RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Tecnologías de Comunicación IoT para Smart Cities

Febrero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IOT PARA ENTORNOS DE SMART CITIES Y SALUD” (CONTR 2024 829153).

Esta guía forma parte de la colección Guías de Ciberseguridad en IoT para las Smart Cities y el sector Salud creada por la Agencia Digital de Andalucía como parte del Proyecto Red Argos, perteneciente al programa RETECH, de Redes Inteligentes de Especialización Tecnológica, en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-NextGenerationEU, financiado por la Unión Europea NextGeneration-EU, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 23/02/2026

Fecha de última actualización: 23/02/2026

ÍNDICE DE CONTENIDOS

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

1. Introducción

El Internet de las Cosas (IoT) se ha consolidado como una tecnología clave para el desarrollo de Smart Cities, al permitir la conexión de sensores, actuadores y sistemas distribuidos que facilitan la monitorización y gestión de los servicios urbanos. Gracias al IoT, es posible optimizar la movilidad, el alumbrado, la gestión de residuos, el agua, la energía y otros servicios, mejorando la eficiencia operativa y la calidad de vida de la ciudadanía.

Sin embargo, los entornos urbanos presentan condiciones exigentes: los dispositivos suelen tener recursos limitados, ubicaciones expuestas y conectividad variable, mientras que las soluciones deben operar sobre múltiples tecnologías de comunicación. Esta complejidad técnica y operativa, unida a factores como cobertura, consumo energético, latencia, escalabilidad, interoperabilidad y ciberseguridad, hace que la selección de la tecnología adecuada sea crítica. Una elección incorrecta puede afectar la eficiencia de los servicios, la sostenibilidad técnica de los proyectos y la seguridad de los sistemas y los datos de la ciudad.

La complejidad aumenta al considerar factores como la cobertura, el consumo energético, la latencia, la escalabilidad, la interoperabilidad y los requisitos de ciberseguridad. Para administraciones públicas y equipos técnicos, seleccionar la tecnología más adecuada para cada caso de uso puede ser una tarea difícil y sujeta a riesgos si no se dispone de criterios claros.

2. Objetivo y alcance

2.1. Objetivo

El objetivo de esta guía es servir como marco de referencia para la selección y el diseño de tecnologías IoT en entornos urbanos. Su finalidad es apoyar a las administraciones públicas y a los equipos técnicos en la identificación de la tecnología más adecuada para cada caso de uso, analizando sus implicaciones en materia de ciberseguridad y definiendo criterios de arquitectura, operación y gestión del ciclo de vida que garanticen la viabilidad y sostenibilidad de los proyectos.

2.2. Alcance

Esta guía se centra en el análisis de las principales tecnologías de comunicación IoT utilizadas en entornos de Smart City, desde una perspectiva técnica y de ciberseguridad. El documento aborda las características generales de cada tecnología, sus arquitecturas de referencia, los principales riesgos y medidas de seguridad asociadas, así como criterios para su selección en función de distintos casos de uso urbanos.

El alcance de la guía se limita al ámbito de las comunicaciones y su integración en el ecosistema IoT urbano, sin entrar en el diseño detallado de aplicaciones, plataformas de analítica avanzada o procesos de explotación del dato. Asimismo, la guía no sustituye a normativas, estándares o pliegos técnicos específicos, sino que actúa como documento de apoyo para la toma de decisiones en fases de planificación y diseño de proyectos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

La guía está orientada principalmente a administraciones públicas, responsables técnico responsable, integradores y otros agentes implicados en el despliegue de soluciones IoT en Smart Cities, proporcionando un marco común que facilite evaluaciones comparables y alineadas con buenas prácticas de seguridad.

2.3. Metodología

El contenido de esta guía se ha elaborado siguiendo una metodología estructurada que combina revisión normativa, análisis técnico y experiencias prácticas:

1. Revisión técnica y normativa: análisis de estándares y especificaciones relevantes (p. ej., 3GPP, IEEE, ETSI), así como de marcos de ciberseguridad y referencias de protección de datos aplicables al sector público.
2. Comparativa tecnológica: evaluación de las capacidades, limitaciones y requisitos de cada familia de tecnología de comunicación (cobertura, latencia, consumo energético, seguridad y operación), así como su adecuación a distintos casos de uso urbanos.
3. Criterios de selección y gobernanza: definición de principios transversales que guíen la elección y operación de tecnologías IoT, tanto técnicos como operativos.
4. Casos de uso representativos: recopilación y detalle de despliegue reales en ámbitos como agua, movilidad, residuos, alumbrado y edificios públicos, con énfasis en el valor operativo y los beneficios aportados.

Esta metodología garantiza que la guía sea neutral tecnológicamente, orientada a la práctica y alineada con la normativa, proporcionando criterios claros para la toma de decisiones y la gestión integral de proyectos IoT en Smart Cities.

3. Referencias normativas

El presente documento se apoya en un marco regulatorio y técnico amplio que integra normativa legal, estándares internacionales y guías de buenas prácticas aplicables a los entornos urbanos conectados.

Dicho marco constituye la base metodológica y conceptual sobre la que se estructura esta guía, asegurando la coherencia con las políticas europeas, nacionales e internacionales en materia de ciberseguridad, movilidad conectada, tratamiento de datos personales e infraestructuras críticas.

- **Normativas:**
  - Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
  - Reglamento (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a las medidas para asegurar un alto nivel común de ciberseguridad en la UE (en adelante, NIS2).
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).

- **Estándares:**
  - ISO/IEC 27400, Seguridad y privacidad en IoT.
  - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
  - ISO/IEC 27001, Gestión de la seguridad de la información.
  - ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
  - ISO/IEC 22301, Gestión de la continuidad de negocio.
  - UNE 178107, Estándares para la gestión de infraestructuras en Ciudades Inteligentes.

- **Guías:**
  - Cloud Security Alliance (CSA), Matriz de controles Cloud (CCM).
  - ENISA, Guía para la securización de IoT.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
  - OWASP IoT y OWASP, Guías de auditorías técnicas.

4. Definiciones

Acrónimos	Definición
AES	Algoritmo de cifrado simétrico para proteger datos en tránsito y en reposo con claves de 128, 192 o 256 bits (del inglés, Advanced Encryption Standard).
EPC	Núcleo de red 4G encargado de gestionar tráfico IP, movilidad y autenticación (del inglés, Evolved Packet Core).
eMBB	Caso de uso 5G orientado a ofrecer velocidades muy altas y gran capacidad (del inglés, enhanced Mobile Broadband).
eSIM	Tarjeta SIM digital integrada en el dispositivo, sin necesidad de una tarjeta física.
gNodeB	Estación base de 5G que gestiona la conexión radio entre dispositivos y la red.
Handover	Proceso mediante el cual una conexión móvil se transfiere de una celda o estación base a otra sin interrumpir la comunicación.
LoRa	Tecnología de modulación de espectro ensanchado de largo alcance y bajo consumo.
LoRaWAN	Protocolo de red sobre LoRa que define la comunicación entre dispositivos y servidores (del inglés, Long Range Wide Area Network).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Acrónimos	Definición
LPWAN	Categoría de redes inalámbricas diseñadas para dispositivos IoT que requieren largo alcance y muy bajo consumo (del inglés, Low Power Wide Area Network).
LTE	Estándar de comunicación inalámbrica que permite la transmisión de datos móviles de alta velocidad (del inglés, Long Term Evolution).
LTE-M	Tecnología celular de bajo consumo basada en LTE, diseñada para dispositivos IoT que requieren movilidad (del inglés, Long Term Evolution Machine Type Communication).
IEEE	Asociación global que desarrolla estándares tecnológicos (del inglés, Institute of Electrical and Electronics Engineers).
IP	Conjunto de reglas para enviar y enrutar paquetes de datos en redes (del inglés Internet Protocol).
MEC	Tecnología que acerca capacidad de computación a la red de acceso (del inglés, Multi-access Edge Computing).
MIC	Código que garantiza la integridad de un mensaje, detectando modificaciones no autorizadas (del inglés, Message Integrity Code).
mMTC	Caso de uso 5G diseñado para soportar millones de dispositivos IoT de bajo consumo (del inglés, massive Machine Type Communications).
NB-IoT	Tecnología de red celular de baja potencia y amplio alcance diseñada para conectar dispositivos IoT con bajo consumo de energía y pequeñas cantidades de datos (del inglés, Narrowband Internet of Things).
Red Mesh	Topología de red en la que los dispositivos se conectan entre sí, permitiendo múltiples rutas de comunicación.
Sigfox	Tecnología de red LPWAN diseñada para conectar dispositivos IoT con bajo consumo energético y transmisión de datos de largo alcance.
SIM	Módulo físico que identifica a la persona usuaria en la red móvil y almacena claves de autenticación.
SLA	Acuerdo que define niveles garantizados de servicio, como latencia, disponibilidad y calidad (del inglés, Service Level Agreement).
URLLC	Caso de uso 5G para comunicaciones ultra fiables y con latencia mínima (del inglés, Ultra-Reliable Low Latency Communications).
VoLTE	Tecnología que permite realizar llamadas de voz sobre la red 4G usando IP (del inglés, Voice over LTE).
WiFi	Tecnología de red inalámbrica basada en estándares IEEE 802.11 para conectar dispositivos a internet.
WPAN	Red inalámbrica de corto alcance para conectar dispositivos personales (del inglés, Wireless Personal Area Network).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Acrónimos	Definición
ZUC	Algoritmo de cifrado en flujo utilizado en 4G y 5G para proteger comunicaciones móviles.
5G-AKA	Procedimiento de autenticación del abonado en redes 5G
3GPP	Organismo internacional que define los estándares de telecomunicaciones móviles (del inglés, 3rd Generation Partnership Project).

TABLA 1: DEFINICIONES EMPLEADAS.

5. Ecosistema IoT en Smart Cities

El IoT constituye uno de los pilares tecnológicos de las Smart Cities, al permitir la conexión de sensores, actuadores y sistemas distribuidos desplegados en el entorno urbano. Estos dispositivos, integrados con infraestructuras de comunicaciones y plataformas de gestión de datos, posibilitan la monitorización del estado de la ciudad y la optimización de servicios públicos como la movilidad, el medio ambiente, la energía, el agua o la gestión de residuos.

A diferencia de otros sistemas TIC tradicionales, el IoT urbano interactúa directamente con el entorno físico y con la ciudadanía, operando en condiciones exigentes y, en muchos casos, con dispositivos de recursos limitados y conectividad variable. Esta realidad condiciona el diseño de las soluciones, que deben ser robustas, energéticamente eficientes y capaces de operar de forma autónoma durante largos periodos, al tiempo que garantizan niveles adecuados de fiabilidad y seguridad.

Un ecosistema IoT en Smart Cities integra múltiples capas: dispositivos de campo, tecnologías de comunicación adaptadas a cada caso de uso (como redes LPWAN, tecnologías celulares o redes de corto alcance), pasarelas o nodos de borde y plataformas centrales de gestión y análisis de datos. Sobre esta base tecnológica se construyen aplicaciones municipales que permiten automatizar procesos, generar alertas, apoyar la toma de decisiones y ofrecer servicios más eficientes y transparentes a la ciudadanía.

5.1. Principales retos del IOT

La implantación de soluciones IoT en entornos urbanos no solo implica seleccionar tecnologías y desplegar dispositivos, también supone afrontar una serie de desafíos técnicos y normativos que condicionan el éxito del proyecto. Estos retos derivan de la complejidad del ecosistema IoT, caracterizado por su heterogeneidad, su escala masiva y su dependencia de infraestructuras compartidas. Además, la naturaleza distribuida de los dispositivos y la sensibilidad de los datos que generan obligan a integrar la ciberseguridad y la protección de la información desde las fases iniciales.

Comprender estos retos es esencial para diseñar arquitecturas robustas, garantizar la continuidad del servicio y cumplir con las obligaciones legales y regulatorias. A continuación, se detallan los principales desafíos que deben considerarse en cualquier iniciativa IoT para Smart Cities:

- **Heterogeneidad tecnológica e interoperabilidad**: El ecosistema IoT urbano integra dispositivos, plataformas y tecnologías de comunicación de múltiples fabricantes y generaciones. Esta diversidad dificulta la interoperabilidad entre sistemas, la integración de

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

datos y la evolución de los servicios, pudiendo generar dependencias tecnológicas que limiten la funcionalidad y el procesamiento de la información.

- **Escalabilidad y gestión del ciclo de vida**: Los proyectos IoT en Smart Cities suelen crecer de forma progresiva, incorporando nuevos dispositivos y casos de uso a lo largo del tiempo. Esto exige mecanismos eficaces para el aprovisionamiento, la monitorización, la actualización y la retirada segura de los dispositivos, así como una planificación que contemple la obsolescencia tecnológica y el mantenimiento a largo plazo.
- **Ciberseguridad**: La naturaleza distribuida del IoT urbano incrementa significativamente la superficie de ataque. Los dispositivos suelen tener recursos limitados, se encuentran en ubicaciones accesibles al público y utilizan redes compartidas, lo que hace imprescindible integrar la seguridad desde el diseño, garantizando la autenticación de los equipos, la protección de las comunicaciones y la gestión segura de credenciales.
- **Disponibilidad del servicio**: Aunque muchas aplicaciones IoT urbanas no son críticas en tiempo real, su indisponibilidad puede afectar a la calidad de los servicios municipales y a la confianza de la ciudadanía. La dependencia de tecnologías inalámbricas, en algunos casos operando en bandas no licenciadas, obliga a diseñar arquitecturas resilientes, con redundancia, monitorización continua y planes de contingencia.
- **Protección de la información y cumplimiento normativo**: El IoT urbano genera grandes volúmenes de datos que pueden incluir información sensible o indirectamente identificable. Para reducir riesgos, es necesario aplicar principios de minimización, anonimización o pseudonimización, así como garantizar la integridad y confidencialidad de los datos tanto en tránsito como en reposo. Además, deben definirse políticas claras sobre acceso, conservación y soberanía del dato, asegurando que la información se gestiona conforme a los estándares de seguridad aplicables.

  Junto a la protección técnica, los proyectos IoT deben cumplir estrictamente con la normativa vigente en materia de protección de datos y seguridad, incluyendo el Reglamento General de Protección de Datos (RGPD) y las regulaciones específicas aplicables

5.2. Clasificación de tecnologías

El ecosistema IoT urbano se sustenta en diferentes tecnologías de comunicación, cada una con características específicas que condicionan su idoneidad para determinados casos de uso. No existe una solución única que cubra todas las necesidades, la elección depende de factores como cobertura, consumo energético, capacidad de transmisión, coste y requisitos de seguridad. A continuación, se presenta una clasificación general de estas tecnologías:

- **LPWAN en bandas no licenciadas**: Incluye tecnologías como LoRaWAN y Sigfox, diseñadas para comunicaciones de muy bajo consumo y largo alcance, utilizando espectro radioeléctrico no licenciado. Son adecuadas para dispositivos que transmiten pequeños volúmenes de datos de forma esporádica, con limitaciones en la capacidad de respuesta y en la confirmación de entrega.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- **LPWAN celulares (estándares 3GPP)**: Engloba tecnologías como NB-IoT y LTE-M, que operan sobre redes móviles en espectro licenciado. Ofrecen mayor fiabilidad, seguridad y calidad de servicio, con capacidades adicionales como movilidad y comunicaciones bidireccionales en el caso de LTE-M. Son idóneas para aplicaciones críticas o que requieren gestión remota y soporte
- **Tecnologías 5G aplicadas a IoT urbano**: El estándar 5G introduce perfiles específicos para IoT: mMTC (del inglés, massive Machine Type Communications), orientado a la conexión masiva de dispositivos, y URLLC (del inglés, Ultra-Reliable Low Latency Communications), diseñado para aplicaciones que exigen alta fiabilidad y baja latencia, como control de tráfico en tiempo real o sistemas de emergencia.
- **Tecnologías de corto alcance**: Incluyen protocolos como IEEE 802.15.4/Zigbee y Bluetooth Low Energy (BLE), que permiten comunicaciones de bajo consumo en entornos reducidos, normalmente complementadas con pasarelas para conectividad hacia la nube. Son habituales en edificios inteligentes, iluminación y control de accesos.
- **Tecnologías complementarias**: Agrupan soluciones que, sin constituir la base principal de conectividad urbana, complementan a las tecnologías anteriores en escenarios específicos. Destaca Wi-Fi HaLow (IEEE 802.11ah), que ofrece mayor alcance y mejor penetración que el Wi-Fi tradicional, manteniendo un consumo optimizado y velocidades moderadas. Asimismo, se incluyen redes mesh propietarias y enfoques híbridos que combinan varias tecnologías para cubrir casos de uso concretos como gestión de alumbrado, riego urbano o movilidad compartida.

5.3. Criterios de selección

La elección de una tecnología IoT para entornos urbanos no debe basarse únicamente en la disponibilidad o el coste inicial, sino en un análisis integral que considere aspectos técnicos, operativos, económicos y de seguridad. Cada caso de uso presenta requisitos específicos que condicionan la idoneidad de la solución. A continuación, se describen los criterios fundamentales que deben evaluarse:

- **Cobertura y penetración**: Es necesario determinar si la tecnología ofrece alcance suficiente para cubrir la zona de despliegue, incluyendo entornos complejos como interiores, subterráneos o áreas con alta densidad urbana. La capacidad de penetración en edificios y la continuidad del servicio en movilidad son factores críticos en aplicaciones como transporte o teleasistencia.
- **Tráfico y latencia**: Debe analizarse el tamaño de los mensajes, la frecuencia de transmisión y la necesidad de confirmación de entrega. Tecnologías como Sigfox o LoRaWAN son adecuadas para comunicaciones esporádicas y mensajes cortos, mientras que LTE-M o 5G resultan más apropiadas para aplicaciones que requieren baja latencia y bidireccionalidad.
- **Consumo energético y autonomía**: La duración de la batería condiciona el coste operativo y la viabilidad del proyecto. Tecnologías LPWAN no licenciadas suelen ofrecer autonomías prolongadas, mientras que soluciones celulares, aunque más versátiles, implican un mayor consumo que debe compensarse con estrategias de optimización.
- **Seguridad y gobernanza**: Es imprescindible evaluar el modelo de autenticación, el cifrado de las comunicaciones y la capacidad de gestión remota. Además, debe considerarse el grado de

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

dependencia del operador y la existencia de acuerdos claros sobre niveles de servicio, gestión de incidentes y cumplimiento normativo.

- **Escalabilidad y ciclo de vida**: La tecnología seleccionada debe permitir la incorporación progresiva de dispositivos y casos de uso, con mecanismos para la actualización remota, la monitorización y la retirada segura. La falta de estas capacidades puede generar riesgos de seguridad y costes elevados a largo plazo.

6. Tecnologías LPWAN en bandas no licenciadas

6.1. LoRaWAN

LoRaWAN (del inglés, Long Range Wide Area Network) es una tecnología de comunicación inalámbrica diseñada para redes IoT que requieren conectar un gran número de dispositivos distribuidos geográficamente, con bajo consumo energético y a largas distancias. Está orientada a aplicaciones donde los dispositivos envían pequeñas cantidades de datos de forma esporádica, como lecturas de sensores, estados de equipos o avisos.

La comunicación se basa en una arquitectura de red en estrella. Los dispositivos finales, normalmente sensores alimentados por batería, transmiten sus mensajes mediante radio utilizando la modulación LoRa, que está optimizada para alcanzar largas distancias incluso en entornos urbanos densos. Estos mensajes pueden ser recibidos simultáneamente por uno o varios gateways, que funcionan como puntos de acceso y no toman decisiones sobre los datos, sino que simplemente los reenvían a través de una conexión IP, Internet o red privada, hacia el sistema central de la red.

En el núcleo de la red LoRaWAN se encuentra el servidor de red, que se encarga de gestionar los dispositivos, eliminar mensajes duplicados, controlar la seguridad, y decidir a través de qué gateway se envían las respuestas a los dispositivos. Sobre este servidor se sitúa el servidor de aplicaciones, que es donde los datos ya procesados se entregan a las aplicaciones finales para su visualización, análisis o integración con otros sistemas.

LoRaWAN opera en bandas de frecuencia de uso libre, como la banda de 868 MHz en Europa, lo que permite desplegar redes propias sin necesidad de licencias de espectro. Para cumplir con la normativa, la tecnología limita la velocidad de transmisión y el tiempo de uso del canal, lo que se traduce en un ancho de banda reducido y comunicaciones no continuas. A cambio, se consigue un consumo energético muy bajo, permitiendo que los dispositivos funcionen durante varios años con baterías de pequeña capacidad.

Desde el punto de vista funcional, LoRaWAN no está pensada para comunicaciones en tiempo real ni para transmitir grandes volúmenes de datos, sino para monitorización y control remoto no crítico. Por ello, se utiliza habitualmente en aplicaciones como ciudades inteligentes, gestión de servicios públicos, monitorización ambiental, agricultura, control de infraestructuras y telemetría distribuida.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

6.1.1. Arquitectura

La arquitectura de LoRaWAN se organiza en varios componentes bien definidos, que permiten la comunicación entre los dispositivos de campo y las aplicaciones finales. Estos componentes forman una cadena lógica que va desde el sensor hasta el sistema que utiliza la información:

ILUSTRACIÓN 1: ARQUITECTURA LORAWAN

❖ Dispositivos finales

Los dispositivos finales son los sensores o actuadores que se instalan en el entorno a monitorizar. Su función principal es recoger información (por ejemplo, temperatura, humedad, nivel, estado de un equipo) o ejecutar una acción simple, y transmitir esos datos a la red LoRaWAN.

Estos dispositivos suelen funcionar con batería y están diseñados para consumir muy poca energía. Para ello, permanecen la mayor parte del tiempo en reposo y solo activan la comunicación cuando necesitan enviar datos o recibir una respuesta puntual. La comunicación se realiza mediante radio, utilizando la tecnología LoRa.

❖ Gateways LoRaWAN

Los gateways son los puntos de acceso que reciben las señales de los dispositivos finales y las reenvían al servidor central. Según su ubicación y alcance, se pueden clasificar en:

- Gateways internos (picocell): Se instalan dentro de edificios o instalaciones cerradas y proporcionan cobertura limitada a espacios concretos, como oficinas, fábricas o almacenes.
- Gateways externos (macrocell): Se instalan en exteriores, en postes, azoteas o torres, y cubren áreas mucho más amplias, de varios kilómetros, llegando incluso a zonas rurales.

❖ Servidor de red (Network Server)

El servidor de red es el núcleo de la arquitectura LoRaWAN. Se encarga de coordinar y gestionar toda la comunicación de la red. Entre sus funciones principales se encuentran:

- Identificar y autenticar los dispositivos
- Eliminar mensajes duplicados recibidos por varios gateways
- Gestionar la seguridad a nivel de red
- Controlar los parámetros de comunicación (velocidad, potencia, frecuencia)
- Decidir por qué gateway se envían las respuestas hacia los dispositivos

Este componente es fundamental para garantizar el funcionamiento eficiente y seguro de la red.

❖ Servidor de red de Roaming (Network Server)

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Cuando un dispositivo se mueve entre redes diferentes, el servidor de red de roaming permite que siga enviando datos sin interrupciones.

- Recibe los datos de la red visitada y los reenvía al servidor de red de origen del dispositivo.
- Mantiene la seguridad y la integridad de la comunicación.
- Facilita que los dispositivos puedan moverse entre redes de distintos operadores o municipios sin perder conectividad.

❖ **Servidor join (Join Server)**

El servidor Join es el encargado de registrar los dispositivos en la red de forma segura. Cuando un dispositivo se enciende por primera vez o quiere conectarse, envía una solicitud de registro y el servidor verifica su identidad y genera las claves de seguridad necesarias para cifrar la comunicación.

Gracias a esto, solo los dispositivos autorizados pueden enviar y recibir información dentro de la red.

❖ **Servidor de aplicación (Application Server)**

El servidor de aplicaciones es el componente donde los datos que envían los dispositivos se transforman en información útil para las personas o sistemas que los usan.

- Recibe los datos desde el servidor de red y los descifra y decodifica, convirtiendo la información enviada por los sensores en valores comprensibles.
- Almacena y organiza los datos para que puedan ser consultados o analizados.
- Permite mostrarlos en paneles de control (dashboards) o integrarlos con otras aplicaciones y sistemas de gestión.
- Puede generar alertas o notificaciones automáticas cuando se detecta un valor fuera de lo esperado, como un nivel de agua crítico o una falla en un equipo.

6.1.2. Medidas de seguridad

La seguridad es un elemento fundamental de LoRaWAN, ya que la información transmitida por los dispositivos IoT puede ser sensible, y los dispositivos suelen estar desplegados en entornos abiertos o de difícil acceso. LoRaWAN implementa varias capas de seguridad para proteger la autenticidad, confidencialidad e integridad de los datos, así como para garantizar que solo los dispositivos autorizados puedan comunicarse con la red.

- **Registro seguro de dispositivos**: El primer evento en materia de seguridad se realiza en el servidor Join, encargado de registrar los dispositivos de manera segura antes de que puedan transmitir datos. Cuando un dispositivo se enciende por primera vez o se conecta a la red, envía una solicitud de registro. El servidor verifica su identidad y genera las claves de cifrado necesarias para que la comunicación sea segura. Gracias a este proceso, solo los dispositivos autorizados pueden formar parte de la red, evitando accesos no deseados o intrusiones.
- **Cifrado de los datos**: Una vez que el dispositivo está autorizado, los datos que transmite se protegen mediante cifrado AES-128. LoRaWAN utiliza dos niveles de cifrado independientes: la clave de red (NwkSKey), que asegura que los mensajes sean válidos y provengan de dispositivos autorizados, y la clave de aplicación (AppSKey), que garantiza que solo el servidor de

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

aplicaciones pueda descifrar y utilizar la información. De esta manera, incluso si un mensaje es interceptado durante la transmisión, no puede ser leído ni modificado por terceros.

- **Integridad de los mensajes**: Cada mensaje incluye un código de autenticación de mensaje (MIC) que permite al servidor detectar cualquier alteración o manipulación. Esta medida protege contra ataques de suplantación de identidad o intentos de enviar datos falsos a la red. De forma complementaria, cuando un dispositivo se conecta a una red diferente mediante roaming, el servidor de roaming asegura que los datos lleguen de manera segura al servidor de red de origen, manteniendo la integridad y confidencialidad de la comunicación.
- **Buenas prácticas y gestión de la red**: LoRaWAN contempla medidas adicionales para proteger toda la red. Por ejemplo, permite la renovación periódica de claves, lo que reduce el riesgo de comprometer la seguridad a largo plazo. Los operadores de red deben supervisar continuamente los gateways y dispositivos, detectar actividades sospechosas y configurar correctamente la potencia y frecuencia de transmisión para minimizar interferencias y vulnerabilidades

6.1.3. Consideraciones

Aunque LoRaWAN ofrece ventajas importantes como bajo consumo energético, gran alcance y facilidad de despliegue, existen ciertas limitaciones y aspectos a tener en cuenta al planificar su implementación. Conocerlos ayuda a diseñar redes más eficientes y adecuadas al tipo de aplicación.

- **Limitaciones de ancho de banda**: Uno de los principales aspectos es el ancho de banda. LoRaWAN está optimizada para transmitir pequeñas cantidades de datos de forma intermitente, por lo que no es adecuada para aplicaciones que requieran transferencias continuas de información o gran volumen de datos, como vídeo o audio en tiempo real. El ancho de banda reducido es una característica inherente a su diseño, que permite mantener el bajo consumo energético y el alcance extendido, pero limita la velocidad de comunicación.
- **Latencia**: LoRaWAN no está diseñada para aplicaciones que requieran respuesta inmediata o control en tiempo real. Los mensajes pueden experimentar retrasos de varios segundos o incluso minutos, especialmente en redes con muchos dispositivos o en configuraciones donde se utilizan las clases B o C de comunicación. Por ello, es ideal para monitorización, telemetría y control remoto no crítico, pero no para sistemas que dependan de reacciones instantáneas.
- **Disponibilidad y cobertura**: Estas características dependen tanto del número de gateways desplegados como de su ubicación (internos o externos) y del entorno. Las redes urbanas densas pueden presentar interferencias y obstáculos que afectan la señal, mientras que en áreas rurales el alcance puede ser mucho mayor. Es importante planificar la densidad de gateways y la topología de la red para garantizar que los dispositivos siempre puedan comunicarse de manera fiable.
- **Seguridad**: Es un aspecto crítico y una fortaleza de LoRaWAN, pero también requiere consideraciones de diseño. La red depende de claves de cifrado y autenticación, y es fundamental gestionar correctamente las credenciales, los servidores de red y de aplicaciones, así como mantener actualizadas las claves y monitorear la red para detectar accesos no

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

autorizados. Un mal manejo de la seguridad puede comprometer la confidencialidad o integridad de los datos.

- **Escalabilidad**: Aunque LoRaWAN permite conectar un gran número de dispositivos, cada red tiene límites prácticos de capacidad por gateway y por frecuencia disponible. En entornos con miles de sensores, es necesario planificar cuidadosamente la distribución de dispositivos, la densidad de gateways y la programación de transmisiones, para evitar colisiones, congestión de la red o pérdida de mensajes.

6.1.4. Casos de uso principales en Smart Cities

LoRaWAN ofrece soluciones para abordar diversos desafíos de las Smart Cities, gracias a su capacidad de cubrir grandes áreas con bajo consumo energético y costes reducidos de infraestructura. Entre sus principales aplicaciones destacan:

- Monitorización del entorno: sensores para calidad del aire, niveles de ruido, temperatura y humedad.
- Gestión de aparcamientos: detección de plazas libres y ocupadas.
- Seguridad de dispositivos y personas: seguimiento de activos urbanos, alarmas y sistemas de control de accesos.
- Alumbrado público: control inteligente de farolas, regulando intensidad y horarios según ocupación y condiciones ambientales.
- Gestión de residuos: monitorización de contenedores.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo LoRaWAN contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Monitorización de flotas de buses en San Sebastián
En San Sebastián se ha desplegado una solución basada en LoRaWAN para mejorar la monitorización de la flota de buses urbanos. Dado que las frecuencias de paso se sitúan entre 10 y 20 minutos, la pérdida de un bus puede suponer un retraso significativo para las personas usuarias del transporte público. El sistema se basa en la instalación de dispositivos IoT de geolocalización en cada bus, que transmiten periódicamente su ubicación y estado a través de la red LoRaWAN. En las paradas se han desplegado nodos receptores que permiten detectar la llegada de los buses y contabilizar cuántos se encuentran en espera, enviando esta información a la plataforma de gestión central. Los datos recogidos se procesan en una aplicación de gestión que permite estimar los tiempos de llegada, optimizar las rutas y adaptar el servicio en función de la demanda, especialmente en horas punta.

TABLA 2: CASO DE USO LORAWAN.

6.2. Sigfox

Sigfox es una tecnología de comunicación inalámbrica diseñada específicamente para aplicaciones IoT que requieren bajo consumo energético, transmisión de mensajes muy compactos y conectividad a largas distancias. Forma parte de las denominadas redes LPWAN y está pensada para escenarios donde

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

los dispositivos envían pequeñas cantidades de información de manera ocasional, como telemetrías, alertas o estados simples.

A diferencia de otras tecnologías IoT, Sigfox opera mediante una arquitectura completamente centralizada, gestionada por un operador de red. Esto significa que las personas usuarias no despliegan su propia infraestructura de comunicaciones, sino que utilizan la cobertura proporcionada por Sigfox o sus socios. Los dispositivos se conectan directamente a la red utilizando modulación de banda ultraestrecha (UNB), una técnica que permite alcanzar distancias muy elevadas con una potencia mínima de transmisión, incluso en entornos urbanos densos o con interferencias.

El funcionamiento de la red se basa principalmente en el envío de mensajes de subida (uplink) no confirmados, con un tamaño máximo de 12 bytes y un número limitado de transmisiones diarias. La comunicación en sentido descendente (downlink) es aún más restringida, ya que solo se permite un número muy reducido de mensajes y con un tamaño máximo de 8 bytes. Esto hace que Sigfox sea idóneo para casos de uso donde el dispositivo envía información de forma autónoma y no requiere un control frecuente desde la nube.

La simplicidad del modelo, tanto en la modulación como en las capacidades de mensajería, contribuye a reducir notablemente el consumo energético y el coste de los dispositivos, alargando la vida útil de las baterías durante varios años. Sin embargo, estas mismas características introducen limitaciones funcionales y de gobernanza, especialmente en aplicaciones que requieren comunicación bidireccional, configuraciones remotas o una mayor capacidad de datos.

Asimismo, Sigfox puede coexistir e integrarse con otras tecnologías dentro de soluciones IoT híbridas, combinándose con Wi-Fi, Bluetooth, NB-IoT, LTE-M o LoRaWAN, dependiendo de las necesidades de conectividad, cobertura y criticidad de cada caso de uso.

6.2.1. Arquitectura

La arquitectura de Sigfox está diseñada para ofrecer comunicación IoT de largo alcance y bajo consumo energético, enfocada en transmitir pequeños volúmenes de datos de manera intermitente. Aunque comparte objetivos similares con LoRaWAN, su enfoque es más centralizado y depende de una red gestionada por el operador Sigfox, lo que simplifica la infraestructura para la persona usuaria.

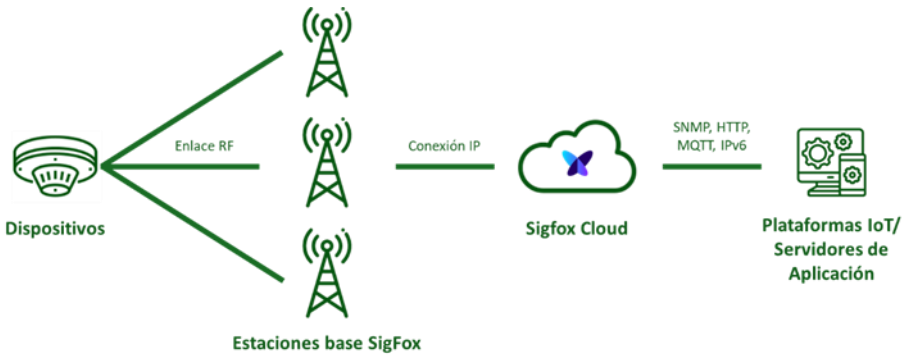

ILUSTRACIÓN 2: ARQUITECTURA SIGFOX

- **Dispositivos finales Sigfox**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Los dispositivos finales son los sensores o actuadores desplegados en el entorno a monitorizar. Están diseñados para bajo consumo, enviando información de manera intermitente y limitada a unos pocos mensajes al día. Su comunicación se realiza mediante radiofrecuencia en las bandas ISM libres (868 MHz en Europa).

A diferencia de LoRaWAN, los dispositivos Sigfox no gestionan gateways directamente ni deciden rutas de comunicación, simplemente transmiten sus mensajes, que son recogidos automáticamente por la red.

- **Estaciones base Sigfox**

En Sigfox, los gateways tradicionales no existen como en LoRaWAN. En su lugar, se utilizan estaciones base desplegadas por el operador. Estas estaciones cumplen varias funciones:

- Recibir los mensajes de los dispositivos finales en un área amplia.
- Reenviar los datos al backend de Sigfox de manera transparente.
- Proporcionar cobertura masiva gracias a su colocación estratégica en ciudades y zonas rurales.

Una diferencia clave es que cada mensaje puede ser recibido por varias estaciones simultáneamente, aumentando la fiabilidad de la red, sin que el dispositivo deba gestionar la redundancia.

Concretamente, en España, el operador responsable de la red Sigfox es UnaBiz, que gestiona la conectividad y delega la instalación de estaciones base en otros socios. En caso de desplegarse en otros países, cada uno dispone de operadores específicos.

- **Sigfox Cloud**

La Sigfox Cloud es el centro neural de la red. Todas las estaciones base envían los mensajes al backend central, que se encarga de:

- Filtrar duplicados cuando el mismo mensaje es recibido por varias estaciones.
- Gestionar la autenticación y seguridad de los dispositivos.
- Encaminar los datos al servidor de aplicaciones del cliente.

A diferencia de LoRaWAN, donde cada operador puede gestionar su propio servidor de red, Sigfox centraliza gran parte de la operación en su infraestructura gestionada. Esto simplifica la implementación, pero reduce la flexibilidad para redes privadas.

- **Servidor de aplicaciones (Application Server)**

El servidor de aplicaciones es donde los datos llegan finalmente y se transforman en información útil para la persona usuaria:

- Descifra y procesa los datos enviados por los dispositivos.
- Los almacena, organiza y pone a disposición mediante API o dashboards.
- Genera alertas o eventos según la información recibida.

Este componente es equivalente al servidor de aplicaciones de LoRaWAN, pero siempre recibe los datos ya filtrados y autenticados por la red Sigfox de la información recibida.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

6.2.2. Medidas de seguridad

La seguridad en Sigfox es un elemento central de la red, ya que los dispositivos IoT suelen estar desplegados en entornos abiertos y transmiten información sensible. A diferencia de otras tecnologías como LoRaWAN, Sigfox utiliza una infraestructura centralizada gestionada por el operador, lo que simplifica la gestión de la seguridad y garantiza que todos los mensajes sean procesados de manera segura desde el dispositivo hasta el servidor de aplicaciones.

- **Autenticación de dispositivos**: Antes de enviar cualquier mensaje, cada dispositivo final debe estar registrado y autorizado en la red. El backend de Sigfox verifica su identidad y asigna claves únicas que se utilizan para proteger la comunicación. Esto asegura que solo los dispositivos autorizados puedan transmitir información, evitando accesos no deseados o intentos de suplantación de identidad.
- **Cifrado de los datos**: Los datos transmitidos están protegidos mediante cifrado AES-128, garantizando la confidencialidad de la información desde el dispositivo hasta el servidor de aplicaciones de la persona usuaria. Incluso si un mensaje es interceptado durante la transmisión, no puede ser leído ni modificado sin las claves correspondientes.
- **Integridad de los mensajes**: El backend de Sigfox valida la integridad de cada mensaje, asegurando que la información no haya sido alterada durante su recorrido a través de las estaciones base. Esto protege frente a manipulaciones y garantiza que los datos recibidos sean confiables y consistentes.
- **Gestión centralizada de la red y los dispositivos**: El operador de Sigfox supervisa continuamente la red, detecta actividad sospechosa, controla las claves de los dispositivos y garantiza que solo los mensajes válidos lleguen al servidor de aplicaciones. Cuando un mensaje es recibido por varias estaciones base, el backend elimina duplicados y asegura que la información llegue íntegra y consistente.

6.2.3. Consideraciones

Antes de seleccionar Sigfox como tecnología de comunicación para un proyecto urbano, es importante tener en cuenta que existen varias limitaciones y consideraciones importantes que deben tenerse en cuenta al planificar un proyecto IoT con esta tecnología:

- **Dependencia del operador**: Sigfox es una red centralizada y gestionada por el proveedor, lo que significa que las persona usuarias dependen de la infraestructura del operador para cobertura, seguridad y funcionamiento. Si existe alguna falla en la red, los dispositivos no podrán enviar ni recibir mensajes hasta que se resuelva el problema, lo que limita la independencia frente a redes privadas.
- **Limitación en la comunicación uplink y downlink**: Los dispositivos Sigfox están diseñados para transmitir pequeñas cantidades de datos de manera intermitente. El uplink (dispositivo a servidor) permite enviar información con frecuencia limitada, mientras que el downlink (servidor a dispositivo) es aún más restringido, con un número limitado de mensajes por día. Esto hace que Sigfox no sea adecuado para aplicaciones que requieran control en tiempo real o alta capacidad de datos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- **Tolerancia a pérdidas de mensajes**: Los mensajes pueden ser recibidos por varias estaciones base, y el backend elimina duplicados y valida la integridad. Aunque esto mejora la confiabilidad, no garantiza que todos los mensajes lleguen siempre, por lo que es importante diseñar las aplicaciones para soportar cierta pérdida de información.
- **Seguridad**: Sigfox utiliza cifrado AES-128 de extremo a extremo y autenticación de dispositivos. Sin embargo, el cifrado de nivel de aplicación depende de cómo la persona usuaria configure sus datos y servidores. Esto significa que los clientes pueden implementar un cifrado adicional dentro de su aplicación para proteger aún más la información sensible, reforzando la confidencialidad más allá de la red.
- **Centralización de la red**: Esto implica que toda la gestión de dispositivos, claves y seguridad está bajo control del operador. Esto simplifica la administración, pero también significa que cualquier fallo en el backend o en la red central puede afectar a todos los dispositivos conectados. Es fundamental evaluar la disponibilidad del servicio y considerar estrategias de monitoreo o redundancia en los sistemas críticos.

6.2.4. Casos de uso principales en Smart Cities

Sigfox se emplea principalmente en escenarios donde se requiere una comunicación muy simple, de bajo coste y con un consumo energético mínimo, tales como:

- Sensores de alarma o detección de eventos puntuales: semáforos, monitorización de intensidad de las luces, gestión de aparcamiento o detección de aperturas no autorizadas.
- Sistemas de movilidad compartida: soluciones de alquiler de bicicletas (Bike Sharing) o seguimiento básico de flotas ligeras.
- Notificación de estados o incidencias no críticas: calidad del aire, humedad en cultivos municipales, niveles de llenado en papeleras inteligentes, entre otros.
- Gestión de activos y localización básica: Seguimiento de contenedores, equipamiento urbano o dispositivos móviles que no requieren actualizaciones frecuentes.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo Sigfox contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Monitorización inteligente de papeleras urbanas en Madrid
En Madrid se ha desplegado una solución basada en conectividad Sigfox para optimizar la gestión de la limpieza urbana mediante la monitorización inteligente de papeleras públicas. En una ciudad con alta densidad peatonal y grandes volúmenes de residuos, la falta de información en tiempo real sobre el estado de las papeleras puede provocar desbordamientos, ineficiencias operativas y un uso inadecuado de los recursos municipales. El sistema se fundamenta en la instalación de sensores IoT integrados en las papeleras del modelo “Cibeles”, capaces de medir el nivel de llenado mediante tecnología infrarroja y detectar parámetros adicionales como la temperatura interna. Estos dispositivos transmiten sus lecturas de forma periódica y ante eventos relevantes a través de la red 0G de Sigfox, lo que permite comunicaciones de bajo consumo, amplia cobertura urbana y mantenimiento reducido.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Monitorización inteligente de papeleras urbanas en Madrid
La información recogida se envía a una plataforma de gestión central utilizada por los servicios municipales de limpieza y las empresas concesionarias, donde se procesan los datos para planificar rutas de vaciado dinámicas, priorizar las papeleras próximas al desbordamiento y detectar incidencias de forma temprana.

TABLA 3: CASO DE USO SIGFOX.

7. Tecnologías LPWAN celulares (estándares 3GPP)

7.1. NB-IoT (Narrowband IoT)

NB-IoT (del inglés Narrowband Internet of Things) es una tecnología de comunicaciones IoT definida por 3GPP y diseñada para ofrecer conectividad de bajo consumo, amplia cobertura y transmisión de datos fiable utilizando la infraestructura celular existente. A diferencia de tecnologías LPWAN como LoRaWAN o Sigfox, que operan en bandas no licenciadas, NB-IoT utiliza espectro licenciado gestionado por operadores móviles, lo que permite garantizar niveles superiores de calidad de servicio, estabilidad y control del enlace.

NB-IoT funciona utilizando un canal de 180 kHz, que puede integrarse de tres formas en la red del operador:

- In-band, reutilizando parte del espectro LTE existente.
- Guard-band, empleando bandas de guarda entre portadoras LTE.
- Standalone, utilizando espectro dedicado, normalmente proveniente de antiguas bandas GSM.

Esto facilita el despliegue y garantiza cobertura en interiores y zonas subterráneas, donde otras tecnologías pueden tener problemas para llegar. La tecnología está optimizada para comunicaciones esporádicas con volúmenes reducidos de datos y requisitos de latencia moderada, priorizando la eficiencia energética y la conectividad confiable.

En cuanto a las capacidades de comunicación, NB-IoT soporta tráfico bidireccional, aunque está orientado a comunicaciones esporádicas y con un volumen moderado de datos. La latencia es mayor que en LTE tradicional, pero suficiente para aplicaciones de telemetría, monitorización remota o activación de comandos poco frecuentes. La existencia de acuerdos de nivel de servicio (SLA) y la gestión centralizada por parte del operador proporcionan una conectividad gestionada, predecible y con garantías, algo fundamental en sectores como servicios públicos o gestión urbana.

En el ámbito de las Smart Cities, NB-IoT se posiciona como una alternativa que combina la cobertura y confiabilidad de las redes móviles con el bajo consumo de las tecnologías LPWAN. Frente a opciones no licenciadas, ofrece mayor robustez y soporte contractual, aunque a costa de una mayor dependencia del operador y un coste por dispositivo más ligado a modelos de suscripción.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

7.1.1. Arquitectura

La arquitectura de NB-IoT está diseñada para ofrecer conectividad IoT confiable, de bajo consumo y amplia cobertura utilizando la infraestructura de red celular existente. A diferencia de redes LPWAN como LoRaWAN o Sigfox, NB-IoT funciona en espectro licenciado, gestionado por operadores de telecomunicaciones, lo que permite garantizar la calidad de servicio, seguridad y disponibilidad de la comunicación.

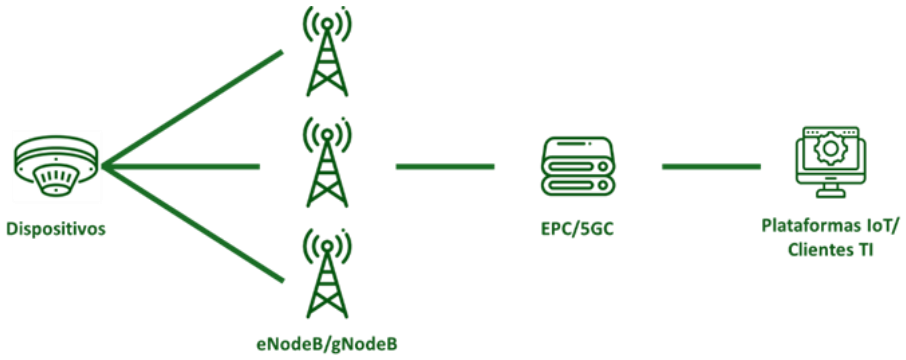

ILUSTRACIÓN 3: ARQUITECTURA NB-IOT

- **Dispositivos finales NB-IoT**

Los dispositivos finales son los sensores o actuadores que recogen información o ejecutan acciones simples. Están diseñados para bajo consumo energético, permitiendo que las baterías duren varios años.

Los dispositivos NB-IoT se comunican directamente con la red celular, enviando y recibiendo mensajes cortos de manera intermitente. A diferencia de Sigfox, los dispositivos no dependen de estaciones base independientes ni gateways privados, se conectan a la infraestructura existente de LTE/5G.

- **Infraestuctura de acceso radio (eNodeB/gNodeB)**

El dispositivo se conecta a la estación base, que puede ser un eNodeB en LTE o un gNodeB en 5G. Estas estaciones cumplen varias funciones:

- Recibir y transmitir mensajes de los dispositivos finales.
- Gestionar el enlace radio para asegurar cobertura, eficiencia energética y confiabilidad.
- Integrarse con el núcleo de red para encaminar los datos hacia los servidores de red y aplicaciones.

Las estaciones base permiten una gran cobertura en interiores y áreas subterráneas, gracias a la banda estrecha y técnicas de repetición de señal de NB-IoT.

- **Núcleo de red del operador (EPC/5GC)**

El core network es el núcleo de la red celular NB-IoT y se encarga de:

- Gestión de la movilidad y autenticación de los dispositivos.
- Enrutamiento de datos entre estaciones base y servidores de aplicaciones.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Control de calidad de servicio, seguridad y confiabilidad, incluyendo cifrado y autenticación end-to-end.

En 5G, esta función es realizada por el 5G Core, ofreciendo aún más flexibilidad y capacidades de segmentación de red (network slicing) para aplicaciones IoT críticas.

- **Servidor de aplicaciones (Application Server)**

El servidor de aplicaciones es el componente donde los datos transmitidos por los dispositivos se procesan y se transforman en información útil para la persona usuaria. La información enviada por los sensores se descifra y decodifica, se almacena y organiza para su consulta o integración con otras aplicaciones, y se generan alertas, informes o acciones automáticas según los valores recibidos.

7.1.2. Medidas de seguridad

La seguridad en NB-IoT se basa en los mecanismos de LTE y 5G, adaptados para dispositivos IoT de bajo consumo. Su diseño garantiza que los datos transmitidos sean confiables, íntegros y confidenciales, incluso en redes públicas gestionadas por operadores.

- **Espectro licenciado**: NB-IoT opera sobre espectro licenciado, lo que proporciona un entorno radio controlado por el operador móvil. Esto reduce significativamente el riesgo de interferencias, ataques de denegación de servicio y escuchas no autorizadas, ofreciendo un nivel de protección superior al de tecnologías LPWAN de bandas libres como LoRaWAN o Sigfox.
- **Autenticación de dispositivos**: Cada dispositivo final está registrado en la red mediante una SIM o eSIM, que almacena las credenciales y claves criptográficas necesarias para conectarse. Esto incluye:
    - Identidad del suscriptor (IMSI): permite que la red reconozca de manera única al dispositivo.
    - Clave de autenticación (K): se utiliza para generar las claves de cifrado e integridad en el enlace radio.
    - Algoritmos de cifrado y autenticación: la SIM/eSIM almacena las funciones necesarias para aplicar AES-128 o ZUC, según la red y el operador.

  Gracias a esto, la red puede verificar que solo dispositivos autorizados puedan comunicarse, evitando accesos no deseados o suplantaciones de identidad.
- **Cifrado de datos**: Los datos transmitidos se protegen mediante cifrado de extremo a extremo, utilizando algoritmos estándar como AES-128 o ZUC, según la red y el operador. Este cifrado garantiza la confidencialidad de la información entre el dispositivo final y el core network, evitando que los mensajes puedan ser leídos por terceros durante la transmisión. Además, el core network verifica la integridad de los mensajes, asegurando que la información no haya sido alterada antes de llegar al servidor de aplicaciones.
- **Cifrado adicional a nivel de aplicación**: NB-IoT permite implementar un cifrado adicional a nivel de aplicación, ofreciendo una capa extra de seguridad para los datos sensibles que se procesan en los servidores del cliente. Esto es especialmente recomendable en aplicaciones

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

críticas, donde la información debe permanecer protegida incluso después de salir del ámbito de la red operadora.

- **Gestión centralizada por el operador**: La gestión de seguridad en NB-IoT es centralizada por el operador de telecomunicaciones. Esto incluye la actualización remota de credenciales, el monitoreo de la red para detectar actividad sospechosa y la garantía de disponibilidad y calidad de servicio. La combinación de SIM/eSIM segura, cifrado de extremo a extremo y gestión centralizada ofrece una red robusta, confiable y adecuada para aplicaciones IoT que requieren alta seguridad y disponibilidad

7.1.3. Consideraciones

Antes de seleccionar NB-IoT como tecnología de comunicación para un proyecto de Smart Cities, es necesario tener en cuenta una serie de aspectos clave:

- **Dependencia del operador**: NB-IoT funciona sobre espectro licenciado, por lo que los dispositivos dependen de la infraestructura celular del operador para conectarse y transmitir datos. Esto significa que la disponibilidad y el rendimiento de la red dependen directamente de la calidad del servicio del proveedor, y cualquier interrupción en la red puede afectar a todos los dispositivos conectados.
- **Acuerdos contractuales**: Los despliegues de NB-IoT requieren acuerdos contractuales por el uso del espectro y servicios asociados, lo que introduce costes adicionales y la necesidad de compromisos legales. Los proyectos están sujetos a acuerdos de nivel de servicio (SLA), que garantizan la cobertura y la confiabilidad, pero también pueden generar vendor lock-in, limitando la flexibilidad para cambiar de operador sin modificar la infraestructura o la suscripción.
- **Latencia**: NB-IoT está optimizado para transmisiones esporádicas y volúmenes de datos reducidos, por lo que no es adecuada para aplicaciones que requieran respuestas en tiempo real o control inmediato. La latencia puede variar dependiendo de la carga de la red y la configuración del operador, por lo que es importante evaluar los requisitos de cada aplicación antes de adoptarla.
- **Control sobre la red**: La tecnología implica la delegación de gran parte de la gestión al operador, incluyendo la autenticación de dispositivos, la administración de claves, el mantenimiento de la red y la seguridad de extremo a extremo. Esto simplifica la operación para la persona usuaria, pero también significa que la capacidad de control directo sobre la red es limitada.
- **Costes**: Los costes asociados no se limitan al despliegue de dispositivos. Existen tarifas de conexión y suscripción, costes por el uso de espectro licenciado y posibles gastos adicionales por servicios de monitoreo o integración. Además, el vendor lock-in puede incrementar los costes futuros si se desea migrar a otro operador o tecnología, ya que la red NB-IoT está estrechamente integrada con la infraestructura del proveedor.

7.1.4. Casos de uso principales en Smart Cities

NB-IoT se emplea habitualmente en servicios urbanos que requieren una conectividad fiable, segura y gestionada, tales como:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Lectura remota de contadores: Agua, gas y electricidad, con envío periódico de datos y alertas por consumo anómalo.
- Monitorización de infraestructuras críticas municipales: Puentes, túneles, estaciones de bombeo, alumbrado público y otros activos que requieren supervisión continua.
- Sensores en entornos subterráneos o de difícil cobertura: Aparcamientos subterráneos, redes de saneamiento, depósitos y galerías técnicas.
- Gestión de activos urbanos de larga vida útil: Contenedores, papeleras inteligentes, equipamiento municipal y sistemas de riego.
- Aplicaciones de movilidad y transporte: Seguimiento básico de flotas, monitorización de bicicletas compartidas o estaciones de carga eléctrica.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo NB-IoT contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Telelectura inteligente de contadores de agua en Gandía
El Ayuntamiento de Gandía, en colaboración con operadores móviles, desplegó una solución basada en NB-IoT para la lectura remota de contadores de agua, con el objetivo de mejorar la eficiencia del servicio y reducir pérdidas. Esta tecnología permite conectar dispositivos en interiores y zonas subterráneas, donde otras redes presentan limitaciones, garantizando una cobertura fiable y un consumo energético mínimo. El sistema recoge datos horarios de los contadores y los envía a una plataforma central, donde se procesan para detectar fugas, prever la demanda y optimizar la distribución. Además, la plataforma permite generar alertas automáticas ante consumos anómalos, mejorar la planificación de mantenimiento y ofrecer información detallada para la toma de decisiones. Gracias a esta conectividad, se ha logrado reducir desplazamientos innecesarios, mejorar la gestión operativa y alcanzar ahorros significativos en el consumo de agua. Este proyecto se ha convertido en un referente en la gestión inteligente del ciclo del agua, demostrando cómo NB-IoT ofrece funcionalidades claves para servicios urbanos críticos y sostenibles. Además, la infraestructura creada abre la puerta a otros usos en la ciudad, como la monitorización de riego, control de calidad del agua o integración con sistemas de eficiencia energética.

TABLA 4: CASO DE USO NB-IOT.

7.2. LTE-M (LTE Cat-M1)

LTE-M (del inglés Long Term Evolution for Machines) es una tecnología IoT estandarizada por 3GPP, diseñada para ofrecer conectividad confiable y eficiente sobre las redes celulares LTE y 5G existentes. Al igual que NB-IoT, LTE-M opera en espectro licenciado, lo que permite garantizar seguridad, calidad de servicio y disponibilidad, aunque introduce una dependencia del operador.

A diferencia de NB-IoT, LTE-M está optimizada para aplicaciones que requieren mayor ancho de banda, movilidad y comunicación bidireccional. Los dispositivos finales se conectan directamente a la red celular mediante las estaciones base LTE o 5G, lo que permite que los datos se envíen y reciban de forma

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

rápida y confiable, incluso cuando los dispositivos se mueven entre distintas celdas de cobertura. Esta capacidad de handover hace que LTE-M sea ideal para seguimiento de vehículos, transporte inteligente y activos móviles.

LTE-M también soporta interacción en tiempo real y voz sobre IP (VoLTE), lo que la diferencia de otras tecnologías LPWAN como NB-IoT o Sigfox, que son principalmente unidireccionales o de baja frecuencia de transmisión. Esto permite aplicaciones donde la latencia es crítica y se requieren respuestas rápidas del dispositivo, sin sacrificar completamente la eficiencia energética.

En términos de consumo, LTE-M mantiene un enfoque de bajo consumo, aunque ligeramente superior al de NB-IoT, compensado por mayor velocidad de transmisión y flexibilidad funcional. Esto permite que los dispositivos puedan mantenerse activos cuando se requiere comunicación frecuente o bidireccional, y mantenerse en reposo durante periodos largos cuando no transmiten, prolongando la vida útil de la batería.

Desde una perspectiva funcional, LTE-M es ideal para aplicaciones de Smart Cities que combinan movilidad, capacidad de datos y seguridad, como seguimiento de flotas, gestión de transporte público, sistemas de emergencia o dispositivos críticos que requieren conectividad confiable, rápida y predecible. Su integración con la red celular permite ofrecer garantías de calidad de servicio, aunque al igual que NB-IoT, implica dependencia del operador y posibles costes asociados o vendor lock-in.

7.2.1. Arquitectura

La arquitectura de LTE-M está diseñada para ofrecer conectividad IoT confiable, eficiente y flexible utilizando la infraestructura de redes LTE y 5G existentes. Al igual que NB-IoT, opera sobre espectro licenciado, lo que permite garantizar seguridad, calidad de servicio y cobertura confiable, aunque introduce dependencia del operador:

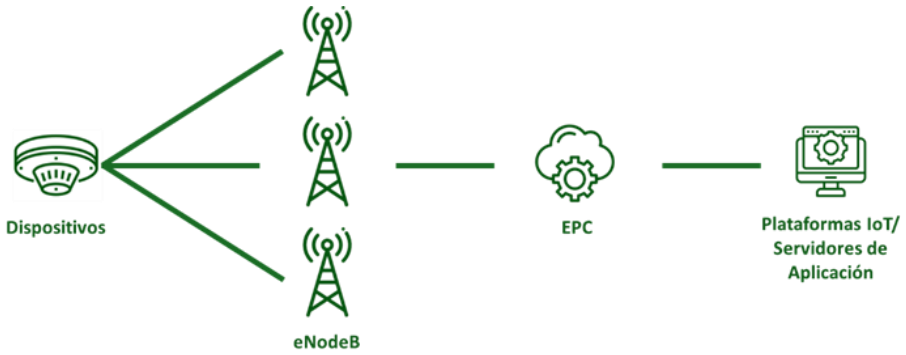

ILUSTRACIÓN 4: ARQUITECTURA LTE-M

- **Dispositivos finales LTE**

Los dispositivos finales son los sensores, actuadores o equipos móviles que recopilan y transmiten información. Están diseñados para bajo consumo energético, pero con capacidad de transmisión más rápida y bidireccional que NB-IoT.

Estos dispositivos se conectan directamente a la red celular LTE o 5G, lo que les permite enviar y recibir datos de manera confiable incluso cuando se desplazan entre distintas celdas (soporte de movilidad y

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

handover). Esto los hace adecuados para aplicaciones como seguimiento de vehículos, transporte inteligente y dispositivos críticos móviles.

- **Infraestuctura de acceso radio (eNodeB/gNodeB)**

El dispositivo final se comunica con la estación base LTE (eNodeB) o 5G (gNodeB), que actúa como puerta de enlace entre el dispositivo y la red central.

Las estaciones base cumplen varias funciones:

- Gestionar el enlace radio para asegurar cobertura y confiabilidad.
- Transmitir y recibir mensajes bidireccionales de los dispositivos.
- Permitir el handover entre celdas, asegurando continuidad en la comunicación cuando los dispositivos están en movimiento.
- Encaminarlos hacia el core network para su procesamiento y entrega al servidor de aplicaciones.
- **Núcleo de red del operador (EPC)**

El core network, idéntico al de la red celular NB-, se encarga de:

- Gestión de la movilidad y autenticación de los dispositivos.
- Enrutamiento de datos entre estaciones base y servidores de aplicaciones.
- Control de calidad de servicio, seguridad y confiabilidad, incluyendo cifrado y autenticación end-to-end.

En 5G, esta función es realizada por el 5G Core, ofreciendo aún más flexibilidad y capacidades de segmentación de red (network slicing) para aplicaciones IoT críticas.

- **Plataforma IoT/Clientes TI**

Los datos se integran en plataformas IoT (del operador o de terceros), donde se procesan para generar alertas, visualizaciones y análisis. Estas plataformas permiten la gestión del ciclo de vida de dispositivos, actualizaciones remotas y conexión con aplicaciones municipales mediante APIs.

7.2.2. Medidas de seguridad

LTE-M comparte los fundamentos de seguridad del ecosistema LTE, con algunas particularidades derivadas de sus capacidades ampliadas.

- **Autenticación y cifrado**: Al igual que NB-IoT, LTE-M utiliza mecanismos robustos de autenticación basados en SIM/eSIM, junto con cifrado de las comunicaciones conforme a los estándares 3GPP. Esto proporciona una base sólida para proteger las transmisiones frente a interceptación y suplantación de identidad.
- **Soporte a comunicaciones bidireccionales**: La capacidad de mantener comunicaciones más frecuentes y con menor latencia permite gestionar los dispositivos LTE-M de forma activa, incluyendo actualizaciones remotas y monitorización continua. Sin embargo, esta ventaja también requiere controles estrictos para evitar accesos no autorizados o uso indebido de los canales de comunicación.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- **Ciclo de vida y actualizaciones**: Los dispositivos LTE-M suelen ofrecer capacidades avanzadas de actualización remota, lo que es positivo para corregir vulnerabilidades. No obstante, la administración debe establecer políticas claras sobre pruebas, despliegue de actualizaciones y gestión de incidentes asociados a fallos de software, evitando riesgos derivados de dispositivos obsoletos o comprometidos.
- **Gestión de la movilidad:** LTE-M soporta handover entre celdas, lo que facilita el uso en vehículos y activos en movimiento. Desde el punto de vista de seguridad, esto introduce consideraciones adicionales sobre protección de la privacidad, seguimiento y gestión segura de identidades en distintos contextos de red.
- **Dependencia del operador y gobernanza:** Como ocurre con NB-IoT, gran parte de la seguridad depende del operador de telecomunicaciones. Para proyectos municipales, es esencial que esta dependencia se gestione mediante acuerdos claros, definiendo responsabilidades, tiempos de respuesta ante incidentes y alineación con los requisitos regulatorios del sector público.

7.2.3. Consideraciones

Antes de seleccionar LTE-M como tecnología de comunicación para un proyecto de Smart Cities, es necesario tener en cuenta una serie de aspectos clave:

- **Dependencia del operador:** LTE-M se apoya en redes celulares gestionadas por operadores, lo que implica que la administración no tiene control directo sobre la infraestructura ni sobre la planificación radioeléctrica. Esta dependencia requiere acuerdos claros que definan niveles de servicio, tiempos de respuesta ante incidencias y mecanismos de notificación.
- **Disponibilidad y calidad del servicio:** El uso de espectro licenciado permite ofrecer mayor estabilidad y calidad que las tecnologías en bandas no licenciadas. Sin embargo, estas garantías están condicionadas a los contratos y políticas del operador, por lo que deben evaluarse cuidadosamente en aplicaciones críticas.
- **Latencia y movilidad:** LTE-M está diseñada para ofrecer menor latencia que NB-IoT y soporta movilidad mediante handover entre celdas, lo que la hace adecuada para dispositivos en movimiento (flotas, teleasistencia). No obstante, no alcanza los niveles de latencia ultra baja que ofrece 5G URLLC, por lo que no es apta para aplicaciones de control en tiempo real.
- **Consumo energético y autonomía:** Aunque LTE-M está optimizada para IoT, su consumo energético es superior al de NB-IoT o LoRaWAN. Esto debe considerarse en dispositivos alimentados por batería, especialmente en despliegues masivos, donde la autonomía es un factor crítico.
- **Seguridad y gobernanza:** LTE-M hereda los mecanismos de seguridad del ecosistema celular, incluyendo autenticación mediante SIM/eSIM y cifrado conforme a los estándares 3GPP. Aun así, la administración debe establecer políticas claras para la gestión del ciclo de vida, actualizaciones remotas y protección de datos, evitando riesgos derivados de dispositivos obsoletos o comprometidos.
- **Escalabilidad y costes a largo plazo:** El despliegue masivo de dispositivos LTE-M implica gestionar eficientemente las SIM y los contratos asociados. A largo plazo, los costes recurrentes y el riesgo de bloqueo tecnológico (vendor lock-in) deben considerarse en la planificación estratégica del proyecto.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

7.2.4. Casos de uso principales en Smart Cities

LTE-M se emplea habitualmente en servicios urbanos que requieren conectividad fiable, movilidad y comunicaciones bidireccionales, tales como:

- Gestión de flotas municipales y vehículos conectados: Gestión de transporte público, vehículos municipales y servicios de emergencia, con capacidad para transmitir datos en movimiento gracias al soporte de handover.
- Dispositivos portátiles y wearables: Sistemas de teleasistencia, pulseras de emergencia y dispositivos para personal de campo, aprovechando la baja latencia y la posibilidad de voz sobre IP (VoLTE).
- Sensores en entornos dinámicos: Aplicaciones que combinan movilidad y datos en tiempo real, como bicicletas compartidas, control de aparcamientos o gestión de residuos en rutas móviles.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo LTE-M contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Balizas inteligentes de emergencia DGT
Las nuevas balizas de emergencia conectadas de la DGT utilizan LTE-M para transmitir su ubicación y estado en tiempo real a los sistemas de gestión del tráfico. Esta tecnología ofrece baja latencia y conectividad fiable, incluso en zonas con cobertura limitada, lo que permite alertar automáticamente a los centros de control cuando se produce una incidencia en carretera. Gracias a LTE-M, las balizas pueden mantener comunicaciones bidireccionales, confirmando la recepción de mensajes y permitiendo ajustes remotos sin intervención física. Además, su diseño optimizado para IoT garantiza consumo energético reducido y autonomía prolongada, características esenciales para dispositivos que deben funcionar en condiciones adversas. Estas balizas, conocidas como dispositivos V16, sustituyen a los triángulos tradicionales y se fijan en el punto más alto del vehículo para emitir luz ámbar visible a más de un kilómetro. Incorporan un módulo celular con SIM/eSIM que envía datos de geolocalización y estado mientras permanecen activadas. A partir del 1 de enero de 2026, su uso es obligatorio en España, integrándose en la plataforma DGT 3.0 para mejorar la seguridad vial y la gestión inteligente del tráfico.

TABLA 5: CASO DE USO LTE-M.

8. Tecnologías 5G aplicadas a IoT urbano

8.1. 5G mMTC (massive Machine Type Communications)

El perfil mMTC (massive Machine Type Communications) definido en el estándar 5G está diseñado para soportar la conexión simultánea de millones de dispositivos IoT por kilómetro cuadrado. Esta capacidad responde a la creciente densidad de sensores y actuadores en entornos urbanos, donde se requiere una infraestructura capaz de gestionar grandes volúmenes de tráfico con eficiencia y estabilidad. A diferencia de tecnologías anteriores, mMTC prioriza la escalabilidad y la optimización del consumo energético, permitiendo que dispositivos de bajo coste y batería limitada se integren en redes de alta capacidad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

mMTC opera sobre espectro licenciado y aprovecha la arquitectura avanzada de 5G, ofreciendo una cobertura amplia y una gestión inteligente del tráfico masivo. Aunque no está orientado a aplicaciones críticas en tiempo real, garantiza una transmisión fiable para datos periódicos o esporádicos, incluso en escenarios con alta congestión. Esto lo convierte en una solución ideal para servicios como monitorización ambiental, gestión de residuos, alumbrado inteligente y control de infraestructuras urbanas, donde la prioridad es la conectividad masiva más que la latencia ultra baja.

Concretamente, la gestión masiva de dispositivos se apoya en el concepto de network slicing, que permite crear segmentos lógicos dentro de la red con recursos y políticas dedicadas. Cada slice se configura para atender un tipo de servicio específico, en el caso de mMTC, se prioriza la conexión simultánea de millones de dispositivos con tráfico reducido, garantizando aislamiento frente a otros servicios como banda ancha móvil (eMBB) o comunicaciones críticas (URLLC). Esto asegura que la conectividad IoT masiva no afecte al rendimiento global de la red y que se mantengan parámetros de calidad y seguridad adaptados a este perfil.

8.1.1. Arquitectura

En un despliegue urbano típico basado en 5G mMTC , intervienen varios elementos que trabajan de manera coordinada para soportar conectividad masiva, segura y eficiente para dispositivos IoT:

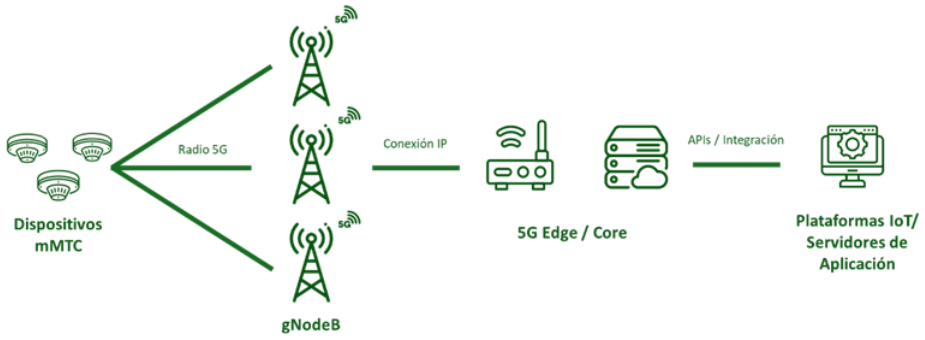

ILUSTRACIÓN 5: ARQUITECTURA 5G MMTC

- **Dispositivos (UE IoT)**

Los dispositivos finales incluyen sensores y actuadores instalados en infraestructuras urbanas, equipados con módulos compatibles con 5G mMTC. Están diseñados para operar durante largos periodos con bajo consumo energético y cuentan con capacidades de seguridad avanzadas, como autenticación reforzada y actualizaciones remotas seguras. Su función principal es recoger datos del entorno urbano o controlar activos, transmitiéndolos de forma eficiente y confiable hacia la red 5G.

- **Red de acceso radio 5G (gNodeB)**

Las estaciones base 5G proporcionan la conectividad inalámbrica a los dispositivos y soportan perfiles específicos para comunicaciones masivas de IoT. Estas infraestructuras son gestionadas por los operadores de telecomunicaciones, quienes controlan la planificación radioeléctrica, la configuración de la red y la optimización del tráfico. La administración usuaria no tiene acceso directo, pero se beneficia de la escala, cobertura y fiabilidad que ofrece la red 5G.

- **Núcleo de red 5G (5GC)**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

El 5G Core incluye todos los sistemas de control, autenticación, gestión de sesiones, seguridad y orquestación necesarios para gestionar grandes volúmenes de dispositivos y servicios IoT. Permite una gestión automatizada, asegurando que los dispositivos puedan conectarse, transmitir datos y recibir comandos de manera confiable y segura, pero permanece bajo control exclusivo del operador.

- **Slice**

Un slice es un segmento lógico de la red creado específicamente para mMTC. Cada slice cuenta con recursos dedicados y políticas adaptadas, garantizando aislamiento, calidad de servicio y seguridad para las comunicaciones masivas de IoT, sin interferir con otros servicios de la misma infraestructura 5G.

- **MEC/Edge**

La computación en el borde MEC (del inglés, Multi-access Edge Computing) permite procesar y filtrar datos cerca de la fuente, reduciendo la latencia y el tráfico hacia la nube central. Aunque su implementación es opcional, se recomienda en Smart Cities para mejorar la resiliencia, eficiencia y rapidez en la toma de decisiones a partir de los datos generados por los dispositivos IoT.

- **Plataformas IoT y servidores de aplicación**

Los datos generados por los dispositivos son entregados a plataformas IoT del operador o de terceros, desde donde se integran con los sistemas municipales. Estas plataformas permiten tratar grandes volúmenes de información, correlacionar datos de distintas fuentes y explotar analítica avanzada, facilitando la toma de decisiones estratégicas y operativas en entornos urbanos inteligentes.

8.1.2. Medidas de seguridad

La seguridad en 5G mMTC se apoya en los avances introducidos por la arquitectura 5G, reforzando los mecanismos ya existentes en generaciones anteriores.

- **Autenticación y gestión de identidades a gran escala**: 5G introduce mejoras significativas en los procedimientos de autenticación, permitiendo una gestión eficiente y segura de identidades en escenarios con un número masivo de dispositivos. Cada dispositivo utiliza credenciales seguras basadas en el estándar 5G-AKA, con identidades protegidas mediante SUPI/SUCI para evitar exposición en claro. Esto garantiza autenticación mutua entre dispositivo y red, reduciendo el riesgo de suplantación.
- **Cifrado y protección de datos**: Las comunicaciones en 5G mMTC están protegidas mediante mecanismos de cifrado avanzados tanto en el plano de usuario como en el plano de control. Estos mecanismos reducen de forma significativa el riesgo de interceptación, manipulación o análisis de tráfico por parte de terceros no autorizados.
- **Aislamiento lógico y segmentación:** La arquitectura 5G permite mecanismos de segmentación lógica de la red que facilitan el aislamiento entre distintos tipos de servicios y dispositivos.

  No obstante, cada slice debe configurarse con políticas específicas de aislamiento, evitando que el tráfico masivo de IoT afecte a otros servicios. Es fundamental garantizar que los recursos asignados al slice mMTC no puedan ser explotados para ataques de denegación de servicio.
- **Gestión de incidentes y visibilidad:** La complejidad y automatización de las redes 5G requieren capacidades avanzadas de monitorización y respuesta ante incidentes. En el caso de 5G mMTC,

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

la detección de anomalías y la gestión de incidentes recaen principalmente en el operador, pero la administración debe disponer de visibilidad suficiente sobre el estado del servicio y los eventos relevantes de seguridad.

- **Ciclo de vida y actualizaciones:** Los dispositivos 5G mMTC están concebidos para ciclos de vida prolongados y suelen soportar mecanismos de actualización remota segura. Sin embargo, la existencia de estas capacidades no garantiza su uso efectivo si no se definen políticas claras de mantenimiento, validación y despliegue de actualizaciones.

  La retirada segura de dispositivos, la desactivación de credenciales y la gestión de equipos obsoletos deben formar parte de los procedimientos estándar de la administración.

8.1.3. Consideraciones

Antes de seleccionar 5G mMTC como tecnología de comunicación para un proyecto de Smart City, es necesario evaluar una serie de aspectos desde el punto de vista técnico, organizativo y de ciberseguridad.

- **Madurez tecnológica:** Aunque 5G mMTC forma parte del estándar 5G, su grado de implantación práctica puede variar significativamente según el territorio y el operador. Es fundamental evaluar la disponibilidad real del servicio y de dispositivos compatibles antes de su adopción.
- **Dependencia del operador:** La administración depende en gran medida del operador de telecomunicaciones para la conectividad, la seguridad de la red y la gestión de incidentes. Esta dependencia debe ser gestionada mediante contratos claros y mecanismos de supervisión adecuados.
- **Complejidad operativa:** La elevada automatización y virtualización de las redes 5G introduce una complejidad técnica que limita la capacidad de intervención directa por parte de la administración. Esto exige una gobernanza sólida y una clara definición de responsabilidades.
- **Costes y planificación a largo plazo:** El despliegue de soluciones basadas en 5G mMTC implica costes recurrentes asociados a conectividad, gestión de SIM y servicios del operador. Estos factores deben considerarse en la planificación estratégica y presupuestaria de los proyectos municipales.
- **Seguridad y control:** Aunque la tecnología ofrece mecanismos de seguridad avanzados, la administración debe asumir que una parte relevante del control está delegada. La seguridad efectiva dependerá tanto de la tecnología como de la relación contractual y operativa con los proveedores.

8.1.4. Casos de uso principales en Smart Cities

5G mMTC está orientado a escenarios de sensorización masiva en entornos urbanos, entre los que destacan:

- Redes extensas de sensores ambientales y urbanos: Centros urbanos, áreas comerciales o espacios públicos extensos.
- Monitorización distribuida de infraestructuras municipales: Sensores integrados en pavimentos, fachadas, mobiliario urbano o elementos estructurales.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Servicios de ciudad inteligente con gran densidad de nodos: Integración de múltiples servicios municipales (medioambiente, mantenimiento, movilidad, energía) sobre una única red 5G.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo 5G mMTC contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Monitorización ambiental con 5G mMTC en Barcelona
En Barcelona se ha desplegado un piloto que utiliza 5G mMTC para conectar miles de sensores distribuidos en la ciudad, con el objetivo de monitorizar parámetros ambientales como calidad del aire, temperatura, humedad y niveles de ruido. Estos dispositivos envían datos pequeños y esporádicos a través de la red 5G, aprovechando el perfil mMTC para soportar una densidad muy elevada de conexiones sin congestionar la red. Los datos se procesan en nodos de computación en el borde (MEC) para filtrar información y generar alertas locales, reduciendo la latencia y el tráfico hacia la nube. Posteriormente, se integran en plataformas municipales para análisis avanzado y toma de decisiones, permitiendo ajustar políticas de movilidad, riego y control de emisiones en tiempo real.

TABLA 6: CASO DE USO 5G MMTC.

8.2. 5G URLLC (Ultra-Reliable Low Latency Communications)

5G URLLC (Ultra-Reliable Low Latency Communications) es uno de los perfiles de servicio definidos por 3GPP dentro del estándar 5G, diseñado para aplicaciones que requieren latencias extremadamente bajas y niveles de fiabilidad muy elevados en la transmisión de datos. A diferencia de otros perfiles como eMBB (banda ancha móvil) o mMTC (comunicaciones masivas), URLLC prioriza la respuesta inmediata, la continuidad del servicio y la previsibilidad del comportamiento de la red, incluso en condiciones adversas.

Estas capacidades se logran mediante optimizaciones específicas en la interfaz radio, en el núcleo de red y a través del uso de mecanismos avanzados como el network slicing, que permite reservar recursos dedicados con garantías estrictas de calidad de servicio. URLLC está orientado a escenarios donde retrasos mínimos, pérdidas de comunicación o comportamientos no deterministas pueden tener consecuencias graves sobre la seguridad física, la movilidad urbana o la continuidad de servicios esenciales.

Desde la perspectiva de las administraciones públicas, 5G URLLC no debe entenderse como una tecnología de uso general, sino como una capacidad especializada para soportar servicios urbanos críticos, donde la ciberseguridad, la disponibilidad y la fiabilidad operativa son requisitos fundamentales.

8.2.1. Arquitectura

Un despliegue urbano basado en 5G URLLC se apoya en una arquitectura altamente optimizada y fuertemente dependiente del operador de telecomunicaciones. En este contexto, intervienen los siguientes elementos:

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

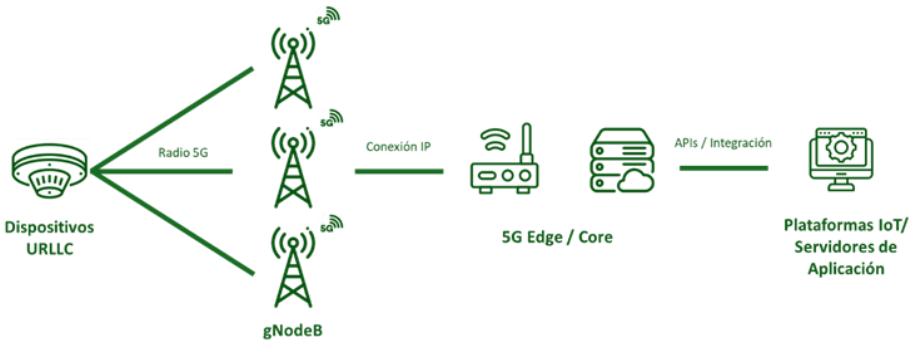

ILUSTRACIÓN 6: ARQUITECTURA 5G URLLC

- **Dispositivos finales (UE IoT)**

Sensores, actuadores y sistemas de control que participan directamente en la operación de servicios críticos, como sistemas de señalización, control de infraestructuras, vehículos conectados o equipamiento de emergencia. Estos dispositivos priorizan la transmisión inmediata y fiable de datos y suelen incorporar mecanismos de autenticación reforzada y capacidades de actualización segura.

- **Red de acceso radio 5G (gNodeB)**

Estaciones base 5G configuradas con optimizaciones específicas para reducir la latencia y garantizar la fiabilidad, como programación rápida de recursos y priorización estricta del tráfico URLLC. Esta infraestructura es gestionada exclusivamente por el operador.

- **Núcleo de red 5G (5GC)**

Incluye las funciones de control, autenticación, gestión de sesiones y políticas de calidad de servicio. El núcleo de red aplica mecanismos avanzados para garantizar la continuidad del servicio, la redundancia y la priorización del tráfico crítico.

- **Segmentación lógica de red (Network Slice URLLC)**

Segmento lógico dedicado que reserva recursos de red específicos, rutas optimizadas y políticas de seguridad adaptadas a los requisitos de latencia y fiabilidad. Este aislamiento es clave para evitar interferencias con otros servicios móviles o IoT.

- **Procesamiento en el borde (MEC / Edge Computing)**

Infraestructura de computación situada cerca del punto de generación de datos, que permite ejecutar análisis, decisiones y controles en tiempo casi real, reduciendo la dependencia del núcleo de red y minimizando los retardos. En URLLC, este elemento resulta esencial para cumplir los requisitos temporales.

- **Plataformas de control y servidores de aplicación**

Sistemas que coordinan los servicios urbanos críticos, integrando la información procedente de los dispositivos y ejecutando acciones de control. Estas plataformas deben alinearse con los requisitos de alta disponibilidad y seguridad definidos para los servicios URLLC.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Desde el punto de vista de la ciberseguridad, esta arquitectura introduce un alto grado de sofisticación técnica, pero también una dependencia estructural del operador y de la correcta configuración de todos los elementos de la cadena.

8.2.2. Medidas de seguridad

La seguridad en 5G URLLC debe abordarse de forma integral y prioritaria, dada la naturaleza crítica de los servicios que soporta y su impacto potencial en la seguridad física y operativa de la ciudad.

- **Autenticación reforzada y control estricto de accesos:** URLLC se apoya en los mecanismos avanzados de autenticación del ecosistema 5G, con un énfasis especial en prevenir accesos no autorizados que puedan interferir en servicios críticos. La gestión rigurosa de identidades, la revocación inmediata de credenciales y la trazabilidad de los accesos son elementos esenciales.

  Para una administración pública, este enfoque exige procesos sólidos de provisión, gestión y retirada de dispositivos, así como una coordinación estrecha con el operador para minimizar riesgos operativos.

- **Integridad y disponibilidad como prioridades:** En el contexto de URLLC, la confidencialidad de los datos, aunque relevante, no es el único objetivo de seguridad. La integridad de las comunicaciones y la disponibilidad continua del servicio son factores críticos, ya que cualquier alteración, retraso o interrupción puede tener consecuencias inmediatas.

  La seguridad debe orientarse tanto a prevenir ataques deliberados como a reducir el impacto de fallos internos, errores de configuración o incidentes en la infraestructura.

- **Dependencia del operador y acuerdos de servicio:** Este tipo de arquitectura depende en gran medida del operador para garantizar los niveles de fiabilidad y seguridad requeridos por URLLC. Esto exige acuerdos contractuales muy claros, que incluyan compromisos explícitos en materia de ciberseguridad, continuidad del servicio y gestión de incidentes.

- **Resiliencia frente a ataques dirigidos:** Los servicios basados en URLLC pueden convertirse en objetivos prioritarios para ataques deliberados debido a su impacto potencial. Aunque la tecnología 5G incorpora medidas avanzadas de protección, la administración debe considerar este riesgo en su análisis global de amenazas y priorizar adecuadamente la protección de estos servicios.

- **Gestión del ciclo de vida y pruebas de seguridad:** Dada la criticidad de los servicios URLLC, los dispositivos y sistemas asociados deben someterse a pruebas de seguridad rigurosas antes de su puesta en servicio. Las actualizaciones de software y firmware deben planificarse y ejecutarse de forma controlada, minimizando el riesgo de interrupciones no previstas.

8.2.3. Consideraciones

Antes de seleccionar 5G URLLC como tecnología de comunicación para un proyecto de Smart City, es imprescindible evaluar una serie de aspectos clave desde el punto de vista técnico, organizativo y de ciberseguridad.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- **Uso restringido a servicios críticos:** URLLC no está diseñada para aplicaciones de sensorización general ni para servicios no críticos. Su adopción debe limitarse a escenarios donde la latencia y la fiabilidad sean determinantes.
- **Alta dependencia del operador:** La correcta operación de URLLC depende de una configuración precisa de la red y de la gestión continua por parte del operador. La administración tiene una capacidad de control directo limitada, lo que exige una gobernanza sólida.
- **Complejidad técnica y operativa:** La combinación de network slicing, MEC y políticas avanzadas de calidad de servicio introduce una complejidad elevada, que debe ser tenida en cuenta en la planificación y supervisión del servicio.
- **Costes y sostenibilidad:** Los servicios URLLC implican costes superiores a otras tecnologías IoT, tanto en términos de conectividad como de infraestructura y operación. Estos costes deben justificarse por la criticidad del servicio soportado.
- **Impacto de fallos y responsabilidad:** Cualquier fallo en un servicio URLLC puede tener consecuencias directas sobre la seguridad ciudadana o la operación urbana, lo que exige una clara definición de responsabilidades y procedimientos de respuesta.

8.2.4. Casos de uso principales en Smart Cities

Los casos de uso de 5G URLLC en Smart Cities son específicos y limitados a servicios donde la latencia mínima y la fiabilidad extrema son requisitos esenciales. Entre ellos destacan:

- Control en tiempo real de sistemas de tráfico urbano: Coordinación dinámica de semáforos, gestión de cruces complejos.
- Operación y control remoto de infraestructuras críticas Operación remota de estaciones eléctricas, centros de control hidráulico o instalaciones industriales.
- Servicios de emergencia y protección civil: Comunicaciones críticas para la coordinación de equipos de emergencia, sistemas de alerta inmediata y respuesta ante incidentes graves.
- Sistemas urbanos de respuesta inmediata: Control de accesos críticos, gestión de incidentes en tiempo real.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo 5G mMTC contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Inspección remota de infraestructuras ferroviarias con 5G URLLC en Galicia
En Galicia se ha desplegado un piloto de inspección remota de vías ferroviarias basado en conectividad 5G, impulsado por Telefónica en colaboración con Adif. El objetivo del caso de uso es mejorar la seguridad y eficiencia de las tareas de mantenimiento ferroviario, reduciendo la necesidad de presencia física del personal en la vía y minimizando interrupciones del servicio. El sistema se basa en el uso de drones equipados con cámaras de alta definición y sensores de navegación, que realizan vuelos de inspección sobre tramos ferroviarios y transmiten vídeo y telemetría en tiempo real a través de la red 5G. La operación remota de estos drones requiere comunicaciones de muy baja latencia y alta fiabilidad, ya que cualquier retraso o pérdida de

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

conectividad puede comprometer el control del dispositivo y la seguridad de la operación, lo que sitúa este caso dentro de escenarios representativos de URLLC en fase piloto.

Los datos capturados se procesan parcialmente en infraestructuras de computación en el borde (edge computing), lo que permite reducir la latencia extremo a extremo y facilitar la detección temprana de incidencias en la infraestructura ferroviaria. Posteriormente, la información se integra en plataformas de supervisión y análisis utilizadas por Adif para apoyar la toma de decisiones en mantenimiento y gestión de la red.

TABLA 7: CASO DE USO 5G MMTC.

9. Tecnologías de corto alcance (redes locales)

9.1. IEEE 802.15.4 / Zigbee

IEEE 802.15.4 es un estándar de comunicaciones inalámbricas diseñado para corto alcance y bajo consumo energético, concebido como base para múltiples protocolos de nivel superior orientados a redes personales inalámbricas WPAN (del inglés, Wireless Personal Area Networks). Este estándar define las especificaciones físicas y de enlace de datos, incluyendo la modulación, el acceso al medio y la eficiencia energética, mientras que protocolos como Zigbee añaden las funciones de red, direccionamiento, seguridad y gestión adaptadas a aplicaciones IoT.

Zigbee es uno de los protocolos más extendidos sobre IEEE 802.15.4, especialmente en entornos urbanos, edificios inteligentes e instalaciones técnicas. Su popularidad se debe a que ofrece mecanismos de red flexibles, seguridad integrada y un bajo consumo energético, lo que lo hace adecuado para sensores, actuadores y sistemas de automatización que requieren operación prolongada con baterías pequeñas.

Estas tecnologías operan habitualmente en bandas de frecuencia no licenciadas, principalmente en 2,4 GHz, aunque también existen variantes en bandas sub-GHz para mejorar la cobertura en interiores o entornos con alta densidad de obstáculos. IEEE 802.15.4/Zigbee permite topologías de red variadas, incluyendo estrella, árbol y malla (mesh). La capacidad de formar redes malladas es especialmente útil para extender la cobertura, ya que los nodos intermedios pueden reenviar mensajes hacia su destino, superando limitaciones de distancia o interferencias en entornos interiores y urbanos densos.

En el contexto de las Smart Cities, IEEE 802.15.4/Zigbee no se utiliza como tecnología de conectividad de ciudad completa, sino como solución para redes locales o de ámbito acotado, normalmente asociadas a edificios municipales, instalaciones cerradas o infraestructuras urbanas concretas. Se emplea principalmente cuando se requiere automatización, control distribuido y bajo consumo energético, permitiendo monitorización de sensores, control de iluminación, climatización y sistemas de seguridad, con una gestión descentralizada y flexibilidad para adaptarse a las condiciones físicas del entorno.

9.1.1. Arquitectura

Un despliegue típico basado en IEEE 802.15.4/Zigbee presenta una arquitectura local, controlada directamente por la entidad usuaria o por sus proveedores. La red está organizada en torno a una

topología mallada o híbrida, que permite ampliar la cobertura, aumentar la resiliencia y gestionar múltiples dispositivos de manera eficiente. Los principales elementos de la arquitectura son:

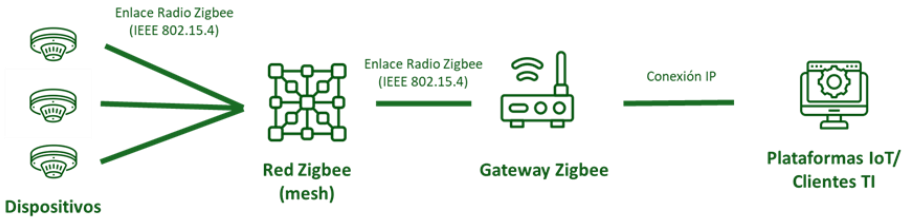

ILUSTRACIÓN 7: ARQUITECTURA ZIGBEE

- **Dispositivos finales**

Sensores y actuadores de bajo consumo, como detectores de presencia, sensores ambientales, dispositivos de control de iluminación o elementos de automatización de edificios. Suelen disponer de capacidades limitadas de procesamiento y almacenamiento, priorizando la eficiencia energética.

- **Nodos intermedios o routers**

Estos dispositivos poseen la capacidad de reenviar tráfico dentro de la red mallada, ampliando la cobertura y aportando resiliencia frente a fallos puntuales. Los nodos intermedios pueden transportar tráfico de múltiples dispositivos finales y son esenciales para mantener la continuidad de la comunicación en redes con múltiples saltos.

- **Coordinadores o nodos maestros**

Actúan como punto central de control de la red Zigbee, encargándose de la creación de la red, la gestión de direcciones y la autorización de nuevos dispositivos. En muchos casos, el coordinador también funciona como pasarela lógica hacia sistemas de gestión superiores, asegurando que la red local se integre de forma segura con plataformas externas.

- **Pasarela o Gateway hacia sistemas de aplicación**

Este dispositivo conecta la red Zigbee con redes IP, plataformas de gestión de edificios o sistemas municipales. La pasarela concentra funciones críticas de seguridad, integración y traducción de protocolos, permitiendo que los datos recogidos por los dispositivos finales se procesen, almacenen y utilicen para la toma de decisiones o control de infraestructuras.

9.1.2. Medidas de seguridad

La seguridad en IEEE 802.15.4/Zigbee se apoya tanto en mecanismos criptográficos definidos en el protocolo como en las prácticas de despliegue y operación, que resultan determinantes para su eficacia real.

- **Protección de las comunicaciones:** Zigbee incorpora cifrado simétrico basado en AES-128 para proteger la confidencialidad e integridad de las comunicaciones dentro de la red. Este cifrado se aplica a nivel de enlace, lo que protege los mensajes frente a escuchas pasivas en el entorno radioeléctrico.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

No obstante, la solidez de esta protección depende directamente de cómo se gestionan las claves de red y de enlace, así como de las configuraciones de seguridad aplicadas durante el despliegue inicial.

- **Gestión de claves y alta de dispositivos:** Uno de los aspectos más sensibles de la seguridad en Zigbee es el proceso de incorporación de nuevos dispositivos a la red. Si este proceso no se controla adecuadamente, existe riesgo de que dispositivos no autorizados se unan a la red o de que las claves sean interceptadas durante el alta.

  En entornos municipales, donde los despliegues pueden ser extensos y realizados por distintos contratistas, es esencial definir procedimientos claros y homogéneos para el aprovisionamiento seguro de dispositivos.

- **Seguridad en redes malladas:** La topología mesh aporta resiliencia, pero también amplía la superficie de ataque. Un nodo comprometido puede afectar al tráfico de otros dispositivos, especialmente si actúa como repetidor. Por ello, resulta importante considerar la confianza asignada a cada tipo de nodo y limitar, cuando sea posible, las funciones críticas a dispositivos mejor protegidos.

- **Exposición física y manipulación:** Muchos dispositivos Zigbee se instalan en ubicaciones accesibles, como cuadros eléctricos, falsos techos, pasillos o espacios comunes. La manipulación física puede permitir la extracción de claves, la reconfiguración del dispositivo o la sustitución por nodos maliciosos.

  Por este motivo, deben establecerse requisitos mínimos de protección física, así como mecanismos de detección de manipulaciones, especialmente cuando los dispositivos soportan servicios relevantes para la operación municipal.

- **Mantenimiento y ciclo de vida:** La capacidad de actualización remota no está siempre presente o habilitada en dispositivos Zigbee, lo que puede dificultar la corrección de vulnerabilidades. Es fundamental evaluar este aspecto en fase de diseño y contratación, especialmente para despliegues de larga duración.

9.1.3. Consideraciones

Antes de seleccionar IEEE 802.15.4/Zigbee como tecnología de comunicación para un proyecto de Smart City, deben tenerse en cuenta los siguientes aspectos:

- **Ámbito limitado de cobertura:** Zigbee está diseñado para redes locales de corto alcance. No resulta adecuado como tecnología de conectividad urbana a gran escala, sino como complemento en edificios o instalaciones concretas.

- **Alta exposición física:** La proximidad de los dispositivos a las persona usuarias y el personal no técnico incrementa el riesgo de manipulación, lo que debe ser considerado en el análisis de amenazas.

- **Gestión descentralizada de la seguridad:** A diferencia de tecnologías celulares, la seguridad depende en gran medida de la correcta configuración y operación local de la red, lo que exige procedimientos claros y personal cualificado.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- **Interferencias en bandas no licenciadas:** Al operar en bandas compartidas, Zigbee puede verse afectado por interferencias de otras tecnologías inalámbricas, especialmente en 2,4 GHz, lo que puede impactar en la disponibilidad del servicio.
- **Escalabilidad limitada:** Aunque las redes malladas permiten ampliar la cobertura, la escalabilidad práctica está condicionada por la complejidad de gestión y por el impacto de los nodos intermedios sobre el rendimiento y la seguridad.

9.1.4. Casos de uso principales en Smart Cities

IEEE 802.15.4/Zigbee se emplea en Smart Cities principalmente en escenarios de ámbito local o de edificio, donde se requiere automatización, bajo consumo energético y control directo de la red. Entre sus principales aplicaciones destacan:

- Control de iluminación interior: Redes de sensores de presencia, reguladores de intensidad de iluminación.
- Sistemas de climatización y eficiencia energética en edificios públicos: Sensores de temperatura, humedad y CO_2
- Gestión de accesos y control de espacios interiores: Cerraduras inteligentes, sensores de apertura, detectores de intrusión.
- Monitorización técnica de instalaciones interiores críticas: Sensores en salas técnicas, cuadros eléctricos o centros de datos para detectar temperaturas anómalas, humedad, etc.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo Zigbee contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Monitorización urbana de calidad del aire y tráfico con redes Zigbee en Santander
En Santander se desplegó un sistema de monitorización urbana a gran escala en el marco del proyecto SmartSantander, uno de los programas de referencia europeos en Smart Cities. El objetivo del despliegue fue obtener información en tiempo casi real sobre calidad del aire, tráfico y condiciones ambientales, con el fin de mejorar la gestión municipal y apoyar la toma de decisiones basada en datos. El sistema se basa en el despliegue masivo de sensores IoT distribuidos por la ciudad, instalados en farolas, fachadas y mobiliario urbano. Estos nodos, basados en plataformas de Libelium, miden parámetros como contaminantes atmosféricos (CO_2, NO_2, O_3), temperatura, humedad, ruido ambiental e intensidad de tráfico. La comunicación entre los sensores y los concentradores locales se realiza mediante tecnología Zigbee (IEEE 802.15.4), formando redes malladas de corto alcance, adecuadas para entornos urbanos densos y de bajo consumo energético. Los datos recogidos por los nodos Zigbee se agregan en gateways urbanos, que los transmiten a través de la red IP municipal hacia la plataforma central SmartSantander, donde se almacenan, procesan y visualizan. Esta información permite analizar patrones de contaminación y movilidad, detectar situaciones anómalas y evaluar el impacto de medidas municipales relacionadas con tráfico, medio ambiente y planificación urbana.

TABLA 8: CASO DE USO ZIGBEE.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

9.2. Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) es una tecnología de comunicaciones inalámbricas de corto alcance diseñada para minimizar el consumo energético mientras mantiene una conectividad flexible y una amplia compatibilidad con dispositivos comerciales. Forma parte del estándar Bluetooth y se ha consolidado como una de las tecnologías más utilizadas para IoT de proximidad y servicios contextuales, especialmente en entornos urbanos y domésticos.

BLE opera en la banda de 2,4 GHz y está orientado principalmente a comunicaciones de corto alcance, tanto en modo punto a punto como en modo difusión (broadcast). Esto permite que los dispositivos intercambien información directamente o envíen datos a múltiples receptores simultáneamente. En versiones más recientes, el estándar incorpora capacidades de red mallada (Bluetooth Mesh), que permiten expandir la cobertura y habilitar control distribuido en redes locales, manteniendo eficiencia energética y confiabilidad en la transmisión.

Una de las principales ventajas de BLE en entornos urbanos es su amplia compatibilidad con teléfonos móviles y otros dispositivos de uso cotidiano, lo que facilita la interacción directa con la ciudadanía y personal municipal. Esta característica hace de BLE una tecnología idónea para aplicaciones donde la cercanía física es un elemento funcional, como sistemas de señalización, guiado indoor, beacons para servicios locales y aplicaciones contextuales.

En el contexto de las Smart Cities, BLE no se emplea como tecnología de conectividad continua ni de sensorización masiva, sino como solución para servicios de proximidad, interacción local y detección contextual. Su uso se centra en escenarios donde los dispositivos necesitan comunicarse de manera directa o mediante redes locales malladas, proporcionando información contextual o servicios personalizados basados en la ubicación y cercanía de los las personas usuarias o los sensores.

9.2.1. Arquitectura

Los despliegues basados en BLE presentan una arquitectura ligera y descentralizada, con control limitado sobre el entorno radioeléctrico y una exposición significativa al espacio público. Esta configuración se adapta bien a aplicaciones de proximidad e interacción local, pero limita la capacidad de planificación y optimización centralizada de la red. Los principales elementos de la arquitectura son:

ILUSTRACIÓN 8: ARQUITECTURA BLE

- **Dispositivos BLE**

Sensores, balizas, actuadores o dispositivos interactivos que emiten o reciben información mediante BLE. Suelen ser equipos de bajo coste, tamaño reducido y capacidades limitadas de procesamiento y almacenamiento.

- **Dispositivos receptores o pasarelas**

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Estos equipos reciben las señales BLE y las integran con otros sistemas o plataformas de gestión. En muchos casos, esta función la realizan dispositivos móviles de las personas usuarias, tablets del personal municipal o pasarelas instaladas en edificios, mobiliario urbano o estaciones fijas. Su papel es esencial para concentrar, filtrar y retransmitir información hacia los sistemas de backend, permitiendo que los datos generados por los dispositivos BLE tengan uso práctico y funcional.

- **Plataformas de gestión y aplicaciones**

Los sistemas backend procesan la información recibida desde los dispositivos BLE, gestionan contenidos, aplican reglas de negocio y generan servicios útiles para la ciudadanía, operadores municipales o sistemas inteligentes de gestión urbana. Estas plataformas permiten almacenar datos, correlacionarlos y explotarlos para análisis o automatización, completando la cadena desde la adquisición local de información hasta la acción o decisión basada en los datos.

9.2.2. Medidas de seguridad

La seguridad en BLE ha evolucionado con las distintas versiones del estándar, pero sigue requiriendo una atención especial en despliegues urbanos, donde los dispositivos están expuestos físicamente y las comunicaciones se producen en entornos abiertos.

- **Emparejamiento y autenticación:** BLE incorpora distintos modos de emparejamiento entre dispositivos, con niveles variables de protección. La seguridad efectiva depende de que se utilicen modos de emparejamiento adecuados y de que se eviten configuraciones débiles, especialmente en entornos públicos.

  Una mala gestión del emparejamiento puede permitir accesos no autorizados o la interceptación de comunicaciones.

- **Cifrado de las comunicaciones:** BLE soporta cifrado de las comunicaciones entre dispositivos emparejados, protegiendo la confidencialidad e integridad de los datos intercambiados. Sin embargo, este cifrado no se aplica necesariamente en todos los modos de funcionamiento, especialmente en comunicaciones de difusión (broadcast), donde la información es accesible para cualquier receptor cercano.

- **Exposición y rastreabilidad en entornos públicos:** Muchos dispositivos BLE están diseñados para ser detectables por cualquier equipo cercano, lo que incrementa su visibilidad y potencial superficie de ataque. En una Smart City, esto puede facilitar intentos de rastreo, suplantación o denegación de servicio local.

  Desde un punto de vista de seguridad y privacidad, es importante evaluar qué información se emite y con qué frecuencia, especialmente cuando los dispositivos interactúan con la ciudadanía.

- **Gestión del ciclo de vida:** Los dispositivos BLE, en particular las balizas, suelen tener ciclos de vida largos y capacidades limitadas de actualización. La falta de mantenimiento puede dar lugar a vulnerabilidades persistentes o a configuraciones obsoletas.

  Las administraciones deben establecer políticas claras para la revisión periódica, sustitución y retirada de dispositivos BLE.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

9.2.3. Consideraciones

Antes de seleccionar BLE como tecnología de comunicación para un proyecto de Smart City, deben considerarse los siguientes aspectos:

- **Alcance limitado:** BLE está diseñada para interacciones de corto alcance. Su uso debe justificarse por la necesidad de proximidad física como parte funcional del servicio.
- **Alta exposición:** Los dispositivos BLE suelen estar visibles y accesibles en espacios públicos, lo que incrementa el riesgo de manipulación, interferencias y ataques locales. Se recomienda un diseño cuidadoso de la ubicación de nodos y balizas para minimizar estas vulnerabilidades.
- **Seguridad de las aplicaciones:** Gran parte de la seguridad efectiva recae en las aplicaciones y plataformas que procesan los datos, más que en la capa de comunicación BLE en sí. Esto implica que la protección de información sensible depende en gran medida de la gestión de cuentas de usuario, autenticación de servicios y cifrado a nivel de aplicación.
- **Implicaciones de privacidad:** Los servicios BLE que interactúan con la ciudadanía deben diseñarse para evitar el rastreo no deseado o la recopilación excesiva de información personal. La privacidad debe ser una consideración central desde la fase de diseño hasta la operación del sistema.
- **Escalabilidad limitada:** BLE no está pensada para redes extensas ni sensorización continua, sino para interacciones puntuales y contextuales. Su capacidad de soportar grandes volúmenes de dispositivos o comunicación masiva es reducida, lo que limita su uso a entornos locales y controlados.

9.2.4. Casos de uso principales en Smart Cities

BLE se utiliza en Smart Cities en escenarios de corto alcance y proximidad, como:

- Balizas informativas y servicios de orientación: Información contextual a través de aplicaciones móviles en museos, bibliotecas o centros culturales.
- Control de acceso local y sistemas de identificación de proximidad: Identificación de personal autorizado, control de aforo o registro de presencia.
- Monitorización localizada en edificios o instalaciones municipales: Seguimiento local de equipamiento municipal, carros de mantenimiento o material logístico.

A continuación, se detalla un caso real de implementación de esta tecnología en un entorno urbano, que ilustra cómo Zigbee contribuye a mejorar la eficiencia operativa y la experiencia de la ciudadanía.

Turismo inteligente y guiado contextual con BLE en la ciudad de Córdoba
En Córdoba, el Ayuntamiento ha desplegado una solución de turismo inteligente basada en tecnología Bluetooth Low Energy (BLE) como parte de su estrategia para consolidarse como Destino Turístico Inteligente. El proyecto se ha desarrollado en colaboración con la empresa OK Located y está orientado a mejorar la experiencia del visitante mediante servicios digitales contextualizados en el entorno urbano y patrimonial.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Turismo inteligente y guiado contextual con BLE en la ciudad de Córdoba
El sistema se basa en el despliegue de balizas BLE (beacons) en puntos de interés turístico de la ciudad. Estas balizas emiten identificadores que son detectados por los dispositivos móviles de los visitantes, permitiendo ofrecer información contextualizada en función de la proximidad de la persona usuaria, sin necesidad de posicionamiento GPS y con un consumo energético muy reducido. La información proporcionada incluye contenidos turísticos, históricos y culturales, así como recomendaciones personalizadas y apoyo al guiado urbano en entornos con alta densidad patrimonial. Los datos de uso se integran en una plataforma de gestión turística, que permite al ayuntamiento analizar flujos de visitantes, evaluar el interés por distintos recursos y optimizar la planificación turística.

TABLA 9: CASO DE USO ZIGBEE.

10. Tecnologías complementarias

Además de las tecnologías de comunicación que constituyen el núcleo de la conectividad urbana, existen soluciones que desempeñan un papel complementario. Estas tecnologías no están concebidas, en general, para actuar como infraestructuras de conectividad urbana de propósito general, sino para cubrir necesidades específicas, escenarios acotados o casos de uso donde los modelos tradicionales presentan limitaciones.

Desde una perspectiva de ciberseguridad, estas soluciones introducen riesgos y consideraciones diferenciadas, derivados de factores como la menor madurez del ecosistema, la ausencia de estándares ampliamente adoptados o la mayor responsabilidad operativa que recae en la entidad usuaria. Por este motivo, su adopción en proyectos municipales debe ir acompañada de un análisis específico que tenga en cuenta no solo sus capacidades técnicas, sino también su impacto en la gobernanza, la sostenibilidad a largo plazo y la gestión del riesgo.

En este apartado se analizan tecnologías y enfoques que, aun no constituyendo la base principal de la conectividad urbana, pueden resultar relevantes como complemento a otras soluciones o en contextos muy concretos, siempre desde la óptica de la seguridad y la resiliencia de los servicios públicos.

10.1. Redes mesh propietarias para servicios urbanos

Las arquitecturas mesh propietarias en servicios urbanos no constituyen una tecnología de comunicación estandarizada, sino un modelo arquitectónico heredado, implementado mediante soluciones cerradas desarrolladas por fabricantes o integradores. Estas soluciones combinan tecnologías de radio, protocolos de encaminamiento y plataformas de gestión definidos por el proveedor, con el objetivo de proporcionar conectividad distribuida en entornos urbanos sin depender exclusivamente de infraestructura centralizada.

El principio fundamental de estas arquitecturas es la utilización de topologías malladas (mesh), en las que los nodos no solo transmiten sus propios datos, sino que también participan activamente en el encaminamiento del tráfico de otros dispositivos. Esta característica permite extender la cobertura y mejorar la resiliencia del sistema, especialmente en entornos urbanos complejos o en despliegues de

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

gran extensión, sin necesidad de desplegar nodos centrales densos. La capacidad de reenviar datos a través de múltiples saltos hace que estas redes sean robustas frente a fallos puntuales y limitaciones de alcance de los nodos individuales.

No obstante, la adopción de estas arquitecturas suele responder a decisiones tecnológicas tempranas y a la integración directa en infraestructuras físicas existentes, más que a criterios de interoperabilidad, estandarización o evolución tecnológica. Por este motivo, su análisis en esta guía se centra en la gestión del riesgo, la seguridad de los sistemas en explotación y la planificación de su evolución o sustitución, en lugar de recomendarlas para nuevos despliegues.

10.1.1. Arquitectura

Un despliegue basado en redes mesh propietarias presenta una arquitectura distribuida, estrechamente integrada en la infraestructura urbana existente. Los elementos habituales son los siguientes:

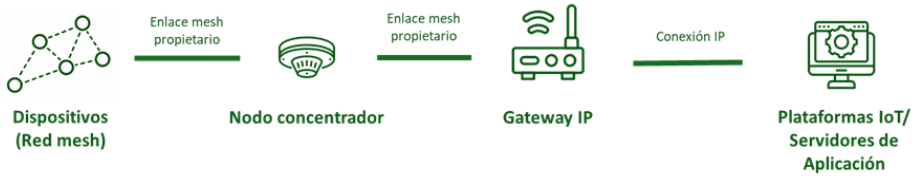

ILUSTRACIÓN 9: ARQUITECTURA REDES MESH

- **Nodos mesh urbanos**

Se trata de dispositivos IoT con capacidades de comunicación y encaminamiento, instalados en farolas, semáforos, armarios eléctricos u otros elementos del mobiliario urbano. Estos nodos forman la malla de comunicaciones y participan activamente en el transporte del tráfico de la red, reenviando mensajes de otros dispositivos para ampliar cobertura y mejorar la resiliencia frente a fallos puntuales.

- **Nodos de concentración o pasarela**

Estos equipos agregan el tráfico de la red mesh y lo conectan con sistemas de gestión municipales o plataformas del proveedor. Funcionan como punto de integración entre la red local y otros sistemas de información, concentrando funciones de seguridad, filtrado de datos y traducción de protocolos.

- **Herramientas de provisión y gestión**

Incluyen software y herramientas específicas del proveedor para la configuración, supervisión, actualización y mantenimiento de la red. Estas herramientas son generalmente propietarias y no interoperables con soluciones de otros fabricantes, lo que obliga a depender del mismo proveedor para soporte y evolución de la infraestructura.

10.1.2. Medidas de seguridad

La seguridad en redes mesh propietarias presenta retos específicos derivados de su carácter no estandarizado, de la dependencia del proveedor y de la integración física de los nodos en infraestructuras urbanas.

- **Ausencia de estándares abiertos y transparencia limitada:** Al tratarse de soluciones propietarias, la visibilidad sobre los mecanismos internos de seguridad puede ser limitada para

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

la administración usuaria. Esto dificulta la evaluación independiente de la robustez criptográfica, la gestión de identidades o la protección frente a ataques conocidos.

Desde un punto de vista institucional, este factor debe ser considerado como un riesgo inherente, mitigable únicamente mediante requisitos contractuales claros y evaluaciones técnicas previas.

- **Gestión de identidades y confianza en la red mesh:** En una red mallada, cada nodo confía parcialmente en otros nodos para el encaminamiento del tráfico. Si un nodo es comprometido, puede afectar al funcionamiento o a la seguridad de una parte significativa de la red.

  La forma en que se gestionan las identidades de los nodos, la autenticación mutua y la revocación de dispositivos comprometidos es crítica, y varía significativamente entre proveedores. La administración debe exigir mecanismos claros para aislar nodos sospechosos o retirarlos de la red.

- **Protección de las comunicaciones:** La mayoría de soluciones mesh propietarias incorporan algún tipo de cifrado para proteger las comunicaciones entre nodos. Sin embargo, la fortaleza y correcta implementación de estos mecanismos no siempre es verificable externamente.

  Es recomendable que los proyectos municipales requieran el uso de cifrado robusto y actualizado, así como la capacidad de renovación de claves a lo largo del ciclo de vida del sistema.

- **Seguridad física y manipulación de nodos:** Los nodos mesh suelen instalarse en ubicaciones accesibles, como farolas o armarios de calle, lo que los expone a manipulaciones físicas. Dado que estos nodos desempeñan un papel activo en la red, su compromiso físico puede tener un impacto desproporcionado.

  La seguridad física, la detección de manipulaciones y los procedimientos de respuesta ante incidentes deben formar parte integral del diseño del servicio.

- **Dependencia del proveedor y riesgo de bloqueo tecnológico:** La seguridad de estas redes está estrechamente ligada al proveedor, tanto en términos de mantenimiento como de evolución frente a nuevas amenazas. La falta de interoperabilidad puede dificultar la sustitución de componentes o la incorporación de mejoras de seguridad independientes.

  Para una administración pública, este riesgo debe gestionarse mediante cláusulas contractuales que garanticen soporte a largo plazo, actualizaciones de seguridad y, en la medida de lo posible, mecanismos de migración o integración con otras tecnologías.

- **Gestión del ciclo de vida y obsolescencia:** Muchas redes mesh propietarias se despliegan con horizontes temporales largos, similares a los de las infraestructuras urbanas físicas. Sin una planificación adecuada, pueden quedar expuestas a vulnerabilidades obsoletas o a la falta de soporte del proveedor.

  Es esencial definir desde el inicio cómo se gestionarán las actualizaciones, la sustitución de nodos y la retirada segura del sistema al final de su vida útil.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

10.1.3. Consideraciones

Antes de seleccionar una arquitectura mesh propietaria para un proyecto de Smart City, deben evaluarse cuidadosamente los siguientes aspectos, y estos dependerán del tipo de sistema y las tecnologías utilizadas para ello:

- **Nivel de dependencia tecnológica del proveedor:** Estas redes suelen ser propietarias y cerradas, lo que implica una fuerte dependencia del fabricante para la provisión de equipos, soporte y actualizaciones. Cambiar de proveedor o integrar otros sistemas puede resultar complejo y costoso.
- **Capacidad de auditoría y evaluación independiente de la seguridad:** Al tratarse de soluciones cerradas, la supervisión independiente de la seguridad puede ser limitada. Es importante asegurar que el proveedor permita auditorías, pruebas de vulnerabilidad y revisión de protocolos, especialmente en sistemas que gestionan infraestructuras críticas urbanas.
- **Impacto de la manipulación física de nodos sobre el servicio:** Dado que los nodos mesh urbanos suelen estar accesibles en farolas, semáforos o mobiliario urbano, su manipulación o sabotaje físico puede afectar la continuidad y disponibilidad del servicio, por lo que deben considerarse medidas de protección y redundancia.
- **Dificultad de integración con otras tecnologías o plataformas:** La interoperabilidad con otras redes o plataformas municipales puede ser limitada. Antes del despliegue, se debe evaluar la compatibilidad con sistemas existentes y la posibilidad de extender o actualizar la red sin depender exclusivamente del proveedor original.
- **Sostenibilidad del soporte y mantenimiento a largo plazo:** Las redes mesh propietarias requieren un plan de mantenimiento y soporte confiable para garantizar su operación continua. La disponibilidad de repuestos, actualizaciones de software y soporte técnico a largo plazo es un factor crítico para la durabilidad de la infraestructura urbana.

10.1.4. Casos de uso principales en Smart Cities

Las redes mesh propietarias se utilizan en Smart Cities en servicios urbanos específicos, entre los que destacan:

- Telegestión y control del alumbrado público.
- Redes de control para semáforos y señalización urbana.
- Monitorización y control de equipamientos urbanos distribuidos.
- Sistemas IoT integrados en infraestructuras municipales existentes.

En estos casos, la seguridad debe evaluarse no solo desde la perspectiva de la protección de datos, sino también considerando el impacto potencial sobre la continuidad y seguridad física de los servicios urbanos.

Red mesh urbana para alumbrado público en París
La ciudad de París ha implementado un despliegue de red mesh urbana para su alumbrado público inteligente, basado en la tecnología Wi-SUN FAN 1.1. Cada farola está equipada con un nodo IoT que

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Red mesh urbana para alumbrado público en París
no solo transmite su propio estado, sino que también reenvía datos de otros nodos, formando una topología mallada que asegura cobertura amplia y resiliencia frente a fallos o interferencias. Esta arquitectura permite que la red continúe operando incluso si algunos nodos fallan, garantizando la continuidad del servicio. Los nodos de concentración o pasarelas agregan el tráfico de la red y lo conectan con los sistemas de gestión municipales, lo que permite control remoto del encendido, apagado y regulación de intensidad de las luminarias. La plataforma central supervisa el estado de cada nodo en tiempo real, genera alertas ante fallos y proporciona datos para planificación de mantenimiento preventivo, optimizando la operación del sistema y reduciendo costes energéticos. Este despliegue ofrece beneficios significativos para la gestión urbana, como un aumento del ahorro energético, la mejora de la eficiencia operativa mediante la monitorización continua y la expansión modular de la red al integrar futuros sensores ambientales u otros dispositivos IoT.

TABLA 10: CASO DE USO REDES MESH.

10.2. Wi-Fi HaLow (IEEE 802.11ah)

Wi-Fi HaLow, estandarizado como IEEE 802.11ah y ratificado en 2016, es una evolución de la familia Wi-Fi diseñada específicamente para aplicaciones IoT. A diferencia del Wi-Fi convencional, que opera en las bandas de 2,4 y 5 GHz, Wi-Fi HaLow funciona en bandas sub-GHz (en Europa, principalmente alrededor de 868 MHz), lo que permite mayor alcance, mejor penetración en interiores y un consumo energético reducido, adaptándose a dispositivos con recursos limitados y necesidades de comunicación esporádica.

El estándar fue concebido para cubrir el espacio intermedio entre redes Wi-Fi locales y tecnologías LPWAN, proporcionando conectividad IP nativa a dispositivos IoT que requieren bajo consumo y tráfico moderado. Para ello, Wi-Fi HaLow adapta los mecanismos tradicionales de Wi-Fi, incluyendo acceso al medio, gestión de energía y escalabilidad, permitiendo soportar un número elevado de nodos sin saturar la red ni comprometer el rendimiento.

Wi-Fi HaLow también introduce mejoras en eficiencia energética, como periodos de reposo prolongados y sincronización de transmisión, lo que permite que los dispositivos operen durante años con baterías pequeñas. Además, soporta topologías flexibles, facilitando despliegues en entornos interiores complejos o infraestructuras urbanas dispersas donde la cobertura de Wi-Fi convencional sería insuficiente.

En el contexto de las Smart Cities, aunque Wi-Fi HaLow es un estándar maduro y bien definido, su implantación práctica es todavía limitada. La coexistencia con tecnologías ya establecidas para conectividad de bajo caudal y largo alcance, junto con un ecosistema industrial reducido y adopción desigual por parte de fabricantes y proveedores, ha condicionado su uso en despliegues urbanos reales. Como resultado, Wi-Fi HaLow se considera actualmente una tecnología complementaria, útil en escenarios específicos donde se necesita conectividad IP directa, eficiencia energética y cobertura extendida, pero sin reemplazar las soluciones LPWAN tradicionales o redes Wi-Fi convencionales.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

10.2.1. Arquitectura

Un despliegue urbano basado en Wi-Fi HaLow presenta una arquitectura similar a la de redes Wi-Fi tradicionales, aunque adaptada a dispositivos IoT y a entornos de mayor alcance. Los elementos principales son los siguientes:

ILUSTRACIÓN 10: ARQUITECTURA WI-FI HALOW

- **Dispositivos finales Wi-Fi HaLow**

Incluyen sensores y actuadores IoT equipados con chipsets compatibles con IEEE 802.11ah. Estos dispositivos están diseñados para operar con bajo consumo energético, aunque suelen ser más complejos que los nodos LPWAN, ya que cuentan con pila IP completa, lo que permite comunicaciones directas y gestión avanzada de datos.

- **Puntos de acceso Wi-Fi HaLow**

Los puntos de acceso proporcionan conectividad a los dispositivos IoT y gestionan el acceso a la red local. Pueden instalarse en edificios municipales, farolas inteligentes, centros de control u otras infraestructuras urbanas, actuando como elementos centrales de la red y concentrando funciones de gestión de tráfico y seguridad.

- **Red IP y sistemas de gestión**

La conectividad IP nativa de Wi-Fi HaLow permite la integración directa con redes municipales, sistemas IoT y plataformas de aplicación, sin necesidad de pasarelas específicas de traducción de protocolos. Esto facilita la interoperabilidad y explotación de datos en tiempo real, así como la integración con sistemas de gestión urbana existentes.

- **Infraestructura de soporte**

Incluye antenas, sistemas de alimentación, cableado y elementos pasivos asociados a los puntos de acceso, similares a los de otras redes Wi-Fi, pero adaptados a la operación en banda sub-GHz para garantizar alcance extendido, penetración en interiores y eficiencia energética.

10.2.2. Medidas de seguridad

La seguridad en Wi-Fi HaLow se apoya en los mecanismos de seguridad del ecosistema Wi-Fi moderno, adaptados a las características de IoT y a despliegues urbanos con gran número de dispositivos.

- **Autenticación y control de acceso:** Wi-Fi HaLow hereda los modelos de autenticación definidos en los estándares Wi-Fi modernos, incluyendo mecanismos basados en credenciales y autenticación mutua entre dispositivos y puntos de acceso. Esto permite implementar controles de acceso relativamente robustos, siempre que se configuren y gestionen adecuadamente.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

En proyectos municipales, es especialmente importante definir cómo se gestionan las credenciales de los dispositivos IoT, evitando el uso de claves compartidas genéricas que puedan comprometer toda la red en caso de exposición.

- **Cifrado y protección de las comunicaciones:** El estándar contempla el uso de cifrado fuerte para proteger la confidencialidad e integridad de los datos transmitidos. Esto resulta especialmente relevante en entornos urbanos densos, donde la probabilidad de intentos de interceptación es mayor.

  No obstante, la seguridad efectiva depende de la correcta configuración de los mecanismos de cifrado y de la capacidad de los dispositivos para soportarlos sin comprometer su autonomía energética.

- **Segmentación y aislamiento de dispositivos:** Wi-Fi HaLow está diseñado para soportar un número elevado de nodos por punto de acceso, lo que introduce retos específicos en términos de gestión y seguridad. Una mala segmentación o un control de acceso insuficiente pueden facilitar la propagación de incidentes entre dispositivos.

  Desde una perspectiva institucional, es recomendable considerar la separación lógica de dispositivos por servicio o criticidad, incluso dentro de una misma infraestructura física.

- **Disponibilidad e interferencias:** Al operar en bandas no licenciadas, Wi-Fi HaLow comparte vulnerabilidades con otras tecnologías inalámbricas en términos de interferencias y posibles ataques de denegación de servicio. Aunque la banda sub-GHz suele estar menos congestionada que 2,4 GHz, no está exenta de riesgos.

  La administración debe asumir que la disponibilidad del servicio no puede garantizarse al mismo nivel que en espectro licenciado y evaluar este aspecto en función de la criticidad de los servicios soportados.

- **Gestión del ciclo de vida del dispositivo:** Los dispositivos Wi-Fi HaLow suelen soportar capacidades de actualización remota más avanzadas que otras tecnologías IoT de bajo consumo. Esto facilita la corrección de vulnerabilidades, pero también requiere procesos claros para la validación y despliegue de actualizaciones.

  La gestión de dispositivos obsoletos, comprometidos o retirados debe formar parte de las políticas de seguridad de la red municipal.

10.2.3. Consideraciones

Antes de seleccionar Wi-Fi HaLow como tecnología de comunicación para un proyecto de Smart City, deben tenerse en cuenta los siguientes aspectos:

- **Ámbito de aplicación intermedio:** Wi-Fi HaLow no sustituye al Wi-Fi tradicional ni a las redes LPWAN, sino que se posiciona para escenarios intermedios, donde se requiere mayor alcance que el Wi-Fi convencional y mayor capacidad de datos que las LPWAN. Su uso debe justificarse por necesidades específicas de cobertura y volumen de información.

- **Responsabilidad operativa directa:** A diferencia de las tecnologías celulares, la administración o el operador local es responsable de la configuración, seguridad y operación de la red, lo que

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

exige recursos técnicos y organizativos adecuados para garantizar su funcionamiento seguro y fiable.

- **Escalabilidad condicionada:** Aunque Wi-Fi HaLow soporta un gran número de dispositivos, la escalabilidad práctica depende de una planificación cuidadosa de puntos de acceso, segmentación de la red y gestión del tráfico. La falta de planificación puede afectar la calidad de servicio y la latencia en aplicaciones críticas.
- **Interferencias en bandas no licenciadas:** El uso de espectro compartido implica riesgos de interferencia por parte de otros dispositivos o redes cercanas. Estos factores deben ser considerados en servicios con requisitos de disponibilidad y fiabilidad elevados, y pueden requerir medidas de mitigación como selección de canales, control de potencia y planificación de cobertura.
- **Compatibilidad IP:** La conectividad IP nativa facilita la integración con plataformas municipales y sistemas de gestión, pero también amplía la superficie de ataque, por lo que se deben aplicar medidas de seguridad adecuadas, incluyendo firewalls, cifrado, autenticación y monitoreo continuo de la red y las aplicaciones.

10.2.4. Casos de uso principales en Smart Cities

Wi-Fi HaLow se emplea en Smart Cities en escenarios donde se requiere conectividad IP nativa, mayor alcance que Wi-Fi tradicional y control directo de la infraestructura. Entre los casos de uso más representativos destacan:

- Control y supervisión de instalaciones técnicas: Estaciones de bombeo, depósitos de agua.
- Dispositivos IoT con gestión y configuración remota: Sistemas que requieren acceso IP para diagnóstico, actualización o parametrización periódica.
- Integración directa de sensores IoT en redes IP municipales: Despliegues donde se aplican políticas de seguridad ya existentes en la red corporativa.

En estos casos, la seguridad debe abordarse de forma integral, combinando mecanismos técnicos con una gestión adecuada de la red y de los dispositivos, acorde con las responsabilidades del sector público.

Piloto de Wi-Fi HaLow en Países Bajos
El piloto de Wi-Fi HaLow en los Países Bajos, realizado dentro del programa europeo Fed4FIRE+, consistió en la instalación de nodos y puntos de acceso HaLow para evaluar su rendimiento en condiciones urbanas reales. El objetivo principal fue probar la cobertura de largo alcance, la densidad de dispositivos soportada y la eficiencia energética de esta tecnología, así como su capacidad para coexistir con otras redes IoT, como Zigbee, en las bandas sub-GHz.. Durante el piloto, los nodos desplegados pudieron transmitir datos de sensores distribuidos y monitorizar infraestructura de forma confiable, incluso en escenarios con interferencias y tráfico de otras redes. Las pruebas demostraron que Wi-Fi HaLow ofrece conectividad estable de largo alcance y bajo consumo, factores críticos para aplicaciones urbanas como monitorización ambiental, alumbrado público inteligente o control de activos distribuidos. Además, se evaluó la interoperabilidad y el comportamiento de la red en entornos compartidos, generando datos valiosos para el diseño de futuras implementaciones urbanas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Piloto de Wi-Fi HaLow en Países Bajos
Aunque este piloto aún no constituye un despliegue comercial a gran escala, representa un hito importante para la adopción de Wi-Fi HaLow en Europa.

TABLA 11: CASO DE USO WIFI HALOW.

11. Comparativa y selección de tecnologías IoT

La elección de la tecnología IoT adecuada para un proyecto de Smart City depende de múltiples factores, entre los que se incluyen alcance de comunicación, consumo energético, latencia, fiabilidad, coste y escalabilidad. Cada tecnología revisada en esta guía presenta ventajas y limitaciones particulares que deben analizarse en función de los requisitos específicos del caso de uso y del entorno urbano donde se desplegará la red. La selección adecuada permite optimizar recursos, maximizar la eficiencia operativa y garantizar la seguridad y resiliencia de la infraestructura urbana.

11.1. Matriz comparativa

A modo de resumen, las principales tecnologías se pueden comparar en función de sus atributos más relevantes:

- **Alcance**: LPWAN como LoRaWAN y Sigfox ofrecen comunicaciones de largo alcance en entornos urbanos y rurales; NB-IoT y LTE-M aprovechan la infraestructura celular existente para cobertura amplia; Wi-Fi HaLow y redes locales como Zigbee y BLE tienen alcance limitado, adecuado para edificios o áreas específicas.
- **Consumo energético**: LoRaWAN, Sigfox y NB-IoT están optimizadas para bajo consumo, permitiendo años de autonomía con baterías; LTE-M y 5G URLLC consumen más energía, aunque ofrecen mayor capacidad de datos y movilidad; Zigbee y BLE son eficientes, pero requieren nodos intermedios para extender cobertura.
- **Latencia y fiabilidad**: URLLC y LTE-M proporcionan latencias bajas y fiabilidad alta, aptas para aplicaciones críticas, mientras que LPWAN y redes locales presentan latencias mayores, suficientes para telemetría y control no crítico.
- **Seguridad**: Las tecnologías celulares y 5G ofrecen cifrado de extremo a extremo y gestión centralizada de credenciales; LPWAN y redes locales requieren implementación de cifrado y gestión de claves a nivel de red y aplicación; Wi-Fi HaLow combina cifrado IP nativo con seguridad en la capa de aplicación.
- **Coste y escalabilidad**: Las soluciones LPWAN no licenciadas tienen costes iniciales bajos y son escalables, pero dependen de gestión propia, las tecnologías celulares implican costes de operador y posibles contratos de licencias, y las redes locales y Wi-Fi HaLow requieren inversión en infraestructura y planificación de nodos para garantizar cobertura y densidad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

11.2. Criterios de selección

La selección de tecnología debe ajustarse al tipo de aplicación:

- **Telemetría y sensorización** masiva: LoRaWAN, Sigfox, NB-IoT o 5G mMTC son ideales por su eficiencia energética y cobertura.
- **Control en tiempo real o movilidad**: LTE-M, 5G URLLC o combinaciones de redes locales con 5G son más apropiadas debido a la baja latencia y fiabilidad.
- **Interacción local o servicios contextuales**: BLE, Zigbee o Wi-Fi HaLow permiten comunicaciones de proximidad y alta compatibilidad con dispositivos comerciales.
- **Casos mixtos**: En escenarios urbanos complejos, la combinación de tecnologías puede maximizar cobertura, resiliencia y eficiencia, por ejemplo, LPWAN para datos remotos y BLE/Zigbee para control local.

11.3. Sinergias y coexistencia de tecnologías

En entornos urbanos reales, es habitual que diferentes tecnologías convivan para cubrir distintos requisitos de servicio:

- LPWAN puede proporcionar sensorización distribuida de largo alcance, mientras que redes locales gestionan automatización y control en edificios o zonas específicas.
- Wi-Fi HaLow puede complementar LPWAN y redes locales en áreas donde se requiere capacidad de datos superior con bajo consumo energético.
- Las redes celulares y 5G aportan resiliencia, cobertura masiva y calidad de servicio garantizada, especialmente en aplicaciones críticas o de movilidad.

Una estrategia integrada que combine tecnologías según sus fortalezas permite optimizar costes, mejorar la cobertura, garantizar seguridad y escalabilidad, y construir un ecosistema IoT urbano sólido y sostenible a largo plazo.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

12. Anexos

Este apartado incluye información complementaría que respalda y amplía el contenido principal del documento.

12.1. Anexo I: Tabla comparativa de las diferentes tecnologías IoT

Tecnología	Ventajas principales	Desventajas principales	Caso de uso más recomendable
LoRaWAN	• Muy bajo consumo energético. • Amplia cobertura con poca infraestructura. • Despliegue en espectro no licenciado. • Ecosistema maduro y ampliamente adoptado.	• Ancho de banda muy limitado. • Latencia elevada y no determinista. • Exposición a interferencias en bandas no licenciadas. • Seguridad muy dependiente de la gestión de claves.	Sensorización distribuida no crítica: medioambiente, residuos, aparcamiento.
NB-IoT	• Uso de espectro licenciado. • Autenticación robusta basada en SIM. • Buena penetración en interiores y subterráneos. • Gestión delegada en operador.	• Dependencia total del operador. • Coste recurrente por dispositivo. • Latencia no adecuada para control en tiempo real. • Menor control directo por parte de la administración.	Lectura remota de contadores y sensores subterráneos de larga vida útil.
5G mMTC	• Soporte para densidades masivas de dispositivos. • Integración con el ecosistema 5G. • Gestión avanzada de identidades y tráfico. • Escalabilidad a gran escala urbana.	• Dependencia del despliegue 5G del operador. • Mayor complejidad técnica. • Costes superiores a LPWAN. • No optimizada para control en tiempo real.	Sensorización urbana masiva de alta densidad y multiservicio.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Tecnología	Ventajas principales	Desventajas principales	Caso de uso más recomendable
5G URLLC	• Latencia extremadamente baja. • Alta fiabilidad y disponibilidad. • Soporte para servicios críticos. • Aislamiento lógico mediante slicing.	• Coste elevado de despliegue y operación. • Dependencia fuerte del operador. • Uso limitado a casos muy específicos. • Complejidad contractual y técnica.	Control en tiempo real de infraestructuras críticas y tráfico urbano.
Zigbee (802.15.4)	• Muy bajo consumo. • Topología mesh que mejora la cobertura interior. • Amplia adopción en edificios inteligentes. • Coste reducido por dispositivo.	• Alcance limitado. • Alta exposición física de los nodos. • Gestión compleja de claves. • No adecuada para grandes áreas urbanas.	Automatización y control energético en edificios municipales.
Bluetooth Low Energy (BLE)	• Amplia compatibilidad con dispositivos móviles. • Bajo consumo energético. • Despliegue rápido y económico. • Adecuada para servicios de proximidad.	• Alcance muy limitado. • Alta exposición en entornos públicos. • Riesgos de privacidad y rastreo. • No adecuada para sensorización continua.	Servicios de proximidad, guiado interior e interacción con la ciudadanía.
Arquitecturas mesh propietarias	• Integración directa en infraestructuras existentes. • Extensión de cobertura sin infraestructura densa. • Diseñadas para servicios urbanos específicos. • Funcionamiento probado en despliegues históricos.	• Dependencia fuerte del proveedor. • Falta de estándares abiertos. • Dificultad de auditoría de seguridad. • Riesgo de obsolescencia tecnológica.	Alumbrado público y sistemas urbanos heredados en explotación.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Tecnología	Ventajas principales	Desventajas principales	Caso de uso más recomendable
Wi-Fi HaLow (802.11ah)	• Conectividad IP nativa. • Mayor alcance que Wi-Fi tradicional. • Mejor penetración en interiores. • Integración con redes IP existentes.	• Implantación limitada en entornos reales. • Ecosistema industrial reducido. • Operación en espectro no licenciado. • Responsabilidad operativa directa.	Monitorización IP de instalaciones técnicas con cobertura propia.

13. Referencias y enlaces a información adicional

1. Boletín Oficial del Estado (BOE). (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*.
https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

2. European Commission. (2021). *Guidance on qualification and classification of software in Regulation (EU)*.
https://ec.europa.eu/docsroom/documents/37581

3. European Union. (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements*.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

4. International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
https://www.iso.org/standard/27001

5. International Organization for Standardization. (2021). *IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices*.
https://www.iso.org/standard/72026.html

6. International Organization for Standardization. (2019). *ISO/IEC 27018:2019: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
https://www.iso.org/standard/76559.html

7. International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements*.
https://www.iso.org/standard/75106.html

8. International Organization for Standardization. (2015). *ISO/IEC 27017:2015: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.
https://www.iso.org/standard/43757.html

9. Oficina de Seguridad del Ciberespacio (OSC-España). (2024). *Guía sobre Seguridad en Dispositivos IoT*.
https://occ.ses.mir.es/publico/occ/dam/jcr:a97a3ac9-1a92-4af0-a5c0-3ac8557244ba/Gu%C3%ADa%20sobre%20Seguridad%20en%20Dispositivos%20IoT.pdf

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

10. OWASP Foundation. (2023). *OWASP Internet of Things Project.* https://owasp.org/www-project-internet-of-things/

11. RedesTelecom. (2017). *Seguridad en IoT: riesgos y desafíos de la Internet de las Cosas*. https://www.redestelecom.es/especiales/seguridad-en-iot-riesgos-y-desafios-de-la-internet-de-las-cosas/

14. Otras referencias de interés

El presente apartado recoge un resumen de los principales temas abordados en la guía, así como la relación de productos y servicios mencionados en ella. Su finalidad es ofrecer una visión global de los ámbitos tratados y facilitar la identificación de posibles referencias o elementos relevantes para futuras consultas o ampliaciones documentales.

14.1. Lista de materias tratadas en la guía

- Ecosistema IoT en Smart Cities
- Tecnologías de comunicación IoT
- LPWAN en bandas no licenciadas: LoRaWAN y LTE-M
- LPWAN celulares (3GPP): NB-IoT y LTE-M
- 5G aplicado a IoT urbano: mMTC y URLLC
- Redes locales de corto alcance: Zigbee y BLE
- Tecnologías IoT complementarias: Redes mesh y Wi-Fi HaLow

14.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

14.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Tecnologías de Comunicación IoT para Smart Cities

Febrero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía