsevier (2020), *AI, big data, cybersecurity and IoT in the era of coronavirus*. Disponible en: <https://www.elsevier.com/connect/ai-big-data-cybersecurity-and-iot-in-the-era-of-coronavirus>

¹² Ericsson (2021). *Ericsson Mobility Report*. Noviembre de 2021. Pág. (18). Disponible en: https://www.ericsson.com/4ae6a5/assets/local/reports-papers/mobility-report/documents/2021/emr_november2021_screen_epsanol.pdf

¹³ Inmarsat (2021), *Inmarsat Research Programme 2021: Industrial IoT in the time of Covid-19*. Disponible en: <https://www.inmarsat.com/en/news/latest-news/enterprise/2021/industry-accelerating-iot-adoption-in-response-to-covid.html>

¹⁴ IoT Analytics (2022), *IoT 2021 in review: The 10 Most Relevant IoT Developments of the Year*. Disponible en: <https://iot-analytics.com/iot-2021-in-review/>

Tabla 1.1. Principales rubros de inversión con relevancia para IoT en 2021.

Compañía	Importe	País	Categoría	Inversor principal
Armis Security	US\$300 millones	Israel	Seguridad IoT	One Equity Partners
Infarm	US\$200 millones	Alemania	Agricultura vertical basada en IoT	Qatar Investment Authority
Wiliot	US\$200 millones	Israel	Seguimiento de productos/ activos basado en IoT	SoftBank Vision Fund
Aqara	US\$160 millones (Aprox.)	China	IoT de consumo / <i>smart home</i>	Shenzhen Capital Group
Hangshun Chips	US\$160 millones (Aprox.)	China	Semiconductores IoT	Shenzhen Investment Holdings
Helium	US\$111 millones (Aprox.)	Estados Unidos	Conectividad IoT	Andreessen Horowitz

Fuente: IFT con información de IoT Analytics (2022), *IoT 2021 in review: The 10 Most Relevant IoT Developments of the Year*. Disponible en: <https://iot-analytics.com/iot-2021-in-review/>

A más de dos años del inicio de la pandemia, se espera que las soluciones de IoT aprovechen las ventajas que ofrecen las conexiones 5G (mejor ancho de banda, mayor velocidad de la red, baja latencia y mayor número de dispositivos conectados¹⁵) y se incrementen los casos de uso, como automóviles conectados, servicios críticos de telecomunicaciones, asistencia robótica en contingencias o emergencias, entre otros¹⁶.

Por otro lado, se espera que la influencia de empresas como Amazon, Google y Microsoft denominadas “hiperescaladores”, incrementen en los próximos años su influencia en la industria del IoT, a partir del uso de redes LoRaWAN, y su inversión en redes privadas 5G y IoT satelital con algunos servicios ya disponibles¹⁷:

Amazon Web Services IoT, provee un servicio de administración completo para el despliegue de proyectos personalizados de IoT, con una plataforma que almacena grandes cantidades de información provenientes de dispositivos IoT y facilita la creación de aplicaciones al ser desplegado a través de cómputo distribuido (v.gr. la nube).

¹⁴ IoT Analytics (2022), *IoT 2021 in review: The 10 Most Relevant IoT Developments of the Year*. Disponible en: <https://iot-analytics.com/iot-2021-in-review/>

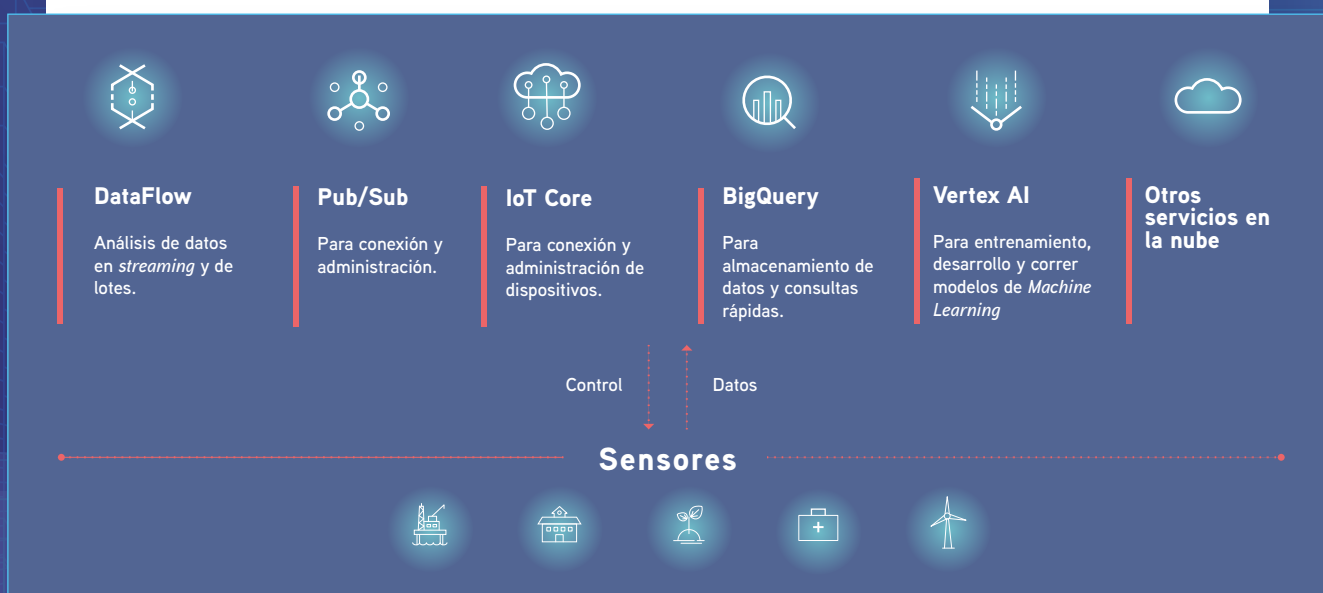
¹⁵ Para conocer a detalle los beneficios de la tecnología inalámbrica 5G, visite el portal institucional Sensor 5G. Disponible en: [Beneficios del uso de 5G | IFT](#)

¹⁶ Para conocer a detalle otros casos de uso asociados a la tecnología inalámbrica 5G, visite el portal institucional Sensor 5G. Disponible en: [Casos de uso 5G | IFT](#)

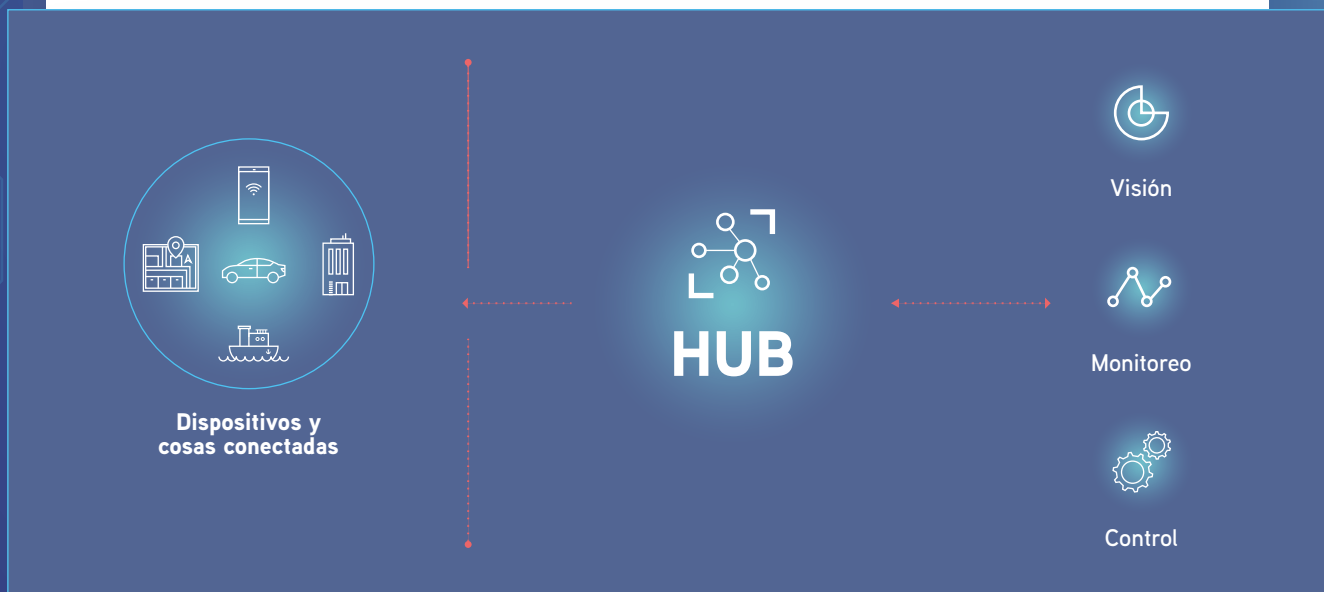
¹⁷ OMDIA (2021), *2022 Trends to Watch: IoT Services and Platforms*. Pág. (5). Disponible en: <https://omdia.tech.informa.com/OM021539/2022-Trends-to-Watch-IoT--Services--Platforms>



Soluciones de Google Cloud IoT, una alternativa de solución en la nube que permite predecir el mantenimiento de los dispositivos, optimizar su rendimiento en tiempo real, prever los tiempos de inactividad, detectar anomalías y hacer un seguimiento de las condiciones, el estado y la ubicación de estos. Su alcance incluye la administración de la cadena de suministro y logística, edificios y ciudades inteligentes, seguimiento de recursos en tiempo real, entre otros.



Azure IoT Hub de Microsoft, es una aplicación que habilita la comunicación entre la nube y los objetos conectados, que permite la explotación de datos para generar inteligencia de negocios, monitoreo y control de los dispositivos.



Tendencias en el desarrollo y aplicaciones de IoT

Las aplicaciones clave para el desarrollo del IoT, incluyen entre otras, el mantenimiento predictivo para equipos industriales, hogares inteligentes, red inteligente y dispositivos portátiles, la transformación digital de las empresas, la implementación de estándares de la Industria 4.0, así como la introducción de redes 5G y la adopción de análisis de datos¹⁸.

En este sentido, los últimos tres años han cambiado la dinámica en el desarrollo de proyectos de IoT. Durante 2019, los proyectos que se desarrollaron a nivel mundial se enfocaban en la manufactura, en específico en tecnología operativa y la industria 4.0 (23% del total), superando a los proyectos de gobierno (19% del total). Otros sectores que tuvieron representación ese año incluyen comunicaciones y tecnologías de la información (TI) (9%) y comercio minorista (9%). La distribución geográfica de esos proyectos fue la siguiente: el 38% de la implementación de proyectos IoT se realizaba en la región de Europa, mientras que en América del Norte se implementó el 30% del total; es decir, entre estas dos regiones se acumulaba el 68% del total de implementaciones¹⁹.

¹⁸ GlobalData (2022), *Global Enterprise Internet of Things (IoT) Market*. Pág. (5). Disponible en: <https://technology.globaldata.com/Analysis/details/global-outlook-report-brief-internet-of-things-iot>

¹⁹ GlobalData (2020), *IoT Deployment Trends in 2019*. Disponible en: <https://technology.globaldata.com/Analysis/CAdetails/IoT-Deployment-Trends-in-2019119344>

Un año después, en 2020, se registró un aumento del 30% en el número de proyectos IoT alrededor del mundo. En el sector manufacturero, el número de proyectos pasó de 76 a 127 atribuible al impacto de las restricciones de movilidad por COVID-19; en el sector de la salud también se incrementó el número de proyectos de 14 a 25. Otros sectores, como logística y construcción/ingeniería mostraron crecimientos en los despliegues, mismos que se aceleraron por la urgencia de soluciones para el monitoreo de personas y el monitoreo de condiciones ambientales por la pandemia provocada por COVID-19. Geográficamente, Europa continuó siendo la región con una mayor cantidad de implementaciones con el 34% del total, seguido de América del Norte con un 28%, destaca la región Asia-Pacífico que aumentó su participación en 15%²⁰.

Con estas tendencias, Global Data pronosticó que los ingresos por servicios de IoT pasarían de US\$539 mil millones en 2021 a US\$807.4 mil millones en 2025, lo que implicaría una CAGR del 10%. Al cierre de 2021, la mayor porción de los ingresos (US\$151.9 mil millones) correspondía a proyectos en los sectores de gobierno, servicios públicos y manufactura²¹.

Nokia, desplegó su tecnología *Scene Analytics* impulsada por Inteligencia Artificial (IA) en una prueba de concepto en Genk, Bélgica, para cuantificar el nivel de contaminación acústica a lo largo de una de las calles principales de la ciudad. Las autoridades de la ciudad abordaron las preocupaciones de salud y seguridad de los residentes y visitantes que soportan el ruido excesivo de los sistemas de escape modificados en automóviles, motocicletas y otros vehículos que utilizan la avenida Stalenstraat. Por lo cual, Nokia trabajó con socios tecnológicos para integrar una solución de prueba de concepto que aprovecha los datos de los micrófonos y las cámaras instaladas, que utilizan sensores de IoT a lo largo de la avenida.

Usuarios de los servicios de Telecomunicaciones y su conocimiento sobre IoT

La industria no es la única que está aprovechando los beneficios del Internet de las Cosas. Los hogares y las personas comienzan a aprovechar las soluciones tecnológicas para mejorar su calidad de vida y realizar de manera más rápida tareas rutinarias, conectando objetos cotidianos a la Internet para recopilar, almacenar y analizar datos que permitan optimizar y automatizar tareas. En este sentido, las principales aplicaciones del IoT en los hogares, se han enfocado en los sistemas de seguridad, teleasistencia, control remoto, programación de iluminación y calefacción.

Global Data estima que el mercado global de IoT alcanzará los US\$1,100 millones de ganancias para el año 2024; el 73% de estas ganancias tendrán origen en el IoT dedicado a las empresas y el restante 27% corresponderá al IoT de consumo en el hogar²².

²⁰ GlobalData (2020), *IoT Deployment Trends in 2020: COVID-19 Impacts and More*. Disponible en: <https://technology.globaldata.com/Analysis/CADetails/IoT-Deployment-Trends-in-2020-COVID19-Impacts-and-More123470>

²¹ GlobalData (2022), *Global Industrial IoT Services: Competitive Landscape Assessment*. Pág. (2). Disponible en: <https://technology.globaldata.com/Analysis/CADetails/Global-Industrial-IoT-Services-Competitive-Landscape-Assessment103024>

²² Global Data (2021), *Thematic Research: Internet of Things (2021)*. Pág. (4). Disponible en: <https://technology.globaldata.com/Analysis/Details/thematic-research-internet-of-things-2021>

La adopción del IoT en los hogares depende en gran medida del conocimiento de los usuarios respecto al uso y beneficios del IoT. Recientemente, la Coordinación General de Política del Usuario (CGPU) del IFT publicó la Cuarta Encuesta 2021 dirigida a Usuarios de Servicios de Telecomunicaciones. Los resultados de esta encuesta muestran que el 8.7% de los usuarios de Internet Fijo mencionó saber o haber escuchado algo sobre el IoT²³, respecto a las ventajas y desventajas percibidas sobre el uso de IoT, los usuarios mencionaron que las principales ventajas de IoT son la practicidad, comodidad y rapidez (53.2%) y que les permite estudiar y/o trabajar en casa/trabajo (12.2%). Por su parte, entre las principales desventajas mencionaron la necesidad de estar conectado todo el tiempo (27.1%), el riesgo de seguridad/hackeo (20.8%) y, por último, las fallas en la conexión (15.3%)²⁴.

El uso de los dispositivos conectados no se ha generalizado en el país, de acuerdo con los datos de la encuesta el 38.1% de los usuarios de Internet Fijo considera innecesario el uso de dispositivos IoT por la necesidad de conexión a Internet, el 34.2% consideran el precio y un 5% respondió que no sabría cómo utilizar el dispositivo²⁵.

Respecto a los usuarios de Telefonía Móvil, solo el 11.9% del total de encuestados mencionó tener conocimientos respecto a IoT²⁶, mientras que el 47.2% de los encuestados señaló conocer que existen dispositivos que pueden ser conectados a Internet y se pueden monitorear o controlar desde su teléfono móvil²⁷. Asimismo, las principales ventajas mencionadas por los encuestados incluyen: (i) El monitoreo/control de sus dispositivos en cualquier lugar (39.4%); (ii) La seguridad (20%), y (iii) El fácil acceso a la información de sus dispositivos (17.3%). Mientras que las principales preocupaciones mencionadas por los usuarios encuestados fueron: (i) El robo de información/hackeo de cuentas bancarias (49.5%), y (ii) El robo o extravío del teléfono móvil con el 14.6% de participación²⁸.

Expectativas sobre el desarrollo de IoT y oportunidades para los operadores de telecomunicaciones

Como se señaló en el reporte previo, la cadena de valor del IoT está altamente integrada, lo que permite a los operadores de telecomunicaciones expandir su posición a otras secciones de la cadena de valor adicional a la conectividad. En este sentido, los operadores de telecomunicaciones tienen una oportunidad de negocio dentro del mercado de IoT a través de la oferta de conectividad, así como las iniciativas que se tienen por parte de algunos operadores de ofrecer soluciones integrales para sus clientes.

²³ IFT (2022), *Cuarta Encuesta 2021. Usuarios de Servicios de Telecomunicaciones*. Pág. (11). Disponible en: <http://www.ift.org.mx/sites/default/files/contenido/general/usuarios-y-audencias/4taencuesta2021.pdf>

²⁴ *Ibidem*. Pág. (13-14).

²⁵ *Ibidem*. Pág. (17).

²⁶ *Ibidem*. Pág. (27).

²⁷ *Ibidem*. Pág. (28).

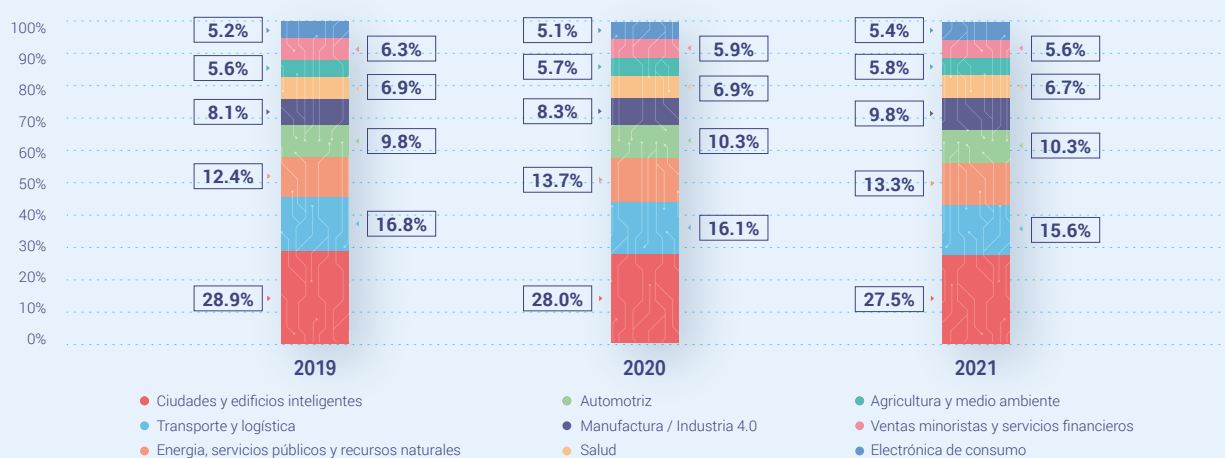
²⁸ *Ibidem*. Pág. (31-32).

Si bien, el mercado de servicios de IoT en el sector Industrial se ha ido desarrollado durante los últimos años, existe un incremento en la velocidad de adopción en virtud de su papel en la provisión de soluciones para afrontar las restricciones provocadas por la pandemia de COVID-19, tales como el monitoreo remoto de atención médica, el seguimiento de vacunas y pruebas, el seguimiento de personas, la ocupación de edificios y la medición de temperatura²⁹.

El reporte de seguimiento *IoT Service Provider Contract Tracker*³⁰ de Global Data, permite conocer los términos generales de los contratos entre empresas y proveedores de servicios de comunicaciones respecto a las soluciones de IoT a nivel mundial, estos contratos provienen de información pública procedente de proveedores de servicios, vendedores, comunicados de prensa de clientes, estudios de casos, blogs y otras fuentes, y constituyen una fuente de información valiosa que refleja las tendencias de inversión y desarrollo de IoT.

Los datos presentan un registro de casos por tipo de solución y número de contratos. En 2019, destacaron en orden de importancia las soluciones dirigidas a ciudades y edificios inteligentes, seguidas de transporte y logística, energía, servicios públicos y recursos naturales. Las aplicaciones que destacan por su crecimiento es el número de contratos en la manufactura e industria 4.0, que representó el 8.1% en 2019 y que para 2021 se incrementó 1.7 puntos porcentuales para ubicarse en 9.8%. No obstante, se confirma que la estructura de participación de los contratos de proyectos IoT por tipo de aplicación no ha cambiado en los últimos tres años (Ver Gráfica 1.1).

Gráfica 1.1. Número de contratos IoT por tipo de aplicación 2019 – 2021



Fuente: IFT con información de OMDIA (2022), *IoT Contracts Trackers* – 1H22. Disponible en: <https://omdia.tech.informa.com/OM023890/IoT-Contracts-Trackers—1H22>

²⁹ GlobalData (2022), *Global Industrial IoT Services: Competitive Landscape Assessment*. Pág. (1). Disponible en: <https://technology.globaldata.com/Analysis/details/Global-Industrial-IoT-Services-Competitive-Landscape-Assessment103024>

³⁰ Esta herramienta toma en cuenta contratos de diferentes empresas de telecomunicaciones como AT&T, Vodafone, Deutsche Telekom, Telefónica, Orange, Telenor, Verizon, MTS y TeliaSonera.

Los operadores de telecomunicaciones tradicionales se enfrentan a un ecosistema de IoT complejo y competitivo; si bien, pueden ofrecer conectividad a través de sus redes de telecomunicaciones, el ARPU de la conectividad para las conexiones IoT es relativamente bajo. Sin embargo, para los operadores, existe un nicho en aquellos proyectos que requieren de conexiones de red de área amplia de baja potencia (LPWAN, por sus siglas en inglés) y que incluyen banda angosta para IoT (NB-IoT) y LTE-M, para un alto volumen de conexiones.

Otra área de oportunidad de creciente dinamismo se encuentra en los despliegues de 5G para IoT masivo, donde se ubican aplicaciones tales como la fabricación en tiempo real, el comercio minorista hiperconectado y el análisis de video, los cuales requieren de un alto ancho de banda y conexiones de baja latencia³¹.

Uno de los principales casos de uso del IoT 5G es el de los vehículos conectados, servicios de comunicación vehicular que incluyen comunicación directa (entre vehículos, vehículo-peatón y vehículo-infraestructura) y comunicaciones soportadas por la red para la conducción autónoma. Estos casos de uso requerirán soluciones sobre la seguridad y comodidad al volante, el uso compartido del coche, la planificación de rutas, la conducción coordinada y las actualizaciones sobre el estado del tráfico en tiempo real³². También se identifican otros casos de uso tales como las redes privadas, los servicios informáticos y las pruebas que aprovechan las altas velocidades y la baja latencia de 5G.

El operador alemán Deutsche Telekom oferta *T-IoT*, el nombre comercial para un sistema de conectividad global de IoT, en asociación con T-Mobile US, que permite a las empresas administrar sus conexiones a nivel internacional. Además, proporciona conectividad de red para admitir NB-IoT, LTE-M, 4G LTE y 5G, así como opciones de administración en diferentes plataformas, incluido el Centro de control de T-Mobile y el Portal de servicios M2M de Deutsche Telekom. Esta solución de IoT es un ejemplo de cómo un operador puede aprovechar sus recursos para crear flujos de ingresos y relaciones que trascienden los modelos tradicionales de servicio móvil.³³

En este sentido, los operadores tradicionales también están integrando los servicios de IoT a sus ofertas comerciales con soluciones que incluyen consultoría sobre prueba de concepto y diseño de IoT; implementación, integración de sistemas, gestión continua y seguridad de las implementaciones de IoT; habilitación de aplicaciones, desarrollo personalizado a través de plataformas de aplicaciones propias o de socios, soluciones verticales de extremo a extremo y análisis de datos.

Otro ejemplo de ello es la estrategia que están adoptando empresas como Vodafone, Deutsche Telekom y Telefónica, buscando proveer soluciones a las grandes empresas y agrupar soluciones de IoT dirigidas a las PYMES³⁴.

³¹ GlobalData (2022), *Global Industrial IoT Services: Competitive Landscape Assessment*. Pág. (2-3). Disponible en: <https://technology.globaldata.com/Analysis/CADetails/Global-Industrial-IoT-Services-Competitive-Landscape-Assessment103024>

³² OpenMind BBVA (2021). *La convergencia del internet de las cosas y el 5G*. Disponible en: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/convergencia-internet-de-las-cosas-y-5g/>

³³ Tarifica (2022), *Deutsche Telekom Introduces Global IoT Connectivity Service*. Disponible en: <https://1b3a08-1e392.icpage.net/tarificastoryoftheweek-23022022article1?slid=75536232&sKey=AXIH&mId=950186>

³⁴ GlobalData (2022), *Global Industrial IoT Services: Competitive Landscape Assessment*. Pág. (2-3). Disponible en: <https://technology.globaldata.com/Analysis/CADetails/Global-Industrial-IoT-Services-Competitive-Landscape-Assessment103024>

2.

Acciones regulatorias para Internet de las Cosas (IoT).

Dentro de las principales conclusiones del análisis exploratorio de datos del IoT elaborado por el IFT en 2020, se identificó la importancia de implementar acciones regulatorias que impulsaran el desarrollo del IoT y la difusión de sus beneficios, así como la importancia de la estandarización y homologación que permita la interoperabilidad, las economías de escala y una mejor seguridad y privacidad de los datos. Adicionalmente, el estudio previo destaca la relevancia de la promoción del desarrollo y disponibilidad de tecnologías de conectividad *ad hoc* para este tipo de servicios (v.gr. 5G, LTE-M, NB-IoT, espectro libre) y la necesidad de replicar experiencias como las zonas de innovación establecidas por la *Federal Communications Commission* (FCC) de Estados Unidos.

El proceso de estandarización de normas en materia de IoT produce beneficios sustanciales para la protección del medio ambiente, la salud y los consumidores, promoviendo la competencia en el mercado, fomentando el comercio internacional y proporcionando interoperabilidad entre productos. Sin embargo, se debe cuidar que estas normas no sean excesivas a efectos de evitar dañar la competencia y crear barreras injustificadas a la entrada³⁵, a partir de cargas administrativas innecesarias.

En esta sección se presenta un análisis comparativo de las principales tendencias en 16 países, incluido México, con particular atención a las iniciativas que buscan fomentar el uso de IoT en cada economía. En este sentido, el acervo de conocimiento regulatorio de IoT que se presenta a continuación incluye iniciativas de los gobiernos centrales de cada país, así como de reguladores sectoriales, incluidos algunos reguladores del sector de Telecomunicaciones. La experiencia internacional indica, por ejemplo, que únicamente el 44% de los países analizados cuentan con algún estándar técnico en materia de IoT, que por lo general son expedidos por los gobiernos centrales de esas economías.

A nivel internacional, la *International Organization for Standardization* (ISO) y sus 165 organismos nacionales de normalización, reúnen a expertos para compartir conocimientos y desarrollar normas técnicas Internacionales voluntarias, basadas en consensos relevantes para el mercado que respaldan la innovación y brinden soluciones a los desafíos globales³⁶. A noviembre de 2022, esta organización cuenta con 45 estándares para IoT³⁷, entre los que destacan los siguientes estándares técnicos más recientes:

[ISO/IEC 30162:2022 Internet of Things \(IoT\) — Compatibility requirements and model for devices within industrial IoT systems.](#) Modelos de red para conectividad industrial de IoT y requisitos generales de compatibilidad para dispositivos y redes dentro de sistemas en términos de: a) interacción de protocolos de transmisión de datos; b) interoperabilidad y gestión de datos distribuidos; c) marco de conectividad; d) conectividad; entre otros.

³⁵ OECD (2018), *Es importante tener un proceso de normalización que respete las mejores prácticas regulatorias, evaluando los efectos de las Normas Oficiales Mexicanas (NOMs) y Normas Mexicanas (NMXs) en la competencia, afirma la OCDE*. Disponible en: <https://www.oecd.org/centrodemexico/medios/esimportantetenerunprocesodenormalizacionquerespetelasmejorespracticaregulatoriasenmexico.htm>

³⁶ ISO (2021), *About Us*, Disponible en: <https://www.iso.org/about-us.html>

³⁷ Para más información visite: https://www.iso.org/search.html?q=Internet%20of%20Things&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard

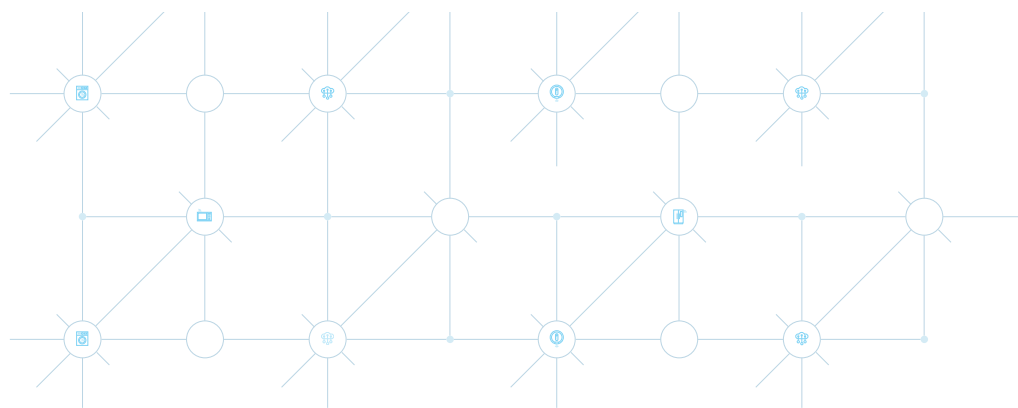
ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines. Este documento proporciona pautas sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de Internet de las cosas (IoT).

ISO/IEC TR 22417:2017 Information technology — Internet of things (IoT) use cases. Este informe técnico identifica escenarios de IoT y casos de uso basados en aplicaciones y requisitos del mundo real. Los casos de uso proporcionan un contexto práctico para las consideraciones sobre interoperabilidad y estándares basados en la experiencia del usuario. También aclaran dónde se pueden aplicar las normas existentes y destacan dónde se necesita trabajo de estandarización.

Como se mencionó en la primera fase del análisis del ecosistema de IoT a nivel mundial, la industria de las tecnologías de la información y las comunicaciones (TIC) se caracteriza por tener diversos componentes que se estructuran como elementos de red (*hardware*, *software* de sistemas operativos, *software* de aplicaciones, administradores de bases de datos, conexiones de redes LAN y WAN, *etc.*), generando ventajas en la compartición de recursos, el intercambio de información y la homogeneización de las aplicaciones. En este sentido, la complementariedad se establece a través de estándares técnicos adoptados por la industria, garantizando en ocasiones la interoperabilidad de los diversos sensores y dispositivos que conforman el ecosistema, generando externalidades positivas para los agentes del mercado, en la producción, comercialización, distribución y consumo de los bienes finales³⁸.

GSMA también reconoce la importancia de la adopción de estándares técnicos, así como modelos de datos compartidos y protocolos de comunicación industrial abiertos para garantizar la interoperabilidad³⁹, lo que permitiría aprovechar las economías de escala que puedan surgir de las soluciones de IoT, así como de una reducción del costo de transacción⁴⁰ que puede surgir durante el desarrollo de las soluciones IoT.

A continuación, se presentan las acciones regulatorias e iniciativas que han venido desarrollando algunos países para efectos de desarrollar el ecosistema IoT en sus economías.



³⁸ IFT (2020), *Análisis Exploratorio de la Comercialización de Servicios de Conectividad para IoT*. Página (55). Disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/analisisexploratorioiot.pdf>

³⁹ GSMA (2021), *The Mobile Economy*. Pág. (33). Disponible en: <https://data.gsmainelligence.com/api-web/v2/research-file-download?id=60621126&file=250621-Mobile-Economy-2021.pdf>

⁴⁰ Swann, P. (2010). *The Economics of Standardization: An Update*. Pág. (12). Disponible en: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.618.5922&rep=rep1&type=pdf>

Arabia Saudita

Communications and Information Technology Commission (CITC)

Regulador de Telecomunicaciones y las Tecnologías de la Información (TI)

La CITC tiene el mandato de regular en el sector de las Telecomunicaciones y las Tecnologías de la Información (TI) en el Reino de Arabia Saudita, en el que se incluye el suministro de servicios de IoT con la visión de convertir a Arabia Saudita en un país líder en el desarrollo de estos servicios. En virtud de lo anterior, la CITC publicó el marco regulatorio de los servicios IoT en 2019⁴¹.

El marco regulatorio de IoT en ese país establece que estos servicios pueden proporcionarse mediante redes cableadas e inalámbricas y, en función del medio de transmisión se pueden clasificar en:

- | Servicios de IoT prestados a través de redes móviles;
- | Servicios de IoT proporcionados a través de redes fijas, y
- | Servicios de IoT prestados utilizando frecuencias exentas de licencia⁴²

Adicionalmente, la Norma Técnica CITC RI114⁴³ incluye todas las bandas de frecuencia que se pueden utilizar para redes de área amplia de baja potencia (LPWAN) exentas de licencia⁴⁴.

Además de las regulaciones anteriores, los proveedores de servicios de IoT deben cumplir con las siguientes obligaciones⁴⁵:

Informar a los usuarios finales sobre:

- La importancia de la seguridad de la red y los datos, así como recomendaciones para proteger su información.
- Cómo utilizar de forma eficaz las redes y soluciones de IoT, explicando las características y la calidad de servicio de cada tecnología.
- El riesgo de interferencia de otros usuarios de bandas compartidas, con un posible efecto perjudicial sobre la calidad del servicio.

Mantener dentro de Arabia Saudita todos los componentes de la red de IoT, los dispositivos y el *host* de los datos.

⁴¹ CITC (2019), *Internet of Things (IoT) Regulatory Framework*. Pág. (3). Disponible: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

⁴² CITC (2019), *Internet of Things (IoT) Regulatory Framework*. Pág. (5). Disponible: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

⁴³ Para más información visite: <https://www.citc.gov.sa/ar/RulesandSystems/RegulatoryDocuments/EquipmentApproval/Documents/TA%20E%20RI114.pdf>

⁴⁴ CITC (2019), *Internet of Things (IoT) Regulatory Framework*. Pág. (6). Disponible: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

⁴⁵ CITC (2019), *Internet of Things (IoT) Regulatory Framework*. Pág. (8-9). Disponible: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

- | Cumplir con las regulaciones de redes de área local inalámbricas (WLAN / WiFi).
- | Proporcionar al CITC informes periódicos que incluyan cualquier información y datos relacionados con los servicios prestados.
- | Cumplir con todas las regulaciones de la CITC.

En marzo de 2022, el CITC realizó una consulta pública respecto a las regulaciones propuestas para IoT del documento publicado en 2019, lo anterior con el fin de que la CITC pueda contar con más insumos para cumplir con su rol de regular y habilitar las tecnologías emergentes dentro de las TIC en el Reino de Arabia Saudita⁴⁶.

La disposición que está siendo discutida en ese país incluye:

1. Las definiciones para el ecosistema de IoT en Arabia Saudita.
2. El procedimiento de acreditación de la conformidad de los dispositivos IoT.
3. La obligación de que el manual de los dispositivos debe incluir información sobre las características del dispositivo y su funcionalidad.
4. La recomendación de utilizar IPv6 que provee el beneficio de una gran capacidad de direcciones.
5. La recomendación técnica de que se asegure la interoperabilidad entre los dispositivos IoT, la conectividad para IoT y la plataforma IoT.
6. La provisión de servicios de conectividad IoT, y en este particular la posibilidad de que se utilicen redes inalámbricas para los dispositivos IoT, utilizando bandas de frecuencias concesionadas y de uso libre, estas últimas clasificadas como áreas de servicio amplio (WAN por sus siglas en inglés) y áreas de servicio local (LAN).
7. Los proveedores de conectividad IoT deberán asegurar que los usuarios de IoT son conscientes de:
 - a. La importancia de la seguridad de la red y proveer recomendaciones sobre protección de datos.
 - b. El uso efectivo, características, calidad y servicio de la conectividad IoT.
 - c. El riesgo de interferencia de otros usuarios y bandas compartidas, con posible detrimento en la calidad del servicio.
8. CITC promueve que los proveedores de soluciones IoT busquen que todas sus ofertas sean públicas.

⁴⁶ CITC (2022), *Public Consultation Document on Updating the IoT Regulations*. Disponible en: <https://istitlaa.ncc.gov.sa/en/transportation/citc/iot/Documents/The%20IoT%20Regulations.pdf>



Argentina

Secretaría de Innovación Pública

Agencia del Gobierno

La Secretaría de Innovación Pública de Argentina elaboró el Plan Nacional de Internet de las Cosas en colaboración con el sector público, privado, académico y la sociedad civil. Este plan consiste en la identificación de sectores verticales prioritarios para el desarrollo económico de Argentina, la identificación de líneas de financiamiento y la conjugación con las tareas de Investigación y Desarrollo de las Universidades, además de estrechar vínculos con el sector privado relacionado con IoT⁴⁷.

En 2021, se realizó el primer encuentro entre el sector público y privado donde se compartieron experiencias sobre el desarrollo del ecosistema IoT en Argentina y tuvo como objetivo crear un espacio de diálogo entre el sector público, el sector privado y el sector académico para el desarrollo del ecosistema IoT en ese país. Entre los asistentes se encontraba personal de la Secretaría de Innovación Pública, representantes de la Unión Internacional de Telecomunicaciones (UIT), de la Cámara Argentina de IoT, de GSMA Latin America, de la Universidad de La Plata y de la Universidad Tecnológica Nacional⁴⁸.

En una iniciativa de la Mesa Nacional de Internet de las Cosas, se publicaron los resultados de la encuesta “Relevamiento Nacional de IoT” a finales de 2021, para efectos de identificar los proyectos que se desarrollan en materia de IoT en el país. En total, se recibieron 154 respuestas, donde se muestra que el sector de IoT cuenta con una variada participación de actores como organismos públicos, empresas, universidades, escuelas secundarias, municipios y cooperativas. Dentro de los resultados se encontró que al menos 8 de cada 10 desarrollos están vinculados con la conectividad y el *software*, 70% de los proyectos está vinculado con Ciudades Inteligentes y 20% de los proyectos IoT cuenta con financiamiento del sector público⁴⁹.

Entre las principales conclusiones de este primer estudio nacional en Argentina, destacan los siguientes:

- Las respuestas obtenidas indican que el ecosistema de IoT en Argentina cuenta con una variada participación de actores: Organismos públicos, empresas, universidades, escuelas secundarias, municipios, cooperativas y organismos internacionales.
- Las zonas de Argentina en donde se detecta un mayor interés por el desarrollo de proyectos de Internet de las Cosas coinciden con las regiones del país con un mayor índice de desarrollo productivo.
- Un 30% son desarrollos experimentales, prototipos o investigaciones básicas, lo cual indica interés en el avance de IoT, por lo que el ecosistema puede ganar mayor dinamismo.

⁴⁷ Gobierno de Argentina (2021), *Mesa Nacional de IoT*. Disponible en: <https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/grupo-de-trabajo/iot>

⁴⁸ Gobierno de Argentina (2021), *Lanzamiento de la Mesa Nacional de Internet de las Cosas*. Disponible en: <https://www.argentina.gob.ar/noticias/lanzamiento-de-la-mesa-nacional-de-internet-de-las-cosas>

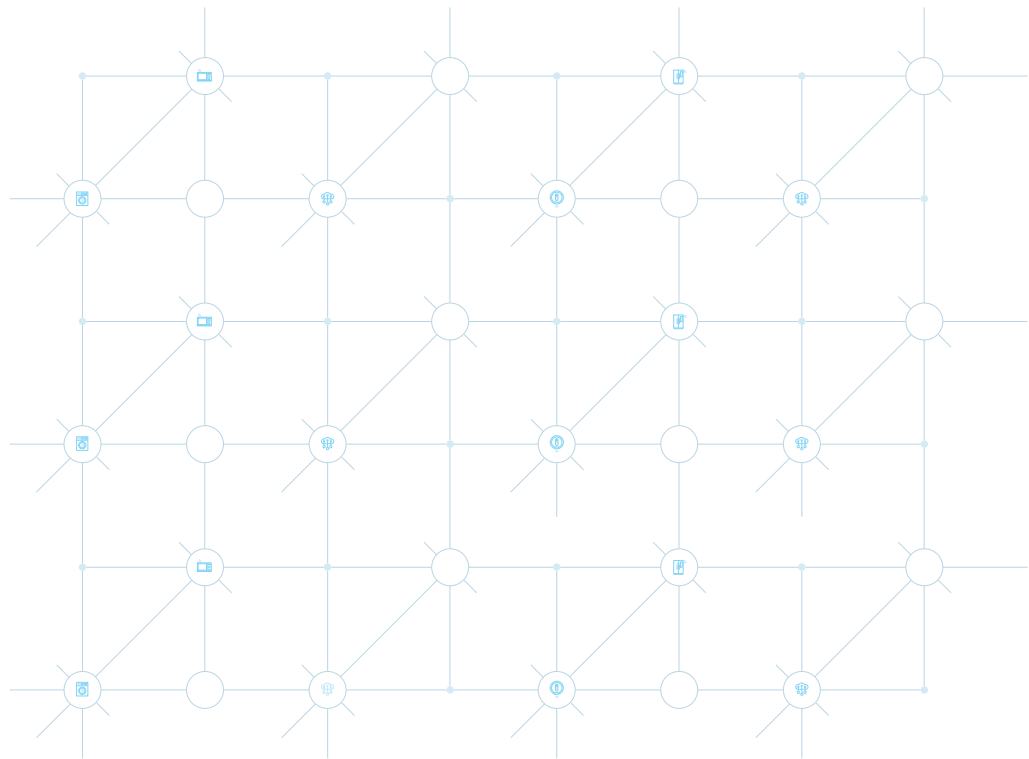
⁴⁹ Gobierno de Argentina (2021), *Se presentaron los resultados del primer relevamiento nacional de IoT*. Disponible en: <https://www.argentina.gob.ar/noticias/se-presentaron-los-resultados-del-primer-relevamiento-nacional-de-iot>

La academia y el sector público son los actores que impulsan la primera etapa de los desarrollos de IoT al tiempo que los privados son aquellos que mayor peso tienen en lo que se refiere a productos ya desarrollados.

Ciudades Inteligentes, Industria y Agro son los rubros con mayor cantidad de proyectos presentados. Estos campos de acción se relacionan con cuestiones sociales para el vivir diario de las personas (Ciudades Inteligentes) y por desarrollos productivos (Agro e Industria).

Las áreas de trabajo en las que se recibieron más respuestas fueron Ciudades Inteligentes, Industria y Agro. Los proyectos relacionados con estos tres sectores, además, tienen un grado de finalización superior al 80%.

El sector público se posicionó como el mayor aportante, financiando el 20% de los desarrollos.





Brasil

Presidencia de la República

Agencia del Gobierno

En 2019, el presidente de Brasil, Jair Messias Bolsonaro, publicó el Plan Nacional de Internet de las Cosas, con los siguientes objetivos:

1. Mejorar la calidad de vida de las personas y promover las ganancias de eficiencia en los servicios, a través de la implementación de soluciones de IoT;
2. Promover la formación profesional relacionada con el desarrollo de aplicaciones de IoT y la generación de empleo en la economía digital;
3. Aumentar la productividad y fomentar la competitividad de las empresas brasileñas que desarrollan IoT, a través de la promoción de un ecosistema de innovación en este sector;
4. Buscar alianzas con los sectores público y privado para la implementación del IoT; e
5. Incrementar la integración del país en el escenario internacional, a través de la participación en foros de estandarización, la cooperación internacional en investigación, desarrollo e innovación y la internacionalización de las soluciones IoT desarrolladas en el país.

En la producción agrícola de Brasil ya se observan casos de implementación de soluciones de Internet de las Cosas (IoT) a escala en la agricultura. De acuerdo con la experiencia brasileña, la aplicación de IoT en áreas rurales trae numerosos beneficios vinculados con el monitoreo de las condiciones climáticas y la evolución de la producción, el rendimiento de las máquinas agrícolas, así como también la supervisión detallada tanto de la salud de los cultivos como la de los animales.

No obstante, los estudios recientes en la aplicación brasileña señalan que una de las barreras que se presenta para la difusión de esta tecnología, es la carencia de conectividad en las áreas rurales remotas, aunque, la introducción de la nueva generación de tecnologías inalámbricas podría ser el catalizador para la aplicación de las soluciones IoT en áreas donde no es posible su despliegue⁵¹.

⁵¹ WIAGRO (2022), *Brasil: Avances y desafíos en la implementación de soluciones IoT para el agro*. Disponible en: <https://www.wiagro.com/brasil-avances-y-desafios-en-la-implementacion-de-soluciones-iot-para-el-agro/>

Agencia Nacional de Telecomunicaciones (ANATEL)

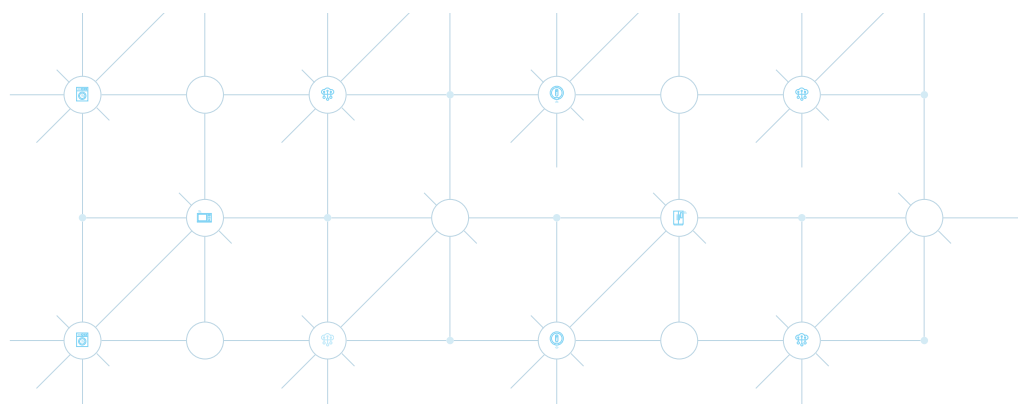
Regulador de Telecomunicaciones

ANATEL es responsable del desarrollo de las telecomunicaciones en Brasil, tiene como objetivo promover el desarrollo de las telecomunicaciones en el país a fin de dotarlo de una infraestructura de telecomunicaciones moderna y eficiente, capaz de ofrecer a la sociedad servicios adecuados, diversificados y a precios justos, en todo el territorio nacional⁵².

El Consejo Directivo de la ANATEL aprobó durante 2020 la reducción de las barreras regulatorias a la expansión de las aplicaciones de IoT y Máquina a Máquina (M2M). Con esta acción los servicios proporcionados por los dispositivos de IoT tienen una carga fiscal menor que las telecomunicaciones. El texto aprobado también modifica el Reglamento General de Portabilidad de ANATEL e impone obligaciones de portabilidad a los accesos destinados exclusivamente a la conexión de dispositivos IoT cuando se dan las condiciones técnicas necesarias.

Asimismo, ANATEL publicó una resolución sobre la regulación de IoT y M2M en relación con los operadores móviles virtuales (OMVs), donde se prevé la posibilidad de que el proveedor virtual acreditado pueda tener más de un proveedor de origen en una área de registro y acuerdos de uso de itinerancia y suministro de uso de la radio de origen⁵³.

Otra de sus principales reformas se concentra en la creación de un régimen de excepción para que a los accesos destinados exclusivamente a la conexión de dispositivos de IoT no les apliquen las obligaciones previstas en el Reglamento General de Delitos al Consumidor de Servicios de Telecomunicaciones⁵⁴.



⁵² ANATEL (2021), *Institucional*. Disponible en: <https://www.gov.br/anatel/pt-br/acao-a-informacao/institucional>

⁵³ ANATEL (2020), *Resolução nº 735, de 03 de novembro de 2020*. Disponible en: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1483-resolucao-735>

⁵⁴ Ídem, disponible en: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1483-resolucao-735>

Canadá

Standards Council of Canada (SCC)

Agencia del Gobierno

Desde 1970, el SCC se encarga de garantizar que los organismos de evaluación de la conformidad y las organizaciones de desarrollo de estándares demuestren competencia técnica, confiabilidad e integridad frente a estándares reconocidos a nivel nacional e internacional⁵⁵. Este organismo registra actualmente **20 estándares canadienses para IoT**⁵⁶, entre los que se encuentran estándares sobre la arquitectura de IoT⁵⁷, la interoperabilidad de los sistemas de IoT⁵⁸, las plataformas de intercambio de información para servicios de IoT⁵⁹, elementos básicos para construir el Internet de las Cosas de los medios (IoMT)⁶⁰, entre otros:

1. [CSA ISO/IEC 30141:19](#) Internet of Things (IoT) — Reference architecture.
2. [CSA ISO/IEC TR 30164:20](#) Internet of things (IoT) — Edge computing.
3. [CSA ISO/IEC 20924:21](#) Internet of things (IoT) — Vocabulary.
4. [CSA ISO/IEC 20924:19](#) Internet of things (IoT) — Vocabulary.
5. [CSA ISO/IEC 21823-1:19](#) Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework.
6. [CSA ISO/IEC 23093-2:20](#) Information technology — Internet of media things — Part 2: Discovery and communication API.
7. [CSA ISO/IEC 21823-2:20](#) Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability.
8. [CSA ISO/IEC 30144:21](#) Internet of things (IoT) — Wireless sensor network system supporting electrical power substation.
9. [CSA ISO/IEC 30161-1:21](#) Internet of things (IoT) — Data exchange platform for IoT services — Part 1: General requirements and architecture.
10. [CSA ISO/IEC 29341-24-1:19](#) Information technology — UPnP Device Architecture — Part 24-1: Internet gateway device control protocol — Level 2 — Internet gateway device.

⁵⁵ SCC (2020), *What we do*. Disponible en: <https://www.scc.ca/en/about-scc/what-we-do>

⁵⁶ Para más información visite: https://www.scc.ca/en/search/standardsdb/internet%20of%20things?f%5B0%5D=source_e%3ACanadian%20Standards

⁵⁷ Para más información visite: <https://www.scc.ca/en/standardsdb/standards/30079>

⁵⁸ Para más información visite: <https://www.scc.ca/en/standardsdb/standards/30059>

⁵⁹ Para más información visite: <https://www.scc.ca/en/standardsdb/standards/31171>

⁶⁰ ISO (2022) señala que el Internet de las Cosas de los Medios (IoMT) es un nuevo estándar que permite que un audio o video unirse a la fiesta como datos masivos y recursos explotables en el ambiente del IoT, para ello se requieren estándares que garanticen la sincronización y la interoperabilidad de los dispositivos y su información. Para más información visite: <https://www.iso.org/news/ref2449.html>

11. [CSA ISO/IEC 29341-24-10:19](#) Information technology — UPnP Device Architecture — Part 24-10: Internet gateway device control protocol — Level 2 — Wide area network internet protocol — Connection service.
12. [CSA ISO/IEC 29341-24-11:19](#) Information technology — UPnP Device Architecture — Part 24-11: Internet gateway device control protocol — Level 2 — Wide area network internet protocol v6 — Firewall control service.
13. [CSA ISO/IEC 14496-33:20](#) Information technology — Coding of audio-visual objects — Part 33: Internet video coding.
14. [CAN/CSA-ISO/IEC 14766-01 \(R2010\)](#) Information Technology - Telecommunications and Information Exchange Between Systems - Use of OSI Applications Over the Internet Transmission Control Protocol (TCP).
15. [CSA ISO/IEC 29341-24-2:19](#) Information technology — UPnP Device Architecture — Part 24-2: Internet gateway device control protocol — Level 2 — Wide area network connection device.
16. [CSA ISO/IEC 29341-24-3:19](#) Information technology — UPnP Device Architecture — Part 24-3: Internet gateway device control protocol — Level 2 — Wide area network device.
17. [CAN/CSA-ISO/IEC TR 18016:04 \(R2014\)](#) Information Technology - Message Handling Systems (MHS) - Interworking with Internet E-mail.
18. [CAN/CSA-ISO/IEC 19500-2:04 \(R2009\)](#) Information Technology - Open Distributed Processing - Part 2: General Inter-ORB Protocol (GIOP)/Internet Inter-ORB Protocol (IIOP).
19. [CAN/CSA-ISO/IEC 18036:04 \(R2014\)](#) Information Technology - Icon Symbols and Functions for World Wide Web Browser Toolbars.
20. [CAN/CSA-ISO/IEC TR 21890:04 \(R2017\)](#) Information Technology - Telecommunications and Information Exchange Between Systems - Interoperation of PISNs with IP Networks.

Canadian Radio-television and Telecommunications Commissions (CRTC)

Regulador de Telecomunicaciones

La CRTC regula y supervisa la radiodifusión y las telecomunicaciones de interés público⁶¹. Dentro de su actuar, la Comisión establece una exención de la obligación de registro de revendedor en los casos en que los servicios de telecomunicaciones ofrecidos y prestados por un revendedor cumplan al menos uno de los siguientes criterios: (i) El servicio se ofrece sin un cargo explícito, (ii) el servicio se ofrece de forma temporal solo a las personas ubicadas en las instalaciones del revendedor, o (iii) el servicio no permite a las personas participar de forma autónoma en telecomunicaciones de voz bidireccionales o acceder a Internet de forma autónoma.

⁶¹ CRTC (2021), *About us*. Disponible en: <https://crtc.gc.ca/eng/acrtc/org.htm>

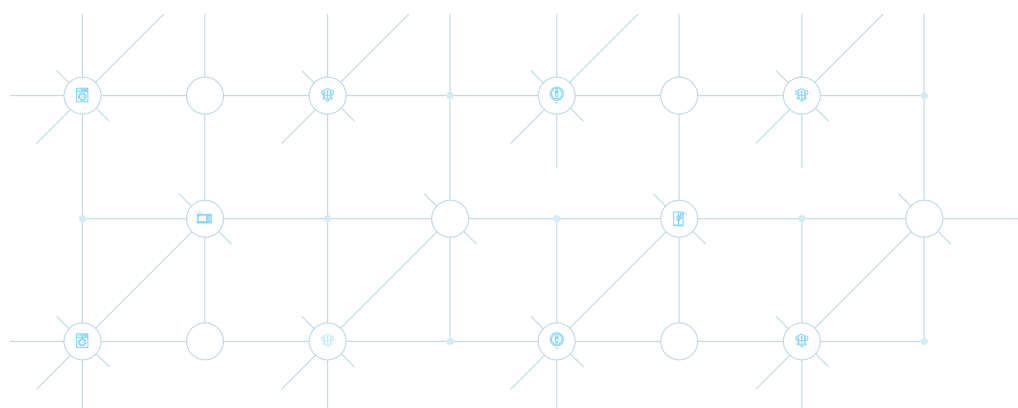
Si bien, la regulación descrita evita cargas administrativas innecesarias para los operadores y los revendedores, la CTRC considera como excepción a varias entidades para el registro de revendedor, como las comunicaciones en hoteles/moteles, cafeterías, centros comerciales y aeropuertos, donde también se puede incluir a proveedores de servicios IoT y a los servicios máquina a máquina (M2M)⁶².

Office of the Privacy Commissioner of Canada (OPC)

Agencia del Gobierno

La OPC establecida en 1983 en términos de la Ley de Privacidad, rige las prácticas de manejo de información personal de los departamentos y agencias federales. En 2001, las funciones de la OPC se ampliaron para incluir empresas del sector privado sujetas a la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) y a la Ley federal de privacidad del sector privado de Canadá⁶³.

Para el ecosistema IoT, la OPC emitió la “*Privacy guidance for manufacturers of Internet of Things devices*” en 2020. Esta disposición establece que los fabricantes de dispositivos de IoT tienen la responsabilidad de que la información personal sea tratada bajo la legislación canadiense sobre privacidad. En esta guía, se incluye a los dispositivos con sensores integrados que recopilan información personal, como luces, timbres, cerraduras, detectores de humo, alarmas, televisores, cámaras, parlantes, electrodomésticos, automóviles conectados, juguetes, ropa, relojes o rastreadores de salud⁶⁴.



⁶¹ CTRC (2019), *Telecom Regulatory Policy CRTC 2019-354*. Disponible en: <https://crtc.gc.ca/eng/archive/2019/2019-354.htm>

⁶² OPC (2018), *Who we are*. Disponible en: <https://www.priv.gc.ca/en/about-the-opc/who-we-are/>

⁶³ OPC (2020), *Privacy guidance for manufacturers of Internet of Things devices*. Disponible en: <https://www.priv.gc.ca/en/privacy-topics/technology/gd-iot-man/>

China

General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ)

Agencia del Gobierno

Este país inició sus esfuerzos regulatorios a partir del plan denominado *China Standards 2025*, un enfoque estratégico que parte de la colaboración del gobierno de China y las principales empresas de tecnología para establecer estándares globales de tecnologías emergentes como Internet 5G, IoT e inteligencia artificial, en coordinación con la política industrial de ese país. Para la construcción de este plan, en 2018 la Administración General de Supervisión de Calidad, Inspección y Cuarentena (AQSIQ) encargó un proyecto de investigación a la Academia China de Ingeniería, el cual tenía un plazo de dos años para concluirse, aunque el informe completo aún no se ha publicado⁶⁵.

Seconded European Standardization Expert for China (SESEC)

Proyecto o iniciativa internacional

El SESEC tiene sus inicios en 2006 como una iniciativa para dar a conocer dentro de China el Sistema Europeo de Normalización. Iniciativa operada por el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI), así como por la Dirección General de Normas Internas de Mercado, Industria, Emprendimiento e Industria de la Comisión Europea (EC DG GROW) y por la Asociación Europea de Libre Comercio (EFTA)⁶⁶.

Esta iniciativa ha logrado mayor cooperación entre los organismos de normalización europeos y chinos y proporciona ayuda continua a la industria europea en relación con la normalización técnica dentro del mercado chino⁶⁷.

Actualmente, el SESEC cuenta con una propuesta de estandarización técnica sobre IoT en tiempo real, esta tecnología se aplica a sistemas como Internet industrial, fabricación inteligente, automóviles autónomos, entre otros. Estos esfuerzos de estandarización son desarrollados conjuntamente por la Universidad de Tongji y el Instituto de Normalización de Electrónica de China (CESI).

En el marco de esta iniciativa, **China ha propuesto los siguientes 11 estándares internacionales de IoT⁶⁸ en 2021:**

⁶⁵ China Briefing (2020), *What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?*. Disponible en: <https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/>

⁶⁶ SESEC (2021), *SESEC Background*. Disponible en: <https://sesec.eu/sesec/>

⁶⁷ CENELEC (2021), *Seconded European Standardization Expert for China (SESEC)*. Disponible en: [https://www.cenelec.eu/intcoop/projects/visibility/SESEC/Pages/default.aspx#:~:text=The%20Seconded%20European%20Standardization%20Expert,and%20ETSI%20\(the%20ESOs\).](https://www.cenelec.eu/intcoop/projects/visibility/SESEC/Pages/default.aspx#:~:text=The%20Seconded%20European%20Standardization%20Expert,and%20ETSI%20(the%20ESOs).)

⁶⁸ SESEC (2019), *ISO/IEC approved China's standards Proposal on IoT*. Disponible en: <https://sesec.eu/2019/others/iso-iec-approved-chinas-standards-proposal-on-iot/>

Código del estándar	Nombre
ISO/IEC 29182-2:2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA)
ISO/IEC 29182-5:2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 5: Interface definitions
ISO/IEC 20005:2013	Information technology — Sensor networks — Services and interfaces supporting collaborative information processing in intelligent sensor networks
ISO/IEC 19637:2016	Information technology — Sensor network testing framework
ISO/IEC 30141:2018	Internet of Things (IoT) — Reference Architecture
ISO/IEC 21823-2	Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability
ISO/IEC 30144	Information technology — Sensor network system architecture for power substations
ISO/IEC TR 30148	Internet of Things (IoT) — Technical requirements and application of sensor network for wireless gas meters.
ISO/IEC 30163	Internet of Things (IoT) — System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services
ISO/IEC TR 30164	Internet of things (IoT) — Edge computing
ISO/IEC 30165	Internet of Things (IoT) — Real-time IoT framework

Fuente: IFT con información de SESEC (2019), *ISO/IEC approved China's standards Proposal on IoT*. Disponible en: <https://sesec.eu/2019/others/iso-iec-approved-chinas-standards-proposal-on-iot/>

Ministry of Industry and Information Technology (MIIT)

Regulador de Telecomunicaciones

El MIIT, junto con ocho ministerios más, emitieron el “Plan de Acción de Tres Años para la Construcción de Nueva Infraestructura (2021-2023)”. En dicho plan, se especifica que, para fines de 2023, la nueva infraestructura para IoT se construirá inicialmente en las principales ciudades de China, lo que será la base de la gobernanza y de la modernización social, la transformación digital industrial y la mejora tecnológica para el consumo de las personas.

A partir de esta iniciativa, el gobierno chino busca crear una serie de entidades para la construcción y operación del ecosistema IoT que permita generar operaciones y servicios replicables, escalables y sostenibles, con aplicaciones industriales y beneficios significativos, así como crear un conjunto de estándares de IoT y sistemas de seguridad⁶⁹.

En 2020, el operador China Mobile anunció que desplegaría 118,000 estaciones base *Narrowband-IoT* (NB-IoT) y que para finales de este mismo año estas estaciones llegarían a más del doble (350,000). Por otro lado, el operador China Telecom se asoció con el operador de red IoT 1NCE para ofertar un servicio de *roaming NB-IoT*, con el fin de proporcionar los recursos de conectividad necesarios para expandir el negocio de las empresas chinas de IoT en todo el mundo. Complementariamente, también se formalizó una alianza con Nokia para el uso de la Red mundial de redes de IoT (WING)⁷⁰, lo que permitiría ofrecer una gestión de conectividad unificada para sus clientes comerciales internacionales⁷¹.

⁶⁹ Office of Central Cyberspace Affairs Commission (2021), *Ocho departamentos, incluido el Ministerio de Industria y Tecnología de la Información, emitieron el “Plan de acción de tres años para la construcción de una nueva infraestructura de Internet de las Cosas (2021-2023)”*. Disponible en: http://www.cac.gov.cn/2021-09/29/c_1634507925423247.htm

⁷⁰ La Worldwide IoT Network Grid (WING) de Nokia ofrece una conectividad global de IoT para todos los consumidores industriales, evitando múltiples acuerdos de *roaming* en muchos mercados, además ofrece conectividad y segura con baja latencia y alto ancho de banda, rápido de configurar e integrar con los sistemas existentes, y ofrece soporte para expandir las operaciones negocio a negocio (B2B). Para más detalle, visite: <https://www.nokia.com/networks/internet-of-things/wing/>

⁷¹ GSMA (2021), *The Mobile Economy China 2021*. Pág. (24). Disponible en: https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/02/GSMA_MobileEconomy2021_China_Eng-1.pdf

Colombia

Comisión de Regulación de Telecomunicaciones (CRC)

Regulador de Telecomunicaciones

En 2016, el regulador colombiano de las telecomunicaciones inició sus esfuerzos por desarrollar el ecosistema del IoT. Una de sus primeras acciones fue el inicio de un proceso consultivo para la “Revisión del marco regulatorio para la Provisión de Contenidos y Aplicaciones (PCA) y condiciones normativas para la adopción del Internet de las Cosas (IoT)”⁷². El objetivo de esta revisión era estimular el mercado de IoT en el país, donde se fomente la libre competencia y la inversión, contando con reglas de juego claras que equilibren constantemente los diferentes tipos de control y los intereses de las partes que intervienen en su cadena de valor.

En dicho documento se identificaron aspectos regulatorios y normativos requeridos para promover la provisión y uso de contenidos y aplicaciones en Colombia, con especial énfasis en aquellas relativas a la promoción y adopción del Internet de las Cosas (IoT). Entre las acciones regulatorias inmediatas, CRC identifica:

Planes de datos masivos para IoT. Observaron planes de conectividad únicamente para empresas grandes o medianas (planes corporativos) sin ofertas masivas de IoT para pequeñas empresas en el corto o mediano plazo.

Un reglamento para redes internas de telecomunicaciones donde se promueva el Hogar Digital e Inteligente, a través de la armonización de las condiciones para el ingreso de sensores requeridos, disminuyendo costos de importación en la medida que se genere un mercado atractivo, el reglamento también se espera que promueva las redes de banda ancha al hogar⁷³.

Fomentar la homologación de equipos de IoT que incluyan el uso de radio frecuencias para verificar que, efectivamente están emitiendo señales dentro de las radiofrecuencias autorizadas. De acuerdo con el estudio, la homologación no debe implicar mayores costos para el proveedor, para evitar el incremento en los precios del usuario final⁷⁴.

⁷² Para más información, visite: https://www.crcm.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20an%C3%A1lisis%20consultor%C3%ADa%20-%20Proyecto%20Revisi%C3%B3n%20del%20marco%20regulatorio%20para%20la%20provisi%C3%B3n%20de%20Contenidos%20y%20Aplicaciones%20%28PCA%29%20y%20condiciones%20normativas%20para%20la%20adopci%C3%B3n%20del%20Internet%20de%20las%20Cosas%20%28IoT%29/informe_6_pca_iot.pdf

⁷³ CRC (2016), *Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las cosas*. Pág. (63). Disponible en: https://www.crcm.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20an%C3%A1lisis%20consultor%C3%ADa%20-%20Proyecto%20Revisi%C3%B3n%20del%20marco%20regulatorio%20para%20la%20provisi%C3%B3n%20de%20Contenidos%20y%20Aplicaciones%20%28PCA%29%20y%20condiciones%20normativas%20para%20la%20adopci%C3%B3n%20del%20Internet%20de%20las%20Cosas%20%28IoT%29/informe_6_pca_iot.pdf

⁷⁴ CRC (2016), *Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las cosas*. Pág. (59). Disponible en: https://www.crcm.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20an%C3%A1lisis%20consultor%C3%ADa%20-%20Proyecto%20Revisi%C3%B3n%20del%20marco%20regulatorio%20para%20la%20provisi%C3%B3n%20de%20Contenidos%20y%20Aplicaciones%20%28PCA%29%20y%20condiciones%20normativas%20para%20la%20adopci%C3%B3n%20del%20Internet%20de%20las%20Cosas%20%28IoT%29/informe_6_pca_iot.pdf

La numeración debe ser interoperable en el ámbito nacional e internacional y sujeta a las obligaciones de portabilidad⁷⁵.

La posibilidad de masificar los servicios IoT con planes que contengan los siguientes conceptos y servicios⁷⁶:

Concepto	Servicios
Emplazamientos sin comunicación con cable	• Puestos de control remoto en selvas o sitios alejados • Acceso a edificios lejanos • Estaciones en playas • Puestos de control de condiciones medioambientales
Vigilancia de elementos de valor	• Localización de personas • Localización de mascotas • Localización de elementos de valor: joyas, bicicletas, bolsas de golf
Hogar digital	• Videovigilancia • Alarmas • Ascensores • Contadores inteligentes • Cuidado de personas • Neveras
Control Industrial	• Monitorización de frigoríficos • Control de acceso • Optimización del uso de la energía
Gestión de vehículos	• Control logístico • Camiones, autos • Vehículos alquilados • Taxi • Navegador GPS • Gestión del tráfico
Comercio	• Máquinas de vending • TPV móvil: pagos electrónicos

En este estudio, también se sugieren acciones específicas como la adopción por parte de los servicios públicos de sensores que optimicen su operación. Por ejemplo, expedir normas para promover el desarrollo y uso del IoT en Colombia para la implementación de dispositivos en los vehículos de transporte público para llamadas de emergencia (eCall) en accidentes de tráfico⁷⁷.

⁷⁵ CRC (2016), *Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las cosas*. Pág. (55). Disponible en: https://www.crcm.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20an%C3%A1lisis%20consultor%C3%ADa%20-%20Proyecto%20Revisi%C3%B3n%20del%20marco%20regulatorio%20para%20la%20provisi%C3%B3n%20de%20Contenidos%20y%20Aplicaciones%20%28PCA%29%20y%20condiciones%20normativas%20para%20la%20adopci%C3%B3n%20del%20Internet%20de%20las%20Cosas%20%28IoT%29/informe_6_pca_iot.pdf

⁷⁶ Ibídem. Pág. (57-58).

⁷⁷ Ibídem. Pág. (66).

En este aspecto, Colombia concluye que se requiere de una regulación concreta para IoT, más allá de la expedición de normas indirectas que promuevan su desarrollo, por ejemplo, normas para implementar edificios inteligentes, hogares digitales, el pago electrónico de servicios de *retail*, etc.⁷⁸.

Como resultado de este ejercicio de regulación colaborativa, la CRC ha venido emitiendo disposiciones relevantes para estimular el mercado de IoT en ese país:

La modernización de las redes en Colombia es uno de los elementos identificados en la Agenda Regulatoria 2019 – 2020, publicada el 21 de marzo de 2019, donde la CRC propone apagar las redes 2G o concentrar su aprovechamiento en tecnologías como IoT y M2M⁷⁹.

El 17 de abril de 2020, la CRC publicó el esquema de administración de recursos de identificación para los servicios de movilidad de los operadores de telecomunicaciones y se asigna el rango de numeración del 910-919 para los servicios de movilidad (M2M y IoT)⁸⁰.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

Agencia del Gobierno

En 2019, MinTIC junto con Telefónica Movistar, el hub de innovación de Wayra, las iniciativas del gobierno colombiano CEemprende e iNNpulsa y el Ministerio de Comercio, Industria y Turismo implementaron el primer Laboratorio de Internet de las Cosas (IoT)⁸¹, su objetivo es brindar a los diferentes actores del ecosistema emprendedor colombiano un ambiente propicio para desarrollar aplicaciones y herramientas con base en tecnología IoT.

En este laboratorio se crean ambientes operativos para las conectividades LPWA (*Low Power Wide Area*), junto a Narrowband-IoT/LTE, chips SIM con perfil NB-IoT/LTE-M, chipset que soportan tecnología LTE para IoT, módulos de comunicaciones que permitirán realizar interacciones a través de NB-IoT/LTE-M, kit de desarrollo de *software* y *hardware* basados en NB-IoT/LTE-M y una mesa de trabajo para desarrolladores y emprendedores.

⁷⁸ CRC (2016), *Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las cosas*. Página (9). Disponible en: https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20an%C3%A1lisis%20consultor%C3%ADa%20-%20Proyecto%20Revisi%C3%B3n%20del%20marco%20regulatorio%20para%20la%20provisi%C3%B3n%20de%20Contenidos%20y%20Aplicaciones%20%28PCA%29%20y%20condiciones%20normativas%20para%20la%20adopci%C3%B3n%20del%20Internet%20de%20las%20Cosas%20%28IoT%29/informe_6_pca_iiot.pdf

⁷⁹ Para más información sobre esta iniciativa, consulte: <https://signalsiot.com/gobierno-de-colombia-definira-futuro-de-redes-2g-apagon-o-uso-m2m/>

⁸⁰ MinTIC (2020), *Resolución 5968 de 2020*. Disponible en: https://normograma.mintic.gov.co/docs/resolucion_crc_5968_2020.htm

⁸¹ MinTIC (2019), *Primer Laboratorio de Internet de las Cosas (IoT LAB) para emprendedores abre sus puertas en Colombia*. Disponible en: <https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/106960:Primer-Laboratorio-de-Internet-de-las-Cosas-IoT-LAB-para-emprendedores-abre-sus-puertas-en-Colombia>

Corea del Sur

Ministry of Science and ICT (MSIT)

Agencia del Gobierno

El MSIT es el organismo encargado de establecer, coordinar, y evaluar las políticas de ciencia y tecnología para la cuarta revolución industrial, esto a través del *New Deal Digital*, plan que establece las bases para el crecimiento de las plataformas en línea y los medios digitales⁸².

En el tema de IoT, en 2014 el MSIT publicó el “*Master Plan for Building the Internet of Things (IoT)*”, cuyo objetivo buscaba que Corea del Sur se convirtiera en uno de los países líderes en el mundo donde los ciudadanos, las empresas y el gobierno estuvieran desarrollando y utilizando activamente los servicios de IoT. Este plan tiene tareas enfocadas al desarrollo de IoT mediante las siguientes actividades:

- 1) Establecer y expandir el mercado de servicios creativos de IoT;
- 2) Fomentar empresas globales especializadas en IoT, y
- 3) Establecer una infraestructura para el desarrollo seguro y dinámico de IoT⁸³.

El MSIT, cuenta con la *National Radio Research Agency* (RRA) un organismo dependiente, cuya función es realizar investigaciones en torno a los recursos y entornos para las ondas de radio, sobre certificación de calidad y criterios técnicos con respecto a los equipos de radiodifusión y comunicaciones⁸⁴.

En 2020, se realizó la primera reunión general de las TIC del Comité Técnico Conjunto de la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC) (JTC 1), del subcomité de normalización de IoT (SC 41). En esta reunión, se discutieron los problemas de estandarización que se abordarían en la SC 41; en particular, los *wearables* y el IoT industrial⁸⁵.

⁸² Para más información visite: <https://www.msit.go.kr/contents/cont.do?sCode=user&mPid=131&mld=198>

⁸³ Ministry of Science and ICT (2014), *Master Plan for Building the Internet of Things (IoT)*. Disponible en: <https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf>

⁸⁴ RRA (2018), *RRA Introduction*. Disponible en: <https://rra.go.kr/en/intro/object.do>

⁸⁵ Ministry of Science and ICT (2020), *Global IoT Standardization Meeting Held > (May 30) - Korea hosts kick-off general meeting of ICT standardization group*. Disponible en: https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&mld=4&mPid=2&pageIndex=1&bbsSeqNo=42&nttSeqNo=254&searchOpt=NTT_SJ&searchTxt=iot



Emiratos Árabes Unidos

Telecommunications and Digital Government Regulatory Authority (TDRA)

Regulador de Telecomunicaciones

La TDRA de los Emiratos Árabes Unidos fue establecida en 2003 bajo la Ley de Telecomunicaciones que regula el sector⁸⁶, entre sus funciones tiene el objetivo de regular los servicios de IoT dentro de los Emiratos Árabes Unidos para **desarrollar un ecosistema coordinado, coherente, seguro y protegido** donde se hacen cumplir ciertos requisitos para proporcionar servicios de IoT⁸⁷.

La TDRA emitió el documento de regulación sobre IoT llamado “*Regulatory Policy Internet of Things*” el 28 de marzo de 2018, en el que se menciona que la Autoridad tiene la intención de permitir que el servicio de IoT se desarrolle de manera coordinada, coherente, segura y protegida, en la cual los ministerios y reguladores de industrias específicas pueden desarrollar sus propias directrices específicas adicionales de IoT en coordinación y consulta con el Comité Asesor de IoT de la TDRA⁸⁸.

En este sentido, la TDRA puede emitir instrumentos regulatorios adicionales, incluidos reglamentos, directivas y/o pautas, según se considere necesario, que brinden incentivos y apoyo para el desarrollo del ecosistema de IoT dentro del país⁸⁹. El enfoque de los Emiratos Árabes se basa en los siguientes principios:

- La política de desarrollo del entorno de IoT está alineado con los objetivos del sector de telecomunicaciones.
- El diseño de esta política considera el punto de vista de los múltiples grupos interesados.
- Mientras que esta política cubre los requerimientos clave para la implementación de IoT, el órgano regulador provee requerimientos específicos para los servicios IoT de misión crítica, que requieren altos niveles de seguridad.

No obstante, en el marco regulatorio creado al momento de publicación de este reporte no se identifica un estándar emitido por las autoridades del país para IoT.

⁸⁶ TDRA (2020), *About TDRA | Vision, Mission & Values*. Disponible en: <https://www.tra.gov.ae/en/about-tra/about-tra-vision-mission-and-values.aspx>

⁸⁷ TDRA (2020), *Internet of Things Services Registration*. Disponible en: <https://tdra.gov.ae/en/Services/internet-of-things-services-registration>.

⁸⁸ TDRA (2016), *Regulatory Policy. Internet of Things*. Pág. (9). Disponible en: <https://www.tra.gov.ae/userfiles/assets/gRSpS8WHHaS.pdf>

⁸⁹ *Ibidem*. Pág. (10).



Estados Unidos

Congreso de Estados Unidos

Agencia del Gobierno

El Congreso de Estados Unidos de América publicó la iniciativa *H.R.1668 — 116th Congress (2019-2020)*⁹⁰, cuyo objetivo principal es establecer estándares mínimos de seguridad para dispositivos de IoT que sean propiedad o estén controlados por el gobierno federal.

Esta iniciativa busca asegurar el más alto nivel de ciberseguridad en las agencias del poder ejecutivo, trabajando en colaboración dentro y entre agencias, la industria y la academia, de conformidad con el informe interno *“Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline”*⁹¹ de la *National Telecommunications and Information Administration* (NTIA), publicado en mayo de 2020.

Esta disposición parte del hecho de que los fabricantes están produciendo una gran cantidad de variedades de dispositivos, muchos de estos dispositivos de IoT no se adaptan a las definiciones estándar de los dispositivos de tecnología de la información (TI) que se han usado como base para definir las capacidades de ciberseguridad de dispositivo (por ejemplo, teléfonos inteligentes, servidores, computadoras portátiles). Los dispositivos de IoT tienen al menos un transductor (sensor o actuador) para interactuar directamente con el mundo físico, y al menos una interfaz de red (por ejemplo, Ethernet, Wi-Fi, Bluetooth, LTE, Zigbee, banda ultra ancha-UWB) que los conecta con el mundo digital. Adicionalmente, los dispositivos de IoT pueden funcionar por sí solos o depender de otros dispositivos específicos (por ejemplo, un concentrador de IoT) o sistemas (por ejemplo, una nube) para algunas funcionalidades.

El objetivo de esta disposición es ofrecer a los fabricantes recomendaciones para mejorar los dispositivos de IoT que fabrican haciéndolos más protegibles. Esto se refiere a las capacidades de ciberseguridad (las características o funciones de ciberseguridad que los dispositivos proporcionan por sus propios medios técnicos, es decir, el *hardware* y el *software* del dispositivo) que ofrecen los dispositivos de IoT y que los clientes, sean organizaciones o personas, necesitan para protegerlos cuando los usan en sus sistemas y entornos.

Entre las actividades recomendadas para el fabricante de dispositivos se encuentran:

- | Definir formas de comunicarse con los clientes;
- | Decidir lo que se comunicará a los clientes y la manera de hacerlo;
- | Expectativas de soporte técnico y vida útil;
- | Composición y capacidades del dispositivo;
- | Actualizaciones de *software*, y
- | Opciones de retirada de dispositivos.

⁹⁰ Congress.Gov (2020), *H.R.1668 - IoT Cybersecurity Improvement Act of 2020*. Disponible en: <https://www.congress.gov/bills/116th-congress/house-bill/1668/text#:~:text=To%20establish%20minimum%20security%20standards,Government%2C%20and%20for%20other%20purposes.&text=This%20Act%20may%20be%20cited,Cybersecurity%20Improvement%20Act%20of%202020%E2%80%9D>.

⁹¹ Versión más reciente del documento disponible en: <https://csrc.nist.gov/publications/detail/nistir/8259/final>

U.S. Department of Commerce

Agencia del Gobierno

El Departamento de Comercio, es el organismo encargado de la creación de empleo y el crecimiento económico⁹², el cual cuenta con un plan estratégico llamado “*U.S. Department of Commerce’s 2018–2022 Strategic Plan*”, dentro del cual, se plantea el objetivo estratégico de “Fortalecer el comercio interno y la Base Industrial de Estados Unidos”, a través de la estrategia particular de “**Generar confianza en el comercio digital mediante sólidos estándares de cifrado**”, buscando un cifrado robusto con el desarrollo de estándares criptográficos del *National Institute of Standards and Technology (NIST)*, incluidos los estándares para el “Internet de las cosas”, dispositivos livianos y entornos de computación cuántica⁹³.

Dentro del *U.S. Department of Commerce* se han realizado diferentes acciones encaminadas al uso, promoción y estandarización del IoT, a continuación, se enumerarán algunas acciones que se han llevado a cabo por las distintas agencias que conforman dicho organismo.

La *National Telecommunications and Information Administration (NTIA)* forma parte del Departamento de Comercio y es responsable por ley de asesorar al presidente de Estados Unidos en temas de políticas de telecomunicaciones e información. Si bien, los programas y la formulación de políticas de la NTIA se centran en el acceso y la adopción de Internet de banda ancha, ampliar el uso del espectro por parte de todos los usuarios y garantizar que Internet siga siendo un motor para la innovación y el crecimiento económico continuos⁹⁴, cuenta con un grupo de trabajo de políticas de Internet, el cual ha analizado los beneficios, desafíos y roles potenciales del gobierno en la promoción del avance en IoT.

En 2016, la NTIA llevo a cabo una investigación sobre Internet de las cosas (IoT) para revisar el panorama tecnológico y político para su desarrollo. Una vez concluida esta investigación, el organismo buscó la opinión de las partes interesadas, incluida la industria privada, los investigadores, el mundo académico y la sociedad civil, sobre los posibles beneficios y desafíos de estas tecnologías y el papel del gobierno estadounidense en este tema. Como resultado de este ejercicio, la NTIA publicó el “libro verde” que identifica los problemas clave que afectan el despliegue de estas tecnologías, como el alcance de los dispositivos de IoT, la escala respecto al número de dispositivos conectados y la seguridad y ciberseguridad de los dispositivos⁹⁵, en el que se destacan los beneficios y desafíos potenciales e identifican los posibles roles del gobierno federal en la promoción del avance de las tecnologías de IoT en asociación con el sector privado⁹⁶.

⁹² U.S. Department of Commerce (2021), *About Commerce*. Disponible en: <https://www.commerce.gov/about>

⁹³ U.S. Department of Commerce (2018), *U.S. Department of Commerce Strategic Plan 2018-2022*. Pág. (13). Disponible en: https://www.commerce.gov/sites/default/files/us_department_of_commerce_2018-2022_strategic_plan.pdf

⁹⁴ NTIA (2021), *About NTIA*. Disponible en: <https://www.ntia.doc.gov/about>

⁹⁵ Para más información visite: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

⁹⁶ NTIA (2016), *Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*. Disponible en: <https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things>

Entre las áreas de trabajo necesarias para el desarrollo del ecosistema IoT se encuentran:

Habilitar la disponibilidad de infraestructura y acceso, tomando en cuenta que el IoT depende de redes de comunicación privadas y públicas, lo que incrementa:

- La demanda de espectro, y
- La demanda de infraestructura.

Adopción del protocolo IPv6.

Fomento del despliegue equitativo, tomando en cuenta que el Internet de las cosas podría exacerbar desigualdades existentes proporcionando los beneficios de la toma de decisiones basada en datos solo a algunos, y colocando a las comunidades ya desatendidas en una desventaja aún mayor.

Promoción de un compromiso coordinado de todos los grupos de interés (gobiernos, sociedad civil, academia, comunidad técnica y el sector privado).

Adopción de políticas de ciberseguridad, privacidad, propiedad intelectual, patentes, secretos industriales.

Generación de políticas de libre flujo de datos a través de las fronteras.

Promoción de mercados a través de asociaciones público privadas.

Cuantificación del sector de IoT.

Basados en estas recomendaciones, este organismo llevó a cabo un proceso de múltiples partes interesadas centrándose en la ciberseguridad de IoT y enfocándose en la transparencia de los componentes del *software*⁹⁷.

El *National Institute of Standards and Technology* (NIST), es una agencia de la administración de tecnología del Departamento de Comercio, se fundó en 1901 y es uno de los laboratorios de ciencias físicas más antiguos del país⁹⁸, este organismo cuenta con un programa para la ciberseguridad de IoT llamado "*NIST Cybersecurity for IoT*", que respalda el desarrollo y la aplicación de estándares, pautas y herramientas relacionadas para mejorar la ciberseguridad de los dispositivos conectados y los entornos en los que se implementan⁹⁹. Actualmente, se cuentan con **cuatro borradores** que brindan orientación a las agencias federales y los fabricantes de dispositivos de IoT sobre la definición de los requisitos de ciberseguridad de IoT¹⁰⁰.

⁹⁷ NTIA (2021), *NTIA Software Component Transparency*. Disponible en: <https://www.ntia.doc.gov/SoftwareTransparency>

⁹⁸ NIST (2017), *About NIST*. Disponible en: <https://www.nist.gov/about-nist>

⁹⁹ NIST (2021), *NIST Cybersecurity for IoT Program*. Disponible en: <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>

¹⁰⁰ Para más información visite: <https://csrc.nist.gov/news/2020/draft-guidance-for-defining-iot-cyber-requirements>

Dentro del NIST, se encuentra el centro de investigación *National Cybersecurity Center of Excellence* (NCCoE), donde se desarrollan algunos proyectos enfocados en IoT¹⁰¹:

Integración y gestión del ciclo de vida de la capa de red de dispositivos IoT de confianza:

Este proyecto se centra en enfoques para la incorporación de dispositivos IoT en la capa de red confiable a través de redes IP y la gestión del ciclo de vida de los dispositivos.

Seguridad en los dispositivos de infusión médicas inalámbricas: Los dispositivos están presentes en casi todos los entornos médicos, la manipulación del ecosistema inalámbrico puede exponer a pacientes a riesgos graves, por lo que este proyecto dio como resultado una guía de ciberseguridad de dispositivos médicos conectados.

Mitigación de ataques Distributed denial-of-Service (DDoS) basados en IoT: Este proyecto tiene como objetivo mejorar la resiliencia de los dispositivos de IoT contra los ataques basados en la red mediante el uso de la arquitectura de descripción de uso del fabricante, lo que permitirá que los dispositivos envíen y reciban solo el tráfico que necesitan para funcionar según lo previsto, y la red prohibirá todas las demás comunicaciones con los dispositivos.

Asegurar la Internet Industrial de las Cosas (IIoT): Este proyecto se centra en la integridad de los datos y la prevención, detección y mitigación de *malware* dentro de los sistemas de control industrial (ICS).

Seguridad de los productos IoT para el hogar: Este proyecto tiene como objetivo proporcionar información de ciberseguridad basada en datos sobre el estado del mercado de hogares inteligentes del consumidor.

Seguridad para las redes de sensores de IoT: Buscando demostrar cómo los sensores con recursos limitados pueden actualizar su *firmware* de forma segura.

Seguridad del ecosistema de monitoreo remoto de pacientes de telesalud: Este proyecto se centra en asegurar que la infraestructura que respalda la prestación de servicios de salud en línea pueda proteger los datos del paciente.

U.S. Department of Homeland Security

Agencia del Gobierno

Este organismo enfoca sus esfuerzos en ciberseguridad y protección de infraestructura crítica para el IoT, sobre todo, en actividades cibernéticas maliciosas que puedan amenazar la infraestructura y la seguridad pública¹⁰². Ha publicado el documento *Strategic Principles for Securing the Internet of Things (IoT)*¹⁰³ en el que se muestra una lista de principios para enfrentar los desafíos de seguridad de IoT dentro de las organizaciones:

- (1) Incorporar la seguridad en la fase de diseño;
- (2) Actualizaciones de seguridad avanzadas y gestión de vulnerabilidades;

¹⁰¹ NCCoE (2021), *Internet of Things (IoT)*. Disponible en: <https://www.nccoe.nist.gov/projects/building-blocks/iot>

¹⁰² U.S. Department of Homeland Security (2019), *Securing the Internet of Things*. Disponible en: <https://www.dhs.gov/securingthelot>

¹⁰³ U.S. Department of Homeland Security (2016), *Strategic Principles for Securing the Internet of Things (IoT)*. Págs. (3-4). Disponible en: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

- (3) Aprovechar las prácticas de seguridad probadas;
- (4) Priorizar las medidas de seguridad según el impacto potencial;
- (5) Promover la transparencia en todo el IoT, y
- (6) Conectarse con cuidado.

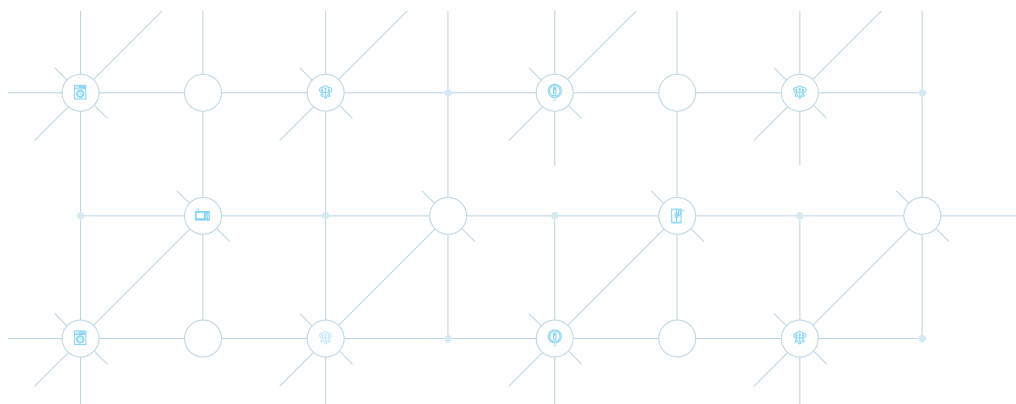
Federal Communications Commission (FCC)

Regulador de Telecomunicaciones

La FCC es el regulador de las comunicaciones por radio, televisión, satélite y cable en Estados Unidos, es una agencia independiente del gobierno y es la autoridad principal para la ley, la regulación y la innovación tecnológica de las comunicaciones¹⁰⁴.

Actualmente, las regulaciones de la FCC aplicables a los sistemas de IoT establecen pautas para la fabricación de dispositivos de IoT, incluida la asignación del espectro a ciertas clases de productos, la imposición de limitaciones de radiación electromagnética en los dispositivos y la exigencia de pruebas y certificación para ciertos componentes y sistemas. El conjunto completo de reglas de la FCC se puede encontrar en el Título 47¹⁰⁵ del Código de Regulaciones Federales (CFR).

Sí un dispositivo electrónico o sistema se comunica de forma inalámbrica o contiene un microprocesador, se considera un dispositivo de radio frecuencia (RF) que está sujeto a la autorización de equipo de la FCC. Si se clasifica dentro de las reglas de la FCC, el dispositivo deberá ser probado para garantizar el cumplimiento de las regulaciones de la FCC, sin embargo, algunos dispositivos pueden calificar para una exención de prueba de interferencia electromagnética (EMI)¹⁰⁶.



¹⁰⁴ FCC (2021), *What We Do*. Disponible en: <https://www.fcc.gov/about-fcc/what-we-do>

¹⁰⁵ Para más información visite: <https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization#step1>

¹⁰⁶ Tempo (s/f), *FCC Regulations and Guidelines for Manufacturing IoT Devices*. Disponible en: <https://www.tempoautomation.com/blog/fcc-regulations-and-guidelines-for-manufacturing-iot-devices/>

India

Ministry of Electronics & Information Technology (MEITY)

Agencia del Gobierno

El MEITY es el ministerio que trata los asuntos sobre la política en electrónica e Internet, promoción de la estandarización, pruebas y calidad para aplicaciones y tareas de tecnologías de la información¹⁰⁷.

En el tema de IoT, este organismo publicó el documento *IoT Policy Development*¹⁰⁸, en el que se mencionan diferentes iniciativas que forman parte del “Programa de India Digital” que tiene como objetivo transformar la India en una sociedad y una economía del conocimiento empoderada digitalmente y se espera contribuya al desarrollo del ecosistema de la industria de IoT en el país. El documento de política sobre IoT se centra en los siguientes objetivos:

- I. Crear una industria de IoT en India con un valor de US\$15 mil millones en 2020.
- II. Llevar a cabo el desarrollo de capacidades (humanas y tecnológicas) para conjuntos de habilidades específicas de IoT en los mercados nacionales e internacionales.
- III. Llevar a cabo la investigación y el desarrollo de todas las tecnologías de asistencia.
- IV. Desarrollar productos de IoT para las necesidades específicas de la India en todos los dominios posibles.

Adicionalmente, se propuso un marco para la Política de IoT, mismo que consta de cinco pilares verticales: Centros de demostración, creación de capacidades e incubación de empresas, investigación, desarrollo e Innovación, incentivos y compromisos, desarrollo de recursos humanos; y 2 horizontales: Estructura de normas y gobernanza¹⁰⁹.

Agricultura inteligente en India

El gobierno de India está promoviendo la adopción de la agricultura inteligente mediante el uso de tecnología e innovación en el sector agrícola del país, a través de la implementación de la Misión de Agricultura Digital (DAM) que incluye el Ecosistema Digital de Agricultura de India (IDEA), la base de datos de agricultores, la interfaz de servicio de agricultores unificados, el financiamiento a los estados y la renovación del Centro Nacional de Pronóstico de Cultivos de Mahalanobis (MNCFC).

Dentro del Plan Nacional de e-Gobernanza en la Agricultura (NeGPA), se contempla la entrega de fondos a los gobiernos estatales para proyectos de agricultura digital que utilizan tecnologías emergentes como IoT, inteligencia artificial y aprendizaje automático (AI/ML), *blockchain*, así como la adopción de drones, con el fin de promover la agricultura inteligente, el Gobierno ha promovido *Startups* en el sector agrícola, por ejemplo, la solución Per Drop More Crop tiene como objetivo aumentar la eficiencia en el uso del agua a nivel a través de tecnologías de microirrigación (sistemas de riego por goteo y aspersión)¹¹⁰.

¹⁰⁷ MEITY (2021), *Functions of Ministry of Electronics and Information Technology*. Disponible en: <https://www.meity.gov.in/about-meity/functions-of-meity>

¹⁰⁸ Para más información visite: https://www.meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20%281%29.pdf

¹⁰⁹ MEITY (2016), *Internet of Things*. Disponible en: <https://www.meity.gov.in/content/internet-things>

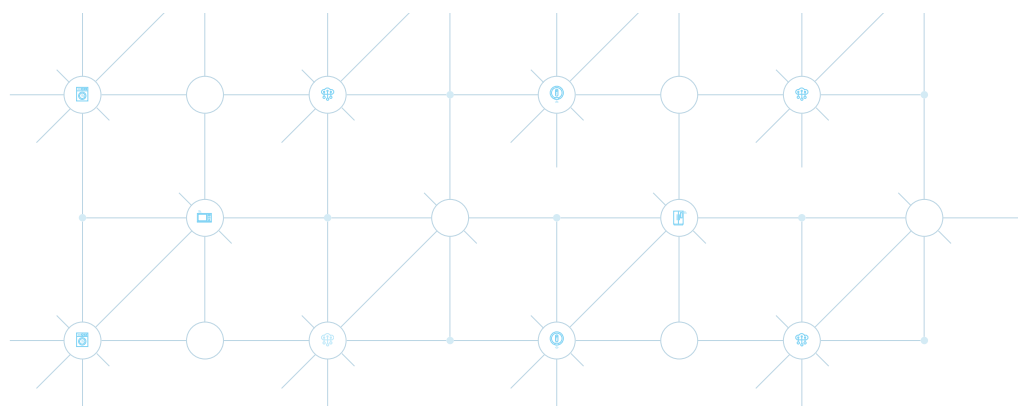
¹¹⁰ Press Information Bureau (2022), *Smart Farming*. Disponible en: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1848720>

En el tema de estandarización de IoT, se busca facilitar la participación global y nacional de la industria y los organismos de investigación para promover estándares en torno a las tecnologías IoT desarrolladas en el país¹¹¹.

El *Telecommunications Engineering Centre* (TEC) forma parte del MEITY y busca posicionar a la India como un “centro líder de fabricación y conocimiento de telecomunicaciones” de las naciones de Asia-Pacífico impulsando los estándares de telecomunicaciones, el apoyo a la fabricación y los conjuntos de habilidades de creación de redes en beneficio de esta región¹¹².

En 2013, se creó una nueva división que comenzó a trabajar en la Comunicación de Máquina a Máquina (M2M) y publicó nueve Informes Técnicos en el año 2015. Más tarde, esta división fue renombrada a *Internet of División of Things* y actualmente participa y contribuye con la Comisión de Estudio (SG) -20 del UIT-T, misma que trata temas sobre IoT y sus aplicaciones en ciudades y comunidades inteligentes¹¹³.

Recientemente, este centro ha publicado el “*Code of Practice for consumer IoT security*”, tomando en cuenta el crecimiento anticipado de los dispositivos IoT, se busca asegurar que IoT cumpla con los estándares y pautas de seguridad para proteger a los usuarios y las redes que conectan estos dispositivos IoT, así como a administrar las vulnerabilidades. Este código está destinado a los fabricantes de dispositivos IoT, proveedores de servicios/integradores de sistemas y desarrolladores de aplicaciones, etc.¹¹⁴



¹¹¹ MEITY (2016), *Draft IoT Policy Development*. Pág. (10). Disponible en: https://www.meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20%281%29.pdf

¹¹² TEC (2021), *Vision & Mission*. Disponible en: <https://tec.gov.in/vision-mission>

¹¹³ TEC (2021), *Internet of Things*. Disponible en: <https://tec.gov.in/internet-of-things-iot>

¹¹⁴ TEC (2021), *Code of Practice for Securing Consumer Internet of Things (IoT)*. Disponible en: https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20prattice.pdf



Japón

Information-technology Promotion Agency (IPA)

Agencia del Gobierno

La IPA fue establecida bajo la Ley de Promoción de Procesamiento de Información en 1970¹¹⁵, pero se reformó en 2004 y ha implementado varias iniciativas de tecnología de la información en conjunto con el Ministerio de Economía, Comercio e Industria¹¹⁶. En cuanto al tema de IoT, la Agencia apoya a los desarrolladores al participar en las siguientes actividades para proporcionar productos y servicios de IoT seguros¹¹⁷:

- 1) Disposición de los requisitos de seguridad, protección y confiabilidad para equipos de IoT: la IPA organizó un conjunto de requisitos de calidad de productos y/o servicios para los proveedores.
- 2) Promoción de procesos de diseño de seguridad y protección en ecosistemas inteligentes: La IPA cuenta con guías de proceso para las prácticas de diseño de seguridad y protección en el proceso de desarrollo y análisis de riesgo, con el fin de promover prácticas de diseño de seguridad y protección en los procesos de desarrolladores.
- 3) Guía para los detalles de los requisitos de calidad en ecosistemas inteligentes: La IPA estableció pautas de calidad para los desarrolladores de productos/servicios para los requisitos de calidad.

La visión de Japón consiste en que en la era de IoT, los productos y servicios estarán conectados y que el flujo e intercambio de datos de IoT impulsan la creación de empresas y la transformación socioeconómica. El ecosistema IoT (ecosistema inteligente) inevitablemente da lugar a riesgos sin precedentes, como conexiones irregulares no asumidas por los desarrolladores, que se traducen en peligros y vulnerabilidades de seguridad. IPA/SEC apoya a los desarrolladores al participar en las siguientes actividades para proporcionar productos y servicios de IoT seguros:

- | Disposición de requisitos de seguridad, protección y confiabilidad para equipos de IoT;
- | Promoción de procesos de diseño de seguridad/protección en ecosistemas inteligentes, y
- | Guía para detalles de requisitos de calidad en ecosistemas inteligentes.

¹¹⁵ IPA (2021), *IPA: Summary of IPA*. Disponible en: <https://www.ipa.go.jp/english/about/summary.html>

¹¹⁶ IPA (2020), *IPA Better Life with IT*. Pág. (2). Disponible en: <https://www.ipa.go.jp/files/000058630.pdf>

¹¹⁷ IPA (2021), *Building safeguards for reliable and affordable Internet of Things (IoT) environments*. Disponible en: <https://www.ipa.go.jp/english/sec/iot/index.html>

Ministry of Economy, Trade and Industry (METI)

Agencia del Gobierno

En 2019, el METI inició el grupo de estudio sobre ciberseguridad industrial, respecto a diversos enfoques para asegurar la confiabilidad de las conexiones mutuas entre el ciberespacio y el espacio físico. Durante 2020, el METI publicó el “Marco de seguridad de IoT”¹¹⁸ que es una compilación de enfoques para garantizar la confiabilidad de las conexiones mutuas entre el ciberespacio y el espacio físico, también busca promover la política de “Sociedad 5.0” y el concepto de política de “Industrias conectadas”, que se logran mediante la utilización de IoT e inteligencia artificial.

En 2021, el Ministerio propuso un estándar basado en “Pautas de seguridad de IoT” y las “Pautas de desarrollo de seguridad/seguridad de IoT”, el Marco general para sistemas seguros de IoT y la serie “IoT” del *IT Knowledge Center of the Information-technology Promotion Agency* (IPA). Asimismo, ha propuesto dos estándares:

1. **ISO/IEC JTC 1/SC 27 (Seguridad de la información, ciberseguridad y protección de la privacidad):** Este estándar incluye métodos, técnicas y pautas para abordar aspectos de seguridad y privacidad, como metodologías de captura de requisitos de seguridad, gestión de la seguridad de la información y las TIC, criptográficos y otros mecanismos de seguridad, documentación de soporte de gestión de seguridad, entre otros¹¹⁹.
2. **ISO/IEC JTC1/SC41 (Internet de las Cosas y gemelos digitales):** Incluye la estandarización en el área de Internet de las Cosas y el llamado gemelo digital (v.gr. modelo virtual diseñado para reflejar con precisión un objeto físico) y sus tecnologías relacionadas¹²⁰.

Se espera que estos estándares se utilicen en el desarrollo y mantenimiento de productos y servicios de IoT, y que contribuya al desarrollo seguro de un mundo conectado¹²¹.

Sociedad 5.0 en Japón

La Organización para el Desarrollo de Nuevas Energías y Tecnologías Industriales (NEDO), incorporado a METI, está desarrollando el proyecto “*Desarrollo de tecnología de detección innovadora para la sociedad IoT*” que busca, mediante la introducción de tecnología de detección innovadora, **la integración del ciberespacio (espacio virtual) y el espacio físico (espacio real) para visualizar y atender los problemas sociales con datos reales de personas y de todo tipo de “cosas”**. En este proyecto se utilizará tecnología con materiales de vanguardia, como nanotecnología y biotecnología para desarrollar el primer dispositivo de detección de partículas ultrapequeñas, lo que ayudará en la operación en entornos hostiles y la medición sin contacto y no destructiva¹²².

¹¹⁸ METI (2020), *IoT Security Safety Framework (IoT-SSF) Formulated*. Disponible en: https://www.meti.go.jp/english/press/2020/1105_002.html

¹¹⁹ Para más información visite: https://www.iec.ch/dyn/www/f?p=103:3A7%3A0%3A3A%3A3AFSP_ORG_ID%3A3401

¹²⁰ Para más información visite: https://www.iec.ch/dyn/www/f?p=103:7:0:::FSP_ORG_ID,FSP_LANG_ID:20486,25

¹²¹ METI (2021), *New International Standard for Safe Use of IoT Products and Systems Issued*. Disponible en: https://www.meti.go.jp/english/press/2021/0621_003.html

¹²² NEDO (2022), *Desarrollo de tecnología de detección innovadora para la sociedad IoT*. Disponible en: https://www.nedo.go.jp/activities/ZZJP_100151.html



Malasia

Ministerio de Ciencia, Tecnología e Innovación (MOSTI)

Agencia del Gobierno

El *Malaysia's National Applied Research and Development Centre* (MIMOS) es una agencia dependiente del Ministerio de Ciencia, Tecnología e Innovación (MOSTI), el cual contribuye a transformar la industria de Malasia a través de plataformas, productos y soluciones tecnológicas patentables desde 1987. En los últimos 12 años, MIMOS ha registrado más de 2,000 propiedades intelectuales en varios dominios tecnológicos¹²³.

En 2015, publicó "*National Internet of Things (IoT) Strategic Roadmap*", con esta estrategia se buscó que Malasia fuera el primer centro regional de desarrollo de IoT y así crear un ecosistema de IoT nacional para permitir la proliferación del uso y la industrialización de IoT como una nueva fuente de crecimiento económico. Esta Hoja de Ruta tiene como objetivo integrar todos los esfuerzos de las partes interesadas en Malasia para centrarse en áreas de creación de valor significativo, esto a través de tres objetivos estratégicos:

- 1) Crear un ecosistema industrial de IoT propicio para fomentar el desarrollo, la difusión y la adopción de tecnologías de IoT.
- 2) Fortalecer las capacidades de los emprendedores tecnológicos y fomentar la generación de productos y servicios de IoT competitivos a nivel mundial para fortalecer aún más la posición de Malasia en la industria de IoT.
- 3) Malasia como centro de desarrollo regional para IoT con el establecimiento de un centro integrado para soluciones de IoT¹²⁴.

Malaysian Communications and Multimedia Commission (MCMC)

Regulador de Telecomunicaciones

La MCMC es el regulador de la industria de comunicaciones y multimedia conforme a la Ley de la Comisión de Comunicaciones y Multimedia de Malasia (1998). Su función es implementar y promover los objetivos gubernamentales para el sector de las comunicaciones y los multimedios. Se encarga de supervisar el marco regulatorio para las industrias convergentes de telecomunicaciones y radiodifusión y las actividades en línea¹²⁵. En el tema de IoT, la MCMC ha emitido algunos reportes sobre los retos regulatorios y las iniciativas con respecto a esta tecnología¹²⁶.

¹²³ MIMOS (2021), *The Company*. Disponible en: <http://www.mimos.my/about-us/the-company/>

¹²⁴ MIMOS (2015), *National IoT Strategic Roadmap*. Pág. (10). Disponible en: http://www.mimos.my/iot/National_IoT_Strategic_Roadmap_Summary.pdf

¹²⁵ MCMC (2021), *About Us. Our Responsibility*. Disponible en: <https://www.mcmc.gov.my/en/about-us/our-responsibility>

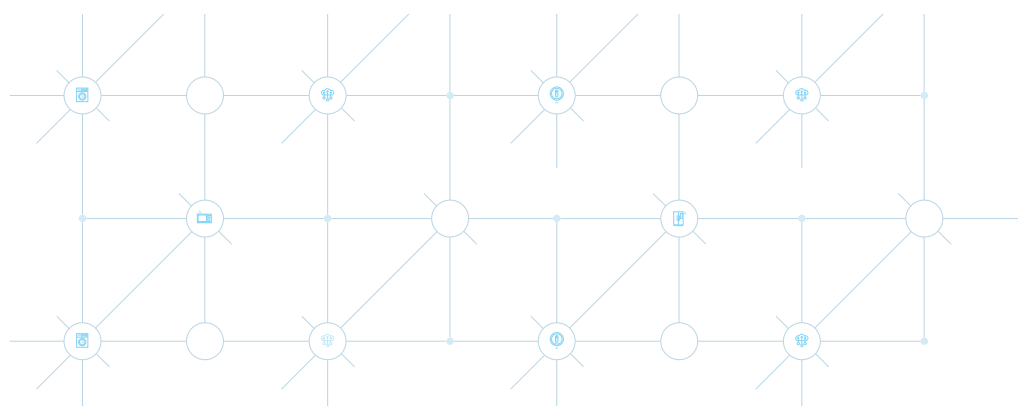
¹²⁶ Para más información, visite: <https://www.mcmc.gov.my/en/resources/publications/technology-and-society>

El *Malaysian Technical Standards Forum Bhd* (MTSFB) fue originalmente una empresa fundada en 2004, misma que fue designada como el Foro de Normas Técnicas por la MCMC, responsable del establecimiento y mantenimiento de códigos técnicos sobre los requisitos de interoperabilidad de red, seguridad y otros aspectos técnicos de las instalaciones de red, servicios de red y aprobación de equipos¹²⁷.

Este organismo cuenta con un grupo de trabajo dedicado para IoT y ciudades inteligentes y sostenibles (WG1). Entre sus actividades se encuentra desarrollar informes técnicos, directrices, recomendaciones y estándares relacionados con IoT, asesorar a organismos regulatorios, legales y gubernamentales sobre IoT, participar en las conferencias y reuniones de estándares de IoT, como ITU SG 20, realizar seminarios sobre estándares de IoT y nuevas aplicaciones emergentes y proporcionar y crear estándares de prueba de interoperabilidad y conformidad para productos de IoT. Actualmente, este grupo de trabajo ha registrado dos códigos técnicos:

El Código para la Especificación para Centros de Datos Ecológicos, que fue desarrollado de conformidad por el Foro de Normas Técnicas de Malasia Berhad (MTSFB) a través de su Grupo de Expertos Técnicos (TEG) sobre Centros de Datos Ecológicos bajo la supervisión del *Green ICT Working Group* y fue desarrollado para proporcionar los requisitos mínimos para los centros de datos verdes con el fin de establecer políticas, sistemas y procesos para mejorar la eficiencia energética de los centros de datos y al mismo tiempo reducir la huella de carbono de la industria¹²⁸.

El Código para Internet de las Cosas (IoT) - Gestión de seguridad, fue desarrollado por el Foro de estándares técnicos de Malasia ('MTSFB') a través de su subgrupo de trabajo de seguridad de IoT. Este Código Técnico se desarrolla en referencia a Estándares Internacionales como ITU-T Y.4000, ITUT Y.4100 y ITU-T Y.4401¹²⁹.



¹²⁷ MTSFB (2021), *About MTSFB*. Disponible en: <https://mtsfb.org.my/about-mtsfb/>

¹²⁸ Para más información visite: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-Green_Data_Centres.pdf

¹²⁹ Para más información visite: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G013_2018_IoT_SECURITY-MANAGEMENT.pdf

México

Secretaría de Economía (SE)

Agencia del Gobierno

La Secretaría de Economía es la encargada de desarrollar e implementar políticas integrales de innovación, diversificación e inclusión productiva y comercial, así como de incentivar la inversión nacional y extranjera en México¹³⁰.

Como un órgano desconcentrado, la Secretaría de Economía cuenta con la Dirección General de Normas, que tiene entre sus atribuciones las conferidas por la Ley Federal sobre Metrología y Normalización, la Ley Federal de Protección al Consumidor, la Ley de Hidrocarburos, la Ley Federal de Telecomunicaciones y Radiodifusión, además atiende los reglamentos y demás disposiciones aplicables en materia de normalización, metrología y evaluación de la conformidad, así como los acuerdos y tratados internacionales en materia comercial¹³¹.

Adicionalmente, se cuenta con un Organismo Nacional de Normalización llamado Normalización y Certificación (NYCE), que se encarga de las Normas Oficiales Mexicanas (NOM) (obligatorias) y Normas Mexicanas (NMX) (voluntarias) de diversas industrias, entre ellas la industria Electrónica, Telecomunicaciones y Tecnologías de Información¹³². Actualmente se cuentan con tres NMX para IoT:

- 1) NORMA MEXICANA NMX-I-320-NYCE-2020, "TELECOMUNICACIONES-TÉRMINOS Y DEFINICIONES PARA EL INTERNET DE LAS COSAS", elaborada, aprobada y publicada como Proyecto de Norma Mexicana bajo la responsabilidad del Organismo Nacional de Normalización denominado "Normalización y Certificación NYCE, S.C."¹³³.
- 2) NORMA MEXICANA NMX-I-321-NYCE-2020, "TELECOMUNICACIONES-DESCRIPCIÓN GENERAL DEL INTERNET DE LAS COSAS", elaborada, aprobada y publicada como Proyecto de Norma Mexicana bajo la responsabilidad del Organismo Nacional de Normalización denominado "Normalización y Certificación NYCE, S.C."¹³⁴.
- 3) NORMA MEXICANA NMX-I-1362-NYCE-2021, "TELECOMUNICACIONES-PROCEDIMIENTO SIMPLE DE ENCRYPTACIÓN PARA ENTORNOS DE INTERNET DE LAS COSAS (IOT)", tiene concordancia modificada (MOD) con la Norma Internacional: *Recommendation X.1362 (2017), Simple encryption procedure for Internet of things (IoT) environments* y proporciona un procedimiento de encriptación para la seguridad del dispositivo IoT, destinado para aplicarse a entornos de IoT, especialmente para dispositivo IoT que tienen capacidades obligatorias para comunicación y capacidades opcionales para detección, accionamiento, almacenamiento de datos y procesamiento de datos¹³⁵.

¹³⁰ Gobierno de México (2021), *Secretaría de Economía ¿Qué hacemos?*. Disponible en: <https://www.gob.mx/se/que-hacemos>

¹³¹ DOF (2019), *REGLAMENTO Interior de la Secretaría de Economía*. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5575714&fecha=17/10/2019

¹³² NYCE (2021), ¿Quiénes somos?. Disponible en: <https://www.nyce.org.mx/quienes-somos/>

¹³³ Diario Oficial de la Federación (2020), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-320-NYCE-2020*. Disponible en: <https://sidof.segob.gob.mx/notas/5593710>

¹³⁴ Diario Oficial de la Federación (2020), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-321-NYCE-2020*. Disponible en: <https://sidof.segob.gob.mx/notas/5593711>

¹³⁵ Diario Oficial de la Federación (2022), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-1362-NYCE-2021*. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5642167&fecha=08/02/2022#gsc.tab=0

Instituto Federal de Telecomunicaciones (IFT)

Regulador de Telecomunicaciones

El IFT, como regulador de las telecomunicaciones y la radiodifusión, se encarga de regular, promover y supervisar el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de telecomunicaciones y la radiodifusión (TyR) en México, así como el acceso a infraestructura y otros insumos esenciales, contribuyendo a garantizar el derecho a la información y el acceso universal a dichos servicios. Asimismo, es la autoridad en materia de competencia económica en los sectores de telecomunicaciones y radiodifusión¹³⁶.

En cuanto al tema de IoT, el IFT elabora el *“Código de mejores prácticas para la ciberseguridad del IoT”*, en dicho documento se establecerán las mejores prácticas de ciberseguridad mediante recomendaciones para dispositivos IoT que puedan hacer uso del espectro radioeléctrico o ser conectados a través de redes de telecomunicaciones; así como aquellos servicios digitales comúnmente vinculados a estos dispositivos que son requeridos para proporcionar la funcionalidad prevista por estos con un enfoque basado en gestión de riesgos y enfatizando la seguridad por diseño. Con la emisión de este Código se coadyuvará a reducir las vulnerabilidades y ciberataques a la seguridad de los dispositivos evitando daños a los usuarios; además de incentivar la innovación tecnológica ante las necesidades cambiantes del sector¹³⁷.

Dentro de su Hoja de Ruta 2021-2025, se plantea una estrategia institucional para un horizonte de planeación de cinco años, donde se reconoce la creciente importancia que tiene el sector de TyR en el contexto del ecosistema digital y en la forma en que se deben enfrentar los desafíos que lleva consigo la era de la transformación digital¹³⁸, sus líneas de acción regulatoria (LAR) enfocadas en IoT son:

LAR 1.3.1: Promover la disponibilidad de espectro radioeléctrico para la provisión de diferentes servicios y aplicaciones de radiocomunicaciones¹³⁹.

LAR 3.2.1: Realizar un monitoreo y análisis tecnológico continuo para identificar de forma anticipada tecnologías y/o casos de uso emergentes, así como evaluar el rol que puede tomar el Instituto en el fomento de su adopción¹⁴⁰.

LAR 3.2.2: Comunicar las ventajas y fomentar la adopción de las nuevas tecnologías y casos de uso en la sociedad y en los sectores productivos¹⁴¹.

LAR 3.2.3: Favorecer el desarrollo regulatorio, en los sectores productivos y en la sociedad, de casos de uso y modelos de negocio asociados a las nuevas tecnologías que se encuentren relacionadas de manera directa con los sectores de TyR¹⁴².

¹³⁶ IFT (2021), *Objetivos Institucionales*. Disponible en: <http://www.ift.org.mx/conocenos/objetivosinstitucionales>

¹³⁷ IFT (2021), *Programa Anual de Trabajo 2021*, Pág. (42). Disponible en: <http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/pat2021.pdf>

¹³⁸ IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (4). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

¹³⁹ IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (47). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

¹⁴⁰ IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (93). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

¹⁴¹ IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (95). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

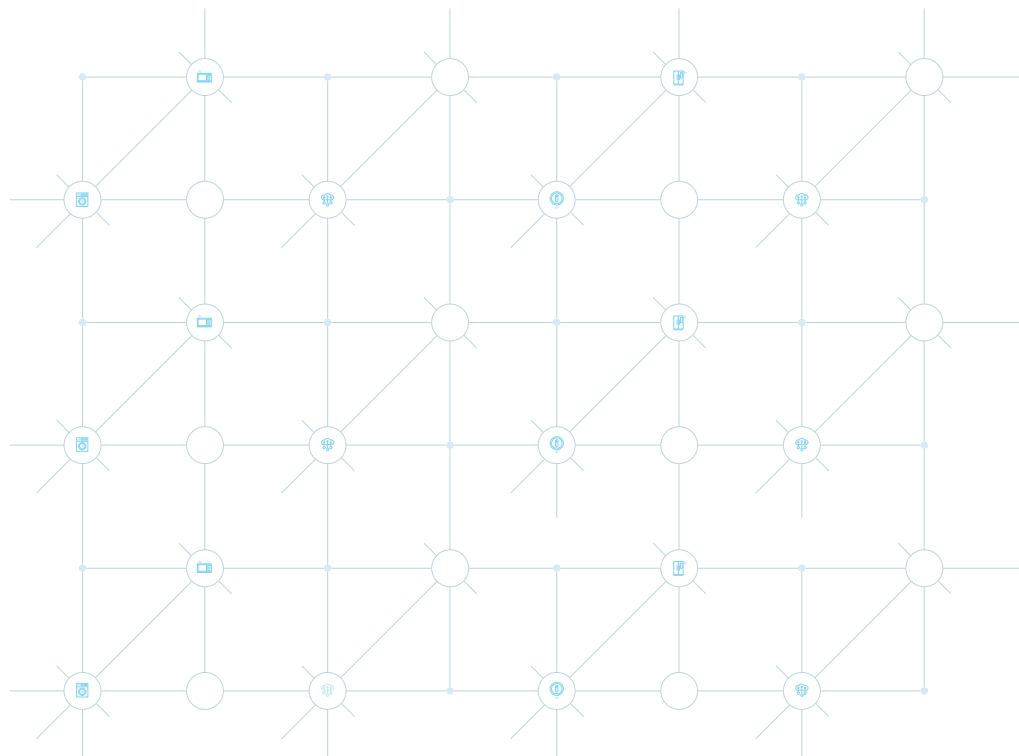
¹⁴² IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (97). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

Secretaría de Innovación, Ciencia y Tecnología, del Estado de Jalisco. Centro de Innovación, Desarrollo Tecnológico y Aplicaciones (CIIoT)

Agencia del Gobierno

La Secretaría de Innovación, Ciencia y Tecnología del Estado de Jalisco en México publicó la convocatoria JAL-015-03 del Fondo Mixto CONACYT - Gobierno del Estado de Jalisco¹⁴³. En 2016 el consorcio conformado por el Instituto Tecnológico de Monterrey (Campus Guadalajara), el CINVESTAV (Sede Guadalajara), y el Instituto Tecnológico José Mario Molina Pasquel y Henríquez (Unidad Zapopan), fue seleccionado como la instancia ganadora y se creó el CIIoT, que es un *hub* de soluciones para la transformación digital en el que se realizan actividades de definición, diseño, prototipado, pruebas y manufactura de soluciones IoT.

Este *hub* brinda servicios especializados en innovación y desarrollo de negocios digitales, cuenta con una red Académica de investigación y desarrollo que impulsará la creación de bases de conocimiento, analítica y explotación de datos, la propiedad intelectual y la investigación tecnológica aplicada; así como la formación de talento técnico especializado en soluciones de IoT.



¹⁴³ Gobierno del Estado de Jalisco (2017), *Centro de Innovación, Desarrollo Tecnológico y Aplicaciones CIIoT*. Disponible en: <https://sicyt.jalisco.gob.mx/innovacion/iniciativas-alta-tecnologia/centro-innovacion-internet>

Reino Unido

Foreign, Commonwealth & Development Office

Agencia del Gobierno

Este organismo cuenta con el programa IoTUK, que inició en 2017 y busca que el Reino Unido sea líder en IoT en el mundo. Esta iniciativa permitirá trabajar con empresas de todos los tamaños para acelerar la adopción de oportunidades y capacidades de IoT en el Reino Unido a gran escala en comunicaciones y electrónica¹⁴⁴.

Department for Digital, Culture, Media & Sport (DCMS)

Agencia del Gobierno

Mediante este organismo, el Gobierno de Reino Unido aboga por que se incorpore seguridad sólida en los dispositivos inteligentes conectados a Internet, por lo que deben de ser “seguros por diseño”¹⁴⁵, por lo que el DCMS realizó una consulta pública sobre propuestas para regular la seguridad cibernética de los dispositivos inteligentes de los consumidores en 2020¹⁴⁶.

Además, ha realizado consultas públicas relacionadas con la seguridad del consumidor en el uso de IoT durante 2019¹⁴⁷, y realiza guías de orientación sobre cómo implementar los requisitos de seguridad en dispositivos IoT¹⁴⁸.

Office of Communications (Ofcom)

Regulador de Telecomunicaciones

Ofcom es el regulador de los servicios de comunicaciones, quien tiene como función asegurar el servicio de banda ancha, teléfono residencial y servicios móviles, televisión y radio, el servicio postal universal y el espectro radioeléctrico¹⁴⁹.

En relación con el IoT, Ofcom otorga licencias para el acceso al espectro por parte de dispositivos IoT, mismos que pueden ser con o sin licencia bajo los lineamientos de la *Wireless Telegraphy Act*¹⁵⁰. Las aplicaciones de IoT que requieren de una licencia son las que utilizan los rangos del espectro radioeléctrico de las siguientes bandas: 55.75625-60 MHz, 62.75625-64.8 MHz, 64.8875-66.2 MHz, 70.5-71.5 MHz, 80.0-81.5 MHz; a estas aplicaciones se les otorga una licencia de *Business Radio Internet of Things*.

Esta licencia cuenta con dos opciones; la primera, es la asignación técnica que autoriza el uso de una amplia variedad de equipos de radio comerciales, misma que esta adecuada para el uso de espectro en un sitio o sitios en particular, mientras la segunda es la asignación por área definida estas licencias dan uso exclusivo de una frecuencia en una cuadrícula de 50 km², un país o todo el Reino Unido¹⁵¹.

¹⁴⁴ Gov.UK (2017), *IoTUK - The world's leading national IoT programme*. Disponible en: <https://www.gov.uk/government/publications/iotuk-the-worlds-leading-national-iot-programme>

¹⁴⁵ Gobierno de Reino Unido (2021), *About us*. Disponible en: <https://www.gov.uk/government/organisations/departament-for-digital-culture-media-sport/about>

¹⁴⁶ Para más información visite: <https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views>

¹⁴⁷ Para más información, visite: <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

¹⁴⁸ Para más información, visite: <https://www.gov.uk/government/collections/secure-by-design>

¹⁴⁹ Ofcom (2021), *What is Ofcom?*. Disponible en: <https://www.ofcom.org.uk/about-ofcom/what-is-ofcom>

¹⁵⁰ Para más información, visite: <https://www.legislation.gov.uk/ukpga/2006/36/contents>

¹⁵¹ Ofcom (2016), *Internet of Things*. Disponible en: <https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/internet-of-things>

Singapur

Infocomm Media Development Authority (IMDA)

Regulador de Telecomunicaciones

La IMDA en Singapur desarrolla y regula los sectores de las comunicaciones y los medios de comunicación y busca crear un entorno para desarrollar contenido de calidad, aprovechar los medios digitales y la cadena de valor¹⁵². Dentro del IMDA existe el Comité de Estándares de Tecnología de la Información (ITSC, por sus siglas en inglés) que fue creado para impulsar y liderar las actividades de estandarización del sector en Singapur¹⁵³.

En cuanto al tema de IoT, IMDA junto con el Comité Técnico de IoT de ITSC ha desarrollado un conjunto de estándares de IoT publicados como referencias técnicas para redes de sensores y IoT con el fin de abordar la ausencia de redes de sensores coherentes o estándares de IoT, con un enfoque en la interoperabilidad de la interfaz. Estas referencias técnicas se enfocan en interfaces estándar abiertas entre los dispositivos y sistemas para ayudar a reducir los costos de implementación, operación y mantenimiento de aplicaciones de sensores. Actualmente se cuentan con **6 estándares** en Singapur de este tipo¹⁵⁴:

TR 38: 2014 Sensor network for smart nation (public areas): Brinda información sobre los estándares de interfaz de aplicación y comunicación para el desarrollo y despliegue de redes de sensores para áreas públicas en Singapur.

TR 40: 2014 Sensor networks for Smart Nation (homes): Proporciona un marco y un conjunto mínimo de estándares de interfaz de aplicación y comunicación para el desarrollo y despliegue de redes de sensores para hogares en Singapur.

TR 47: 2016 IoT reference architecture for Smart Nation: Recomienda un conjunto de estándares industriales e internacionales para la interoperabilidad de la interfaz de información y servicios en múltiples industrias para su implementación en Singapur.

TR 50: 2016 IoT information and services interoperability for Smart Nation: Especifica una arquitectura de referencia independientemente de la tecnología para aplicaciones o sistemas para IoT o redes de sensores que son interoperables entre sí a través de un conjunto de interfaces definidas para lograr un intercambio de datos y un uso de la información fluidos.

TR 64: 2018 Guidelines for IoT security for smart nation: Esta guía presenta los conceptos básicos de seguridad y la terminología para los sistemas de Internet de las cosas (IoT) y sus aplicaciones.

IMDA IoT Cyber Security Guide (2019): Esta guía sirve como una guía práctica para las empresas que tienen la intención de implementar soluciones de IoT, así como para sus proveedores, proporcionando recomendaciones de referencia, conceptos básicos y listas de verificación, centrándose en los aspectos de seguridad para la adquisición, desarrollo, operaciones y mantenimiento de IoT.

¹⁵² IMDA (2021), *About IMDA*. Disponible en: <https://www.imda.gov.sg/Who-We-Are/about-imda>

¹⁵³ IMDA (2021), *IT Standards Committee (ITSC)*. Disponible en: <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/industry-committees-and-working-groups/IT-Standards-Committee>

¹⁵⁴ IMDA (2021), *Internet of Things (IoT)*. Disponible en: <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Internet-of-Things>

Unión Europea

Comisión Europea

Agencia del Gobierno

La Comisión Europea ha adoptado un conjunto de acciones de apoyo para acelerar la adopción de IoT¹⁵⁵, en 2015 creó la “*Alliance for Internet of Things Innovation*” (AIOTI) con el fin de apoyar la creación de un ecosistema europeo de Internet de las Cosas innovador e impulsado por la industria. Esta alianza tiene como misión impulsar el desarrollo de negocios, políticas, investigación e innovación en IoT, *Edge Computing* y otras tecnologías convergentes a lo largo de la cadena de valor digital para respaldar la digitalización y la competitividad de Europa¹⁵⁶. Además, colabora en diferentes niveles con organizaciones internacionales, europeas y de normalización¹⁵⁷.

En 2016, la Comisión Europea publicó el documento “*Advancing the Internet of Things in Europe*”¹⁵⁸, que forma parte de la iniciativa “Digitalización de la industria europea”¹⁵⁹ y especifica la visión de IoT para la región. Adicionalmente, se creó *IoT-European Platforms Initiative* (IoT-EPI)¹⁶⁰ con el fin de crear un ecosistema de IoT en Europa, maximizando las oportunidades para el desarrollo de plataformas, la interoperabilidad y el intercambio de información.

Otra iniciativa es la “*European data economy*”¹⁶¹ de 2017 donde se plantean soluciones, políticas y legislaciones relativas al libre flujo de datos a través de la Unión Europea; en particular para el caso de IoT, esta iniciativa busca mejorar la seguridad jurídica en torno a los productos y servicios de IoT.

Asimismo, la Comisión Europea ha apoyado en la investigación y desarrollo del IoT. En este contexto, el reporte denominado “*Cluster Study*”¹⁶² se enfocó en los clústeres físicos y virtuales de empresas, organizaciones de investigación y académicos que trabajan en la innovación, el desarrollo y la implementación en el mercado de tecnologías y aplicaciones de IoT.

Durante 2020, se desarrolló el programa “*Horizon 2020*”¹⁶³, enfocado en la investigación e innovación, y en el que se invirtieron cerca de €500 millones en investigación, innovación y despliegue relacionados con IoT. Para el período 2021-2027, la Unión Europea invertirá alrededor de €95.5 millones en investigación, innovación y despliegue de tecnologías emergentes, en línea con el programa *Horizon 2020* y contribuyendo a las transiciones verde y digital de Europa.

En el marco de las convocatorias 2021-2022 sobre “Tecnologías informáticas y de datos líderes en el mundo”, la Comisión actualmente apoya proyectos de IoT y otras actividades en *Horizon Europe’s Cluster 4 Destination 3: From Cloud to Edge to IoT*, lo que impulsará la colaboración industrial a través de plataformas y estándares abiertos¹⁶⁴.

¹⁵⁵ European Commission, (2021), *Europe’s Internet of Things Policy*. Disponible en: <https://digital-strategy.ec.europa.eu/en/policies/iot-policy>

¹⁵⁶ AIOTI (2021), *About AIOTI*. Disponible en: <https://aioti.eu/about-us/organisation/>

¹⁵⁷ AIOTI (2023), *Research and Partnerships*. Disponible en: <https://aioti.eu/about-us/our-groups/research-and-partnerships/>

¹⁵⁸ Para más información visite: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110>

¹⁵⁹ Para más información visite: <https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=54619>

¹⁶⁰ Para más información visite: <https://iot-eipi.eu/>

¹⁶¹ Para más información visite: https://eur-lex.europa.eu/content/news/building_EU_data_economy.html

¹⁶² Para más información visite: https://ec.europa.eu/growth/industry/policy/cluster/excellence_en

¹⁶³ Para más información visite: <https://ec.europa.eu/programmes/horizon2020/>

¹⁶⁴ Para más información visite: <https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy>

En resumen, la Comunidad Europea ha desarrollado iniciativas que abordan aspectos clave para la promoción de la industria del IoT¹⁶⁵, entre las que destacan:

Impulsar el desarrollo de negocios, políticas, investigación e innovación en IoT, *Edge Computing* y otras tecnologías convergentes a lo largo de la cadena de valor digital para respaldar la digitalización y la competitividad de Europa.

Atender los retos más importantes para el desarrollo del ecosistema de IoT, conforme a la visión de la Comunidad Europea:

- Las pequeñas y medianas empresas podrían tener una vocación mayor a la adopción de IoT que las grandes empresas.
- Ausencia de estándares comunes y soluciones interoperables a través del ciclo de vida de los servicios y productos. Se considera la interoperabilidad como esencial para el despliegue de IoT y para asegurar el flujo masivo de datos entre los sectores y sus cadenas de valor. Lo anterior a partir de una serie de pasos: (i) Generación de datos; (ii) transferencia de datos; (iii) almacenamiento de datos; (iv) procesamiento de datos, y (v) provisión de servicios de datos.
- Las conexiones M2M se consideran el requerimiento más básico para los ecosistemas IoT.
- Obstáculos de conectividad: Espectro y cobertura de las redes de telecomunicaciones.
- Numeración.
- Seguridad y confianza, respondiendo las siguientes preguntas: ¿Quién es responsable de garantizar la seguridad de los productos?, ¿Cómo deben distribuirse los pasivos en caso de que la tecnología se comporte de una manera insegura, causando daño? Y ¿Quién es el responsable de garantizar la seguridad de manera continua?

Impulsar plataformas abiertas para fomentar la innovación IoT es un elemento clave para alcanzar el liderazgo en esta industria.

Fomentar la innovación y el desarrollo de tecnologías de IoT.

Desarrollar sinergias entre la Estrategia Europea de Datos y la Estrategia de Movilidad Sostenible e Inteligente, con un enfoque particular en el despliegue de un espacio europeo común de datos de movilidad.

Entornos inteligentes de IoT para el cuidado de adultos mayores

ACTIVAGE es una iniciativa para entornos de vida inteligente, cuyo objetivo principal es construir el primer ecosistema europeo de IoT, a través de 9 sitios de implementación en siete países europeos, reutilizando y escalando plataformas, tecnologías y estándares de IoT abiertos y patentados subyacentes, e integrando nuevas interfaces necesarias para proporcionar interoperabilidad entre estas plataformas heterogéneas, que permitirá el despliegue y la operación a gran escala de soluciones y servicios basados en IoT para el envejecimiento activo y saludable, apoyando y ampliando la independencia de los adultos mayores en sus entornos de vida.

El conjunto de ecosistemas ACTIVAGE IoT (AIOTES) integró servicios que monitoreaban la actividad diaria y la movilidad para garantizar la seguridad y la comodidad en el hogar. Así, como el seguimiento de la salud y el apoyo a los cuidadores para prevenir el deterioro mental de las personas mayores a través de la estimulación cognitiva¹⁶⁶.

¹⁶⁵ European Commission (2022), *Europe's Internet of Things Policy*. Disponible en: <https://digital-strategy.ec.europa.eu/en/policies/iot-policy>

European Telecommunications Standards Institute (ETSI)

Agencia del Gobierno

ETSI es la organización europea de estándares. Se trata del organismo de normalización regional de las telecomunicaciones, la radiodifusión y otras redes y servicios de comunicaciones electrónicas y respalda el desarrollo, la ratificación y la prueba de estándares aplicables a nivel mundial para sistemas, aplicaciones y servicios habilitados para las Tecnologías de la Información y Comunicación (TIC)¹⁶⁷.

En cuanto a IoT, ETSI se encarga de la estandarización de 3GPP (LTE-M, NB-IoT y EC-GSM-IoT), de las comunicaciones inteligentes de máquina a máquina (M2M), la interoperabilidad de IoT, de la gestión de la información, aplicaciones en el IoT y soporte de IoT¹⁶⁸. Esta organización cuenta con **158 estándares dedicados para IoT**¹⁶⁹, entre los que se encuentran el estándar con enfoque técnico sobre cómo lograr la interoperabilidad de las plataformas IoT estandarizadas existentes¹⁷⁰, el estándar sobre calidad de transmisión de voz y multimedia (STQ) y aspectos de calidad de servicio para IoT¹⁷¹, el estándar de código abierto y estándares para *software* nativo en la nube aplicable para una capa de servicio de IoT virtualizado¹⁷², así como las directrices para el uso de la interoperabilidad semántica en la industria IoT¹⁷³.

A manera de resumen, en la Tabla 3.1, podemos observar tanto las iniciativas enfocadas al desarrollo de IoT como las acciones para la estandarización y normalización de esta tecnología en los países seleccionados.

Es importante resaltar que todos los países analizados cuentan con algún tipo de iniciativa para el desarrollo de IoT, estas iniciativas dependen de organismos gubernamentales y de los reguladores de Telecomunicaciones. Sin embargo, respecto a las acciones de estandarización y normalización de IoT, únicamente el 44% de los países cuentan con algún estándar técnico en IoT, y éste es atendido por algún organismo, ministerio, secretaría de estado o agencia del gobierno de los países analizados.

¹⁶⁶ CORDIS (2020), *Activating Innovative IoT smart living environments for Ageing well*. Disponible en: <https://cordis.europa.eu/project/id/732679>

¹⁶⁷ ETSI (2021), *About ETSI*. Disponible en: <https://www.etsi.org/about>

¹⁶⁸ ETSI (2021), *Internet of Things*. Disponible en: <https://www.etsi.org/technologies/internet-of-things>

¹⁶⁹ Para más información visite: <https://www.etsi.org/standards-search#page=1&search=iot&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=&harmonized=0&keyword=IoT&TB=&stdType=&frequency=&mandate=&collection=&sort=1>

¹⁷⁰ Para más información visite: https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf

¹⁷¹ Para más información visite: https://www.etsi.org/deliver/etsi_tr/103400_103499/103467/01.01.01_60/tr_103467v010101p.pdf

¹⁷² Para más información visite: https://www.etsi.org/deliver/etsi_tr/103500_103599/103528/01.01.01_60/tr_103528v010101p.pdf

¹⁷³ Para más información visite: https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf

Tabla 2.1. Iniciativas y estándares IoT en países seleccionados.

País	Iniciativas enfocadas en IoT		Estandarización/Normalización	
	Agencia de Gobierno	Regulador de Telecomunicaciones	Agencia de Gobierno	Regulador de Telecomunicaciones
Arabia Saudita		✓		De los países seleccionados ningún regulador tiene la atribución de emitir estándares o normas
Argentina	✓			
Brasil	✓	✓		
Canadá	✓	✓	✓	
China	✓		✓	
Colombia	✓	✓		
Corea del Sur	✓			
Emiratos Árabes Unidos		✓		
Estados Unidos	✓	✓	✓	
India	✓	✓		
Japón	✓			
Malasia	✓	✓	✓	
México	✓	✓	✓	
Reino Unido	✓	✓		
Singapur	✓		✓	
Unión Europea	✓		✓	

Fuente: IFT con información de los países seleccionados.

Las experiencias internacionales presentadas en esta sección generan un acervo de conocimiento regulatorio destinado al desarrollo de la industria de IoT, a partir del cual es posible plantear una lista de iniciativas potenciales y recomendaciones para el fomento y desarrollo de IoT en México:

Iniciativas potenciales para el desarrollo de IoT en México

- (1) La conformación de un compendio de regulaciones para IoT en México (sujeto a un proceso consultivo con un enfoque de múltiples partes interesadas, el proceso consultivo podría incluir también grupos de enfoque, encuestas, entre otros). Este compendio buscaría estimular el desarrollo del mercado de Internet de las Cosas en el país, donde se fomente la libre competencia y la inversión, contando con reglas de juego claras que equilibren constantemente los diferentes tipos de control y los intereses de las partes que intervienen en su cadena de valor¹⁷⁴.

Esta propuesta de compendio regulatorio debería estar basado en un diagnóstico que permita identificar los problemas clave que afectan el despliegue de estas tecnologías, como el alcance de los dispositivos de IoT, la escala respecto al número de dispositivos conectados y la seguridad y ciberseguridad de los dispositivos, destacando los beneficios y desafíos potenciales e identificando los posibles roles del gobierno y los entes reguladores en la promoción del avance de las tecnologías de IoT en asociación con el sector privado.

- (2) Establecer el consenso respecto a las definiciones que deben imperar en el ecosistema de IoT en México. Este paso es crucial y depende de un profundo conocimiento del ecosistema de IoT, así como de los múltiples servicios que se pueden ofrecer.
- (3) Continuar con la difusión de las ventajas sobre el uso de IPv6, por otro lado, como regla general la numeración debe ser interoperable en el ámbito nacional e internacional y sujeta a las obligaciones de portabilidad. Esto permitirá que una aplicación pueda evolucionar desde versiones que no requieran interoperatividad a versiones más sofisticadas que permitan funcionalidades adicionales, todo ello sin cambiar la numeración y de manera flexible.
- (4) Establecer un manual de la industria donde se establezcan las mejores prácticas comerciales y de información para los usuarios en la industria de IoT en México (v.gr. seguridad de la red, protección de datos, manual de usuario, calidad del servicio, riesgos de interferencia, entre otros).
- (5) Promover las iniciativas público-privadas para proyectos o soluciones con un gran volumen de dispositivos conectados, fomentando la transparencia y la posibilidad de que pequeños proveedores de IoT participen.
- (6) Crear un plan que incentive la expansión de las aplicaciones de IoT y M2M. Este plan podría incluir la promoción de incentivos fiscales, modificaciones a las reglas de portabilidad y obligaciones mínimas y claras para la portabilidad de los accesos destinados exclusivamente a conexiones de dispositivos IoT (considerando la experiencia de ANATEL, en particular para este punto).

¹⁷⁴ En este sentido, hay que recordar que la CRC ha identificado que México tiene una fuerte industria de soporte al segmento automotriz, mientras que en Colombia ello no existe y Colombia a su vez dispone de *retailers* con gran énfasis en el marketing de *wearables*, a diferencia de Brasil, y una penetración de dispositivos relacionados con IoT del 16%, mientras que en Brasil es solo del 10% (IDC). En este sentido, el esfuerzo que se realice en México debe considerar el contexto de aquellas industrias o actividades que son más afines a la adopción de IoT y que este esfuerzo debe partir de un enfoque de múltiples partes interesadas.

- (7) Explorar la posibilidad de elaborar un reglamento para redes de telecomunicaciones dentro de los hogares donde se promueva el Hogar Digital e Inteligente (Smart Home), a través de la armonización de las condiciones para el ingreso de sensores y disminuyendo costos de importación en la medida que se genere un mercado atractivo, se espera que este promueva el desarrollo de redes de banda ancha al hogar propicias para este tipo de servicios y la capacitación de personal idóneo para atender las redes internas.
- (8) Incluir la homologación de equipos de IoT que incluyan el uso de radio frecuencias para verificar que, efectivamente están emitiendo señales dentro de las radiofrecuencias autorizadas. Dicha homologación no debe implicar mayores costos para el proveedor, lo que evitaría el incremento en los precios del usuario final. Una alternativa podría ser adoptar la certificación de homologación del exterior (certificados de tercer parte) expedidos por organismos acreditados.
- (9) Se sugieren acciones específicas como la adopción por parte de los servicios públicos de sensores que optimicen su operación. Por ejemplo, expedir normas para promover el desarrollo y uso del IoT en México para la implementación de dispositivos en los vehículos de transporte público para llamadas de emergencia (eCall) en accidentes de tráfico.
- (10) Fomentar la implementación de un laboratorio de IoT en conjunto con la iniciativa privada y los centros académicos y de investigación del país. El objetivo de este centro, como en otros países, podría ser brindar a los diferentes actores del ecosistema empresarial un ambiente propicio para desarrollar aplicaciones y herramientas con base en tecnología IoT.
- (11) La realización de un diagnóstico sobre los problemas de estandarización de IoT en México y sus posibles soluciones.
- (12) Fomentar la disponibilidad de infraestructura y acceso, tomando en cuenta que las soluciones de IoT pueden requerir de redes de comunicación privadas y públicas, lo que incrementa la demanda de espectro radioeléctrico y de infraestructura de telecomunicaciones.
- (13) Fomentar el despliegue equitativo, tomando en cuenta que el Internet de las cosas podría exacerbar desigualdades existentes proporcionando los beneficios de la toma de decisiones basada en datos solo a algunos, y colocando a las comunidades ya desatendidas en una desventaja aún mayor.
- (14) Colaborar en la generación de políticas de libre flujo de datos a través de las fronteras.
- (15) Participar en la creación de estadísticas para la cuantificación del sector en México.
- (16) Fomentar estrategias para la adopción de IoT por parte de las PyMEs, tomando en cuenta que podrían tener mayor vocación para la adopción de estas tecnologías.

3.

Análisis exploratorio de datos de IoT en México

Esta sección presenta información de los siguientes aspectos:

- | Metodología y aplicación de herramientas de Ciencia de Datos;
- | Proyectos de IoT que se desarrollan en México¹⁷⁵;
- | Análisis exploratorio de los datos obtenidos por *Web Scraping* de las empresas que comercializan servicios de IoT en México;
- | Distribución geográfica de los servicios de IoT en el territorio nacional, y
- | Análisis de clúster de las empresas identificadas.

Metodología y aplicación de herramientas de Ciencia de Datos

La tercera parte de este análisis continua con mejoras en la metodología presentada en el reporte de 2020 sobre el IoT a nivel mundial. Con el objeto de tener información estructurada sobre la comercialización de soluciones IoT en México se utiliza la herramienta de *Web Scraping*, con un nuevo código desarrollado en lenguaje de programación R, el cual se acompañó de otro script para efectos de tener actualizaciones automáticas de los sitios web de las empresas que ofertan conectividad para IoT en México (para mayor detalle sobre el algoritmo utilizado, por favor visite el Anexo 1).

La herramienta de *Web Scraping* ha sido utilizada y aplicada en diversos ámbitos, por ejemplo, en el Reino Unido, la *Office for National Statistics* (ONS) elaboró un algoritmo de *Machine Learning* para clasificar de manera automática la información recopilada mediante el *Web Scraping* de páginas web de comerciantes minoristas, con el fin de producir índices de precios al consumidor. Antes de este algoritmo, se realizaba la extracción de la información de manera manual y podían extraer información de 20,000 productos mensualmente, ahora con el uso del *Web Scraping* y el *Machine Learning*, pueden extraer información de poco más de 900,000 productos únicos mensualmente. Para entrenar el algoritmo, recolectaron y clasificaron datos de manera manual de 50,000 productos, lo que permitió al algoritmo tener un acierto del 88.8%¹⁷⁶.

La *Office for National Statistics* (ONS) de Reino Unido cataloga al *Web Scraping* como un mecanismo alternativo de recopilación de datos que **puede complementar y mejorar las formas tradicionales de recopilación de datos**. Cabe destacar que esta recolección de información produce estadísticas nacionales y permite realizar investigaciones de tipo exploratoria, análisis y asesoramiento para el bien público y para que los gobiernos de la región tomen mejores decisiones. Adicionalmente, la ONS ha elaborado sus propias políticas que establecen las prácticas y los principios que debe seguir su personal para un uso correcto de la técnica y sin perjudicar a ninguna empresa o página web de la cual se va a extraer información¹⁷⁷.

¹⁷⁵ Global Data (2022), *IoT Deployment Tracker*. Disponible en: <https://technology.globaldata.com/Analytics/CompetitorTrackers/IoTDeploymentTracker>. Visitado en mayo de 2022.

¹⁷⁶ Sands, H. (2020), *Automated classification of web-scraped clothing data in consumer price statistics*. Office for National Statistics. Disponible en: <https://www.ons.gov.uk/economy/inflationandpriceindices/articles/automatedclassificationofweb-scrapedclothingdatainconsumerpricestatistics/2020-09-01>

¹⁷⁷ Office for National Statistics. (2020), *Web Scraping Policy*. Disponible en: <https://www.ons.gov.uk/aboutus/transparencyandgovernance/datastrategy/datapolicies/web-scrapingpolicy>

Quizá el caso más conocido del uso de esta herramienta es de la empresa tecnológica Google, que emplea el *Web Crawling* para indexar el contenido de las páginas web en todo Internet para que puedan aparecer en los resultados de su motor de búsqueda. Este proceso lo realiza mediante un algoritmo de rastreo denominado Googlebot. El rastreo de páginas web o *Web Crawling* forma parte del *Web Scraping*, en el cual, los algoritmos rastreadores se conocen como bot, robot o araña¹⁷⁸.

Las herramientas de automatización también pueden utilizarse de forma maliciosa, tal es el caso de algunas redes sociales que se han visto afectadas por personas que usan el *Web Scraping* para extraer información personal de los perfiles de usuarios para crear bases de datos y después compartirlas en Internet, exponiendo a los usuarios a posibles fraudes. El 3 de abril de 2021, el sitio web de noticias *Business Insider* publicó una nota sobre la filtración de datos de más de 530 millones de usuarios, esta información filtrada se había hecho pública en Internet en una base de datos no segura, el problema de filtración se atribuyó a *Scrapers* que se valieron del importador de contactos de una red social para encontrar perfiles de usuarios ingresando números telefónicos aleatorios¹⁷⁹. Actualmente, la red social no permite el *Web Scraping* en su sitio web y cuentan con un equipo de más de 100 personas, que incluye a científicos, analistas e ingenieros de datos enfocados en detectar, bloquear y disuadir el *Web Scraping*¹⁸⁰.

En México, el Consejo Nacional de Ciencia y Tecnología (CONACyT) y el Centro de Investigación y Docencia Económicas (CIDE) crearon en 2015 el Laboratorio Nacional de Políticas Públicas (LNPP), el cual ofrece asesoría técnica y metodológica para el desarrollo de proyectos de Ciencia de Datos que tengan como objetivo generar soluciones a problemas públicos a los diferentes niveles de gobierno, instituciones gubernamentales y a organizaciones nacionales e internacionales, y en su Unidad de Ciencia de Datos (UCD), hacen uso del *Web Scraping* para la creación de bases de datos no estructuradas¹⁸¹.

Por último, a través del proyecto gubernamental *Datalab*¹⁸², el LNPP participó en la investigación sobre agresiones en contra de personas defensoras de derechos humanos y periodistas, para ello elaboraron un algoritmo de *Web Scraping* que les permitió hacer una búsqueda de palabras clave y así recuperar títulos de notas periodísticas, texto, fuente y fecha de todas las notas identificadas como relevantes para su investigación y para la conformación de su base de datos¹⁸³.

Estas aplicaciones sustentan las bondades en uso del *Web Scraping* como una herramienta para recolectar datos que difícilmente se pueden obtener en fuentes oficiales. Para este ejercicio, el *Web Scraping* se complementa con la utilización de una metodología de Ciencia de Datos, *Knowledge Discovery in Databases* (KDD), que se centra en el desarrollo de métodos y técnicas para entender los datos y en la aplicación de métodos de *data mining* en la búsqueda de patrones en las bases de datos.

A diferencia de otras metodologías, el KDD se centra en la búsqueda de patrones entendibles que pueden ser interpretados como conocimiento útil, esta metodología sigue evolucionando junto con las innovaciones en *Machine Learning*, reconocimiento de patrones, bases de datos, estadística no paramétrica, Inteligencia artificial, adquisición de conocimientos, visualización de información y computación de alto desempeño (para mayor detalle consulte el Anexo 2).

¹⁷⁸ Google (2021), *Cómo funciona la Búsqueda de Google*. Disponible en: <https://developers.google.com/search/docs/beginner/how-search-works>

¹⁷⁹ Clark, M. (2021), *Los hechos detrás de la noticia sobre los datos de Facebook*. Disponible en: <https://about.fb.com/ltam/news/2021/04/los-hechos-sobre-la-noticia-de-los-datos-de-facebook/>

¹⁸⁰ Clark, M. (2021), *¿Cómo combatimos el scraping?* Disponible en: <https://about.fb.com/ltam/news/2021/04/como-combatimos-el-scraping/>

¹⁸¹ Laboratorio Nacional de Políticas Públicas (2021), *¿Qué hacemos?* Disponible en: <https://www.lnpp.mx/que-hacemos>

¹⁸² Presidencia de la República EPN. (2017), *Datalab: análisis de datos para políticas públicas basadas en evidencia*. Gobierno de México. Disponible en: <https://www.gob.mx/epn/es/articulos/datalab-analisis-de-datos-para-politicas-publicas-basadas-en-evidencia>

¹⁸³ Unidad de Prevención Seguimiento y Análisis, Coordinación de Estrategia Digital Nacional y Laboratorio Nacional de Políticas Públicas. (2017), *Sistematización, análisis y visualización de agresiones contra personas defensoras de derechos humanos y periodistas*. Laboratorio Nacional de Políticas Públicas. Disponible en: https://www.lnpp.mx/uploads/publications/24_a4b36.pdf

La aplicación de esta metodología es recurrente en muchas áreas de conocimiento, como el *marketing* digital, las finanzas, la detección de fraudes, la manufactura, las telecomunicaciones y en empresas tecnológicas, por citar algunos ejemplos. En el trabajo de Leece (1999) se utiliza la metodología KDD y la visualización de datos para descubrir agrupaciones en la propiedad de activos financieros de riesgo. Los resultados de su investigación muestran que se tienen dos grupos importantes entre los tenedores de activos de riesgo¹⁸⁴. Por su parte, el trabajo de Lima, Mues y Baesens (2009)¹⁸⁵ muestra cómo se puede incorporar los procesos de minería de datos para la predicción de abandono de clientes (*churn*). Lo anterior mediante la evaluación de signos de coeficientes en un modelo de regresión logística y mediante el análisis de una tabla de decisión extraída de un árbol de decisión; además, presentan un algoritmo para verificar las tablas de decisión y evitar una contracción de tablas para detectar patrones contraintuitivos. Los dos enfoques se utilizaron en dos conjuntos de datos de empresas de telecomunicaciones para demostrar empíricamente cómo se aplica la minería de datos y así poder interpretar los resultados.

La metodología KDD requiere elegir una técnica de *data mining* acorde a la información que se tiene, para este análisis, considerando los datos que se tienen, se decidió usar el análisis de clúster, este pertenece al conjunto de técnicas no supervisadas de *Machine Learning*, cuya finalidad es encontrar patrones o grupos (clústeres) dentro de un conjunto de observaciones. Para llevar a cabo la similitud entre las observaciones se necesita emplear el término distancia, que dentro del análisis de clúster se emplea como la cuantificación de la similitud o diferencia entre observaciones¹⁸⁶.

Para esta investigación, se empleó el método de *K-means clustering*, que es un método no jerárquico para agrupar objetos (no variables) que divide el set de datos en clústeres distintos, donde ninguna observación puede pertenecer a más de un clúster¹⁸⁷ (para mayor detalle consulte el Anexo 3).

Figura 3.1. Metodología para el análisis de IoT en México.



Fuente: IFT con información de University of Regina (2018), *Overview of the KDD Process*. Disponible en: http://www2.cs.uregina.ca/~dbd/cs831/notes/kdd/1_kdd.html#:~:text=The%20term%20Knowledge%20Discovery%20in,of%20particular%20data%20mining%20methods.&text=The%20unifying%20goal%20of%20the,the%20context%20of%20large%20databases.

¹⁸⁴ Leece, D. (1999), *Applying Data Visualization and Knowledge Discovery in Databases to Segment the Market for Risky*. Financial. Manage. Decis. Econ. 20. Pág. (267). Disponible en: https://www.jstor.org/stable/pdf/3108110.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A62d09bff98dbf9df4ffa1d9318988967

¹⁸⁵ Lima, E., Mues, E. y Baesens, B. (2009), *Domain knowledge integration in data mining using decision tables: case studies in churn prediction*. Journal of the Operational Research Society. Núm. 60. Pág. (1096). Disponible en: https://www.jstor.org/stable/pdf/40206835.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3Aee6d45ad75a9ace526e4567447e20c02

¹⁸⁶ Amat, J. (2017), *Clustering y heatmaps: aprendizaje no supervisado*. Disponible en: <https://www.cienciadedatos.net/documentos/37-clustering-y-heatmaps>

¹⁸⁷ Gil, C. (2018), *Métodos de Clustering*. Disponible en: https://rpubs.com/Cristina_Gil/Clustering

De manera general, en la Figura 2.1, se describe el proceso de elaboración del análisis, primero se utilizó de base el análisis previo publicado en 2020, después se construyó el nuevo código de *Web Scraping*, con los datos recopilados se realizó un análisis exploratorio de Datos, seguido de un análisis de clúster con *k-means*. Finalmente, utilizando la metodología KDD se realizó un análisis que permitió identificar los patrones de la información.

Proyectos IoT en México

El análisis realizado por el IFT en 2020 documentó la existencia del desarrollo de 14 grandes proyectos de IoT en México. El dato más reciente muestra que el número de proyectos se ha incrementado a un total de 34, con un promedio anual de 3 proyectos desde 2012 a 2021 (ver Tabla 3.1).

La distribución de los referidos proyectos en México se concentra en el seguimiento y monitoreo de vehículos con 12 proyectos, seguido por el monitoreo de equipamiento industrial (9), monitoreo de personas (4) y la gestión de recursos naturales (4). Este dato permite corroborar que el segmento automotriz es para México una fuerte industria de soporte para el desarrollo del IoT.

Tabla 3.1. Distribución total de proyectos IoT en México.

Año	Nombre del Proyecto	Sector	Oferente	Servicio	Dispositivos conectados	Tipo de conectividad
2021	Siemens: Monitoreo ¹⁸⁸ de Energía	Equipamiento	Besser Lighting, Dhyan	Monitoreo de Condiciones	100 - 499	Corto alcance, baja potencia
	Metro Ciudad de México ¹⁸⁹ : Monitoreo de Equipamiento	Equipamiento	Advantech	Pagos Inteligentes	< 100	Corto alcance, baja potencia
	Prologis ¹⁹⁰ : Seguimiento de Vehículos	Vehículos	Nedap, ASPI Systems	Edificios Inteligentes	< 100	Celular
2020	Nafta Frigo ¹⁹¹ : Monitoreo y Seguimiento de Otros Activos	Logística	Roambee	Seguimiento de Activos	< 100	Narrowband IoT (NB-IoT)
	Newmont ¹⁹² : Monitoreo de Personas	Personas	HID Global, Alutel Mobility	Monitoreo de Personas	> 10,000	Corto alcance, baja potencia
	Orbia Advance Corporation ¹⁹³ : Monitoreo de Equipamiento	Equipamiento	SAP	Monitoreo de Condiciones	< 100	Celular
	Cruz Roja Mexicana ¹⁹⁴ : Seguimiento y Monitoreo de Vehículos	Vehículos	Samsara	Telemática	< 100	Satélite

¹⁸⁸ Para más información de este proyecto visite: <https://www.dhyan.com/resources/success-stories/siemens/>

¹⁸⁹ Para más información de este proyecto visite: <https://www.advantech.com/resources/case-study/building-reliable-and-efficient-ticket-vending-machines-in-the-mexico-metro>

¹⁹⁰ Para más información de este proyecto visite: <https://www.nedapidentification.com/wp-content/uploads/2021/07/Prologis-Mexico-chooses-Nedaps-ANPR-LUMO-for-admission-to-their-industrial-parks.pdf>

¹⁹¹ Para más información de este proyecto visite: <https://enterpriseiotinsights.com/20201015/channels/fundamentals/vehicles-to-vaccines-five-key-asset-tracking-use-cases>

¹⁹² Para más información de este proyecto visite: https://www.hidglobal.com/doclib/files/resource_files/newmont-cs-final-eng.pdf

¹⁹³ Para más información de este proyecto visite: <https://www.sap.com/documents/2020/06/8cca5899-9d7d-0010-87a3-c30de2ffd8ff.html>

¹⁹⁴ Para más información de este proyecto visite: <https://www.samsara.com/customers/cruz-roja>

Año	Nombre del Proyecto	Sector	Oferente	Servicio	Dispositivos conectados	Tipo de conectividad
2020	OnStar Corporation ¹⁹⁵ : Seguimiento y Monitoreo de Vehículos	Vehículos	Telefónica	Telemática	> 10,000	Celular
	Eurotranciatra Mexico ¹⁹⁶ : Monitoreo de Equipamiento	Equipamiento	Plex System, SCM Malagón & Asociados	Automatización Avanzada	< 100	Corto alcance, baja potencia
	Ciudad de León ¹⁹⁷ : Monitoreo ambiental	Recursos Naturales	Urbiotica	Ciudades Inteligentes	100 – 499	Corto alcance, baja potencia
	Michelin Car Centers ¹⁹⁸ : Seguimiento y Monitoreo de Vehículos	Vehículos	CalAmP	Telemática	100 – 499	Celular
2019	Tequila, Jalisco ¹⁹⁹ : Monitoreo de Infraestructura Civil	Monitoreo Obras Civiles	Hitachi	Ciudades Inteligentes	< 100	Corto alcance, baja potencia
	LIMRE ²⁰⁰ : Seguimiento y Monitoreo de Vehículos	Vehículos	Samsara	Telemática	< 100	Satélite
	Braskem ²⁰¹ : Monitoreo de Equipamiento	Vehículos	Honeywell	Publicidad Inteligente (Smart Signage)	< 100	Corto alcance, baja potencia
	Grupo Bafar ²⁰² : Monitoreo de Otros Activos	Monitoreo Industrial	SAP	Seguimiento de Activos	< 100	Conectividad Alámbrica
2018	Mina San Juan ²⁰³ : Monitoreo de Equipamiento	Equipamiento	Azima	Monitoreo de Condiciones	100 – 499	Corto alcance, baja potencia
	Torre Anseli ²⁰⁴ : Control de edificios y monitoreo	Edificios	OTI	Edificios Inteligentes	< 100	Conectividad Alámbrica
	Ana Seguros ²⁰⁵ : Monitoreo de Vehículos	Vehículos	Octo Telematics, Software AG	Telemática	2,500 - 4,999	Celular
	Siemens ²⁰⁶ : Monitoreo de Equipo	Equipamiento	Amazon Web Services	Monitoreo de Condiciones	< 100	Corto alcance, baja potencia
	BANOBRAS ²⁰⁷ : Monitoreo de Vehículos	Vehículos	SICE, OCACSA-GAMI	Sistemas de pago inteligentes	< 100	Conectividad Alámbrica

¹⁹⁵ Para más información de este proyecto visite: <https://www.telefonica.com.mx/prensa/2017/marzo/onstar-selecciona-a-telefonica-como-proveedor-para-ofrecer-4g-lte-en-vehiculos-general-motors>

¹⁹⁶ Para más información de este proyecto visite: <https://www.plex.com/company/customers/how-to-improve-inventory-accuracy>

¹⁹⁷ Para más información de este proyecto visite: <https://blogs.uoregon.edu/4523su20/2020/07/24/research-1-smart-cities-and-shared-streets-2/>

¹⁹⁸ Para más información de este proyecto visite: <https://investor.calamp.com/press-releases/press-release-details/2020/CalAmps-LoJack-Mexico-Partners-with-GNP-to-Combat-Car-Theft-Across-Mexico/default.aspx>

¹⁹⁹ Para más información de este proyecto visite: https://social-innovation.hitachi/en/case_studies/tequila_inteligente

²⁰⁰ Para más información de este proyecto visite: <https://www.samsara.com/customers/liimre>

²⁰¹ Para más información de este proyecto visite: <https://www.honeywell.com/us/en/press/2019/08/honeywell-helps-transform-mexican-petrochemical-leaders-operations>

²⁰² Para más información de este proyecto visite: <https://www.sap.com/documents/2019/08/7461464c-607d-0010-87a3-c30de2ffd8ff.html>

²⁰³ Para más información de este proyecto visite: <https://symphonyazimaai.com/wp-content/uploads/San-Juan-Coal-Mine.pdf>

²⁰⁴ Para más información de este proyecto visite: <https://www.otipro.com/torre-anseli>

²⁰⁵ Para más información de este proyecto visite: <https://www.octotelematics.com/blog/ana-seguros-chooses-octo-telematics-for-fleet-telematics/>

²⁰⁶ Para más información de este proyecto visite: <https://aws.amazon.com/es/blogs/apn/case-study-siemens-factory-rolls-out-aws-iiot-project-in-less-than-8-weeks/>

²⁰⁷ Para más información de este proyecto visite: <https://transparencia.banobras.gob.mx/wp-content/uploads/2017/08/79-FID-1936-PDAL-02012017.pdf>

Año	Nombre del Proyecto	Sector	Oferente	Servicio	Dispositivos conectados	Tipo de conectividad
2017	CONAPESCA ²⁰⁸ : Seguimiento y Monitoreo de Vehículos	Vehículos	ORBCOMM, Astrum Satelita	Telemática	< 100	Satélite
	SkyAlert ²⁰⁹ : Monitoreo de Recursos Naturales	Recursos Naturales	Microsoft	Ciudades Inteligentes	< 100	Corto alcance, baja potencia
	Grupo Crio ²¹⁰ : Seguimiento y Monitoreo de Vehículos	Vehículos	Geotab	Telemática	100 - 499	Satélite
2016	Aguas de Saltillo ²¹¹ : Seguimiento y Monitoreo de Recursos Naturales	Recursos Naturales	Inductive Automation	Monitoreo de Condiciones	5,000 - 9,999	Conectividad Alámbrica
	Toreo Parque Central ²¹² : Monitoreo de Equipamiento	Equipamiento	Intelli Site Solutions, JMA Wireless	Monitoreo de Condiciones	< 100	Celular
2015	Tren Ligero de la Ciudad de México: Monitoreo de Vehículos	Vehículos	Bombardier, Ikusi, Cisco	Edificios Inteligentes	< 100	Corto alcance, baja potencia
	Comisión Federal de Electricidad ²¹³ : Control y Monitoreo de Equipo	Equipamiento	Freewave	Medición Inteligente	1,000 - 2,499	Celular
	Nube ²¹⁴ : Monitoreo de Recursos Naturales	Recursos Naturales	Sierra Wireless	Monitoreo de Condiciones	500 - 999	Celular
	Ciudad de México ²¹⁵ : Monitoreo de Recursos Naturales	Recursos Naturales	Silver Spring Networks, Tecnologías EOS	Medición Inteligente	500 - 999	Corto alcance, baja potencia
	Aeropuerto Internacional de Cancún: Monitoreo de Personas	Personas	ST Electronics	Ciudades Inteligentes	< 100	Celular
	Aeropuerto Internacional de Cozumel: Monitoreo de Personas	Personas	ST Electronics	Ciudades Inteligentes	< 100	Celular
2014	Stanley Black & Decker ²¹⁶ : Monitoreo de Equipamiento	Equipamiento	Cisco, AeroScout	Automatización Avanzada	< 100	Celular
2013	Instituto de la Salud Carlos Slim ²¹⁷ : Monitoreo de Personas	Personas	Treeline Interactive	Salud	100 - 499	Corto alcance, baja potencia
2012	Promofront: Seguimiento de Vehículos	Vehículos	Impinj, CADi	Seguimiento de Activos	< 100	Corto alcance, baja potencia

Fuente: IFT con información de Global Data (2022), *IoT Deployment Tracker*. Disponible en: <https://technology.globaldata.com/Analytics/CompetitorTrackers/IoTDeploymentTracker>

²⁰⁸ Para más información de este proyecto visite: <https://www.orbcomm.com/pdf/casestudies/VMS-Astrum-CS.pdf>

²⁰⁹ Para más información de este proyecto visite: <https://customers.microsoft.com/en-gb/story/sky-alert>

²¹⁰ Para más información de este proyecto visite: <https://www.geotab.com/case-study/grupo-crio-ensuring-driver-safety/>

²¹¹ Para más información de este proyecto visite: <https://inductiveautomation.com/resources/casestudy/water-agency-welcomes-the-future-with-ignition>

²¹² Para más información de este proyecto visite: <https://www.rcrwireless.com/20160411/network-infrastructure/das-case-study-connected-toreo-parque-central-mexico-city-tag17>

²¹³ Para más información de este proyecto visite: <https://www.freewave.com/wp-content/uploads/2018/12/case-study-smart-grid.pdf>

²¹⁴ Para más información de este proyecto visite: <https://www.sierrawireless.com/company/newsroom/pressreleases/2017/10/nube-selects-sierra-wireless-and-microsoft-azure-cloud-services-to-reinvent-gas-delivery/>

²¹⁵ Para más información de este proyecto visite: <https://www.itron.com/na/company/newsroom/2017/05/17/silver-spring-networks-expands-smart-grid-program-in-mexico-city>

²¹⁶ Para más información de este proyecto visite: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/c36-732293-00-stanley-cs.pdf

²¹⁷ Para más información de este proyecto visite: <https://treelineinteractive.com/case-study/westwireless>

En esta actualización se encontró que el proyecto más grande en cuanto al número de dispositivos conectados es el de OnStar Corporation, en colaboración con Telefónica, que tiene como objetivo el seguimiento y monitoreo de 125,000 vehículos. El segundo proyecto más grande es el de Newmont, el cual busca monitorear el control de acceso de 19,800 personas en diversas minas ubicadas en Zacatecas, México. En tercer lugar, se encuentra el proyecto de Aguas de Saltillo que monitorea a 7,500 dispositivos encargados del monitoreo de la extracción y distribución de agua. En cuarto sitio, el proyecto con el mayor número de dispositivos conectados corresponde a la Comisión Federal de Electricidad que tiene como objetivo proporcionar comunicación M2M para aplicaciones de *Smart Grid* con un intervalo de dispositivos conectados de entre 1,000 y 2,499.

En una encuesta realizada por OMDIA durante 2021, se encontró que el 47% de los proyectos IoT a nivel mundial se aceleraron, aunque el 30% de este mismo universo se detuvo o pospuso. Los proyectos de IoT que aceleraron su implementación fueron aquellos relacionados con servicios públicos, energía, logística, cadena de suministro, comercio al por menor y hospitalidad. En contraste, las áreas agrícolas y cuidado de la salud disminuyeron su crecimiento. En cuanto al número de dispositivos conectados, la encuesta de OMDIA muestra que el 64% de las empresas conectan menos de 1,000 dispositivos, mientras que, el 25% desarrollan proyectos con menos de 500 dispositivos conectados²¹⁸.

Con esta tendencia, se confirma un cambio en el número de dispositivos conectados en los proyectos IoT en México, el 62% de los proyectos (21 de 34) prevén la conexión de menos de 100 dispositivos (ver Gráfica 3.1), mientras que en el análisis de 2020 este porcentaje representaba el 71% de los proyectos documentados en México.

Gráfica 3.1. Distribución total de proyectos de IoT en México por el número de dispositivos conectados



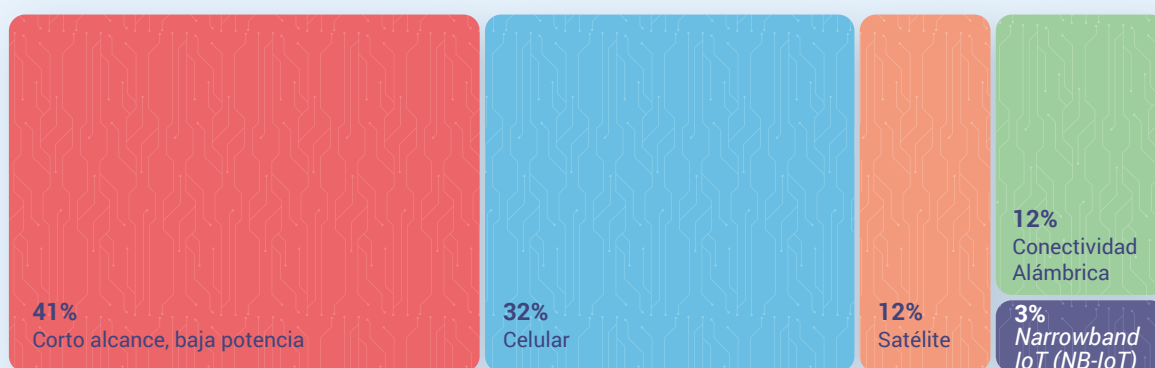
Fuente: IFT con información de Global Data (2022), *IoT Deployment Tracker*. Disponible en: <https://technology.globaldata.com/Analytics/CompetitorTrackers/IoTDeploymentTracker>

²¹⁸ OMDIA (2021), *IoT Enterprise Survey: Summary Report – 2021*. Pág. (11). Disponible en: <https://omdia.tech.informa.com/OM016688/IoT-Enterprise-Survey-Summary-Report--2021>

En cuanto a la conectividad utilizada por los proyectos de IoT en México, un gran porcentaje utiliza tecnologías de Corto alcance y baja potencia (41%), seguido de redes Celulares (32%) y de conectividad Satelital y Alámbrica (12% cada una) (ver Gráfica 3.2). Se identificó también un proyecto que utiliza NB-IoT para el monitoreo de activos de al menos 50 dispositivos.

Adicionalmente, se confirma que la conectividad móvil aumentó su uso como tecnología para el despliegue de proyectos IoT en México, pasando de 4 a 11 proyectos en el periodo comprendido entre 2020 y 2021, respectivamente.

Gráfica 3.2. Distribución total de proyectos de IoT en México por conectividad utilizada



Fuente: IFT con información de Global Data (2022), *IoT Deployment Tracker*. Disponible en: <https://technology.globaldata.com/Analytics/CompetitorTrackers/IoTDeploymentTracker>

Desarrollos tecnológicos clave para el desarrollo de IoT²¹⁹.

De acuerdo con Global Data, existen cuatro tecnologías clave que permitirán un mayor desarrollo del ecosistema de IoT:

- Inteligencia Artificial (IA): Beneficiará al sector de IoT con “inteligencia-optimización” mediante el análisis y toma de decisiones de datos en tiempo real.
- Computo en la nube (*Cloud computing*): El uso de la nube permitiría que IoT sea flexible mediante acceso bajo demanda de recursos computacionales.
- Ciberseguridad: El IoT deber ser seguro y prevenir ataques digitales en dispositivos, redes, aplicaciones e información.
- 5G: Medio de comunicación necesario por sus características tecnológicas como mayor ancho de banda, mayor velocidad de red, baja latencia y mayor número de datos²²⁰.

²¹⁹ Global Data (2021), *Thematic Research: Internet of Things (2021)*. Pág. (9). Disponible en: <https://technology.globaldata.com/Analysis/Details/thematic-research-internet-of-things-2021>

²²⁰ Para más información sobre los beneficios de la tecnología inalámbrica 5G, por favor visite: <https://sensor5g.ift.org.mx/Beneficios>

Comercialización de los servicios de IoT en México

Para identificar las empresas que proveen soluciones IoT en México, se utilizó información pública obtenida mediante el algoritmo desarrollado para efectos de aplicar el *Web Scraping*. Este código se realizó mediante el *software* R-Studio con la librería RSelenium para automatizar el control del buscador de Google y también para extraer el código fuente y la dirección (URL) de las páginas web (Anexo 1).

De los resultados del *Web Scraping* se extrajo una gran cantidad de información respecto a las direcciones web de las empresas de IoT, debido a la complejidad en la programación y heterogeneidad en las estructuras de los sitios web, realizar un *Web Scraping* a cada página de manera automática podría significar una pérdida de información por lo que se optó por visitar los sitios web para identificar a las empresas que ofrecen servicios de IoT en México y que tuvieran presencia física en el país; es decir, confirmar una dirección para poder localizarlas.

Esto dio como resultado una base de datos con información de 176 empresas en México, estas empresas cuentan con presencia en diferentes estados del país, para este estudio consideramos este aspecto geográfico y cada localización es tomada en cuenta como una observación o empresa individual, esto resulta en la información de 270 empresas, que se clasificaron en 5 categorías dependiendo del tipo de empresa y cómo se incorpora cada empresa en los diferentes eslabones de la cadena de valor de la industria del IoT:

1. **Proveedor de conectividad:** Se definen como proveedores de conectividad a través de espectro libre, operadores móviles, proveedores de Internet, operadores móviles virtuales, entre otros.
2. **Proveedor de *software*:** Se definen como desarrolladores de aplicaciones.
3. **Proveedor de *hardware*:** Se definen como proveedores de sensores, actuadores y dispositivos IoT.
4. **Otros mercados laterales:** Estas empresas se dedican a otros servicios relacionados con IoT, como la analítica de datos, ciberseguridad, diseño de productos IoT, publicidad, productores de chip, servicios de consultoría y otros servicios especializados²²¹.
5. **Proveedor extremo a extremo:** Este tipo de empresas son aquellas que además de proveer la plataforma de IoT, integran la oferta de conectividad, *software*, *hardware* y otros mercados lateral en el mismo servicio.

En una encuesta realizada por OMDIA, se estima que el 62% de las empresas mencionaron que los servicios de consultoría IoT han participado en el desarrollo de una solución al interior de éstas. En cuanto al crecimiento del mercado de consultoría IoT en términos de beneficios económicos, se espera una tasa de crecimiento compuesta (CAGR) de 16.1% entre 2021 y 2026, pasando a un valor económico de US\$22,500 millones a US\$63,400 millones²²².

²²¹ Cabe destacar que durante la revisión de los sitios web de las empresas que ofrecen servicios de IoT en México se ha observado un incremento de la categoría de otros mercados laterales, por lo que esta categoría será incluida en la clasificación. Para mayor información consulte: Evans, D. (2003), *The antitrust economics of multi-sided platform markets*. Yale Journal of Regulation, 20(2). Pág. (325-381). Disponible en: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1144&context=yjreg>

²²² OMDIA (2021), *IoT Consultancy – 2021 Analysis*. Pág. (4-5). Disponible en: <https://omdia.tech.informa.com/OM018686/IoT-Consultancy--2021-Analysis>

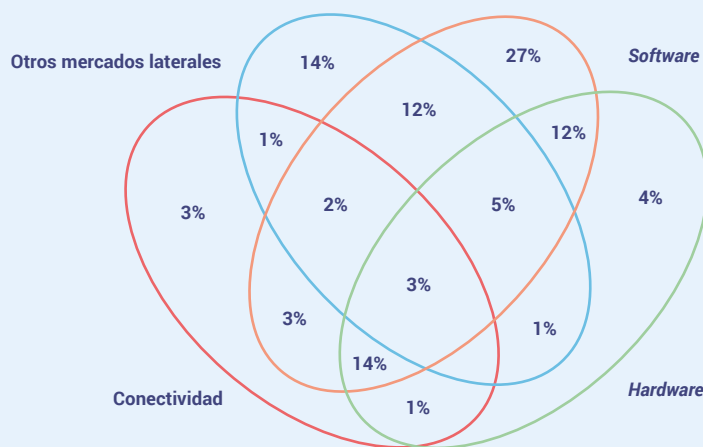
En cuanto a los precios de los servicios de IoT, se encontró que **sólo 17 del total de empresas (9.7% del total) publican el precio tanto de los dispositivos IoT como de las SIMs que se utilizan para el segmento de conectividad.** En su mayoría, los sitios de estas páginas pueden ser catalogadas como tiendas en línea, que ofrecen su catálogo de dispositivos IoT a través de venta directa por Internet.

En México la oferta de servicios asociada a los mercados de IoT se encuentra fragmentada alineándose a la tendencia mundial identificada en 2020. El 47.2% de las empresas identificadas se dedican a un solo servicio (equivalente a 83 de las 176). De este subconjunto, el 26.7% ofrecen sólo servicios de *Software* (47 empresas), el 13.6% ofrece servicios en otros mercados laterales como ciberseguridad IoT, analítica de datos y servicios de consultoría (23 empresas), por su parte, el 4% sólo provee *Hardware* y un 2.8% se dedican a Conectividad (5 empresas).

Respecto a las combinaciones o combos de los servicios provistos (*Hardware*, *Software*, Conectividad, y otros mercados laterales), destacan los paquetes de Conectividad, *Hardware* y *Software* con un 13.6%, por su parte, las combinaciones de *Software* y *Hardware*, así como la combinación de *Software*, *Hardware* y otros mercados laterales suman un 11.9% (21 empresas) de participación, respectivamente. Finalmente, el 2.8% ofrecen servicios de extremo a extremo (5 empresas).

De los sitios web de las empresas que ofrecen servicios de IoT en México existe una diversidad respecto al tipo de empresas que ofrecen IoT. En el ecosistema mexicano, se identifican operadores móviles y virtuales; productores de sensores, proveedores de dispositivos o actuadores; proveedores de aplicaciones, entre otros. Del mismo modo, la diversidad también se encuentra en los protocolos y tecnologías que utilizan las empresas para ofrecer servicios de IoT en México.

Gráfica 3.3. Porcentaje de empresas que se dedican a un solo mercado de IoT en México.

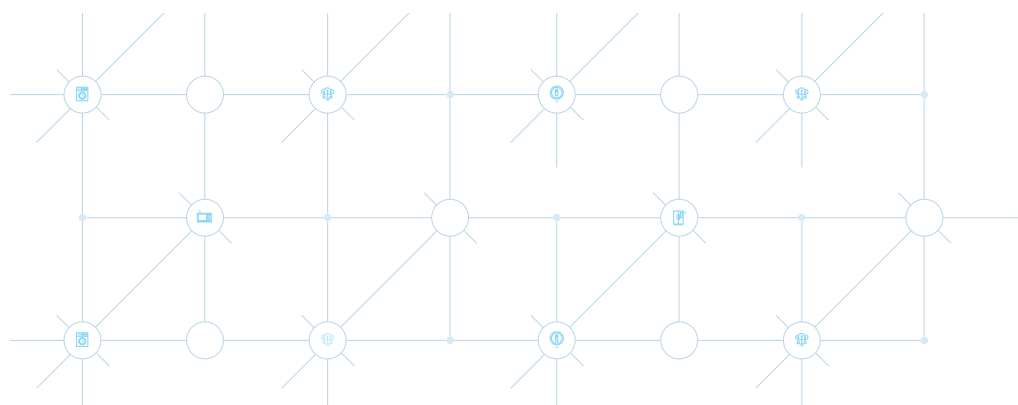


Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Nota: Cabe destacar que la combinación entre los servicios (*Hardware*, Conectividad y Otros mercados laterales) no tiene observaciones.

Los 176 participantes en el entorno del IoT en México tienen diversos sectores de interés o especialidad. Una vez analizados los principales sectores a los que se dirigen sus ofertas, se encontró que existen 22 actividades específicas que son más comunes²²³.

Entre las ofertas comerciales se puede observar una tendencia hacia los sectores terciario y secundario de la economía, **con un énfasis en los servicios relacionados con la industria manufacturera y el seguimiento y gestión de activos (Ver Gráfica 3.4)**. De igual manera, se destacan los servicios dirigidos a la defensa, seguridad y control de acceso, servicios dedicados para ciudades inteligentes y para servicios públicos. Un caso de importancia son las ofertas dirigidas al **sector automotriz**, que si bien, al segundo trimestre de 2022, contribuye al 16.9% del PIB manufacturero y el 2.8% del PIB nacional²²⁴, es uno de los sectores con menor número de ofertas comerciales encontradas para el caso mexicano, situación que llama la atención considerando que este sector es muy activo en la adopción de soluciones de IoT.

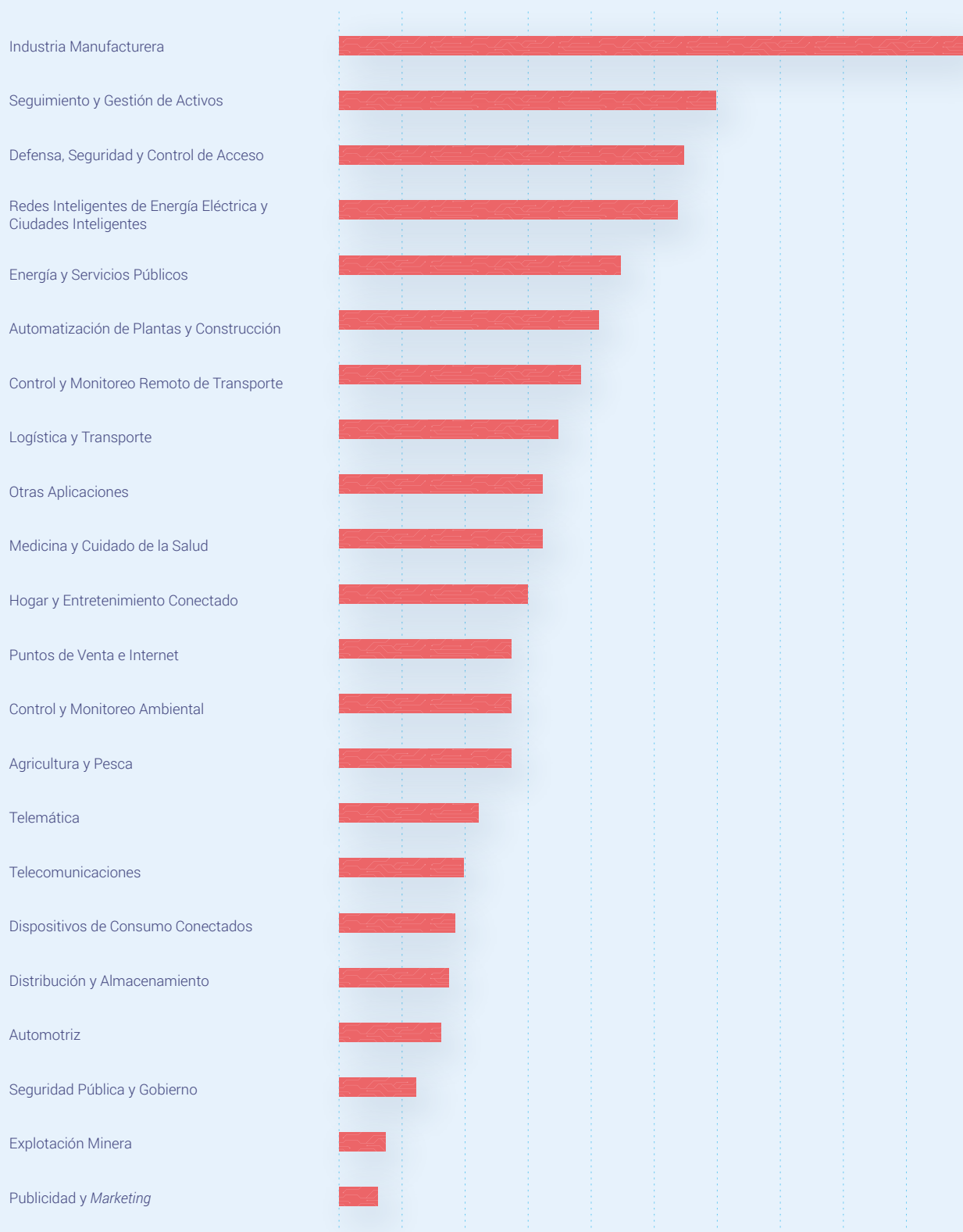


²²³ Actividades por orden alfabético

- i. Agricultura y Pesca;
- ii. Automatización de Plantas y Construcción;
- iii. Automotriz;
- iv. Control y Monitoreo Ambiental;
- v. Control y Monitoreo Remoto;
- vi. Defensa, Seguridad y Control de Acceso;
- vii. Dispositivos de Consumo Conectados;
- viii. Distribución y Almacenamiento;
- ix. Energía y Servicios Públicos;
- x. Explotación Minera;
- xi. Hogar y Entretenimiento Conectado;
- xii. Industria Manufacturera;
- xiii. Logística y Transporte;
- xiv. Medicina y Cuidado de la Salud;
- xv. Otras Aplicaciones;
- xvi. Publicidad y Marketing;
- xvii. Puntos de Venta e Internet;
- xviii. Redes Inteligentes de Energía Eléctrica y Ciudades Inteligentes;
- xix. Seguimiento y Gestión de Activos;
- xx. Seguridad Pública y Gobierno;

²²⁴ Se consideró la suma de las subramas Fabricación de automóviles y camiones y Fabricación de partes para vehículos automotores de INEGI (2022), *Producto Interno Bruto Trimestral por actividad económica*. Disponible en: <https://www.inegi.org.mx/temas/pib/#Tabulados>

Gráfica 3.4. Frecuencia de ofertas de los servicios IoT disponibles en línea en México

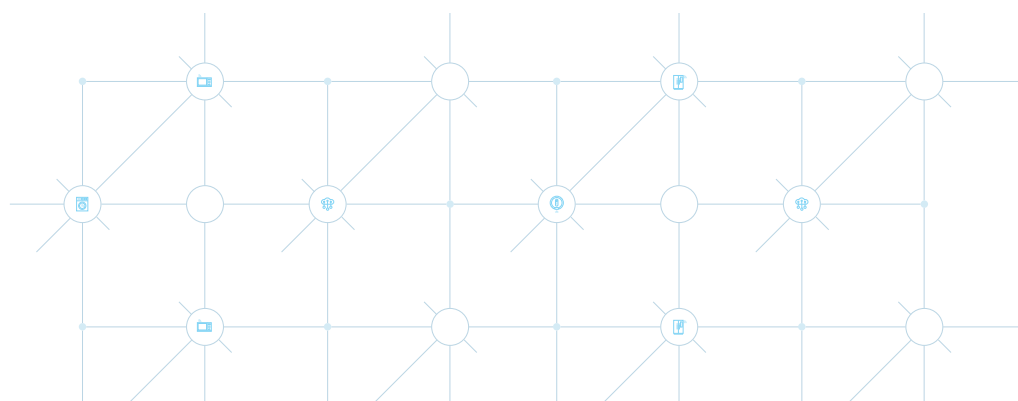


Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*. Otras aplicaciones incluyen: Paneles solares, Recursos hidráulicos, Explotación de petróleo y gas, Máquinas de juego, Cámaras de velocidad, Rastreo de mascotas, Monitoreo de centros de datos.

Asimismo, con la información disponible dentro de las páginas de Internet de las empresas que ofrecen servicios IoT en México por perfil o tipo de clientes se pudieron identificar 16 de las 17 categorías encontradas en el análisis de 2020²²⁵. Es decir, en México existe una oferta comercial de soluciones de IoT similar a la internacional, con excepción de un tipo de aplicación que no fue posible encontrar en la información disponible en línea para México: Plataformas de servicios de entrega.

Como se aprecia en la Gráfica 3.5, los clientes de las empresas identificadas a través del *Web Scraping* se agrupan principalmente en **clientes relacionados con servicios de control y manejo de información y sistemas, de administración de dispositivos, seguido de servicios profesionales para el desarrollo de *Software y Hardware*, y plataformas de inteligencia de negocio y analítica.**

Como se puede ver a continuación, los sectores donde se detecta un mayor interés por el desarrollo de proyectos de IoT coinciden con aquellos que tienen mayor participación en el PIB de México: Sector Terciario (63.7% del PIB al segundo trimestre de 2022) y Sector Secundario (28.6%)²²⁶.

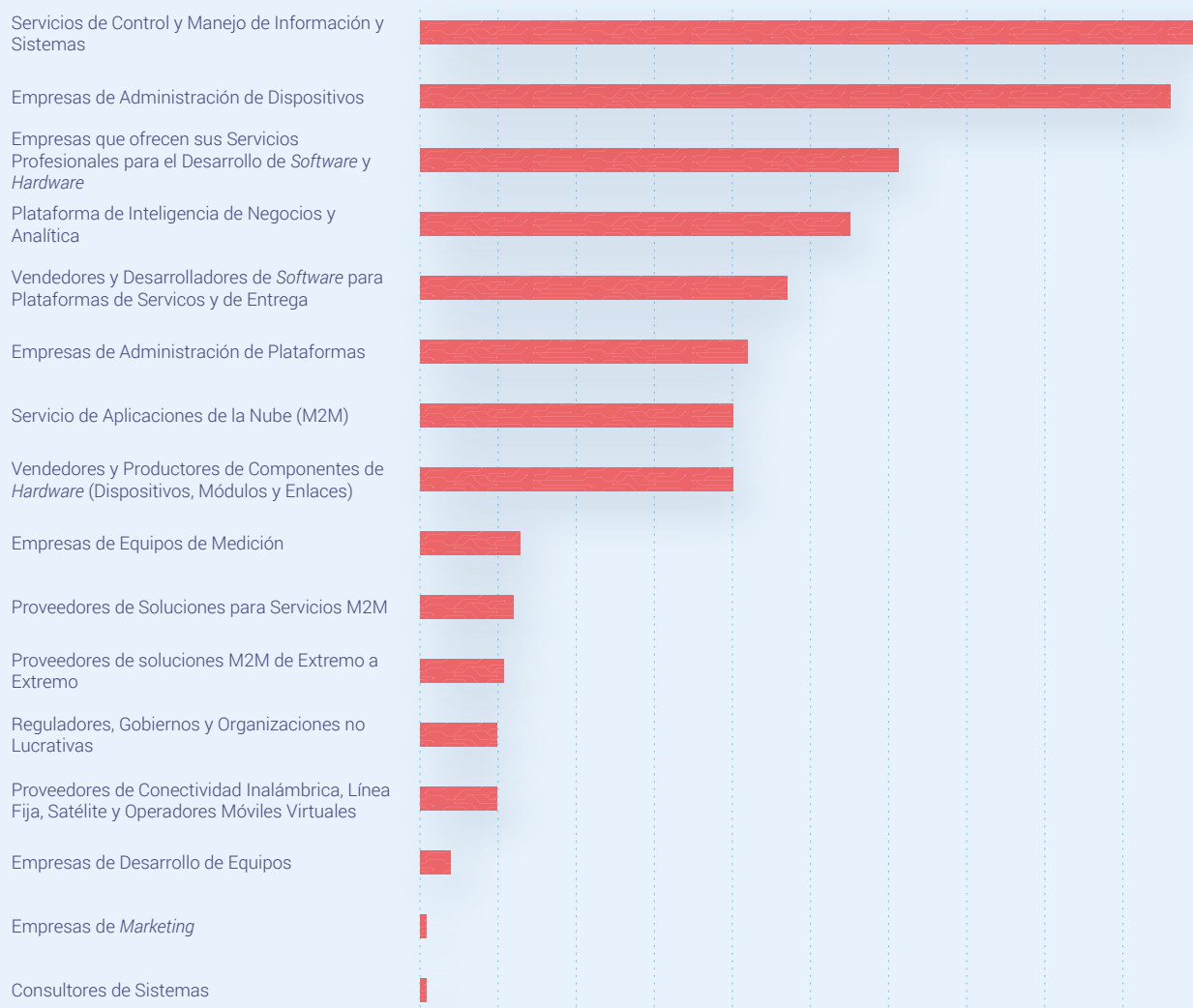


²²⁵ Las ofertas comerciales que fue posible confirmar en México y que ya habíamos identificado internacionalmente son:

- | | | |
|--|---|---|
| 1. Consultores de Sistemas; | 7. Plataforma de Inteligencia de Negocios y Analítica; | 12. Reguladores, Gobiernos y Organizaciones no Lucrativas; |
| 2. Empresas de Administración de Dispositivos; | 8. Plataformas de Servicio de Entrega; <i>Software</i> para Manejo de Dispositivos; | 13. Servicio de Aplicaciones en la Nube (M2M); |
| 3. Empresas de Administración de Plataformas de Negocios; | 9. Proveedores de Conectividad, Inalámbrica, Línea Fija, Satélite y Operadores Móviles Virtuales; | 14. Servicios de Control y Manejo de Información y Sistemas; |
| 4. Empresas de Desarrollo de Equipos; Empresas de Equipos de Medición; | 10. Proveedores de Soluciones M2M de Extremo a Extremo; | 15. Vendedores y Desarrolladores de <i>Software</i> para Plataformas de Servicio de Entrega, y |
| 5. Empresas de <i>Marketing</i> ; | 11. Proveedores de Soluciones para Servicios M2M; | 16. Vendedores y Productores de Componentes de <i>Hardware</i> (Dispositivos, Módulos y Enlaces). |
| 6. Empresas que ofrecen sus Servicios Profesionales para el Desarrollo de <i>Software y Hardware</i> | | |

²²⁶ INEGI (2022), *Producto Interno Bruto Trimestral por actividad económica*. Disponible en: <https://www.inegi.org.mx/temas/pib/#Tabulados>

Gráfica 3.5. Frecuencia de ofertas por perfiles y tipo de clientes en México



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

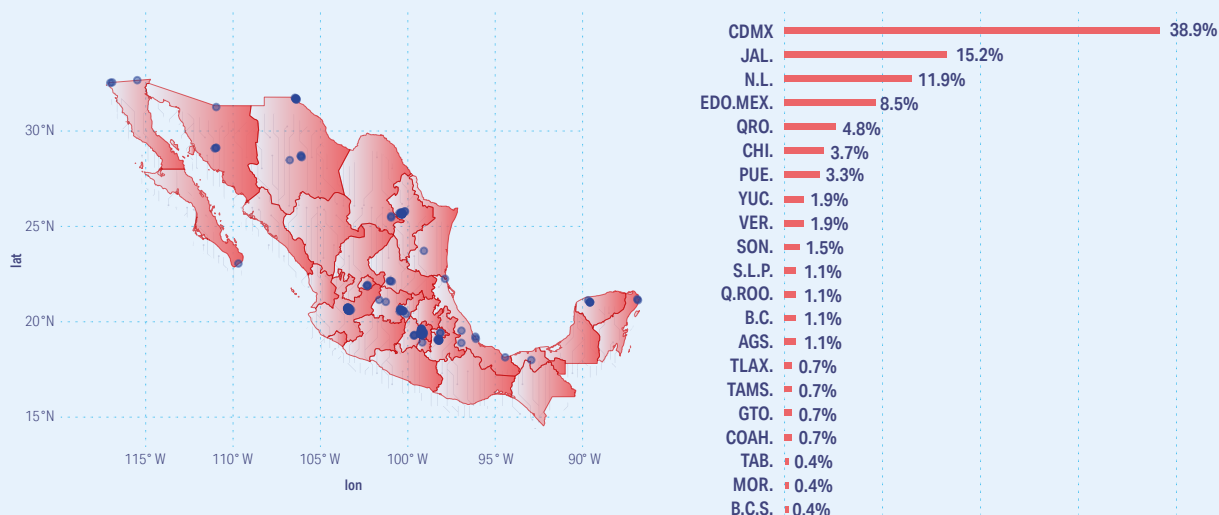
Aunado a lo anterior y con el objetivo de identificar patrones en la distribución y localización geográfica de las empresas de IoT que fueron exploradas mediante la técnica de *Web Scraping*, se obtuvo la dirección que la compañía proporciona en su página electrónica (*v.gr.* calle, código postal, ciudad y país). Con esta información, se utilizó la interfaz de programación de aplicaciones (API) de Google Maps²²⁷ y se gestionaron los datos de manera automatizada con la función Geocode para el lenguaje R²²⁸, para finalmente obtener las coordenadas cartesianas de localización de cada empresa en términos de latitud y longitud decimal, con el fin de crear un *locus* geográfico específico.

²²⁷ Para más información visite: <https://developers.google.com/maps/documentation>

²²⁸ La documentación está disponible en: <https://www.rdocumentation.org/packages/ggmap/versions/2.6.1/topics/geocode>

El resultado del proceso anterior nos permite presentar el mapa 3.1, donde se puede ver que a nivel nacional las empresas que ofrecen servicios de IoT se encuentran en 21 de los 32 estados del país, concentrándose principalmente en la Ciudad de México (38.9%), Jalisco (15.2%), Nuevo León (11.9%) y el Estado de México (8.5%), con presencia también en Querétaro (4.8%) y Chihuahua (3.7%).

Mapa 3.1. Localización de las empresas que ofrecen servicios IoT en México a nivel nacional

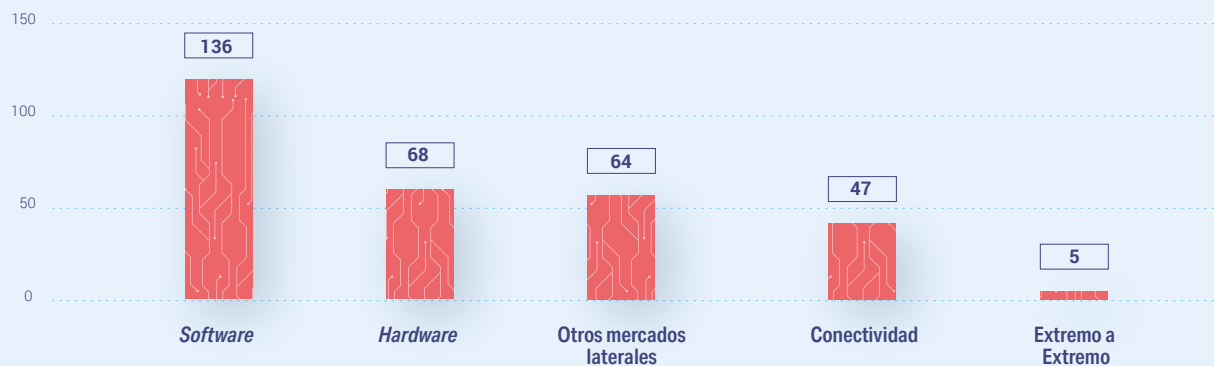


Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Nota: Para la presencia estatal de las 176 empresas que ofrecen servicios de IoT se utilizaron las distintas localizaciones de estas, lo que resulta en un total de 270 observaciones.

Como señalamos previamente, las 176 empresas se distribuyen en función del tipo de servicio que ofrecen de la siguiente forma, tal y como ilustra la gráfica 3.6:

Gráfica 3.6. Total de empresas por categoría de servicio.



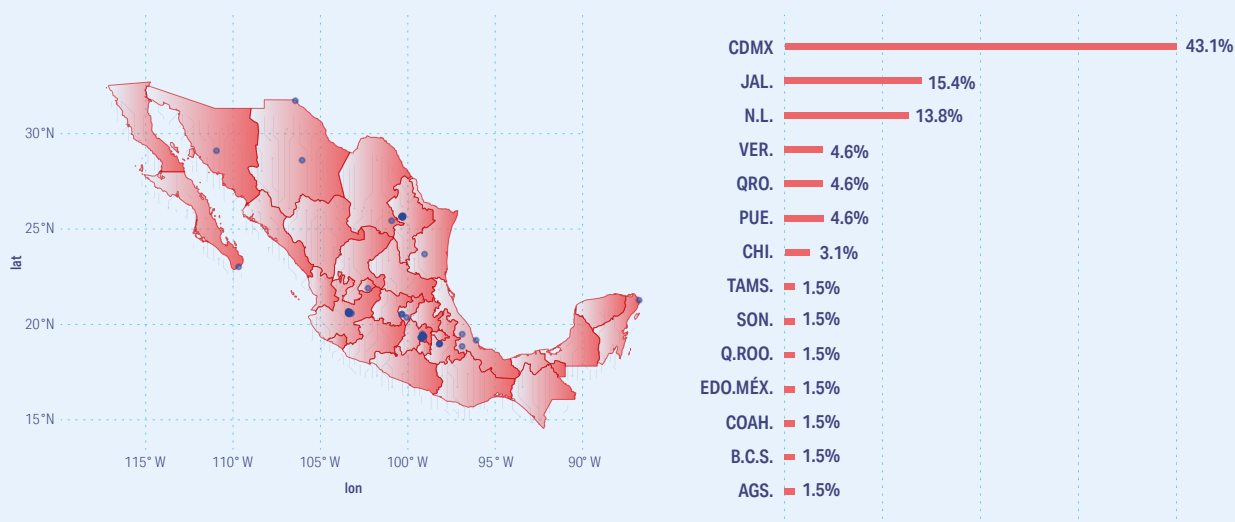
Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Nota: Se consideró el total de empresas por cada categoría, incluyendo si ofrecen más de un servicio.

Continuando con la localización de las empresas que ofrecen servicios IoT en México, una pregunta que surge es cómo se distribuyen estos modelos de negocio en todo el país basados en la información obtenida.

En cuanto a las empresas que ofrecen exclusivamente servicios de conectividad (ver Mapa 3.2), se encontró presencia en 14 de los 32 estados del país, destacando una mayor concentración en la Ciudad de México, Jalisco y Nuevo León. Otras empresas con vocación para ofrecer servicios de conectividad para IoT se encuentran en Veracruz, Querétaro, Puebla, Chihuahua y Tamaulipas.

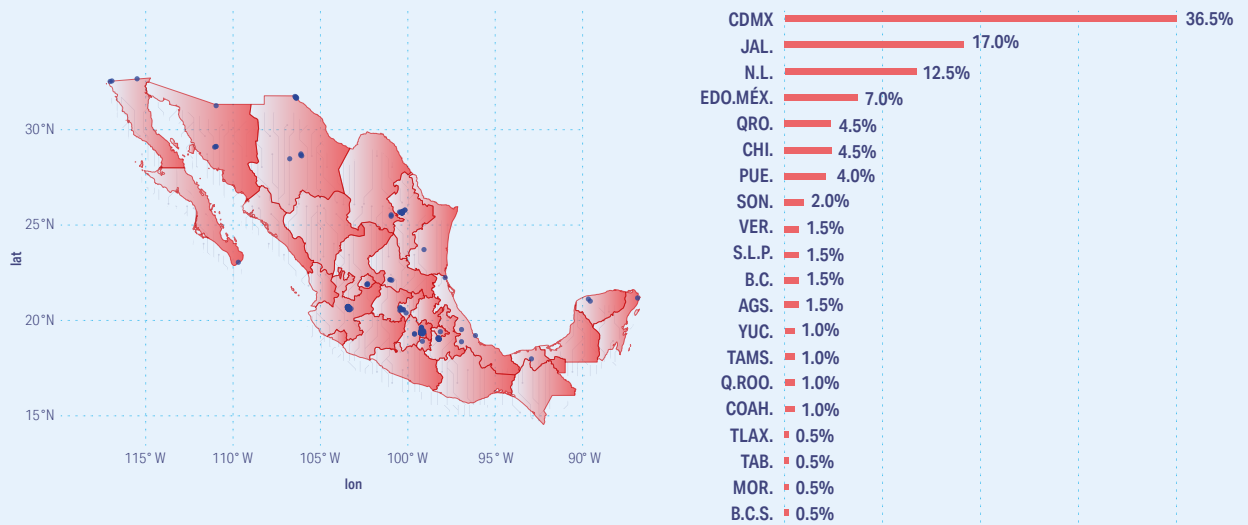
Mapa 3.2. Localización de las empresas identificadas que ofrecen servicios de conectividad para IoT en México



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

En cuanto a las empresas que ofrecen servicios de *software*, éstas tienen presencia en 20 de los 32 estados del país, destaca la Ciudad de México, Jalisco, Nuevo León, Estado de México y Querétaro con la mayor concentración de empresas en este rubro.

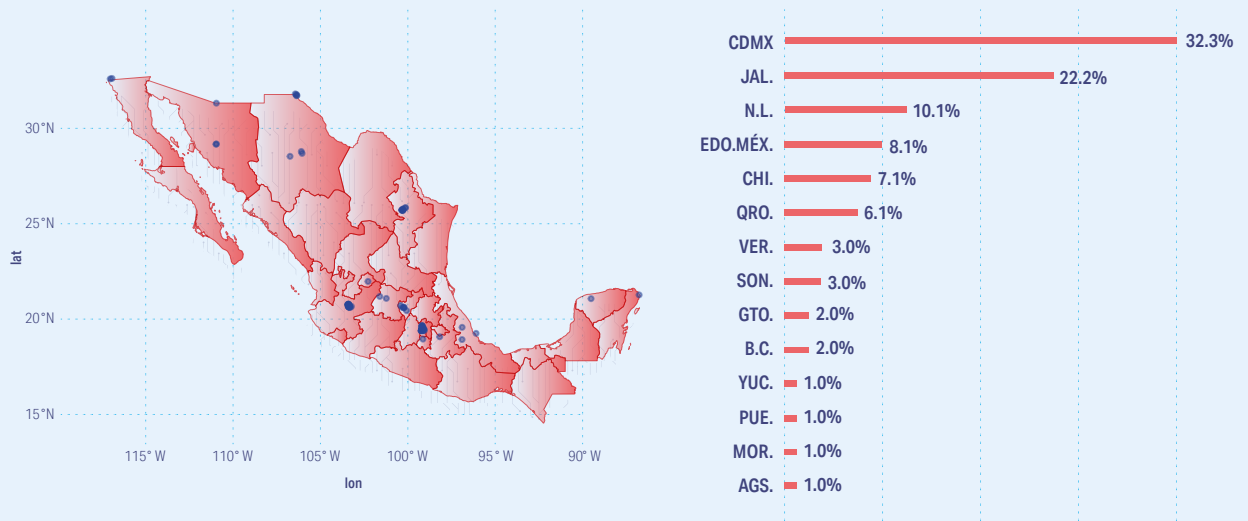
Mapa 3.3. Localización de las empresas identificadas que ofrecen servicios de *software* para IoT



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Las empresas que ofrecen servicios de *hardware* para IoT en México tienen presencia en 14 de los 32 estados del país y se localizan principalmente en Ciudad de México, Jalisco y Nuevo León, destaca la presencia de estas empresas en estados como Chihuahua, Querétaro y Veracruz (ver mapa 3.4).

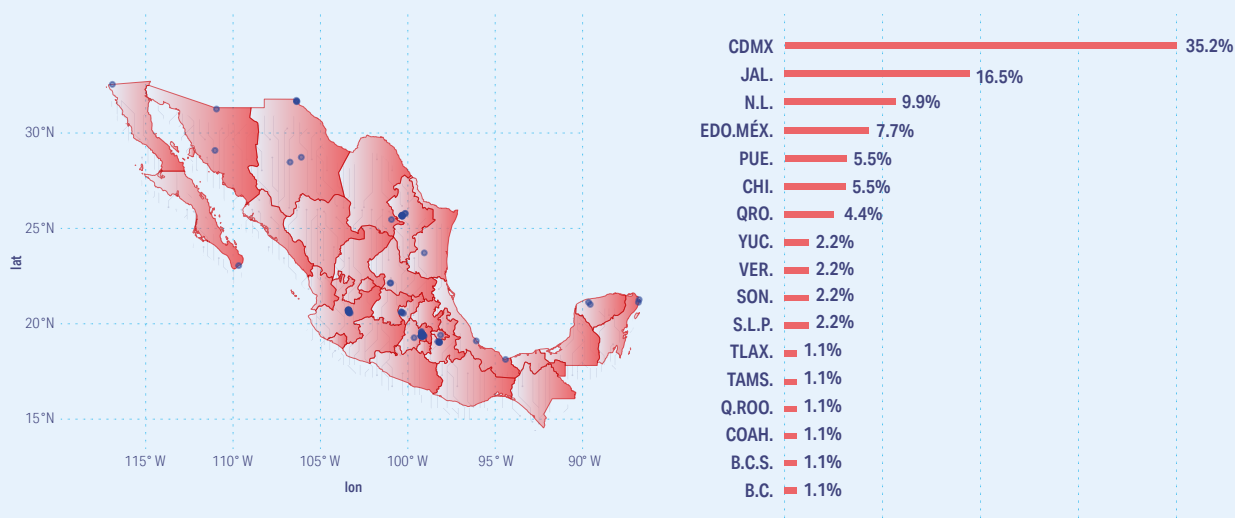
Mapa 3.4. Localización de las empresas identificadas que ofrecen servicios de *hardware* para IoT



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

En cuanto a las empresas que se incluyen en la categoría de “otros mercados laterales”, dan principalmente servicios relacionados a Ciberseguridad y Consultoría IoT, este tipo de empresas tienen presencia en 17 estados del país y se localizan principalmente en Ciudad de México, Jalisco, Nuevo León, Estado de México, Puebla y Chihuahua (ver mapa 3.5).

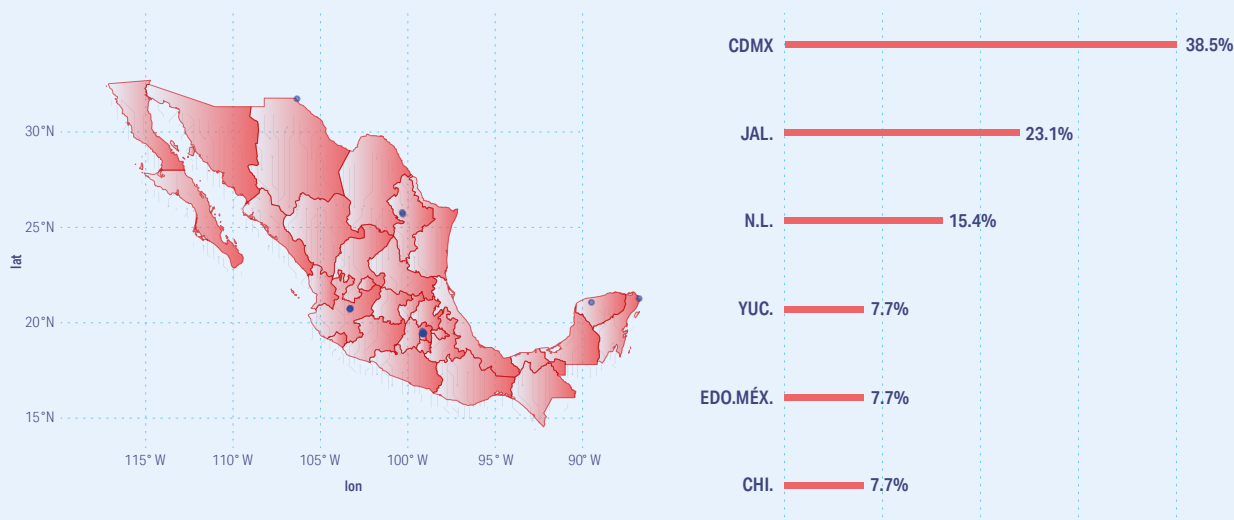
Mapa 3.5. Localización de las empresas identificadas que ofrecen servicios de otros mercados laterales para IoT



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Por último, las empresas que ofrecen servicios de extremo a extremo para IoT en México, tienen presencia en 6 de los 32 estados del país. Este tipo de empresa se localiza principalmente en Ciudad de México, Jalisco y Nuevo León (ver mapa 3.6).

Mapa 3.6. Localización de las empresas identificadas que ofrecen servicios de extremo a extremo para IoT



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Análisis de Clúster

Como se advierte en la información anterior, existe un patrón evidente respecto a la localización de las empresas que ofrecen algún servicio IoT en México, las cuales se concentran principalmente en la Ciudad de México (36.3%), Jalisco (17.9%), Nuevo León (11.8%), y el Estado de México (6.6%).

Para entender mejor las similitudes de las empresas de IoT en función de su modelo de negocio, a continuación se presenta un análisis de conglomerados o clústeres; se trata de un algoritmo de aprendizaje automático no supervisado que busca identificar los elementos (*v.gr.* las empresas de IoT que operan en México y fueron identificadas a través de la técnica de *Web Scraping*) que son similares en función de sus características específicas (*v.gr.* en este caso, los tipos de servicios que ofrecen y la ubicación geográfica de las mismas).

Para ello, se parte del concepto básico de “distancia” a fin de determinar similitudes entre las empresas de IoT. Por ejemplo, si tomamos la localización geográfica de las empresas y el tipo de servicios que ofrecen, **la distancia entre sus respectivos datos es una medida del grado de cercanía o similitud que existe entre las mismas**²²⁹

²²⁹ En la literatura especializada existen diversas funciones de distancia que se adaptan a las particularidades del análisis y a la naturaleza de los datos: Distancia euclidiana —que, para este caso en particular, es recomendable—, o la distancia Manhattan, entre otras. En este sentido, se utiliza el agrupamiento basado en prototipos donde los objetos o ingresos de los Operadores de Telecomunicaciones están más cercanos a su prototipo o centroide. En este sentido, la metodología de *K-medias* toma como insumos los ingresos de los Operadores de Telecomunicaciones y una función de distancia que se debe minimizar (suma de las distancias euclidianas) y regresa una partición óptima del conjunto total de los datos. Para una explicación más detallada se sugiere visitar la siguiente dirección electrónica:

<https://bookdown.org/rdpeng/exdata/hierarchical-clustering.html#hierarchical-clustering-1>

Una de las ventajas de esta técnica es que este análisis no se guía por ideas *a priori* de qué variables o muestras pertenecen a algún clúster, sino que el algoritmo “aprende” cómo agrupar la información optimizando una función de aprendizaje que en este caso se refiere a la minimización de la distancia euclidiana de cada empresa tomando en cuenta factores como la localización geográfica y el tipo de servicios que ofrece²³⁰.

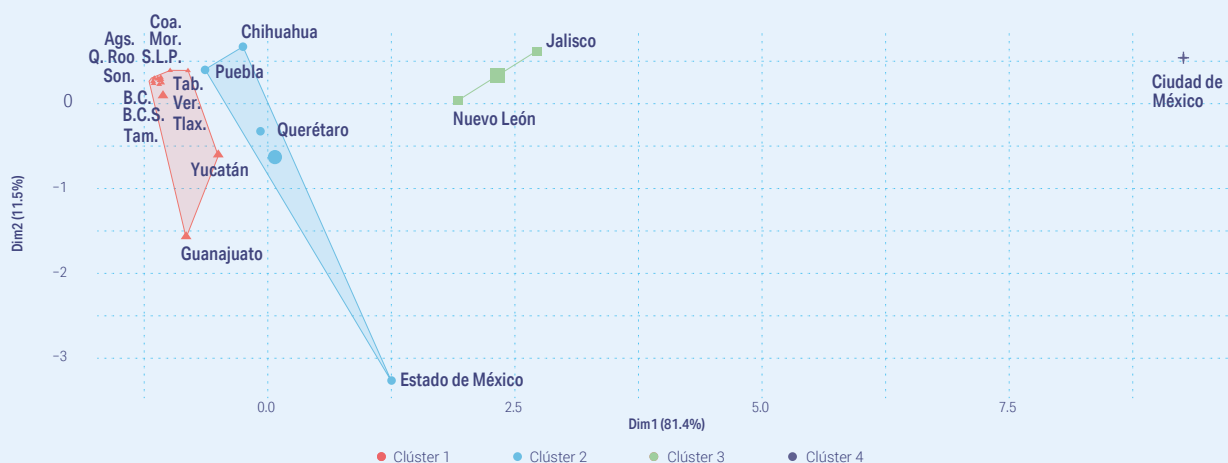
El algoritmo de aprendizaje se elaboró en lenguaje R y utilizó la información obtenida a través de la técnica de *Web Scraping*. Los datos incluyen 176 empresas con datos de sus localizaciones en México (270 diferentes localizaciones, donde 40 empresas cuentan con más de dos localizaciones) que ofrecen servicios de IoT y clasificadas por los servicios que ofrecen: (i) Conectividad, (ii) *Software*, (iii) *Hardware*, (iv) Otros Mercados Laterales (*v.gr.* Consultoría en IoT y ciberseguridad para IoT), y sus combinaciones (dos servicios, tres servicios y Extremo a Extremo).

Para realizar el análisis, se normalizaron los datos con el fin de calcular la matriz de distancias utilizando la distancia euclidiana y tomando en cuenta que este tipo de modelos es sensible a números particularmente grandes.

El resultado fue la identificación de 4 clústeres mediante el uso de la información de las empresas agrupadas por estado conforme el número de servicios, es decir, de manera individual a los servicios de Conectividad, *Software*, *Hardware* y Otros Mercados Laterales, así como la suma de las combinaciones de 2 servicios, las combinaciones de 3 servicios y la provisión de los 4 servicios (Extremo a extremo). El análisis completo que llevó a la identificación de 4 clústeres está disponible en el Anexo 3.

Podemos observar en la gráfica 3.7 que la Ciudad de México es la ciudad donde se localiza la mayor cantidad de empresas, por lo que forma un clúster con su propio centroide (clúster 4), le sigue el clúster formado por los estados de Jalisco y Nuevo León (clúster 3). Otro clúster está conformado por los estados de Chihuahua, Estado de México, Puebla y Querétaro (clúster 2). Por último, encontramos el clúster del resto de los estados (Aguascalientes, Baja California, Baja California Sur, Coahuila, Guanajuato, Morelos, Quintana Roo, San Luis Potosí, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz y Yucatán, clúster 1).

Gráfica 3.7. Clúster por estado de empresas que ofrecen servicios IoT en México



Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping*.

Nota: la conformación de los clústeres en dos dimensiones abarca el 92.9% de la varianza explicada.

²³⁰ Kassambara, A. (2017), *Practical Guide to Cluster Analysis in R. Unsupervised Machine Learning*. STHDA. Pág. (3).

Uno de los principales objetivos de la clasificación de clústeres es la de identificar y agrupar observaciones con características similares, en este sentido, si comparamos la clasificación resultante con un aspecto económico, por ejemplo, podemos considerar la participación estatal en términos de valor agregado bruto censal²³¹ y las Unidades Económicas con la información de los últimos Censos Económicos, como se puede observar en la tabla 3.2, el clúster conformado por los estados de Jalisco y Nuevo León cuenta con el 14.7% de las empresas que prestan servicios de IoT y tienen valores similares respecto a su participación del valor agregado bruto a nivel nacional. Por su parte, el clúster conformado por la Ciudad de México concentra el mayor valor agregado bruto a nivel nacional (23%).

El valor agregado bruto a nivel nacional promedio del clúster conformado por el Estado de México, Querétaro, Chihuahua y Puebla es de 4%, en tanto, el clúster conformado por el resto de los estados donde se encuentran las empresas que ofrecen servicios de IoT tienen la característica que el total de unidades económicas representa el 17.50% del total nacional y un valor agregado bruto promedio de 2.29% en cuanto a su participación nacional.

Tabla 3.2 Información Censal Estatal por clúster

Clúster	Estado	Total de empresas IoT (%)	Total de Unidades Económicas	Valor agregado censal bruto (millones de pesos)	Total de Unidades Económicas (%)	Valor agregado censal bruto (%)
4	Ciudad de México	38.89%	427,959	2,292,636	8.90%	23.00%
3	Jalisco	15.19%	335,120	595,162	7.00%	6.00%
	Nuevo León	11.85%	151,448	872,782	3.20%	8.70%
2	Estado de México	8.52%	624,472	769,506	13.00%	7.70%
	Querétaro	4.81%	81,224	252,065	1.70%	2.50%
	Chihuahua	3.70%	106,430	288,368	2.20%	2.90%
	Puebla	3.33%	298,183	290,524	6.20%	2.90%
1	Veracruz	1.85%	278,230	321,810	5.80%	3.20%
	Yucatán	1.85%	112,503	102,448	2.30%	1.00%
	Sonora	1.48%	99,804	325,240	2.10%	3.30%
	Aguascalientes	1.11%	53,939	154,829	1.10%	1.60%
	Baja California	1.11%	105,215	297,155	2.20%	3.00%
	Quintana Roo	1.11%	53,642	124,705	1.10%	1.20%
	San Luis Potosí	1.11%	97,773	265,702	2.00%	2.70%
	Coahuila	0.74%	95,230	433,579	2.00%	4.30%
	Guanajuato	0.74%	242,534	450,628	5.10%	4.50%
	Tamaulipas	0.74%	112,589	275,777	2.30%	2.80%
	Tlaxcala	0.74%	69,715	50,653	1.50%	0.50%
	Baja California Sur	0.37%	30,601	53,168	0.60%	0.50%
	Morelos	0.37%	96,462	96,050	2.00%	1.00%
	Tabasco	0.37%	73,616	245,299	1.50%	2.50%
	Nacional	100.00%	4,800,157	9,983,800	100.00%	100.00%

Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping* y de los Censos Económicos 2019²³² del INEGI.

²³¹ La elección del valor agregado es debido a que este considera la producción de bienes y servicios finales, además que permite una comparación sectorial de cuantificación agregada, lo que evita sesgos que pueden surgir de utilizar otros valores dentro de los Censos Económicos como el Valor Bruto de la Producción, como se menciona en Brown, F. (1998), *Productividad y cambio técnico: un análisis metodológico*. Universidad Nacional Autónoma de México.

²³² INEGI (2020), *Censos Económicos 2019. Características principales e indicadores económicos de las unidades económicas del sector privado y paraestatal que tuvieron actividades en 2018, según entidad federativa y actividad económica*. Disponible en: <https://www.inegi.org.mx/programas/ce/2019/#Tabulados>

Otra variable económica que se puede utilizar es la contribución del valor agregado bruto entre las actividades económicas de cada uno de los estados en la tabla 3.3. La Ciudad de México tiene la contribución más alta del valor agregado bruto con 17.7%, muy por arriba del dato siguiente (Jalisco 6.9%). El clúster conformado por Jalisco y Nuevo León presenta contribuciones en cuantías similares de las actividades secundarias y terciarias al valor agregado bruto a nivel nacional.

El clúster conformado por Estado de México, Querétaro, Chihuahua y Puebla cuenta con una contribución similar en cuanto a los valores del valor agregado bruto de las actividades económicas. El resto de los estados, aportan un 41.6% del valor agregado bruto de las actividades secundarias y un 28.1% de las actividades terciarias. Esto podría dar indicios de que probablemente las empresas que ofrecen servicios de IoT en México se ubican en entidades con una actividad económica mayor y con características relacionadas con las actividades terciarias y secundarias.

Tabla 3.3 Valor Agregado Bruto (VAB) Estatal por clúster

Clúster	Estado	Total de empresas IoT (%)	Valor Agregado Bruto (VAB)	Actividades Primarias (VAB)	Actividades Secundarias (VAB)	Actividades Terciarias (VAB)	Valor Agregado Bruto (%)	Actividades Primarias (%)	Actividades Secundarias (%)	Actividades Terciarias (%)
4	Ciudad de México	35.90%	3,133,609	1,236	294,372	2,838,002	17.70%	0.20%	5.50%	24.10%
3	Jalisco	12.90%	1,217,550	70,997	364,220	782,333	6.90%	12.00%	6.90%	6.60%
	Nuevo León	12.90%	1,373,593	6,359	481,033	886,201	7.80%	1.10%	9.10%	7.50%
2	Estado de México	7.80%	1,577,637	19,811	387,653	1,170,173	8.90%	3.30%	7.30%	9.90%
	Querétaro	5.10%	403,161	9,810	161,811	231,540	2.30%	1.70%	3.00%	2.00%
	Chihuahua	2.80%	572,787	33,799	227,786	311,202	3.20%	5.70%	4.30%	2.60%
	Puebla	4.60%	596,318	24,378	207,508	364,432	3.40%	4.10%	3.90%	3.10%
1	Veracruz	0.90%	801,506	42,784	249,951	508,771	4.50%	7.20%	4.70%	4.30%
	Yucatán	1.80%	264,441	9,986	70,245	184,209	1.50%	1.70%	1.30%	1.60%
	Sonora	2.30%	580,481	40,517	254,679	285,284	3.30%	6.80%	4.80%	2.40%
	Aguascalientes	1.80%	222,652	9,056	91,913	121,683	1.30%	1.50%	1.70%	1.00%
	Baja California	1.40%	575,784	15,472	221,202	339,110	3.30%	2.60%	4.20%	2.90%
	Quintana Roo	1.40%	290,272	2,101	32,742	255,429	1.60%	0.40%	0.60%	2.20%
	San Luis Potosí	1.40%	368,701	14,381	144,420	209,900	2.10%	2.40%	2.70%	1.80%
	Coahuila	0.90%	604,192	14,030	298,752	291,410	3.40%	2.40%	5.60%	2.50%
	Guanajuato	1.80%	702,633	26,592	244,559	431,481	4.00%	4.50%	4.60%	3.70%
	Tamaulipas	1.40%	517,770	15,059	189,358	313,354	2.90%	2.50%	3.60%	2.70%
	Tlaxcala	0.50%	103,823	3,415	39,665	60,743	0.60%	0.60%	0.70%	0.50%
	Baja California Sur	0.50%	159,010	5,336	45,541	108,133	0.90%	0.90%	0.90%	0.90%
	Morelos	0.50%	201,084	6,533	61,684	132,866	1.10%	1.10%	1.20%	1.10%
	Tabasco	0.90%	448,091	8,624	266,151	173,316	2.50%	1.50%	5.00%	1.50%
	Nacional	100.00%	17,669,844	592,193	5,306,377	11,771,274	100.00%	100.00%	100.00%	100.00%

Fuente: IFT con base en los datos obtenidos a través de la técnica de *Web Scraping* y del Producto Interno Bruto por Entidad Federativa²³³ del INEGI.

²³³ INEGI (2020), *Producto Interno Bruto por Entidad Federativa. Año base 2013*. Disponible en: <https://www.inegi.org.mx/programas/pibent/2013/#Tabulados>

4

Encuesta a las empresas que ofrecen servicios IoT en México

Como parte de un ejercicio de regulación colaborativa y en relación con la reciente denominación del Instituto como regulador de quinta generación, la CGPE realizó la primera Encuesta para las empresas que ofrecen servicios relacionados con el IoT en México. Se trata de una “encuesta de tendencia de negocio” cuyo objetivo es generar información cualitativa para efectos de profundizar sobre la experiencia de las empresas que ofrecen servicios de IoT en México.

Lo anterior enmarcado dentro de las acciones del IFT que se desprenden de la Hoja de Ruta del IFT 2021-2025, donde se establece como una de sus líneas estratégicas fundamentales el fomento a la adopción de nuevas tecnologías y casos de usos digitales en la sociedad (Estrategia 3.2). Sobre este tema, el Instituto ha abordado en sus programas anuales de trabajo proyectos y estudios relacionados con el desarrollo del ecosistema digital.

Las respuestas de esta encuesta permiten ampliar la visión sobre la evolución de los servicios de IoT en México, así como identificar los retos, logros y expectativas sobre este mercado. La encuesta estuvo disponible del 03 de octubre al 11 de noviembre de 2022, donde se invitó a 176 empresas vía correo electrónico, en este sentido agradecemos a todas las empresas que participaron y en especial a las 17 empresas que autorizaron publicar su nombre:

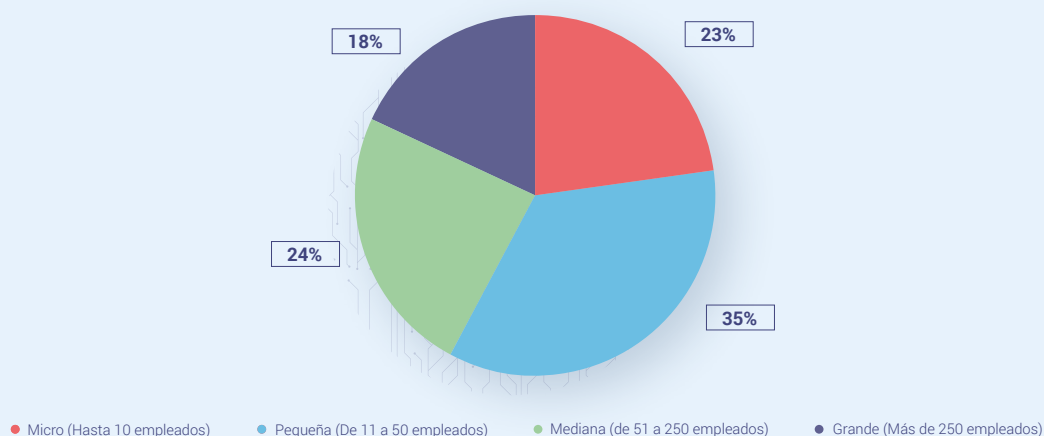
EVCON Group	Telefónica	Advantech Electronics	Kolibers Group
S4IoT	Yamazen Mexicana	Evolutel	Tautenet International de México
MEXIoT Solutions	SINCI	ENL REN Energi	
Installernet	Sento 40	Censystems	
AT&T México	Convergía, Inc.	Logicbus	

Uno de los aspectos relevantes consistió en determinar el tipo de perfil de empresa que opera en el mercado mexicano, los resultados de la encuesta revelan que en promedio las unidades económicas tienen al menos 3 años de operaciones en México, pero existen algunas empresas (24%) con una trayectoria de más de 17, 21 y 33 años de operaciones en el país.

Respecto al tamaño de la empresa, medido por número de empleados²³⁴, el 23% de los encuestados se ubica en la categoría de micro empresa (hasta 10 empleados), el 35% de las mismas se identificaron como pequeñas (de 11 a 50 empleados), el 24% se identifica como mediana (de 51 a 250 empleados), y el 18% se refiere a empresas con más de 250 empleados (Ver Gráfica 4.1).

²³⁴ La estratificación fue tomada de Secretaría de Economía (2022), *ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas*. Disponible en: https://www.economia.gob.mx/files/marco_normativo/A539.pdf

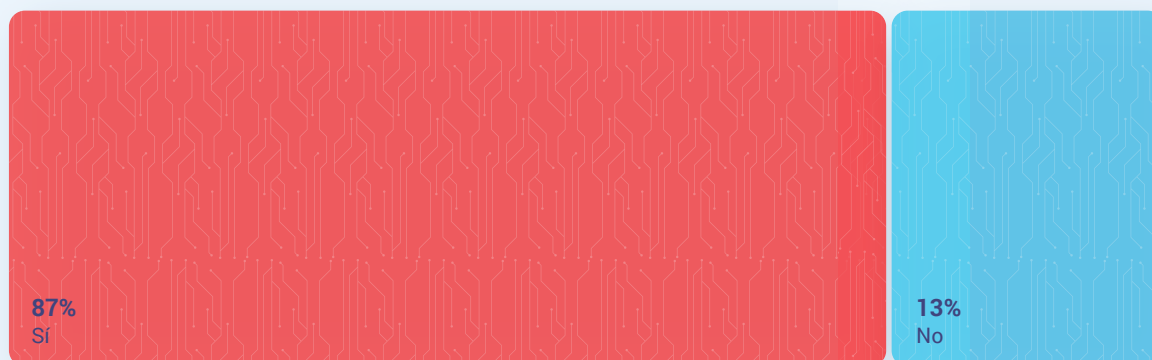
Gráfica 4.1. Porcentaje de empresas que ofrecen servicios IoT por tamaño de empresa



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

En concordancia con lo establecido en el capítulo anterior, un aspecto importante para el desarrollo de proyectos y aplicaciones que utilizan IoT son los estándares y normas que existen en el país, en este sentido, el 87% de las empresas que ofrecen servicios de IoT conocen de la existencia de normas técnicas (Normas Oficiales Mexicanas y/o NYCE) para IoT (Ver Gráfica 4.2). Para el 13% restante existe una necesidad de orientación y difusión de estas.

Gráfica 4.2. Conocimiento de las empresas que ofrecen IoT en México sobre las normas mexicanas (NOM y/o NYCE).



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Para profundizar en este tema, se les preguntó a las empresas sobre la existencia de algún otro estándar que no esté homologado en México y que requiera de su operación, algunas empresas señalaron estándares relacionados con la ciberseguridad como es el caso del IEC-62443-3-3²³⁵, también mencionaron las Normas Oficiales Mexicanas (NOMs):

NOM-001-SCFI-2018, Aparatos electrónicos-Requisitos de seguridad y métodos de prueba²³⁶.

NOM-024-SCFI-2013, Información comercial para empaques, instructivos y garantías de los productos electrónicos, eléctricos y electrodomésticos²³⁷.

NOM-208-SCFI-2016, Productos. Sistemas de radiocomunicación que emplean la técnica de espectro disperso-Equipos de radiocomunicación por salto de frecuencia y por modulación digital a operar en las bandas 902 MHz-928 MHz, 2400 MHz-2483.5 MHz y 5725 MHz-5850 MHz-Especificaciones y métodos de prueba²³⁸.

Para identificar el papel de las telecomunicaciones en la cadena de valor de IoT, es necesario, identificar las interacciones de las capas que integran la cadena de valor de las soluciones de IoT de manera general. En este sentido, el documento [Análisis Exploratorio de la Comercialización de Servicios de Conectividad para IoT](#), publicado en 2020, propone la siguiente cadena de valor para la industria de IoT.



²³⁵ Este estándar pretende cubrir todas las situaciones que puedan ocurrir durante el ciclo de vida de un sistema, desde su implantación hasta su retirada de la red. Los diferentes grupos de requisitos fundamentales (RF) son: Identificación y Control de Autenticación (ICA). Para más información visite: [https://www.incibe-cert.es/blog/nivel-seguridad-segun-el-iec-62443-3-3-sistemas-control-industrial#:~:text=Requisitos%20de%20seguridad%20en%20el%20IEC%2062443%2D3%2D3&text=Este%20est%C3%A1ndar%20pretende%20cubrir%20todas,Control%20de%20Autenticaci%C3%B3n%20\(ICA\)](https://www.incibe-cert.es/blog/nivel-seguridad-segun-el-iec-62443-3-3-sistemas-control-industrial#:~:text=Requisitos%20de%20seguridad%20en%20el%20IEC%2062443%2D3%2D3&text=Este%20est%C3%A1ndar%20pretende%20cubrir%20todas,Control%20de%20Autenticaci%C3%B3n%20(ICA)).

²³⁶ Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5572453&fecha=17/09/2019#gsc.tab=0

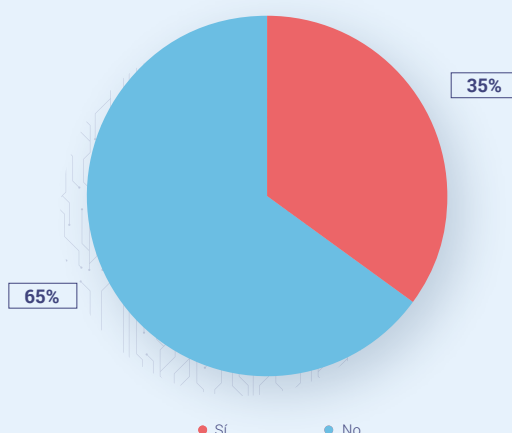
²³⁷ Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5309980&fecha=12/08/2013#gsc.tab=0

²³⁸ Disponible en: https://www.dof.gob.mx/normasOficiales/6413/seeco11_C/seeco11_C.html

Con estos eslabones en mente, se consultó a los encuestados sobre su participación en cada uno de ellos.

1. **Módulo inteligente:** El 44% de las empresas atienden esta parte de la cadena de valor
2. **Objetos inteligentes:** La mitad de las empresas mencionó que cubren también este eslabón;
3. **Operador de red:** El 60% mencionó que la conectividad es realizada por un tercero. El 65% de las empresas señalaron que no ofrecen servicios de telecomunicaciones fijas o móviles y el resto tienen esos servicios dentro de su cartera comercial. (Ver Gráfica 4.3).

Gráfica 4.3. Empresas que ofrecen servicios de IoT y que ofertan servicios telecomunicaciones fijas / móviles.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Fabricación de wearable technology

MoTeBo es una empresa mexicana de innovación textil que está enfocada en la fabricación de *Wearable Technology* (Wt) (tecnología que se utiliza como accesorio, relojes y otras prendas) y en IoT²³⁹. En colaboración con el operador de telecomunicaciones AT&T, implementaron una red dedicada para la creación de prendas con diversas funcionalidades que van desde la localización GPS hasta el monitoreo de signos vitales en tiempo real²⁴⁰.

4. **Habilitador de servicio:** El 79% de los encuestados mencionaron que es un proceso que incluye la plataforma, la habilitación de capacidad y aplicaciones y que han adoptado en sus empresas
5. **Integrador del sistema:** El 63% mencionaron que ellas mismas son responsables de este eslabón de la cadena, generando interfases, elaboración de soluciones, *hardware* y *back-end*.

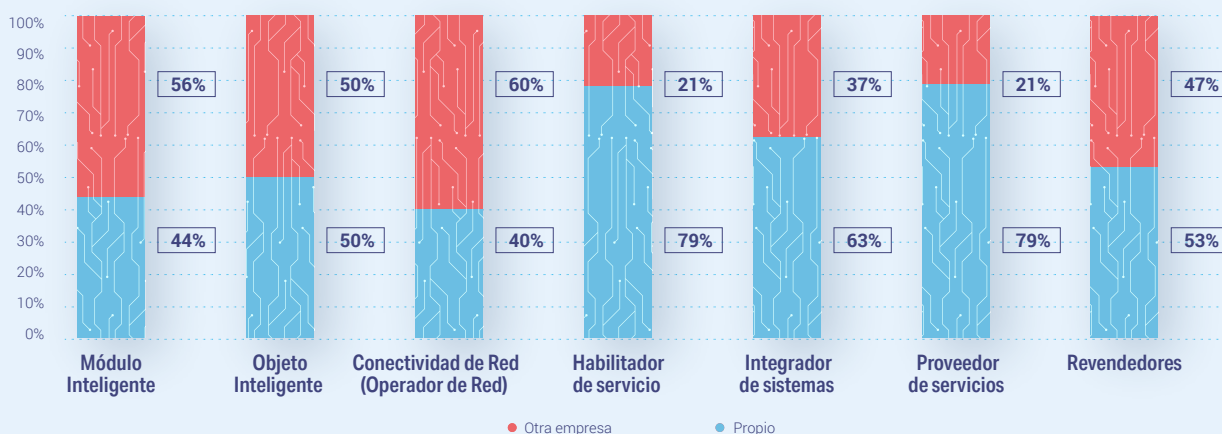
²³⁹ Para más información visite: <https://coolhuntermx.com/moda-tecnologia-motebo-textiles-inteligentes-0818/>

²⁴⁰ Para más información visite: <https://www.att.com.mx/negocios/casos-de-exito>

6. Provisión de servicios: El 79% de las empresas mencionaron que integran en su oferta este eslabón (embalaje, empaquetado, provisión de servicios y facturación).

7. Revendedores: El 53% de las empresas realizan este proceso (Ver Gráfica 4.4).

Gráfica 4.4. Participación de las empresas en los eslabones de la cadena de valor de IoT.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

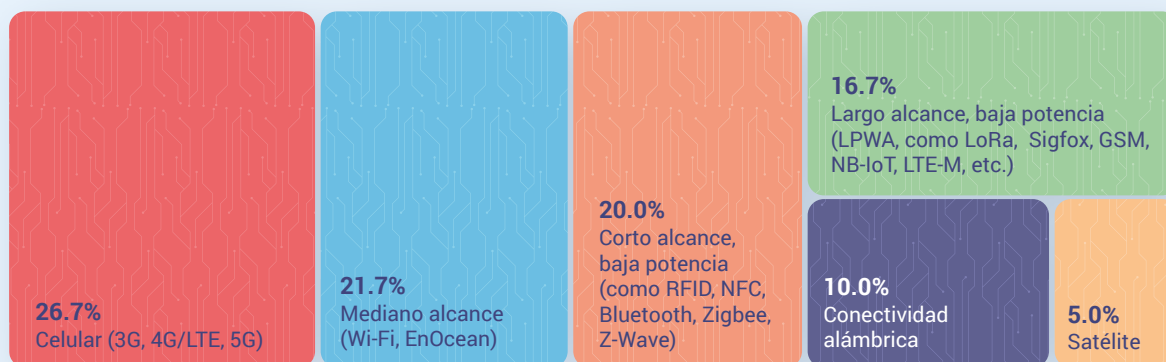
Conectividad automotriz en México

El operador de telecomunicaciones Telefónica, a través de Telefónica Tech proporciona sus servicios a la empresa OnStar mediante el uso de la plataforma de conectividad gestionada, Kite Platform. Lo que permite dotar de conectividad celular a OnStar y que este pueda comunicarse con los vehículos que cuentan con este servicio de navegación paso a paso, respuesta automática en caso de accidente y asistencia para vehículos robados²⁴¹.

Como se planteó desde el análisis realizado en 2020, existe una gran variedad de servicios y ofertas de IoT que pueden optar por diferentes tecnologías de conectividad dependiendo de la solución IoT. En este aspecto, se preguntó a los participantes sobre el tipo de tecnología que utilizan para brindar conectividad a los dispositivos IoT. En orden de importancia, las empresas señalaron que en primer lugar se encuentra la conectividad celular (3G, 4G/LTE y 5G), seguido de tecnologías de mediano alcance (Wi-Fi y EnOcean) y de corto alcance y baja potencia (RFID, NFC, Bluetooth, Zigbee, Z-Wave), después se encuentra la conectividad de largo alcance y baja potencia (LoRa, SigFox, GSM, NB-IoT, LTE-M), seguido de la conectividad alámbrica y satelital (ver Gráfica 4.5).

²⁴¹ Para más información visite: <https://aiofthings.telefonicatech.com/casos-exito/onstar>

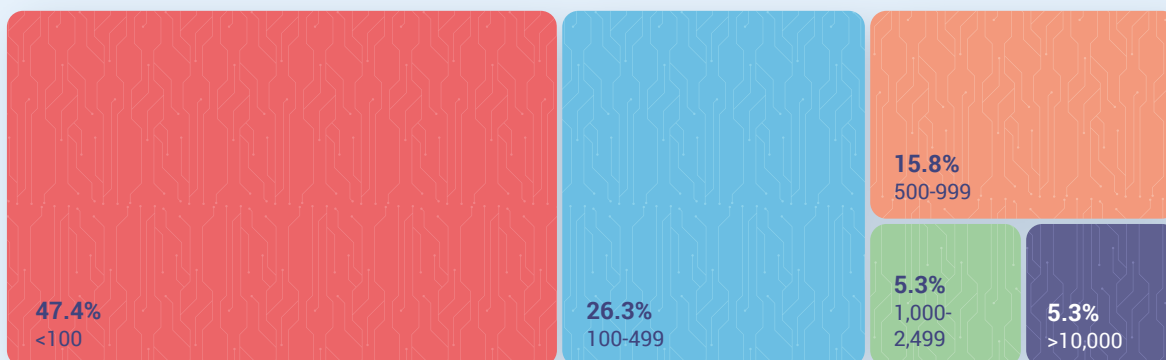
Gráfica 4.5. Tecnología utilizada por las empresas que ofrecen servicios IoT para la conectividad de dispositivos



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

De acuerdo con las empresas consultadas, la principal razón para elegir una u otra tecnología de conectividad es la cantidad de dispositivos que se tendrían que conectar para cada solución, tomando en cuenta que las empresas participantes informaron sobre el número de dispositivos promedio que son conectados en sus proyectos. En este sentido y en congruencia con la tendencia internacional identificada en el reporte de 2020, los resultados muestran que las empresas conectan menos de 100 dispositivos en la mayoría de sus proyectos, seguido de 100 a 499 y de 500 a 999 dispositivos (Ver Gráfica 4.6)

Gráfica 4.6. Número de dispositivos promedio conectados en proyectos de las empresas que ofrecen servicios de IoT en México.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Monitoreo de campos agrícolas mexicanos

AppGricola es una herramienta para el análisis de datos predictivos que permite medir, en tiempo real, las condiciones de los cultivos y, con ello, prevenir enfermedades y plagas, enviando alertas con recomendaciones específicas que ayuda a mejorar la productividad y permite ver información histórica del monitoreo²⁴².

Esta aplicación elaborada en conjunto con Evolutel y socios del Instituto Jalisciense de Tecnologías de la Información (IJALTI), fueron seleccionados en el *Top List* dentro del certamen *Technology & Innovation Leaders 2019*²⁴³.

De acuerdo con las respuestas de las empresas encuestadas, las tecnologías de conectividad que podrían predominar en los servicios IoT que se consumen en México son:

- | Tecnologías inalámbricas como 4G y 5G, y
- | Otras tecnologías como LoRA, NB-IoT, Bluetooth, redes privadas IoT y Sigfox.

Uno de los objetivos de la encuesta fue identificar los retos, logros y expectativas sobre la industria de IoT en México desde la perspectiva de las empresas que ofrecen estos servicios. En este sentido, las principales dificultades identificadas son:

- | El elevado costo de los dispositivos;
- | La homologación de equipos hechos en el extranjero;
- | El desconocimiento de la tecnología para su implementación en soluciones;
- | La falta de madurez en el conocimiento de la tecnología;
- | La concentración de mercado;
- | La lenta adopción sobre casos masivos de uso de IoT;
- | Los problemas de ciberseguridad, y
- | La disponibilidad de conectividad e Internet.

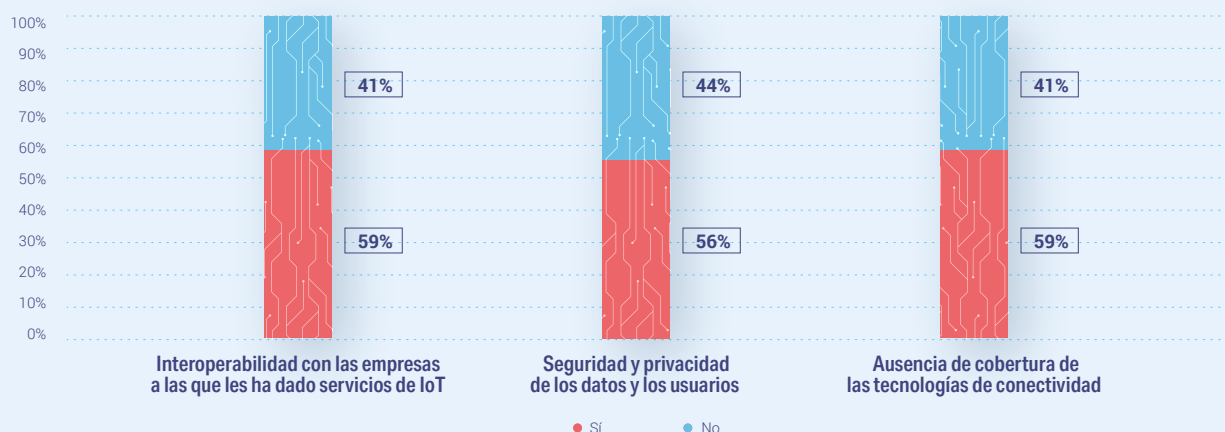
Los principales desafíos identificados por los encuestados dentro de la operación y ejecución de los proyectos de IoT en el país son:

- | La interoperabilidad con las empresas a las que les han dado servicio (59% han tenido problemas);
- | Problemas con la cobertura de las tecnologías de conectividad (59%), un 56% señaló tener problemas con la seguridad y privacidad de los datos y de los usuarios, y
- | La falta de divulgación sobre los beneficios del uso de IoT, la actualización de las tarifas en el mercado, la rentabilidad y la justificación sobre el uso de estos servicios (Ver Gráfica 4.7).

²⁴² Para más información visite: https://www.youtube.com/watch?v=KWDyT_pQKWw

²⁴³ Para más información visite: <https://twitter.com/ijalti/status/1149347929783750656>

Gráfica 4.7. Desafíos que enfrentan las empresas que brindan servicios IoT en México.

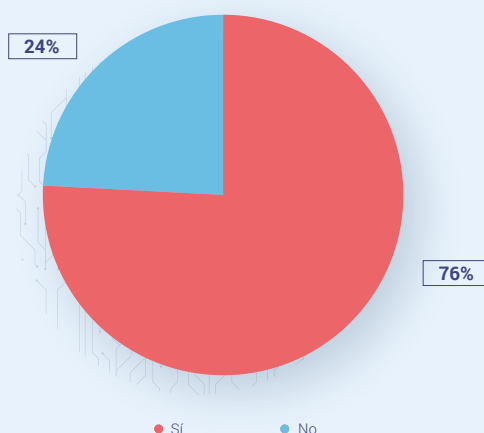


Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Existe una tendencia global donde las condiciones tecnológicas para IoT evolucionan positivamente con un creciente interés para estandarizar los dispositivos de IoT y garantizar la interoperabilidad entre productos, aplicaciones, servicios y sistemas de comunicación. En este contexto, las empresas que ofrecen servicios de IoT en México consideran que existen diferentes aplicaciones que requieren diferentes tecnologías, mismas que se complementan. Adicionalmente, consideran que existe una tendencia a la convergencia, donde los beneficios en la homologación de la estandarización y el uso de las redes 5G como plataforma preponderante en esta industria podrán impulsar la adopción de las soluciones IoT.

A raíz de la contingencia sanitaria provocada por COVID-19, se incrementaron las aplicaciones de IoT a nivel mundial. Este efecto se presenta también en el mercado nacional; al respecto, un 76% de los encuestados confirmó como factor clave del incremento en el uso de IoT en el país a la nueva normalidad y las medidas de distancia social (Ver Gráfica 4.8).

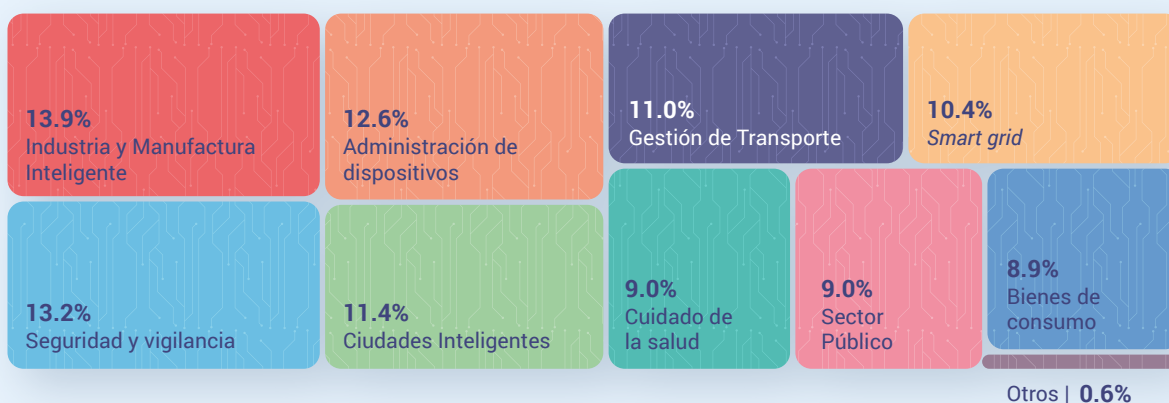
Gráfica 4.8. Percepción sobre el incremento en el uso de IoT en México por las empresas que ofrecen servicios de IoT.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

En cuanto a las oportunidades de negocio y el uso de IoT, se preguntó cuáles servicios de IoT tienen mayores oportunidades de crecimiento en México. Al respecto, se señalan en orden de importancia: (i) La industria y manufactura inteligente; (ii) La seguridad y vigilancia; (iii) La administración de dispositivos, y (iv) Las ciudades inteligentes. (Ver Gráfica 4.9).

Gráfica 4.9. Servicios IoT con mayores oportunidades de crecimiento según las empresas que ofrecen servicios IoT en México

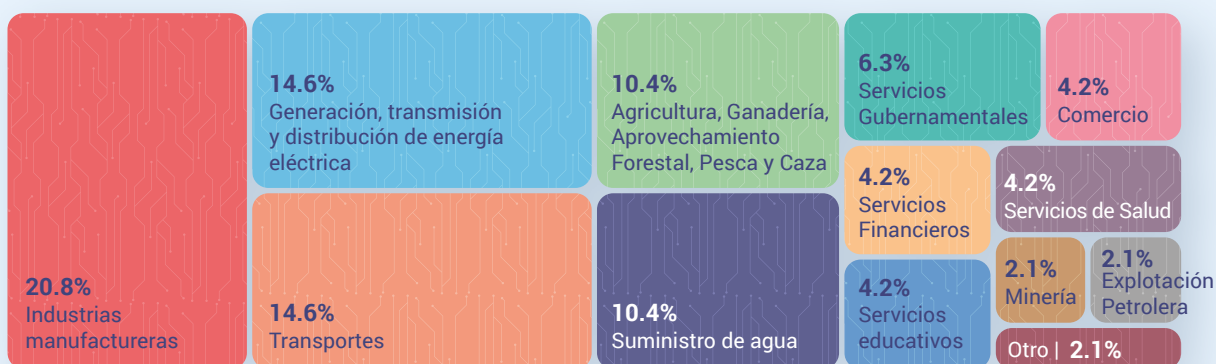


Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Otras categorías mencionadas que podrían tener oportunidades de crecimiento son las estaciones de recarga eléctrica, *backhaul* celular para soluciones LoRa, Sigfox, entre otras tecnologías, y servicios relacionados con la minería.

En este sentido, la actividad económica que tiene los mayores beneficios del uso de IoT, es la Industria Manufacturera, seguida de la Generación, transmisión y distribución de energía eléctrica, Transportes y Agricultura, Ganadería, Aprovechamiento Forestal, Pesca y Caza, otra de las actividades mencionadas es la Seguridad (Ver Gráfica 4.10).

Gráfica 4.10. Sectores con mayores beneficios del uso de IoT según las empresas que ofrecen servicios IoT en México



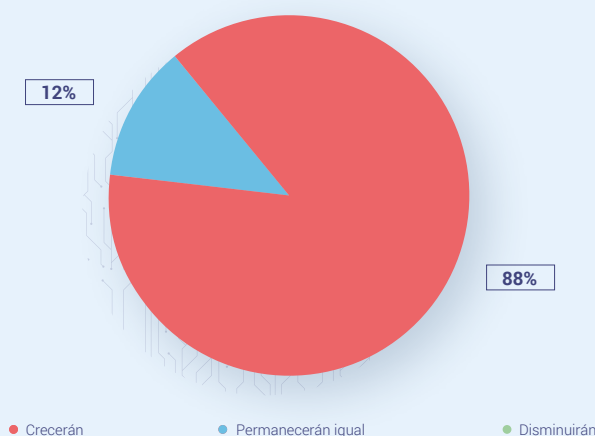
Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Seguridad en Transporte Público del Estado de México.

La empresa Censys integró equipos de videovigilancia al interior de las unidades del MEXIBUS, así como telemetría, equipos GPS para geolocalización, botones de pánico para atención inmediata a incidentes y ruteo y comunicaciones. Estos equipos están conectados al Centro de Control, Comando, Comunicación, Cómputo y Calidad (C5) del Estado de México, con una conexión ininterrumpida para coordinarse con las autoridades municipales, estatales y federales. Esto brindó una solución tecnológica para hacer del transporte público un lugar seguro, eficiente y con respuesta ante cualquier tipo de incidente, que beneficia a más de 130 mil usuarios al día²⁴⁴.

Respecto al crecimiento del uso de los servicios de IoT para 2023, las expectativas son positivas, el 88% de las empresas esperan que el uso de los servicios crecerá para el siguiente año (Ver Gráfica 4.11).

Gráfica 4.11. Expectativas de uso de los servicios de IoT en México para 2023.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Gas doméstico a un toque de distancia

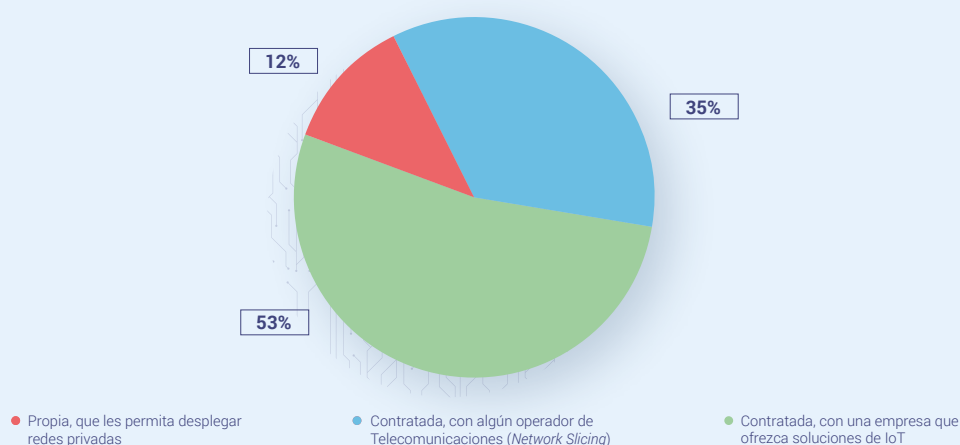
La empresa Sento40 elaboró una solución (*hardware*, desarrollo de una aplicación y una plataforma web) de gestión de clientes para una empresa de distribución de gas. La solución consiste en la instalación de un botón IoT conectado a la empresa de gas y que se pega magnéticamente en los refrigeradores de los hogares, lo que permite a los clientes solicitar una pipa de gas para su suministro al hogar²⁴⁵.

²⁴⁴ Censys (2022), *SITRAMyTEM*. Disponible en: <https://censystems.com.mx/project/sitramytem/>

²⁴⁵ Para más información, visite: <https://sento40.io/pages/casos-de-estudio>

La conectividad por redes 5G será una alternativa para las soluciones de IoT, se cuestionó a las empresas sobre cómo perciben en el largo plazo el uso de las redes 5G como red de conectividad de las empresas que buscan soluciones IoT. Al respecto, el 53% de los encuestados considera que la conectividad será contratada con una empresa que oferte soluciones de IoT, seguido en 35% de la opción, donde un operador de Telecomunicaciones (utilizando *Network Slicing*) provea esta conectividad, y, por último, solo un 12% considera contar con red propia donde se permita desplegar redes privadas (Ver Gráfica 4.12).

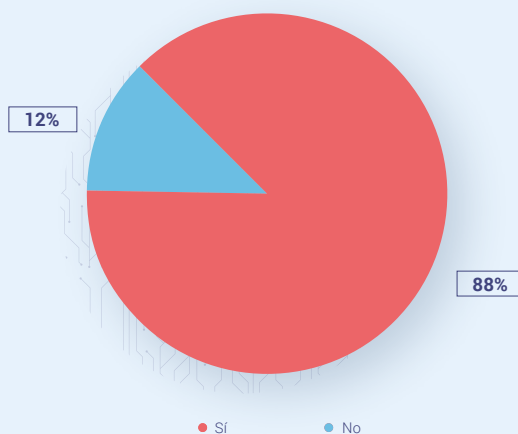
Gráfica 4.12. Conectividad en redes móviles 5G en el largo plazo para empresas que buscan soluciones IoT.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Una las principales acciones que lleva a cabo el IFT para el fomento de nuevas tecnologías es la liberación de espectro radioeléctrico, al respecto se les preguntó a las empresas que ofrecen servicios IoT en México sobre esta acción y si consideran que ésta puede incentivar el desarrollo del uso de IoT en el país. La mayoría de las empresas mencionaron que estas acciones incentivan el desarrollo del uso de IoT, al respecto mencionaron que el 5G ampliaría la velocidad de transmisión de datos, así como la cobertura, la calidad y la capacidad de los servicios y fortalecería la calidad de las comunicaciones (Ver Gráfica 4.13).

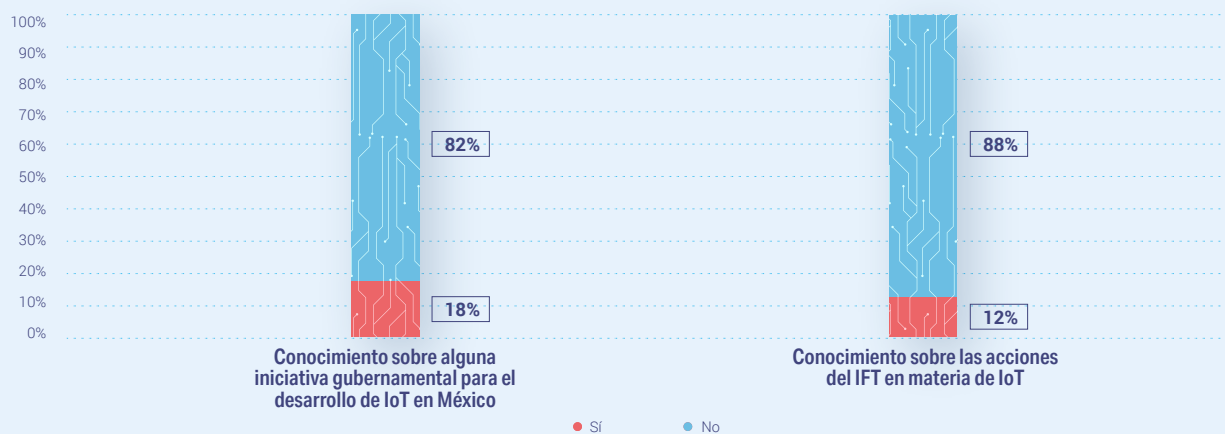
Gráfica 4.13. La liberación de espectro radioeléctrico como incentivo en el desarrollo del uso de IoT en México.



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Si bien, existen iniciativas o acciones para el desarrollo de IoT tanto a nivel nacional como internacional, se les preguntó a las empresas sobre el conocimiento de este tema, la gran mayoría de las empresas desconoce alguna acción o iniciativa gubernamental para el desarrollo de IoT en México, así como de las acciones del IFT en la materia (Ver Gráfica 4.14).

Gráfica 4.14. Conocimiento sobre las acciones e iniciativas gubernamentales respecto al desarrollo de IoT en México



Fuente: IFT con datos de la Primera Encuesta para las Empresas que ofrecen servicios relacionados con el IoT en México.

Al respecto, también se les preguntó a las empresas que ofrecen servicios de IoT en México sobre otras tendencias regulatorias que podrían incentivar el desarrollo de esta industria, **las empresas señalan como necesidad trabajar conjuntamente en los siguientes puntos:**

- (i) La Dirección General de Normas de la Secretaría de Economía podría promover las actualizaciones de las NOMs aplicables a los dispositivos IoT para efectos de que en su ámbito de aplicación se incluyan los dispositivos IoT²⁴⁶;
- (ii) El costo del espectro razonable y equivalente al que se establece en otros países con mayor desarrollo de IoT;
- (iii) La generación de incentivos para la compartición de la banda de 6 GHz para IMT y el acceso a bandas de uso libre para proyectos de IoT;
- (iv) Facilidades para la instalación de infraestructura que permita ampliar la cobertura y
- (v) La reducción del costo de la certificación de equipos y dispositivos (v.gr. Reducción de cargas administrativas y costos de operación).

Respecto a los aspectos comerciales, regulatorios y de competencia que las empresas consideran como cruciales para el desarrollo del mercado de IoT en México, destacan:

1. Eliminar certificaciones redundantes;
2. Facilitar la homologación de equipos;
3. Difundir el uso de la tecnología;
4. Definir e incluir condiciones técnicas y tarifarias para IoT y M2M;
5. Reducir el precio del espectro;
6. Fomentar la estandarización de dispositivos;
7. Aumentar la cobertura;
8. Disminuir los aranceles de importación de dispositivos;
9. Acceder a la infraestructura del AEP de telecomunicaciones;
10. Actualizar las NOM, así como
11. Homologar los permisos a nivel estatal y municipal para el despliegue de infraestructura.

²⁴⁶ Lo anterior es efectivamente benéfico para el desarrollo de la industria de IoT, tomando en cuenta los beneficios de las NOMs como reglamentación técnica:

1. Las NOMs protegen de los principales riesgos identificados, promoviendo la seguridad de las personas, su salud y el medio ambiente.
2. Crean una cultura de empoderamiento de los consumidores al proporcionar más información para la adquisición de productos, procesos y servicios.
3. Generan una mejor decisión de compra al incluir toda la información necesaria sobre productos, procesos y servicios.
4. Fomentan el desarrollo económico y la calidad en la producción de bienes y servicios al hacer obligatorio el cumplimiento de requisitos, especificaciones, características y métodos de prueba.
5. Impulsan el comercio internacional. Al armonizar los requisitos nacionales con los internacionales, se facilitan las importaciones y exportaciones.
6. Generan un equilibrio entre los competidores y elimina las prácticas desleales, al establecer igualdad de condiciones para productos, procesos y servicios.

Conclusiones

Este análisis profundiza en la investigación realizada en 2020 para el caso de México y considera las conclusiones identificadas respecto a la coadyuvancia en los esfuerzos internacionales para la homologación de dispositivos y tecnologías de conectividad; la promoción del desarrollo y disponibilidad de tecnologías de conectividad *ad hoc* para este tipo de servicios (v.gr. 5G, LTE-M, NB-IoT, espectro libre) y la posibilidad de replicar experiencias como las zonas de innovación establecidas por la FCC.

En la revisión de las iniciativas para fomentar el uso de IoT y de estandarización de IoT de la muestra de países seleccionados se encontró que al menos el 44% de las economías cuentan con un estándar específicamente para IoT; para el caso de México, se identificaron tres normas específicas:

NOM-001-SCFI-2018, Aparatos electrónicos-Requisitos de seguridad y métodos de prueba²⁴⁷.

NOM-024-SCFI-2013, Información comercial para empaques, instructivos y garantías de los productos electrónicos, eléctricos y electrodomésticos²⁴⁸.

NOM-208-SCFI-2016, Productos. Sistemas de radiocomunicación que emplean la técnica de espectro disperso-Equipos de radiocomunicación por salto de frecuencia y por modulación digital a operar en las bandas 902 MHz-928 MHz, 2400 MHz-2483.5 MHz y 5725 MHz-5850 MHz-Especificaciones y métodos de prueba²⁴⁹.

No obstante, se recomienda realizar un análisis detallado de la normatividad técnica vigente en México y el mundo para efectos de armonizar el régimen técnico con el de nuestros principales socios comerciales a efectos de buscar una zona común para la comercialización de servicios IoT.

Para el Instituto, el desarrollo de la industria de IoT es crucial, tal y como se muestra en la Hoja de Ruta que cuenta con líneas de acción regulatorias con un planteamiento estratégico que busca promover la disponibilidad de espectro radioeléctrico para la provisión de diferentes servicios y aplicaciones de radiocomunicaciones²⁵⁰, en este sentido, se reconoce que la determinación del uso de la banda de 6 GHz, para uso no licenciado o para servicios 5G podría generar un beneficio económico y social. A partir del mismo planteamiento estratégico, el IFT actualmente se encuentra elaborando el “Código de mejores prácticas para la ciberseguridad del IoT”, un compendio de buenas prácticas que permitirá promover las mejores prácticas dentro de la industria.

En cuanto a los proyectos IoT en nuestro país, se ha encontrado que se han desarrollado 29 proyectos con un promedio de 3 proyectos nuevos cada año desde 2012 a 2021. En estos proyectos, el 66% (19 de 29) prevén la conexión de menos de 100 dispositivos, las tecnologías de conectividad más utilizadas son las tecnologías de corto alcance y baja potencia (38%), seguido de redes celulares (31%) y de conectividad satelital y alámbrica (14% cada una).

²⁴⁷ Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5572453&fecha=17/09/2019#gsc.tab=0

²⁴⁸ Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5309980&fecha=12/08/2013#gsc.tab=0

²⁴⁹ Disponible en: https://www.dof.gob.mx/normasOficiales/6413/seeco11_C/seeco11_C.html

²⁵⁰ IFT (2020), *Estrategia IFT 2021-2025. Hoja de Ruta*. Pág. (47). Disponible en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

En cuanto a los resultados del *Web Scraping*, se observa que la oferta en México asociada a los servicios de IoT se encuentra fragmentada. De las empresas que se dedican a un solo servicio, el 26.7% ofrecen solo servicios de *Software*, el 13.6% se encuentra en otros mercados laterales, el 4.0% solo *Hardware*, el 2.8% ofrecen servicios de extremo a extremo y un 2.8% se dedican a la Conectividad.

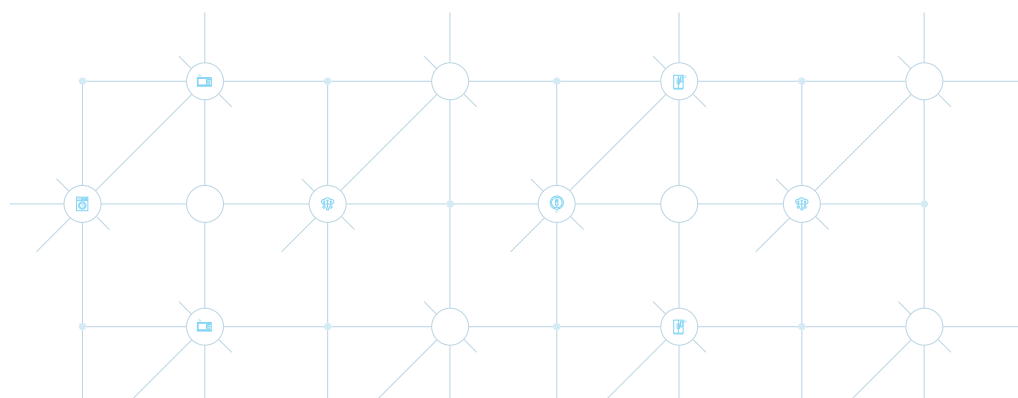
Entre las ofertas comerciales se puede observar una tendencia de despliegue de proyectos en los sectores económicos terciario y secundario, con énfasis en los servicios relacionados con la Industria Manufacturera y los Servicios de Transporte. De igual manera, se destacan los servicios dirigidos hacia el control de dispositivos, servicios dedicados para ciudades inteligentes y la telemática.

Otro patrón que se observó consiste en que los clientes de las empresas están relacionados con servicios de administración de plataformas y control y manejo de la información, seguido de consultores de sistemas y servicios profesionales para el desarrollo de *Software* y *Hardware*.

En cuanto a la localización de las empresas que ofrecen servicios de IoT en México, éstas se encuentran en 21 de los 32 estados del país y se concentran principalmente en la Ciudad de México (38.9%), Jalisco (15.2%), Nuevo León (11.9%) y el Estado de México (8.5%), así como Querétaro (4.8%) y Chihuahua (3.7%).

El análisis de clústeres permitió confirmar que la Ciudad de México es un host de desarrollo por sí misma, le siguen los estados de Jalisco, Nuevo León y Estado de México, siendo consistente con el patrón encontrado en otros países como Argentina, donde se observa una relación positiva entre la actividad económica en la región y el interés por el desarrollo de IoT.

Las empresas que ofrecen servicios de IoT en México son Micro, Pequeñas y Medianas empresas, las cuales utilizan en mayor medida las tecnologías celulares (3G, 4G y 5G) y la conectividad de mediano alcance (Wi-Fi, EnOcean, principalmente) para proyectos en los que en promedio se utilizan 100 dispositivos. Asimismo, se identifican como una oportunidad de crecimiento para el negocio de IoT los proyectos enfocados a la industria y manufactura inteligente, seguridad y vigilancia, así como la administración de dispositivos, siendo la Industria Manufacturera la actividad económica que se beneficiaría de manera más acelerada por la adopción de IoT, seguido por la generación de energía eléctrica, transporte y actividades agrícolas y agropecuarias.



Anexo 1. Metodología de Web Scraping.

El propósito de esta sección es mostrar la metodología que se utilizó para identificar y construir la base de datos de las empresas que ofertan productos y servicios de Internet de las Cosas (IoT) en México, mediante la técnica de *Web Scraping* para la búsqueda y extracción de información de páginas web de manera automática. Este ejercicio dio como resultado una base de datos con información de 176 empresas que ofrecen productos y servicios de IoT en México.

A continuación, se presentará brevemente en que consiste la técnica de *Web Scraping*, las herramientas utilizadas, cómo se generó el algoritmo para la búsqueda de los sitios en Internet, los pasos utilizados para la búsqueda manual de la información para la conformación de la base de datos, y por último las limitantes y dificultades que se presentaron.

¿Qué es *Web Scraping*?

El *Web Scraping*, o en español “raspado web”, es el proceso de extracción de datos (estructurados o no estructurados) provenientes de páginas web, usando herramientas informáticas como *software* especializado o algoritmos programados en diversos lenguajes de programación, con el objetivo de automatizar la recopilación de datos y hacer eficiente el proceso de conformación de bases de datos²⁵¹, estos datos pueden ser: Números, texto, imágenes o cualquier formato de información que pueda ser útil.

Con esta técnica se busca obtener una gran cantidad de datos (*Big Data*) de manera automática, evitando que intervengan personas en el proceso de recolección, ahorrando tiempo y recursos monetarios²⁵². Esta técnica forma parte de las herramientas empleadas por las nuevas soluciones o tecnologías que ofrece la Ciencia de Datos para descubrir nuevo conocimiento, como son el *Big Data*²⁵³, el *Data Mining*²⁵⁴ y el *Machine Learning*²⁵⁵, también el *Web Scraping* puede emplear algunas de estas tecnologías para robustecer el proceso de extracción de datos.

²⁵¹ Castrillo-Fernández, O. (2015), *Web Scraping: Applications and Tools*. European Public Sector Information Platform. Topic Report No.2015/10. Disponible en: https://data.europa.eu/sites/default/files/report/2015_web_scraping_applications_and_tools.pdf

²⁵² López, D. (2017), *¿Qué es el Web Scraping?* Disponible en: <http://www.icorp.com.mx/blog/que-es-el-web-scraping/>

²⁵³ Comisión Económica para América Latina (2019), *Big Data para la medición de la economía del Internet*. Autor. Disponible en: <https://www.cepal.org/es/big-data/investigacion>

²⁵⁴ Fuentes, S. y Ruiz, M. (2007), *Minería Web: un recurso insoslayable para el profesional de la información*. Scientific Electronic Library Online. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352007001000011

²⁵⁵ Li, J., Xu, Q. y, Shah, N. y Mackey, T. (2019), *A Machine Learning Approach for the Detection and Characterization of Illicit Drug Dealers on Instagram: Model Evaluation Study*. National Center for Biotechnology Information. Disponible en: <https://pubmed.ncbi.nlm.nih.gov/31199298/>

El *Web Scraping*, se puede emplear para diferentes propósitos²⁵⁶:

- | Rastreo de precios de productos o servicios y comparación de estos.
- | Aglutinamiento de contenido del mismo tipo proveniente de distintos sitios web, como pueden ser noticias, ventas online, etc.
- | Medición y clasificación de opiniones sobre cualquier tema en redes sociales o páginas web de opiniones²⁵⁷.
- | Monitoreo de indicadores que se actualizan de manera frecuente.

Herramientas utilizadas y generación de algoritmo

Para la generación del algoritmo se utilizó el lenguaje R en su versión 4.0.3²⁵⁸ y su entorno de desarrollo RStudio²⁵⁹, ambos de uso libre y ampliamente utilizados en diversos sectores e investigaciones que involucran el análisis de datos por su potente lenguaje de programación, que asemeja su sintaxis de programación a lenguajes empleados en la informática y en la ciencia, por ejemplo, al lenguaje de programación C^{260,261}, que permiten el análisis de datos de manera interactiva, así como la escritura de programas o algoritmos.

En específico, para la elaboración del algoritmo de búsqueda de páginas web que tuviesen información sobre la venta de productos y servicios IoT en México, se empleó la librería RSelenium²⁶² a efectos de automatizar el control del buscador de Google y también para extraer el código fuente y la dirección (URL) de las páginas web, además de la librería readr²⁶³ para manipular la información extraída de las páginas web.

Como resultado, el algoritmo recopiló las direcciones web (URLs) de las páginas de venta de productos y servicios IoT en México y las guardó en un archivo de texto en formato CSV con el fin de consultarlas posteriormente de manera manual y poder realizar una clasificación de estas. Con el fin de tener un mayor rango posible de resultados, se ejecutó el algoritmo con tres diferentes criterios de búsqueda:

- | Búsqueda de páginas con información de “IoT Mexico Servicios”
- | Búsqueda de páginas con información de “IoT MX Services”
- | Búsqueda de páginas con información de “IoT MX Servicios”

²⁵⁶ Hostingplus (2020), *Qué es y cómo hacer web scraping*. Disponible en: <https://www.hostingplus.mx/blog/que-es-y-como-hacer-web-scraping/>

²⁵⁷ González, F. (2019), *Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales*. Scientific Electronic Library Online. Disponible en: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0717-554X2019000200267

²⁵⁸ R Project (2021), *The R Project for Statistical Computing*. Disponible en: <https://www.r-project.org/>

²⁵⁹ RStudio (2021), *About RStudio*. Autor. Disponible en: <https://www.rstudio.com/about/>

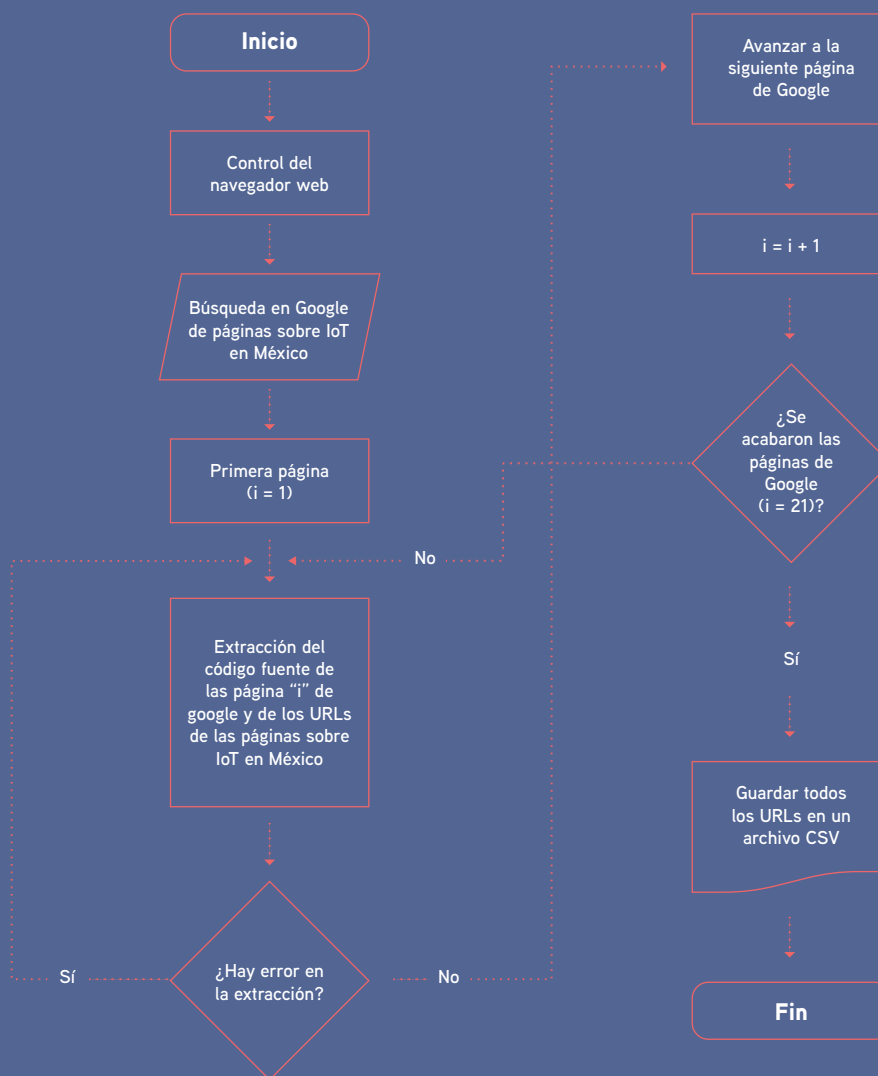
²⁶⁰ Ritchie, D. (2003), *The Development of the C Language**. Bell Labs/Lucent Technologies. Disponible en: <https://www.bell-labs.com/usr/dmr/www/chist.html>

²⁶¹ GNU Astronomy Utilities. (2021), *Why C programming language?* Disponible en: https://www.gnu.org/software/gnuastro/manual/html_node/Why-C.html

²⁶² Harrison, J. (2020), *RSelenium: R Bindings for 'Selenium WebDriver'*. R Project. Disponible en: <https://cran.r-project.org/web/packages/RSelenium/index.html>

²⁶³ Wickham, H. & Hester, J. (2020), *readr: Read Rectangular Text Data*. R Project. Disponible en: <https://cran.r-project.org/web/packages/RSelenium/index.html>

A continuación, se presenta el diagrama de flujo del algoritmo programado en R:



Procesamiento de la información

Clasificación de las páginas web

Después de extraer las URLs y guardarlas en un archivo con formato CSV, se realizó una primera consulta de cada una de las URLs de manera manual para eliminar páginas web que no contenían información sobre IoT en México, después se realizó la clasificación de las URLs para conocer en primera instancia su contenido y poder clasificarlas según su tipo de ofertas: Conectividad, *Software*, *Hardware*, Extremo a Extremo y Otros mercados laterales²⁶⁴.

Conformación de la base de datos

De las páginas web seleccionadas y clasificadas en el paso anterior, se realizó una segunda consulta y se extrajo la siguiente información para la conformación de la base de datos:

- | URL principal.
- | URL en donde se encuentra la información de IoT.
- | Tipo de producto o servicio de IoT ofertado.
- | Dirección o domicilio de las oficinas en México.
- | Precio de los productos.

La base de datos quedó conformada con información de 176 empresas que ofertan productos y servicios de IoT en México, aunque algunas empresas no tienen oficinas en México, sí ofrecen el producto o servicio en México.

Limitantes y dificultades

Google no permite los tráficos de datos “inusuales provenientes de sólo una dirección IP”, por lo que la repetición de la ejecución del algoritmo se realizó de manera pausada, es decir en pequeños intervalos de tiempo de separación entre una ejecución y la siguiente.

Adicionalmente, para este ejercicio, se construyó otro algoritmo utilizando *Web Scraping* enfocado a extraer el texto de las páginas web, este segundo algoritmo se utilizó para extraer de manera automática la información contenida en las páginas web para la conformación de una base de datos de texto; sin embargo, la información no tenía la calidad deseada, esto debido a que cada una de las páginas está estructurada de manera diferente, en este sentido, cada una de las páginas web requiere el desarrollo de un código de descarga único, de acuerdo con sus características: Idioma, seguridad y tecnología utilizada en la interfaz de usuario de cada página web, por lo que se optó por realizar la selección de información de los sitios web de manera manual.

²⁶⁴ Para mayor información visite: <http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/analisisexploratorioiot.pdf>

Código para R Studio

```
library(RSelenium)
library(readr)

rD<-rsDriver(browser=c("chrome"), chromeversion="90.0.4430.24")
remDr<-rD[["client"]]

tryCatch({
  remDr$navigate("https://www.google.com/")
},
error=function(e){
  remDr$navigate("https://www.google.com/")
}
)
webElem <- remDr$findElement(using = "css", "[name = 'q']")
webElem$maxWindowSize()
webElem$sendKeysToElement(list("IoT Mexico Servicios", key = "enter"))
u=1
doc_4<-NULL
p=1

for (o in 1:21) {
  cat("pagina",o,"\\n")
  doc <- remDr$getPageSource()[[1]]
  doc_1<-read_lines(doc)
  doc_2<-doc_1[grepl("yuRUbf",doc_1)]
  h<-length(doc_2)
  doc_3=NULL
  l=1
  for (j in 2:h) { a<- unlist(strsplit(doc_2[j], split = "class=\"yuRUbf\"><a href="))
    k<-length(a)

    for (i in 2:k) {
      doc_3[l] <- a[i]
      l=l+1
    }
  }

  m<-length(doc_3)
  k<-NULL
  for (i in 1:m) {
    k<-unlist(strsplit(doc_3[i], split = "\\\""))
    doc_4[p]<-k[2]
    q=0
    if(is.na(doc_4[p])==TRUE){
      doc_4[p]="pdf"
      p=p-1
    }
  }
}
```

```
while((doc_4[p]==doc_4[u]) & (o!=1))
{
  if(q==0){
    print("entró al while")
  }

  tryCatch({
    remDr$refresh()
    webElem <- remDr$findElement("css", "body")
    webElem$sendKeysToElement(list(key = "end"))
    webElem<-remDr$findElement("link text", "Siguiete")
    webElem$clickElement()
  },
  error=function(e){
    remDr$refresh()
    webElem <- remDr$findElement("css", "body")
    webElem$sendKeysToElement(list(key = "end"))
    webElem<-remDr$findElement("link text", "Siguiete")
    webElem$clickElement()

  }
)
doc =NULL
doc_1 =NULL
doc_2 = NULL
a = NULL
k = NULL
m = NULL

doc <- remDr$getPageSource()[[1]]
doc_1<-read_lines(doc)
doc_2<-doc_1[grepl("yuRbf",doc_1)]
h<-length(doc_2)
doc_3=NULL
l=1
for (j in 2:h) {
  a<- unlist(strsplit(doc_2[j], split = "class=\"yuRbf\"><a href= "))
  k<-length(a)

  for (v in 2:k) {
    doc_3[l] <- a[v]
    l=l+1
  }
}
```

```

        m<-length(doc_3)
        k<-NULL
        k<-unlist(strsplit(doc_3[i], split = "\\\""))
        doc_4[p]<-k[2]
        q=q+1
        cat("it while:",q,"\n")

    }

    if(q>0){
        print("salió del while")
    }
    print(doc_4[p])
    p=p+1

}
u=p-m
tryCatch({
    remDr$refresh()
    webElem <- remDr$findElement("css", "body")
    webElem$sendKeysToElement(list(key = "end"))
    webElem<-remDr$findElement("link text", "Siguiente")
    webElem$clickElement()
},
error=function(e){
    remDr$refresh()
    webElem <- remDr$findElement("css", "body")
    webElem$sendKeysToElement(list(key = "end"))
    webElem<-remDr$findElement("link text", "Siguiente")
    webElem$clickElement()

}
)
}
links<-data.frame(doc_4)
write.csv(links, file="urls_búsqueda_iot_1.csv")

remDr$close()
rD$server$stop()

```

Anexo 2. Metodología de Ciencia de Datos utilizadas

Metodología *Knowledge Discovery in Data Bases* (KDD).

La metodología *Knowledge Discovery in Databases* (KDD) es una metodología de Ciencia de Datos que se centra en el desarrollo de métodos y técnicas para entender los datos y en la aplicación de métodos específicos de *data mining* para la búsqueda de patrones²⁶⁵ dentro de las bases de datos. Esta metodología puede ser aplicada en muchas áreas de conocimiento, desde *marketing*, finanzas, detección de fraudes, manufactura, telecomunicaciones y empresas tecnológicas²⁶⁶.

A diferencia de otras metodologías, KDD se centra en la búsqueda de patrones entendibles que pueden ser interpretados como conocimiento útil o interesante²⁶⁷; además, esta metodología sigue evolucionando junto con las innovaciones en *Machine Learning*, reconocimiento de patrones, bases de datos, estadística, Inteligencia artificial, adquisición de conocimientos, visualización de información y computación de alto desempeño²⁶⁸.

Pasos de la metodología KDD.

La metodología KDD es un proceso interactivo e iterativo²⁶⁹, el proceso general de encontrar e interpretar patrones a partir de datos implica la aplicación repetida de los siguientes pasos²⁷⁰:

1. Desarrollar una comprensión del dominio de la aplicación, el conocimiento previo relevante y los objetivos del usuario final.
2. Crear un conjunto de datos objetivo: Seleccionar un conjunto de datos o centrarse en un subconjunto de variables o muestras de datos en las que se va a realizar el análisis.
3. Limpieza y pre-procesamiento de datos: Eliminación de ruido o valores atípicos; recopilar la información necesaria para modelar; técnicas para manejar campos de datos faltantes y seguimiento de la información en secuencia y cambios conocidos.

²⁶⁵ Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996), *From Data Mining to Knowledge Discovery in Databases*. American Association for Artificial Intelligence. Vol.17. No. 3. Pág. (37). Disponible en: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1230/1131>

²⁶⁶ Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996), *From Data Mining to Knowledge Discovery in Databases*. American Association for Artificial Intelligence. Vol.17. No. 3. Pág. (38). Disponible en: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1230/1131>

²⁶⁷ Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996), *From Data Mining to Knowledge Discovery in Databases*. American Association for Artificial Intelligence. Vol.17. No. 3. Pág. (39). Disponible en: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1230/1131>

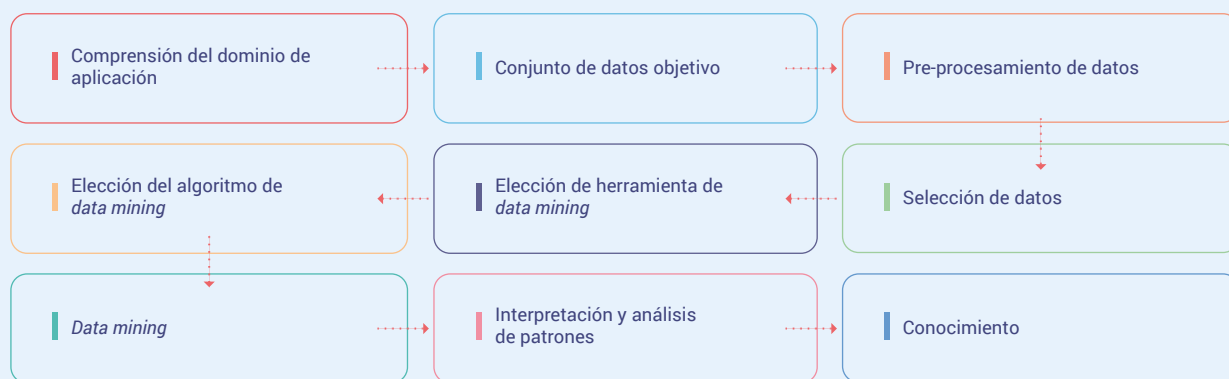
²⁶⁸ Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996), *From Data Mining to Knowledge Discovery in Databases*. American Association for Artificial Intelligence. Vol.17. No. 3. Pág. (39). Disponible en: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1230/1131>

²⁶⁹ Fayyad, U., Piatetsky-Shapiro, G. y Smyth, P. (1996), *From Data Mining to Knowledge Discovery in Databases*. American Association for Artificial Intelligence. Vol.17. No. 3. Pág. (41-42). Disponible en: <https://www.aaai.org/ojs/index.php/aimagazine/article/view/1230/1131>

²⁷⁰ University of Regina (2018), *Overview of the KDD Process*. Disponible en: http://www2.cs.uregina.ca/~dbd/cs831/notes/kdd/1_kdd.html#:~:text=The%20term%20Knowledge%20Discovery%20in,of%20particular%20data%20mining%20methods.&text=The%20unifying%20goal%20of%20the,the%20context%20of%20large%20databases.

4. Selección de datos (Reducción y proyección de datos): Encontrar características útiles para representar los datos según los objetivos planteados y usar métodos de transformación o reducción de dimensionalidad para reducir el número efectivo de variables en consideración o para encontrar representaciones invariantes para los datos.
5. Elección de la herramienta de minería de datos: Decidir si el objetivo del proceso KDD es clasificación, regresión, agrupación (*clustering*), etc.
6. Elección de los algoritmos de minería de datos: Selección de métodos que se utilizarán para buscar patrones en los datos; decidir qué modelos y parámetros pueden ser apropiados y hacer coincidir un método de minería de datos en particular con los criterios generales del proceso KDD.
7. *Data mining* (Procesamiento de datos): Búsqueda de patrones de interés en una forma de representación particular o un conjunto de representaciones tales como reglas de clasificación o árboles, regresión, agrupamiento (*clustering*), etc.
8. Interpretación de patrones extraídos.
9. Consolidar el conocimiento descubierto.

Figura A.1. Metodología KDD.



Fuente: IFT con información de University of Regina (2018), *Overview of the KDD Process*. Disponible en: http://www2.cs.uregina.ca/~dbd/cs831/notes/kdd/1_kdd.html#:~:text=The%20term%20Knowledge%20Discovery%20in,of%20particular%20data%20mining%20methods.&text=The%20unifying%20goal%20of%20the,the%20context%20of%20large%20databases.

Anexo 3: Análisis de Clúster

En esta sección se mostrará la metodología utilizada para el análisis de conglomerados o *clustering* empleado en la información de las empresas encontradas en México que ofrecen servicios de IoT en los diferentes estados del país clasificadas por el número de empresas que ofrecen servicios de Conectividad, *Software*, *Hardware*, Extremo a Extremo y Otros Mercados Laterales.

Para ello se elaboró un código en el *software* R Studio siguiendo la metodología para este análisis, lo que resultó en los siguientes cálculos: la normalizaron de los datos para calcular la matriz de distancias utilizando la distancia euclidiana y el cálculo de los clústeres correspondientes.

Metodología para el análisis de clúster

El análisis de conglomerados o mejor conocido como *clustering* es una técnica de exploración de datos que permite agrupar objetos con características similares para facilitar su análisis²⁷¹. Esta técnica es uno de los métodos más utilizados en minería de datos para adquirir conocimiento e identificar patrones o grupos similares dentro de un conjunto de datos de interés.²⁷²

Comúnmente se le clasifica como una técnica de aprendizaje no supervisado para el aprendizaje automático (*Machine Learning*)²⁷³, esto último se debe a que este análisis no se guía por ideas *a priori* de qué variables o muestras pertenecen a qué clústeres, sino que el algoritmo de la máquina “aprende” cómo agrupar la información²⁷⁴.

Para llevar a cabo la aplicación de esta técnica entre las observaciones se necesita emplear el término distancia, que dentro del análisis de clúster se emplea como la cuantificación de la similitud o diferencia entre observaciones²⁷⁵. En la literatura se pueden emplear distintas mediciones para el análisis de clúster, para fines de esta investigación se utilizó la distancia euclídea, que sirve para dar mayor peso a aquellas observaciones que están más alejadas al cuadrado.

La distancia euclídea se define como la longitud del segmento que une a dos puntos, p o q , en coordenadas cartesianas y se calcula empleando el teorema de Pitágoras. En el caso del *clustering*, donde se busca agrupar observaciones que minimicen la distancia, pero en una mayor influencia de aquellas observaciones que están más distantes, la distancia euclídea entre dos observaciones equivale a la raíz cuadrada de la suma de las longitudes de los segmentos que unen cada par de puntos²⁷⁶.

²⁷¹ Pham, D., Dimov, S. y Nguyen, C. (2004), *Selection of K in K-means clustering*. Proc. IMechE Vol. 219. Pág. (103). Disponible en: <https://www.ee.columbia.edu/~dpwe/papers/PhamDN05-kmeans.pdf>

²⁷² Kassambara, A. (2017), *Practical Guide to Cluster Analysis in R. Unsupervised Machine Learning*. STHDA. Pág. (3).

²⁷³ Sinaga, K. y Yang, M. (2020), *Unsupervised K-means Clustering Algorithm*. IEEE Access. Pág. (80716). Disponible en: <https://ieeexplore.ieee.org/document/9072123>

²⁷⁴ Kassambara, A. (2017), *Practical Guide to Cluster Analysis in R. Unsupervised Machine Learning*. STHDA. Pág. (3).

²⁷⁵ Amat. J. (2017), *Clustering y heatmaps: aprendizaje no supervisado*. Disponible en: https://www.cienciadedatos.net/documentos/37-clustering_y_heatmaps

²⁷⁶ Amat. J. (2017), *Clustering y heatmaps: aprendizaje no supervisado*. Disponible en: https://www.cienciadedatos.net/documentos/37-clustering_y_heatmaps

Para evitar que se tengan problemas con la magnitud de las distintas variables y esta afecte a la varianza y a los resultados obtenidos por *clustering*, se realizó una estandarización de las variables donde, todas ellas tengan media 0 y desviación estándar 1 antes de calcular la matriz de distancias asegura que todas las variables tengan el mismo peso cuando se realice el *clustering*²⁷⁷.

De la misma manera en que se tienen diferentes distancias para calcular el espacio entre dos puntos en el análisis de clúster, también se ocupan diferentes métodos para su obtención, para esta investigación se empleó el método de *K-means clustering*, que es un método no jerárquico para agrupar objetos (no variables) que divide el set de datos en clústeres distintos, donde ninguna observación puede pertenecer a más de un clúster²⁷⁸.

Para su cálculo se realiza el siguiente procedimiento²⁷⁹: siendo $C_1, \dots, C_k$ el número de variables, la varianza intra-clúster para el clúster C_k , que es una medida $W(C_k)$ de la cantidad que difieren las observaciones dentro del mismo. Se busca minimizar:

$$\sum_{k=1}^k W(C_k)$$

De tal manera que la varianza total dentro de cada clúster, de todos los K clústeres, sea lo más pequeña posible, por lo que se utiliza la distancia euclídea y se obtiene:

$$W(C_k) = \frac{1}{|C_k|} \sum_{i, i' \in C_k} \sum_{j=1}^p (x_{ij} - x_{i'j})^2$$

Siendo $|C_k|$ el número de observaciones en el k -ésimo clúster. Combinando ambas ecuaciones anteriores obtenemos el problema de optimización que define *K-means clustering*:

$$\text{minimize}_{C_1, \dots, C_k} \left\{ \sum_{k=1}^k \frac{1}{|C_k|} \sum_{i, i' \in C_k} \sum_{j=1}^p (x_{ij} - x_{i'j})^2 \right\}$$

Para dividir en n observaciones de k clúster pueden existir al menos K^n maneras, por lo que este puede ser un número muy alto si K y n no son pequeños. Para el caso del algoritmo iterativo de *K-means clustering* para proporcionar un óptimo local se necesita:

1. Asignar un clúster inicial (de 1 a K) de manera aleatoria a cada observación.
2. Iterar hasta que la asignación de cada clúster deje de cambiar: Para cada uno de los K clústeres, calcular el centroide del clúster (vector de medias de las variables j para las observaciones del clúster K).
3. Asignar cada observación al clúster cuyo centroide esté más próximo.

²⁷⁷ Amat, J. (2017), *Clustering y heatmaps: aprendizaje no supervisado*. Disponible en: https://www.cienciadedatos.net/documentos/37_clustering_y_heatmaps

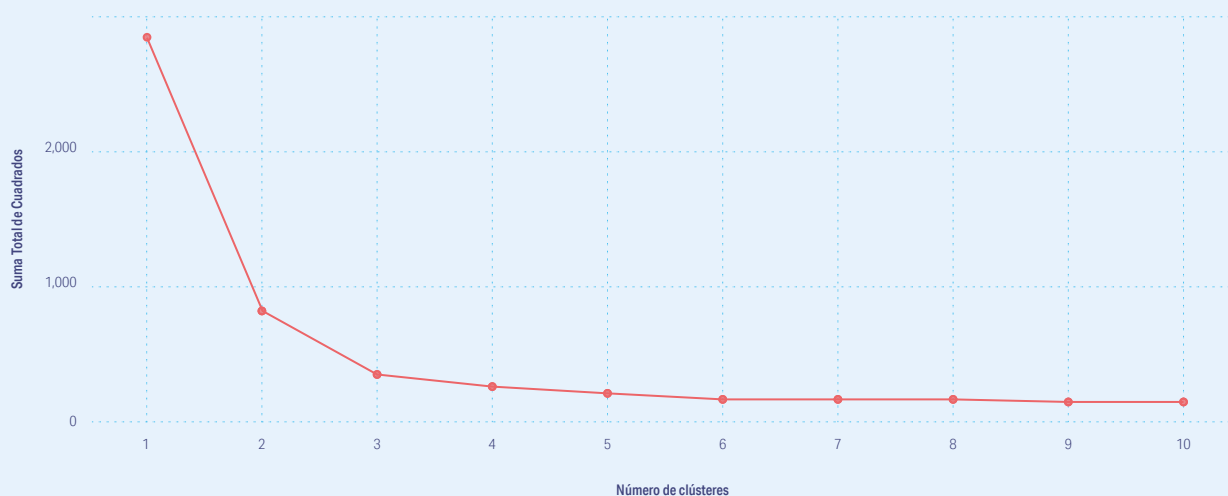
²⁷⁸ Gil, C. (2018), *Métodos de Clustering*. Disponible en: https://rpubs.com/Cristina_Gil/Clustering

²⁷⁹ Gil, C. (2018), *Métodos de Clustering*. Disponible en: https://rpubs.com/Cristina_Gil/Clustering

Algoritmo utilizado en R Studio

El algoritmo k-medias utilizado en el *software* R Studio para el análisis de las 176 empresas encontradas México que ofrecen servicios de IoT en los diferentes estados del país se puede resumir de la siguiente manera:

1. Se estandarizaron los datos de las empresas encontradas en México que ofrecen servicios de IoT en los diferentes estados del país clasificadas por el número de empresas que ofrecen servicios de manera individual, considerando Conectividad, *Software*, *Hardware*, y Otros Mercados Laterales, así como las empresas que ofrecen la combinación de dos, tres y cuatro servicios (Extremo a Extremo) utilizando la librería "norm".
2. El cálculo de la matriz de distancia utilizando la distancia euclidiana mediante el comando "get_dist".
3. El cálculo del número de clúster óptimo utilizando la suma de cuadrados total resulta en 4 clústeres, aunque en la gráfica se observa que con 2 clúster puede resultar óptimos, los resultados mejoraron con la inclusión de los clústeres 3 y posteriormente 4 clústeres, a partir del número 5, la efectividad disminuye marginalmente, por lo que se decidió mantener 4 clúster.
4. Se graficó la información mediante el comando "fviz_cluster", en el caso que existan más de dos dimensiones (variables), el comando realizará un análisis de componentes principales (PCA) y trazará los puntos de datos de acuerdo con los dos primeros componentes principales que explican la mayor parte de la varianza²⁸⁰.



²⁸⁰ AFIT (2017), *K-means Cluster Analysis*. Disponible en: https://afit-r.github.io/kmeans_clustering

ANÁLISIS EXPLORATORIO DE
COMERCIALIZACIÓN DE SERVICIOS DE
**CONECTIVIDAD PARA EL IOT
EN MÉXICO**



INSTITUTO FEDERAL DE
TELECOMUNICACIONES



<http://www.ift.org.mx>

Insurgentes Sur #1143,
Col. Nochebuena, Demarcación
Territorial Benito Juárez,
C.P. 03720, CDMX

Tel: 55 5015 4000 / 800 2000 120