



GOBIERNO DE
MÉXICO



CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES
CIENCIAS Y TECNOLOGÍAS



**BIBLIOTECA INFOTEC
VISTO BUENO DE TRABAJO TERMINAL**

Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC)

Ciudad de México, a 5 de enero de 2024

**UNIDAD DE POSGRADOS
PRESENTE**

Por medio de la presente se hace constar que el trabajo de titulación:

"Directrices mínimas dentro del ecosistema del Internet de las Cosas y su implementación en México"

Desarrollado por el alumno: **Miguel Ángel Acosta García**, bajo la modalidad del **Diplomado en Derecho, TIC e Innovación del INFOTEC** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Mtro. Carlos Josué Lavandeira Portillo
Director Adjunto de Innovación y Conocimiento

Jeh CJLP/jah

C.c.p. Felipe Alfonso Delgado Castillo.- Gerente de Capital Humano.- Para su conocimiento.
Miguel Ángel Acosta García.- Alumno de la Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC).- Para su conocimiento.

Avenida San Fernando No. 37, Col. Toriello Guerra, CP. 14050, CDMX, México.
Tel: 55 5624 2800 www.infotec.mx





MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS
DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E
INNOVACIÓN EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y
CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“Directrices mínimas dentro del ecosistema del Internet de las Cosas y su implementación en México”

Trabajo final del Diplomado
Que para obtener el grado de MAESTRO EN
DERECHO DE LAS TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIÓN

Presenta:

Acosta García Miguel Ángel

Ciudad de México, 28 de noviembre de 2023



Título: Directrices mínimas dentro del ecosistema del Internet de las Cosas y su implementación en México.

Title: Minimum guidelines within the Internet of Things ecosystem and its implementation in Mexico.

Acosta García Miguel Ángel*

RESUMEN

Durante los últimos años el crecimiento del Internet de las Cosas ha sido exponencial ya que presta servicios mediante la interconexión de objetos físicos o virtuales. Lo anterior con apoyo de la interoperabilidad de las tecnologías de la comunicación y de la infraestructura transfronteriza en beneficio de la sociedad de la información. En ese sentido el estado mexicano requiere analizar la viabilidad de establecer la posible regulación del IoT para aumentar la competitividad económica en el mercado y el bienestar de los ciudadanos, pero con una visión regulatoria integral con la participación de diversos sectores para el desarrollo del ecosistema del IoT.

PALABRAS CLAVE: Internet de las Cosas (IoT), regulación, ecosistema del internet, implementación, dispositivos IoT.

ABSTRACT

In recent years, the growth of the Internet of Things has been exponential since it provides services through the interconnection of physical or virtual objects, the above with the support of the interoperability of communication technologies and cross-border infrastructure for the benefit of the society of Information. In this sense, the Mexican state needs to analyze the viability of establishing the possible regulation of the IoT to increase economic competitiveness in the market and the well-being of citizens, but with a comprehensive regulatory vision with the participation of various sectors for the development of the ecosystem of the IoT.

KEYWORDS: *Internet of Things (IoT), regulation, internet ecosystem, implementation, IoT devices.*

* Miguel Ángel Acosta García, miguel_acosta_garcia@outlook.com

Descripción del problema: No existe a nivel nacional ni internacional una regulación jurídica uniforme en materia de IoT, hay múltiples documentos e iniciativas que han buscado su regulación, sin que hasta el momento se haya tenido éxito. En México la regulación existente, la cual no es obligatoria se enfoca a los dispositivos IoT, por lo que se requiere la participación *multistakeholder* para crear una reglamentación jurídica obligatoria a nivel nacional.

Objetivo general: Identificar las directrices mínimas regulatorias del ecosistema del Internet de las Cosas (IoT), que podrían aplicarse en el estado mexicano.

Objetivos específicos: i) Evaluar el marco normativo internacional existente; ii) Analizar la viabilidad de una regulación jurídica del IoT; iii) Establecer directrices mínimas para regular jurídicamente el ecosistema del IoT en México.

Resultados esperados: a) Examinar la implementación de una regulación por parte del Estado mexicano. b) Comparar la regulación implementada en otros países, c) Proponer directrices mínimas de IoT para su ejecución en el estado mexicano.

Lo anterior, resulta viable ya que la comunicación *multistakeholder* genera regulación adecuada para todos los sectores participantes. El principal obstáculo que se observa es la falta de compromiso entre instituciones de gobierno.

Metodología: se utilizó una **metodología cualitativa**, toda vez que la finalidad del presente trabajo fue recoger datos, analizarlos, compararlos y finalmente proponer una regulación jurídica en el Estado mexicano, ya que actualmente no existe un marco normativo obligatorio que deba implementarse para esta tecnología emergente.

En virtud de lo cual, en este trabajo se optó por una metodología cualitativa, misma que se encuentra justificada y centrada en una investigación exploratoria, inductiva, pero sobre todo descriptiva. En ese sentido, esta regulación debe ser dinámica, ajustada a la realidad, lo más apegada a lo que otros países para implementarse en el Estado mexicano.

Máxime que, en otros países también están revisando la viabilidad de regular el ecosistema del Internet de las Cosas, por ello se requiere realizar una serie de actividades como la de estudiar algunos casos, recopilar información, analizar contenido textual y documental, pero sobre todo seleccionar la información más novedosa y reciente que resulte más valiosa para dar cabal cumplimiento a los objetivos del artículo académico.

Método: Se trató de una investigación flexible, seleccionando diversos métodos para contar con información sólida, realista y congruente con el ecosistema del IoT para su posible regulación. En ese orden de ideas, se utilizaron los siguientes métodos: I) Documental: se revisaron fuentes físicas y digitales; II) Histórico: se analizaron algunos acontecimientos pasados previos al IoT; III) Sistemático: se hizo una ordenación coherente de los conocimientos, criterios y doctrina nacional-internacional de la regulación del IoT; IV) Comparativo: se examinó la regulación del IoT en otros países ya que al ser una tecnología emergente su evolución es distinta, de manera que se debe analizar desde la óptica de cada estado para que sea funcional; V) Inductivo: se consideraron hechos aceptados en otros países para intentar aplicarlos en México. VI) Analítico: se hizo una descomposición de diversas regulaciones, VII) Deductivo: se analizaron las conclusiones y aplicaciones de otras propuestas de regulación en diversos países.

Técnicas: Se aplicó la observación para percibir los elementos básicos que deben encontrarse dentro del ecosistema del IoT, se recopiló, revisó, analizó y se propusieron diversas directrices que deben de implementarse en el Estado mexicano por cuanto hace al ecosistema del IoT, las cuales podrán ser utilizadas para establecer un piso mínimo para hacer a la regulación mexicana.

1. Introducción

El Internet de las Cosas (IoT), es una tecnología de la información revolucionaria que combina el mundo físico-digital, creando un ecosistema de objetos conectados a internet a efecto de que funcionen en el mundo terrenal. En muchos países se ha discutido desde los 2000's sobre su importancia, características y conceptos básicos, así como una posible regulación.

De esta manera, el IoT se basa en la correcta funcionalidad ofrecida por todas las tecnologías de la información y comunicación (TIC) emergentes, en la que todo el entorno físico conviva conectado mediante una red totalmente interactiva y receptiva. Por ello, resulta necesario analizar la viabilidad de regular el IoT en México para que sea plenamente funcional para promover directrices mínimas en función de respetar los derechos humanos dentro y fuera del mundo digital¹.

Ello es así, debido a que el IoT llegó a cambiar la forma y el entorno de: 1) las empresas, que deben realizar sus actividades operativas, mejorar la productividad, reducir los costos finales así como buscar nuevos mercados para la generación de ingresos; 2) los estados, deben implementar mecanismos para fomentar su crecimiento, incentivar la inversión, mejorar la infraestructura y convertirse en un gobierno que ejecute las TIC para que sean seguras y durables; para lograr lo anterior, se requieren mecanismos regulatorios para su pleno funcionamiento; 3) la población en general, para utilizar y explotar el ecosistema del IoT, con la finalidad de lograr mayores beneficios colectivos.

Con base en lo anteriormente señalado, es evidente que el IoT, es una tecnología emergente, transformadora y disruptiva, que debe ser llevada por la trilogía social: el sector público, privado, y la sociedad, -siendo el dirigente el gobierno-, ya que implica cuestiones culturales, económicas, sociales y políticas. Por ello deben

¹ Unión Internacional de Telecomunicaciones (2005), The Internet of Things, fecha de consulta: 01 de julio de 2023, disponible en: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

implementarse algunos mecanismos o directrices, debido a que actualmente no existe una regulación obligatoria en el país para esta tecnología emergente, por ello se requiere un piso mínimo para apresurar la implementación y adopción del IoT en el país.

Por esta razón, hay que precisar que el objetivo del presente trabajo de investigación es identificar las directrices mínimas para una posible regulación jurídica del ecosistema del IoT, dentro del estado mexicano. En ese orden de ideas, se revisó el marco internacional y nacional existente; se identificaron varias tendencias regulatorias y se analizaron algunos foros, seminarios, conferencias, talleres, mesas redondas, llevados a cabo por autoridades, organizaciones nacionales o internacionales. Revisada toda la información recopilada, se depuró, analizó y concluyó la necesidad de implementar una serie de directrices mínimas que deberían tomarse en consideración para la regulación del ecosistema del IoT en México.

2. Generalidades del ecosistema del Internet de las Cosas.

2.1. Teorías.

En el presente artículo solo se mencionarán algunas teorías relativas al ámbito de regulación del Internet de las Cosas:

El IoT puede ser analizado desde distintas perspectivas, ya sea: i) técnica-jurídica, analizando la normatividad técnica aplicable al ecosistema IoT, -la cual no es vinculante-; la implementación de una estandarización de los objetos e infraestructura para su debido uso o su homologación a efecto de armonizar todo el régimen técnico a nivel nacional e internacional; ii) arquitectura de objetos inteligentes, hardware y software que puedan convivir en los entornos físicos creando un aprendizaje que se pueda adaptar y optimizar de manera autónoma. En esta teoría se examinan las capas de aplicaciones que permiten interactuar con los diferentes dispositivos inteligentes mediante la aplicación de procedimientos y, iii) tipo de mercado-proyecto que se desarrolla e implementa en un mercado específico,

utilizando tecnologías de corto alcance, de redes móviles, conectividad satelital o el uso de espectro radioeléctrico para la provisión de servicios y aplicaciones de radiocomunicaciones.

Ahora bien, al presente trabajo de investigación le corresponde examinar una perspectiva regulatoria desde el ámbito del gobierno, en el que se debe establecer un panorama básico fundamental para que se respeten, protejan, promuevan y salvaguarden los derechos humanos en todos los equipos, dispositivos, productos, infraestructura que tenga relación con el Internet de las Cosas.

2.2. Conceptos clave.

Para el presente trabajo se utilizarán los siguientes conceptos y definiciones:

Autoridad: Toda entidad de la Federación, de los Estados, de la Ciudad de México, de los Municipios, de sus entidades y dependencias, así como instituciones y organismos autónomos, y cualquier otro ente público;

Dispositivo IoT: Componente o fragmento de un equipo, el cual puede utilizar espectro radioeléctrico o bien estar conectado a redes de telecomunicaciones, los cuales pueden ser fijos o portátiles con capacidad opcional de teledetección, accionamiento, captura, almacenamiento y/o procesamiento de datos, guardando relación con un servicio asociado².

Fabricante de Dispositivos IoT: Persona física o moral que crea un Dispositivo IoT y se puede integrar a otros productos o componentes³.

² Instituto Federal de Telecomunicaciones (2022), Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las Cosas (IoT), fecha de consulta: 01 de julio de 2023, disponible en: https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

³ *Ídem.*

Internet de las cosas (IoT): Infraestructura mundial al servicio de la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas gracias a la interoperabilidad de tecnologías de la información y la comunicación (existentes y en evolución)⁴;

Entidad del mundo real: Entidad física y lógica que actúa principalmente o se utiliza en el mundo real, tal como un objeto físico, un objeto lógico, un lugar o una persona.

Objeto: Se trata de cualquier cosa del mundo físico o virtual que puede identificarse e integrarse en las redes de comunicaciones⁵.

TIC: Tecnologías de la Información y Comunicación

2.3 Antecedentes del IoT

A partir del surgimiento del Internet en los 60's, se ha buscado que las máquinas, estén conectadas, transmitan información y por supuesto se comuniquen entre ellas, pero fue hasta la década de los 80's cuando se monitorearon medidores conectados a una red eléctrica de manera remota a través de líneas telefónicas, o cuando una empresa refresquera (Coca Cola), fue capaz de supervisar a la distancia -conectada a internet- una maquina dispensadora, con la finalidad de saber si el producto estaba frio y había disponibilidad del mismo, evitando inspecciones por personal técnico. Esta nueva tecnología emergente consistía en la comunicación máquina a máquina (M2M), la cual era una red especial dedicada al monitoreo de equipos, (misma que no abordaremos en esta investigación).

Pero fue hasta 1999 cuando Kevin Ashton, un profesor del MIT, uso el término Internet de las Cosas para describir a un sistema en el que cualquier objeto del

⁴ Unión Internacional de Telecomunicaciones (2012), Recomendación UIT-T Y.2060, Descripción General de Internet de los objetos, fecha de consulta: 26 de septiembre de 2023, disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2060-201206-1!!PDF-S&type=items

⁵ *Ídem*, p. 8.

mundo terrenal puede conectarse a Internet mediante la utilización de sensores o las etiquetas de identificación por radiofrecuencia utilizados en el seguimiento de las mercancías de una empresa, sin la necesidad de la intervención humana. Un año después la empresa LG anunció la creación de un refrigerador que se podía conectar a Internet.

Entre 2008 y 2009, esta tecnología emergente, rápidamente escaló en diversos mercados a nivel mundial ya que se comenzó a utilizar en diversos dispositivos para conectarlos a la red de redes, lo que trajo un crecimiento exponencial en el uso de dispositivos inteligentes como: celulares, tabletas, computadoras y electrodomésticos. Actualmente la lista comienza a ser interminable debido a que se busca conectar cualquier objeto a internet.

Actualmente, la mayoría de los dispositivos están conectados al protocolo de internet (IP), mismo que ayuda al intercambio de información entre redes, ya que instauró un esquema de numeración, que facilita la conexión de dispositivos al Internet, mismo que se encuentra conformado por 32 bits con hasta 12 caracteres divididos en 4 de bloques de 3 caracteres cada uno (IPV4). No obstante, lo anterior, este protocolo ya se encuentra casi en su máxima capacidad, de modo que comienza a ser desplazado por la última versión del Protocolo de internet (IPV6), el cual cuenta con mayor capacidad ya que utiliza 128 bits lo que se compara con la disponibilidad de granos de arena en el planeta⁶.

Bajo esa tesitura, el IPV6 es el complemento perfecto para el IoT, ya que potenciará la conexión de cualquier dispositivo, la comunicación será más fluida, sus los procesos más eficientes para lograr una conectividad universal. De esta manera, como consecuencia de la Cuarta Revolución Industrial, se ha buscado que el IoT logre la hiperconectividad de equipos y de personas, con directrices básicas

⁶ Unión Internacional de Telecomunicaciones (2013), Cuestiones relativas a IPv4 e IPv6, fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ipv4-ipv6-es.pdf>

suficientes para abarcar todo el espectro regulatorio del IoT y ejercer el derecho humano al progreso científico y sus aplicaciones⁷.

En suma, IoT, es una infraestructura global de la sociedad de la información, la cual consiste en la recepción y transferencia de datos a través de redes inalámbricas, en la interconexión de objetos físicos o virtuales llevándolo a un ecosistema en el que se detectará, adaptará, comunicará e interconectará cualquier objeto con la vida de las personas haciéndolas más eficientes, seguras y fáciles de usar dentro del mundo digital en beneficio al mundo terrenal. Por ello se requieren servicios avanzados e interoperables, con la finalidad de reducir tiempos y emplear de manera efectiva las nuevas tecnologías en la vida cotidiana de cualquier persona.

2.4. Regulación del IoT a nivel internacional

La seguridad y la protección en el Internet son fundamentales para los millones de objetos que ya se encuentran conectados; por ello es necesario contar con regulación precisa y clara, o bien, establecer reglas internacionales que combinen aspectos sociales, económicos, políticos, tecnológicos, pero sobre todo incentivar la inversión de infraestructuras.

2.4.1. Unión Europea

En ese orden de ideas, en 2005 la Unión Europea emitió el plan “*2010: Una sociedad de la información europea para el crecimiento y el empleo*”, en el que se propuso una serie de políticas básicas para el desarrollo del espacio único europeo de información, innovación e inversión en la investigación e inclusión, mejorando los servicios para los ciudadanos.

⁷ Organización de las Naciones Unidas, (2023) Pacto Internacional de Derechos Económicos, Sociales y Culturales, artículo 15, inciso b), fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>

Consecuencia de lo anterior, se han emitido diversas directivas entre las que destacan la Directiva 2014/53/UE (Estandarización); el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), que trata sobre la privacidad, protección de datos y propiedad; la Directiva 2013/40/UE (cibercriminalidad); la Iniciativa de Comunidades Conectadas (Infraestructura); y la Unión por la innovación de Europa 2020 (Financiación mediante los Programas Macro).

De las iniciativas anteriores, se desprende que la Comisión Europea como agente regulador se ha enfocado en cinco temas y políticas sobre IoT, con la finalidad de que las empresas europeas generen mayor competitividad, inversión y con ello incentivar la economía basada en las tecnologías emergentes para lograr la transición digital. En 2022, se lanzó la iniciativa de la Comisión Europea “*Alianza para la Innovación en Internet de las Cosas y Edge computing*”⁸, la cual ha buscado promover la construcción de ecosistemas, que use IoT y *Edge Computing* para las empresas europeas que decidan participar.

En ese sentido, la Unión Europea a través de una cooperación eficaz y estrecha entre sus distintas autoridades, está liderando ámbitos como la legislación, la normalización, la interoperabilidad, la ciberseguridad y las TIC sostenibles. Además, se ha preocupado por la investigación, la innovación y el despliegue de infraestructura en todo el territorio, logrando trabajar con el sector privado y la sociedad para acelerar todos los procesos tecnológicos.

2.4.2. Reino Unido

En 2017, la Oficina de Relaciones Exteriores, Territorio y Desarrollo del Reino Unido, implementó el programa *IoTUK*⁹, con el cual logró la adopción más rápida dentro del sector público-privado, generando para este último la posibilidad de crear

⁸ Alliance for IoT and Edge Computing Innovation IVZW (AIOTI), (2021), fecha de consulta: 25 de septiembre de 2023, disponible en: <https://aioti.eu/>

⁹ IoTUK, (2018), Benefits and Challenges of IoT, fecha de consulta: 25 de septiembre de 2023; disponible en: <https://iotuk.org.uk/wp-content/uploads/2018/09/IoTUK-survey-report.pdf>

nuevos nichos de mercados, inversión en la innovación y actualización de productos, así como visualizar a la IoT como una tecnología confiable y benéfica para cualquier persona.

Por otro lado, Ofcom, el regulador de telecomunicaciones ha otorgado licencias especiales de espectro radioeléctrico para que sean usadas por dispositivos IoT, los cuales pueden contar o no con licencia. Lo anterior, bajo los lineamientos de la *Wireless Telegraphy Act*. Para el caso de que se requiera de licencia debe ser en las 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; otorgándoles una licencia de *Business Radio Internet of Things*.

2.4.3. Japón

La Agencia de Promoción de la Tecnología de Información¹⁰ (IPA, por sus siglas en inglés), incentiva a que los desarrolladores participen en actividades para proporcionar productos y servicios de IoT, desde requisitos de seguridad, protección confiabilidad de los dispositivos hasta temas de calidad. Por lo anterior, la IPA ha desarrollado varias guías en aspectos técnicos, de seguridad, protección del proceso, calidad del producto y servicio.

De igual manera, en 2020, el Ministerio de Economía, Comercio e Industria (METI, por sus siglas en inglés), publicó el “*Marco de seguridad de IoT*”¹¹, en el cual introdujo los conceptos de “industrias conectadas” y “Sociedad 5.0” con la intención de usar IoT para garantizar la confiabilidad de las conexiones entre el ciberespacio y el espacio físico, logrando la conversión de la información entre fronteras.

2.4.4. Arabia Saudita

¹⁰ Information-technology Promotion Agency (2023), fecha de consulta: 25 de septiembre de 2023; disponible en: <https://www.ipa.go.jp/en/about/index.html>

¹¹ Ministry of Economy, Trade and Industry (2020), IoT Security Safety Framework (IoT-SSF), fecha de consulta: 25 de septiembre de 2023; disponible en: https://www.meti.go.jp/english/press/2020/1105_002.html

La Comisión de Comunicaciones y Tecnología de la Información (CITC, por sus siglas en inglés), es el regulador de Telecomunicaciones y las Tecnologías de la Información (TI), incluyendo por supuesto el IoT. Arabia Saudita buscó ser el pionero en la regulación del Internet de las Cosas, por lo que dividió los servicios que se pueden hacer a través de esta tecnología emergente en servicios de IoT que se proveen a través de: i) redes móviles; ii) redes fijas y, iii) frecuencias que no requieren licencia.

En los dos primeros casos se requiere contar con una licencia para poder ofrecer el servicio, mientras que para la última existe la **disposición técnica RI114**, que describe los requisitos para estas frecuencias de manera regulada por el estado¹².

2.4.5. Estados Unidos

En 2017, el Departamento de Comercio, publicó el documento “*Fostering the advancement of the internet of things*”¹³, cuyo objetivo fue identificar todos los elementos necesarios para fomentar la implementación del IoT a través de una estrategia nacional de IoT. Además, se analizaron las diferencias tecnológicas que representa el IoT, así como sus beneficios y desafíos, con lo cual se concluyó la necesidad de la participación obligatoria del Estado para la correcta funcionalidad del IoT en el país. Por otro lado, en 2020, el Congreso de Estados Unidos publicó la iniciativa H.R.1668 sobre la ley de mejora de la ciberseguridad de IoT¹⁴,

¹² Communications and Information Technology Commission of Saudi Arabia, (2019), CITC Technical Specification, RI114, Specification for License-Exempt LPWAN Devices, fecha de consulta: 25 de septiembre de 2023; disponible en: cst.gov.sa/ar/RulesandSystems/RegulatoryDocuments/EquipmentApproval/Documents/TA E RI114.pdf

¹³ Department of Commerce, (2017), Fostering the advancement of the internet of things, fecha de consulta: 27 de septiembre de 2023, disponible en: https://www.ntia.gov/sites/default/files/publications/iot_green_paper_01122017_0.pdf

¹⁴ Congreso de Estados Unidos, (2020), H.R.1668 - IoT Cybersecurity Improvement Act of 2020, fecha de consulta: 27 de septiembre de 2020, disponible en: <https://www.congress.gov/bill/116th-congress/house-bill/1668/text#:~:text=To%20establish%20minimum%20security%20standards,Government%2C%20and%20>

estableciendo estándares mínimos de seguridad en la fabricación de dispositivos IoT.

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), dependencia del Departamento de Comercio cuenta con un programa de ciberseguridad enfocado al IoT, denominado “NIST Cybersecurity for IoT”, el cual en septiembre de 2022¹⁵, realizó un taller para determinar los pasos a seguir en materia de ciberseguridad de los dispositivos conectados al IoT, no obstante, aún no se cuenta con una versión final del documento.

2.4.6. Canadá

El Consejo de Normas de Canadá (SCC, por sus siglas en inglés), es la institución que se encarga de emitir normas y estándares técnicos sobre un campo en específico, siendo relevante señalar que, actualmente hay más de veinte estándares para IoT, referentes a temas como la seguridad y privacidad de IoT, requisitos básicos del dispositivo, ciberseguridad, arquitectura, interoperabilidad, aplicaciones de IoT, entre otras¹⁶.

La Oficina del Comisionado de Privacidad (OPC, por sus siglas en inglés), emitió la Guía de privacidad para fabricantes de dispositivos de Internet de las Cosas, enfocada para aquellas personas que producen o diseñan dispositivos con tecnología de IoT, a fin de cumplir con los aspectos de privacidad estipulados en la ley de la materia.

¹⁵ Megas, K., Fagan, M., Cuthill, B., Hoehn, B., Lemire, D. y Herold, R. (2022), Informe resumido del taller para "Building on the NIST Foundations: Next Steps in IoT Cybersecurity", NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, fecha de consulta: 27 de septiembre de 2023, disponible en: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8431.pdf>

¹⁶ Standards Council of Canadá (2023), listado de estándares, fecha de consulta: 27 de septiembre de 2023, disponible en: <https://www.scc.ca/en/search/standardsdb/iot>

2.4.7. Brasil

En junio de 2019, mediante el decreto 9.854¹⁷, el gobierno brasileño implementó el Plan Nacional de Internet de las Cosas que creó una Cámara de Gestión y Seguimiento del Desarrollo de los Sistemas de Comunicación Máquina a Máquina y del IoT, la cual se encargará de monitorear su implementación. Sin lugar a duda este documento da la certeza jurídica que se requiere para el desarrollo de esta tecnología emergente ya que brinda soluciones viables y eficaces en distintos sectores como el industrial, la agricultura, el crecimiento y la creación de ciudades inteligentes, la seguridad pública, la educación y por supuesto la salud.

Por su parte la Agencia Nacional de Telecomunicaciones (ANATEL), se encuentra desarrollando un modelo regulatorio para IoT, con la finalidad de eliminar las barreras regulatorias que pudieran existir y que impiden la expansión de las aplicaciones de IoT.

3. México ante el ecosistema del Internet de las Cosas.

En 2013, derivado del Pacto por México¹⁸, se llevó a cabo la reforma en materia de telecomunicaciones y radiodifusión, la cual modificó el artículo 6° constitucional para garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluyendo la banda ancha y el internet.

En consecuencia, el gobierno mexicano emitió la Estrategia Digital Nacional 2013-2018, con la finalidad de fomentar la adopción y el desarrollo de las TIC, a través de

¹⁷ Ministerio de Ciencia, Tecnología, Innovación y Comunicaciones (2019), Decreto No. 9.854 de 25 de junio de 2019, fecha de consulta 27 de septiembre de 2023, disponible en: https://www.planalto.gov.br/ccivil_03/ato2019-2022/2019/decreto/d9854.htm

¹⁸ Secretaría de Relaciones Exteriores (2012). Pacto por México, fecha de consulta: 25 de septiembre de 2023; disponible en: https://embamex.sre.gob.mx/bolivia/images/pdf/REFORMAS/pacto_por_mexico.pdf

cinco objetivos para que la población se convirtiera en una sociedad de la información y el conocimiento. No obstante, lo anterior, dicha estrategia no logró el objetivo dentro del plazo señalado, resultando importante precisar que este documento federal tampoco estipuló alguna estrategia en beneficio del Internet de las Cosas.

Debe señalarse que, de 2018 a 2020, no se contó con alguna Estrategia Digital Nacional, implementada por el gobierno mexicano. En septiembre de 2021, el Gobierno Federal publicó la Estrategia Digital Nacional 2021-2024¹⁹ con la intención de exponer las acciones que se implementarían para el uso y desarrollo eficiente e incluyente de las TIC, en torno a dos ejes: i) Política Digital en la Administración Pública Federal y ii) Política Social Digital en cumplimiento al artículo 6° garantizando el derecho de acceso a las TIC, sin embargo, también se omitió considerar alguna directriz para la implementación del IoT.

Empero lo anterior, el Instituto Federal de Telecomunicaciones (IFT), en años recientes ha tratado de abordar el tema del IoT en diversos documentos, siendo uno de los más importantes la Hoja de Ruta 2021-2025,²⁰ la cual busca ser un instrumento que de claridad al camino que debe seguirse para la transformación digital. Este documento cuenta con diversos objetivos, siendo importante para el tema de investigación el objetivo 3, que busca “*promover el desarrollo del ecosistema digital y la adopción de nuevas tecnologías y casos de uso digitales*”, con lo cual se ha buscado favorecer un desarrollo regulatorio en los sectores productivos de la sociedad.

¹⁹ Diario Oficial de la Federación, Estrategia Digital Nacional 2021-2024, fecha de consulta: 25 de septiembre de 2023, disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0

²⁰ Instituto Federal de Telecomunicaciones (2020), Estrategia IFT 2021-2025, Hoja de Ruta, fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025.pdf>

A partir de lo supra señalado, el regulador en telecomunicaciones y radiodifusión se ha dado a la tarea de emitir en 2020 y en 2022 un “*análisis sobre la comercialización de servicios de conectividad para IoT*”²¹, que ha servido para que las empresas que ofrecen servicios de IoT informen sobre la evolución, retos, logros y expectativas que se tienen sobre esta tecnología emergente y su comercialización en los próximos años, pero no se menciona nada sobre los aspectos regulatorios técnicos o jurídicos que deben emplearse para guiar a las empresas.

En esa misma tesitura, el IFT en la Cuarta Encuesta 2021 Usuarios de Servicios de Telecomunicaciones²², encontró que la sociedad refirió que conoce algo sobre el IoT (8.7%), e inclusive manifestaron que adquirirían algún dispositivo con esta tecnología (55.9%), debido a que se tratan de dispositivos más prácticos, cómodos y seguros (53.2%), empero, también encontraron desventajas como el hecho de que los dispositivos deben permanecer en todo momento conectados a internet (27.1%), lo cual podría traer como consecuencia fallas en la conexión (15.3%), o bien una posible vulneración a sus sistemas de seguridad (20.8%), lo que podría afectar su vida digital.

Finalmente hay que precisar que el IFT se ha centrado en la elaboración de un “*código de mejores prácticas para la ciberseguridad del IoT*”, enfocado en los dispositivos IoT que utilicen espectro radioeléctrico o bien sean conectados a través de redes de telecomunicaciones.

Pero lo cierto es que el regulador en telecomunicaciones y radiodifusión en el país tampoco se ha preocupado por análisis la viabilidad de contar con una regulación

²¹ Instituto Federal de Telecomunicaciones (2022), Análisis exploratorio de comercialización de servicios de conectividad para el IOT en México, fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/analisisexploratorioiotmexico.pdf>

²² Instituto Federal de Telecomunicaciones (2021), Cuarta encuesta 2021, Usuarios de Servicios de Telecomunicaciones, fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/4taencuesta2021acc.pdf>

del ecosistema del IoT, ya que no ha emitido ninguna consulta pública, ni mucho menos ha publicado alguna disposición técnica, por lo que, los documentos existentes solamente se enfocan en recopilar información.

3.1 Regulación Técnica del IoT en México

En México existen seis normas mexicanas las cuales fueron impulsadas por el Organismo Nacional de Normalización y Certificación (NYCE), quien se encarga de ajustar y adaptar el proceso y sus características a todos los productos, servicios o procedimientos con la finalidad de homologación dentro del ecosistema del IoT²³. Dichas normas mexicanas -las cuales no son obligatorias-, abordan los siguientes temas:

1. NMX-I-1362-NYCE-2021. Telecomunicaciones-Procedimiento simple de encriptación para entornos de Internet de las Cosas (IoT);
2. NMX-I-4903-NYCE-2021. Telecomunicaciones- Indicadores clave de desempeño relacionados con las ciudades inteligentes y sostenibles, para evaluar el logro de los objetivos de desarrollo sostenible;
3. NMX-I-20000-3-NYCE-2021. Tecnologías de la información-Gestión del servicio;
4. NMX-I-22301-NYCE-2021 1. Tecnologías de la información-Seguridad y resiliencia Sistemas de gestión de la continuidad del negocio- Requerimientos;
5. NMX-I-20000-7-NYCE-2021. Tecnologías de la Información – Gestión del Servicio Parte 7;
6. NMX-I-22316-NYCE-2021. Tecnologías de la información-Seguridad y resiliencia-Resiliencia organizacional-Principios y atributos

²³ Alonso, Jessica, (2022), Normas Oficiales Mexicanas para Dispositivos IoT, Asociación Mexicana del Internet de las Cosas (IoT), fecha de consulta: 25 de septiembre de 2023, disponible en: <https://www.asociacioniot.org/2022/10/27/normas-oficiales-mexicanas-para-dispositivos-iot/>

Resulta importante precisar que las seis normas mexicanas supra señaladas no tienen el estatus legal de obligatorias para la sociedad mexicana, por esta razón su observancia es optativa y en consecuencia puede o no seguirse dentro del campo regulatorio mexicano.

3.2 Regulación Jurídica del IoT en México

Después de una revisión al marco jurídico mexicano, se puede apreciar una falta de regulación para el Internet de las Cosas, si bien existen normas mexicanas, las mismas tienen el carácter de voluntarias, lo cual impide en algunos casos su implementación total y correcta. Por ello resulta importante que cada *stakeholder*, en el ámbito de sus atribuciones pueda participar en la creación de una normativa que sea dinámica y establezca un piso mínimo a seguir.

En esa tesitura, el gobierno mexicano debe legislar en materia de IoT para que todos los participantes dentro del ecosistema conozcan su responsabilidad, en el entendido de que las empresas deben tener un marco regulatorio claro y un procedimiento sencillo, para que la sociedad pueda contar con dispositivos de calidad y el gobierno consiga dar directrices básicas y concretas a seguir dentro del IoT.

En virtud de lo anterior, regular el IoT debe ser abordado desde una perspectiva técnica-jurídica, en el entendido de que no solo se conectarán pequeños objetos, sino que se pretende conectar todos los servicios que se puedan ofrecer a una ciudad, sin embargo, el estado mexicano no ha emitido un parámetro mínimo asociado al IoT.

Lo anterior resulta relevante pues, la propuesta de este artículo radica en el establecimiento de unas directrices mínimas técnicas-jurídicas que deban tomarse en consideración para un posible programa nacional que se encargue de regular el ecosistema del IoT que se utilice en todo el territorio mexicano y, por supuesto debe ser homologado con las mejores prácticas en el mundo. Así como la manera en que deban ser tratados todos los datos que se recopilen, almacenen y analicen con la

finalidad de optimar y automatizar tareas, lo cual implicará la participación de todos los *stakeholders* del estado mexicano.

4. Posible Regulación.

En 2022, se encontraron conectados al ecosistema del IoT alrededor de 35.370 millones de dispositivos con tecnología IoT, motivo por el cual se estima que el número de objetos conectados a IoT aumente en los siguientes años hasta alcanzar cerca de 66.000 millones de unidades en 2026.²⁴ Por ello es necesario acelerar la implementación de conceptos únicos y soluciones precisas dentro del ecosistema IoT, lo cual llevará a contar con una regulación concisa y precisa para el gobierno mexicano, automatizar los procesos para las empresas, mejorar la experiencia de los usuarios finales pero sobre todo planificar sobre los posibles retos y tendencias innovadoras que se podrán implementar gracias al uso de la tecnología del IoT.

Lo anterior, sin lugar a duda es un gran desafío, ya que la demanda de objetos conectados a internet sigue en aumento, hasta interconectar cosas más grandes por ello es imperante la existencia de una regulación que permita el máximo aprovechamiento de la tecnología emergente, su conexión con cualquier dispositivo y el máximo aprovechamiento de la infraestructura de cada país.

Actualmente, no existen estándares internacionales que puedan ser aplicados al uso del Internet de las Cosas, a pesar de los múltiples esfuerzos realizados por organizaciones internacionales, varios países han tratado de crear parámetros para la regulación del Internet de las Cosas, pero lo cierto es que, tampoco existen parámetros aceptados a nivel internacional.

La propuesta de atención al objetivo planteado dentro del presente artículo cumpliría con los alcances y metodología desarrollada previamente ya que, va enfocada a la

²⁴ Perez, Cecilia, (2023) The Top Growth Opportunities for IoT in 2023, Frost & Sullivan, fecha de consulta: 01 de octubre de 2023, disponible en: <https://www.frost.com/frost-perspectives/the-top-growth-opportunities-for-iot-in-2023/>

creación de directrices que sean aceptadas a nivel nacional, los cuales deben ser dinámicos y actualizables de manera sencilla y rápida junto con la evolución del IoT.

Ahora bien, resulta preciso enunciar que el IoT puede encontrarse en todos los sectores dentro de una sociedad, entre ellos tenemos los hogares, que serán espacios en los que se permite automatizar el entorno de una persona a sus gustos, entorno, habitaciones sala, cocina, baño, entre otros.

Por otro lado, la importancia del IoT en diversos mercados ha sido tan relevante que las ciudades inteligentes comienzan a analizar la viabilidad de controlar y monitorizar el tráfico, las luces, la inspección a distancia de las casas, edificios, puentes por medio de sensores mostrando en tiempo real cualquier defecto. Los automotores buscan monitorear, controlar, revisar parámetros de gasolina, aceite o aire, los cuales serían reportados por la computadora y corregidos evitando mayores riesgos.

En ese mismo sentido, el IoT puede ayudar a curar o prevenir enfermedades a monitorear los tratamientos, enviar reportes a los médicos con el objetivo de preservar la salud del paciente. Otro mercado es el medio ambiente, ya que se puede utilizar para cultivar, recolectar, avisar sobre la necesidad de líquidos para flora o fauna e indicar niveles de contaminación dentro de una localidad.

Por todo lo anteriormente señalado se deben tomar en cuenta los siguientes parámetros dentro de la regulación del IoT:

La Alianza *Multistakeholder*²⁵, será una herramienta esencial para que los gobiernos, la academia e investigación y los propios miembros de la sociedad implementen mejoras en la forma en que se van a utilizar los objetos que se encuentren conectados a la red.

²⁵ Internet Society, (2016), Gobernanza de Internet- Porqué funciona el enfoque de múltiples partes interesadas, fecha de consulta: 01 de octubre de 20223, disponible en: <https://www.internetsociety.org/es/resources/doc/2016/gobernanza-de-internet-por-que-funciona-el-enfoque-de-multiples-partes-interesadas/>

La Confianza: la influencia mutua entre los distintos *multistakeholder* permitirá la creación de motores de construcción de IoT para que disfruten de mejoras y su buen funcionamiento.

La continuidad y disponibilidad: consiste en que los objetos que serán utilizados por el usuario final se vayan agregando al IoT sin necesidad de comenzar desde cero cada vez que adquiera un nuevo producto.

Los términos y condiciones, deben ser cláusulas legales básicas que expresen la forma en que se utilizará, entre otras cosas, la información recopilada por los dispositivos IoT.

La **actualización del software:** permitirá que todos los objetos se encuentren con las protecciones más recientes y que pueden ser utilizados sin mayor contratiempo o problemática, lo que se busca es que cada software al igual que va actualizándose estas disposiciones puedan hacer lo mismo.

La **comunicación segura** ya que se encargará de que toda la interconexión y toda la información que atraviese el ecosistema de una persona pueda ser totalmente fiable y sin preocupaciones de posibles fallas a la interacción entre el usuario final y su objeto.

La **privacidad:** permitirá que todas las personas conozcan el uso que se dará a su información y quien puede acceder a ella, es decir, ejercer su derecho a la autodeterminación informativa de las personas.

La **protección de datos:** será todas aquellas prerrogativas que tienen las personas de que su información se mantenga y sea procesada de manera adecuada, sin el temor de que puedan ser encontradas por usuarios que pudieran hacer mal uso de ellas, por ello, resulta esencial el cuidado de la información personal.

El respeto a los **derechos fundamentales:** para detectar cualquier vulneración o restricción a estos derechos y prever mecanismos para su defensa y protección, fungiendo como eje vertebral del enfoque del IoT.

La **interconexión** es necesaria para enlazar múltiples puntos de intercambio de información.

Las **normas éticas**: tendrán como objetivo la dignificación y el reconocimiento social en el mundo digital, a efecto de regular las acciones de los seres humanos, y que sus efectos no sean trasladados y afectados durante dicha digitalización, por ello se debe de reconocer estos elementos con la característica de ser universales.

El **almacenamiento** debe cuidarse toda la información procesada y guardada, mediante la ejecución de medidas de seguridad adecuadas que la protejan.

La **adaptabilidad** de los dispositivos IoT debe ser una realidad, conforme avance la innovación tecnológica.

Con los elementos anteriormente señalados, y dada la importancia e impactó que está teniendo IoT en la transformación digital, se hace notable la necesidad crear un Comité de Internet de las Cosas, con sus reglas de operación siguientes:

5. Propuesta de directrices mínimas para la regulación del IoT en México.

- I. Las presentes directrices mínimas tienen por objeto establecer las pautas y límites a las que deberán sujetarse todos los gobiernos, empresas, fabricantes, usuarios finales que utilicen el ecosistema del Internet de las Cosas, así como los dispositivos físicos o virtuales que utilicen la tecnología del Internet de las cosas en cualquier lugar del territorio nacional.
- II. Las directrices mínimas se rigen por los principios de certeza, independencia, objetividad, eficiencia, legalidad, igualdad, confiabilidad, profesionalismo, eficacia y respeto a los derechos humanos.
- III. El gobierno mexicano a través de la Secretaría de Gobernación y de manera específica la Coordinación de Estrategia Digital Nacional y el Instituto Federal de Telecomunicaciones se encargarán de coordinar la correcta implementación del IoT en el Estado mexicano.

- IV.** Los dispositivos físicos o virtuales deben de contar al menos con capacidad de comunicación para poder emplear la tecnología IoT.
- V.** Los elementos básicos del IoT son los siguientes:
- VI.** Comunicación:
 - a. Conectividad: Encadenamiento entre un objeto y el Internet de las Cosas.
 - b. Compatibilidad: Condición que hace que un objeto y el ecosistema del Internet de las Cosas se logren comprender e intercambien información y servicios.
 - c. Seguridad: Mecanismo que protege todo objeto conectado a internet frente a amenazas, en ámbitos tales como la confidencialidad, autenticidad e integridad de datos y servicios, así como corregir las vulnerabilidades de los dispositivos IoT.
 - d. Privacidad de datos:
 - e. Protección de la privacidad: Toda la información y datos que contengan los dispositivos IoT
 - f. Dinamismo: Entender que los dispositivos se modificarán en su contexto, ubicación, velocidad, transferencia de datos, por ende, se requiere que los dispositivos se vayan adecuando al ecosistema del IoT.
 - g. Implementación;
 - h. Integración de sistemas;
 - i. Interconexión;
 - j. Interoperabilidad:
 - k. Homogenización:
- VII.** Se crea el Comité de Internet de las Cosas, que será un órgano colegiado que permitirá la interacción entre instituciones públicas, la industria, la academia y cualquier interesado en participar, en el que se expondrán las estrategias, estudios y necesidades de los servicios del ecosistema del IoT actuales y futuras, con la finalidad de elaborar, desarrollar e implementar el funcionamiento correcto del IoT.

- VIII.** Los temas principales que deberán abordarse dentro del Comité son las siguientes: i) Conectividad e Infraestructura; ii) Seguridad y Vigilancia; iii) Procesos y Automatización; iv) Innovación Tecnológica; v) Ciudades Inteligentes; vi) Ética e IoT; vii) Industria 4.0 y Tecnologías Emergentes; viii) Privacidad y Protección de Datos; ix) Mercados Digitales en el IoT, los anteriores temas son enunciativos más no limitativos.
- IX.** El Comité estará integrado diversas Autoridades entre ellas:
- a. La Secretaría de Gobernación, a través de la Coordinación de Estrategia Digital Nacional
 - b. La Secretaría de Economía, a través de la Dirección General de Normas.
 - c. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
 - d. El Instituto Federal de Telecomunicaciones.
 - e. La Comisión Federal de Competencia Económica,
 - f. Procuraduría Federal del Contribuyente, a través de la Subprocuraduría de Telecomunicaciones;
 - g. Poder Legislativo, a través de las Comisiones de Ciencia, Tecnología e Innovación de ambas cámaras, con opiniones de las comisiones que se consideren pertinentes;
 - h. Poder Judicial, a través del Consejo de la Judicatura Federal.
 - i. Cualquier otra autoridad que se considere necesaria su participación.
- X.** También podrán participar en el Comité otras Autoridades Internacionales, siempre y cuando exista una solicitud formal de pertenecer a dicho Comité o bien, se realice una invitación, la cual podrá ser remitida vía correo electrónico de alguno de los miembros del Comité.
- XI.** De igual forma estará integrado por miembros de la Academia, el sector empresarial y cualquier interesado en el desarrollo del ecosistema del IoT;
- XII.** Cada miembro del Comité podrá tener hasta dos suplementes, quienes lo sustituirán en ausencias o impedimentos.

- XIII.** El Comité tendrá que monitorear las iniciativas que se presenten.
- XIV.** El Comité podrá disponer reglas adicionales para la implementación del Programa de IoT;
- XV.** El Comité podrá crear Grupos de Trabajo para desarrollar sus actividades en diversos temas propuestos que permita la innovación e implementación del ecosistema del IoT.
- XVI.** Los Grupos de Trabajo, deberán presentar sus propuestas con anterioridad a la sesión del Comité, sin embargo, se podrá tratar directamente cualquier propuesta en dicha sesión.
- XVII.** Todos los usuarios tienen la libertad de elegir los tipos y características de dispositivos que están vinculados al Internet de las Cosas, de suerte que, no pueden limitarse, restringirse o discriminar la conectividad de estos.
- XVIII.** Se debe respetar la privacidad de los usuarios finales; así como la inviolabilidad de las comunicaciones privadas de los usuarios finales por cualquier dispositivo conectado física o virtualmente al Internet de las Cosas.
- XIX.** En la medida de lo posible utilizar el protocolo básico utilizado IPv6, y el de respaldo que sea IPv4.
- XX.** Las sesiones que lleve a cabo el Comité se notificarán con anticipación suficiente y podrán ser:
 - a) Ordinarias: por lo menos 12 veces al año
 - b) Extraordinarias: las ocasiones que sean necesarias para el cumplimiento de los fines del Comité.
- XXI.** Las decisiones que se adopten en el Comité sólo serán válidas cuando estén presentes más de la mitad de los miembros del Comité.

La propuesta de directrices mínimas, anteriormente señalada se considera que es la adecuada para el despliegue del ecosistema del IoT, ya que se requiere de todos los *multistakeholder*, para exponer las necesidades, estrategias, prospectiva y

estudios sobre el ecosistema del IoT con el propósito de establecer parámetros mínimos que fomentarán el desarrollo eficiente de esta materia.

En ese orden de ideas con la creación de un Comité de IoT a cargo de la Secretaría de Gobernación y de manera específica la Coordinación de Estrategia Digital Nacional y el Instituto Federal de Telecomunicaciones, se facultarán para coordinar su creación, así como identificar las actividades existentes, analizar los posibles y potenciales beneficios, las amenazas, para obtener una visión general y real del ecosistema del IoT en México.

Asimismo, se considera que esta propuesta es muy superior a otras porque en ella se realizaría un posicionamiento concreto y estratégico, mediante el análisis de estudios del ecosistema del IoT en su integralidad, con la finalidad de incentivar la innovación, el estudio, análisis, dialogo y debate en el desarrollo del ecosistema del IoT.

6. Conclusiones

La falta de regulación del IoT ha generado que en múltiples países se discuta el mejor rumbo para esta tecnología emergente, se ha tratado de implementar una ruta en diversos documentos nacionales e internacionales, sin embargo, aún no existe un punto de acuerdo en común, todos los trabajos analizados muestran una disparidad de criterios generales.

Lo anterior debido a que, no existen parámetros obligatorios, solamente existen normas no vinculantes y que pueden ser aplicables o no por los fabricantes de dispositivos IoT, pero estas disposiciones jurídicas no se enfocan en analizar todo el ecosistema del IoT, esto ha sucedido con otras tecnologías emergentes, las cuales debido a su rápido crecimiento han ido adaptándose de múltiples formas en cada país con reglas tan diversas que hacen difícil la convivencia regulatoria entre países.

De esta manera, en la actual investigación se realizó un análisis sobre la falta de claridad en la regulación en distintos países, toda vez que no existe un parámetro básico aceptado universalmente, además de que no hay unidad entre los *multistakeholder*, lo cual dificulta la aceptación de una regulación equilibrada, consensuada y aceptada. A nivel nacional, si bien hay alguna regulación técnica (normas oficiales mexicanas), tampoco existe un estándar totalmente aceptado.

Por ello, se destaca la necesidad de implementar una serie de directrices mínimas que buscan ordenar y generar condiciones regulatorias sencillas para quien use el IoT y que se puedan operar de manera eficiente y con la debida viabilidad técnica-jurídica.

Aunado a ello, la creación de un Comité IoT, es viable para el desarrollo más eficiente de esta tecnología emergente. Esta institución resulta importante debido a que sentará las bases regulatorias con conceptos concretos, principios esenciales, características y mecanismos de participación, debate y comunicación entre todos los *multistakeholder*.

7. Fuentes

Acosta Molina, Cesar Mauricio, (2019). El estado del arte sobre el Internet de las Cosas. Amenazas y vulnerabilidades de seguridad informática evidenciadas desde la domótica, disponible en: <https://repository.unad.edu.co/bitstream/handle/10596/28446/Monografia.pdf?sequence=1&isAllowed=y>

Alonso, Jessica, (2022), Normas Oficiales Mexicanas para Dispositivos IoT, Asociación Mexicana del Internet de las Cosas (IoT), disponible en: <https://www.asociacioniot.org/2022/10/27/normas-oficiales-mexicanas-para-dispositivos-iot/>

Alliance for IoT and Edge Computing Innovation IVZW (AIOTI), (2021), disponible en: <https://aioti.eu/>

Andalucía, Conectada (2021), Estado del arte y tendencias internet de las cosas e internet de todo, disponible en: <https://coitaoc.org/wp-content/uploads/2021/06/Estado-del-Arte-IoT.pdf>

Australian Council of Learned Academies (2020), The Internet of Things, disponible en: https://acola.org/wp-content/uploads/2020/10/hs5_internet-of-things_report.pdf

Bacelli, Emmanuel, (2021), Internet de las Cosas (IoT), retos sociales y campos de investigación científica en relación con la IoT, disponible en: <https://www.inria.cl/sites/default/files/2022-12/libro-blanco-iot-es.pdf>

Barrio Andrés, Moisés, (2018), Internet de las Cosas, Reus Editorial, disponible en: https://www.editorialreus.es/media/pdf/primeraspaginas_9788429020380_internetdelascosas.pdf

Basilio Sánchez, Gilberto, (2020), El Internet de las Cosas (IoT) y la ciencia, disponible en: http://www.cienciorama.unam.mx/a/pdf/671_cienciorama.pdf

Bonilla, Isaías, et. al., IoT, (2017) el Internet de las Cosas y la innovación de sus aplicaciones, Vincula Téctica, disponible en: <http://www.web.facpya.uanl.mx/vinculategica/Revistas/R2/2313-2340%20-%20Iot,%20El%20Internet%20De%20Las%20Cosas%20Y%20La%20Innovacion%20De%20Sus%20Aplicaciones.pdf#page=1>

Comisión de Regulación de Comunicaciones de la República de Colombia (2016), Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las Cosas, disponible en: [Capítulo 1 \(crcom.gov.co\)](#)

Communications and Information Technology Commission of Saudi Arabia, (2019), CITC Technical Specification, RI114, Specification for License-Exempt LPWAN Devices, disponible en: [cst.gov.sa/ar/RulesandSystems/RegulatoryDocuments/EquipmentApproval/Documents/TA E RI114.pdf](#)

Communications, Space & Technology Commission (2019), Internet of things (IoT) Regulatory Framework, disponible en: [IoT_REGULATORY_FRAMEWORK.pdf \(cst.gov.sa\)](#)

Congreso de Estados Unidos, (2020), H.R.1668 - IoT Cybersecurity Improvement Act of 2020, disponible en: [https://www.congress.gov/bill/116th-congress/house-bill/1668/text#:~:text=To%20establish%20minimum%20security%20standards,Government%2C%20and%20](#)

Department of Commerce, (2017), Fostering the advancement of the internet of things, disponible en: [https://www.ntia.gov/sites/default/files/publications/iot_green_paper_01122017_0.pdf](#)

Diario Oficial de la Federación, (2021), Norma Mexicana NMX-I-20000-7-NYCE-2021, disponible en: [https://dof.gob.mx/nota_detalle.php?codigo=5628903&fecha=06/09/2021#gsc.tab=0](#)

Diario Oficial de la Federación, (2022) 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](#)

Diario Oficial de la Federación, (2022), Norma Mexicana NMX-I-4903-NYCE-2021, disponible en: [https://dof.gob.mx/nota_detalle.php?codigo=5642168&fecha=08/02/2022&print=true](#)

Diario Oficial de la Federación, (2022), Norma Mexicana NMX-I-20000-3-NYCE-2021, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5642169&fecha=08/02/2022#gsc.tab=0

Diario Oficial de la Federación, (2022), Norma Mexicana NMX-I-22301-NYCE-2021, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5642171&fecha=08/02/2022#gsc.tab=0

Diario Oficial de la Federación, (2022) Norma Mexicana NMX-I-22316-NYCE-2021, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5642172&fecha=08/02/2022#gsc.tab=0

Espinoza Carrión, Cecibel, Pérez Espinoza María, y otros, (2017), El Internet de las Cosas: Antecedentes, conceptualización y riesgos, disponible en: <https://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/download/117/96/180>

Evans, Dave, (2011), Internet de las Cosas, cómo la próxima evolución de internet lo cambia todo, Cisco, disponible en: [Internet_of_Things_IoT_IBSG_0411FINAL.pdf \(cisco.com\)](#)

Flores, Zermeño, Francisco, Cossio Franco, Edgar, (2021), Aplicaciones, Enfoques y Tendencias del Internet de las Cosas (IoT): Revisión Sistemática de la Literatura, disponible en: <https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/543/1/Aplicaciones%20enfoques%20y%20tendencias%20del%20IoT.pdf>

Fundación de la Innovación Bankinter, (2011), El Internet de las Cosas, en un mundo conectado de objetos inteligentes, disponible en: https://www.fundacionbankinter.org/wp-content/uploads/2021/09/Publicacion-PDF-ES-FTF_IOT.pdf

Gallego Gómez, Cristina (2022), Internet de las Cosas: la tecnología como aliada de la sostenibilidad, disponible en: <https://recursos.bps.com.es/files/1068/49.pdf>

Gutiérrez, Elsa, (2018), Jalisco tuvo 4.1% de crecimiento económico en el segundo trimestre, Diario Milenio, disponible en:

<https://www.milenio.com/politica/comunidad/jalisco-4-1-crecimiento-economico-trimestre>

Information-technology Promotion Agency (2023), disponible en: <https://www.ipa.go.jp/en/about/index.html>

Instituto Federal de Telecomunicaciones (2020), Estrategia IFT 2021-2025, Hoja de Ruta, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025.pdf>

Instituto Federal de Telecomunicaciones (2021), Cuarta encuesta 2021, Usuarios de Servicios de Telecomunicaciones, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/4taencuesta2021acc.pdf>

Instituto Federal de Telecomunicaciones (2022), Análisis exploratorio de comercialización de servicios de conectividad para el IOT en México, disponible en: <https://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/analisisexploratorioiotmexico.pdf>

Instituto Federal de Telecomunicaciones (2022), Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las cosas (IOT), disponible en: https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf

Instituto Federal de Telecomunicaciones (2023), análisis exploratorio de comercialización de servicios de conectividad para el IoT en México, disponible en: <https://www.ift.org.mx/estadisticas/analisis-exploratorio-de-datos>

Instituto Nacional de Estadística y Geografía, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022, disponible en: <https://www.inegi.org.mx/programas/dutih/2022/>

Internet Society, (2016), Gobernanza de Internet- Porqué funciona el enfoque de múltiples partes interesadas, disponible en: <https://www.internetsociety.org/es/resources/doc/2016/gobernanza-de-internet-por-que-funciona-el-enfoque-de-multiples-partes-interesadas/>

IoTUK, (2018), Benefits and Challenges of IoT, disponible en: <https://iotuk.org.uk/wp-content/uploads/2018/09/IoTUK-survey-report.pdf>

Megas, K., Fagan, M., Cuthill, B., Hoehn, B., Lemire, D. y Herold, R. (2022), Informe resumido del taller para "Building on the NIST Foundations: Next Steps in IoT Cybersecurity", NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, disponible en: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8431.pdf>

Ministry of Economy, Trade and Industry (2020), IoT Security Safety Framework (IoT-SSF), disponible en: https://www.meti.go.jp/english/press/2020/1105_002.html

Ministerio de Ciencia, Tecnología, Innovación y Comunicaciones (2019), Decreto No. 9.854 de 25 de junio de 2019, disponible en: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm

National Telecommunications and Information Administration (2017), Fostering the advancement of the Internet of Things, disponible en: [Fostering the Advancement of the Internet of Things \(doc.gov\)](#)

Nieto Pacheco, A. J., Villegas Pilay, Y. E., & Galarza Alay, J. I. (2023). Avances actuales de las IoT y sus diversas aplicaciones, disponible en: <https://doi.org/10.33262/concienciadigital.v6i1.244>

Organización para la Cooperación y el Desarrollo Económicos (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, disponible en: [Microsoft Word - InternetOfThings_FINAL.docx \(oecd-ilibrary.org\)](#)

Organización para la Cooperación y el Desarrollo Económicos (2018), "Consumer product safety in the Internet of Things", *OECD Digital Economy Papers*, No. 267, OECD Publishing, disponible en: <https://doi.org/10.1787/7c45fa66-en>.

Organización Mundial del Comercio (2022), El papel de las tecnologías avanzadas en el comercio transfronterizo: una perspectiva aduanera, disponible en: https://www.wto.org/spanish/res_s/booksp_s/wcotech22_s.pdf

Organización de las Naciones Unidas, (2023) Pacto Internacional de Derechos Económicos, Sociales y Culturales, disponible en:

<https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>

Perez, Cecilia, (2023) The Top Growth Opportunities for IoT in 2023, Frost & Sullivan, disponible en: <https://www.frost.com/frost-perspectives/the-top-growth-opportunities-for-iot-in-2023/>

Rose, Karen, Eldridge Scott, Chapin Lyman, (2015), La Internet de las Cosas una breve reseña, Internet Society, disponible en: <https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf>

Salazar, Jordi, Silvestre Santiago, (s.f.), Internet de las Cosas, Techpedia, disponible en: https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

Secretaría de Tecnologías de la Información y las Comunicaciones de Argentina, (s.f.), Internet de las Cosas, disponible en: <https://www.argentina.gob.ar/sites/default/files/paperbenchmarkinternacional-iot.pdf>

Standards Council of Canadá (2023), listado de estándares, disponible en: <https://www.scc.ca/en/search/standardsdb/iot>

Secretaría de Relaciones Exteriores (2012). Pacto por México, disponible en: https://embamex.sre.gob.mx/bolivia/images/pdf/REFORMAS/pacto_por_mexico.pdf

Unión Internacional de Telecomunicaciones (2005), The Internet of Things, disponible en: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

Unión Internacional de Telecomunicaciones (2012), Recomendación UIT-T Y.2060, Descripción General de Internet de los objetos, disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2060-201206-!!!PDF-S&type=items