GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCÍA DIGITAL

Internet de las Cosas (IoT)

Departament d'informàtica.
Autor: Francisco Aldarias Raya
Febrero-2026

Preparació Proves d'Accés

ÍNDEX

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

[Importante]

[Atención]

[Interesante]

1 Introducción

En las últimas décadas hemos pasado de tener **unos pocos ordenadores** conectados a Internet a convivir con **millones de dispositivos inteligentes**: relojes, altavoces, cámaras, termostatos, sensores de movimiento, bombillas Wi-Fi, pulseras deportivas, robots de cocina conectados, etc.

A esta enorme red de **objetos físicos con capacidad de comunicarse por Internet** la llamamos **Internet de las cosas** o **IoT (Internet of Things)**.

La IoT es una de las tecnologías clave de la **transformación digital**: está cambiando la manera en la que producimos, consumimos energía, nos desplazamos por las ciudades o cuidamos la salud.(techfablab.es)

En este tema veremos:

- Qué es exactamente el Internet de las cosas.
- De qué elementos se compone un sistema IoT.
- Cómo se conectan y comunican los dispositivos.
- Ejemplos prácticos en la vida diaria y en distintos sectores.
- Riesgos, seguridad y cuestiones éticas que debemos conocer como ciudadanos digitales.

2 ¿Qué es el Internet de las cosas?

2.1 Definición básica

Internet de las cosas (IoT) es la red formada por **objetos físicos** equipados con:

- **Sensores** (captan datos: temperatura, luz, movimiento, posición…).
- **Actuadores** (ejecutan acciones: encender un motor, abrir una válvula, subir persianas…).
- **Conectividad** (Wi-Fi, Bluetooth, 4G/5G, etc.).

- A veces, cierta **capacidad de procesamiento** (microcontroladores, pequeños sistemas embebidos).

Estos dispositivos pueden **enviar y recibir datos por Internet**, comunicarse entre sí y con aplicaciones en la nube, y actuar de forma **automática o semiautomática**.

Ejemplos de objetos IoT:

- Termostatos inteligentes que regulan la calefacción según la temperatura y nuestra presencia.
- Sensores de humedad en cultivos que activan el riego solo cuando hace falta.
- Relojes inteligentes que miden pasos, ritmo cardíaco y calidad del sueño.
- Sensores de aparcamiento y semáforos conectados en una “ciudad inteligente”.

2.2 De Internet de personas a Internet de las cosas

En los inicios, Internet conectaba principalmente:

- Ordenadores de sobremesa.
- Algunos servidores.

Después se sumaron:

- Portátiles, móviles y tablets.
- Televisores y consolas.

Hoy se conectan **todo tipo de “cosas”**, muchas de ellas pequeñas y casi invisibles: sensores en fábricas, contadores de agua y luz, cámaras, vehículos, wearables…

Se calcula que hay **decenas de miles de millones** de dispositivos IoT en el mundo, y el número sigue creciendo cada año.(techfablab.es)

Figura 1: Línea de tiempo con la evolución de la IoT. Fuente: ChatGPT

3 Arquitectura básica de un sistema IoT

Aunque existen muchas variaciones, la mayoría de soluciones IoT siguen una **arquitectura por capas**.

3.1 Capa de dispositivos (sensores y actuadores)

Es la parte "física" del IoT:

- **Sensores**: temperatura, humedad, luz, movimiento, presión, sonido, posición GPS, nivel de batería, etc.
- **Actuadores**: relés para encender o apagar aparatos, motores, válvulas, luces, alarmas…

Estos dispositivos suelen contar con:

- Un **microcontrolador** (por ejemplo, ESP32, Arduino, etc.).
- Una **interfaz de comunicación** (Wi-Fi, Bluetooth, radio de baja potencia…).
- Alimentación (batería, pilas, red eléctrica, energía solar).

3.2 Capa de comunicación

Se encarga de **llevar los datos** desde los dispositivos hasta otros sistemas (pasarela, servidores) y de recibir órdenes.

Los dispositivos IoT pueden comunicarse:

- Directamente con Internet (por ejemplo, por Wi-Fi).

- A través de una **pasarela o gateway**: un dispositivo intermedio que recoge datos de muchos sensores locales (por radio, Zigbee, LoRa…) y los envía a Internet por Ethernet, fibra o 4G/5G.

3.3 Capa de procesamiento y almacenamiento (nube o servidores)

Los datos enviados por los dispositivos se almacenan y procesan en:

- **Servidores en la nube** (cloud): Amazon Web Services, Microsoft Azure, Google Cloud…
- Servidores propios de la empresa o del centro.

En esta capa se pueden:

- Guardar grandes cantidades de datos (historiales).
- Analizar la información (estadísticas, gráficos, IA, aprendizaje automático).
- Detectar patrones y generar alarmas (por ejemplo, consumo anómalo de energía).

3.4 Capa de aplicaciones y usuarios

Es la parte que vemos los usuarios:

- Aplicaciones móviles.
- Páginas web de control.
- Cuadros de mando (dashboards).
- Integraciones con otros sistemas (por ejemplo, avisos por correo o mensajes push).

Desde aquí podemos:

- Ver el estado de los dispositivos.
- Recibir notificaciones.
- Enviar órdenes (encender luces, cambiar temperatura, etc.).

4 Tecnologías de comunicación en IoT

En IoT se utilizan muchas tecnologías de red. Aquí veremos las más importantes, sobre todo las que se pueden relacionar con redes LAN (tema que también entra en el currículo).

4.1 Tecnologías para distancias cortas

4.1.1 Wi-Fi

Muy usada en hogares y oficinas:

- Ventajas: alta velocidad, routers muy extendidos.
- Inconvenientes: consumo de energía relativamente alto para sensores a pilas; alcance limitado.

Es habitual que **dispositivos del hogar conectado** (enchufes inteligentes, bombillas, cámaras) se conecten directamente al **router Wi-Fi** de la casa.

4.1.2 Wi-Fi para IoT

La **Red IoT** es una **SSID (nombre de red Wi-Fi) dedicada específicamente para dispositivos del Internet de las Cosas (IoT)** —por ejemplo, **enchufes inteligentes, luces inteligentes, cámaras IP, sensores, asistentes de voz, termostatos, etc.**.

En lugar de conectar todos los dispositivos de casa (móviles, PCs, tablets y dispositivos IoT) a la **misma red Wi-Fi principal**, la Red IoT te permite crear **una red separada únicamente para esos dispositivos inteligentes**.

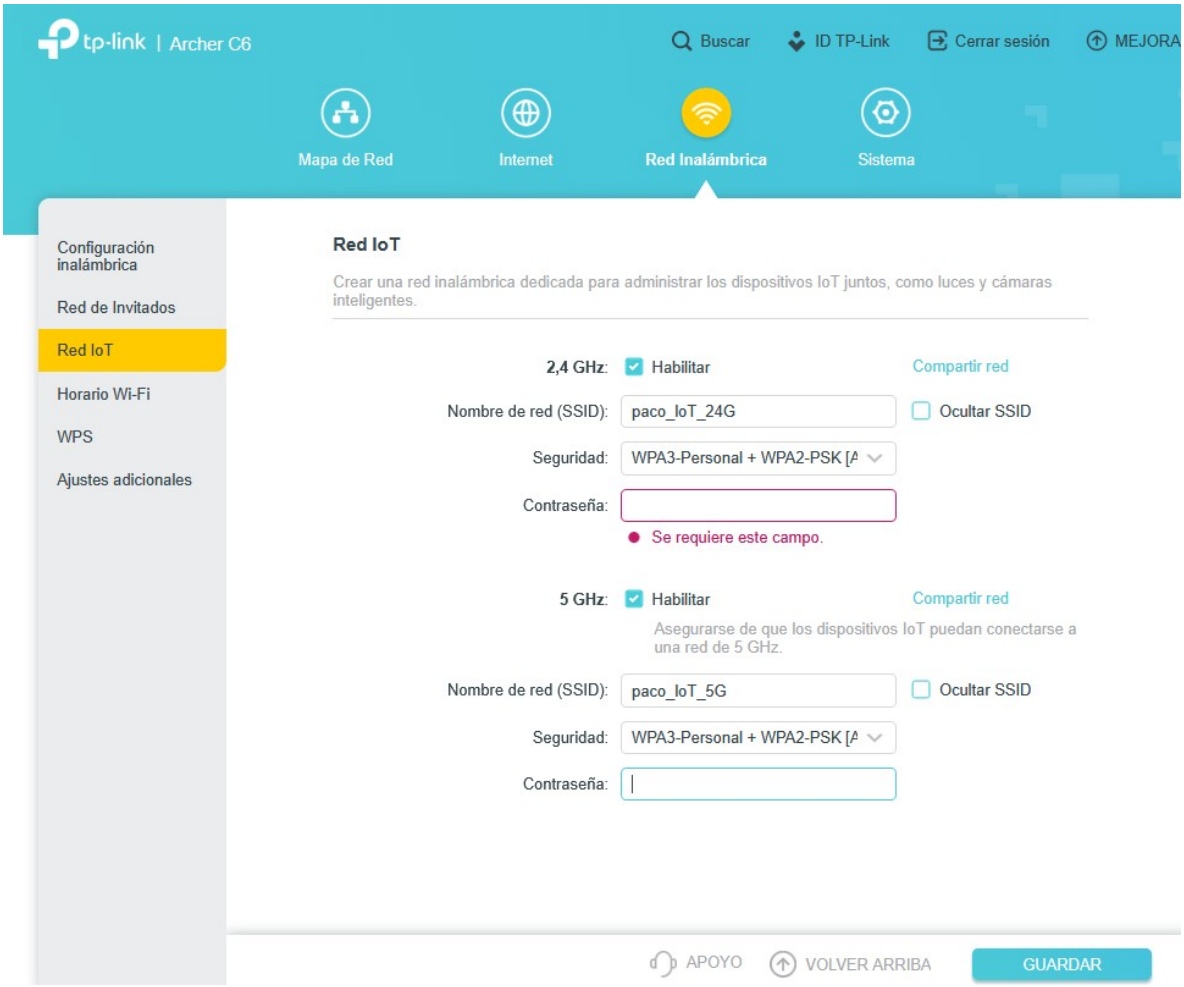

Figura 2: Red IoT" en el router TP-Link Archer C6

Para poder comunicarnos con los dispositivos de la red domestica se utiliza de un ordenador servidor externo que hace de intermediario. Es decir, que no nos conectamos directamente con el dispositivo sino con un ordenador remoto que cada x tiempo le informa al dispositivo de su estado. Esto se debe a que los dispositivos domésticos están detrás del router que tienen ips privadas en lugar de ips públicas.

- https://www.xataka.com/basics/chromecast-que-como-funciona-que-se-puede-hacer

4.1.3 Bluetooth y Bluetooth Low Energy (BLE)

- Alcance corto (habitualmente unos metros).
- BLE está optimizado para **bajo consumo**, lo que lo hace ideal para pulseras deportivas, relojes, sensores cercanos al móvil, etc.(Fempa)

Se suele usar:

- Para comunicar el dispositivo con el **móvil**, que actúa como pasarela hacia Internet.

4.1.3 Zigbee, Z-Wave y otros

Son tecnologías pensadas para:

- Redes de sensores en el hogar y automatización (domótica).
- Formar **redes malladas**: cada dispositivo ayuda a repetir la señal.

Ventajas:

- Bajo consumo.
- Redes flexibles con muchos nodos.

Inconvenientes:

- Requieren un **hub o pasarela** conectado al router para llegar a Internet.(Fempa)

4.2 Tecnologías para largas distancias

4.2.1 Redes móviles (3G, 4G, 5G)

Muchos dispositivos IoT se conectan mediante **tarjetas SIM o eSIM**:

- Cámaras de vigilancia sin Wi-Fi.
- Contadores inteligentes de agua, gas o luz.
- Sensores en vehículos (geolocalización, flotas).

El 5G está especialmente pensado para IoT masivo: puede gestionar **miles de dispositivos por antena con baja latencia**.(techfablab.es)

4.2.2 LPWAN (Low Power Wide Area Network)

Son tecnologías diseñadas para:

- Bajísimo consumo de energía.
- Grandes distancias (varios kilómetros).
- Transmisión de pocos datos (por ejemplo, una medición cada 10 minutos).

Ejemplos:

- LoRaWAN.
- Sigfox (en algunos países).

Son muy usadas en **agricultura, ciudades inteligentes e industria**.

5 Protocolos y estándares en IoT

Además de las tecnologías físicas de comunicación, IoT utiliza **protocolos** que definen cómo se intercambian los datos.

5.1 IP, TCP/UDP y HTTP/HTTPS

Muchos dispositivos IoT usan protocolos "clásicos de Internet":

- **IPv4 e IPv6**: direcciones IP de los dispositivos o pasarelas.(Fempa)
- **TCP y UDP**: transporte de datos (TCP es fiable, UDP más ligero).
- **HTTP/HTTPS**: para enviar datos a servidores web, APIs REST, etc.

En IoT es especialmente importante **HTTPS**, ya que cifra la comunicación y protege los datos enviados por los dispositivos.

5.2 Protocolos específicos de IoT

Algunos muy habituales son:

5.2.1 MQTT (Message Queuing Telemetry Transport)

- Protocolo ligero de **publicación-suscripción**.
- Ideal para enviar pequeños mensajes desde muchos dispositivos a un servidor ("broker").
- Muy usado en domótica, sensores, automatización.

Ejemplo:
Un sensor de temperatura "publica" datos en el tema `casa/salon/temperatura` y una app "se suscribe" para recibirlos.

5.2.2 CoAP (Constrained Application Protocol)

- Diseñado para dispositivos con pocos recursos.
- Funciona sobre UDP, similar a HTTP pero más ligero.
- Útil para redes de sensores con baja potencia de procesamiento.

6 Ejemplos de aplicaciones de IoT

6.1 Hogar inteligente (domótica)

Ejemplos típicos:

- Enchufes inteligentes que se controlan por app o por voz.
- Bombillas LED conectadas que cambian de color y se programan.
- Termostatos que aprenden nuestras rutinas y ahorran energía.
- Robots aspiradores que se pueden arrancar desde el móvil.

Ventajas:

- Comodidad (automatización de tareas).
- Ahorro energético (apagar luces, regular calefacción).
- Mayor seguridad (sensores de humo, fugas de gas, cámaras).

Riesgos:

- Si la red Wi-Fi o las contraseñas están mal configuradas, un intruso podría tomar control de los dispositivos.

6.2 Ciudades inteligentes

Las **smart cities** incorporan IoT para:

- Gestionar el tráfico (sensores, semáforos inteligentes).
- Monitorizar la calidad del aire.
- Gestionar el alumbrado público (encendido según presencia o luz ambiente).
- Controlar contenedores de basura (llenos/vacíos).(ces.gva.es)

Objetivos:

- Mejorar la calidad de vida de los ciudadanos.
- Reducir consumo energético y contaminación.
- Optimizar servicios públicos.

6.3 Industria 4.0

En fábricas y empresas:

- Sensores en máquinas que detectan vibraciones anómalas.
- Sistemas de mantenimiento predictivo (se arregla antes de que se rompa).
- Trazabilidad de productos en tiempo real.(techfablab.es)

Beneficios:

- Menos paradas por averías.
- Mayor eficiencia y calidad en la producción.

6.4 Salud y deporte

- Pulseras y relojes que miden pasos, calorías, ritmo cardíaco.
- Dispositivos médicos conectados (medidores de glucosa, tensiómetros).
- Telemedicina: envío de datos desde casa al hospital.

Ventajas:

- Monitorización continua de pacientes.
- Detección temprana de problemas.

Riesgos:

- Datos de salud muy sensibles: es crítico proteger la **privacidad** y el uso ético de la información.

6.5 Agricultura y medio ambiente

- Sensores de humedad y temperatura en suelos.

- Estaciones meteorológicas conectadas.
- Control remoto de riego y fertilización.

Resultados:

- Uso más eficiente del agua.
- Menos productos químicos.
- Mejores cosechas.

7 Datos masivos, análisis e inteligencia artificial

Los sistemas IoT generan una enorme cantidad de datos (**Big Data**). Para sacarles partido se utilizan:

- Herramientas de **almacenamiento en la nube**.
- Plataformas de análisis de datos (estadística, gráficos).
- **Modelos de inteligencia artificial** que aprenden patrones.

Ejemplo:

- Una red de sensores de energía en un edificio recopila datos cada minuto.
- Un sistema de IA detecta consumos anómalos y propone medidas de ahorro.

Para el nivel de prueba de acceso, es suficiente entender que:

- IoT **no es solo "cosas conectadas"**, sino también **datos + análisis + decisiones automatizadas**.

8 Riesgos, seguridad y privacidad en IoT

La implantación masiva de IoT plantea retos importantes de seguridad y protección de datos. La propia Generalitat insiste en la necesidad de formar una **ciudadanía digital crítica y responsable**.(JurisNoticias)

8.1 Riesgos principales

1. **Ataques a dispositivos inseguros**
    - Contraseñas por defecto.
    - Falta de actualización de firmware.
    - Puertos abiertos sin control.
2. **Robo de información**
    - Datos personales (hábitos, horarios, ubicación, salud…).
    - Información empresarial sensible.
3. **Perdida de control físico**
    - Encendido/apagado de sistemas críticos (cerraduras, alarmas, vehículos).
    - Manipulación de semáforos, sistemas industriales, etc.

4. **Vigilancia excesiva**
    - Cámaras en casa, micrófonos, sensores en el trabajo.
    - Riesgo de usos abusivos por parte de empresas o gobiernos.

8.2 Buenas prácticas de seguridad en IoT

Como usuarios y futuros profesionales, conviene seguir algunas **reglas básicas**:

1. **Cambiar siempre las contraseñas por defecto**
    - Poner claves robustas (mezcla de letras, números y símbolos).
    - Usar contraseñas diferentes para diferentes servicios.
2. **Actualizar el firmware de los dispositivos**
    - Muchos fabricantes corrigen fallos de seguridad con actualizaciones.
    - Comprobar periódicamente si hay nuevas versiones.
3. **Proteger la red Wi-Fi**
    - Usar WPA2 o WPA3.
    - Desactivar WPS.
    - Crear red de invitados para móviles de visitas y algunos dispositivos IoT.(Fempa)
4. **Segregar redes**
    - Separar la red de administración/trabajo de la red de dispositivos IoT cuando sea posible (subredes, VLAN).
5. **Revisar la política de privacidad**
    - Antes de instalar una app IoT, leer qué datos recoge y cómo los usa.
    - Desactivar permisos innecesarios.
6. **Desconectar lo que no se usa**
    - Desactivar funciones “siempre encendido” si no son esenciales.
    - Apagar dispositivos que no necesitan estar conectados 24/7.

9 Impacto social, ético y ambiental del IoT

El currículo de competencia digital en la Comunitat Valenciana insiste en **valorar las implicaciones éticas y ecosociales** de las tecnologías.(JurisNoticias)

9.1 Beneficios sociales

- Mejora de la eficiencia energética (edificios y ciudades más sostenibles).
- Optimización del transporte y reducción de atascos.
- Mejor atención sanitaria en zonas rurales gracias a telemedicina.
- Aumento de la seguridad en el hogar y en el trabajo.

9.2 Problemas y dilemas éticos

- **Privacidad**: ¿quién controla los datos generados por los sensores?
- **Transparencia**: muchas veces no sabemos qué información están recopilando los dispositivos.
- **Vigilancia**: riesgo de sociedades demasiado controladas (cámaras por todas partes, sensores en el lugar de trabajo).
- **Desigualdad digital**: no todas las personas ni regiones tienen acceso equitativo a estas tecnologías.

9.3 Impacto ambiental

Aspectos positivos:

- Ahorro de energía y recursos (todo más medido y optimizado).

Aspectos negativos:

- Producción de millones de dispositivos (consumo de materiales, residuos electrónicos).
- Necesidad de diseñar sistemas IoT **reparables y reciclables**, con mayor vida útil.

Como ciudadanía digital crítica, es importante:

- Valorar **no solo la comodidad**, sino también los efectos a largo plazo.
- Exigir a empresas y administraciones un uso **ético y sostenible** de estas tecnologías.

10 IoT y currículo de “Tratamiento de la información y competencia digital”

Aunque el temario oficial de la prueba se centra en contenidos como:

- Arquitectura básica de sistemas informáticos.
- Redes, Internet y servicios en la nube.
- Seguridad informática y ciudadanía digital.(pruebaaccesogradosuperior.com)

El IoT encaja en varios bloques:

1. **Redes y comunicaciones**
    - Lancemos la visión de que una LAN ya no conecta solo ordenadores, sino también “cosas” (sensores, cámaras…).
2. **Sociedad digital**
    - IoT como parte de la digitalización de empresas, ciudades y hogares.
3. **Seguridad y protección de datos**
    - Riesgos específicos de IoT (dispositivos expuestos, datos continuos, salud, geolocalización).
4. **Competencia ciudadana**

- Uso responsable y crítico de tecnologías emergentes.

Por tanto, comprender el Internet de las cosas te ayudará no solo a aprobar la prueba, sino a interpretar muchas noticias y situaciones de tu vida diaria relacionadas con tecnología.

11 Actividades propuestas

Algunas actividades que podrías usar con el alumnado (o proponer como tareas):

1. **Detectives IoT en casa**
    - Lista de objetos que ya están conectados a Internet (televisión, router, móvil, reloj…).
    - Responder: ¿qué datos recogen?, ¿qué riesgos pueden tener?, ¿qué medidas de seguridad aplicarías?
2. **Diseño de una mini-red IoT para un aula**
    - Elegir: sensores de temperatura, presencia, luz…
    - Esquematizar cómo se conectan (Wi-Fi, router, nube).
    - Proponer qué información mostraría el panel de control.
3. **Debate sobre privacidad**
    - ¿Aceptarías que en tu ciudad se midan tus movimientos mediante cámaras inteligentes para mejorar el tráfico?
    - ¿Dónde pondrías los límites?
4. **Cuestionario de repaso**
    - Definir IoT.
    - Nombrar dos tecnologías inalámbricas de corto alcance.
    - Explicar qué es un sensor y qué es un actuador.
    - Citar tres medidas de seguridad básicas en una red IoT doméstica.

12 Resumen del tema

- El **Internet de las cosas (IoT)** es la red formada por **objetos físicos conectados a Internet**, capaces de recoger datos y actuar sobre el entorno.
- Un sistema IoT se compone de **dispositivos (sensores/actuadores)**, **red de comunicación**, **servidores o nube** y **aplicaciones** que usan esos datos.
- Utiliza diversas **tecnologías de comunicación** (Wi-Fi, Bluetooth, Zigbee, 4G/5G, LoRa…) y protocolos como **MQTT** o **CoAP**, además de los clásicos **IP, TCP, HTTP**.
- Tiene aplicaciones en el **hogar, las ciudades, la industria, la salud y la agricultura**, entre otros sectores.
- Genera grandes volúmenes de datos que se analizan con técnicas de **Big Data** e **inteligencia artificial** para tomar decisiones automáticas o asistidas.

- Plantea importantes **retos de seguridad y privacidad**, que hacen necesario configurar bien redes y dispositivos, y adoptar buenas prácticas de uso.
- Su impacto no es solo técnico: también tiene **implicaciones sociales, éticas y ambientales**, que debemos conocer para ejercer una **ciudadanía digital crítica y responsable**.

Con este tema los alumnos cuentan con una base sólida para entender las preguntas relacionadas con el Internet de las cosas que puedan aparecer en la **Prueba de acceso a ciclos formativos de grado superior** y, sobre todo, para interpretar la presencia cada vez mayor de estos sistemas en su vida cotidiana.

13 Biblbiografía

1. Materiales divulgativos de la propia Generalitat sobre IoT y sociedad digital.(cindi.gva.es)