UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"PROPUESTA DE MARCO REGULATORIO PARA LA IMPLEMENTACIÓN DE IOT EN EL COMERCIO LOCAL DEL ECUADOR, SUSTENTADO EN LOS MODELOS DE MÉXICO Y BRASIL"

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

Línea de investigación: Innovación tecnológica y de productos.

AUTOR:

Quilumbaquín Chicaiza Karen Nicole

DIRECTOR:

Ing. Vásquez Ayala Carlos Alberto, Msc

Ibarra - Ecuador 2026

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
APELLIDOS Y NOMBRES:	KAREN NICOLE QUILUMBAQUÍN CHICAIZA

DATOS DE LA OBRA	
TÍTULO:	"PROPUESTA DE MARCO REGULATORIO PARA LA IMPLEMENTACIÓN DE IOT EN EL COMERCIO LOCAL DEL ECUADOR, SUSTENTADO EN LOS MODELOS DE MÉXICO Y BRASIL"
AUTOR (ES):	QUILUMBAQUÍN CHICAIZA KAREN NICOLE
FECHA:	22/07/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TÍTULO POR EL QUE OPTA:	INGENIERA EN TELECOMUNICACIONES
DIRECTOR/ASESOR	ING. VÁSQUEZ AYALA CARLOS ALBERTO, MSC ING. ALVARADO SÁNCHEZ JAIME GUSTAVO

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 22 días del mes de julio de 2026

EL AUTOR:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
KAREN NICOLE QUILUMBAQUIN CHICAIZA

……

Karen Nicole Quilumbaquín Chicaiza

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 22 de Julio de 2026

ING. VÁSQUEZ AYALA CARLOS ALBERTO, MSC

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.



(f) ……

Ing. Vásquez Ayala Carlos Alberto, Msc

DIRECTOR

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios, por darme la fuerza, la sabiduría, la constancia necesaria para culminar esta hermosa etapa de mi vida.

A mi mami Lucy, por ser mi mayor apoyo, por su amor incondicional, sus consejos, su paciencia y por empujarme siempre para no rendirme. Gracias por confiar en mí y en este proceso.

A mi hermana Jazmín, por caminar conmigo a lo largo de la vida, por su cariño, su apoyo, por estar presente en los momentos en que más la necesité.

A mi abuelita Rosario, que, aunque ya no está físicamente, vive siempre en mi corazón. Este logro también es por ti, porque sé que desde el cielo me has cuidado y acompañado en cada paso.

A mi persona especial, Lenin, por su amor, su paciencia, su apoyo y por animarme cuando sentía que todo se volvía difícil.

A ustedes, gracias por ser parte de mi vida, de mi esfuerzo y de este sueño cumplido. Este logro también les pertenece, porque en cada paso de este camino hubo amor, apoyo y razones para no rendirme.

Karen Nicole Quilumbaquín Chicaiza

AGRADECIMIENTO

Mi más sincero agradecimiento a Dios, por darme vida, salud, fortaleza y sabiduría para culminar esta importante etapa de mi formación académica.

A mi mami Lucy y a mi hermana Jazmín, por ser mi mayor apoyo, por su amor incondicional, paciencia, confianza y por acompañarme en cada paso de este camino. Gracias por cada esfuerzo y sacrificio que hicieron para que hoy pueda alcanzar esta meta.

A mi familia, por su cariño, apoyo y palabras de aliento que me motivaron a seguir adelante. De manera especial, a mis compañeros Alejandro, Andrés y Grace, por compartir conmigo esta etapa, por su amistad, apoyo y por los momentos que hicieron de este camino una experiencia inolvidable.

A mi director del trabajo de titulación, Msc. Carlos Alberto Vásquez Ayala, y a mi asesor, Msc. Jaime Gustavo Alvarado Sánchez, por su guía, conocimientos y acompañamiento durante el desarrollo de este trabajo. Asimismo, agradezco a los docentes que fueron parte de mi formación académica.

Finalmente, agradezco a la Universidad Técnica del Norte y a todas las personas que, de una u otra manera, contribuyeron a que este sueño hoy sea una realidad.

Karen Nicole Quilumbaquín Chicaiz

RESUMEN

El Internet de las Cosas (IoT) se ha convertido en una tecnología clave para la transformación digital. Conecta dispositivos, recoge información en tiempo real y automatiza procesos en distintos sectores. En el comercio local, ayuda a manejar inventarios, rastrear productos, mejorar la logística, atender clientes y tomar decisiones con datos. Pero en Ecuador no hay una normativa específica para el IoT. Eso genera problemas en espectro, homologación, interoperabilidad, ciberseguridad, protección de datos y coordinación entre entidades.

Este trabajo propone un marco regulatorio para el IoT en el comercio local ecuatoriano. Donde se compararon los modelos de México y Brasil. Se usó un enfoque cualitativo, con diseño documental y alcance descriptivo-comparativo, revisando normas, documentos técnicos, artículos y otras fuentes relacionadas con el tema.

Se identificaron tecnologías como LoRaWAN, NB-IoT, ZigBee, Sigfox y 5G, y también los desafíos técnicos, legales e institucionales que enfrenta Ecuador. Luego se comparan los modelos de México y Brasil con una tabla de valoración, teniendo como resultado que Brasil es el principal referente en gobernanza, homologación, ciberseguridad e implementación progresiva. México destacó en espectro, bandas de operación y tecnologías habilitadas.

Con esos resultados, se plantearon lineamientos y se realizó una propuesta de marco regulatorio con títulos, capítulos y artículos. La propuesta busca ser una base para futuras normas sobre IoT en el comercio local, integrando aspectos legales, técnicos e institucionales adaptados al país, y aportando a la transformación digital, la innovación y la competitividad del sector comercial.

Palabras Clave: Internet de las Cosas (IoT), marco regulatorio, comercio local, espectro radioeléctrico, interoperabilidad, ciberseguridad.

ABSTRACT

The Internet of Things (IoT) has become a key technology for digital transformation. It connects devices, collects real-time information, and automates processes in different sectors. In local commerce, it helps manage inventories, track products, improve logistics, serve customers, and make data-driven decisions. However, in Ecuador there is no specific regulation for IoT. This creates problems in spectrum management, homologation, interoperability, cybersecurity, data protection, and coordination among entities.

This work proposes a regulatory framework for IoT in Ecuadorian local commerce, where the models of Mexico and Brazil were compared. A qualitative approach was used, with a documentary design and a descriptive-comparative scope, reviewing regulations, technical documents, articles, and other sources related to the topic.

Technologies such as LoRaWAN, NB-IoT, ZigBee, Sigfox, and 5G were identified, as well as the technical, legal, and institutional challenges faced by Ecuador. Then, the models of Mexico and Brazil are compared through an evaluation table, resulting in Brazil being the main reference in governance, homologation, cybersecurity, and progressive implementation. Mexico stood out in spectrum, operating bands, and enabled technologies.

Based on these results, guidelines were proposed and a regulatory framework proposal was developed with titles, chapters, and articles. The proposal seeks to serve as a basis for future IoT regulations in local commerce, integrating legal, technical, and institutional aspects adapted to the country, and contributing to digital transformation, innovation, and the competitiveness of the commercial sector.

Keywords: Internet of Things (IoT), regulatory framework, local commerce, radio spectrum, interoperability, cybersecurity.

LISTA DE CONTENIDOS

1. Capítulo I: Antecedentes 18

1.1 Tema 18

1.2 Problema 18

1.3 Objetivos 21

1.3.1. Objetivo General 21

1.3.2. Objetivos Específicos 21

1.4 Alcance 21

1.5 Justificación 25

2. Capítulo II: Marco Teórico 27

2.1 Internet de las Cosas (IoT) 27

2.1.1. Características de IoT 28

2.1.2. Arquitectura de IoT 29

2.1.3. Tecnologías IoT 32

2.1.3.1. LoRaWAN 32

2.1.3.2. ZigBee 32

2.1.3.3. SigFox 33

2.1.4. Aplicaciones del IoT en el Comercio Local 33

2.2 Marco Regulatorio de IoT 35

2.2.1. Importancia de un marco regulatorio para el IoT 35

2.2.2. Gestión del espectro radioeléctrico 36

2.2.3. Homologación de dispositivos IoT 37

2.2.4. Interoperabilidad 38

2.2.5. Ciberseguridad en IoT 39

2.2.6. Normativas internacionales relevantes sobre IoT 41

2.2.6.1. Principales organismos y estándares internacionales 41

2.3 Regulación de IoT en América Latina 43

2.3.1. Regulación del IoT en México 43

2.3.2. Regulación del IoT en Brasil 45

2.3.3. Comparación de la regulación de IoT en América Latina 46

2.3.4. Modelos regulatorios aplicables al contexto ecuatoriano 48

2.4 Análisis comparativo de los marcos regulatorios de IoT en México y Brasil .. 49

2.4.1. Gestión del espectro radioeléctrico en México y Brasil 49

2.4.2. Homologación de dispositivos IoT 49

2.4.3. Interoperabilidad 50

2.4.4. Ciberseguridad 51

2.4.5. Tabla comparativa de los marcos regulatorios de IoT de México y Brasil .. 51

2.5 Análisis del caso ecuatoriano 53

2.5.1. Gestión del espectro radioeléctrico en Ecuador 53

2.5.2. Homologación de dispositivos IoT 53

2.5.3. Interoperabilidad 54

2.5.4. Ciberseguridad 54

2.5.5. Resumen del marco regulatorio aplicable al IoT en Ecuador 55

2.6 Comparativa entre México, Brasil y Ecuador 56

2.6.1. Convergencias y divergencias regulatorias de México, Brasil y Ecuador ... 56

2.6.1. Comparativa de parámetros entre México, Brasil y Ecuador 60

2.6.2. Evaluación comparada de los parámetros principales de IoT en México, Brasil y Ecuador 62

3. Capítulo III: Marco metodológico 64

3.1 Normativas relevantes internacionales en México, Brasil y Ecuador 64

3.2 Estrategias e incentivos regulatorios en México, Brasil y Ecuador 66

3.3 Desafíos técnicos, legales e institucionales 67

3.3.1. Retos técnicos y de infraestructura digital 67

3.3.2. Desafíos normativos y regulatorios 68

3.3.3. Ciberseguridad y protección de datos 69

3.3.4. Gobernanza institucional y capacidades nacionales 71

3.3.5. Sistematización de los desafíos identificados para la regulación del IoT en Ecuador 72

3.4 Análisis comparativo de requerimientos para la regulación del IoT en Ecuador 73

3.4.1. Requerimientos legales 73

3.4.2. Requerimientos institucionales 77

3.4.3. Requerimientos técnicos 80

3.4.4. Integración general de requerimientos para la regulación del IoT en Ecuador 83

3.4.5. Síntesis concluyente de los parámetros identificados 84

3.4.6. Valoración comparativa del nivel de desarrollo regulatorio del IoT en Ecuador, México y Brasil. 85

4. Capítulo IV: Resultados 94

4.1 Fundamentos para el desarrollo de la propuesta del marco regulatorio 95

4.2 Estructura general del marco normativo propuesto 97

4.3 Desarrollo preliminar de los títulos propuestos 101

4.3.1. Título I: Disposiciones generales 101

4.3.2. Título II: Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT 102

4.3.3. Título III: Homologación y certificación de dispositivos IoT. 104

4.3.4. Título IV: Interoperabilidad y estándares técnicos. 105

4.3.5. Título V: Ciberseguridad y protección de datos. 106

4.3.6. Título VI: Aplicaciones sectoriales del IoT. 108

4.3.7. Título VII: Gobernanza y coordinación institucional..... 109

4.3.8. Título VIII: Implementación, seguimiento y disposiciones finales. 111

4.4 Propuesta de marco regulatorio para la implementación del Internet de las Cosas en el comercio local en Ecuador. 113

5. Conclusiones..... 128

6. Recomendaciones 130

7. Bibliografía 132

LISTA DE TABLAS

Tabla 1 *Comparativa de bandas y aplicaciones para tecnologías IoT* 37

Tabla 2 *Niveles de interoperabilidad en IoT* 39

Tabla 3 *Comparación de normativas clave* 42

Tabla 4 *Comparación de los enfoques regulatorios de México y Brasil sobre el IoT* 47

Tabla 5 *Síntesis comparativa de los marcos regulatorios de IoT en México y Brasil* 52

Tabla 6 *Síntesis del marco regulatorio del IoT en Ecuador* 55

Tabla 7 *Comparación de los marcos regulatorios de IoT en México y Brasil* 57

Tabla 8 *Comparación general de los marcos regulatorios de IoT en México, Brasil y Ecuador* 62

Tabla 9 *Resumen de los desafíos técnicos, legales e institucionales para el desarrollo del IoT en Ecuador* 72

Tabla 10. *Requerimientos legales para la regulación del IoT en el comercio local ecuatoriano* 74

Tabla 11. *Requerimientos institucionales para la gobernanza del IoT en Ecuador* 78

Tabla 12. *Requerimientos técnicos para la implementación del IoT en el comercio local ecuatoriano.* 81

Tabla 13. *Integración de requerimientos para la regulación del IoT en el comercio local ecuatoriano* 83

Tabla 14. *Fundamentos para el desarrollo de la propuesta del marco regulatorio* 95

Tabla 15. *Estructura general del marco normativo para IoT en Ecuador.* 97

Tabla 16. *Desarrollo del Título I: Disposiciones generales.* 101

Tabla 17. *Desarrollo del Título II: Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT.* 103

Tabla 18. *Desarrollo del Título III: Homologación y certificación de dispositivos IoT.* 104

Tabla 19. *Desarrollo del título IV: Interoperabilidad y estándares técnicos.* 106

Tabla 20. *Desarrollo del Título V: Ciberseguridad y protección de datos.* 107

Tabla 21. *Desarrollo del Título VI: Aplicaciones sectoriales del IoT.* 108

Tabla 22. *Desarrollo del Título VII: Gobernanza y coordinación institucional.* 110

Tabla 23. *Desarrollo del Título VIII: Implementación, seguimiento y disposiciones finales.* 112

LISTA DE FIGURAS

Figura 1 *Árbol de problemas sobre sobre la Regulación del Uso de Tecnologías IoT en el Comercio Local*..... 20

Figura 2 *Ciclo de deming*..... 24

Figura 3 *Arquitectura de tres capas en IoT*..... 30

Figura 4. *Arquitectura de cinco capas en IoT*..... 31

Figura 5 *Bandas de espectro 5G en México.* 45

Capítulo I: Antecedentes

1.1 Tema

Propuesta de marco regulatorio para la implementación de IoT en el comercio local del ecuador, sustentado en los modelos de México y Brasil.

1.2 Problema

En el contexto actual, las tecnologías IoT (Internet de las Cosas) están revolucionando diversos sectores a nivel mundial (Dixit & Rani, 2025), incluyendo el comercio local. En países como México y Brasil, estas tecnologías han sido impulsadas mediante marcos regulatorios especializados que permiten su implementación legal, segura e interoperable. En el caso de Ecuador, sin embargo, es posible observar lo contrario: no existe un marco específico de normativa que regule el uso de IoT, lo que implica un vacío técnico y legal que condiciona su aplicación en sectores estratégicos considerados como el comercio local. La regulación ecuatoriana en este sector y en el ámbito de telecomunicaciones, principalmente ejercida por ARCOTEL, abarca el manejo de bandas de frecuencias para dispositivos de corto alcance, pero no regula expresamente el uso de tecnologías como LoRaWAN, ZigBee o SigFox, que son las más aplicadas para el uso de aplicaciones de IoT (Ochoa Zezzatti et al., 2021).

Así pues, la falta de un marco regulador que dé cabida a las telecomunicaciones y a otras tecnologías emergentes como el IoT provoca incertidumbre tanto en los empresarios como en los consumidores, como bien advierte Coello Mora (2010), en definitiva, no hay inversión en tecnología, ni homologación para dispositivos, ni planificación institucional para su incorporación al ecosistema productivo del país. Lo mismo señala Nader Conti (2024), quien indica que la falta de un marco regulador en Ecuador es aún incipiente para tecnologías emergentes como blockchain, IA o IoT, generando inseguridad jurídica y deteniendo el desarrollo de soluciones innovadoras, así

como también la falta de reconocimiento legal, no existencia de sandboxes regulatorios o vacíos normativos sobre el tratamiento de datos sobre producciones tecnológicas complejas refuerzan un ecosistema poco propenso hacia la experimentación o al uso de tecnologías disruptivas para el desarrollo de sectores estratégicos.

A la inversa de lo anterior, se tienen países como Brasil que han construido estrategias para estimular estas tecnologías, en tanto que el Decreto N.º 9.854, que establece el Plan Nacional de Internet de las Cosas, promueve la libre competencia, protección de datos y cooperación público-privada en sectores como el urbano, rural, salud e industrial. Según la Presidencia de la República de Brasil (2019), “la implementación de soluciones IoT debe orientarse por criterios de eficiencia, productividad y cooperación internacional” (Presidencia de la República de Brasil, 2019).

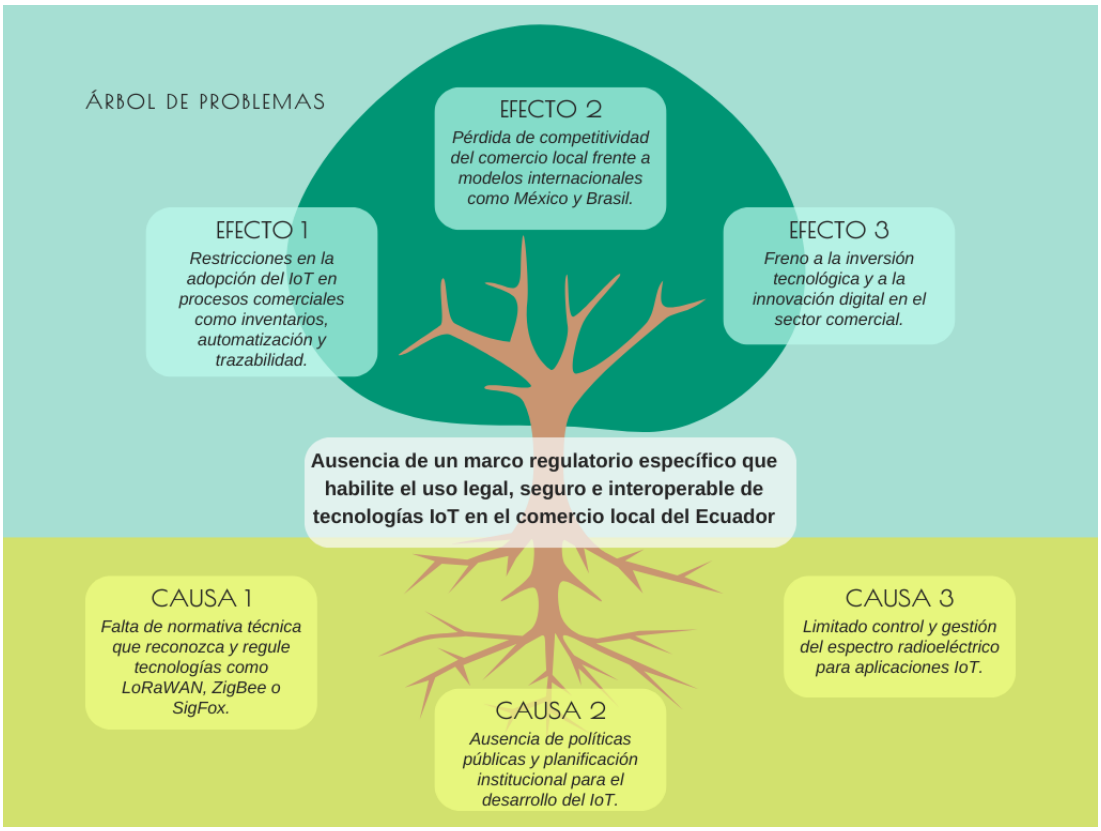
Por su parte, México, a través del Instituto Federal de Telecomunicaciones (IFT), ha publicado lineamientos para el uso compartido del espectro, homologación de equipos, transición a IPv6 y ciberseguridad en IoT. Como destaca el IFT (2019), “es fundamental establecer regulación que facilite la conectividad de un gran número de dispositivos, con uso eficiente del espectro” (Instituto Federal de Telecomunicaciones, 2019) .

Este problema no solo afecta la competitividad de los comercios locales, sino que también limita su capacidad para integrarse en una economía digital regional. De acuerdo con García Murillo (2007), "la falta de una regulación adaptada a las nuevas tecnologías impide la expansión de mercados eficientes y competitivos, afectando el desarrollo económico del país".

En la siguiente Figura 1 se representa de forma esquemática la problemática central del estudio, sus causas estructurales y efectos visibles. Este recurso permite visualizar la relación lógica entre la falta de regulación para el IoT y sus implicaciones en el comercio local. Sirve como base referencial para el desarrollo del presente trabajo.

Figura 1

Árbol de problemas sobre sobre la Regulación del Uso de Tecnologías IoT en el Comercio Local



Nota. Autoría propia.

Por lo tanto, es necesario un análisis detallado de modelos normativos internacionales exitosos, como los de Brasil y México, y su adaptación al contexto ecuatoriano, con el fin de proponer una regulación que garantice el uso seguro, legal e interoperable de las tecnologías IoT. Tal como afirma Coello Mora (2010), “la creación de un entorno regulatorio flexible y adaptado a las nuevas tendencias tecnológicas es esencial para fomentar la inversión en sectores estratégicos como el de telecomunicaciones y IoT”

1.3 Objetivos

1.3.1. *Objetivo General*

Proponer un marco regulatorio para la implementación de tecnologías IoT en el comercio local del Ecuador, mediante un análisis comparativo con los marcos normativos de México y Brasil, para el fortalecimiento normativo en el contexto nacional.

1.3.2. *Objetivos Específicos*

- Identificar las tecnologías IoT utilizadas en el comercio local de Ecuador, México y Brasil, así como su relación con los marcos normativos vigentes en estos dos últimos países.
- Comparar el marco regulatorio de México y Brasil en cuanto a la utilización de tecnologías del tipo IoT en el comercio local, respecto a la situación actual en el Ecuador, abordando aspectos como espectro radioeléctrico, licencias, interoperabilidad y seguridad y logran así la identificación de elementos adaptables en el ámbito nacional.
- Determinar los retos técnicos, legales e institucionales en el Ecuador para implementar regulaciones sobre IoT en el comercio local.
- Elaborar lineamientos regulatorios para el Ecuador que puedan servir de lineamientos para una propuesta normativa específica fundamentados en las mejores prácticas de México y Brasil.

1.4 Alcance

El presente trabajo de titulación tiene la finalidad de presentar un marco regulatorio que se utilice como base para la implementación de tecnologías IoT (Internet de las Cosas) en los comercios locales de Ecuador a partir de un análisis comparativo con los marcos normativos aplicables en México y Brasil. La investigación se centra en los casos de los establecimientos pequeños y medianos que pueden estar utilizando o tener la intención de utilizar tecnologías como

LoRaWAN, ZigBee y SigFox para automatizar procesos, manejar el inventario, mejorar la atención al cliente y monitorizar las operativas en tiempo real. Se excluyen a los sectores agricultura, salud y manufactura, así como el desarrollo de software o dispositivos, considerando que la investigación hace exclusivamente foco sobre lo normativo y legal.

Existen avances tecnológicos en Ecuador, pero no tenemos normativa específica que regule el uso del IoT. Estas tecnologías operan bajo disposiciones generales de espectro no licenciado, lo que genera inseguridad jurídica para proveedores y usuarios. Coello Mora (2010) afirma que la no existencia de un entorno regulado adaptado a las tecnologías emergentes produce inseguridad a los actores del mercado y repercute negativamente sobre la innovación y el interés de inversión en sectores clave. Alfonzo Guzmán (2020) refuerza esta idea al señalar que tecnologías como LoRaWAN y ZigBee ya han sido probadas técnicamente en el país, pero su implementación formal es limitada debido a vacíos legales que impiden su aplicación comercial a gran escala (Comisión Económica para América Latina y el Caribe (CEPAL), 2022)

Para resolver esta problemática, la investigación adopta una metodología cualitativa, comparativa, documental y aplicada. Se fundamenta en las normas nacionales y los documentos técnicos de las entidades reguladoras, tales como lo son: ARCOTEL y MINTEL y los marcos jurídicos que ha producido el Instituto Federal de Telecomunicaciones (IFT) en México; así como la legislación que ha desarrollado la Agencia Nacional de Telecomunicaciones (ANATEL) en Brasil. También se consideran las directrices internacionales: la de la Agenda Digital para América Latina y el Caribe eLAC2024, que busca fomentar políticas públicas inclusivas y sostenibles, alineadas con los procesos de transformación digital.

El proceso investigativo se estructura a través del Ciclo de Deming (PDCA), una herramienta de mejora continua que permite organizar y ejecutar el estudio en cuatro fases En la

fase de Planificación se identifica y analiza el uso actual de tecnologías IoT en el comercio local de Ecuador, México y Brasil, así como su relación con los marcos regulatorios vigentes en México y Brasil. Esta etapa cumple con el primer objetivo específico del estudio, ya que permite comprender el estado del arte tecnológico y normativo para fundamentar el análisis comparativo posterior. Esta etapa está alineada con lo planteado por Guzmán (2020), quien evidencia la necesidad de estructurar normativas específicas que garanticen la integración segura del IoT.

Durante la fase de ejecución (Do) se recopila información normativa, doctrinal y técnica relevante. Se analiza el entorno legal ecuatoriano en materia de telecomunicaciones, el uso del espectro y la ausencia de disposiciones específicas para redes IoT. Paralelamente, se estudian las políticas regulatorias de México, donde el IFT ha implementado estrategias para facilitar la conectividad masiva de dispositivos mediante el uso eficiente del espectro (Trujillo et al., 2020). En Brasil, se valoriza el Plan Nacional de Internet de las Cosas, el cual es ideado por la ANATEL y que incluye, entre otros aspectos, la reducción de las barreras fiscales y la flexibilidad normativa, además de la delimitación de sectores y de las ciudades inteligentes (Presidencia de la República de Brasil, 2019).

En la etapa de verificación (Check) se contraponen los elementos regulatorios identificados con la concreta realidad jurídica e institucional del Ecuador. Se analizan, entre otros temas: licencias de operación, homologación de dispositivos, control de interferencias, interoperabilidad o mecanismos de gobernanza. Esta fase de análisis permite determinar qué elementos del marco normativo mexicano y brasileño pueden ser transferibles y/o adaptados al marco normativo ecuatoriano, conforme a criterios de pertinencia técnica, legal y económica. Camacho Castillo (2019) recuerda que esta pieza de comparativa es clave para entender los limites y oportunidades

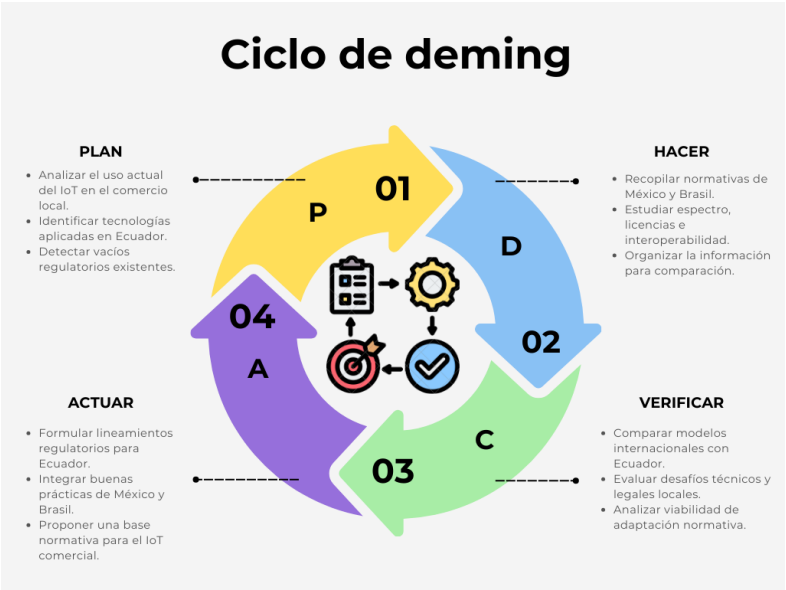
de la implementación local, en función tanto de la infraestructura disponible como del grado de madurez institucional que tenga el país.

Por último, en la etapa de acción (Act), se plantea una propuesta de lineamientos regulatorios para poder establecer un marco normativo específico para el uso de tecnologías IoT en el comercio local del Ecuador. Esta propuesta incorpora principios como la neutralidad tecnológica, la interoperabilidad y la seguridad operativa, asegurando su alineación con estándares internacionales y necesidades nacionales. Como lo establece la CEPAL (2022), la gobernanza digital efectiva exige regulaciones claras, dinámicas y técnicamente fundamentadas para asegurar una transformación digital inclusiva y sostenible.

En la Figura 2 se expone de forma visual el ciclo de mejora continua de Deming (PDCA), aplicado como guía metodológica en el presente trabajo. Este diagrama permite observar las cuatro fases principales: Planificar, Hacer, Verificar y Actuar, cada una vinculada directamente con uno de los objetivos de la investigación.

Figura 2

Ciclo de deming



Nota: Se muestra el ciclo de Deming aplicado al proceso metodológico de la propuesta regulatoria para IoT en el comercio local del Ecuador.

1.5 Justificación

La ausencia de un marco regulatorio específico para el Internet de las Cosas (IoT) en el comercio local del Ecuador limita el avance hacia la digitalización eficiente del sector (Gaibor García et al., 2024). A pesar de que tecnologías como LoRaWAN, ZigBee o SigFox han sido utilizadas en experiencias aisladas dentro del comercio minorista, su implementación se da sin lineamientos legales claros, generando incertidumbre en cuanto al uso del espectro, licencias y seguridad de los dispositivos conectados. Esta investigación se plantea como una oportunidad para proponer un marco normativo adaptado al contexto nacional, con base en las experiencias regulatorias exitosas de México y Brasil, donde existen políticas públicas orientadas al desarrollo del IoT con enfoque sectorial (MCTIC, 2018; Instituto Federal de Telecomunicaciones, 2019).

Desde la óptica tecnológica, la propuesta plantea facilitar la llegada del IoT al ecosistema empresarial ecuatoriano, de modo que pequeñas y medianas empresas puedan asimilar soluciones inteligentes de automatización, control de inventarios, mejora de servicios, etcétera, y que eso tenga un impacto directo en la productividad, la eficiencia operacional y la competencia, sobre todo en zonas urbanas, donde existe potencial de poblarse de entornos inteligentes (Pérez Ramos et al., 2022). Con todo esto, el estudio se alinearía con los Objetivos de Desarrollo Sostenible (en adelante, ODS), y más concretamente con el ODS 9 (Industria, innovación e infraestructura), porque deberá fomentar una base legal asociada a las tecnologías emergentes; el ODS 8 (Trabajo decente y crecimiento económico) porque promueve la innovación del comercio y; y, en último

lugar, el ODS 11 (Ciudades y comunidades sostenibles) por aportar a la transformación digital urbana (ONU, 2016).

Desde lo que podemos entender como los aspectos teóricos, la investigación conlleva un incentivo sobre el debate en torno a la regulación de las tecnologías emergentes en países que no poseen regulaciones específicas. La investigación comparativa hace evidente cómo podría replicarse o adaptarse una estructura jurídica clara como la que ha adoptado Brasil mediante su Plan Nacional de IoT en Ecuador con el objeto de atraer inversión tecnológica y mejorar el entorno del comercio. Además, también promueve el debate académico en torno a la neutralidad tecnológica, la gobernanza de la innovación y la adaptación normativa, que además son las recomendaciones de las políticas digitales en América Latina (Comisión Económica para América Latina y el Caribe (CEPAL), 2022).

Y para finalizar, desde la vertiente metodológica, el estudio tiene una perspectiva cualitativa, documental y, por último, comparativa, centrándose en el análisis normativo de los marcos regulatorios de México y Brasil y de su aplicación al ecosistema ecuatoriano; esta estrategia servirá para construir propuestas concretas y realistas de líneas regulatorias adaptadas a la realidad institucional, jurídica y tecnológica de Ecuador. A diferencia de otros estudios descriptivos, el presente proyecto va dirigido a una aplicación práctica de los resultados buscando proporcionar herramientas útiles para la formulación de políticas públicas vinculadas a las telecomunicaciones, el comercio y la transformación digital.

Capítulo II: Marco Teórico

Este capítulo presenta una revisión teórica detallada sobre la implementación de tecnologías del Internet de las Cosas (IoT) en el comercio local del Ecuador. Se comenzará con la definición, el concepto de IoT, las características, la arquitectura y las principales tecnologías utilizadas, y de esta manera también resaltando la importancia para el sector comercial al automatizar los procesos, la gestión eficiente de inventarios, realizar monitoreo en tiempo real y en sí mejorar la experiencia del cliente. Sin embargo, al incorporar estas soluciones no es que solo depende de los avances tecnológicos, sino también que requiere de un entorno regulatorio donde se establezca reglas claras para la implementación, por lo cual se abordará aspectos como las gestión del espectro radioeléctrico, la homologación de dispositivos, la interoperabilidad y la ciberseguridad, ya que estos elementos afectan directamente en la seguridad operativa, la compatibilidad de los equipos y la protección de la información y de los usuarios.

El análisis que a continuación se realiza presenta una comparación de los marcos regulatorios de Brasil y de México ante la realidad del caso de Ecuador, comparativa que permite identificar aquellos elementos que han contribuido a robustecer la regulación del IoT, así como también los déficits que aún presenta la legislación ecuatoriana. Así se aporta un marco de análisis que propicia la interpretación del contexto nacional y se aportan con puntos relevantes que sustentan la propuesta regulatoria que se plantea.

2.1 Internet de las Cosas (IoT)

El Internet de las Cosas (IoT) se refiere a la interconexión de objetos físicos y virtuales a través de redes de comunicación, para que dispositivos como sensores, actuadores, electrodomésticos, vehículos e infraestructura recojan, intercambien y procesen datos de forma autónoma y en tiempo real. Cada dispositivo cuenta con un identificador único y se integra a la

red para ofrecer servicios avanzados mediante tecnologías de información y comunicación interoperables. Este conjunto de tecnologías permite la automatización de tareas, el monitoreo constante y el funcionamiento a distancia. Gracias a estas capacidades, es posible mejorar la eficiencia en entornos industriales, urbanos, residenciales. De este modo, se impulsa la transformación digital en el país y, al mismo tiempo, se abre paso a nuevas oportunidades de negocio. Sin dejar de lado la precisión y la confiabilidad necesarias en estos procesos (Bhat et al., 2007).

2.1.1. *Características de IoT*

. El Internet de las Cosas (IoT) posee características que permiten su integración en sistemas de monitoreo, automatización y control, facilitando procesos en distintos sectores (Radouan Ait Mouha, 2021).

- Sensado y actuación: El IoT utiliza sensores para recopilar información del entorno físico (temperatura, humedad, luz, movimiento) y actuadores que permiten realizar acciones basadas en la información recibida, como el control de riego con sensores de humedad o la gestión del tráfico con sensores de ocupación.
- Procesamiento de información: Los datos capturados son enviados y procesados en tiempo real para la toma de decisiones automáticas, mediante algoritmos que operan en distintos entornos y análisis en la nube.
- Conectividad entre dispositivos: Se basa en la comunicación M2M (Machine-to-Machine), donde los dispositivos intercambian datos de forma autónoma, utilizando tecnologías como Bluetooth, Zigbee, Wi-Fi y redes celulares.

- Escalabilidad y flexibilidad: La estructura del IoT permite conectar millones de dispositivos y aplicarse en distintos ámbitos como: salud, industria, agricultura y ciudades inteligentes.
- Integración física y virtual: Busca ofrecer aplicaciones que agrupan el mundo físico y virtual, permitiendo a los dispositivos mostrar su propio estado y también lo que ocurre a su alrededor. Ayudando así con esa información a vigilar procesos o hacer que las cosas funcionen de forma automática.

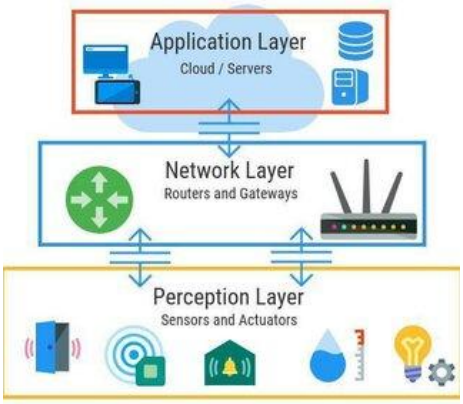
2.1.2. *Arquitectura de IoT*

La arquitectura del Internet de las Cosas (IoT) organiza el flujo de datos desde la captura hasta la entrega de servicios al usuario final. Eso permite que los sistemas sean escalables, funcionen bien y sean sencillos de implementar.

Como se observa en la Figura 3, la arquitectura de tres capas de IoT de manera jerárquica para facilitar la comunicación y el procesamiento de datos.

Figura 3

Arquitectura de tres capas en IoT



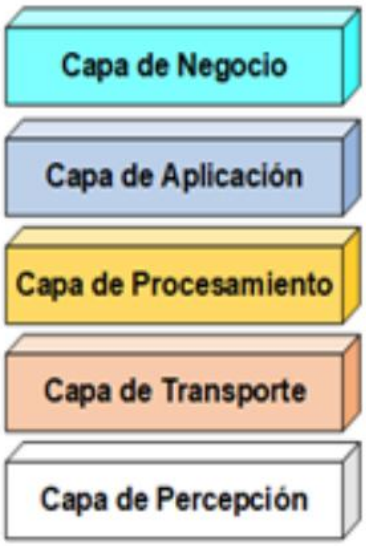
Nota: Se muestra la división del IoT en tres niveles: percepción, red y aplicación (Lo & Niang, 2021) .

- Capa de percepción: Se encarga de recoger información del entorno físico, usando sensores y dispositivos inteligentes que detecten lo que pasa a su alrededor.
- Capa de red: Los datos recogidos son enviados, ya sea por redes inalámbricas o cableadas hacia los sistemas que los van a procesar.
- Capa de aplicación: Con los datos ya procesados, se ofrecen servicios concretos, utilizados en áreas como ciudades inteligentes, salud o automatización del hogar.

Como se muestra en la Figura 4, el modelo de cinco capas en IoT integra desde la captura de datos hasta la gestión empresarial.

Figura 4.

Arquitectura de cinco capas en IoT



Nota: Se observa la arquitectura IoT de cinco capas: percepción, transporte, procesamiento, aplicación, negocio (Tonato Chuquimarca & Sinche Maita, 2022) .

- Percepción: Captura de datos mediante sensores.
- Transporte: Los datos se envían hacia donde van a ser procesados utilizando tecnologías como Wi-Fi, LTE, Bluetooth y RFID, según lo que mejor funcione en cada caso.
- Procesamiento: Los datos se analizan en la nube con algoritmos inteligentes que ayudan a extraer información importante.
- Aplicación: Presenta servicios al usuario basados en los datos procesados.
- Negocio: Con los resultados ya analizados, se toman decisiones, se diseñan estrategias y se ajustan los procesos del sistema IoT para mejorar el funcionamiento.

2.1.3. *Tecnologías IoT*

2.1.3.1. *LoRaWAN*

LoRaWAN (Long Range Wide Area Network) es una tecnología LPWAN que permite enviar información a larga distancia usando muy poca energía. Se usa en ciudades inteligentes, en la agricultura o en negocios, donde los dispositivos necesitan transmitir datos a distancias considerables sin depender de un suministro constante de energía. Su arquitectura se basa en una topología en estrella: los nodos finales envían datos a unos dispositivos intermedios llamados gateways, y estos retransmiten la información mediante redes IP hacia servidores centrales, donde se procesa y gestiona (Andrade & Yoo, 2019).

Esta tecnología destaca por el bajo consumo de energía, su cobertura de largo alcance de hasta 15 km en zonas rurales y entre 2 y 5 km en entornos urbanos, y la capacidad para soportar miles de dispositivos sin perder rendimiento (Döníz & Lajos, 2022). Su soporte para calidad de servicio (QoS) y que puede funcionar tanto en redes públicas como en privadas. LoRaWAN es especialmente adecuado para tareas como control de inventarios, vigilancia ambiental o seguridad en tiendas y almacenes (Ruckebusch et al., 2018).

2.1.3.2. *ZigBee*

Zigbee es un protocolo inalámbrico, pensado para distancias cortas y basado en el estándar IEEE 802.15.4. Está diseñado para sistemas de bajo consumo de energía y para redes con varios sensores. Su estructura puede configurarse en topología estrella, árbol o malla, lo que permite que tenga gran resistencia a fallos y hace que los datos puedan viajar de manera eficiente (Zhao, 2021).

En aplicaciones urbanas y comerciales, Zigbee ha demostrado ser útil en sistemas de automatización, iluminación inteligente, y monitoreo ecológico. Por ejemplo, Yan et al. (2021) desarrollaron un sistema de monitoreo fisiológico para plantas, basado en Zigbee, que registra la evolución desde la germinación hasta la fructificación y envía los datos a un centro de procesamiento. El bajo costo, el diseño modular y la independencia energética convierten a Zigbee en una alternativa factible para el comercio local.

2.1.3.3. *SigFox*

Sigfox es una tecnología LPWAN que permite enviar paquetes muy pequeños de información, de hasta 12 bytes, a grandes distancias y con gasto mínimo de energía. Funciona usando una modulación de banda ultraestrecha (UNB) en frecuencias de 868 MHz (Europa) y 902 MHz (América), y pueden alcanzar hasta 50 kilómetros de cobertura en áreas rurales (Robinson, 2024).

Entre sus aplicaciones más reconocidas se encuentran los sistemas de estacionamiento inteligente, donde sensores instalados en la vía pública envían información sobre la disponibilidad de espacios hacia la nube, para consulta en tiempo real desde aplicaciones móviles (Robinson, 2024). Además, su arquitectura de red permite que varias estaciones base trabajen juntas para asegurar que los mensajes lleguen a su destino, y también incluye funciones de geolocalización que no requieren el uso de GPS (Osman & Abbas, 2022).

2.1.4. *Aplicaciones del IoT en el Comercio Local*

El Internet de las Cosas (IoT) ha transformado el comercio local al incorporar tecnologías inteligentes en los procesos tradicionales de venta, promoción e inventario. Una de las aplicaciones

más destacadas es la gestión inteligente de inventarios, que ahora permite saber en tiempo real qué productos hay y dónde están, mediante sensores RFID y redes IoT, ayudando así a reducir gastos, mejorar los tiempos de reposición y ofrecer un mejor servicio al cliente. Jin & Karki (2025) destacan que la combinación de IoT con blockchain en las cadenas de suministro ofrece una visibilidad de todo lo que pasa con los productos en cada paso, detectando los problemas antes de que ocurran y acortando tiempos de entrega. Todo eso hace que el comercio funcione de mejor manera.

Otra aplicación relevante es la gestión de promociones en tiendas físicas. A través de plataformas IoT, se detecta cuando los clientes están cerca y se ajustan en tiempo real las promociones, además de medir qué tan efectivas resultan. Un ejemplo de este tipo es la implantación de una plataforma IoT en los puntos de venta, para presentar ofertas de manera automática y personalizada, y ajustada a la hora del día o la temporada. Esto favorece la competitividad de los pequeños negocios sin tener que realizar importantes inversiones (Barbecho & Gutiérrez, 2021) .

Además, el concepto de carritos inteligentes se ha convertido en una alternativa cada vez más utilizada en las tiendas físicas. Estos usan tecnología RFID para ir identificando los productos que se van agregando y realizar cobros directos, sin necesidad de pasar por caja y reduciendo el tiempo de compra. Esta clase de soluciones, combinadas con computación en la nube o en la niebla, ha demostrado que mejoran tanto la eficiencia del negocio como la experiencia de quienes compran (Wang, 2025) .

También se ha explorado el uso de IoT en ciudades inteligentes, y eso ha traído beneficios al comercio local. Por ejemplo, hay sistemas que miden cuánta gente pasa por una zona, luces adaptativas en las áreas de exhibición que se ajustan según la hora del día, y ofertas que llegan al

celular cuando alguien está cerca de una tienda. Según Mouha (2021),el IoT transforma los objetos físicos en fuentes de información que ayudan a mejorar la logística, la seguridad y la forma en que se ofrecen los servicios comerciales.

En el contexto latinoamericano, un informe de la Coordinación General de Planeación Estratégica en México señala que tecnologías como Zigbee, LoRa y Sigfox se están usando cada vez más, sobre todo porque resultan económicas de operar y ofrecen opciones tanto para distancias cortas como de largo alcance. Estas tecnologías se implementan en servicios como monitoreo de vitrinas, seguridad, y control ambiental dentro de locales comerciales (Trujillo et al., 2020).

2.2 Marco Regulatorio de IoT

2.2.1. *Importancia de un marco regulatorio para el IoT*

El incremento de la cantidad de dispositivos IoT en todo el mundo ha hecho que sea necesario y urgente contar con reglas claras que guíen su crecimiento de manera ordenada, segura y eficiente. Un entorno normativo bien planteado ayuda a proteger los derechos de quienes usan estos sistemas, a promover la innovación se haga con responsabilidad y asegurar la interoperabilidad de dispositivos en distintas plataformas (Barbecho & Gutiérrez, 2021).

Según el estudio de Alfonzo Guzmán (2020), en el contexto ecuatoriano todavía no existe una normativa propia que regule el uso del IoT, aunque ya se esté usando en transporte, salud, comercio y agricultura. Este vacío regulatorio puede comprometer la seguridad de la información, la compatibilidad entre dispositivos, y la calidad del servicio que recibe el usuario final.

A nivel internacional, la Unión Internacional de Telecomunicaciones (UIT) ha señalado que la regulación anticipada del IoT debería centrarse en cinco aspectos importantes: gestión del espectro, licencias, ciberseguridad, interoperabilidad y gobernanza de datos (International Telecommunication Union (ITU), 2024). Estos elementos son clave para construir confianza en el

ecosistema digital y habilitar modelos de negocio escalables, como demuestra el caso de México a través del Instituto Federal de Telecomunicaciones (Instituto Federal de Telecomunicaciones, 2019).

2.2.2. *Gestión del espectro radioeléctrico*

Uno de los elementos fundamentales para poner en marcha soluciones IoT es hacer un buen uso del espectro radioeléctrico.Tecnologías IoT como LoRaWAN, Zigbee y Sigfox suelen funcionar en bandas que no necesitan licencia, lo que facilita que se usen sin tener que cumplir con trámites complicados. Sin embargo, eso no quiere decir que requiera una planificación adecuada de la gestión del espectro porque si no, pueden aparecer problemas como interferencias, congestión o dificultades para que nuevos actores tecnológicos puedan acceder de forma justa.

En Ecuador, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ha reconocido que es necesario actualizar los marcos legales que regulan el uso del espectro para dispositivos de corto alcance y bajo consumo, como los que se usan en redes IoT (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2018). A diferencia de países como Brasil, donde ANATEL ya ha identificado bandas específicas para IoT y ha establecido mecanismos de licenciamiento dinámico, Ecuador aún presenta vacíos en esta materia.

Según el informe de (Robinson, 2024), tecnologías como Sigfox usan bandas muy estrechas que les permiten llegar hasta 50 km con muy poca energía, mientras que Zigbee y LoRaWAN se usan más en ciudades y para distancias más cortas. Esta variedad de tecnologías hace que no sea fácil coordinar a los operadores, fabricantes y entes reguladores.

En la Tabla 1 se presentan algunas comparaciones entre las tecnologías que se han mencionado anteriormente.

Tabla 1

Comparativa de bandas y aplicaciones para tecnologías IoT

Tecnología	Frecuencia	Tipo de banda	Aplicaciones comunes
Zigbee	2.4 Ghz	No licenciada	Domótica, comercio, automatización
LoRaWAN	868/915 MHz	No licenciada	Agroindustria, ciudades inteligentes
Sigfox	868/902 MHz	No licenciada	Monitoreo ambiental, activos remotos

Nota. *Elaboración propia con base en Trujillo et al. (2020) y Al-Shareeda et al. (2023).*

2.2.3. *Homologación de dispositivos IoT*

El crecimiento del ecosistema del Internet de las Cosas (IoT) ha traído nuevos desafíos normativos para los reguladores, sobre todo cuando se trata de revisar si los dispositivos que se quieren usar en el país cumplen con lo que exige la ley. La homologación, entendida como el proceso de certificación técnica que asegura básicamente que un equipo es seguro, no interfiere con otros aparatos y usa bien el espectro. Convirtiendo así en una condición esencial para el desarrollo controlado de esta tecnología (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2018).

En Ecuador, las normas actuales no están hechas para tomar en cuenta las características técnicas de los dispositivos IoT, como que gastan poca energía, operan en bandas sin licencia o

envían datos de forma intermitente. Eso genera mucha duda entre quienes fabrican o desarrollan estos dispositivos, porque los trámites que deben seguir fueron diseñados para dispositivos más tradicionales, como routers o celulares.

Por su parte, el país azteca ha inclinado su postura hacia un enfoque más normativo pero no tan rígido. El Instituto Federal de Telecomunicaciones (2019) menciona que sí permite equipos IoT ya homologados en otros países como pueden ser Estados Unidos o Canadá a ingresar el mercado sin necesidad de volver a pasar por los procesos de certificación, con tal que cumplan con las Normas Oficial Mexicanas (NOM), con la NOM-208-SCFI-2016 que regula tecnologías inalámbricas como Zigbee, Wi-Fi y Bluetooth.

Brasil, en cambio, optó por una estrategia diferenciada basada en el riesgo del dispositivo. Según MCTIC (2018) explican que la Agencia Nacional de Telecomunicaciones (ANATEL) ha optado por clasificar los dispositivos IoT según el nivel de riesgo que representan. Así, los que usan en medicina o en industria deben pasar por procesos de certificación más estrictos, mientras que los sensores ambientales o de monitoreo básico pueden seguir trámites más rápidos. Esta resolución fue formalizada mediante el acto regulatorio 735/2020.

Si los países de América Latina lograran ponerse de acuerdo en cómo certificar los dispositivos IoT, se facilitaría la venta de estos equipos entre naciones, se reducirían los gastos en trámites y se lograría que funcionaran mejor entre sí. A este tipo de acuerdo se le conoce como reconocimiento mutuo y se ha propuesto como una vía práctica para avanzar tecnológicamente sin bajar los niveles de calidad (Trujillo et al., 2020).

2.2.4. *Interoperabilidad*

La interoperabilidad es uno de los elementos clave para el funcionamiento eficiente del Internet de las Cosas (IoT), sin importar quién haya fabricado, qué sistema usen o cómo estén

hechos. Y se vuelve fundamental cuando en un mismo lugar se puede combinar distintas tecnologías, como en el comercio local y en la agricultura, donde todo tiene que estar conectado y actualizarse en tiempo real (Barbecho & Gutiérrez, 2021).

Algunos niveles de interoperabilidad se describirán a continuación en la Tabla 2.

Tabla 2

Niveles de interoperabilidad en IoT

Nivel	**Descripción**
Técnico	Capacidad de conectar físicamente dispositivos mediante protocolos estándar
Semántico	Capacidad de interpretar correctamente los datos intercambiados
Organizativo	Alineación de procesos y objetivos entre organizaciones
Legal y contractual	Normativas que regulan el uso compartido de datos y servicios

Nota. *Elaboración propia con base en Barbecho & Gutiérrez (2021) e UIT-T (2012).*

La UIT, en su recomendación Y.2060, explica la interoperabilidad como la habilidad que tienen diferentes sistemas y organizaciones de colaborar entre sí de forma coordinada, sin que una persona tenga que intervenir en medio (UIT-T, 2012). Esa definición es clave para entender cómo deberían organizarse las plataformas IoT que se usan hoy en día.

2.2.5. *Ciberseguridad en IoT*

El Internet de las Cosas (IoT) ha hecho que haya más puntos vulnerables en temas de seguridad. En el comercio, las industrias o casas, los dispositivos conectados están expuestos a riesgos como accesos sin autorización, robo de información, alteración del software o ataques que los saturan hasta que dejan de responder. Todo esto afecta la privacidad y la confianza de quienes lo utilizan. De acuerdo con el Instituto Federal de Telecomunicaciones (IFT), los problemas de seguridad en IoT suelen venir de tres lados: dispositivos que no son muy resistentes, falta de reglas

básicas que los protejan, y canales de comunicación que no están bien resguardados (Trujillo et al., 2020).

Para hacer frente a esos riesgos, organismos internacionales como la ISO y la IEC han creado normas como la ISO/IEC 27400:2022, que ofrece directrices sobre privacidad y seguridad para dispositivos IoT. Lo que propone es pensar en la seguridad desde el momento en que se diseña el dispositivo, usar varios niveles de autenticación y estar siempre revisando si aparecen nuevas vulnerabilidades (Campos & Cavada, 2021).

En el caso latinoamericano, Campos & Cavada (2021) ha señalado que menos del 40% de los países cuentan con estrategias propias de ciberseguridad para el IoT. Esto afecta directamente en áreas sensibles como salud, agricultura y transporte. Al no haber reglas claras, los fabricantes y operadores no tienen un camino definido para proteger los datos desde que empiezan a diseñar un dispositivo hasta que empiezan a funcionar en el mundo real.

En Ecuador, si bien la Ley Orgánica de Protección de Datos Personales (LOPDP) promulgada en 2021 constituye un avance relevante. Pero lo que dice la ley todavía no aborda de manera directa los rasgos propios del IoT. La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ha identificado ese vacío y se insiste en que se deberóan incluir dentro de la regulación cómo recoger los datos necesarios, pedir permiso de forma flexible y tener registro de lo que se hace con la información (Asamblea Nacional del Ecuador, 2021; Instituto Federal de Telecomunicaciones (IFT), 2022).

Desde el punto de vista técnico, la segmentación de redes mediante tecnologías como Zigbee y LoRaWAN, junto con la implementación de controladores de acceso lógico y de cifrado ligero, se consideran buenas prácticas para mitigar ataques en el entorno digital. Estas

recomendaciones han sido aplicadas en entornos comerciales y de automatización (Instituto Federal de Telecomunicaciones (IFT), 2022).

2.2.6. *Normativas internacionales relevantes sobre IoT*

El avance del IoT ha llevado a organismos internacionales a crear marcos normativos que aseguren interoperabilidad, seguridad, privacidad y sostenibilidad en sistemas conectados. Estas reglas buscan condiciones técnicas y legales para integrar soluciones IoT a nivel global, sin afectar derechos fundamentales ni la calidad del servicio.

2.2.6.1. *Principales organismos y estándares internacionales*

Entre las organizaciones que lideran la elaboración de estándares para el IoT se destacan:

- La Unión Internacional de Telecomunicaciones (UIT), con la recomendación Y.2060 sobre arquitectura de referencia IoT.
- La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), con normas como ISO/IEC 30141 e ISO/IEC 27400.
- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que ha promovido protocolos como IEEE 802.15.4 utilizados en tecnologías como Zigbee y Thread.

La norma ISO/IEC 30141 ofrece una guía para describir cómo se organizan los sistemas IoT, especificando los elementos que los componen y cómo se comunican entre nodos, redes y plataformas. Esto ayuda a que distintas soluciones funcionen bien juntas, incluso cuando vienen de fabricantes diferentes. También pone el

enfoque en la seguridad y en poder rastrear lo que pasa con los datos, algo importante en entornos comerciales e industriales (Alfonzo Guzmán, 2020).

Por su parte, el estándar IEEE 802.15.4 es un estándar muy utilizado en IoT para distancias cortas y transmisiones ligeras, ya que sirve como base para tecnologías como ZigBee. Lo que lo hace útil es que gasta poca energía, es resistente a interferencias y conecta muchos dispositivos a la vez, por esta razón, se usa en entornos residenciales, industriales y comerciales (Alfonzo Guzmán, 2020; Instituto Federal de Telecomunicaciones, 2019). A continuación, se presenta la Tabla 3 con algunos de los principales estándares y recomendaciones internacionales sobre IoT.

Tabla 3

Comparación de normativas estándares y lineamientos internacionales

Norma/Marco	**Organismo**	**Enfoque principal**
ISO/IEC 30141:2018	ISO / IEC	Arquitectura de referencia de IoT.
IEEE 802.15.4	IEEE	Comunicaciones inalámbricas de bajo consumo.
Y.2060	UIT-T	Modelo conceptual del Internet de las Cosas.
ISO/IEC 27400	ISO / IEC	Guía de seguridad y privacidad en IoT.

Nota. *Elaboración propia con base en Alfonzo Guzmán (2020) e Instituto Federal de Telecomunicaciones (2019).*

Adoptar estas normas internacionales ayuda a gobiernos y actores del IoT a impulsar un desarrollo tecnológico seguro, que funcione bien entre distintos sistemas y que respete los derechos digitales. Para países como Ecuador, estas referencias son fundamentales para diseñar la regulación.

2.3 Regulación de IoT en América Latina

En América Latina, el desarrollo del Internet de las Cosas (IoT) enfrenta retos importantes por la variedad de normas, el distinto nivel de adopción tecnológica y las capacidades de cada país. A medida que estas tecnologías IoT llegan al comercio, la agricultura, el transporte o la salud, se vuelve necesario contar con reglamentos que aseguren que los sistemas sean compatibles, seguros, protejan los datos y hagan buen uso del espectro.

Este apartado revisa lo que han hecho dos países clave en la región: México y Brasil. Ambos tienen estrategias claras, lideradas por entidades como el Instituto Federal de Telecomunicaciones (IFT) en México y la Agencia Nacional de Telecomunicaciones (ANATEL) en Brasil, para facilitar la implementación del IoT.

2.3.1. *Regulación del IoT en México*

México ha realizado avances significativos en la regulación del IoT. El Instituto Federal de Telecomunicaciones (IFT), como órgano autónomo, ha impulsado políticas para que las redes inteligentes puedan desarrollarse, tocando temas como el uso del espectro, la seguridad y la compatibilidad entre tecnologías.

Una de sus principales estrategias ha sido administrar bien el espectro radioeléctrico. Las bandas de 700 MHz, 600 MHz y 2.5 GHz han sido fundamentales para ofrecer conectividad IoT con baja latencia y buen alcance, incluso en zonas rurales (Trujillo et al., 2020).

Además, el IFT ha impulsado el “Código de Mejores Prácticas para la Ciberseguridad del IoT”, el cual se plantea principios como diseñar los dispositivos pensando en la seguridad desde el inicio, poder actualizarlos a distancia y gestionar bien las identidades, alineado con recomendaciones internacionales como las del NIST (Instituto Federal de Telecomunicaciones (IFT), 2022).

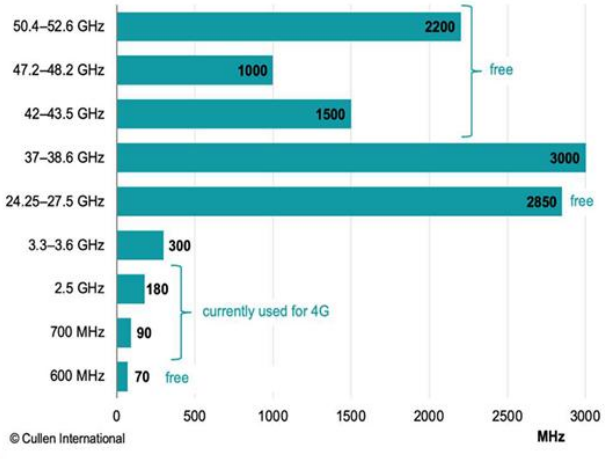
Dentro de su Hoja de Ruta 2021–2025, el IFT planteó acciones para ampliar el espectro disponible, estudiar el avance de nuevas tecnologías y mejorar las condiciones regulatorias para servicios digitales como el IoT. Pero esas iniciativas no han llegado con claridad al sector. Una encuesta entre proveedores del IoT en México mostró que el 82% no sabía de ningún programa gubernamental al respecto, y el 88% desconocía lo que el IFT había hecho en ese tema (Trujillo et al., 2020).

Estos datos muestran que hace falta mejorar la difusión y la coordinación entre el gobierno y las empresas. Siendo necesario seguir avanzando en temas como el espectro, la transición a IPv6, la interoperabilidad, seguridad y la privacidad de los dispositivos IoT.

Como se muestra en la Figura 5, el Instituto Federal de Telecomunicaciones ha identificado diversas bandas de frecuencia para el despliegue de 5G, tanto en rangos altos como medios. Algunas de esas bandas todavía se usan para 4G.

Figura 5

Bandas de espectro 5G en México.



Nota: Distribución de bandas de frecuencia disponibles para 5G en México, según el IFT (ITU, 2019).

2.3.2. *Regulación del IoT en Brasil*

Brasil ha tomado la delantera en América Latina en cuanto a regulación del IoT. Su marco normativo se apoya en planes estratégicos y en instituciones sólidas que impulsan la conectividad, la innovación y la sostenibilidad tecnológica.

El Plan Nacional de Internet de las Cosas, promulgado en 2019 mediante el Decreto N.º 9.854, establece lineamientos para implementar y desarrollar el IoT en el país. Se basa en principios como libre competencia, seguridad de la información y protección de datos personales. Y define cuatro áreas prioritarias: salud, ciudades, industria y el medio rural. Busca mejorar la calidad de vida, hacer más eficientes los servicios, fomentar la innovación, elevar la productividad y competitividad de las empresas, y promover la colaboración entre lo público y lo privado (Presidencia de la República de Brasil, 2019).

La Agencia Nacional de Telecomunicaciones (ANATEL) ha emitido regulaciones como la Resolución N.º 735/2020, introdujo reglas aplicables a operadores móviles virtuales y a servicios

IOT y M2M. Por ejemplo, se permite que un proveedor virtual acreditado tenga acuerdos con más de un operador de origen dentro de la misma área de registro,, además de acuerdos de roaming y uso de red. Con esto se busca flexibilizar la oferta de servicios y reducir obstáculos para que el IoT pueda crecer (Trujillo et al., 2020).

Brasil también estableció un tratamiento regulatorio específico para los sistemas de comunicación máquina a máquina. El decreto N.° 9.854/2019 los define como redes de telecomunicaciones que transmiten datos para monitorear, medir o controlar dispositivos y su entorno desde aplicaciones remotas. Además, le asigna a la ANATEL la tarea de reglamentar y supervisar su uso. Con esto se busca que los servicios M2M e IoT puedan desarrollarse con reglas ajustadas a sus propias características técnicas (Presidencia de la República de Brasil, 2019).

El ecosistema regulatorio se complementa con la Cámara para la gestión y seguimiento del desarrollo de los sistemas M2M e IoT, conocida como Cámara IoT. Es un órgano consultivo que monitorea y evalúa la ejecución del Plan Nacional del IoT, promueve alianzas entre lo público y lo privado, alianzas con los temas del plan de acción y aporta a la formulación de proyectos estratégicos. Está formada por representantes de los ministerios de tecnología, economía, agricultura, salud y desarrollo regional y puede convocar a otras entidades cuando lo considere necesario (Presidencia de la República de Brasil, 2019).

2.3.3. *Comparación de la regulación de IoT en América Latina*

México y Brasil han adoptado enfoques regulatorios distintos para promover el IoT, cada uno ajustando a sus prioridades tecnológicas, capacidades institucionales y estrategias de transformación digital. Aunque comparten ciertos puntos, se diferencian en cómo manejan el espectro, la gobernanza, la ciberseguridad y los mecanismos para llevar a cabo las políticas.

En la Tabla 4 se presentan los principales enfoques regulatorios sobre IoT adoptados por México y Brasil.

Tabla 4

Comparación de los enfoques regulatorios de México y Brasil sobre el IoT

Eje comparativo	**México**	**Brasil**
Marco Estratégico	Hoja de Ruta 2021–2025 para el desarrollo del IoT.	Plan Nacional de IoT (Decreto 9.854/2019)
Gestión del Espectro	Asignación bandas 700, 600 MHz y 2.5 GHz para IoT.	Reducción de barreras para servicios M2M e IoT.
Ciberseguridad	Código de Mejores Prácticas IoT, enfoque basado en NIST.	Coordinación desde la Cámara IoT, alineada a la Estrategia Digital.
Gobernanza institucional	Escasa articulación público-privada reportada.	Modelo colaborativo Cámara IoT
Desafíos identificados	Baja adopción empresarial, desconocimiento de políticas.	Limitaciones de conectividad y expansión del ecosistema.

Nota. *Elaboración propia con base en el Instituto Federal de Telecomunicaciones (2019), Instituto Federal de Telecomunicaciones (IFT) (2022) y la Presidencia de la República de Brasil (2019).*

Brasil y México vienen por caminos distintos, si bien se complementan entre sí. El mexicano se encuentra más avanzado en la planificación del espectro, el análisis de las tecnologías habilitadas o la elaboración de propuestas técnicas propias en IoT, sin embargo transita con dificultades a partir de la comunión de estas acciones, que no son conocidas por las empresas. En Brasil, en cambio, se cuenta ya con una política nacional algo más organizada, con propósitos

claros, la definición de sectores e incluso en un mecanismo de seguimiento de la política nacional, como es la Cámara IoT.

2.3.4. *Modelos regulatorios aplicables al contexto ecuatoriano*

La evolución del marco regulatorio del IoT en América deja lecciones útiles que Ecuador puede considerar para orientar sus propias estrategias normativas. Tanto México como Brasil han majeado el tema de forma diferente, pero ambos tienen cosas que se pueden tomar como buena práctica y ajustar a la realidad del país.

En Brasil, la implementación del Plan Nacional de IoT a través del Decreto N.º 9.854 ha dado una estructura clara para desarrollar soluciones IoT en varios sectores. Prioriza salud, ciudades, industria y el medio rural. Busca fomentar la innovación, mejorar la productividad, hacer más competitivas a las empresas, formar profesionales y promover la colaboración entre lo público y lo privado. También incluye mecanismos para gestionar y hacer seguimiento a todo el plan a nivel nacional (Presidencia de la República de Brasil, 2019).

Por su parte, el enfoque técnico del Instituto Federal de Telecomunicaciones (IFT) de México ha priorizado la gestión del espectro y la ciberseguridad como ejes para la conectividad inteligente. El IFT detalla en su Hoja de Ruta que las políticas de espectro para IoT deben estar acompañadas de estrategias claras de adopción, estándares abiertos y un modelo de gobernanza flexible (Trujillo et al., 2020).

Otra enseñanza clave es la Cámara IoT en Brasil. Es la entidad encargada que le da seguimiento al plan, que une a entidades públicas y privadas y que apoya proyectos para desarrollar soluciones IoT (Trujillo et al., 2020).

Además, usar estándares internacionales ayuda a que el IoT sea más seguro y funcione mejor entre distintos sistemas. El NIST ofrece guías y herramientas para proteger los dispositivos

conectados, y la UIT trabaja en normas que aseguran que sensores, redes y plataformas puedan entenderse entre sí (Instituto Federal de Telecomunicaciones (IFT), 2022).

2.4 Análisis comparativo de los marcos regulatorios de IoT en México y Brasil

2.4.1. *Gestión del espectro radioeléctrico en México y Brasil*

En México, el Instituto Federal de Telecomunicaciones (IFT) ha tomado decisiones importantes para habilitar espectro que sirva al IoT. El Pleno del Instituto resolvió que "la banda de frecuencias 5925-6425 MHz se clasifica como de uso libre" (Instituto Federal de Telecomunicaciones (IFT), 2023), lo que abrió la puerta al WiFi 6E y a aplicaciones IoT de corto alcance. Asimismo, el IFT también ha estudiado la forma en la que crece la demanda de la conectividad, ya que se tiene pronosticado que las tecnologías LPWA (Low Power Wide Area) pasarán del 2% de las conexiones de IoT en 2016 al 63% de las conexiones en 2026, lo que hace que deba planificarse espectro específico para estas tecnologías (Camacho Castillo, 2019).

En Brasil, el Decreto Nº 9.854/2019 crea el Plan Nacional de Internet de las Cosas y establece que el desarrollo de este debe ser a partir de "principios de libre competencia, libre circulación de datos, seguridad de la información y protección de datos personales" (Presidencia de la República de Brasil, 2019). Aunque el decreto no asigna bandas específicas, crea una Cámara de Gestión y Acompañamiento responsable de coordinar políticas de espectro e innovación en salud, industria, ciudades y agro.

2.4.2. *Homologación de dispositivos IoT*

En México, los lineamientos de 2019 sobre homologación de equipos de telecomunicaciones y radiocomunicación (TyR) incluyeron la categoría de equipos de corto alcance, donde entran tecnologías como RFID, ZigBee o LoRa. El IFT, en su Análisis exploratorio de IoT señaló que acortar los tiempos y economizar los costos de homologación resulta

fundamental para que el IoT puede crecer en el mercado mexicano (Instituto Federal de Telecomunicaciones, 2019). Además, en materiales técnicos se menciona que desde 2018 los dispositivos de radiocomunicaciones de corto alcance ya estaban en la agenda regulatoria, lo que luego derivó en los lineamientos del 2019 (Camacho Castillo, 2019).

La ley general de telecomunicaciones de Brasil, la ley n.º 9.472/1997, prevé que todos los equipos sean homologados por ANATEL para propiciar una adecuada compatibilidad técnica y seguridad del usuario. La resolución nº 680/2017 de ANATEL regula los equipos de radiación restringida, es decir, de corto alcance; les permite funcionar, sin requerir licenciamiento adicional, durante el período que hayan sido evaluados en condiciones de conformidad y certificados de manera oficial (ANATEL, 2017). El decreto 9.854/2019 fortalece este entorno al relacionar el IoT con el cumplimiento de las normas técnicas y de homologación (Presidencia de la República de Brasil, 2019) .

2.4.3. *Interoperabilidad*

En México, el IFT tiene claro que el 5G va a conectar una cantidad grande de dispositivos. Para que funcione de manera correcta requiere “plataformas interoperables y estandarizadas” para garantizar que no queden atados a una sola tecnología, y que el sistema pueda crecer sin problemas (Camacho Castillo, 2019).

En Brasil, la interoperabilidad se establece como uno de los principios fundamentales en el Plan Nacional de IoT, señalando que los servicios y dispositivos tienen que integrarse de forma clara y abierta, sin complicaciones que impidan que funcionen juntos (Presidencia de la República de Brasil, 2019).

2.4.4. *Ciberseguridad*

En México, el IFT publicó el Código de Mejores Prácticas en Ciberseguridad para IoT, que recomienda que los dispositivos se diseñen pensando en la seguridad desde el principio, que los datos estén protegidos durante el uso del dispositivo, y que las redes y servicios sean capaces de mantenerse estables incluso ante fallos o ataques (Instituto Federal de Telecomunicaciones (IFT), 2022). El código mencionado arriba constituye una guía voluntaria para fabricantes y operadores.

Brasil ha dado un paso adelante al adoptar un modelo normativo más estricto. La Resolução nº 740/2020 de ANATEL contiene reglas de ciberseguridad aplicadas a las redes de telecomunicaciones, en el que se fijan tres principios: que la información sea confidencial, que no se altere sin autorización y que esté disponible cuando sea necesaria (ANATEL, 2020). A su vez, el Ato nº 77/2021 impone a los equipos, entre otras intervenciones, el cumplimiento de ciertos requisitos de ciberseguridad. Por ejemplo, los fabricantes tienen que asegurarse de que se puedan corregir fallos mediante actualizaciones de firmware, y también deben presentar una declaración donde certifiquen que el dispositivo cumple con lo que pide la norma (ANATEL, 2021).

2.4.5. *Tabla comparativa de los marcos regulatorios de IoT de México y Brasil*

En la Tabla 5 se presenta un resumen comparativo de los principales elementos regulatorios analizados en México y Brasil respecto al Internet de las Cosas, tomando en cuenta los parámetros desarrollados en este apartado.

Tabla 5

Síntesis comparativa de los principales componentes regulatorios de IoT en México y Brasil

Parámetro	**México**	**Brasil**	**Diferencia principal**
Gestión del espectro radioeléctrico	Categoría de bandas de uso libre y planificación del espectro para tecnologías IoT.	El Plan Nacional de Internet de las Cosas sincroniza políticas de espectro partiendo de principios estratégicos sectoriales.	México da relevancia primordial a la planificación técnica del espectro; Brasil la implementa dentro de una política nacional.
Homologación de dispositivos IoT	Procedimientos de simplificación de la certificación y de reducción de los tiempos de homologación.	Homologación obligatoria a la luz de la Ley 9.472/1997 y regulación especializada sobre radiación restringida.	México modelo flexible, Brasil modelo imperativo y regulador.
Interoperabilidad	Fomento de estándares abiertos y de compatibilidad tecnológica.	Principio primario en el marco del Plan Nacional de la Internet de las Cosas.	Coinciden en su relevancia, si bien Brasil la incorpora al seno de su política nacional.

Ciberseguridad	Código de buenas prácticas y recomendaciones para el refuerzo de la seguridad.	Resolución 740/2020 y Acto 77/2021 con requisitos obligatorios para la ciberseguridad de equipos de telecomunicaciones.	México privilegia lineamientos técnicos; Brasil, incorpora requisitos regulatorios obligatorios.

Nota. *Elaboración propia con base en la normativa de la (ANATEL (2017, 2020, 2021), Camacho Castillo, (2019), Instituto Federal de Telecomunicaciones (2019), Instituto Federal de Telecomunicaciones (IFT) (2022, 2023) y la Presidencia de la República de Brasil (2019).*

2.5 Análisis del caso ecuatoriano

2.5.1. *Gestión del espectro radioeléctrico en Ecuador*

En Ecuador, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es la entidad encargada de la administración del espectro radioeléctrico. Así lo establece la Ley Orgánica de Telecomunicaciones, es la encargada de decidir cómo se usa, quién puede usar y bajo qué condiciones. (Asamblea Nacional del Ecuador, 2015). El Plan Nacional de Frecuencias aprobado por ARCOTEL define qué bandas pueden usarse sin licencia, como 902–928 MHz, 2.4 GHz y 5 GHz, utilizadas en tecnologías de corto alcance como WiFi, ZigBee y LoRa (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021). Estas bandas son clave para aplicaciones IoT en comercio, logística y agricultura.

2.5.2. *Homologación de dispositivos IoT*

En Ecuador, cualquier equipo que quiera conectarse a redes públicas tiene que pasar por un proceso de homologación, siendo la ARCOTEL la entidad encargada, con base en el Reglamento para Homologación y Certificación Técnica de Equipos de Telecomunicaciones. La resolución ARCOTEL-2018-0661 establece los requisitos técnicos que deben cumplir, cómo

controlar las interferencias y también acepta certificaciones de referencia como las de FCC o CE, para que el trámite sea más ágil. Así se aseguran de que los equipos sean compatibles y seguros antes de que empiecen a usarse en el país. La ARCOTEL también tiene lineamientos y matrices técnicas disponibles para que cualquiera pueda consultarlos y verificar si un equipo cumple o no con lo que pide la norma (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2018).

2.5.3. *Interoperabilidad*

La interoperabilidad en Ecuador se maneja a través de la Norma Técnica de Interoperabilidad Gubernamental, publicada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información en 2018. Lo que busca es que los sistemas de las entidades públicas puedan compartir información de manera ordenada y segura, usando estándares que no dependan de una sola tecnología o proveedor (Secretaría Nacional de la Administración Pública (SNAP), 2015). Aunque esa norma se hizo pensando en el sector público, lo que dice también se aplica al IoT. Esto es porque muchas soluciones IoT necesitan conectar dispositivos y plataformas de diferentes marcas o fabricantes, y para eso se requiere que puedan entenderse entre sí. En la Agenda de Transformación Digital 2022–2025, se señala que para que el ecosistema digital funcione correctamente, se necesitan sistemas que sean interoperables y seguros, y eso es justo lo que se necesita para fomentar la innovación en producción y servicios (Meza et al., 2022).

2.5.4. *Ciberseguridad*

El marco de privacidad y seguridad de la información se consolidó con la aprobación de la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento 459 del 26 de mayo de 2021. Establece que para usar datos personales se necesita el consentimiento de la persona, que se usen solo para lo que se acordó y que no se pida más información de lo que se

necesita realmente (Asamblea Nacional del Ecuador, 2021). Al mismo tiempo, el MINTEL, con apoyo de la OEA y el BID, trabajó en la Política de Ciberseguridad, donde señaló que es prioritario proteger las infraestructuras que son importantes para el país y también fortalecer las capacidades para manejar incidentes de seguridad cuando ocurran (Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), 2021). La Agenda de Transformación Digital 2022–2025 refuerza estos lineamientos con su eje de "confianza digital", que plantea como objetivo central la resiliencia frente a ciber amenazas y generar confianza en el uso de servicios digitales (Meza et al., 2022).

2.5.5. *Resumen del marco regulatorio aplicable al IoT en Ecuador*

En la Tabla 6 se resumen los principales elementos regulatorios que influyen en el desarrollo del IoT en Ecuador, según los parámetros previamente analizados.

Tabla 6

Síntesis del marco regulatorio del IoT en Ecuador

Parámetro	**Marco normativo ecuatoriano**	**Característica principal**
Gestión del espectro radioeléctrico.	Ley Orgánica de Telecomunicaciones y Plan Nacional de Frecuencias con bandas de uso libre 902–928 MHz, 2.4 GHz y 5 GHz.	Uso de los bandos libres para las aplicaciones del IoT, pero no planificando de forma especial en esta tecnología.
Homologación de dispositivos.	Resolución ARCOTEL-2018-0661 y normativa general de homologación, con posibilidad de aceptar certificaciones internacionales.	Especifica que todos los equipos tienen que pasar la homologación, aunque en el caso de dispositivos IoT no hay ningún requerimiento de este tipo.

Interoperabilidad.	Norma Técnica de Interoperabilidad Gubernamental y lineamientos de transformación digital que promueven estándares abiertos.	Aplicación orientada al sector público, y no aborda directamente la interoperabilidad del ecosistema IoT.
Ciberseguridad y protección de datos.	Política Nacional de Ciberseguridad, Ley Orgánica de Protección de Datos Personales y Agenda de Transformación Digital 2022-2025.	Lineamientos generales sobre seguridad digital y manejo de datos, pero no fija requerimientos particulares para dispositivos IoT.

Nota. *Elaboración propia con base en la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) (2018, 2021), la Asamblea Nacional del Ecuador (2015, 2021), Meza et al. (2022), el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) (2021) y la Secretaría Nacional de la Administración Pública (SNAP) (2015),*

2.6 Comparativa entre México, Brasil y Ecuador

2.6.1. *Convergencias y divergencias regulatorias de México, Brasil y Ecuador*

México y Brasil coinciden en reconocer la interoperabilidad, la ciberseguridad y la alineación con estándares internacionales como aspectos importantes para el despliegue del IoT. Es necesario mencionar, sin embargo, que el avance de cada uno de los países es distinto. En México ya se tienen lineamientos técnicos, estudios, prácticas sobre la conectividad y la adopción del IoT. En Brasil existe una política nacional mucho más estructurada, con preceptos institucionales y reglas en tema de política pública. En Ecuador, se encuentran normas generales en temas de telecomunicaciones, de datos y de transformación digital, pero no existe todavía un

marco regulatorio propio que integre la mayoría de los elementos técnicos, legales e institucionales del IoT.

En cuanto a si las normas son obligatorias o no, los tres países también se diferencian. México ha optado por un modelo más flexible y progresivo, basado en guías y códigos en buenas prácticas, como el de Ciberseguridad en IoT en 2019 (Instituto Federal de Telecomunicaciones (IFT), 2022). Brasil, en cambio, ha ido por un esquema normativo más definido, sustentado en la Lei Geral de Proteção de Dados (2018) y en disposiciones específicas de la Agência Nacional de Telecomunicações (Anatel), entre ellas la Resolución nº 740/2020 y el Acto nº 77/2021, que establecen exigencias en materia de ciberseguridad aplicadas a redes y dispositivos (ANATEL, 2020) (ANATEL, 2021). Ecuador, por su lado, tiene leyes generales sobre telecomunicaciones, datos personales y ciberseguridad, pero aún no ha desarrollado requisitos obligatorios específicos para dispositivos o servicios IoT, las normas están dispersas en varios documentos, sin una regulación unificada (Asamblea Nacional del Ecuador, 2015, 2021; Meza et al., 2022).

La Tabla 7 compara los principales parámetros regulatorios del IoT en México, Brasil y Ecuador. Muestra las semejanzas y diferencias que existe en estos países.

Tabla 7

Comparación descriptiva de los marcos regulatorios de IoT en México, Brasil y Ecuador.

Parámetro	**México**	**Brasil**	**Ecuador**	**Comparación general**
Espectro	Banda 5925–6425 MHz de uso libre; análisis para LPWA	Plan Nacional de IoT con planificación estratégica del espectro.	Bandas de uso libre definidas en el Plan Nacional de Frecuencias, no se pone ningún	Uruguay y Brasil han incluido estrategias para el IoT; en el caso de Ecuador tiene una

			tipo de planificación para IoT.	regulación general.
Homologación	Lineamientos que incluyen equipos de corto alcance y reduce el proceso de certificación.	Ley 9.472/1997; Res. 680/2017; Ato 77/2021 obligan certificación de equipos.	Homologación obligatoria de los equipos de telecomunicaciones, pero no para IoT.	Brasil ofrece la regulación más concreta; México está expresando la flexibilidad de los procedimientos; Ecuador se limita a un régimen general, de homologación.
Interoperabilidad	Plataformas estandarizadas para el desarrollo del IoT.	Principio rector del Plan Nacional de IoT.	Uso mediante norma de interoperabilidad gubernamental y estándares abiertos.	Los tres países reconocen la interoperabilidad, aunque Ecuador aún no la refiere expresamente para el caso del IoT.
Ciberseguridad	Código de Buenas Prácticas en IoT.	Res. 740/2020 y Ato 77/2021 con requisitos	Política Nacional de Ciberseguridad y Ley Orgánica	Brasil tiene obligaciones específicas; México fomenta

		regulatorios obligatorios.	de Protección de Datos Personales.	las buenas prácticas; Ecuador cuenta únicamente con la regulación general.
Normativas internacionales	Vinculación con UIT-T Y.2060y experiencias internacionales.	Participación en procesos internacionales de normalización e innovación.	Adopción referencial de estándares internacionales en telecomunicaciones y transformación digital.	Utilizan los estándares internacionales como una referencia, eso sí, con un nivel de incorporación al IoT diferente.
Estrategias	Consultas públicas, transición a IPv6 y estudios de mercado.	Centros de competencia, innovación y coordinación institucional.	Agenda de Transformación digital y políticas nacionales de digitalización.	En el caso de México y Brasil tienen iniciativas específicas para el IoT, mientras que en el caso de Ecuador el tema se presenta combinado con

	las estrategias generales de la transformación digital.

Nota. *Elaboración propia con base en el análisis comparativo desarrollado en las secciones 2.4 y 2.5.*

2.6.1. *Comparativa de parámetros entre México, Brasil y Ecuador*

En gestión de espectro, México liberó la banda de 5925–6425 MHz, lo que permite el Wi-Fi 6E y aplicaciones IoT de corto alcance en ciudades. Además, el regulador monitorea cómo crece la demanda de tecnologías LPWA, y usa esa información para tomar decisiones de política (Camacho Castillo, 2019; Instituto Federal de Telecomunicaciones (IFT), 2023). Brasil, con el Decreto N.º 9.854/2019, creó el Plan Nacional de IoT y organizó la acción estatal por sectores: salud, industria, ciudades y agro. También estableció instancias de coordinación para tomar decisiones sobre espectro y adopción tecnológica (Presidencia de la República de Brasil, 2019). En Ecuador, el Plan Nacional de Frecuencias de ARCOTEL mantiene bandas de uso libre, como las de 2.4 y 5 GHz, que usan soluciones IoT de corto alcance. La administración general del espectro sigue rigiéndose por la Ley Orgánica de Telecomunicaciones (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021; Asamblea Nacional del Ecuador, 2015). Los tres países amplían sus respectivos stock de espectro dedicado para IoT. México liberó la banda de 6 GHz, Brasil eligió priorizar una organización por sectores, y Ecuador cuenta con bandas liberadas, ya definidas.

Con respecto a la homologación de dispositivos, México realizó la actualización de lineamientos para equipos de corto alcance y propuso que una de las líneas de acción sería la de reducir tiempos y costos de la evaluación como forma de ampliar el mercado IoT (Instituto Federal

de Telecomunicaciones, 2019). Brasil se mantiene con un esquema mandatorio y mucho más denso. La ANATEL pide certificación y agrega requisitos de seguridad según norma (Res. N.º 740/2020; Ato N.º 77/2021) (ANATEL, 2020, 2021). Ecuador también pide homologación obligatoria para comercializar o conectar dispositivos a redes públicas. Y acepta certificaciones de referencia como FCC o CE a efectos de comprobar la conformidad técnica, según establece la resolución ARCOTEL-2018-0661 (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2018). Los tres marcos exigen homologaciones. Brasil los integra en el proceso de autorregulación, con requisitos de ciberseguridad. México privilegia los trámites más básicos para la autorización. Ecuador centraliza el control en ARCOTEL, con criterios técnicos que son reconocidos internacionalmente.

En interoperabilidad, México observa la misma como una condición necesaria al ecosistema 5G e IoT, conforme los análisis del IFT. Por eso promueve plataformas estándar y neutrales (Instituto Federal de Telecomunicaciones, 2019). Brasil se constituye como un principio básico del Plan Nacional de IoT, para aquellas industrias prioritarias a efectos de que las aplicaciones se encajen entre sí bien (Presidencia de la República de Brasil, 2019). Ecuador establece que la Norma Técnica de Interoperabilidad Gubernamental señala los lineamientos para un intercambio seguro en el sector público, y esos criterios también aplican para proyectos IoT que requieran interoperar con plataformas existentes o bien con sistemas que provengan de diferentes proveedores (Meza et al., 2022). Los tres países concuerdan en la interoperabilidad como requisito de escalabilidad y neutralidad tecnológica.

En ciberseguridad, México adoptó con un Código de Mejores Prácticas en Ciberseguridad que funciona como una guía voluntaria para los fabricantes, proveedores y operadores (Instituto Federal de Telecomunicaciones (IFT), 2022). Brasil hizo un avance al establecer requisitos

obligatorios, ya que la Resolução N.º 740/2020 fija las pautas de seguridad en las redes y el Ato N.º 77/2021 incluye requisitos de ciberseguridad para los equipos, como la gestión de vulnerabilidades, las actualizaciones de firmware y una declaración de conformidad (ANATEL, 2020, 2021). Ecuador encuentra la confianza digital en la Ley Orgánica de Protección de Datos Personales de 2021 y en los trabajos de la Agenda de Transformación Digital 2022–2025 que prioriza las capacidades e infraestructura de seguridad como condición para los servicios emergentes, incluido el IoT (Asamblea Nacional del Ecuador, 2021; Meza et al., 2022). La diferencia principal es que Brasil ha optado por un enfoque obligatorio, mientras que México usa guías orientativas y Ecuador se apoya en un marco de privacidad y confianza digital.

2.6.2. *Evaluación comparada de los parámetros principales de IoT en México, Brasil y Ecuador*

En la Tabla 8 se presenta una comparación de los parámetros más importantes para la regulación del IoT en México, Brasil y Ecuador, conforme al análisis desarrollados en este capítulo.

Tabla 8

Comparación de los principales parámetros regulatorios de IoT en México, Brasil y Ecuador

Parámetro	**México**	**Brasil**	**Ecuador**
Gestión del espectro	Banda 5925–6425 MHz catalogada como de uso libre por sus condiciones técnicas y modelo de uso; análisis predictivo de LPWA.	El Plan Nacional de IoT prevé en su inclusión el proceso de planificación del espectro como parte de la estrategia nacional.	Plan Nacional de Frecuencias que cuenta con bandas de frecuencia libres en 2.4 y 5 GHz; administración general

			que corresponde a ARCOTEL.
Homologación de dispositivos	Normas 2019; incorpora estándares de la tecnología para equipos de corto alcance; plazos, costes.	Homologación obligatoria; requisitos técnicos y de seguridad obligatorios.	Homologación obligatoria a raíz de la disposición ARCOTEL-2018-0661; posibilidad de reconocimiento de certificaciones internacionales.
Interoperabilidad	Incentivo a las plataformas interoperables y los estándares abiertos.	Principio rector del Plan Nacional de IoT.	Norma Técnica de Interoperabilidad Gubernamental; su ámbito de aplicación se reduce al sector público.
Ciberseguridad	Código de Mejores Prácticas en IoT de carácter no vinculante (IFT, 2019).	Resolución 740/2020 + Ato 77/2021 con obligaciones (ANATEL, 2020; 2021).	Ley Orgánica de Protección de Datos Personales y Agenda de Transformación Digital 2022-2025, con enfoque general en seguridad digital,

Nota. *Elaboración propia con base en la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) (2018, 2021), la ANATEL (2020, 2021), la Asamblea Nacional*

del Ecuador (2015, 2021), Camacho Castillo (2019), el Instituto Federal de Telecomunicaciones (2019, 2023), Meza et al. (2022) y la Presidencia de la República de Brasil (2019),

Capítulo III: Marco metodológico

En este capítulo se plantea un análisis de la posición que ocupa el Internet de las Cosas (IoT) en Ecuador desde el ámbito normativo, institucional y técnico, a partir de su potencial integración a la normativa de comercio local. Este análisis es inspirado en las que se han realizado en México y Brasil cuyas normativas permiten establecer formas de comparación del avance, las mejores prácticas, y los enfoques que sean más pertinentes al contexto ecuatoriano.

Primero se centra en las normas y en los enfoques regulatorios internacionales sobre el IoT, luego profundiza sobre los descriptos a partir de los principales problemas que enfrenta el Ecuador en materia de infraestructura digital, de la gestión del espectro radioeléctrico, de la certificación de dispositivos, de la ciberseguridad, la protección de datos o de gobernanza institucional. Esto posibilita esbozar limitaciones existentes en el contexto nacional y factores que pueden hacer compete en parte la incorporación de modo fluido de IoT respecto de la actividad comercial.

Además, se presentan los requerimientos identificados para Ecuador, clasificando los criterios de análisis más importantes. Esta estructura permite establecer la conexión entre los desafíos identificados y los elementos que deben fortalecerse para la creación de la futura regulación del IoT en el comercio local, considerando tanto el contexto ecuatoriano como las mejores prácticas observadas en México y Brasil.

3.1 Normativas relevantes internacionales en México, Brasil y Ecuador

En México, el Instituto Federal de Telecomunicaciones ha destacado la importancia de alinear el IoT con marcos internacionales como la Recomendación UIT-T Y.2060, que define al IoT como una infraestructura global escalable e interoprable (Instituto Federal de

Telecomunicaciones, 2019). Además, el organismo señala que México debería fijarse en lo que han hecho otras regiones, como Estados Unidos, Europa y Asia, para tomar buenas prácticas regulatorias y ajustarlas al contexto nacional (Camacho Castillo, 2019).

En Brasil, el Plan Nacional de IoT incluye como uno de sus objetivos integrar al país en el ámbito internacional. Para eso, plantea participar en foros de estandarización y fomentar la cooperación en investigación, desarrollo e innovación (Presidencia de la República de Brasil, 2019).

Ecuador es miembro de la Unión Internacional de Telecomunicaciones (UIT) desde 1884, lo que le permite participar en la estandarización y en la definición de lineamientos internacionales sobre telecomunicaciones y tecnologías digitales (UIT, 2023). Una de las recomendaciones importantes es la UIT-T Y.2060. El IoT se define, en efecto, como una infraestructura abierta, a la escala del mundo, orientada a la sociedad de la información. Integra objetos físicos y virtuales de modo de proporcionar servicios de alto nivel (UIT-T, 2012). Aunque Ecuador no ha incorporado explícitamente esta recomendación en su normativa, como es miembro, tiene acceso esos marcos técnicos y puede utilizarlos a modo de referencia.

En el ámbito nacional, la Agenda de Transformación Digital 2022–2025 expresa que Ecuador debe integrarse mejor a los marcos internacionales y regionales para lograr en consecuencia que los servicios digitales sean interoperables y seguros. El documento también plantea que la cooperación internacional es clave para consolidar el ecosistema digital y para adoptar estándares que le den competitividad al país en la economía digital (Meza et al., 2022). En la misma línea, el Plan de Creación de Oportunidades 2021–2025 reconoce que la innovación y la digitalización son ejes clave para impulsar la productividad y modernizar sectores como comercio, agricultura y servicios (Secretaría Nacional de Planificación, 2021). Más recientemente, el Plan de

Desarrollo para el Nuevo Ecuador 2024–2025 subraya que hace falta impulsar la infraestructura digital y la capacitación tecnológica. Lo ve como condiciones básicas para que el país sea competitivo y pueda avanzar en transformación digital (Secretaría Nacional de Planificación, 2024).

3.2 Estrategias e incentivos regulatorios en México, Brasil y Ecuador

En México, el IFT ha promovido consultas públicas sobre el uso del espectro, para diseñar políticas con base en datos reales, además de fomentar la transición a IPv6, considerada fundamental para el IoT puede crecer (Instituto Federal de Telecomunicaciones, 2019). También han hecho estudios sobre la comercialización de servicios IoT, para usarlos como base y definir incentivos regulatorios (Trujillo et al., 2020).

En Brasil, el Decreto nº 9.854/2019 que crea el Plan Nacional de IoT, plantea estrategias como la creación de plataformas de innovación y centros de competencia. La idea es que lo público y lo privado trabajen juntos en el desarrollo de soluciones tecnológicas (Presidencia de la República de Brasil, 2019).

En Ecuador, las estrategias regulatorias se manejan a través de la Agenda de Transformación Digital 2022-2025. Este documento plantea cuatro ejes principales: conectividad, confianza digital, economía digital y talento humano. Todo eso busca crear condiciones favorables para tecnologías como el IoT. La Agenda también resalta la importancia de realizar proyectos piloto en sectores clave, reducir las trabas regulatorias y apoyar a las pymes mediante programas de capacitación y digitalización (Meza et al., 2022). Además, la Ley de Protección de Datos de 2021 ofrece un marco legal que refuerza la seguridad y la confianza en los entornos digitales. Eso es justo lo que se necesita para que los servicios basados en IoT puedan desplegarse con mayor tranquilidad (Asamblea Nacional del Ecuador, 2021).

También están el Plan de Creación de Oportunidades 2021–2025 y el Plan de Desarrollo para el Nuevo Ecuador 2024–2025. Ambos plantean la transformación digital como herramienta clave para aumentar la productividad, se enfocan en tres aspectos: inversión tecnológica, cobertura de infraestructura y fortalecimiento de talento digital (Secretaría Nacional de Planificación, 2021;Secretaría Nacional de Planificación, 2024). A esto se le debe añadir el Plan Nacional de Frecuencias de ARCOTEL, que ha liberado bandas como 902–928 MHz, 2.4 GHz o 5 GHz para aquellos dispositivos de corto alcance, facilitando el despliegue de soluciones IoT en el sector del comercio y la agricultura (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021). Todos ellos son hitos en las políticas públicas y los incentivos regulatorios. Aun así, Ecuador debe superar la serie de desafíos que le permita contar con un ecosistema digital competitivo, acorde a lo que de él demanda el IoT.

3.3 Desafíos técnicos, legales e institucionales

3.3.1. *Retos técnicos y de infraestructura digital*

El IoT en Ecuador todavía enfrenta problemas de base: la conectividad no llega igual a todas partes, la cobertura es irregular y la capacidad tecnológica es limitada. La Agenda de Transformación Digital 2022-2025 lo dice claro: hay una brecha marcada entre lo urbano y lo rual, y eso frena las soluciones tecnológicas puedan crecer de forma sostenible (Meza et al., 2022). Esas diferencias en conectividad limitan la posibilidad de implementar plataformas IoT a nivel nacional, sobre todo en agricultura o logística, donde el comercio local necesita de infraestructura básica para funcionar.

De acuerdo con el Plan Nacional de Frecuencias de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), la mayoría de tecnologías IoT que se usan hoy operan en bandas libres como 2.4 GHz o 5GHz. Sin embargo, no existe una planificación elaborada para

redes LPWAN, ni para NB-IoT (Agencia de Regulación y Control de las Telecomunicaciones (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021). Asimismo, Ecuador no cuenta con redes 5G disponibles en el comercio, y su capacidad para interconectar dispositivos y transmitir información en tiempo real es muy escasa. La Comisión Económica para América Latina y el Caribe (CEPAL) afirma que los países andinos deben trabajar para mejorar la cobertura y la velocidad en las redes de telefonía móvil para aprovechar la economía digital (Comisión Económica para América Latina y el Caribe (CEPAL), 2022).

En este contexto, Ecuador necesita invertir de forma constante en infraestructura digital y en actualizar el uso del espectro. También se requieren incentivos regulatorios que ayuden a llevar Internet a zonas rurales y a fortalecer la base técnica del IoT en el país.

3.3.2. *Desafíos normativos y regulatorios*

Ecuador aún no tiene una ley propia para el IoT, y eso frena bastante su avance. La Ley de Telecomunicaciones de 2015 regula lo básico del espectro y los servicios de telecomunicaciones, pero no toca temas como los requisitos técnicos, la certificación de dispositivos o cómo hacer que distintos sistemas funcionen entre sí. Y el IoT moderno necesita justo eso. (Asamblea Nacional del Ecuador, 2015). Por otro lado, la Resolución ARCOTEL-2018-0661 exige que cualquier equipo de telecomunicaciones pase por homologación antes de venderse o conectarse a redes públicas, sin distinguir entre dispositivo convencional o destinado para IoT (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2018).

La Agenda de Transformación Digital 2022–2025 insiste que hace falta ajustar el marco normativo. La idea es crear un entorno que realmente permita innovar y usar tecnologías emergentes (Meza et al., 2022). Pero el problema es que las normas están repartidas entre

protección de datos, telecomunicaciones y comercio electrónico, dejando espacios sin cubrir, sobre todo cuando hay que definir quién responde por la información que generan los dispositivos conectados .De acuerdo con la Comisión Económica para América Latina y el Caribe (CEPAL) (2022), esta fragmentación se da en varios países de la región, lo que hace retrasar la adopción de políticas que aborden el IoT de manera integral, cuando justamente es una tecnología que atraviesan muchos sectores.

Ecuador tiene el reto de poner en orden en su legislación y sumar disposiciones que reconozcan explícitamente las redes y dispositivos IoT, siguiendo la experiencia de México y Brasil, donde los reguladores ya han establecido lineamientos técnicos específicos y estrategias nacionales para digitalizar el comercio y la industria.

3.3.3. *Ciberseguridad y protección de datos*

Cuando se habla de datos generados por dispositivos IoT, la protección tiene que ser más fuerte. En Ecuador, la Ley de Protección de Datos Personales establece principios como el de licitud, lealtad, transparencia, minimización y seguridad; así como también establece la necesidad de implementar medidas técnicas y organizativas en función del nivel de riesgo que suponga la actividad de tratamiento, tal como establecen los artículos del 3 al 7 (Asamblea Nacional del Ecuador, 2021). La ley regula y establece las bases legales para el tratamiento, derechos de los titulares, así como los sujetos del tratamiento de datos, responsables y encargados, incluyendo la gestión de incidentes y la notificación de brechas. También contempla transferencias internacionales con garantías adecuadas y, en casos de alto riesgo, evaluaciones de impacto previas al tratamiento. (Asamblea Nacional del Ecuador, 2021). Aunque la ley no usa la palabra "IoT" de manera explícita, su alcance abarca cualquier tratamiento automatizado de datos, así que aplica sin problema a soluciones conectadas en el comercio local.

En ciberseguridad, la Política Nacional de Ciberseguridad 2018–2021 prioriza proteger infraestructuras y servicios digitales, en la gestión de riesgos, la respuesta a incidentes y en coordinar entre lo público-privada, con líneas de acción para fortalecer capacidades y cultura de seguridad a nivel nacional (Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), 2021). La Agenda de la Transformación Digital 2022-2025 incluye la confianza digital como eje y propone medidas para reforzar la seguridad y la protección de datos en servicios emergentes (Meza et al., 2022). De este modo, para proyectos orientados al comercio de IoT, implica pensar en seguridad desde el diseño; cifrar los datos durante el trayecto como cuando están guardados, cumplir con el establecimiento de controles de acceso bien definidos, la gestión de vulnerabilidades, el registro de los eventos que recogen los dispositivos e ir manejando los datos en la línea que establece LOPDP.

En la práctica, hay que mantener un registro claro de los dispositivos IoT empleados, tales como sensores o pasarelas, así como la clasificación de los datos que gestionan, ya sean personales, sensibles o de telemetría. Un aspecto importante es determinar el tiempo que se guardan y que la privacidad esté considerada desde el principio. Cuando el volumen de los datos o el contexto pone a las personas en alto riesgo, se debe llevar a cabo una evaluación de impacto. Y, si el caso lo amerita, designar a un delegado de protección de datos que vigile que se cumpla todo (Asamblea Nacional del Ecuador, 2021). Estos requisitos legales van de la mano con lo que plantea la política pública. La idea es que el IoT se extienda en comercios y cadenas de suministro con controles acordes al riesgo, y que existan mecanismos de respuesta a incidentes coordinados entre las instituciones.

3.3.4. *Gobernanza institucional y capacidades nacionales*

Para que el IoT avance en Ecuador, se necesita una buena coordinación entre el sector público, el privado y la academia. El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) es quien diseña las políticas digitales, y la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) se encarga del espectro, la homologación de equipos y la supervisión técnica. Pero la propia Agenda de Transformación Digital 2022–2025 reconoce que la coordinación entre instituciones sigue siendo débil, y eso frena proyectos digitales que podrían tener un impacto real a nivel nacional (Meza et al., 2022). Esa fragmentación entre instituciones se nota, sobre todo, en que no hay un órgano que junte las políticas de telecomunicaciones, innovación y protección de datos con una misma visión estratégica.

El Plan de Creación de Oportunidades 2021–2025 resalta la necesidad de tener una gestión estatal bien articulada que impulse el desarrollo productivo y tecnológico (Secretaría Nacional de Planificación, 2021). Pero la falta de mecanismos estables de coordinación entre el MINTEL, la SENPLADES, el Ministerio de Producción y la Superintendencia de Protección de Datos hace que las políticas digitales a largo plazo no se ejecuten bien. Además, la Política Nacional de Ciberseguridad 2018–2021 ya había señalado que el país tiene poco personal técnico especializado, y recomendó crear programas de formación y certificación para fortalecer las capacidades nacionales (Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), 2021)

También es clave fortalecer las capacidades digitales y técnicas para que el IoT crezca. La Agenda de Transformación Digital 2022–2025 incluye, como uno de sus ejes, el desarrollo del talento humano, con el objetivo de formar especialistas en ciberseguridad, análisis de datos e inteligencia artificial (Meza et al., 2022). Aún persiste, en efecto, una distancia considerable entre

lo que enseñan las universidades y lo que el sector profesional tecnológico realmente necesita. Esta situación provoca el estancamiento de la innovación y la adopción de tecnologías por parte del comercio local. Para aproximarse a esa distancia es necesario afianzar la gobernanza digital entendida como el conjunto de instituciones que trabajan de manera conectada, con procesos claros y con una visión compartida de la transformación tecnológica que se quiere lograr, y debe alinearse con los Objetivos de Desarrollo Sostenible y con las estrategias digitales de la región.

3.3.5. *Sistematización de los desafíos identificados para la regulación del IoT en Ecuador*

La Tabla 9 recoge los principales desafíos que Ecuador enfrenta para integrar el IoT en el comercio local. Están agrupados en cuatro áreas: técnica, normativa, ciberseguridad e institucional.

Tabla 9

Resumen de los desafíos técnicos, legales e institucionales para el desarrollo del IoT en Ecuador

Dimensión	**Situación identificada**
Técnica	Hay diferencias grandes en conectividad entre ciudades y zonas rurales. La mayoría de aplicaciones IoT usan bandas libres, y todavía no hay redes 5G disponibles en el mercado.
Normativa	No hay una ley propia para el IoT. Las normas están repartidas entre telecomunicaciones, protección de datos y transformación digital.
Institucional	Hay poca coordinación entre las entidades encargadas, no existe un organismo dedicado al IoT y hace falta fortalecer las capacidades técnicas del país.

Nota. *Elaboración propia a partir del análisis de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) (2021) y de la Asamblea Nacional del Ecuador (2015, 2021),*

Meza et al. (2022) , el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) (2021) y la Secretaría Nacional de Planificación (2021).

3.4 Análisis comparativo de requerimientos para la regulación del IoT en Ecuador

3.4.1. *Requerimientos legales*

El análisis realizado permite identificar que Ecuador tiene normas generales para el entorno digital, pero no regulaciones específicas para el IoT aplicado al comercio. La Ley de Telecomunicaciones maneja lo relacionado con servicios y espectro, y la LOPDP establece reglas sobre datos personales. No obstante, ninguna de las dos toca directamente aquello que significa para el comercio del lugar que exista el uso de dispositivos interconectados, de sensores o plataformas automatizadas (Asamblea Nacional del Ecuador, 2015, 2021).

A la diferencia del Ecuador, México y Brasil ya cuentan con instrumentos regulatorios que incorporan al IoT de manera expresa ya sea en la manera de códigos de buenas prácticas, lineamientos técnicos o planes nacionales. Estas experiencias demuestran que la carencia de definiciones y normativas, sea en materia de responsabilidad civil, protección de los consumidores digitales, o incluso de la seguridad de la información, produce incertidumbre jurídica. Pero esto no significa que sea necesario crear una normativa completamente nueva desde cero. Se puede complementar el marco existente, tal como lo plantea la Agenda de Transformación Digital 2022–2025 (Meza et al., 2022).

En la Tabla 10 se resumen los principales requerimientos legales que se han identificado para regular el IoT en el comercio local ecuatoriano. Para elaborarla, se tomó como base el análisis del marco normativo del país y las experiencias regulatorias de México y Brasil.

Tabla 10.

Requerimientos legales para la regulación del IoT en el comercio local ecuatoriano

Elemento legal	Situación en Ecuador	Referencia comparada (México / Brasil)	Requerimiento identificado
Protección de datos personales	La LOPDP es la que regula de forma general el tratamiento de datos de carácter personal, no ofrece determinaciones específicas para el caso del IoT.	México: Código de Buenas Prácticas en IoT; Brasil: LGPD con demandas técnicas.	Incluir criterios específicos para los datos que sean generados de forma automática por los dispositivos IoT
Banda de operación (licenciamiento)	El Plan Nacional de Frecuencias establece como bandas de uso libre las de 2,4 GHz y 5 GHz, pero en él tampoco se encuentra una categoría específica como IoT.	México asigna bandas de frecuencia específicas para promover el IoT, Brasil suma la planificación del espectro a su planificación nacional.	Introducir categoría normativa que defina o estime determinadas bandas definidas o priorizadas para el IoT
Reconocimiento jurídico del IoT	No está reconocido el IoT como una categoría jurídica, estableciendo por ende los criterios específicos de la misma.	Brasil admite el IoT en su Plan Nacional, México aborda el tema por medio de estudios regulatorios.	Añadir definición legal/reglamentaria del IoT dentro del marco normativo ecuatoriano

Responsabilidad de los actores	Las responsabilidades que puedan surgir por el uso del IoT no se suelen diferenciar entre fabricantes, operadores y usuarios.	Brasil fija obligaciones técnicas diferenciadas, México promueve una distribución de obligaciones y deberes entre los diferentes actores del ecosistema.	Definir responsabilidades legales en función del rol en el ecosistema IoT.
Homologación de dispositivos	Homologación obligatoria de carácter general, no diferenciada para IoT.	México y Brasil estudian tecnologías de corto alcance y especificaciones concretas	Adaptar la homologación a las propiedades técnicas y operativas de los dispositivos IoT.
Regulación de aplicaciones y servicios	No hay disposición alguna específica para aplicaciones IoT de comercio local.	Brasil promueve el IoT para sectores estratégicos; México genera su uso en sectores concretos	Prever lineamientos para utilizar y fomentar aplicaciones y servicios IoT en comercio, logística y otros sectores productivos.
Tecnologías habilitadas	No hay listado o reconocimiento normativo de tecnologías IoT (LPWAN, NB-IoT, etc.).	México examina el desarrollo de las LPWA, mientras que Brasil esboza la categorización como sector industrial.	Definir criterios técnico-normativos para el reconocimiento de tecnologías IoT

			habilitadas o recomendadas.
Seguridad de la información	Regulada transversalmente tanto por la LOPDP como por las políticas de la ciberseguridad.	Brasil propone requisitos obligatorios; México lo hace con orientaciones.	Regular los requisitos mínimos de seguridad de dispositivos, redes y servicios IoT.
Protección del consumidor digital	No admite el uso del IoT en las relaciones de consumo por parte de la normativa comercial.	México y Brasil promueven el IoT en el comercio bajo marcos sectoriales.	Incorporar disposiciones para garantizar la protección del consumidor como consecuencia del uso de IoT en el comercio local.
Uso de IoT en actividades comerciales	No hay disposiciones para su aplicación en un comercio local.	Ambos países promueven el IoT como herramienta para la productividad.	Regular las bases requeridas para la buena regulación del uso del IoT en el comercio local que sean seguras, transparentes y responsables.

Nota. *Elaboración propia con base en el análisis de (Asamblea Nacional del Ecuador, 2015, 2021; Meza et al., 2022) y los marcos regulatorios del Internet de las Cosas desarrollados en México y Brasil.*

Desde el punto de vista jurídico, estos requerimientos muestran que Ecuador ya tiene una base normativa que puede servir para empezar a regular el IoT. Pero hacen falta ajustes puntuales que den más certeza a quienes participan en el comercio local. Incorporar estos elementos de forma gradual permitiría fortalecer la seguridad jurídica, proteger derechos fundamentales y facilitar que el IoT se adopte como una herramienta de innovación comercial, sin necesidad de cambiar la estructura general del ordenamiento legal vigente.

3.4.2. *Requerimientos institucionales*

El análisis del contexto ecuatoriano muestra que los principales retos para implementar el IoT no son solo normativos. También tienen que ver con la estructura institucional y cómo se coordinan las entidades. A diferencia de México y Brasil, donde los reguladores tienen funciones claras y mecanismos de articulación entre instituciones, en Ecuador las competencias están repartidas entre varios organismos y no hay uno específico que coordine estas iniciativas (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021; Meza et al., 2022).

La Tabla 11 recoge los principales requerimientos institucionales para fortalecer la gobernanza del IoT en Ecuador. Para elaborar, se tomaron como referencia las experiencias de México y Brasil, así como el marco institucional del país.

Tabla 11.

Requerimientos institucionales para la gobernanza del IoT en Ecuador

Elemento institucional	Situación en Ecuador	Referencia comparada (México / Brasil)	Requerimiento institucional identificado
Coordinación institucional	Competencias distribuidas entre MINTEL, ARCOTEL y otras entidades, sin órgano coordinador específico.	Brasil: Cámara de Gestión del Plan Nacional de IoT; México: rol articulador del IFT.	Crear un mecanismo formal de coordinación interinstitucional para el desarrollo del IoT.
Rol del regulador	ARCOTEL regula espectro y homologación, sin enfoque específico en IoT.	IFT y ANATEL desarrollan estudios y lineamientos específicos para IoT.	Fortalecer las competencias técnicas del organismo regulador en materia de IoT.
Articulación público-privada	Iniciativas sectoriales y proyectos de POC descontinuados.	Brasil promueve los centros de competencia; México promueve las consultas públicas.	Crear espacios de articulación con el sector productivo de forma permanente.
Capacidades institucionales	Limitaciones en la disponibilidad de personal especializado en IoT y en ciberseguridad.	Brasil y México promueven el fortalecimiento institucional y de capacidades.	Reforzar en la medida de lo posible las capacidades técnicas y especializadas de las

			entidades rectoras y reguladoras.
Planificación estratégica	No existe un plan nacional específico de IoT.	Brasil dispone de un Plan Nacional de IoT; México de informes sectoriales.	Definir una estrategia nacional que sirva de guía para el desarrollo e implementación del IoT.
Análisis del espectro	ARCOTEL maneja el espectro de acuerdo con la Ley Orgánica de Telecomunicaciones, pero no existe un análisis específico en este sentido en IoT.	México realiza análisis prospectivos (LPWA); Brasil coordina las decisiones sectoriales estratégicas.	Incorporar análisis técnico periódico del espectro orientado a IoT.
Gestión de aplicaciones y servicios	No hay ninguna entidad que supervise o articule aplicaciones de IoT en los sectores productivos.	Brasil define áreas estratégicas (salud, industriales, agro, etc.); México promueve informes sectoriales.	Crear unidad técnica que articule las aplicaciones del IoT en comercio y sectores productivos.
Título habilitante	La LOT regula títulos habilitantes de telecomunicaciones pero no diferencia el IoT como una	Brasil incorpora IoT en su proceso de planificación estratégica; México lo aborda en el marco regulatorio existente.	Determinar si la regulación actual de los títulos habilitantes debería incorporar

	categorización específica.	disposiciones específicas para IoT o si se requiere un esquema regulatorio diferente.

Nota. *Elaboración propia a partir de la Agenda de Transformación Digital del Ecuador 2022–2025, el Plan Nacional de Frecuencias de ARCOTEL y los marcos institucionales de México y Brasil.*

Desde el punto de vista institucional, estos requerimientos muestran que el principal reto para Ecuador no es tanto crear nuevas entidades, sino lograr que las que ya existen trabajen de forma articulada. Fortalecer la coordinación, definir roles con claridad y desarrollar capacidades técnicas permitiría avanzar hacia una gobernanza del IoT más coherente y sostenible, sobre todo en aplicaciones orientadas al comercio local.

3.4.3. *Requerimientos técnicos*

Desde lo técnico, el IoT en Ecuador también enfrenta limitaciones. Abarcan la infraestructura de conectividad, la regulación del espectro, la interoperabilidad de los sistemas y la seguridad de los dispositivos. El país cuenta con una base tecnológica que permite el uso de soluciones IoT de corto alcance, y carece de una planificación específica para tecnologías como LPWAN o 5G; carece de lineamientos técnicos diferenciados, lo que condiciona la adopción a gran escala (Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), 2021; Meza et al., 2022).

La Tabla 12 recoge los principales requerimientos técnicos que Ecuador debería considerar para facilitar el despliegue del IoT en el comercio local. Se elaboró a partir del análisis comparativo con México y Brasil, y del marco técnico nacional vigente.

Tabla 12.

Requerimientos técnicos para la implementación del IoT en el comercio local ecuatoriano

Elemento técnico	Situación actual en Ecuador	Referencia comparada (México / Brasil)	Requerimiento técnico identificado
Infraestructura de conectividad	Brechas de conectividad entre zonas urbanas y rurales y capacidad limitada para IoT masivo.	México y Brasil generen redes móviles de última generación y planifican IoT.	Reforzar la infraestructura de conectividad orientada a la IoT.
Gestión del espectro	Uso predominante de bandas libres (2.4 y 5 GHz), sin asignaciones específicas para IoT.	México introduce nuevas bandas y Brasil, determina crear la gestión del espectro en la estrategia nacional de IoT.	Planificar el espectro en función de las tecnologías IoT de corto alcance y largo alcance.
Homologación técnica	Procesos generales sin diferenciación para dispositivos IoT de bajo consumo.	México contempla equipos de corto alcance mediante criterios específicos y Brasil contempla equipos de corto alcance mediante criterios específicos.	Adecuar criterios técnicos de homologación de dispositivos IoT.
Interoperabilidad técnica	Existen normas generales, sin lineamientos técnicos específicos para IoT.	México y Brasil establecen plataformas interoperables y estandarizadas.	Generar criterios técnicos que aseguren la interoperabilidad

			entre los sistemas IoT.
Seguridad técnica de dispositivos	Requisitos generales de seguridad, sin estándares técnicos específicos para IoT.	Brasil impone requisitos técnicos obligatorios; México expide guías técnicas.	Incorporar requisitos técnicos mínimos de seguridad de los dispositivos IoT.
Tecnologías aplicables	No existe reconocimiento normativo específico de tecnologías IoT como LPWAN, NB-IoT, LoRa, Sigfox o 5G.	México estudia la evolución LPWA y Brasil introduce tecnologías IoT en sectores estratégicos.	Reconocer y definir tecnológicamente las tecnologías IoT habilitadas para el comercio local, asegurando la neutralidad tecnológica y la compatibilidad normativa.

Nota: Elaboración propia a partir del Plan Nacional de Frecuencias de ARCOTEL, la Agenda de Transformación Digital del Ecuador 2022-2025 y las experiencias técnicas en México y Brasil.

Desde la parte técnica, estos requerimientos muestran que Ecuador tiene las condiciones mínimas para usar IoT, pero necesita mejorar su planificación tecnológica para que los sistemas puedan crecer, funcionar entre sí y ser seguros. Atender estos aspectos permitiría que el IoT se integrara de forma gradual y sostenible en el comercio local, reduciría las brechas tecnológicas y facilitaría la adopción de soluciones innovadoras.

3.4.4. *Integración general de requerimientos para la regulación del IoT en Ecuador*

A partir de los requisitos legales, institucionales y técnicos que se han recogido, se construye una visión general que recoge algunos de los aspectos clave que Ecuador podría llegar a considerar si desarrolla regulaciones específicas para el IoT. En otras palabras, la visión general no se presenta como una propuesta regulatoria, sino como un marco de análisis que recoge los elementos básicos en función de los cuales se pueden elaborar las orientaciones futuras.

En la Tabla 13 se presenta un resumen detallado de los requisitos identificados para la regulación del IoT en Ecuador, agrupados en aspectos legales, institucionales y técnicos.

Tabla 13.

Integración de requerimientos para la regulación del IoT en el comercio local ecuatoriano

Dimensión	Requerimientos identificados	Finalidad normativa
Legal	• Definición legal del Internet de las Cosas (IoT). • Protección de los datos generados por dispositivos conectados. • Regulación de las bandas de frecuencia • Responsabilidades de los actores involucrados. • Aplicaciones y servicios de IoT. • Tecnologías de habilitadas. • Protección del consumidor digital.	Garantizar la seguridad jurídica y establecer normas claras y precisas para el uso de IoT en el comercio local.
Institucional	• Coordinación interinstitucional • Fortalecimiento del papel de ARCOTEL Y MINTEL.	Mejorar la gobernanza y la coordinación entre las instituciones

	• Análisis periódico del espectro. • Gestión de aplicaciones y servicios. • Evaluación del régimen de títulos habilitantes. • Desarrollo de capacidades técnicas.	responsables de la implementación del IoT.
Técnica	• Modernización de infraestructura digital • Planificación del espectro. • Licenciamiento diferenciado. • Interoperabilidad. • Seguridad de los dispositivos. • Tecnologías aplicables como LPWAN, NB-IoT, LoRaWAN, Sigfox y 5G.	Garantizar la conectividad, la interoperabilidad, la escalabilidad y la seguridad para el despliegue de IoT.

Nota: Elaboración propia en base a los requerimientos legales, institucionales y técnicos especificados en las Tablas Tabla 10Tabla 11Tabla 12 *, basada en un análisis del marco jurídico ecuatoriano y la experiencia comparativa de México y Brasil.*

3.4.5. *Síntesis concluyente de los parámetros identificados*

Con base en los parámetros identificados en los ámbitos legal, institucional y técnico, se definieron criterios clave para orientar una futura regulación del IoT en Ecuador. Estos criterios permiten organizar los resultados del análisis y señalar aquellos aspectos que necesitan atención prioritaria para que el IoT se implemente de forma segura y ordenada en el comercio local.

En lo que corresponde al ámbito legal, se prioriza el reconocimiento jurídico del IoT. Eso implica definir responsabilidades claras para fabricantes, operadores, proveedores y usuarios, y establecer reglas sobre cómo se procesan los datos que generan los dispositivos conectados. Con

ello, se pretende reducir vacíos normativos y dar más seguridad jurídica a quienes participan en la utilización de este tipo de tecnologías.

Desde el punto de vista institucional, se destaca la importancia de poder articular a las personas que se encargan de manera principal de MINTEL y ARCOTEL . La regulación del IoT no puede depender de una labor individual. Es necesario que exista una buena coordinación entre las instituciones que manejan el espectro, homologación, políticas digitales, protección de datos, supervisión técnica.

Desde el componente técnico, se recuperan criterios como la planificación del espectro, la certificación diferenciada de dispositivos, la interoperabilidad, la ciberseguridad, el reconocimiento de tecnologías como LPWAN, NB-IoT, LoRa, Sigfox o 5G. Estos aspectos son importantes para que las soluciones IoT puedan operar de manera correcta, segura y crecer sin inconvenientes.

Entonces, esos criterios que fueron priorizados funcionan como un referente, sirven para ir desde lo que se detectó como problema hasta llegar a propuestas más concretas de regulación que hagan que un determinado proceso tenga sentido.

3.4.6. *Valoración comparativa del nivel de desarrollo regulatorio del IoT en Ecuador, México y Brasil.*

A partir de la identificación de los requerimientos legales, institucionales y técnicos, se establecieron los elementos clave para regular el IoT en el comercio local ecuatoriano. El análisis realizado no es suficiente, ya que nos hace falta comparar cómo están Ecuador, México y Brasil en cada uno de esos aspectos.

Por eso se realizará el cuadro de valoración de los requerimientos identificados anteriormente, donde cada uno se evaluará en una escala de cumplimiento con una nota del 1 al

10. Esta valoración mostrará de forma objetiva las fortalezas y debilidades de cada uno de los países. La información ayudará a la propuesta normativa del siguiente capítulo. Identificando qué aspectos necesita reforzar en Ecuador y cuáles podría ir tomando como referencia lo han hecho México y Brasil, pero adaptado a las necesidades del Ecuador.

En la Tabla 14 se observará la escala de valoración que tomaremos en cuenta en la Tabla 15 que es de los requerimientos identificados.

Tabla 14.

Escala de valoración utilizada para el análisis comparativo

Valor	Nivel de cumplimiento	Descripción
1-2	Muy bajo	No hay cláusulas precisas para el IoT o se encuentran referencias generales vacías.
3-4	Bajo	Existen iniciativas aisladas o la regulación parcial sin una visión específica para el IoT.
5-6	Medio	Se identifican cláusulas aplicables aunque aún tienen limitaciones para el desarrollo completo del IoT.
7-8	Alto	Hay regulación desarrollada que integra casi la mayoría de los elementos requeridos para el IoT.
9-10	Muy alto	Existen marco regulatorio consolidado, con estrategias, regulación específica y mecanismos institucionales claramente trazados.

Nota. Elaboración propia con base en los criterios de análisis definidos durante el trabajo.

Para completar el análisis cualitativo, se realizó una comparación del nivel regulatorio del IoT en los dos países que se va a sustentar. Se tomaron en cuenta los aspectos legales, técnicos e

institucionales que influyen en el comercio local. La valoración refleja lo que se observó en cada país, con base en la evidencia recopilada.

La Tabla 15 mostrará la valoración dada. Cada componente se evaluó con la escala de la Tabla 14. Así se observará lo bueno y lo malo de cada país.

Tabla 15.

Valoración comparativa de los requerimientos regulatorios para el IoT en México y Brasil.

Componente regulatorio	**Requerimiento regulatorio**	**Elemento normativo**	**Criterio de valoración**	**México**	**Brasil**
DISPOSICIONES GENERALES	Objeto, ámbito de aplicación y finalidad.	Objeto.	Existencia de un marco específico que delimite la regulación de IoT.	7	9
		Ámbito de aplicación.	Identificación de actores, servicios y actividades vinculados al IoT.	7	9
		Finalidad.	Orientación normativa hacia la innovación, seguridad e interoperabilidad.	8	9
	Definiciones básicas.	Definiciones básicas	Reconocimiento técnico-jurídico de conceptos IoT.	7	9
	Principios y disposiciones generales de aplicación.	Principios rectores.	Incorporación de principios de innovación, seguridad e interoperabilidad.	8	10

	Bandas de operación.	Bandas de operación para IoT.	Planificación de bandas destinadas o priorizadas para IoT.	9	8
Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT.	Uso de bandas libres y licenciadas.	Uso de bandas libres.	Existencia de condiciones técnicas para el uso libre de IoT.	9	8
		Uso de bandas licenciadas.	Regulación de autorizaciones para servicios IoT de mayor cobertura o de mayor criticidad.	8	8
	Tecnologías habilitadas y planificación del espectro.	Tecnologías habilitadas.	Reconocimiento de tecnologías LPWAN, NB-IoT, LTE-M, LoRaWAN, ZigBee, Sigfox o 5G.	9	8
		Planificación espectral.	Evaluación periódica del espectro para nuevas demandas IoT.	9	9
Homologación y certificación de dispositivos IoT.	Homologación de dispositivos.	Homologación obligatoria.	Existencia de procedimientos específicos para dispositivos IoT.	8	9
	Certificación técnica.	Requisitos técnicos mínimos.	Definición de requisitos técnicos diferenciados para equipos IoT.	8	9
		Certificación de conformidad.	Verificación de conformidad técnica antes de comercialización o uso.	8	9
	Reconocimiento de certificaciones internacionales.	Reconocimiento de certificaciones.	Aceptación de certificaciones internacionales o equivalentes.	8	8

		Registro de dispositivos homologados.	Existencia de registro público o control de equipos IoT homologados.	7	9
	Interoperabilidad de sistemas.	Interoperabilidad.	Capacidad normativa para integrar dispositivos, plataformas y servicios IoT.	8	9
Interoperabilidad y estándares técnicos.	Estándares técnicos.	Estándares abiertos.	Estándares abiertos y uso de distintas tecnologías.	8	9
	Compatibilidad entre plataformas y dispositivos.	Compatibilidad de plataformas.	Compatibilidad entre plataformas y dispositivos de distintos proveedores.	7	9
		Integración tecnológica.	Integración de IoT con sistemas públicos, privados y comerciales.	8	9
	Seguridad de dispositivos IoT.	Seguridad desde el diseño.	Incorporación de seguridad desde diseño, desarrollo e implementación.	8	9
	Gestión de vulnerabilidades.	Gestión de vulnerabilidades.	Procedimientos para identificar, corregir y reducir vulnerabilidades en IoT.	8	9
Ciberseguridad y protección de datos.		Actualización de firmware.	Exigencia de actualizaciones seguras.	8	10
	Protección de datos personales.	Protección de datos personales.	Regulación del tratamiento de datos generados por dispositivos IoT.	8	9
		Gestión de riesgos.	Evaluación y tratamiento de riesgos asociados a datos, redes y dispositivos.	8	9
Aplicaciones sectoriales del IoT.	Aplicaciones en el comercio local.	Aplicaciones comerciales.	Normativa del IoT para inventarios activos, atención y decisiones comerciales.	7	9

	Logística y seguimiento de productos.	Seguimiento inteligente de productos.	Uso de IoT para el control de productos, monitoreo y logística comercial.	7	9
		Automatización de procesos.	Aplicación de IoT para automatizar procesos y optimizar la gestión comercial.	7	9
	Innovación y transformación digital.	Transformación digital basada en IoT.	Existencia de lineamientos para impulsar el uso del IoT en distintos sectores.	8	9
	Competencias institucionales.	Competencias de MINTEL.	Entidad responsable de las políticas digitales y de IoT.	7	9
		Competencias de ARCOTEL.	Entidad reguladora del espectro, la homologación y el control técnico.	8	9
		Participación de las entidades competentes.	Participación de entidades vinculadas a datos, producción, comercio e innovación.	7	9
Gobernanza y coordinación institucional.	Coordinación interinstitucional.	Coordinación institucional.	Mecanismo de coordinación interinstitucional para el IoT.	7	10
	Supervisión y seguimiento.	Supervisión y control.	Supervisión técnica y regulatoria del ecosistema IoT.	8	9
		Evaluación y mejora regulatoria.	Evaluación periódica y mejora de lineamientos regulatorios sobre IoT.	8	9
Implementación, seguimiento y	Implementación progresiva.	Implementación progresiva.	Aplicación progresiva de la regulación según las capacidades del país.	7	9

disposiciones finales.		Proyectos piloto.	Uso de pruebas pilotos para validar soluciones IoT antes de regularlas.	7	9
	Seguimiento y actualización normativa.	Evaluación periódica.	Seguimiento de resultados, adopción del IoT y cumplimiento de la regulación.	8	9
		Actualización normativa.	Actualización de la normativa ante cambios tecnológicos, nuevos riesgos y nuevas aplicaciones.	8	9
	Disposiciones finales.	Disposiciones finales.	Utilidad del marco para una futura regulación del IoT con apoyo del Estado, el sector productivo y organismos técnicos.	7	9

Nota. Elaboración propia con base en los requerimientos legales, técnicos e institucionales identificados en el análisis en México y Brasil.

Con los resultados de la Tabla 15, se identificó el país que tiene mayor desarrollo regulatorio en cada componente analizado. Así se reconoce qué experiencia internacional aporta mejores prácticas como referencia para armar los lineamientos regulatorios en Ecuador.

En la Tabla 16 se mostrará el referente predominante en cada uno de los componentes regulatorios.

Tabla 16.

Referente predominante por componente regulatorio.

Fundamento	**Referente predominante**	**Justificación**
Disposiciones generales.	Brasil	Su estrategia nacional reconoce el IoT con principios, objetivos y áreas definidas.

Gestión del espectro y tecnologías habilitadas.	México	Ha avanzado más en el análisis del espectro, bandas libres y tecnologías para IoT.
Homologación y certificación.	México/Brasil	México da flexibilidad y acepta certificaciones; Brasil ejerce gran control sobre equipos.
Interoperabilidad y estándares técnicos.	México/Brasil	México establece lineamientos técnicos y flexibilidad del tipo tecnológico; mientras que Brasil establece la interoperabilidad como prioridad, junto a las fases de planificación.
Ciberseguridad y protección de datos.	Brasil	Ha avanzado más, en la exigencia de seguridad en dispositivos, gestión de vulnerabilidades y protección de datos.
Aplicaciones sectoriales del IoT.	Brasil	Se delimitan sectores estratégicos de IoT, y ese enfoque se lo puede trasladar al comercio local ecuatoriano.
Gobernanza y coordinación institucional.	Brasil	Posee mecanismos institucionales más claros para articular políticas y organismos dedicados al IoT.
Implementación, seguimiento y disposiciones finales.	México/Brasil	México da mecanismos de análisis, consulta y actualización; Brasil, una implementación gradual junto a su estrategia nacional.

Nota. Elaboración propia con base a los resultados obtenidos de la Tabla 15 y del análisis de buenas prácticas regulatorias de México y Brasil.

Para completar la interpretación de la Tabla 15, se sacaron promedios generales de Ecuador, México y Brasil. En la Tabla 17 se ve de forma resumida el nivel regulatorio de cada país en los componentes analizados.

Tabla 17.

Promedio general de la valoración comparativa por país.

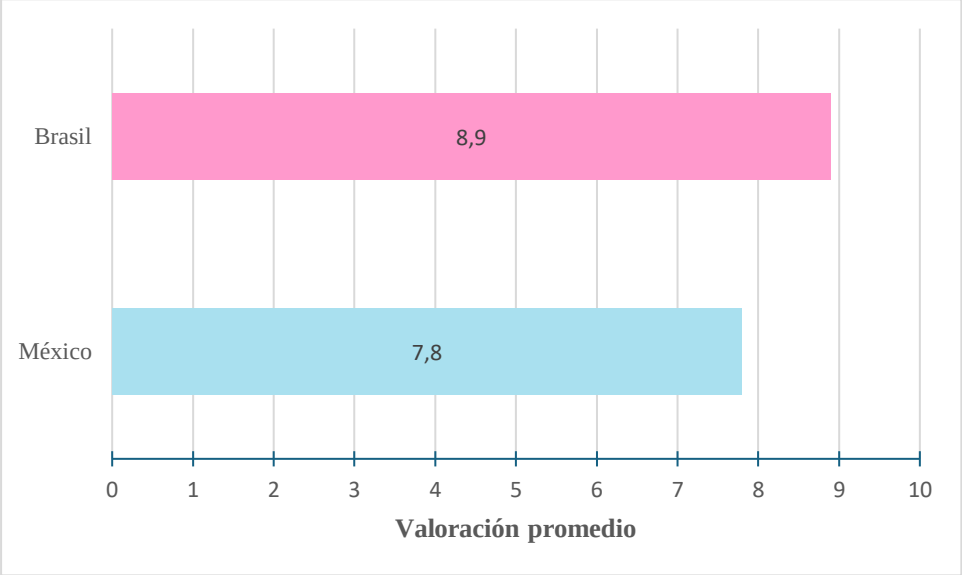
País	**Promedio**
México	7.8
Brasil	8.9

Nota. Elaboración propia con base en los promedios obtenidos de la valoración comparativa.

Con los datos de la Tabla 17. se realizó la Figura 6 como representación gráfica de la diferencia de los promedios de México y Brasil.

Figura 6.

Promedio de valoración comparativa



Nota. Elaboración propia con base en los promedios obtenidos.

La Figura 6 pone de manifiesto que es Brasil el país que logra el promedio más elevado (8.9), es decir, por debajo de ese promedio, se encuentra México (7.8), esto posiciona a Brasil como el referente principal de la propuesta para los lineamientos, sobre todo en gobernanza, ciberseguridad, homologación e implementación progresiva, mientras que México es un referente complementario en cuanto a espectros, bandas libres y tecnologías habilitadas y, por tanto, la propuesta para Ecuador ha de aunar las prácticas de ambos países; la estructura se la toma de Brasil y la referencia técnica de México en el espectro y la conectividad.

Capítulo IV: Resultados

En este capítulo se presentan los principales resultados del análisis comparativo y metodológico que se ha realizado en los capítulos anteriores.

Aquí, los requisitos legales, institucionales y técnicos que se han identificado para Ecuador se agrupan de forma ordenada en una propuesta de marco regulatorio. Facilitando así la

incorporación del Internet de las Cosas (IoT) al comercio local. De esta manera, los hallazgos del diagnóstico se convierten en una estructura normativa inicial, que puede servir de guía para las futuras regulaciones que se desarrollen en el país.

Esta propuesta toma como referencia las buenas prácticas observadas en México y Brasil, pero como siempre considerando la realidad actual de Ecuador en temas como telecomunicaciones, protección de datos, homologación de dispositivos, interoperabilidad, ciberseguridad y gobernanza institucional.

4.1 Fundamentos para el desarrollo de la propuesta del marco regulatorio

Los aspectos analizados en los capítulos anteriores constituyen la base del marco regulatorio propuesto. Un análisis comparativo permitió identificar que México y Brasil han integrado el Internet de las Cosas (IoT) en sus ordenamientos jurídicos mediante regulaciones, directrices técnicas y estrategias sectoriales. Por otro lado, la evaluación realizada de Ecuador, reveló que, a pesar de la existencia de regulaciones generales sobre telecomunicaciones, protección de datos personales y transformación digital, el país aún carece de regulaciones específicas que rija el uso de IoT en el comercio local (Asamblea Nacional del Ecuador, 2015, 2021; Meza et al., 2022).

La Tabla 18 presenta los fundamentos del marco regulatorio propuesto para el IoT en Ecuador considerando el marco legal vigente, la experiencia internacional relevante y los requisitos previamente identificados.

Tabla 18.

Fundamentos para el desarrollo de la propuesta del marco regulatorio

Fundamento	Descripción	Aplicación en la propuesta

Marco Regulatorio Nacional	Toma en cuenta las leyes ecuatorianas vinculadas a las telecomunicaciones, a la protección de datos de carácter personal, a la certificación de equipos y los procesos de transformación digital.	Asegura que la propuesta regulatoria que aquí se expone no paliará un vacío regulatorio a la vez que complementará el ordenamiento jurídico vigente.
Comparativo de mejores prácticas	Las experiencias de México y Brasil en la materia del espectro radioeléctrico, la certificación de equipos, la interoperabilidad de sistemas y la ciberseguridad constituyen el referente.	Permite posteriormente complementar los criterios regulatorios regionales adaptándolos a las circunstancias de Ecuador.
Requerimientos identificados	Comprenden los requerimientos legales, institucionales y técnicos dados en el Capítulo III.	Facilita la organización de la propuesta de regulación en títulos, capítulos y artículos normativos.
Desarrollo progresivo de la regulación	La ampliación de la propuesta debe ser considerada de forma gradual, en función de las capacidades institucionales y técnicas del país.	Facilita la presentación de una propuesta de regulación viable y a la vez acorde con las características de la realidad de Ecuador.

Nota. Elaboración propia con relación a aquellos requerimientos identificados en el análisis realizado en los capítulos anteriores.

Partiendo de los propios principios, podemos desarrollar del marco regulatorio propuesto de manera ordenada de ahí su coherencia con el análisis realizado anteriormente. Y podemos

hacerlo porque su estructura se plantea conforme a una lógica similar a la de los cuerpos legales nacionales, por medio de títulos, capítulos y artículos normativos. Facilitando así el desarrollo de esta propuesta.

4.2 Estructura general del marco normativo propuesto

Partiendo de los fundamentos establecidos en la sección anterior, se propone un marco general para la organización del marco regulatorio del Internet de las Cosas (IoT) en Ecuador. Este marco responde directamente a los requisitos identificados en el Capítulo III. Estos fundamentos incluyen el espectro radioeléctrico, la certificación de equipos, la interoperabilidad de sistemas, la ciberseguridad, las aplicaciones comerciales, la gobernanza y los mecanismos de implementación por fases. El objetivo de esta integración es estructurar el contenido que podría formar parte de la propuesta regulatoria que se está desarrollando.

La Tabla 19 presenta la estructura general del marco regulatorio propuesto para el IoT en el comercio local en Ecuador.

Tabla 19.

Estructura general del marco normativo para IoT en Ecuador.

Título	Denominación del título	Capítulos propuestos	Artículos normativos
Título I	Disposiciones generales.	Cap. I: Objeto, ámbito de aplicación y finalidad. Cap. II: Definiciones básicas. Cap. III: Principios y disposiciones generales de aplicación.	Art. 1: Objeto. Art. 2: Ámbito de aplicación. Art. 3: Finalidad. Art. 4: Definiciones básicas.

			Art. 5: Principios rectores.
			Art. 6: Bandas de operación para IoT.
Título II	Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT.	Cap. I: Bandas de operación Cap. II: Uso de bandas libres y licenciadas. Cap. III: Tecnologías habilitadas y planificación del espectro.	Art. 7: Uso de bandas libres. Art. 8: Uso de bandas licenciadas. Art. 9: Tecnologías habilitadas. Art. 10: Planificación espectral.
			Art. 11: Homologación obligatoria.
			Art. 12: Requisitos técnicos mínimos.
Título III	Homologación y certificación de dispositivos IoT.	Cap. I: Homologación de dispositivos. Cap. II: Certificación técnica. Cap. III: Reconocimiento de certificaciones internacionales.	Art. 13: Certificación de conformidad. Art. 14: Reconocimiento de certificaciones. Art. 15: Registro de dispositivos homologados.
Título IV	Interoperabilidad y estándares técnicos.	Cap. I: Interoperabilidad de sistemas. Cap. II: Estándares técnicos.	Art. 16: Interoperabilidad. Art. 17: Estándares abiertos.

		Cap. III: Compatibilidad entre plataformas y dispositivos.	Art. 18: Compatibilidad de plataformas. Art. 19: Integración tecnológica. Art. 20: Seguridad desde el diseño.
Título V	Ciberseguridad y protección de datos.	Cap. I: Seguridad de dispositivos IoT. Cap. II: Gestión de vulnerabilidades. Cap. III: Protección de datos personales.	Art. 21: Gestión de vulnerabilidades. Art. 22: Actualización de firmware. Art. 23: Protección de datos personales. Art. 24: Gestión de riesgos.
Título VI	Aplicaciones sectoriales del IoT.	Cap. I: Aplicaciones en comercio local. Cap. II: Logística y seguimiento de productos. Cap. III: Innovación y transformación digital.	Art. 25: Aplicaciones comerciales. Art. 26: Seguimiento inteligente de productos. Art. 27: Automatización de procesos. Art. 28: Transformación digital basada en IoT.
Título VII	Gobernanza y coordinación institucional,	Cap. I: Competencias institucionales.	Art. 29: Competencias de MINTEL.

		Cap. II: Coordinación interinstitucional. Cap. III: Supervisión y seguimiento.	Art. 30: Competencias de ARCOTEL. Art. 31: Participación de las entidades competentes. Art. 32: Coordinación institucional. Art. 33: Supervisión y control. Art. 34: Evaluación y mejora regulatoria.
Título VIII	Implementación, seguimiento y disposiciones finales.	Cap. I: Implementación progresiva. Cap. II: Seguimiento y actualización normativa. Cap. III: Disposiciones finales.	Art. 35: Implementación progresiva. Art. 36: Proyectos piloto. Art. 37: Evaluación periódica. Art. 38: Actualización normativa. Art. 39: Disposiciones finales.

Nota. Elaboración propia con base en los requerimientos identificados en el Capítulo III.

Este marco propuesto sistematiza los requerimientos previamente analizados, integrándolos en un marco regulatorio caracterizado por una lógica interna y un carácter progresivo. Cada sección de este marco se dedica a un elemento clave de la regulación del IoT en Ecuador, desde disposiciones generales hasta mecanismos de implementación en fases. Esta

configuración facilita el desarrollo posterior de contenido más específico dentro del marco regulatorio presentado.

4.3 Desarrollo preliminar de los títulos propuestos

Una vez que fue definida la estructura general del marco regulatorio, en esta sección se desarrolla, como paso preliminar, el contenido correspondiente a cada una de las secciones propuestas. El objetivo no es redactar un reglamento completo, sino definir el alcance de cada sección, los capítulos que incluirá y la función de cada uno de los artículos dentro del futuro marco regulatorio para el Internet de las Cosas en Ecuador. Esto establece una base conceptual, sin la perspectiva de una versión final.

4.3.1. *Título I: Disposiciones generales*

Establece los fundamentos conceptuales y legales del marco regulatorio propuesto. Esta sección define el objetivo de la regulación, su ámbito de aplicación subjetivo y objetivo sobre el cual esta se aplicaría, la finalidad última de la norma, así como los conceptos principales que se vinculan de manera directa con el Internet de las Cosas. También incluye un conjunto de criterios generales, entre los que se encuentran la seguridad, la interoperabilidad, el fomento de la innovación, la privacidad y el uso flexible de tecnologías.

La Tabla 20 presenta el desarrollo preliminar del Título I, que establece las disposiciones generales del marco normativo que ha sido propuesto.

Tabla 20.

Desarrollo del Título I: Disposiciones generales.

Capítulo	Artículos	Finalidad

Capítulo I: Objeto, ámbito de aplicación y finalidad.	Art. 1: Objeto. Art. 2: Ámbito de aplicación. Art. 3: Finalidad.	Definir el alcance de la normativa y aclarar que su aplicación se limita exclusivamente al comercio local.
Capítulo II: Definiciones básicas.	Art. 4: Definiciones básicas.	Fijar conceptos mínimos para prevenir ambigüedades en el marco regulatorio.
Capítulo III: Principios y disposiciones generales de aplicación.	Art. 5: Principios rectores.	Determinar la aplicación del marco normativo conforme a los criterios de seguridad, interoperabilidad e innovación.

Nota. Elaboración propia con base en la estructura general propuesta en la Tabla 19.

El Título I se considera fundamental porque garantiza una definición clara del marco regulatorio desde el principio. Al definir el alcance, los conceptos y los principios que regirán su uso, se evita una interpretación limitada del Internet de las Cosas (IoT) que se consideraría únicamente como una tecnología aislada. En cambio, esta definición reconoce el IoT como un ecosistema complejo compuesto por dispositivos, plataformas, servicios, datos y participantes que interactúan con el comercio local.

4.3.2. *Título II: Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT*

El Título II establece disposiciones relativas al uso del espectro radioeléctrico y las tecnologías que apoyan la implementación de soluciones de IoT en Ecuador. Su objetivo principal es garantizar el funcionamiento de los dispositivos y redes IoT dentro de las bandas de frecuencia previamente autorizadas y, además, de acuerdo con criterios orientados a un uso eficiente del

espectro. Asimismo, fomenta la adopción de tecnologías que faciliten la conectividad de objetos y sistemas en el sector comercial local.

La Tabla 21 presenta el progreso en la implementación del Título II, que hace referencia a la gestión del espectro radioeléctrico y las tecnologías relacionadas con IoT.

Tabla 21.

Desarrollo del Título II: Gestión del espectro radioeléctrico y tecnologías habilitadas para el IoT.

Capítulo	**Artículos**	**Finalidad**
Capítulo I: Bandas de operación.	Art. 6: Bandas de operación para IoT.	Determinar las bandas de frecuencia disponibles para aplicaciones de IoT en el país.
Capítulo II: Uso de bandas libres y licenciadas.	Art. 7: Uso de bandas libres. Art. 8: Uso de bandas licenciadas.	Determinar las condiciones de uso del espectro según el tipo de servicio y la tecnología utilizada.
Capítulo III: Tecnologías habilitadas y planificación del espectro.	Art. 9: Tecnologías habilitadas. Art. 10: Planificación espectral.	Establecer los distintos tipos de tecnologías de IoT que hayan sido valoradas y los criterios aplicables para una planificación y gestión correcta del espectro.

Nota. Elaboración propia a partir de la estructura general que ha sido propuesta en la Tabla 19.

El objetivo de Título II es concretar el marco regulador para la ejecución de tecnologías de IoT en el país, marco regulador que engloba tanto las bandas de frecuencia sin licencia como las previamente autorizadas. De igual manera, aborda la necesidad de reconocer tecnologías de amplia

adopción internacional como LoRaWAN, NB-Iot, LTE-M y Sigfox, así como futuros desarrollos basados en la tecnología 5G. Contribuyendo así a la creación de un entorno regulatorio adecuado para la innovación y el desarrollo del ecosistema digital.

4.3.3. *Título III: Homologación y certificación de dispositivos IoT.*

Se definen las directrices para los procesos de aprobación y certificación de dispositivos conectados. Se considera que resulta necesario el presente marco regulatorio ya que, a diferencia de los equipos de telecomunicaciones típicos, los dispositivos conectados no poseen la misma idiosincrasia, ya que suelen operar a una gran escala, tienen un bajo consumo de energía y utilizan distintas tecnologías de comunicación, lo que motiva la propuesta de un modelo de aprobación diferenciada tanto para mantener el control técnico sobre los equipos como para facilitar su integración en el mercado ecuatoriano.

La Tabla 22 presenta el desarrollo preliminar del Título III, el cual se refiere a la aprobación y certificación de equipos IoT.

Tabla 22.

Desarrollo del Título III: Homologación y certificación de dispositivos IoT.

Capítulo	**Artículos**	**Finalidad**
Capítulo I: Homologación de dispositivos.	Art. 11: Homologación obligatoria.	Establecer requisitos técnicos mínimos para dispositivos conectados usados o vendidos en el país.
Capítulo II: Certificación técnica.	Art. 12: Requisitos técnicos mínimos. Art. 13: Certificación de conformidad.	Definir criterios técnicos clave para compatibilidad, seguridad operativa y control de interferencias.

Capítulo III: Reconocimiento de certificaciones internacionales.	Art. 14: Reconocimiento de certificaciones. Art. 15: Registro de dispositivos homologados.	Facilitar verificación de equipos mediante certificados equivalentes y mantener un registro actualizado de dispositivos IoT autorizados.

Nota. Elaboración propia con base en la estructura general propuesta en la Tabla 19.

Mediante el Título III, sería posible adaptar los procesos de aprobación a las características específicas del IoT, evitando así que todos los dispositivos sean tratados bajo un marco genérico que no tenga en cuenta su nivel de implementación, diversidad tecnológica ni uso comercial. Además, el reconocimiento de certificados internacionales puede contribuir a reducir el tiempo de evaluación, siempre que se mantengan los controles adecuados en áreas como la compatibilidad técnica, la seguridad operativa y el uso correcto del espectro radioeléctrico.

4.3.4. *Título IV: Interoperabilidad y estándares técnicos.*

Establece directrices para garantizar que los dispositivos, plataformas y sistemas IoT cuenten con las capacidades necesarias para un intercambio de información eficiente, seguro y estandarizado. La interoperabilidad se considera un elemento fundamental del desarrollo del IoT, ya que las soluciones implementadas suelen integrar equipos de diferentes fabricantes, múltiples tecnologías de comunicación y diversas plataformas de gestión. Por esta razón, el marco normativo planteado incluirá también determinadas previsiones tendentes a favorecer la utilización de los estándares abiertos como la consideración de mecanismos que aseguren la interoperabilidad tecnológica.

La Tabla 23 muestra el desarrollo inicial del Título IV, que, como hemos mencionado antes, se refiere a la interoperabilidad y los estándares técnicos relativos a IoT.

Tabla 23.

Desarrollo del Título IV: Interoperabilidad y estándares técnicos.

Capítulo	Artículos	Finalidad
Capítulo I: Interoperabilidad de sistemas.	Art. 16: Interoperabilidad.	Garantizar un intercambio de información eficiente y seguro entre sistemas y dispositivos IoT.
Capítulo II: Estándares técnicos.	Art. 17: Estándares abiertos.	Fomentar la implementación de estándares reconocidos internacionalmente para la integración tecnológica.
Capítulo III: Compatibilidad entre plataformas y dispositivos.	Art. 18: Compatibilidad de plataformas. Art. 19: Integración tecnológica.	Garantizar la interoperabilidad entre dispositivos, aplicaciones y plataformas de diferentes proveedores.

Nota. Elaboración propia con base en la estructura general propuesta en la Tabla 19.

En este Título IV, la integración de mecanismos de interacción busca prevenir dos obstáculos que dificultan el desarrollo del IoT: la dispersión tecnológica y la dependencia de soluciones propietarias. Además, esta integración promueve la escalabilidad de los proyectos IoT y facilita la incorporación de nuevas aplicaciones al entorno comercial local. De esta manera, permite que sistemas de distintos tipos operen de forma coordinada e interoperable dentro de un mismo entorno tecnológico.

4.3.5. *Título V: Ciberseguridad y protección de datos.*

Establece directrices para tres áreas clave: seguridad de dispositivos conectados, gestión de vulnerabilidades y protección de datos personales. Esta parte se considera fundamental, dado

que los sistemas IoT generan, transmiten y almacenan información de forma continua. Este flujo de información puede incluir datos sobre los usuarios, sus hábitos de consumo, geolocalización, inventario, transacciones de pago y monitoreo de productos. Por lo tanto, es esencial que la normativa establezca requisitos mínimos de seguridad que, por un lado, mitiguen la confianza en el uso de soluciones IoT en el sector minorista local.

La Tabla 24 presenta el desarrollo preliminar del Título V, que aborda cuestiones de ciberseguridad y protección de datos dentro del marco propuesto.

Tabla 24.

Desarrollo del Título V: Ciberseguridad y protección de datos.

Capítulo	**Artículos**	**Finalidad**
Capítulo I: Seguridad de dispositivos IoT.	Art. 20: Seguridad desde el diseño.	Integrar criterios de seguridad durante la producción, configuración e implementación de dispositivos IoT.
Capítulo II: Gestión de vulnerabilidades.	Art. 21: Gestión de vulnerabilidades. Art. 22: Actualización de firmware.	Implementar mecanismos para identificar, corregir y mitigar vulnerabilidades de seguridad en dispositivos y plataformas IoT.
Capítulo III: Protección de datos personales.	Art. 23: Protección de datos personales. Art. 24: Gestión de riesgos.	Garantizar el procesamiento de datos personales generados por IoT de acuerdo con los criterios de seguridad, proporcionalidad y prevención de riesgos.

Nota. Elaboración propia con base en la estructura general propuesta en la Tabla 19.

En esta parte del Título V, garantizará que la ciberseguridad se integre como un elemento esencial del ecosistema IoT, y no solo como una recomendación técnica. Además, la protección de la privacidad debe considerarse desde la fase de diseño de las soluciones, especialmente cuando los dispositivos recopilan información relacionada con los consumidores, las operaciones comerciales o las cadenas de suministro. El objetivo es asegurar que la implementación de IoT en el comercio local se base en tres principios fundamentales: la confianza del usuario, la prevención de riesgos y la responsabilidad de las partes interesadas.

4.3.6. *Título VI: Aplicaciones sectoriales del IoT.*

Se centra específicamente en la aplicación del IoT en la parte de comercio local. Este enfoque se basa en el principio de que la regulación no debe limitarse únicamente a aspectos técnicos o administrativos, sino que también debe crear un marco que facilite el desarrollo de soluciones tecnológicas aplicables a varios procesos de negocio. Este apartado tiene como objetivo promover el uso del IoT como herramienta para: mejorar la eficiencia operativa, optimizar la gestión de inventarios, mejorar el seguimiento de los productos y apoyar a la transformación digital de los minoristas.

La Tabla 25 forma parte del desarrollo inicial del Título VI que aborde las aplicaciones del IoT en el sector propuesto en el marco regulatorio.

Tabla 25.

Desarrollo del Título VI: Aplicaciones sectoriales del IoT.

Capítulo	Artículos	Finalidad
Capítulo I: Aplicaciones en el comercio local.	Art. 25: Aplicaciones comerciales.	Fijar criterios generales de uso del IoT en el comercio local.

Capítulo II: Logística y seguimiento de productos.	Art. 26: Seguimiento inteligente de productos. Art. 27: Automatización de procesos.	Promover el uso del IoT para mejora del seguimiento, de la gestión de inventarios, de la gestión de la logística y de la automatización de las operaciones comerciales.
Capítulo III: Innovación y transformación digital.	Art. 28: Transformación digital basada en IoT.	Promover la implantación del IoT en el marco de la innovación tecnológica y de los procesos de mejora de la competitividad.

Nota. Elaboración propia con base en la estructura general propuesta en la Tabla 19.

En esta parte del Título VI, responde a la necesidad de una regulación que vaya más allá de la simple imposición de obligaciones a los actores involucrados. Buscando promover el uso responsable de las tecnologías del Internet de las Cosas (IoT) en las actividades industriales y comerciales. En este sentido, el marco regulatorio propuesto pretende crear un entorno adecuado para la digitalización del comercio local. Esta facilitación se logrará mediante la implementación de soluciones tecnológicas que ayuden a mejorar varios aspectos, como: la calidad de los servicios prestados, la toma de decisiones basadas en información en tiempo real. De esta manera, la normativa busca simultáneamente controlar los aspectos técnicos y fomentar la innovación.

4.3.7. *Título VII: Gobernanza y coordinación institucional.*

Establece la estructura de gobernanza necesaria para la implementación y el monitoreo del marco regulatorio propuesto. El objetivo de este apartado es, precisamente, definir las funciones que les corresponde asumir a las instituciones que participan en la gobernanza del framework normativo propuesto, facilitar los mecanismos de concertación interinstitucional, establecer

sistemas de supervisión de la aplicación de las normativas y de la gobernanza de las funciones que puedan estar despachando las instituciones del gobierno, evitando la fragmentación de las funciones que puedan emerger entre las instituciones del gobierno y consolidando una gobernanza coordinada.

La Tabla 26 presenta el componente de desarrollo inicial del Título VII en donde se abordan las cuestiones de gobernanza y de la concertación interinstitucional dentro de la práctica reguladora propuesta.

Tabla 26.

Desarrollo del Título VII: Gobernanza y coordinación institucional.

Capítulo	**Artículos**	**Finalidad**
Capítulo I: Competencias institucionales.	Art. 29: Competencias de MINTEL. Art. 30: Competencias de ARCOTEL. Art. 31: Participación de las entidades competentes.	Definir las funciones y responsabilidades de las organizaciones encargadas del desarrollo de políticas, la gestión del espectro radioeléctrico y el seguimiento del cumplimiento de los requisitos reglamentarios en el IoT.
Capítulo II: Coordinación interinstitucional.	Art. 32: Coordinación institucional.	Establecer mecanismos de cooperación entre organismos gubernamentales que trabajan en los ámbitos de las telecomunicaciones, la transformación digital, la

		protección de datos, la definición de estándares técnicos y el desarrollo industrial.
Capítulo III: Supervisión y seguimiento.	Art. 33: Supervisión y control. Art. 34: Evaluación y mejora regulatoria.	Definir procedimientos para la supervisión, la evaluación y el apoyo para el cumplimiento normativo.

Nota. Elaboración propia a partir de la estructura general que propone la Tabla 19.

A través de este núcleo se busca consolidar la estructura institucional que dirige las responsabilidades de las distintas entidades inmersas en el desarrollo del IoT, evitando de esta manera la disgregación de dichas competencias y favoreciendo una ejecución coordinada de las regulaciones. Con lo cual, MINTEL será responsable del desarrollo de las políticas y de las estrategias públicas para la transformación digital y el ARCOTEL, además de sus competencias de gestión del espectro, certificación de dispositivos o vigilancia técnica de la red, además de tener las funciones que se tratan del con una buena participación de otras entidades competentes en relación a la protección de datos, la normalización técnica, el desarrollo industrial y la innovación, favorece que se genere la coordinación entre los diferentes espacios de regulación del IoT.

4.3.8. *Título VIII: Implementación, seguimiento y disposiciones finales.*

Establece las disposiciones para la implementación del marco regulatorio propuesto. Describe la aplicación progresiva de las directrices, así como los mecanismos para evaluar el desarrollo en función de la evolución de las tecnologías IoT. El objetivo es facilitar la implementación progresiva de las regulaciones y fomentar procesos de mejora continua que aborden de manera simultánea los desarrollos tecnológicos y las necesidades del comercio local en Ecuador.

La Tabla 27 presenta el desarrollo preliminar del Título VIII, que abarca la implementación, el monitoreo y las disposiciones finales del marco regulatorio propuesto.

Tabla 27.

Desarrollo del Título VIII: Implementación, seguimiento y disposiciones finales.

Capítulo	**Artículos**	**Finalidad**
Capítulo I: Implementación progresiva.	Art. 35: Implementación progresiva. Art. 36: Proyectos piloto.	Implementar por fases el marco legal y regulatorio.
Capítulo II: Seguimiento y actualización normativa.	Art. 37: Evaluación periódica. Art. 38: Actualización normativa.	Definir mecanismos para la revisión y actualización periódica de la reglamentación.
Capítulo III: Disposiciones finales.	Art. 39: Disposiciones finales.	Definir disposiciones adicionales y establecer la duración del marco regulatorio.

Nota. Elaboración propia en base a la estructura general propuesta en la Tabla 19.

En este apartado del Título VIII tiene como objetivo garantizar la implementación progresiva y la adaptación a la constante evolución del IoT. Debido a la constante evolución de las tecnologías, las regulaciones no deben ser estáticas, sino incluir mecanismos para la revisión y actualización periódica.

4.4 Propuesta de marco regulatorio para la implementación del Internet de las Cosas en el comercio local en Ecuador.

Tomando como base la estructura normativa que fue desarrollada previamente, a continuación, se presenta la propuesta regulatoria para el uso del Internet de las Cosas (IoT) en el comercio local ecuatoriano.

Esta propuesta organiza los lineamientos regulatorios de manera clara y estructurada en títulos, capítulos y artículos. En ella se incorporan los principales requerimientos que han sido identificados a lo largo de la investigación, adaptándolos cuidadosamente a las condiciones técnicas, legales e institucionales propias del contexto ecuatoriano.

Título I

DISPOSICIONES GENERALES

CAPÍTULO I

OBJETO, ÁMBITO DE APLICACIÓN Y FINALIDAD

Artículo 1.- Objeto.

El propósito del marco regulador que se establece mediante este reglamento consiste en definir el régimen jurídico, técnico e institucional aplicable a la ejecución, operación y supervisión del Internet de las Cosas (IoT) en el ámbito del comercio local (o de cercanía) ecuatoriano, y su finalidad es para garantizar que su aplicación sea segura, interoperable, eficiente y sostenible en el ámbito de dispositivos, redes, plataformas y servicios en relación con este ecosistema.

Artículo 2.- Ámbito de aplicación

Las disposiciones del presente marco regulatorio serán de obligatorio cumplimiento para las personas físicas o jurídicas, públicas o privadas, que realicen actividades que tengan que ver

con el diseño, el desarrollo, la importación, la comercialización, la implementación, la operación o la gestión de soluciones IoT en Ecuador.

Artículo 3.- Finalidad

El objetivo de este marco regulatorio es crear un entorno normativo adecuado para la integración progresiva del Internet de las Cosas en el comercio local de Ecuador. Para ello, se garantizarán los siguientes aspectos: uso eficiente del espectro radioeléctrico, interoperabilidad de dispositivos y plataformas, certificación de equipos, protección de datos personales, ciberseguridad y coordinación institucional.

CAPÍTULO II

DEFINICIONES BÁSICAS

Artículo 4.- Definiciones

Las definiciones que se recogerán en este marco regulador son las siguientes:

a) **Internet de las Cosas (IoT):** Se refiere a un ecosistema de tecnología dada por dispositivos físicos, sensores, actuadores, plataformas y redes de comunicación con el que se puede realizar la recolección, transmisión, procesamiento, e intercambio por medio de una conexión a internet para la automatización de procesos, soporte para la toma de decisiones y creación de servicios digitales.

b) **Dispositivos IoT:** Se refiere a los equipos físicos que son capaces de realizar, recopilar, procesar o transmitir información mediante redes de comunicación, que incorpora por ello sensores, actuadores o módulos de comunicación que permiten la interacción con otros dispositivos o plataformas digitales.

c) **Plataforma IoT:** Se refiere a la infraestructura, física o virtual, pensada para recibir, almacenar, procesar, gestionar y visualizar la información generada por los

dispositivos IoT, además de garantizar la interoperabilidad de las aplicaciones, los usuarios y los servicios.

d) **Sensor:** Dispositivo electrónico que detecta, mide o monitoriza variables físicas, químicas o ambientales, que luego se convierten en información utilizable por un sistema IoT.

e) **Actuador:** Dispositivo que realiza una acción física en respuesta a una instrucción generada automáticamente por una plataforma, aplicación o sistema IoT.

f) **Red IoT:** Conjunto de canales de comunicación que permite la interconexión de dispositivos IoT para el intercambio seguro de información mediante tecnología cableadas o inalámbricas.

g) **Interoperabilidad:** Capacidad de los dispositivos, plataformas, aplicaciones y sistemas para intercambiar información y utilizarla de manera con el mismo significado que la herramienta de interoperabilidad y cualquier fabricante o tecnología usada.

h) **Ciberseguridad:** Conjunto de políticas, procedimientos, controles y medidas técnicas destinados a proteger los dispositivos, redes, plataformas, datos del ecosistema IoT de amenazas, vulnerabilidades y accesos no autorizados.

i) **Datos personales:** Información que facilita la identificación de una persona, que es objeto de tratamiento por dispositivos, aplicaciones o plataformas, en el entorno del Internet de las Cosas.

j) **Comercio local:** Actividad económica vinculada a la comercialización de bienes o servicios efectuada en el Ecuador y/o dentro de Ecuador. Las actividades pueden ser realizadas por medio de objetos materiales, soluciones de plataforma digital o

con modelos híbridos del objeto de comercio (es decir, donde se integren soluciones del IoT).

CAPÍTULO III

PRINCIPIOS Y DISPOSICIONES DE APLICACIÓN

Artículo 5.- Principios rectores

La aplicación e interpretación de este marco normativo estarán sujetas a los principios siguientes:

a) Innovación tecnológica: Fomento al desarrollo, implementación y despliegue de las soluciones de IoT a la transformación digital y a mejorar la competitividad de las empresas locales.

b) Seguridad desde el diseño: Los dispositivos, las plataformas y los servicios de IoT deberán tener en cuenta los mecanismos de seguridad en cada una de las fases desde el diseño, desarrollo y despliegue para reducir las vulnerabilidades.

c) Interoperabilidad: Los sistemas, las plataformas y los dispositivos de IoT facilitarán el intercambio de información a partir de la utilización de estándares y mecanismos abiertos garantizando la interoperabilidad entre diferentes tecnologías y fabricantes.

d) Protección de datos personales: Las operaciones de la información que genere la IoT deberán ser conformadas por parte de los titulares de los datos en cuanto a la confidencialidad, la integridad y la disponibilidad de la misma, de acuerdo con la normativa que sea aplicable.

e) Uso eficiente del espectro radioeléctrico: Las bandas del espectro radioeléctrico asignadas al IoT deberán ser usadas de forma eficiente, evitando interferencias

dañinas, y se deberá considerar, al mismo tiempo, el uso racional de los recursos del espectro radioeléctrico.

f) Neutralidad tecnológica: La normativa deberá permitir el uso de múltiples tecnologías de comunicación consumidoras de la IoT y no establecer preferencia innecesaria por determinados proveedores, plataformas o protocolos, siempre que la comunicación que éstas logran cumplir satisface los requerimientos de la normativa y técnica específicos.

g) Sostenibilidad: La puesta en práctica de las soluciones de la IoT debe promover que se haga un uso eficiente de los recursos tecnológicos y energéticos, promoviendo, a su vez, el desarrollo sostenible y la reducción del impacto ambiental.

h) Mejora continua: El marco regulatorio deberá adaptar la normativa en función de la evolución del desarrollo tecnológico, los riesgos emergentes y las necesidades de comercio local ecuatoriano.

i) Implementación gradual de la normativa: La integración de la nueva normativa del Internet de las Cosas será gradual. Dicha implementación progresiva se verá determinada por la concurrencia de tres factores: el progreso tecnológico, la capacidad institucional del Estado, y las necesidades del comercio local ecuatoriano.

TÍTULO II

GESTIÓN DEL ESPECTRO RADIOELÉCTRICO Y TECNOLOGÍAS HABILITADAS PARA EL IoT.

CAPÍTULO I

BANDAS DE OPERACIÓN

Artículo 6.- Bandas de operación para IoT.

PER(ARCOTEL) incluirá en el Plan Nacional de Frecuencias criterios específicos para la operación de tecnologías dedicadas al Internet de las Cosas. Para ello, se distinguirá entre bandas libres y bandas con licencia, según las necesidades de conectividad del comercio local y el desarrollo tecnológico.

CAPITULO II

USO DE BANDAS LIBRES Y LICENCIADAS

Artículo 7.- Uso de bandas libres.

Se fomentará el uso de bandas de frecuencias libres para aplicaciones IoT de corto alcance, sujeto a las condiciones técnicas establecidas por ARCOTEL.

Artículo 8.- Uso de bandas licenciadas.

Para aplicaciones consideradas críticas o que requieran alta disponibilidad, ARCOTEL podrá establecer procedimientos especiales de asignación de espectro para soluciones IoT.

CAPÍTULO III

TECNOLOGÍAS HABILITADAS Y PLANIFICACIÓN DEL ESPECTRO

Artículo 9.- Tecnologías habilitadas.

Las tecnologías que cumplan con las especificaciones técnicas establecidas por ARCOTEL serán reconocidas como tecnologías habilitantes para el desarrollo de soluciones de Internet de las Cosas (IoT). Dentro de estas tecnologías incluyen, LPWAN, LoRaWAN, NB-IoT, LTE-M, ZigBee, Bluetooth Low Energy, Wi-Fi, 5G y cualquier otra tecnología que pueda integrarse como resultado de los avances tecnológicos.

Artículo 10.- Planificación espectral.

ARCOTEL establecerá mecanismos permanentes para la planificación, evaluación y actualización del espectro radioeléctrico asignado para aplicaciones de IoT. El desarrollo de estos mecanismos tendrá en cuenta los siguientes factores: el crecimiento del ecosistema digital, la demanda de nuevos servicios, la integración de nuevas tecnologías y las necesidades dentro del comercio local.

TÍTULO III

HOMOLOGACIÓN Y CERTIFICACIÓN DE DISPOSITIVOS IoT.

CAPÍTULO I

HOMOLOGACIÓN DE DISPOSITIVOS.

Artículo 11.- Homologación obligatoria.

ARCOTEL establecerá un procedimiento especial de aprobación para dispositivos destinados a aplicaciones del Internet de las Cosas (IoT). Este procedimiento considerará criterios relacionados con los siguientes aspectos: tecnología de comunicación, nivel de potencia, consumo de energía, ámbito de aplicación y nivel de riesgo. Su objetivo es garantizar el funcionamiento seguro e interoperable de los dispositivos dentro del ecosistema nacional de telecomunicaciones.

CAPITULO II

CERTIFICACIÓN TÉCNICA.

Artículo 12.- Requisitos técnicos mínimos.

Todos los dispositivos IoT deben demostrar el cumplimiento de los requisitos mínimos como requisito previo para su aprobación y comercialización. Estos requisitos abarcan áreas como: ciberseguridad, interoperabilidad, compatibilidad electromagnética, uso eficiente del espectro radioeléctrico y actualizaciones seguras de software o firmware.

Artículo 13.- Certificación de conformidad.

Se verificará que todos los dispositivos IoT cumplan con los requisitos técnicos, operativos y de seguridad establecidos para su homologación, mediante informes de ensayo, certificaciones internacionales reconocidas o evaluaciones técnicas aceptadas por ARCOTEL.

CAPÍTULO III

RECONOCIMIENTO DE CERTIFICACIONES INTERNACIONALES.

Artículo 14.- Reconocimiento de certificaciones.

ARCOTEL podrá reconocer los certificados técnicos emitidos por organizaciones internacionales acreditadas, siempre que se garantice un nivel equivalente de seguridad, calidad, compatibilidad y cumplimiento con los requisitos de este marco regulatorio.

Artículo 15.- Registro de dispositivos homologados.

Créase el Registro Nacional de Dispositivos IoT Aprobados, administrado por ARCOTEL. El objetivo de este registro es mantener actualizada la información sobre los equipos autorizados para su venta y uso en el país. Facilitará los procedimientos de verificación técnica, el control regulatorio y la consulta pública.

TÍTULO IV

INTEROPERABILIDAD Y ESTÁNDARES TÉCNICOS.

CAPÍTULO I

INTEROPERABILIDAD DE SISTEMAS.

Artículo 16.- Interoperabilidad.

Se debe garantizar la interoperabilidad entre dispositivos, plataformas, aplicaciones y servicios del Internet de las Cosas (IoT). Esta interoperabilidad debe lograrse mediante un intercambio de información seguro, fiable y eficiente, que permita la integración de los diferentes fabricantes, tecnologías y sistemas utilizados en el comercio ecuatoriano.

CAPÍTULO II

ESTÁNDARES TÉCNICOS

Artículo 17.- Estándares abiertos.

Las soluciones IoT deben incorporar normas abiertas y protocolos de comunicación ampliamente reconocidos. Estas normas y protocolos deben promover la interoperabilidad, la escalabilidad, la innovación tecnológica y la integración fluida entre dispositivos, plataformas y servicios digitales. Esto ayudará a evitar las limitaciones que puedan surgir del uso exclusivo de tecnologías propietarias.

CAPÍTULO III

COMPATIBILIDAD ENTRE PLATAFORMAS Y DISPOSITIVOS.

Artículo 18.- Compatibilidad de plataformas.

Las plataformas orientadas a la solución de IoT deberán garantizar la compatibilidad de dispositivos de fabricantes y tecnologías diversas. Deben permitir el intercambio de datos, la gestión centralizada de la información y la incorporación progresiva de dispositivos, sin interrumpir la continuidad del servicio.

Artículo 19.- Integración tecnológica.

Las soluciones de IoT implementadas en el ámbito del comercio local deberán permitir la integración con los sistemas de información y plataformas digitales, así como con los servicios tecnológicos que usan las organizaciones públicas o privadas. De este modo, fomentan la creación de un ecosistema digital interoperable, escalable y orientado a la transformación digital.

TÍTULO V

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

CAPÍTULO I

SEGURIDAD DE DISPOSITIVOS IoT.

Artículo 20.- Seguridad desde el diseño.

Los dispositivos, las plataformas y las aplicaciones del Internet de las Cosas (IoT) deben incluir mecanismos de seguridad en las fases de diseño, desarrollo e implementación porque tienen que garantizar la protección de la información, la autenticación de dispositivos, el control de acceso y la mitigación de vulnerabilidades a través de todo el ciclo de vida del sistema.

CAPÍTULO II

GESTIÓN DE VULNERABILIDADES

Artículo 21.- Gestión de vulnerabilidades.

Los fabricantes, desarrolladores, proveedores y operadores de soluciones IoT deben implementar procedimientos para identificar, evaluar, corregir y mitigar las vulnerabilidades que podrían comprometer la disponibilidad, la integridad, la autenticidad o la confidencialidad de los sistemas y la información procesada.

Artículo 22.- Actualización de firmware.

Los dispositivos IoT deben contar con mecanismos robustos para actualizar periódicamente el firmware. Estos mecanismos garantizarán la corrección de vulnerabilidades, el mantenimiento de la seguridad y se garantice la continuidad operativa de los servicios implementados.

CAPÍTULO III

PROTECCIÓN DE DATOS

Artículo 23.- Protección de datos.

El tratamiento de datos personales obtenidos a través de dispositivos, plataformas o aplicaciones del Internet de las Cosas (IoT) debe cumplir con los principios de legalidad, finalidad

específica, proporcionalidad, minimización de datos, confidencialidad y seguridad. Esto hace que la recolección, así como el uso, sean rigurosamente conformes a la finalidad para la que se obtuvo la autorización.

Artículo 24.- Gestión de riesgos.

Las organizaciones que aplican soluciones IoT van a tener que poner en marcha procesos cíclicos para la identificación, evaluación y tratamiento del riesgo que afecta a los dispositivos, a las redes, a las plataformas y a los datos que se procesan. Así como también definir e implementar medidas preventivas para disminuir los efectos de incidentes que puedan impactar la continuidad del negocio.

TÍTULO VI

APLICACIONES SECTORIALES DEL IoT.

CAPITULO I

APLICACIONES EN EL COMERCIO LOCAL

Artículo 25.- Aplicaciones comerciales.

Las soluciones del Internet de las Cosas (IoT) pueden encontrar aplicación en empresas comerciales traduciendo dicha aplicación en mejoras en los procesos de automatización de los mismos, en la gestión inteligente del inventario, en el seguimiento de los productos, en el control de los activos, en la atención al cliente o en la toma de decisiones en tiempo real a partir de datos. Esta aplicación debe garantizar la compatibilidad, la seguridad de la información y el cumplimiento de las prescripciones que contiene este texto normativo.

CAPÍTULO II

LOGÍSTICA Y SEGUIMIENTO DE PRODUCTOS

Artículo 26.- Seguimiento inteligente de productos.

Las soluciones IoT para el seguimiento de productos deben permitir la identificación, el posicionamiento y el seguimiento de las mercancías durante las diferentes etapas que componen el almacenamiento, el transporte y la distribución de las mercancías, facilitando así la gestión logística, reduciendo las pérdidas de productos y optimizando la misma cadena de suministro existía.

Artículo 27.- Automatización de procesos.

Las organizaciones pueden combinar soluciones IoT para automatizar procesos vinculados a las siguientes áreas: inventario y control de activos, monitorización ambiental, mantenimiento de equipos, gestión energética, y en general, automoción de tareas y de actividades orientadas a mejorar la eficiencia operativa y la productividad.

CAPÍTULO III

INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

Artículo 28.- Transformación digital basada en IoT.

Los organismos gubernamentales competentes facilitarán la integración gradual de soluciones de IoT en el comercio local. Esto se logrará mediante las siguientes herramientas: programas de innovación, fortalecimiento de capacidades digitales, cooperación con el sector manufacturero y la creación de condiciones favorables para el desarrollo tecnológico del país.

TÍTULO VII

GOBERNANZA Y COORDINACIÓN INSTITUCIONAL

COMPETENCIAS INSTITUCIONALES

Artículo 29.- Competencias de MINTEL.

El Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) es responsable de desarrollar las políticas públicas, estrategias nacionales y programas que permitan

integrar el Internet de las Cosas (IoT) en el comercio de proximidad, para poder impulsar la transformación digital, la innovación tecnológica y el fortalecimiento de las capacidades institucionales y técnicas que sean requeridas para el desarrollo del ecosistema IoT en Ecuador.

Artículo 30.- Competencias de ARCOTEL.

La Agencia Reguladora y de Control de Telecomunicaciones (ARCOTEL) es responsable de la gestión del espectro radioeléctrico asignado para aplicaciones IoT, así como de establecer los procedimientos de aprobación y certificación de dispositivos, garantizando el cumplimiento de las disposiciones técnicas del presente marco normativo, y manteniendo el Registro Nacional de Dispositivos IoT Aprobados.

Artículo 31.- Participación de las entidades competentes.

Las autoridades gubernamentales competentes en materia de transformación digital, protección de datos personales, estandarización técnica, desarrollo industrial, comercio e innovación participarán, dentro de sus respectivas competencias, en la implementación, el seguimiento y la actualización de este marco regulatorio. Esta participación debería facilitar la coordinación interinstitucional encaminada a fortalecer el ecosistema nacional de IoT.

CAPÍTULO II

COORDINACIÓN INTERINSTITUCIONAL

Artículo 32.- Coordinación institucional.

MINTEL y ARCOTEL establecerán un mecanismo de coordinación con las agencias gubernamentales pertinentes en materia de protección de datos, estandarización técnica, desarrollo industrial, comercio e innovación. El objetivo de esta coordinación es armonizar las acciones relacionadas con la implementación, el seguimiento y la actualización del marco regulatorio para el Interne de las Cosas en el comercio interno ecuatoriano.

CAPÍTULO III

SUPERVISIÓN Y SEGUIMIENTO

Artículo 33.- Supervisión y control.

ARCOTEL supervisará el cumplimiento de las disposiciones técnicas relacionadas con las siguientes áreas: espectro radioeléctrico, homologación, certificación e interoperabilidad de dispositivos IoT. Esta supervisión se llevará a cabo sin perjuicio de las facultades de otras agencias gubernamentales en materia de protección de datos, seguridad digital, comercio y desarrollo industrial.

Artículo 34.- Evaluación y mejora regulatoria.

El MINTEL, en coordinación con la ARCOTEL y las entidades públicas generales correspondientes, efectuará evaluaciones periódicas respecto a cuál es el grado de aplicación y efectividad de este marco regulatorio. Y dichas evaluaciones se construirán a partir de las siguientes consideraciones: avances tecnológicos, incorporación de nuevas perspectivas de soluciones de IoT, necesidades de negocio, así como resultados de la implementación.

Con la información obtenida de las evaluaciones realizadas se podrán generar recomendaciones para la actualización de las guías para la técnica, procedimientos regulatorios, así como de los mecanismos de coordinación institucional, todo ello con el objeto de contribuir a una mejora.

TÍTULO VIII

IMPLEMENTACIÓN, SEGUIMIENTO Y DISPOSICIONES FINALES.

CAPÍTULO I

IMPLEMENTACIÓN PROGRESIVA

Artículo 35.- Implementación progresiva.

La puesta en marcha de este marco normativo se implementará por fases. Se ejecutará de forma paulatina, determinada por algunos criterios: la evolución que tome la infraestructura digital, la existencia de tecnologías requeridas, la capacidad institucional y el nivel de adopción del Internet de las Cosas (IoT) en el comercio local ecuatoriano.

Las autoridades competentes establecerán mecanismos para instrumentar la integración gradual de las previsiones de este marco normativo. Para ello se dará prioridad a las aplicaciones que generen el mayor impacto en la modernización, la eficiencia y competitividad del comercio.

Artículo 36.- Proyectos piloto.

El Ministerio de Telecomunicaciones (MINTEL), en coordinación con la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), los organismos públicos competentes, la academia y el sector manufacturero, impulsará la elaboración de proyectos piloto. Estos proyectos pilotarán las aplicaciones del IoT en el comercio local,

los resultados que se obtengan de la ejecución de estos proyectos se emplearán para reforzar las políticas públicas, modernizar la normativa y promover la integración gradual de las tecnologías e Internet de las Cosas (IoT) en distintos sectores productivos.

CAPÍTULO II

SEGUIMIENTO Y ACTUALIZACIÓN NORMATIVA

Artículo 37.- Evaluación periódica.

Las autoridades competentes realizarán evaluaciones periódicas de la aplicación de este marco regulatorio. Estas evaluaciones tendrán en cuenta los siguientes puntos: desarrollos tecnológicos, resultados obtenidos durante la implementación, necesidades del comercio local y el comportamiento del ecosistema nacional del Internet de las Cosas (IoT).

Artículo 38.- Actualización normativa.

Esta normativa se actualizará en respuesta a los desarrollos tecnológicos, la introducción de nuevas tecnologías, la aparición de nuevos riesgos o las necesidades dentro del comercio ecuatoriano. Esto garantizará la relevancia, pertinencia y adaptabilidad a los cambios en el entorno digital.

CAPÍTULO III

DISPOSICIONES FINALES

Artículo 39.- Disposiciones finales.

Los organismos gubernamentales competentes promoverán la cooperación con el sector de la fabricación, el mundo académico, las organizaciones normalizadoras, los centros de investigación y el resto de los actores del ecosistema digital, al objeto de propiciar la innovación, el desarrollo tecnológico, la investigación aplicada y la transferencia del conocimiento relativo al Internet de las Cosas. El marco reglamentario referido es una propuesta técnica que busca abrir paso a la formalización de disposiciones concretas sobre el Internet de las Cosas (IoT) en el comercio local del Ecuador; de este modo, se contribuye al proceso de identidad de un ecosistema digital seguro, interoperable, innovador y sostenido que reactive el camino hacia la transformación digital y la competitividad nacional.

Conclusiones

- Se alcanzó el objetivo general al formular una propuesta de un marco regulador sobre el IoT en el comercio local ecuatoriano, que se fundamentaba en una comparación con México y Brasil. Para ello se presentaron lineamientos legales, técnicos e institucionales en función del país, con el objetivo de contribuir a robustecer el desarrollo normativo del IoT.

- Se identificó que tecnologías IoT que se usan en el comercio local, se encontró que LoRaWAN, NB-IoT, ZigBee, Sigfox y 5G son las opciones más comunes para tareas como control de inventarios, seguimiento de productos, monitoreo de equipos y automatización de procesos comerciales. También se evidenció que México y Brasil ya han incluido estas soluciones en sus estrategias y normas, mientras que Ecuador hace uso de estas tecnologías todavía bajo una normativa general que no considera disposiciones particulares del IoT.
- Al examinar los marcos regulatorios, se puede observar que México y Brasil han desarrollado mecanismos para regular el espectro, la homologación, la interoperabilidad, la ciberseguridad y la planificación IoT. El país que principalmente se considera de referencia en la elaboración de los marcos regulatorios es Brasil, mientras que México complementa en espectro y tecnologías habilitadas. En el caso de Ecuador solo se han encontrado normas de tipo general en temas de telecomunicaciones, datos y transformación digital, pero no hay una regulación específica de IoT.
- Se encontraron diversos desafíos para regular el IoT en Ecuador. Entre lo que se encontró están el mejorar la infraestructura digital, una mejor planificación del espectro, criterios claros para homologar dispositivos, promover la interoperabilidad, incorporar ciberseguridad y la coordinar mejor las instituciones competentes. Se consideran estos aspectos importantes para que la adopción del IoT en el comercio local sea segura y sostenible.
- Con base en los resultados obtenidos del análisis, se plantearon lineamientos para una normativa específica del IoT en el comercio local ecuatoriano. Entre los

lineamientos existen disposiciones generales, espectro, homologación, interoperabilidad, protección de datos, ciberseguridad, aplicaciones de tipos sectoriales, gobernanza e implementación progresiva, los cuales se realizan tomando en cuenta buenas tecnologías y su práctica en México y Brasil.

- La propuesta final, no solo ordena los lineamientos, sino que se convierte en una base normativa aplicable a Ecuador, es decir, que su mayor aporte es de cerrar los vacíos locales con buenas prácticas de México y Brasil, y la orientación que puede dárseles en regulaciones futuras para que se puedan obtener como resultado seguridades jurídicas, innovaciones y competitividad en el comercio local.

Recomendaciones

- Se sugiere que el MINTEL, junto con la ARCOTEL tomen la propuesta de marco regulatorio de esta investigación como insumo técnico para futuras disposiciones sobre IoT en el comercio local ecuatoriano.
- Se recomienda fomentar el uso progresivo de tecnologías IoT en el comercio local, a través de programas de capacitación y acompañamiento técnico para pequeñas o medianas empresas. Así se facilitará la incorporación de soluciones en monitoreo, seguimiento de productos, la gestión de inventario y la automatización de procesos comerciales.
- Futuras regulaciones sobre IoT deberían tomar en cuenta las buenas prácticas de México y Brasil, priorizando los componentes con mayor desarrollo identificados en el análisis: gobernanza, espectro, homologación, interoperabilidad y ciberseguridad.

- Fortalecer la coordinación entre las instituciones encargadas de telecomunicaciones, transformación digital, protección de datos, innovación y desarrollo productivo. El objetivo es establecer mecanismo de cooperación que faciliten políticas públicas para el desarrollo del ecosistema IoT en Ecuador.
- Las regulaciones propuestas deben ser revisadas y discutidas técnicamente. Sería enriquecedor que participen universidades, reguladores, el sector productivo, especialistas en IoT, para enriquecer su contenido y considerar su adecuación antes de ser incorporadas al cuerpo regulatorio nacional.
- Las futuras investigaciones podrían evaluar la propuesta regulatoria en diferentes sectores económicos del país, a través de estudios piloto o casos concretos. Eso serviría para retroalimentar mejoras o para mantener los lineamientos actualizados a medida que avanza la tecnología IoT o cambian las necesidades del comercio ecuatoriano local.

Bibliografía

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). (2018). *Resolución ARCOTEL-2018-0661*.

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). (2021). *Plan Nacional de Frecuencias. Versión 6.0*.

Alfonzo Guzmán, M. I. (2020). *Análisis Técnico y Regulatorio de Nuevas Redes de Transmisión para Dispositivos IoT (Internet of Things) en la ciudad de Guayaquil*.

Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2023). Long range technology for internet of things: review, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics*, *12*(6), 3758–3767. https://doi.org/10.11591/eei.v12i6.5214

ANATEL. (2017, junio 29). *Resolución No. 680, de 27 de junio de 2017*. https://informacoes.anatel.gov.br/legislacao/resolucoes/2017/936-resolucao-680?utm_source=chatgpt.com

ANATEL. (2020). *Resolución N° 740, de 21 de diciembre de 2020*. https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740

ANATEL. (2021). *Ley n.º 77, de 5 de enero de 2021*. https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

Andrade, R. O., & Yoo, S. G. (2019). A comprehensive study of the use of LoRa in the development of smart cities. En *Applied Sciences (Switzerland)* (Vol. 9, Número 22). MDPI AG. https://doi.org/10.3390/app9224753

Asamblea Nacional del Ecuador. (2015). Ley Orgánica de Telecomunicaciones. *Registro Oficial del Ecuador*, (Suplemento del Registro Oficial No. 439).

Asamblea Nacional del Ecuador. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Barbecho, E., & Gutiérrez, I. (2021). *DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA BASADA EN IOT PARA LA GESTIÓN DE PROMOCIONES DE ARTÍCULOS EN ESTABLECIMIENTOS COMERCIALES*.

Bhat, O., Gokhale, P., & Bhat, S. (2007). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology ISO*, *3297*(1). https://doi.org/10.17148/IARJSET.2018.517

Camacho Castillo, R. (2019). *IoT y 5G*.

Campos, N. O., & Cavada, J. C. (2021). Analysis for the implementation of 5G technology based on the GSMA model and its interaction with the Internet of Things in Ecuador. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2021*(43), 38–54. https://doi.org/10.17013/RISTI.43.38-54

Coello Mora, E. D. (2010). *Análisis de la Regulación de Telecomunicaciones en el Ecuador y las Nuevas Tendencias del Sector*.

Comisión Económica para América Latina y el Caribe (CEPAL). (2022). *eLAC2024*. 8.

Dixit, E., & Rani, S. (2025). Integrated Trends, Opportunities, and Challenges of 5G and Internet of Things. *Current and Future Cellular Systems: Technologies, Applications, and Challenges*, 139–152. https://doi.org/10.1002/9781394256075.CH7

Döníz, B., & Lajos, B. (2022). Challenges of LoRaWAN technology in smart city solutions. *Interdisciplinary Description of Complex Systems*, *20*(1), 1–10. https://doi.org/10.7906/indecs.20.1.1

García Murillo, M. (2007). *Las Instituciones como marco de referencia en el proceso de convergencia de las TIC*.

Instituto Federal de Telecomunicaciones. (2019). *Análisis exploratorio de la comercialización de servicios de conectividad para IoT*.

Instituto Federal de Telecomunicaciones (IFT). (2022). *Código de mejores prácticas para la ciberseguridad de los dispositivos del Internet de las Cosas (IoT)*.

Instituto Federal de Telecomunicaciones (IFT). (2023). *Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones clasifica la banda de frecuencias 5925-6425 MHz como espectro libre y emite las condiciones técnicas de operación de la banda.*

International Telecommunication Union (ITU). (2024, febrero 5). *Guiding principles for ICT regulators to enhance cyber resilience*. https://digitalregulation.org/guiding-principles-for-ict-regulators-to-enhance-cyber-resilience/

ITU. (2019). *5G and spectrum: different approaches ITU workshop: 5G and new technologies*.

Jin, S., & Karki, B. (2025). Integrating IoT and blockchain for intelligent inventory management in supply chains: A multi-objective optimization approach for the insurance industry. *Journal of Engineering Research (Kuwait)*, *13*(2), 527–537. https://doi.org/10.1016/j.jer.2024.04.021

Lo, N., & Niang, I. (2021). A comparison of qos-based architecture solutions for iot/edge computing environment. *Advances in Science, Technology and Innovation*, 355–364. https://doi.org/10.1007/978-3-030-53440-0_37

MCTIC. (2018). *Estratégia Nacional de Ciência, Tecnologia e Inovação*.

Meza, P., Íñiguez, F., Becerra, M., Rivera, O., Vera, J., Chiluiza, J. C., Ortega, J., Malla, R., Simbaña, F., Valverde, A., López, S., & Sotaminga, M. (2022). Agenda de Transformación Digital del Ecuador 2022-2025. *Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). (2021). *Acuerdo Ministerial 006-2021 -Política de Ciberseguridad*.

Nader Conti, M. (2024, diciembre). *Transformación Digital en el Ámbito Societario y de Seguros en Ecuador: Desafíos, Oportunidades y Estrategias para la Innovación*. https://ojs.supercias.gob.ec/index.php/X-pedientes_Economicos/article/view/183/144

Ochoa Zezzatti, A., Contreras Masse, R., & Mejía, J. (2021). Multicriteria Analysis for LPWAN Selection for Industry 4.0 Based on TOPSIS and a Model of Proportionality. *Studies in Computational Intelligence*, *953*, 15–46. https://doi.org/10.1007/978-3-030-73819-8_2

ONU. (2016). *Objetivos de Desarrollo Sostenible | Programa De Las Naciones Unidas Para El Desarrollo*. https://www.undp.org/es/sustainable-development-goals

Osman, Dr. N., & Abbas, E. (2022). Performance Evaluation of LoRa and Sigfox LPWAN Technologies for IoT. *Academic Journal of Research and Scientific Publishing*, *4*(38), 05–24. https://doi.org/10.52132/Ajrsp.e.2022.38.1

Pérez Ramos, C., León Venegas, A., & Casanova Galán, B. U. (2022). *TOWARDS THE CONSTRUCTION OF SMART CITIES IN LATIN AMERICA AND THE CARIBBEAN THROUGH THE USE OF SPACE TECHNOLOGY*. https://www.scopus.com/pages/publications/85167583433

Presidencia de la República de Brasil. (2019). *DECRETO N° 9.854, DE 25 DE JUNIO DE 2019*. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm#:~:text=DECRETO

Radouan Ait Mouha, R. A. (2021). Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, *09*(02), 77–101. https://doi.org/10.4236/jdaip.2021.92006

Robinson, R. J. (2024). IoT Solutions for Smart Parking- Sigfox Technology. *Computer Science & Engineering: An International Journal*, *14*(2), 01–13. https://doi.org/10.5121/cseij.2024.14201

Ruckebusch, P., Giannoulis, S., Moerman, I., Hoebeke, J., & De Poorter, E. (2018). Modelling the energy consumption for over-the-air software updates in LPWAN networks: SigFox, LoRa and IEEE 802.15.4g. *Internet of Things (Netherlands)*, *3–4*, 104–119. https://doi.org/10.1016/j.iot.2018.09.010

Secretaría Nacional de la Administración Pública (SNAP). (2015). *Norma Técnica de Interoperabilidad Gubernamental*. www.lexis.com.ec

Secretaría Nacional de Planificación. (2021). *Plan de Creación de Oportunidades 2021-2025*.

Secretaría Nacional de Planificación. (2024). *Plan de Desarrollo para el Nuevo Ecuador 2024 - 2025*.

Tonato Chuquimarca, C., & Sinche Maita, S. (2022). Análisis comparativo entre arquitecturas de sistemas IoT. *Revista de Investigación en Tecnologías de la Información*, *10*(21), 55–70. https://doi.org/10.36825/RITI.10.21.006

Trujillo, M. C., Ramos, T. S., Esqueda Martínez, R., Ponce Leyva, J. E., Guarneros Gutiérrez, R., & Terrazas Briones, P. J. (2020). *ANÁLISIS EXPLORATORIO DE COMERCIALIZACIÓN DE SERVICIOS DE CONECTIVIDAD PARA EL IOT EN MÉXICO*. https://www.

UIT. (2023). *Members Directory - ITU*. https://www.itu.int/hub/membership/our-members/directory/?myitu-members-states=true&request=countries

UIT-T. (2012). *Redes de la próxima generación – Marcos y modelos arquitecturales funcionales. Descripción general de Internet de los objetos. Recomendación UIT-T Y.2060*. http://handle.itu.int/11.1002/1000/11830-en.

Wang, J. (2025). Enhancing the e-commerce shopping experience with IoT-enabled smart carts in smart stores. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00128-2

Yan, J., Yang, J., Zhu, F., & Teng, Z. (2021). Green city and government ecological environment management based on ZigBee technology. *Environmental Technology and Innovation*, *23*. https://doi.org/10.1016/j.eti.2021.101711

Zhao, Y. (2021). Research on Wireless Sensor Network System based on Zigbee Technology for short distance transmission. *IOP Conference Series: Earth and Environmental Science*, *1802*(2). https://doi.org/10.1088/1742-6596/1802/2/022008