

Módulo 3.1: Introducción al IoT

MSc. Carlos Cedeño

Al finalizar esta sesión, definir qué es el IoT y aprenderás a pensar como un arquitecto de soluciones IoT, considerando los elementos clave para diseñar proyectos que sean viables, escalables y seguros.

1. El Dilema de la Comunicación en IoT

Imagina que tienes 10,000 sensores de temperatura repartidos por una ciudad. Deben funcionar con una pequeña batería durante 5 años y reportar la temperatura cada 15 minutos.

- ¿Cómo logramos que se comuniquen de forma eficiente?
- ¿Cómo gestionamos el consumo de energía para que la batería dure años?
- ¿Cómo aseguramos que los mensajes lleguen de forma fiable?

Durante décadas, "Internet" significaba conectar personas a través de computadoras. El **Internet de las Cosas (IoT)** representa la siguiente evolución: conectar **objetos** del mundo físico a Internet.

Definición simple: IoT es una red de objetos físicos (cosas) equipados con sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet.

Ejemplos que ya vives:

- **Hogar Inteligente:** Un termostato que ajusta la temperatura según si estás en casa o no.
- **Wearables:** Un reloj que monitorea tu ritmo cardíaco y niveles de actividad.
- **Ciudades Inteligentes:** Sensores de aparcamiento que te indican en una app dónde hay un lugar libre.
- **Industria:** Un motor en una fábrica que avisa que necesita mantenimiento *antes* de que se rompa.

2. Pensando como un Arquitecto de IoT: Las 5 Capas del Diseño

Crear una solución de IoT es como construir un edificio. Requiere un plano y considerar múltiples capas interconectadas. Un fallo en una capa puede derrumbar todo el sistema.

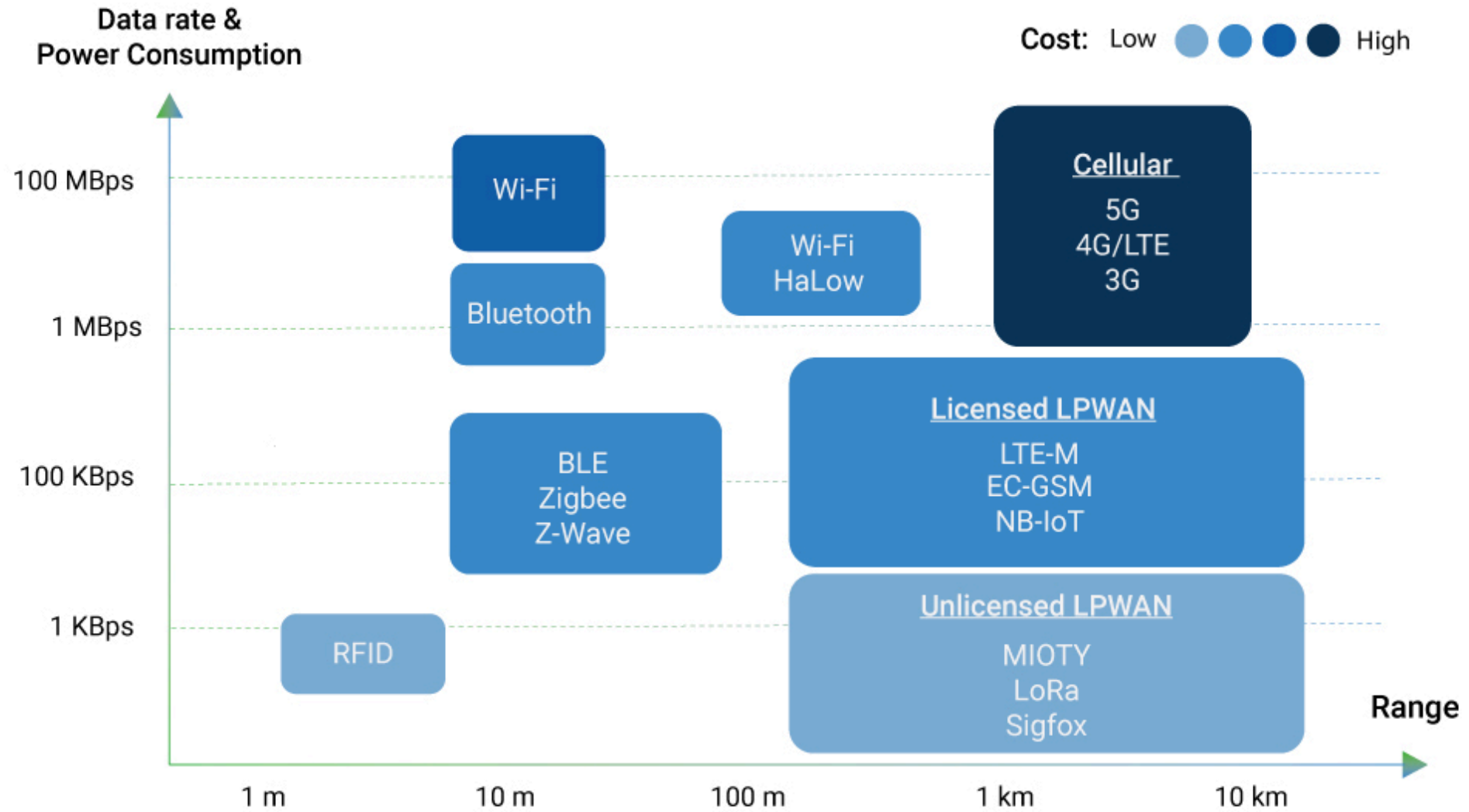
Capa 1: El Dispositivo (La "Cosa")

Es la base de todo. Aquí nos preguntamos:

- **Hardware:** ¿Qué microcontrolador o procesador necesito? (¿Un simple ESP32 o una potente Raspberry Pi?)
- **Sensores/Actuadores:** ¿Qué necesito medir (temperatura, movimiento, GPS)? ¿Qué necesito hacer (encender una luz, cerrar una válvula)?
- **Gestión de Energía:** ¿Funcionará con batería o estará conectado a la red eléctrica? Esta es una de las decisiones más críticas. ¡Define la viabilidad de muchos proyectos!

Capa 2: La Conectividad

- **Corto Alcance:**
 - **Wi-Fi:** Gran ancho de banda, pero alto consumo de energía. Ideal para interiores.
 - **Bluetooth / Zigbee / Z-Wave:** Bajo consumo de energía, ideal para redes personales (domótica, wearables).
- **Largo Alcance (LPWAN - Low Power Wide Area Network):**
 - **LoRaWAN / Sigfox:** Alcance de kilómetros, muy bajo consumo de energía (baterías que duran años), pero bajo ancho de banda (solo para enviar datos pequeños).
 - **Celular (4G/5G/NB-IoT):** Gran cobertura y ancho de banda, pero mayor costo y consumo de energía.



Capa 3: La Plataforma y el Procesamiento de Datos

Los datos de los sensores son inútiles si no se recopilan, procesan y almacenan.

- **Ingesta de Datos:** ¿Cómo recibimos los miles de mensajes de nuestros dispositivos? (Aquí es donde entran protocolos como **MQTT**).
- **Procesamiento:** ¿Necesitamos actuar en tiempo real (análisis de streaming) o podemos procesar los datos por lotes (batch)?
- **Almacenamiento:** ¿Qué tipo de base de datos necesitamos? (Bases de datos de series temporales como InfluxDB son muy populares en IoT).
- **Plataformas IoT:** Servicios como AWS IoT, Google Cloud IoT o Microsoft Azure IoT que nos dan todas estas herramientas ya integradas.

Capa 4: La Aplicación y la Experiencia de Usuario (UX)

Es la capa visible para el usuario final. ¿Cómo interactuamos con los datos y controlamos los dispositivos?

- **Paneles de Control (Dashboards):** Para visualizar tendencias y estados en tiempo real (ej. Grafana).
- **Aplicaciones Móviles:** Para controlar tu hogar inteligente o ver tu actividad física.
- **Sistemas de Alertas:** Notificaciones por email, SMS o push cuando algo anormal sucede.

Capa 5: Seguridad y Privacidad (¡La capa transversal y no negociable!)

La seguridad no es un añadido, sino un requisito desde el primer día en todas las capas.

- **En el Dispositivo:** Asegurar que no pueda ser hackeado físicamente.
- **En la Red:** Cifrar todas las comunicaciones (usando TLS/DTLS).
- **En la Nube:** Proteger los datos almacenados y gestionar quién tiene acceso a ellos.
- **Privacidad:** Ser transparentes sobre qué datos se recopilan y para qué se usan. Un solo fallo de seguridad puede destruir la confianza del cliente y la reputación de la empresa.

3. La Importancia Crítica de la Arquitectura de Comunicación

Antes de elegir un protocolo, debemos pensar como arquitectos. La forma en que nuestros dispositivos se comunican define el éxito o el fracaso de un proyecto de IoT. Una mala decisión aquí puede llevar a:

- **Baterías agotadas en semanas** en lugar de años.
- **Costos de red y datos móviles disparados** por tráfico ineficiente.
- **Sistemas que colapsan** cuando el número de dispositivos crece.
- **Pérdida de datos críticos** por una comunicación no fiable.

Diseñar la arquitectura de comunicación no es un paso técnico, es el pilar estratégico de tu proyecto. Debes preguntarte: ¿Necesito que un sensor hable con una aplicación (1 a 1)? ¿O que un sensor envíe datos que muchos sistemas deben recibir (1 a muchos)? ¿La entrega del dato es crítica o puedo permitirme perder alguno ocasionalmente?

Cómo diseñar una solución para IoT

- **Identifica un problema:** Piensa en un problema o una ineficiencia en tu casa, tu barrio o tu lugar de estudio.
- **Diseña una solución IoT (en papel):** Sin escribir una línea de código, intenta describir las 5 capas de tu solución.
 - ¿Qué sensor usarías? ¿Necesitaría batería?
 - ¿Cómo lo conectarías a Internet?
 - ¿Qué harías con los datos?
 - ¿Cómo lo visualizarías?
 - ¿Cuál sería el mayor riesgo de seguridad?

4. Trabajos relacionados para IoT

- **Ingenieros de Hardware y Firmware:** Para diseñar los dispositivos.
- **Desarrolladores de Software:** Para construir las plataformas y aplicaciones.
- **Científicos de Datos:** Para encontrar patrones y valor en los datos generados.
- **Expertos en Ciberseguridad:** Para proteger todo el ecosistema.
- **Diseñadores de UX/UI:** Para hacer que la tecnología sea útil y fácil de usar.