RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

# Ciberseguridad IoT en Smart Cities: Retos y Amenazas

**Noviembre de 2025**

**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, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 25/11/2025

Fecha de última actualización: 25/11/2025

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE TABLAS





Financiado por la Unión Europea NextGenerationEU

# ÍNDICE DE FIGURAS

# 1. Introducción

El desarrollo de las Smart Cities representa uno de los mayores avances tecnológicos y sociales de los últimos años. La integración de Internet de las Cosas (IoT) en los entornos urbanos ha permitido mejorar la eficiencia de los servicios públicos, optimizar recursos, reducir costes operativos y ofrecer una mejor calidad de vida a los ciudadanos. Desde la gestión del tráfico y el alumbrado inteligente hasta los sistemas de salud conectados o la monitorización ambiental, el IoT se ha convertido en la columna vertebral del ecosistema urbano moderno.

Sin embargo, esta creciente interconectividad también ha ampliado la superficie de exposición a ciberamenazas. Cada sensor, cámara o dispositivo conectado constituye un posible punto de entrada para ataques que pueden comprometer datos personales, infraestructuras críticas o incluso la seguridad física de las personas. Las ciudades inteligentes, al depender cada vez más de sistemas digitales integrados, se enfrentan a riesgos que van más allá del ámbito puramente tecnológico, afectando directamente a la gobernanza, la privacidad y la resiliencia de los servicios urbanos.

En este contexto, la ciberseguridad del IoT en Smart Cities se ha convertido en un pilar esencial para garantizar la confianza, la continuidad de los servicios y la protección de los ciudadanos. La gestión de estos riesgos requiere un enfoque integral que combine tecnología, regulación, concienciación y cooperación entre los sectores público y privado.

# 2. Objetivo y alcance

## 2.1. Objetivo

La presente guía tiene como propósito ofrecer una visión estructurada y práctica sobre los retos, amenazas y tendencias en materia de ciberseguridad IoT en entornos urbanos, sirviendo como base para el diseño y la actualización de políticas, estrategias y procedimientos orientados a fortalecer la seguridad de las ciudades inteligentes.

A través del análisis de las superficies de ataque, los riesgos tecnológicos y organizativos, y los marcos regulatorios emergentes, se pretende:

- Identificar las principales vulnerabilidades y amenazas en los entornos IoT urbanos.
- Analizar los desafíos de gobernanza, interoperabilidad y responsabilidad compartida.
- Revisar los marcos normativos, estándares y buenas prácticas aplicables.
- Ofrecer recomendaciones orientadas a la mejora de la seguridad y resiliencia de las Smart Cities.

De esta forma, la guía busca servir como herramienta de apoyo para responsables de ciberseguridad, administraciones públicas, operadores de servicios urbanos y entidades tecnológicas que participan en el desarrollo o gestión de infraestructuras conectadas.

## 2.2. Alcance

El documento aborda los aspectos de ciberseguridad vinculados al uso y despliegue de tecnologías IoT en el ámbito urbano, con especial atención a su integración en sistemas críticos y servicios públicos.

Incluye el análisis de:

- Arquitecturas y componentes del ecosistema IoT en Smart Cities.
- Superficies de ataque y riesgos específicos del entorno urbano conectado.
- Amenazas técnicas, físicas y de privacidad.
- Retos de interoperabilidad, estandarización y gobernanza.
- Tendencias emergentes en ciberseguridad, inteligencia artificial y regulación.

### 2.3. Metodología

La elaboración de esta guía se ha basado en una revisión exhaustiva de marcos normativos, estándares internacionales y documentos de referencia en materia de ciberseguridad e IoT.

Asimismo, se ha complementado con el análisis de casos reales, estudios de incidentes y revisiones de estrategias de organismos públicos sobre Smart Cities y ciberseguridad urbana en distintas regiones.

El enfoque metodológico combina la identificación de riesgos y evaluación de amenazas con una visión estratégica orientada a la resiliencia y gobernanza, buscando alinear los principios de ciberseguridad con los objetivos de sostenibilidad e innovación tecnológica de las ciudades inteligentes.

## 3. Referencias normativas

El presente documento se fundamenta en un marco regulador y técnico amplio, que combina normativa legal, estándares internacionales y guías de buenas prácticas, con el objetivo de asegurar la alineación con las exigencias del sector urbano, la protección de los datos personales y la resiliencia de los entornos IoT en las Smart Cities.

Estas referencias constituyen la base metodológica y conceptual sobre la que se estructura la guía, garantizando la coherencia con las políticas europeas, nacionales e internacionales en materia de ciberseguridad, privacidad y gestión de infraestructuras críticas.

- **Normativas**:
  - Reglamento (UE) 2024/1680 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
  - Reglamento (UE) 2016/679: relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD).
  - 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).
  - Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).
  - Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
- **Estándares**:
  - ISO/IEC 30141, Arquitectura de referencia para sistemas IoT.



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

- 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 24518, Gestión de crisis en el suministro de agua.
- ISO/IEC 22301, Gestión de la continuidad de negocio.
- ISO/IEC 50001, Gestión del suministro eléctrico.
- ISO/SAE 21434, Gestión de riesgos de ciberseguridad en transporte conectado.
- IEC 62443, Seguridad para sistemas de automatización y control industrial.
- ETSI EN 303 645, Requisitos de ciberseguridad para dispositivos IoT de consumo.
- UNE 178107 y 178108, 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).
  - NIST IR 8259 Serie, Guía de Ciberseguridad para fabricantes de dispositivos IoT.
  - NIST SP 800-213 Serie, Guía de Ciberseguridad para dispositivos IoT.
  - 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 |
|---|---|
| **Ataque Man-In-The Middle** | Técnica de interceptación en la que un atacante se sitúa entre dos partes que se comunican, capturando, modificando o redirigiendo la información sin que lo detecten. |
| **API** | Conjunto de reglas que permiten que programas se comuniquen entre sí (del inglés, Application Programming Interface). |
| **Botnet** | Red de dispositivos infectados con programas maliciosos que son controlados de forma remota por un atacante, sin que los usuarios lo sepan |
| **Cloud Computing** | Modelo de prestación de servicios que permite acceder a recursos a través de internet, sin necesidad de infraestructura física local. |
| **Edge Computing** | Modelo de procesamiento de datos que se realiza cerca del lugar donde se generan, en lugar de depender exclusivamente de centros de datos remotos. |
| **Digital twins** | Réplicas virtuales de objetos, sistemas o procesos físicos que permiten simular, monitorear y analizar su comportamiento en tiempo real. |
| **Firmware** | Programa que está integrado directamente en el equipo físico de un dispositivo de un dispositivo, controlando sus funciones básicas. |
| **JTAG** | Estándar usado para probar, programar y depurar circuitos integrados directamente desde sus pines (del inglés, Joint Test Action Group). |



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** | Tecnología de comunicación inalámbrica de largo alcance entre dispositivos con bajo consumo energético (del inglés, Low Power Wide Area Network). |
| **Machine Learning** | Rama de la inteligencia artificial que permite a los sistemas aprender y mejorar a partir de datos sin intervención directa. |
| **Model Poisoning** | Ataque en el que se manipulan los datos o parámetros de un modelo de inteligencia artificial para alterar su comportamiento o resultados. |
| **Model Stealing** | Ataque donde alguien copia o recrea un modelo de inteligencia artificial accediendo a sus respuestas, sin tener el modelo original. |
| **Ransomware** | Programa malicioso que bloquea el acceso a sistemas o archivos y exige un pago para restaurarlo. |
| **Smart Grid** | Sistema de distribución de energía que utiliza tecnologías digitales para monitorear, gestionar y optimizar el flujo eléctrico en tiempo real. |
| **Spyware** | Programa malicioso diseñado para recopilar información del usuario sin su consentimiento. |
| **UART** | Protocolo de comunicación que transmite datos bit a bit sin necesidad de una señal de reloj (del inglés, Universal Asynchronous Receiver-Transmitter). |
| **USB** | Tipo de conexión física que permite transferir daros entre dispositivos (del inglés, Universal Serial Bus). |

TABLA 1: DEFINICIONES EMPLEADAS.

# 5. Smart Cities y el Ecosistema IoT urbano

El concepto de Smart City (Ciudad Inteligente) se fundamenta en la aplicación integrada de tecnologías digitales, sensores conectados, análisis de datos y sistemas de comunicación para optimizar la gestión de los recursos urbanos, mejorar la eficiencia de los servicios públicos y elevar la calidad de vida de los ciudadanos.

En este entorno, el Internet de las Cosas (IoT) actúa como el sistema nervioso de la ciudad digital, proporcionando la infraestructura necesaria para la recolección, transmisión y análisis continuo de información procedente del entorno urbano.

La sinergia entre IoT, inteligencia artificial, computación en la nube y Edge computing impulsa la creación de ecosistemas urbanos cada vez más autónomos, predictivos y conectados. Sin embargo, esta interdependencia tecnológica genera también nuevos vectores de riesgo y exposición, que requieren una visión de ciberseguridad transversal, adaptativa y basada en la gestión del riesgo.


ILUSTRACIÓN 1: ECOSISTEMA IOT URBANO

## 5.1. Smart Cities

Las Smart Cities se caracterizan por la integración de tecnologías digitales en áreas como la movilidad, la energía, la gestión de residuos, la administración pública, la seguridad ciudadana y la sostenibilidad ambiental.

Su modelo se apoya en la conectividad, la interoperabilidad de sistemas y la toma de decisiones basada en datos.

Los principales objetivos de una ciudad inteligente son:

- Mejorar la eficiencia de los servicios públicos mediante la digitalización.
- Reducir el impacto ambiental y optimizar el uso de los recursos.
- Aumentar la participación ciudadana a través de plataformas digitales.
- Garantizar la seguridad, la resiliencia y la continuidad de los servicios esenciales.

El éxito de una Smart City no depende únicamente de la tecnología, sino también de su gobernanza digital, la coordinación entre los distintos niveles administrativos y la confianza en la infraestructura tecnológica que la sostiene.

## 5.2. IoT en Smart Cities

El Internet de las Cosas (IoT) constituye la base tecnológica que permite conectar dispositivos físicos, como sensores, cámaras, vehículos, luminarias, estaciones meteorológicas, sistemas de control industrial o dispositivos móviles, a redes de comunicación que recopilan y procesan información en tiempo real.



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 el contexto urbano, el IoT facilita la creación de infraestructuras inteligentes que transforman la gestión de los servicios públicos, como por ejemplo:

- Movilidad y transporte inteligente: sistemas de tráfico adaptativo, aparcamiento conectado, transporte público monitorizado.
- Energía y alumbrado: redes eléctricas inteligentes (Smart grids) y alumbrado público con control remoto.
- Gestión medioambiental: sensores de calidad del aire, control de residuos y monitorización de recursos hídricos.
- Seguridad y emergencias: cámaras conectadas, sistemas de detección temprana, alarmas comunitarias y análisis predictivo.
- Administración Electrónica y participación ciudadana: plataformas de gestión de incidencias urbanas y servicios digitales para la ciudadanía.

No obstante, la presencia de millones de dispositivos heterogéneos y distribuidos plantea grandes desafíos en materia de seguridad, interoperabilidad y mantenimiento, especialmente cuando estos sistemas operan sobre infraestructuras críticas o gestionan datos personales.

## 5.3. Interconectividad y dependencias entre sistemas urbanos

El ecosistema IoT urbano no funciona de manera aislada, sino que forma parte de una red compleja e interdependiente de sistemas, donde la información fluye entre distintos dominios tecnológicos y administrativos.

Entre las principales dependencias y elementos de interconexión se encuentran:

- Infraestructura de comunicaciones: redes 5G, fibra óptica, Wi-Fi urbano y tecnologías LPWAN (LoRa, Sigfox, NB-IoT).
- Capas de procesamiento: Edge computing y cloud computing para el tratamiento de datos distribuidos.
- Plataformas de integración urbana: sistemas que recopilan, correlacionan y visualizan datos de diferentes fuentes (energía, movilidad, agua, seguridad, etc.).
- Sistemas de análisis y toma de decisiones: inteligencia artificial, machine learning y digital twins urbanos.
- Sistemas de gestión y control: interfaces de supervisión que permiten la operación remota de los servicios urbanos.

Esta interconexión, aunque esencial para la eficiencia y la innovación, incrementa la superficie de ataque y los riesgos de propagación de incidentes. Un fallo o vulnerabilidad en un subsistema puede tener efectos en cascada sobre otros servicios urbanos, lo que refuerza la necesidad de arquitecturas seguras, segmentadas y resilientes desde la fase de diseño.



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. Superficie de ataques y riesgos asociados

Este apartado describe la arquitectura IoT en entornos urbanos, identifica los puntos críticos de exposición que amplían la superficie de ataque y analiza los principales riesgos asociados a la interconectividad de los sistemas que conforman una Smart City.

El objetivo es ofrecer una visión integral de cómo la complejidad, la heterogeneidad y la dependencia tecnológica influyen directamente en la ciberseguridad y en la capacidad de respuesta ante incidentes en el ecosistema urbano digital.

## 6.1. Arquitectura IoT urbana

La arquitectura del Internet de las Cosas (IoT) en una ciudad inteligente puede representarse como una estructura de capas funcionales que van desde los dispositivos físicos hasta las plataformas de gestión centralizadas. Cada capa cumple un rol específico y presenta vulnerabilidades propias que deben considerarse siguiendo el principio de seguridad desde el diseño.

A continuación, se muestra de forma esquemática la arquitectura IoT urbana, compuesta por cinco capas funcionales que interactúan entre sí: percepción o dispositivo, red o comunicación, procesamiento y análisis, aplicación y gobierno y gestión.

Cada una de estas capas contribuye al funcionamiento integral del ecosistema urbano conectado, pero también introduce riesgos específicos que deben abordarse mediante medidas de seguridad adecuadas.


ILUSTRACIÓN 2: ARQUITECTURA IOT URBANA

### 6.1.1. Capa de percepción o dispositivo

Incluye sensores, cámaras, actuadores, contadores inteligentes, dispositivos móviles o nodos de control. Son los puntos más cercanos al entorno físico y, al mismo tiempo, los más numerosos, por lo que constituyen el frente más amplio de exposición.

Riesgos: manipulación física, suplantación de identidad, firmware inseguro, falta de actualizaciones, contraseñas por defecto.



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

### 6.1.2. Capa de red o comunicación

Los datos recopilados por los sensores se envían a esta capa mediante tecnologías cableadas e inalámbricas (5G, Wi-Fi, NB-IoT, Zigbee, Bluetooth, Sigfox, etc.).

Esta capa actúa como intermediario entre los dispositivos y los sistemas de procesamiento, que pueden encontrarse tanto en infraestructuras locales como en plataformas en la nube, especialmente en el caso de dispositivos implantables o de monitorización remota

Sus funciones principales incluyen la conversión de protocolos, el filtrado y agregación de datos, así como la aplicación de medidas de seguridad, tales como encriptación y desencriptación, antes de transmitir la información.

Riesgos: intercepción de datos, ataques Man-in-the-Middle (MitM), denegación de servicio (DDoS), explotación de protocolos inseguros o configuraciones erróneas.

### 6.1.3. Capa de procesamiento y análisis

Recoge, almacena y analiza los datos que envían los dispositivos para transformarlos en información útil. Concretamente intervienen distintos entornos:

- Edge computing: el procesamiento se realiza cerca del lugar donde se generan los datos, como en un semáforo inteligente o en una cámara de vigilancia, permitiendo responder rápidamente sin depender de la conexión con servicios en la nube.
- Fog computing: actúa como un nivel intermedio, donde los datos se procesan parcialmente en servidores locales o regionales antes de enviarse a la nube.
- Cloud computing: es el nivel más centralizado, donde los datos se almacenan y analizan en grandes centros de datos.

Riesgos: brechas de datos, configuraciones inseguras en la nube, exposición de APIs, acceso no autorizado a plataformas de análisis.

### 6.1.4. Capa de aplicación

Esta capa comprende las plataformas de gestión urbana, los paneles de control, las aplicaciones móviles y los sistemas de decisión automatizada que interactúan con los servicios públicos.

Riesgos: explotación de vulnerabilidades de software, inyección de código, escalada de privilegios, errores en la autenticación o autorización.

### 6.1.5. Capa de gobierno y gestión

Incluye las políticas de seguridad, los modelos de interoperabilidad, los mecanismos de auditoría y las responsabilidades compartidas entre administraciones, proveedores y operadores.

Riesgos: ausencia de segregación de responsabilidades, deficiencias de coordinación en la respuesta a incidentes y debilidades en la gestión del ciclo de vida de los dispositivos.

## 6.2. Puntos críticos de exposición

La superficie de ataque en una ciudad inteligente es amplia, dinámica y distribuida, debido a la enorme cantidad de dispositivos interconectados, sistemas heterogéneos y actores implicados. Cada elemento



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

de la infraestructura urbana puede convertirse en un potencial vector de entrada para ataques que comprometan la confidencialidad, integridad y disponibilidad de los servicios públicos digitales.

A continuación, se describen los principales puntos críticos de exposición que deben ser considerados en el diseño y operación de los entornos IoT urbanos:

- **Dispositivos no securizados**

Sensores, cámaras, controladores y otros nodos IoT pueden operar con firmware obsoleto, sin mecanismos de autenticación sólidos o con contraseñas por defecto. Estos equipos, al ser numerosos y físicamente accesibles, representan un punto de vulnerabilidad recurrente. La falta de actualizaciones y de controles de integridad los convierte en una puerta de entrada para ataques dirigidos o automatizados.

- **Gestión inadecuada del ciclo de vida**

Muchos de los proyectos desplegados en las ciudades inteligentes carecen de políticas claras para el alta, el mantenimiento, la auditoría y la retirada segura de los dispositivos. La ausencia de procedimientos estandarizados puede provocar que equipos antiguos o vulnerables permanezcan activos en la red, aumentando el riesgo de explotación. La gestión del ciclo de vida debe contemplar desde la incorporación del dispositivo hasta su retirada segura o desactivación controlada.

- **Proveedores y terceros**

La cadena de suministro en el entorno urbano involucra a múltiples actores, como fabricantes, integradores, desarrolladores de software y proveedores de servicios, con niveles de madurez en ciberseguridad muy dispares. La incorporación de componentes no verificados, software de terceros sin control o dispositivos con vulnerabilidades conocidas puede introducir riesgos difíciles de detectar. Resulta fundamental establecer mecanismos de verificación y auditoría, tanto en la fase de contratación como durante la prestación de los servicios.

- **Redes de comunicación heterogéneas**

La coexistencia de diversas tecnologías y protocolos, como 5G, Wi-Fi, LoRaWAN, ZigBee, NB-IoT, entre otros, genera entornos con niveles de cifrado y autenticaciones desiguales. Esta falta de homogeneidad puede facilitar ataques de intercepción, suplantación o denegación de servicio (DDoS). Se recomienda la segmentación de redes y el uso de estándares de seguridad consistentes en todas las comunicaciones.

- **Plataformas cloud y Edge**

Tanto las plataformas en la nube como las de procesamiento local son esenciales para la gestión de datos urbanos, pero también pueden presentar errores de configuración, exposición de servicios o falta de controles de acceso y monitorización. Una configuración incorrecta puede permitir accesos no autorizados, filtraciones de datos o usos indebidos de recursos.

- **Integración entre sistemas verticales**

La interconexión entre servicios urbanos, como energía, transporte o agua, incrementa la eficiencia, pero también aumenta el riesgo de propagación de incidentes. Si no existen mecanismos de segmentación o aislamiento adecuados, una brecha en un sistema puede comprometer a otros servicios críticos interdependientes.

- **Datos y privacidad**

El volumen de información generada por los dispositivos IoT incluye datos personales y sensibles. Un almacenamiento o intercambio inadecuado puede derivar en violaciones de privacidad o incumplimientos normativos, como los definidos en el Reglamento General de Protección de Datos (RGPD). La anonimización, el cifrado y la gestión del consentimiento son medidas esenciales para garantizar la protección de la información.

- **Falta de supervisión y monitorización continua**

La ausencia de sistemas de detección temprana de amenazas o de correlación de eventos entre dominios limita la capacidad de respuesta ante incidentes. En entornos urbanos complejos, la visibilidad integral es clave para identificar anomalías y contener ataques antes de que afecten a los servicios públicos.

En conjunto, estos puntos críticos evidencian la necesidad de adoptar un enfoque de seguridad integral y transversal, que abarque todas las capas de la arquitectura IoT urbana y cubra todo el ciclo de vida del sistema, desde el diseño hasta la operación y el mantenimiento.

Solo mediante una estrategia coordinada de ciberseguridad es posible garantizar la resiliencia y confianza digital de las ciudades inteligentes.

## 6.3. Riesgos asociados

Los riesgos derivados de la exposición de los sistemas IoT urbanos pueden clasificarse en tres dimensiones principales: técnica, operativa y estratégica.

Cada una de ellas agrupa amenazas que afectan a distintos niveles de la infraestructura, desde el funcionamiento interno de los dispositivos hasta la confianza ciudadana en los servicios digitales.

A continuación, se detallan las principales categorías de riesgo:


ILUSTRACIÓN 3: RIESGOS IOT EN SMART CITIES



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

### 6.3.1. Riesgos técnicos

Los riesgos técnicos están relacionados con las vulnerabilidades inherentes a los componentes físicos, lógicos y de comunicación que integran la infraestructura IoT. Su explotación puede comprometer la disponibilidad, integridad y confidencialidad de los datos clínicos, además de afectar directamente la seguridad de los ciudadanos.

Entre los más relevantes se encuentran:

- Vulnerabilidades en firmware y software: muchos dispositivos operan con sistemas embebidos propietarios o versiones antiguas que no admiten actualizaciones, prolongando la exposición a fallos conocidos y limitando la aplicación de parches de seguridad.
- Protocolos de comunicación inseguros: el uso de estándares sin cifrado o autenticación robusta, como Bluetooth clásico o Wi-Fi abierto, facilita la interceptación o manipulación de datos en tránsito.
- Ataques de denegación de servicio (DDoS) dirigidos a dispositivos o plataformas, capaces de saturar redes o interrumpir la prestación de servicios públicos.
- Autenticación débil y gestión deficiente de credenciales: el uso de contraseñas por defecto, ausencia de autenticación multifactor o cuentas compartidas permite accesos no autorizados a sistemas de gestión y equipos críticos.
- Infección por malware o ransomware: el software malicioso puede cifrar datos, alterar parámetros de tratamiento o dejar inoperativos sistemas esenciales, afectando los servicios públicos.
- Compromiso en la cadena de suministro: actualizaciones de firmware adulteradas, bibliotecas externas vulnerables o componentes falsificados pueden introducir puertas traseras en equipos.
- Manipulación o suplantación de dispositivos (device spoofing): la falsificación o sustitución de sensores, actuadores o módulos de comunicación permite inyectar datos falsos o alterar el comportamiento del dispositivo, con el consiguiente riesgo de un funcionamiento operativo inadecuado.

### 6.3.2. Riesgos operativos

Los riesgos operativos afectan a la continuidad, interoperabilidad y fiabilidad de los servicios urbanos, pudiendo generar disrupciones significativas en la gestión de la ciudad. Entre los más frecuentes destacan:

- Interrupción de servicios urbanos esenciales: fallos técnicos o ciberataques sobre dispositivos conectados, como semáforos inteligentes, sensores de tráfico o sistemas de gestión de agua y electricidad, pueden paralizar la prestación de servicios y obligar a recurrir a operaciones manuales de emergencia.
- Alteración o pérdida de datos críticos: la corrupción, eliminación o manipulación de datos de sensores urbanos, registros de movilidad o sistemas de gestión energética puede generar decisiones erróneas, retrasos en la respuesta a incidentes y riesgos directos para la ciudadanía.



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

- Falta de interoperabilidad segura: la coexistencia de dispositivos de distintos fabricantes y generaciones puede provocar incompatibilidades y vulnerabilidades derivadas del uso de protocolos inseguros o no estandarizados.
- Propagación de incidentes en redes no segmentadas: la ausencia de aislamiento entre redes de control de infraestructuras críticas, administrativas y de servicios urbanos facilita la expansión de malware o ataques DDoS hacia sistemas esenciales.
- Dependencia de servicios externos o en la nube: la externalización de funciones de gestión urbana, como almacenamiento de datos de sensores o análisis de tráfico, incrementa la exposición ante fallos de proveedores o interrupciones de conectividad.
- Errores humanos y gestión inadecuada del ciclo de vida: la falta de protocolos claros para la instalación, mantenimiento o retirada de dispositivos IoT puede derivar en configuraciones inseguras o en la permanencia de equipos vulnerables en la red.
- Ausencia de monitorización y respuesta ante incidentes: muchos sistemas urbanos carecen de centros de operaciones de seguridad (SOC) especializados o de capacidades de detección de anomalías en redes IoT, dificultando la identificación y mitigación de ataques.

### 6.3.3. Riesgos estratégicos

Los riesgos estratégicos se relacionan con las consecuencias a largo plazo sobre la gobernanza, la reputación institucional y la confianza ciudadana. Estos riesgos pueden tener un impacto más difuso, pero con efectos profundos sobre la sostenibilidad del modelo de ciudad inteligente:

- Compromiso de la seguridad de los ciudadanos: cualquier manipulación, fallo o indisponibilidad de un dispositivo IoT urbano conectado puede derivar en consecuencias directas para la población, desde accidentes o interrupción de servicios esenciales hasta daños físicos. Este riesgo requiere una coordinación estrecha entre ingeniería de infraestructura urbana y ciberseguridad.
- Pérdida de confianza de la ciudadanía: los incidentes de seguridad o filtraciones de datos pueden erosionar la confianza en la digitalización urbana y ralentizar la adopción de tecnologías conectadas y servicios públicos digitales.
- Impacto reputacional e institucional: una brecha en sistemas IoT puede afectar gravemente la imagen de administraciones públicas, operadores responsables de los servicio y fabricantes, generando consecuencias legales, económicas y sociales de gran alcance.
- Incertidumbre jurídica y responsabilidades compartidas: la compleja relación entre administraciones públicas, fabricantes, proveedores tecnológicos y reguladores puede generar vacíos legales ante incidentes. La ausencia de acuerdos de responsabilidad o cumplimiento de normativas como el RGPD, MDR o NIS2 agrava el riesgo.
- Uso indebido de datos urbanos: la explotación de información urbana para fines no autorizados, como el entrenamiento de modelos de inteligencia artificial o estudios comerciales, supone un riesgo ético y de cumplimiento normativo significativo.



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 tecnológica y ausencia de soberanía digital: la concentración de infraestructuras y servicios en plataformas externas o nubes fuera de la Unión Europea puede comprometer la soberanía de los datos y la continuidad operativa ante crisis geopolíticas o regulatorias.

# 7. Amenazas de ciberseguridad IoT en Smart Cities

La Internet de las Cosas (IoT) ha revolucionado la manera en que interactuamos con el entorno físico y digital, conectando desde pequeños sensores domésticos hasta infraestructuras críticas de transporte, energía o salud. En las Smart Cities, los dispositivos IoT permiten una gestión más eficiente de los recursos, una mejora en los servicios públicos y una mayor calidad de vida para los ciudadanos.

No obstante, esta conectividad masiva también amplifica la superficie de ataque. Los dispositivos IoT suelen presentar limitaciones de hardware y software, falta de estandarización y dependencia constante de la red, lo que los convierte en objetivos atractivos para los ciberdelincuentes. Además, su ciclo de vida corto y la obsolescencia prematura hacen que muchos equipos queden sin soporte ni actualizaciones, manteniendo abiertas vulnerabilidades críticas.

Las amenazas de seguridad en entornos IoT pueden clasificarse en tres grandes categorías, técnicas, físicas y de privacidad, aunque en la práctica estas suelen estar interconectadas y afectar simultáneamente a diferentes capas del ecosistema urbano.

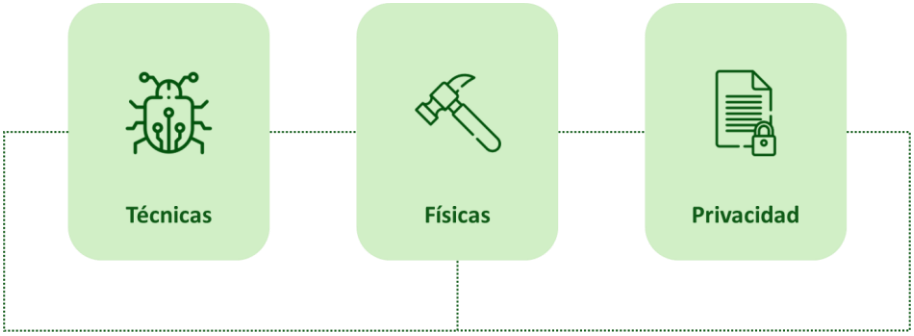


ILUSTRACIÓN 4: CATEGORÍAS AMENAZAS IOT

## 7.1. Amenazas Técnicas

Las amenazas técnicas representan el núcleo de los riesgos en los ecosistemas IoT, ya que afectan directamente a la infraestructura lógica que sustenta el funcionamiento de los dispositivos conectados. Comprenden amenazas relacionadas con vulnerabilidades en el software, fallos en los mecanismos de autenticación, exposición a redes públicas, debilidades en los protocolos de comunicación y carencias en las plataformas de gestión.

En el contexto de las Smart Cities, estas amenazas adquieren una dimensión crítica, debido que al comprometer un único sensor, cámara o pasarela permite al atacante escalar privilegios y acceder a redes completas, afectando a servicios esenciales como la gestión del tráfico, el alumbrado público o los sistemas de emergencia.



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. Amenazas relacionadas con el software

El software es el elemento más crítico de los dispositivos IoT, por ello pueden ser objeto de ataques que comprometan su funcionamiento, la integridad de los datos o la seguridad de los ciudadanos. La presión por lanzar productos rápidamente al mercado, junto con la falta de auditorías de seguridad y la reutilización de librerías obsoletas, deriva en sistemas inseguros y difíciles de mantener.

Entre las condiciones que facilitan la materialización de estas amenazas destacan:

- Credenciales por defecto o inmutables, que permanecen activas desde la fábrica y pueden encontrarse fácilmente en repositorios públicos o bases de datos de configuración.
- Cuentas embebidas o de mantenimiento con privilegios elevados, no documentadas por el fabricante, que permiten el acceso remoto sin conocimiento del usuario.
- Desbordamientos de búfer (Buffer Overflow), que facilitan la ejecución arbitraria de código malicioso.
- Condiciones de carrera y errores de validación de entradas, que pueden ser explotados para alterar el flujo lógico de los programas.
- Fugas de memoria y fallos de gestión de recursos, que generan bloqueos o denegaciones de servicio (DoS).

Un solo dispositivo vulnerable, como un sensor de tráfico, una cámara IP o un controlador de alumbrado público, puede ser aprovechado por un atacante como punto de entrada para comprometer toda la infraestructura urbana conectada.

### 7.1.2. Ataques sobre contraseñas y credenciales

La autenticación débil o mal implementada es una de las principales puertas de entrada en los sistemas IoT. Muchos dispositivos siguen utilizando contraseñas predeterminadas o mecanismos de acceso inseguros, lo que facilita ataques automatizados.

Entre las técnicas más utilizadas se incluyen:

- Ataques de fuerza bruta, que prueban sistemáticamente todas las combinaciones posibles hasta lograr el acceso.
- Ataques de diccionario, basados en listas de contraseñas comunes o predecibles.
- Credential Stuffing, reutilizando credenciales filtradas en otras plataformas.
- Ingeniería social y phishing, engañando a usuarios o administradores para obtener información de acceso.
- Explotación de servicios ocultos o cuentas embebidas, que permiten la escalada de privilegios.

Una vez obtenidas las credenciales, el atacante puede controlar remotamente el dispositivo, modificar su configuración o incluso desplegar software malicioso que comprometa toda la red a la que pertenece.

### 7.1.3. Amenazas derivadas de la exposición a Internet

Muchos dispositivos IoT permanecen conectados permanentemente a a Internet para mantenimiento o monitorización remota.



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

En este sentido, ciertas herramientas disponibles en el mercado permiten rastrear dispositivos expuestos y obtener información sobre sus puertos, versiones de firmware o servicios activos.

Estos datos facilitan ataques dirigidos o automatizados que pueden conducir al control remoto del dispositivo y su integración en botnets.

Una vez comprometidos, los equipos suelen integrarse en botnets IoT, utilizadas para:

- Robar información o espiar comunicaciones.
- Propagar malware de forma masiva.
- Ejecutar ataques DDoS o minería de criptomonedas encubierta.

El caso del botnet Mirai demostró la magnitud del problema, ya que miles de cámaras y routers mal configurados fueron utilizados para lanzar ataques que colapsaron grandes servicios de Internet a nivel global.

### 7.1.4. Ataques de denegación de servicio (DDoS)

Los ataques DDoS son una consecuencia directa del uso de dispositivos IoT comprometidos. Mediante la coordinación de miles de equipos infectados, los atacantes logran saturar servidores o servicios críticos enviando grandes volúmenes de tráfico simultáneo.

En una ciudad inteligente, un ataque de este tipo podría afectar la disponibilidad de sistemas de tráfico, alumbrado público, comunicaciones de emergencia o gestión de residuos, comprometiendo el funcionamiento normal de la urbe.

Además, estos dispositivos infectados pueden seguir siendo utilizados como nodos de ataque incluso sin que sus propietarios sean conscientes, extendiendo el impacto del incidente.

### 7.1.5. Integración con otras redes

El IoT utiliza una gran diversidad de tecnologías de comunicación, como Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, 5G, entre otras, cada una con sus propias debilidades de seguridad. Esta variedad introduce múltiples vectores de ataque y aumenta la complejidad de su gestión.

Entre las amenazas más comunes se incluyen:

- Intercepción de señales inalámbricas para capturar datos sin cifrar.
- Ataques de desautenticación (Deauth), que fuerzan la desconexión de dispositivos para suplantarlos posteriormente.
- Falsificación de nodos o gateways, insertando equipos maliciosos que actúan como intermediarios en la red.
- Ataques de repetición o suplantación de identidad, especialmente en protocolos que no implementan cifrado fuerte ni control de integridad.

Estas vulnerabilidades pueden permitir el acceso lateral a redes corporativas, industriales o municipales, generando un efecto cascada con consecuencias graves para la seguridad global de la infraestructura urbana.

### 7.1.6. Amenazas relacionadas con plataformas de administración

La administración de dispositivos IoT suele realizarse mediante interfaces web, aplicaciones móviles o APIs en la nube. Si estos entornos carecen de medidas de seguridad robustas, los atacantes pueden comprometerlos para obtener control total sobre flotas completas de dispositivos.

Entre las condiciones que facilitan la materialización de estas amenazas destacan:

- Ausencia de autenticación multifactor o gestión deficiente de sesiones.
- Protocolos de comunicación sin cifrado o certificados expirados.
- Paneles de administración expuestos directamente a Internet.
- Falta de controles de acceso granulares, permitiendo acciones críticas a usuarios no autorizados.

El compromiso de una plataforma de gestión puede tener efectos devastadores, ya que permite desplegar firmware malicioso, modificar configuraciones a gran escala o desactivar servicios esenciales en tiempo real.

## 7.2. Amenazas Físicas

Las amenazas físicas se refieren a cualquier ataque o manipulación que comprometa un dispositivo IoT a nivel de hardware o entorno físico. A diferencia de las amenazas técnicas, que se dirigen al software, credenciales o redes, las amenazas físicas aprovechan el acceso directo o indirecto al dispositivo para alterar su funcionamiento, extraer información sensible o causar daño permanente.

Estos riesgos son especialmente relevantes en entornos industriales, urbanos o domésticos, donde los dispositivos se encuentran expuestos o con un control físico limitado, como cámaras de seguridad, sensores de tráfico, estaciones meteorológicas, contadores inteligentes o sistemas de iluminación conectados.

La seguridad física, por tanto, se convierte en un componente esencial de la ciberseguridad IoT, ya que un atacante con acceso físico puede burlar protecciones digitales, modificar firmware, clonar dispositivos o incluso sabotear infraestructuras críticas.

### 7.2.1. Acceso físico al dispositivo

El acceso físico constituye una de las formas más directas y efectivas de comprometer un dispositivo IoT. Permite al atacante interactuar directamente con el hardware, desmontar el equipo o conectarse a interfaces internas para manipular su comportamiento.

Dependiendo de la ubicación y del tipo de dispositivo, los riesgos pueden clasificarse en:

- Exteriores: dispositivos como cámaras de vigilancia, sensores de tráfico, contadores inteligentes o farolas conectadas son vulnerables a manipulaciones, desactivaciones o robos. Un atacante podría alterar las lecturas, desactivar sistemas de detección o manipular datos enviados al centro de control, afectando a servicios públicos esenciales.
- Interiores: aunque suelen estar más protegidos, los dispositivos ubicados en oficinas, fábricas o viviendas pueden ser objeto de manipulación por personal no autorizado, lo que permite alterar configuraciones o introducir malware a través de puertos físicos.



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

- Acceso remoto indirecto: algunos dispositivos incluyen interfaces de mantenimiento o puertos de depuración (como USB, UART o JTAG) que pueden ser explotados si no están adecuadamente protegidos, permitiendo la instalación de firmware malicioso o la extracción de datos.

El acceso físico no solo pone en riesgo al dispositivo en cuestión, sino que también puede servir de punto de entrada a toda la red IoT conectada.

### 7.2.2. Ataques basados en el hardware

Los ataques de hardware explotan vulnerabilidades en los componentes físicos del dispositivo, ya sea durante su diseño, fabricación o implementación. Muchos dispositivos IoT priorizan la funcionalidad y el bajo coste frente a la seguridad, dejando brechas que pueden ser aprovechadas por atacantes.

Algunos ejemplos destacados incluyen:

- Interfaz de depuración no protegida: acceso a puertos JTAG, UART o SPI para leer memoria, extraer claves criptográficas, modificar firmware o instalar código malicioso.
- Manipulación de sensores o actuadores: al alterar la entrada o salida de estos elementos, el atacante puede falsificar lecturas o forzar acciones que afecten a procesos industriales o servicios urbanos.
- Explotación de componentes inseguros: el uso de chips, módulos de comunicación o componentes reutilizados con vulnerabilidades conocidas permite ataques a la integridad del sistema.
- Ataques de canal lateral (side-channel): técnicas avanzadas que analizan consumo eléctrico, radiación electromagnética o tiempos de ejecución para inferir datos sensibles como claves de cifrado.
- Extracción de firmware o memoria: mediante el desmontaje del dispositivo y la lectura directa de la memoria Flash o EEPROM, un atacante puede clonar el software, copiar configuraciones o analizar vulnerabilidades.
- Ingeniería inversa: desmontar el dispositivo para estudiar su funcionamiento interno, identificar puntos débiles o reproducir su diseño, facilitando ataques posteriores o la creación de copias falsas.

En conjunto, estos ataques pueden permitir el control total del dispositivo, el robo de datos o el sabotaje de infraestructuras, especialmente si los equipos no incluyen medidas de protección física ni cifrado en sus componentes internos.

### 7.2.3. Manipulación ambiental y sabotaje

Los factores ambientales también pueden emplearse de manera intencionada para comprometer dispositivos IoT. Al alterar las condiciones del entorno o provocar fallos físicos, los atacantes pueden interrumpir la operación, dañar el hardware o manipular los datos recopilados.

Ejemplos de este tipo de amenazas incluyen:

- Condiciones extremas: exposición a temperaturas elevadas, humedad o vibraciones excesivas que pueden afectar el rendimiento de sensores, memoria o módulos de comunicación.



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 electromagnéticas (EMI): ataques que generan campos electromagnéticos o señales de radio para perturbar sensores, anular comunicaciones inalámbricas o corromper datos.
- Ataques acústicos u ópticos: algunos sensores (por ejemplo, de movimiento o ultrasónicos) pueden ser engañados mediante ondas de sonido o luz especialmente moduladas.
- Sabotaje deliberado: incluye cortocircuitos, desconexión de energía, manipulación de cables o la introducción de objetos físicos (como líquidos conductores o polvo metálico) para dañar los dispositivos.
- Alteración del entorno operativo: modificar las condiciones físicas o químicas detectadas por el sensor para provocar lecturas falsas (por ejemplo, alterar la composición del aire, la iluminación o el ruido ambiente).

Este tipo de ataques puede tener consecuencias graves, especialmente en infraestructuras críticas, al provocar alteraciones en los datos que conducen a mediciones erróneas y, en consecuencia, a fallos operativos, alarmas falsas o interrupción de servicios esenciales.

### 7.2.4. Robo o sustitución de dispositivos

El robo, pérdida o sustitución de dispositivos IoT representa una amenaza creciente, especialmente en entornos distribuidos donde la supervisión física es limitada. Un atacante puede:

- Sustituir un dispositivo legítimo por otro comprometido o clonado, que capture datos o inyecte información manipulada sin ser detectado.
- Extraer del dispositivo robado información sensible, como credenciales, certificados digitales o claves criptográficas.
- Usar el dispositivo sustraído como vector para atacar la red interna o suplantar su identidad en el sistema.

Este tipo de ataque es especialmente relevante en plataformas industriales, sistemas de transporte o redes de servicios públicos, donde la manipulación de un único sensor o controlador puede afectar a todo un entorno operativo.

### 7.2.5. Manipulación durante la cadena de suministro

Otra amenaza física relevante en el ecosistema IoT son los riesgos asociados a la cadena de suministro. Estos se producen cuando un dispositivo o alguno de sus componentes se ve comprometido durante las fases de diseño, fabricación, distribución o instalación, antes incluso de llegar al usuario final.

Los atacantes pueden introducir firmware adulterado, componentes falsificados, chips maliciosos o configuraciones inseguras, aprovechando la falta de control en alguno de los eslabones de la cadena. En muchos casos, el dispositivo llega aparentemente intacto, pero ya contiene vulnerabilidades o puertas traseras (backdoors) difíciles de detectar.

Este tipo de amenaza resulta especialmente peligroso porque socava la confianza en la base del ecosistema, afectando a miles de equipos simultáneamente y dificultando la trazabilidad del origen del ataque.



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

## 7.3. Amenazas a la privacidad

La privacidad de los datos generados, transmitidos y almacenados por los dispositivos IoT constituye uno de los retos más críticos en el ámbito de la ciberseguridad. Estos dispositivos operan constantemente en contacto con el entorno físico y con los usuarios, recopilando información personal, conductual y sensible (ubicación, hábitos, salud, consumo energético, entre otros).

Un ataque exitoso puede tener consecuencias directas en la intimidad, seguridad y confianza de los ciudadanos y organizaciones. Las principales amenazas a la privacidad en el IoT incluyen el malware y ransomware, la intercepción de datos en tránsito y los ataques directos a la información almacenada o procesada.

### 7.3.1. Malware y ransomware para IoT

Los ataques de malware y ransomware se han convertido en una de las principales amenazas para los entornos IoT. Estos programas maliciosos se aprovechan de vulnerabilidades del software o de configuraciones inseguras para:

- Bloquear el acceso a los dispositivos o a sus datos, exigiendo un rescate económico.
- Robar información personal o corporativa, especialmente aquella que no se encuentra cifrada.
- Incorporar dispositivos a botnets, redes de equipos infectados que ejecutan ataques coordinados, como DDoS o campañas de spam.

Actualmente, las variantes modernas de ransomware IoT no solo bloquean los dispositivos, sino que también amenazan con difundir información sensible o alterar datos críticos para incrementar la presión sobre las víctimas.

### 7.3.2. Intercepción de datos de tránsito

La transmisión de datos entre dispositivos, pasarelas y servidores es un punto especialmente vulnerable del ecosistema IoT. Si la comunicación no se cifra adecuadamente, los atacantes pueden ejecutar ataques Man-in-the-Middle (MitM) para interceptar, espiar o modificar la información transmitida.

Existen dos modalidades principales:

- MitM pasivo: el atacante intercepta y monitoriza las comunicaciones sin alterarlas, obteniendo datos sensibles como credenciales, patrones de uso o información privada.
- MitM activo: además de interceptar el tráfico, el atacante modifica o inyecta datos falsos antes de reenviarlos, pudiendo alterar el comportamiento del dispositivo o manipular las decisiones de los sistemas conectados.

La falta de cifrado extremo a extremo (E2E), la ausencia de autenticación mutua y el uso de protocolos obsoletos son factores que incrementan significativamente el riesgo de estos ataques.

### 7.3.3. Ataques sobre la privacidad de los datos

Más allá de los ataques técnicos, los ciberdelincuentes también centran sus esfuerzos en explotar la información gestionada por los dispositivos IoT. Esta información puede incluir datos personales, financieros o de seguridad que, una vez comprometidos, se convierten en un recurso valioso en el mercado negro.



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

Entre las principales amenazas destacan:

- Robo de datos personales: desde historiales médicos y localizaciones GPS hasta claves de cerraduras inteligentes o datos de cuentas bancarias.
- Venta o difusión de información sensible: los datos extraídos pueden ser revendidos o utilizados para campañas de suplantación, espionaje o chantaje.
- Perfilado y seguimiento de usuarios: los atacantes pueden analizar los patrones de comportamiento de los ciudadanos (horarios, consumo, movilidad) para generar perfiles precisos.
- Reidentificación de datos anonimizados: combinando datos públicos y privados, es posible revertir procesos de anonimización y asociar la información a personas concretas.
- Ataques a la nube o pasarelas de datos: los sistemas que centralizan la información de múltiples dispositivos se convierten en objetivos de alto valor.

La protección de la privacidad en IoT exige, por tanto, un enfoque integral que combine cifrado de extremo a extremo, anonimización de datos, control de acceso, auditoría continua y cumplimiento estricto de normativas como el Reglamento General de Protección de Datos (RGPD) o el Cyber Resilience Act (CRA).

# 8. Retos de ciberseguridad IoT en Smart Cities

La adopción masiva de dispositivos IoT en las ciudades inteligentes ha supuesto un avance significativo en la optimización de recursos, la gestión de infraestructuras y la mejora de los servicios públicos. No obstante, este progreso también ha introducido nuevos desafíos en materia de ciberseguridad, derivados de la gran diversidad de tecnologías empleadas, la falta de estándares comunes, la limitada capacidad de muchos dispositivos y la complejidad de los ecosistemas urbanos interconectados.

Garantizar una ciberseguridad robusta en entornos IoT urbanos resulta considerablemente más complejo que en sistemas informáticos tradicionales, ya que las medidas de protección deben salvaguardar no solo la confidencialidad de la información, sino también la disponibilidad y continuidad operativa de los dispositivos que sustentan los servicios públicos esenciales.

La interoperabilidad entre equipos de distintos fabricantes y la coexistencia de dispositivos de consumo dentro del mismo entorno urbano pueden introducir vulnerabilidades adicionales, por ejemplo, una brecha en un sensor doméstico conectado a la red municipal podría comprometer sistemas críticos.

En este contexto, asegurar la seguridad, la privacidad y la resiliencia de las Smart Cities exige un enfoque integral que combine medidas tecnológicas, organizativas y humanas para mitigar los riesgos asociados a la conectividad masiva y garantizar la confianza en los servicios digitales urbanos.



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

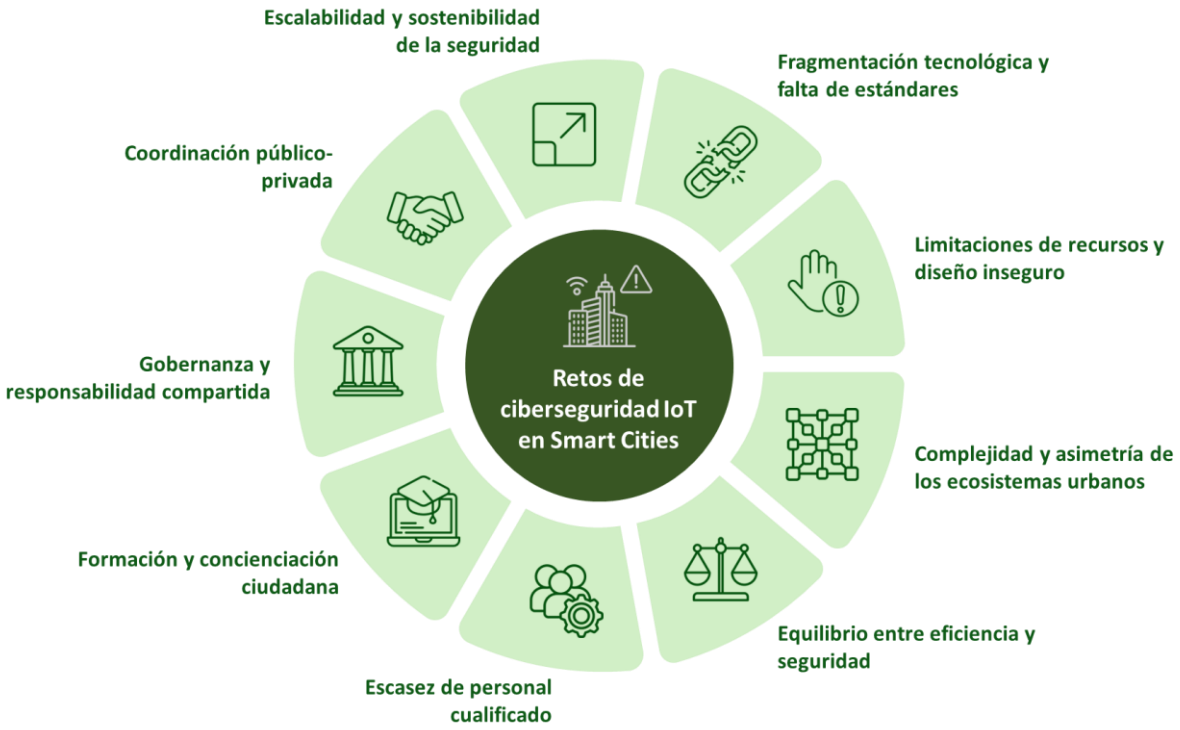


ILUSTRACIÓN 5: RETOS DE CIBERSEGURIDAD IOT EN SMART CITIES

## 8.1. Fragmentación tecnológica y falta de estándares

Uno de los principales retos en la ciberseguridad de las Smart Cities es la heterogeneidad del ecosistema IoT. Los entornos urbanos inteligentes integran dispositivos de múltiples fabricantes, con diferentes protocolos de comunicación, sistemas operativos y niveles de seguridad.

Esta fragmentación complica la interoperabilidad y dificulta la implementación de políticas de seguridad homogéneas. La falta de estándares de seguridad consolidados impide aplicar buenas prácticas de manera consistente, lo que genera brechas y vulnerabilidades que pueden ser explotadas por atacantes.

El desarrollo de marcos comunes de certificación, estándares abiertos y mecanismos de actualización universal es esencial para reducir el riesgo derivado de esta diversidad tecnológica.

## 8.2. Limitaciones de recursos y diseño inseguro

Muchos dispositivos IoT desplegados en entornos urbanos son equipos de bajo coste y recursos limitados (procesamiento, memoria o energía). Estas restricciones dificultan la implementación de medidas de seguridad robustas como cifrado avanzado, autenticación multifactor o monitorización continua.

Además, en muchos casos los fabricantes priorizan la funcionalidad, el tiempo de salida al mercado o la eficiencia energética por encima de la seguridad, lo que da lugar a fallos en el diseño y desarrollo del hardware o firmware.

Entre los principales problemas destacan la ausencia de mecanismos de actualización segura, contraseñas por defecto, servicios innecesarios habilitados y falta de validación del software. Estas



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

deficiencias hacen que los dispositivos sean objetivos fáciles para botnets, ransomware o ataques de denegación de servicio distribuidos (DDoS).

## 8.3. Complejidad y asimetría de los ecosistemas urbanos

Las Smart Cities operan sobre ecosistemas extremadamente complejos, donde convergen redes de transporte, energía, sanidad, comunicaciones y servicios públicos. Esta interconectividad genera asimetría de la información entre los distintos actores, dificultando el control global de la seguridad.

A menudo, las administraciones públicas carecen de visibilidad completa sobre los componentes, firmware o proveedores implicados, lo que limita la capacidad de detección temprana de amenazas.

Asimismo, la dependencia de múltiples operadores y proveedores complica la trazabilidad y la respuesta ante incidentes, pudiendo amplificar el impacto de una vulnerabilidad localizada

## 8.4. Equilibrio entre eficiencia y seguridad

En muchos proyectos de Smart City existe una tensión entre eficiencia operativa y seguridad. La presión por optimizar costes, reducir tiempos de despliegue y mejorar la experiencia del ciudadano puede llevar a descuidar los requisitos de ciberseguridad.

Del mismo modo, las medidas de seguridad más estrictas pueden aumentar la latencia o el consumo de recursos, afectando la eficiencia de los servicios.

Encontrar un equilibrio sostenible entre rendimiento, coste y protección será un desafío constante para las administraciones y operadores urbanos, que deberán integrar la seguridad desde el diseño y durante todo el ciclo de vida de los sistemas

## 8.5. Escasez de personal cualificado

La rápida expansión de las Smart Cities y la proliferación de dispositivos IoT han generado una demanda creciente de profesionales con competencias específicas en seguridad digital, redes, análisis de vulnerabilidades y gestión de incidentes. Sin embargo, la oferta de personal cualificado no crece al mismo ritmo que las necesidades del sector.

Esta brecha de talento se traduce en una dependencia excesiva de proveedores externos, retrasos en la detección de incidentes y dificultades para mantener actualizadas las infraestructuras críticas. En muchos casos, los equipos municipales o técnicos responsables de la gestión urbana carecen del conocimiento necesario para aplicar políticas de ciberseguridad coherentes, supervisar contratos tecnológicos o evaluar el cumplimiento de normativas.

Para afrontar este desafío, resulta indispensable impulsar programas de formación especializada, incentivos a la contratación de expertos y alianzas con universidades, centros tecnológicos y organismos públicos. La creación de perfiles híbridos, capaces de comprender tanto los sistemas urbanos como las implicaciones de ciberseguridad, será clave para garantizar la resiliencia de las ciudades inteligentes.

## 8.6. Formación y concienciación ciudadana

La ciberseguridad en entornos IoT urbanos no depende únicamente de la tecnología, sino también del comportamiento de las personas que interactúan con ella. La falta de concienciación y formación entre



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 empleados públicos, técnicos, empresas colaboradoras y ciudadanía en general constituye un factor de riesgo crítico.

Los errores humanos, como el uso de contraseñas débiles, la falta de actualización de dispositivos o la conexión de equipos no autorizados, pueden comprometer la integridad de sistemas enteros. En este sentido, la formación continua y la educación digital son esenciales para fortalecer la primera línea de defensa frente a las amenazas.

Las administraciones deben promover campañas de sensibilización adaptadas a distintos públicos, como empleados municipales, proveedores y usuarios, combinadas con ejercicios de simulación y certificaciones profesionales. Fomentar una cultura de ciberseguridad sólida, donde la protección de los datos y la privacidad se perciban como una responsabilidad compartida, permitirá avanzar hacia una Smart City más segura y confiable.

## 8.7. Gobernanza y responsabilidad compartida

La gestión de la ciberseguridad en entornos urbanos inteligentes requiere una gobernanza clara y bien estructurada. La coexistencia de múltiples actores —administraciones, proveedores tecnológicos, contratistas y operadores privados— plantea dificultades para definir quién es responsable de la seguridad de cada dispositivo, red o servicio.

Sin un marco de responsabilidades bien delimitado, las brechas de seguridad pueden quedar sin atender o ser objeto de conflictos de competencias. Es fundamental establecer políticas de cumplimiento, auditoría y respuesta coordinada ante incidentes, que definan de forma precisa los roles y obligaciones de cada parte

## 8.8. Coordinación público-privada

La cooperación entre el sector público y el privado es un pilar esencial para la seguridad de las Smart Cities. La ciberseguridad requiere un enfoque compartido, donde se facilite el intercambio de información sobre amenazas, vulnerabilidades e incidentes.

Además, deben definirse mecanismos de colaboración que incluyan protocolos conjuntos de respuesta, planes de contingencia y desarrollo de estándares comunes.

La falta de coordinación puede generar duplicidades, vacíos de protección o respuestas descoordinadas ante incidentes graves, afectando a la confianza y la resiliencia de los servicios urbanos.

## 8.9. Escalabilidad y sostenibilidad de la seguridad

A medida que las ciudades inteligentes crecen y se incorporan nuevos dispositivos y servicios, garantizar una seguridad escalable se vuelve un reto cada vez mayor.

La gestión de millones de nodos conectados requiere sistemas automatizados de monitorización, actualización y detección de anomalías, capaces de operar en tiempo real y adaptarse al crecimiento constante del entorno.

La planificación de la ciberseguridad debe, por tanto, concebirse como un proceso dinámico y evolutivo, con capacidad de adaptación tecnológica, presupuestaria y organizativa a largo plazo.

# 9. Casos reales

Tras haber detallado las amenazas y retos asociados a los sistemas IoT en ciudades inteligentes, resulta fundamental analizar incidentes reales que ejemplifiquen cómo estas vulnerabilidades y desafíos se traducen en impactos concretos sobre los servicios urbanos. El estudio de casos permite comprender mejor la naturaleza de los riesgos, identificar patrones de ataque y extraer lecciones útiles para fortalecer las estrategias de ciberseguridad.

En esta sección, los incidentes se presentan clasificados en tres categorías de impacto. Para cada categoría se incluyen dos casos reales en formato de tabla, lo que permite una visualización clara y comparativa de la fecha, ubicación, tipo de incidente, sistema afectado y consecuencias principales.

## 9.1. Filtración de datos

Los ataques de filtración de datos se producen cuando la información sensible generada o gestionada por los sistemas IoT urbanos es expuesta de manera no autorizada. Esto puede incluir datos personales de ciudadanos, información de sensores urbanos o registros de operación de servicios críticos. Las filtraciones suelen originarse por vulnerabilidades en plataformas cloud, APIs inseguras, configuraciones incorrectas o falta de cifrado en la transmisión y almacenamiento de datos.

El impacto de este tipo de incidentes puede variar desde la pérdida de privacidad hasta riesgos legales, pérdida de confianza ciudadana y consecuencias económicas para la administración pública.

| **Vulnerabilidad en Lavadoras Inteligentes en Residencias Estudiantiles de Ámsterdam** | |
|---|---|
| **Fecha** | Julio de 2025 |
| **Víctima** | Estudiantes residentes en complejos universitarios de Ámsterdam |
| **Activo comprometido** | Lavadoras inteligentes conectadas a red IoT doméstica |
| **Tipo de Amenaza** | Exposición de datos personales por vulnerabilidad en dispositivos conectados |
| **Vector del ataque** | Acceso no autorizado a interfaces de gestión sin cifrado ni autenticación |
| **Origen del ataque** | IPs extranjeras no identificadas; posible explotación automatizada |
| **Impacto** | Filtración de datos personales (nombres, horarios de uso, ubicación de dispositivos); interrupción del servicio de lavandería. |



Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

| Vulnerabilidad en Lavadoras Inteligentes en Residencias Estudiantiles de Ámsterdam | |
|---|---|
| **Descripción** | En julio de 2025, se detectó una vulnerabilidad crítica en lavadoras inteligentes instaladas en residencias estudiantiles de Ámsterdam. Los dispositivos, conectados a una red IoT doméstica para permitir reservas y pagos digitales, fueron comprometidos por actores externos que accedieron a las interfaces de gestión sin necesidad de autenticación.<br>La intrusión permitió extraer datos personales de los usuarios, incluyendo nombres, horarios de uso y ubicación de los dispositivos. Además, se alteraron los ciclos de lavado, lo que provocó interrupciones en el servicio y riesgo de contagio por uso de equipos no higienizados correctamente.<br>El incidente fue reportado por expertos en ciberseguridad tras una auditoría interna impulsada por las autoridades locales, lo que permitió identificar fallos críticos en la configuración de los dispositivos. El caso evidenció cómo la falta de medidas básicas de protección en entornos IoT domésticos puede derivar en la exposición de datos sensibles de los ciudadanos. |

TABLA 2: CASO REAL 1: VULNERABILIDAD EN LAVADORAS INTELIGENTES

| Fuga de datos en aplicación de gestión de aparcamientos | |
|---|---|
| **Fecha** | Diciembre de 2023 |
| **Víctima** | Operador de apps de aparcamiento en Europa |
| **Activo comprometido** | Plataformas de aparcamiento |
| **Tipo de Amenaza** | Exposición no autorizada de datos sensibles |
| **Vector del ataque** | Acceso no autorizado a sistemas del proveedor |
| **Origen del ataque** | Investigadores de seguridad y actores externos con acceso a entornos mal configurados |
| **Impacto** | Exposición de datos de clientes (nombres, emails, teléfonos, datos de pago) |



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

| Fuga de datos en aplicación de gestión de aparcamientos | |
|---|---|
| **Descripción** | En diciembre de 2023, se reveló una fuga de datos que afectó a las principales aplicaciones de aparcamiento urbano de Europa, gestionadas por el grupo EasyPark. La brecha se originó por un fallo de seguridad en entornos de prueba expuestos a Internet, que permitió accesos no autorizados a bases de datos de usuarios.<br>Los registros filtrados incluían nombres, direcciones de correo electrónico, teléfonos y fragmentos cifrados de información de pago. Aunque no se detectó uso fraudulento de los datos, la empresa notificó a las autoridades de protección de datos de la UE y reforzó sus protocolos de cifrado y autenticación.<br>Este caso puso de manifiesto la importancia de proteger los sistemas que gestionan servicios urbanos y datos de movilidad. |

TABLA 3: CASO REAL 2: FUGA DE DATOS GESTIÓN DE APARCAMIENTOS

## 9.2. Manipulación de sistemas

La manipulación de sistemas implica que un atacante logra alterar el comportamiento de dispositivos o plataformas urbanas, afectando al control de servicios críticos. Esto puede incluir cambios no autorizados en semáforos inteligentes, sistemas de alumbrado, cámaras de vigilancia o plataformas de información ciudadana.

Estos ataques suelen aprovechar contraseñas por defecto, vulnerabilidades en firmware o software, y accesos remotos inseguros. Sus consecuencias incluyen desinformación, riesgo físico para los ciudadanos, pérdida de confianza y, en algunos casos, daños materiales.

| Manipulación de semáforos en Países Bajos | |
|---|---|
| **Fecha** | Agosto de 2020 |
| **Víctima** | Ciudades neerlandesas (Dordrecht y Tilburg) |
| **Activo comprometido** | Sistemas de gestión de tráfico y sensores para prioridad ciclista |
| **Tipo de Amenaza** | Manipulación remota |
| **Vector del ataque** | Vulnerabilidad en apps y entradas de sensores que aceptaban datos no validados |



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

| Manipulación de semáforos en Países Bajos | |
|---|---|
| **Origen del ataque** | IPs extranjeras no identificadas; posible automatización mediante scripts |
| **Impacto** | Saturación de redes urbanas, interrupción de servicios digitales y caída de plataformas dependientes del ISP afectado |
| **Descripción** | En agosto de 2020, investigadores de seguridad neerlandeses identificaron una vulnerabilidad crítica en los sistemas de prioridad ciclista de los semáforos de Dordrecht y Tilburg. Las aplicaciones móviles empleadas por los ciclistas para solicitar prioridad en los cruces enviaban señales a los sistemas de gestión de tráfico sin validación ni autenticación adecuadas.<br>Esta deficiencia permitió a cualquier usuario, o incluso a scripts automatizados, enviar solicitudes falsas que forzaban el cambio de luces en los semáforos. Aunque no se registraron accidentes, el hallazgo demostró la posibilidad real de manipular el flujo del tráfico urbano y afectar la seguridad vial. Tras el incidente, las autoridades locales implementaron mecanismos de autenticación criptográfica, validación de mensajes y segmentación de red para evitar accesos no autorizados.<br>El caso se considera un referente temprano de los riesgos asociados a la integración de sistemas IoT en infraestructuras urbanas críticas. |

TABLA 4: CASO REAL 3: MANIPULACIÓN DE SEMÁFOROS EN PAÍSES BAJOS

| Manipulación Remota de Infraestructura Eléctrica en Kiev | |
|---|---|
| **Fecha** | 17 de diciembre de 2016 |
| **Víctima** | Ukrenergo (operador nacional de energía de Ucrania) |
| **Activo comprometido** | Subestación eléctrica Pivnichna y red de distribución en Kiev |
| **Tipo de Amenaza** | Manipulación remota de sistemas industriales |
| **Vector del ataque** | Acceso no autorizado a sistemas SCADA mediante malware especializado |
| **Origen del ataque** | Presunta autoría de grupos vinculados al Estado ruso |
| **Impacto** | Corte de energía en barrios del norte de Kiev durante más de una hora |



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

| Manipulación Remota de Infraestructura Eléctrica en Kiev | |
|---|---|
| **Descripción** | En la noche del 17 de diciembre de 2016, Kiev experimentó un apagón que afectó a varios barrios del norte de la ciudad. El incidente fue atribuido a un ciberataque que logró acceder de forma remota a los sistemas SCADA de la subestación eléctrica Pivnichna, operada por Ukrenergo. A través de esta intrusión, los atacantes manipularon directamente el flujo eléctrico, provocando la desconexión de líneas de distribución clave.<br>El restablecimiento del servicio se logró en 75 minutos gracias a la intervención manual de los ingenieros, quienes desactivaron los sistemas comprometidos. Investigaciones posteriores vincularon este ataque con una campaña más amplia de sabotaje digital contra infraestructuras críticas ucranianas, que ya había tenido un precedente en 2015 con un apagón masivo.<br>Este caso es uno de los primeros ejemplos documentados de manipulación física de infraestructuras urbanas a través de medios cibernéticos, y marcó un antes y un después en la seguridad de los sistemas industriales conectados. |

TABLA 5: CASO REAL 4: MANIPULACIÓN REMOTA DE INFRAESTRUCTURA ELÉCTRICA

## 9.3. Interrupción de servicios

Los ataques de interrupción de servicios buscan degradar o paralizar la operación de funciones críticas de la ciudad. Pueden involucrar ataques DDoS, ransomware o fallos derivados de la interdependencia de sistemas urbanos conectados.

Su objetivo es afectar la disponibilidad de servicios esenciales como transporte, energía, agua o emergencias. Los efectos incluyen interrupciones significativas, caos operativo, riesgos para la seguridad ciudadana y consecuencias económicas y reputacionales para los operadores y administraciones públicas.

| Ciberataque al Sistema de Riego del Jardín del Turia | |
|---|---|
| **Fecha** | 16 de septiembre de 2025 |
| **Víctima** | Ayuntamiento de Valencia (España) |
| **Activo comprometido** | Sistema de riego automatizado del Jardín del Turia |
| **Tipo de Amenaza** | Acceso no autorizado |
| **Vector del ataque** | Explotación de vulnerabilidad en el software de gestión |



Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

| Ciberataque al Sistema de Riego del Jardín del Turia | |
|---|---|
| **Origen del ataque** | Dirección IP ubicadas en Rusia |
| **Impacto** | Interrupción del servicio municipal de riego urbano |
| **Descripción** | El Ayuntamiento de Valencia ha comunicado una intrusión informática en el sistema de riego automatizado del Jardín del Turia, uno de los mayores parques urbanos de España.<br>Según los responsables municipales, el incidente se originó desde direcciones IP ubicadas en Rusia, aprovechando una vulnerabilidad en el software de gestión, lo que permitió el acceso no autorizado al sistema.<br>La incidencia fue detectada cuando los técnicos municipales observaron un funcionamiento irregular del sistema de riego. Tras la detección, procedieron a aislar los dispositivos afectados, logrando contener la incidencia sin que se produjera impacto alguno en otros sistemas municipales.<br>Cabe destacar que este incidente no es un caso aislado: diversos informes señalan que Rusia figura entre los países que más promueven campañas de ciberataques contra instituciones y organismos públicos en Europa, con el objetivo de aprovechar vulnerabilidades en los sistemas y demostrar su capacidad para controlar y obtener información sensible. |

TABLA 6: CASO REAL 5: CIBERATAQUE SISTEMA DE RIEGO JARDÍN DEL TURIA

| Ciberataque de la Botnet Mirai a Dispositivos IoT Urbanos | |
|---|---|
| **Fecha** | 29 de octubre de 2024 |
| **Víctima** | Proveedor de servicios de internet en Asia Oriental (no identificado públicamente) |
| **Activo comprometido** | Más de 13,000 dispositivos IoT (cámaras IP, routers, sensores urbanos) |
| **Tipo de Amenaza** | Denegación de servicio distribuida (DDoS) |
| **Vector del ataque** | Variante de Mirai que explotó dispositivos IoT vulnerables mediante el protocolo UDP |
| **Origen del ataque** | Dispositivos comprometidos en múltiples países, botnet distribuida globalmente |



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

| Ciberataque de la Botnet Mirai a Dispositivos IoT Urbanos | |
|---|---|
| **Impacto** | Saturación de redes urbanas, interrupción de servicios digitales, caída de plataformas dependientes del ISP afectado |
| **Descripción** | El 29 de octubre de 2024, Cloudflare detectó y bloqueó un ataque DDoS de 5.6 Terabits por segundo (Tbps), el más grande registrado hasta la fecha. El ataque fue ejecutado por una variante de la botnet Mirai, que logró comprometer más de 13,000 dispositivos IoT mal protegidos, incluyendo cámaras de vigilancia, routers y sensores urbanos.<br>El ataque duró 80 segundos y utilizó el protocolo UDP para generar un volumen masivo de tráfico malicioso. La infraestructura urbana digital del proveedor de servicios de internet (ISP) afectado colapsó temporalmente, lo que provocó interrupciones en servicios esenciales como transporte, comunicaciones y gestión energética.<br>Este incidente demuestra que las botnets basadas en IoT siguen evolucionando, y que los dispositivos conectados en entornos urbanos representan una amenaza creciente si no se actualizan y protegen adecuadamente. |

TABLA 7: CASO REAL 6: CIBERATAQUE BOTNET MIRAI

# 10. Marco regulatorio actual y necesidades futuras

El desarrollo del IoT está redefiniendo el modelo de gestión urbana mediante la conexión de sensores inteligentes, infraestructuras críticas, vehículos conectados y sistemas de administración pública digital. Esta red interconectada optimiza el uso de los recursos, mejora la eficiencia de los servicios públicos y potencia la sostenibilidad de las ciudades, sin embargo, también amplía la superficie de exposición a riesgos de seguridad y vulnerabilidades que pueden afectar directamente la seguridad ciudadana, la continuidad operativa y la privacidad de los datos urbanos.

Por ello, la ciberseguridad se ha consolidado como un eje estratégico dentro de las políticas de transformación digital y de las estrategias de desarrollo de las Smart Cities. La protección de los dispositivos y sistemas IoT urbanos requiere un marco regulatorio sólido que combine aspectos técnicos, normativos y organizativos, garantizando tanto la fiabilidad operativa como el cumplimiento ético y legal en la gestión de la información generada en el entorno urbano.

En este apartado se examinan las principales regulaciones, estándares internacionales y estrategias de ciberseguridad aplicables al IoT en ciudades inteligentes, así como las necesidades regulatorias futuras que permitan afrontar los nuevos riesgos derivados de la digitalización masiva.


ILUSTRACIÓN 6: MARCO REGULATORIO IOT

## 10.1. Estándares internacionales de ciberseguridad aplicables al IoT y Smart Cities

El marco normativo de la ciberseguridad aplicada al Internet de las Cosas (IoT) y a las Smart Cities se apoya en un conjunto de estándares internacionales que proporcionan las bases metodológicas y técnicas para la protección de la información, los servicios y las infraestructuras críticas frente a un panorama de amenazas cada vez más complejo.

En este contexto, destacan los siguientes referentes globales:

- ISO/IEC 27001: establece los requisitos para los sistemas de gestión de la seguridad de la información (SGSI), promoviendo un enfoque basado en la gestión de riesgos.
- ISO/IEC 27701: extensión de la 27001 centrada en la gestión de la privacidad y la protección de datos personales. Define controles y responsabilidades específicos para garantizar el cumplimiento de normativas como el RGPD, aspecto esencial en entornos urbanos donde se tratan grandes volúmenes de datos de ciudadanos.
- ISO/IEC 27400:2022: aborda de forma específica la seguridad y privacidad en entornos IoT, incluyendo principios de diseño seguro y gestión del ciclo de vida de los dispositivos conectados.
- Serie IEC 62443: orientada a la protección de sistemas industriales y de automatización, define buenas prácticas para la segmentación de redes, control de accesos y gestión de vulnerabilidades en entornos críticos.

No obstante, la mayor parte de las normas de carácter vinculante y de impacto directo sobre el ecosistema IoT urbano proceden del ámbito europeo, donde la Unión Europea y los Estados Miembros, incluido España, han impulsado reglamentos y directivas específicas que buscan unificar criterios, elevar



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

el nivel de protección y definir responsabilidades claras entre fabricantes, operadores, administraciones públicas y proveedores tecnológicos.

## 10.2. Iniciativas regionales y nacionales sobre ciberseguridad en Smart Cities

Partiendo de los estándares mencionados anteriormente, tanto la Unión Europea como los Estados miembros, incluido España, han desarrollado iniciativas específicas orientadas a reforzar la seguridad digital y la resiliencia de las infraestructuras conectadas.

En el contexto de las Smart Cities, estas políticas resultan especialmente relevantes, ya que los entornos urbanos inteligentes integran una gran diversidad de sistemas interconectados, como dispositivos IoT, plataformas de gestión, servicios digitales y redes de comunicación, cuya protección requiere una coordinación multinivel entre instituciones europeas, nacionales y locales.

### 10.2.1. Iniciativas Europeas

La Unión Europea ha desempeñado un papel clave en la creación de un marco regulador común en materia de ciberseguridad, impulsando normas, directivas y reglamentos destinados a reforzar la protección de los sistemas digitales, la resiliencia de las infraestructuras críticas y la confianza de los ciudadanos.

Estas iniciativas responden a la creciente interconexión de dispositivos, servicios y plataformas, como ocurre en las Smart Cities, donde la superficie de ataque aumenta y los riesgos asociados a los ciberincidentes pueden tener consecuencias directas sobre la seguridad, la economía y el bienestar social.

- **Reglamento General de Protección de Datos (2016)**

El Reglamento General de Protección de Datos de la Unión Europea (RGPD) regula el tratamiento y protección de los datos personales en todos los Estados miembros. Su objetivo principal es garantizar que la información de los ciudadanos sea procesada de manera legal, transparente y segura, protegiendo la privacidad y los derechos individuales.

En el contexto de Smart Cities y entornos IoT, el RGPD adquiere especial relevancia, ya que estos sistemas recopilan grandes volúmenes de datos personales, incluyendo información sobre movilidad, consumo energético, salud, hábitos de los ciudadanos y servicios urbanos conectados.

El cumplimiento del RGPD es obligatorio para cualquier sistema conectado que gestione datos de ciudadanos europeos, incluyendo dispositivos IoT, plataformas de gestión urbana y servicios digitales. Su aplicación refuerza la confianza de los ciudadanos, la responsabilidad de los operadores y la resiliencia de las infraestructuras urbanas inteligentes, siendo un elemento central en la gobernanza de las Smart Cities.

- **EU Cybersecurity Act (2019)**

El EU Cybersecurity Act (EUCA), en vigor desde 2019, establece un marco europeo de certificación de ciberseguridad para productos, servicios y procesos digitales. Su objetivo es crear un sistema común y reconocido en toda la UE que garantice un nivel mínimo de seguridad y confianza en los productos conectados.

La norma también refuerza el papel de ENISA, otorgándole un mandato permanente y mayores competencias para coordinar políticas de ciberseguridad, fomentar la cooperación entre los Estados miembros y liderar la respuesta europea ante incidentes.

- **Directiva NIS2 (2022)**

La Directiva NIS2 (del inglés, Network and Information Systems Directive), aprobada en 2022, actualiza la normativa europea sobre ciberseguridad y amplía su alcance respecto a la versión anterior.

Su propósito es reforzar la resiliencia de las infraestructuras críticas y los servicios esenciales frente a incidentes, imponiendo obligaciones de seguridad y notificación de incidentes tanto a entidades públicas como privadas.

Entre sus principales novedades destacan:

- Ampliación del ámbito de aplicación a sectores clave como energía, transporte, sanidad, agua, administración pública y servicios digitales.
- Obligación de gestión de riesgos, formación en ciberseguridad y comunicación temprana de incidentes graves.
- Refuerzo de la cooperación entre los Estados miembros y creación de un mecanismo europeo de respuesta coordinada ante incidentes.

La transposición de NIS2 a la legislación española está en curso, y su cumplimiento será esencial para las Smart Cities, al involucrar tanto infraestructuras municipales como operadores tecnológicos.

- **EU Cyber Resilience Act (2024)**

El CRA de la Unión Europea (del inglés, EU Cyber Resilience Act) constituye uno de los avances normativos más importantes en materia de seguridad digital. Su objetivo es garantizar que todos los productos con elementos digitales, incluidos los dispositivos IoT, incorporen medidas de ciberseguridad desde su diseño y durante todo su ciclo de vida.

Entre sus principales objetivos se encuentran:

- Reducir la cantidad de vulnerabilidades presentes en los productos comercializados dentro de la UE.
- Asegurar que los fabricantes mantengan la responsabilidad de la seguridad de sus productos durante todo su ciclo de vida.
- Mejorar la transparencia sobre las características de ciberseguridad, permitiendo a los consumidores tomar decisiones informadas.
- Reforzar la trazabilidad en la cadena de suministro, exigiendo la documentación del software incorporado.
- Obligar a informar a la European Union Agency for Cybersecurity (ENISA) de los incidentes que afecten a la seguridad de los productos.

El CRA será de aplicación obligatoria a partir del 10 de diciembre de 2024 para todos los productos digitales comercializados en el mercado europeo.

### 10.2.2. Iniciativas nacionales

A nivel nacional, España ha consolidado en la última década un marco estratégico y normativo cada vez más robusto en materia de ciberseguridad, con el objetivo de alinear su política digital con las directrices europeas y las necesidades de las Smart Cities. Estas iniciativas buscan no solo proteger las infraestructuras críticas, sino también fomentar una cultura de seguridad que abarque a ciudadanos, empresas y administraciones públicas.

- **Ley Protección de Infraestructuras Críticas (2011)**

La Ley 8/2011 para la Protección de Infraestructuras Críticas (LPIC), junto con su desarrollo reglamentario mediante el Real Decreto 704/2011, constituye el pilar de la protección de las infraestructuras críticas nacionales.

Esta norma establece los mecanismos de coordinación entre el sector público y privado para proteger los servicios esenciales frente a ataques o incidentes graves.

Con la proliferación del IoT y la interconexión de los sistemas urbanos, muchos servicios de Smart City, como transporte, energía, agua o salud, se consideran operadores críticos o esenciales, por lo que deben alinearse con las obligaciones de la Ley PIC, incluyendo la elaboración de Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE).

- **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (2018)**

La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), adapta y desarrolla en España los principios del RGPD, incluyendo obligaciones concretas para administraciones públicas, empresas y operadores de servicios digitales. Esta ley define responsabilidades, derechos de los ciudadanos y medidas de seguridad, relevantes en el contexto de Smart Cities, donde dispositivos IoT recopilan datos de movilidad, energía, salud y consumo.

- **Estrategia Nacional de Ciberseguridad (2019)**

La Estrategia Nacional de Ciberseguridad de España, revisada en 2019 en sustitución de la versión de 2013, constituye el marco de referencia fundamental para la protección del ciberespacio nacional. Promueve una visión integral que abarca desde la protección de infraestructuras críticas hasta la capacitación y concienciación ciudadana.

Entre sus líneas de acción destacan:

- Fortalecer la resiliencia nacional ante amenazas de ciberseguridad.
- Impulsar la cooperación público-privada en la gestión de incidentes.
- Fomentar la investigación y la innovación tecnológica en materia de ciberseguridad.
- Integrar la ciberseguridad como un componente esencial en el desarrollo de las Smart Cities y la administración digital.

La estrategia se implementa mediante el Consejo Nacional de Ciberseguridad, órgano dependiente del Consejo de Seguridad Nacional, que coordina la actuación de organismos como el INCIBE, el CCN-CERT, la Guardia Civil o la Policía Nacional.



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

Asimismo, el Consejo de Seguridad Nacional, el 24 de abril de 2025, aprobó el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad, con el objetivo de actualizar el marco estratégico ante la evolución del panorama de amenazas y las nuevas prioridades nacionales.

- **Esquema Nacional de Seguridad (2022)**

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece los principios básicos y los requisitos mínimos que deben cumplir las administraciones públicas y los proveedores de servicios tecnológicos para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información.

El ENS define tres niveles de seguridad (bajo, medio y alto) y actúa como una referencia obligada para el diseño de infraestructuras digitales seguras, especialmente en los sistemas urbanos de gestión de tráfico, alumbrado, energía o servicios al ciudadano.

Su adaptación al contexto IoT resulta esencial para reforzar la seguridad en las plataformas de Smart Cities y para cumplir con los nuevos requisitos de resiliencia digital europeos.

- **Plan Nacional de Ciberseguridad (2022)**

Aprobado como desarrollo operativo de la Estrategia Nacional, este plan incluye más de 100 actuaciones concretas dirigidas a reforzar la seguridad digital del país. Entre sus líneas prioritarias destacan la protección del IoT y de las infraestructuras urbanas inteligentes, la creación de capacidades de detección temprana y la cooperación internacional.

El plan también fomenta la formación de especialistas en ciberseguridad IoT y la implantación de un marco nacional de certificación, en consonancia con el Cybersecurity Act europeo.

## 10.3. Necesidades regulatorias

A pesar de los avances descritos, aún existen vacíos normativos que deben abordarse para consolidar un ecosistema IoT urbano seguro, resiliente e interoperable. Entre las principales necesidades destacan:

- Unificación de criterios normativos entre los distintos marcos europeos y nacionales, evitando solapamientos o contradicciones.
- Actualización continua de las regulaciones, dada la rápida evolución tecnológica y la aparición de nuevos tipos de amenazas.
- Desarrollo de certificaciones específicas para dispositivos IoT urbanos, que garanticen un nivel mínimo de seguridad y privacidad.
- Definición clara de responsabilidades entre fabricantes, operadores, administraciones y proveedores tecnológicos.
- Refuerzo de la cooperación internacional y público-privada, esencial para gestionar incidentes globales y compartir inteligencia sobre amenazas.

El futuro de la ciberseguridad en las Smart Cities dependerá de la capacidad de los reguladores para crear un marco normativo coherente, dinámico y centrado en la protección de los ciudadanos, sin frenar la innovación tecnológica que impulsa la transformación digital urbana.



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

# 11. Tendencias futuras y Riesgos emergentes

El ecosistema IoT evoluciona a un ritmo acelerado hacia modelos más inteligentes, autónomos y distribuidos, impulsados por la convergencia entre la Inteligencia Artificial (IA), el Edge Computing y las infraestructuras urbanas digitales. En el contexto de las Smart Cities, esta evolución redefine la forma en que se gestionan los recursos, se prestan los servicios públicos y se protege la información.

Sin embargo, este avance también introduce nuevas superficies de ataque, mayores dependencias tecnológicas y riesgos de ciberseguridad emergentes que requieren estrategias adaptativas y colaborativas. El reto no es solo proteger los dispositivos o las redes, sino garantizar la confianza digital, la resiliencia operativa y el respeto a la privacidad ciudadana en un entorno cada vez más interconectado.

## 11.1. Expansión de dispositivos conectados

El número de dispositivos IoT desplegados en las ciudades inteligentes crece de manera exponencial, desde sensores ambientales y cámaras de tráfico hasta sistemas de alumbrado, gestión energética o control de transporte público. Además, la integración de servicios inteligentes en hogares, vehículos y edificios amplía el perímetro del ecosistema IoT urbano más allá de las infraestructuras municipales.

Principales desafíos introducidos:

- Mayor superficie de ataque derivada de la diversidad de dispositivos, fabricantes y protocolos de comunicación presentes en el entorno urbano.
- Exposición de datos sensibles (como patrones de movilidad o consumo energético) en redes públicas o domésticas con controles de seguridad limitados.
- Riesgos asociados a dispositivos personales conectados al ecosistema urbano, que pueden ser manipulados o configurados de forma insegura.
- Dificultad para mantener inventarios precisos y gestionar el ciclo de vida de dispositivos distribuidos geográficamente y operados por múltiples entidades.

## 11.2. Integración con IA y Edge Computing

La integración de IA y Edge Computing constituye una de las principales tendencias en el desarrollo del IoT de próxima generación.

El Edge Computing acerca el procesamiento de datos al lugar donde se generan, en el borde de la red, reduciendo la latencia, mejorando la eficiencia y preservando la privacidad al minimizar el envío de datos a la nube.

Por su parte, la Inteligencia Artificial dota a estos sistemas de capacidad para analizar información en tiempo real, tomar decisiones autónomas y optimizar recursos urbanos en áreas como la gestión del tráfico, la energía, la seguridad ciudadana o el tratamiento de residuos.

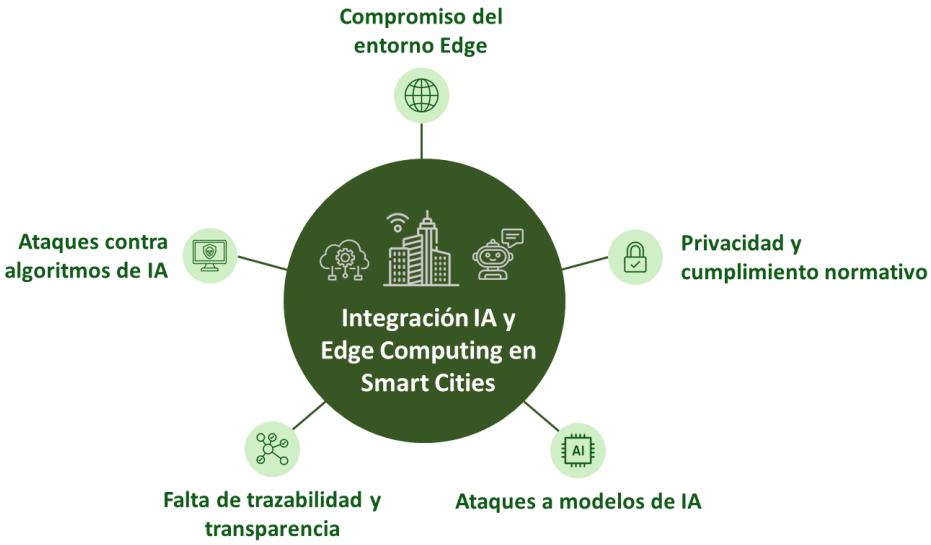


ILUSTRACIÓN 7: TENDENCIAS FUTURAS Y RIESGOS ASOCIADOS

No obstante, esta convergencia también introduce nuevos desafíos de ciberseguridad que deben abordarse desde el diseño:

- Ataques adversariales contra algoritmos de IA: los modelos de aprendizaje automático pueden ser manipulados mediante la introducción de datos falsos o modificados, alterando la toma de decisiones automatizada.
- Compromiso del entorno Edge: los nodos de borde procesan información crítica y pueden ser vulnerables si no cuentan con mecanismos robustos de autenticación, cifrado y actualización remota.
- Falta de trazabilidad y transparencia: los sistemas de IA operan con un nivel de autonomía que dificulta la auditoría y la detección de incidentes o sesgos.
- Privacidad y cumplimiento normativo: el procesamiento distribuido de datos personales plantea nuevos retos para el cumplimiento de regulaciones como el Reglamento General de Protección de Datos (RGPD) y el Cyber Resilience Act (CRA).
- Ataques a modelos de IA: técnicas como el model poisoning o la extracción de modelos (model stealing) pueden comprometer los sistemas inteligentes que sustentan la toma de decisiones urbanas.

En el futuro, la convergencia entre IA, Edge Computing e IoT será esencial para la eficiencia de las ciudades inteligentes, pero también exigirá una seguridad integrada por diseño, con capacidades de monitorización continua, validación de modelos, actualización segura de firmware y resiliencia basada en IA defensiva.

## 11.3. Riesgos Emergentes

A medida que el ecosistema IoT madura y se expande a nuevas áreas de aplicación, surgen riesgos emergentes que afectan tanto a la infraestructura técnica como a la gobernanza y la confianza social.



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

Estos riesgos no solo derivan de vulnerabilidades técnicas, sino también de la creciente interdependencia entre sistemas urbanos y del papel que juegan los datos en la toma de decisiones

Algunos de los riesgos emergentes más relevantes incluyen:

- Ciberataques dirigidos a infraestructuras críticas: los sistemas de transporte, energía, agua o salud conectados son objetivos prioritarios para actores maliciosos, tanto criminales como estatales, que buscan causar disrupción o extraer información estratégica.
- Interconectividad masiva y cascadas de fallos: la dependencia entre dispositivos y plataformas puede provocar efectos dominó, donde una brecha de seguridad en un componente compromete sistemas enteros.
- Ataques híbridos (físico-digitales): la combinación de acciones físicas y cibernéticas, como sabotear un sensor y manipular sus datos simultáneamente, amplía el impacto de las ofensivas.
- Saturación del espectro y conflictos entre protocolos: la coexistencia de múltiples tecnologías inalámbricas (Wi-Fi, 5G, Zigbee, LoRa, Bluetooth) puede generar interferencias y nuevas oportunidades de ataque a nivel de comunicación.
- Dispositivos de bajo coste y sin mantenimiento: el mercado IoT crece a través de dispositivos económicos que, a menudo, carecen de mecanismos de actualización o certificación, generando una “brecha de seguridad estructural” en las redes urbanas.
- Dependencia tecnológica y soberanía digital: el uso de soluciones propietarias o de fabricantes externos puede comprometer la autonomía y la seguridad de los datos urbanos, especialmente cuando no existen estándares abiertos ni control nacional sobre la cadena de suministro.
- Manipulación de datos y desinformación algorítmica: los sistemas de IA que procesan información urbana pueden ser objeto de ataques que alteren los datos de sensores o generen decisiones erróneas (por ejemplo, falsos patrones de tráfico o alarmas).
- Gemelos digitales y entornos virtuales urbanos: la simulación de infraestructuras mediante digital twins puede ser explotada para espiar, predecir o manipular el comportamiento de los sistemas reales.
- Riesgos éticos y sociales: la expansión del IoT y la analítica avanzada de datos plantea dilemas sobre la privacidad, el consentimiento ciudadano y el uso legítimo de tecnologías de vigilancia o reconocimiento facial.

Frente a estos desafíos, las ciudades deben adoptar un enfoque proactivo, resiliente y basado en el riesgo, que combine:

- Anticipación de amenazas mediante inteligencia cibernética.
- Colaboración público-privada para compartir información y buenas prácticas.
- Seguridad desde el diseño y por defecto en infraestructuras y servicios urbanos.
- Actualización normativa y formación continua para los profesionales encargados de la gestión digital.

Solo integrando la ciberseguridad como eje estratégico de la transformación urbana, las Smart Cities podrán evolucionar de manera sostenible, confiable y centrada en el ciudadano.

# 12. Conclusiones

La seguridad en el Internet de las Cosas constituye un desafío ineludible para la sostenibilidad y la confianza en los entornos conectados, especialmente en el contexto de las Smart Cities. Aunque alcanzar una protección absoluta resulta prácticamente imposible, dado que los cibercriminales actúan con gran rapidez, adaptabilidad e incentivados por motivaciones económicas, la adopción de buenas prácticas, políticas adecuadas y medidas preventivas puede reducir significativamente el riesgo y aumentar la resiliencia de los sistemas.

El IoT combina entornos digitales y físicos, por lo que una brecha en su seguridad puede traducirse no solo en la pérdida de datos, sino también en impactos reales sobre la ciudadanía y los servicios públicos. La clave, por tanto, reside en aplicar una visión integral que abarque la tecnología, la gestión, la formación y la concienciación de todos los actores implicados.

## 12.1. Recomendaciones

A continuación, se recogen algunas recomendaciones prácticas para fortalecer la seguridad de los dispositivos IoT y las redes a las que se conectan, tanto en entornos domésticos como corporativos o municipales.

- **Mantener los dispositivos y el software actualizados**

Los dispositivos IoT suelen carecer de soluciones tradicionales de protección, como antivirus o cortafuegos, por lo que las actualizaciones periódicas de firmware y software son la principal defensa frente a vulnerabilidades.

Es fundamental asegurarse de que el fabricante proporcione actualizaciones de seguridad y aplicarlas de forma inmediata, ya sea automática o manualmente desde fuentes oficiales. En el caso de organizaciones, los dispositivos IoT deben integrarse en la política general de gestión de parches y mantenimiento, garantizando su revisión continua y la planificación de actualizaciones programadas.

- **Conocer las amenazas y evaluar los riesgos**

Comprender los vectores de ataque más probables y realizar evaluaciones de riesgo permite priorizar medidas de protección. Se recomienda identificar los dispositivos más críticos o vulnerables, analizar las posibles consecuencias de un incidente y clasificar los riesgos por nivel de impacto.

Este proceso debe complementarse con una formación continua y simulaciones de ataques, tanto para usuarios como para equipos de TI, con el fin de detectar debilidades antes de que sean explotadas.

Cada nuevo dispositivo supone una potencial puerta de entrada, por lo que conviene mantener un inventario actualizado de activos IoT y monitorizar su comportamiento de forma constante.

- **Cambiar las contraseñas por defecto**

El uso de credenciales por defecto o repetidas es una práctica muy común y extremadamente peligrosa. Es imprescindible cambiar los nombres de usuario y contraseñas de fábrica en todos los dispositivos IoT y emplear combinaciones únicas para cada uno de ellos.

Asimismo, se recomienda verificar que el dispositivo admite mecanismos de autenticación segura y aplicar una gestión adecuada de accesos en sus interfaces de administración.



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

- **Utilizar contraseñas seguras**

Las contraseñas deben ser robustas y complejas, combinando letras mayúsculas y minúsculas, números y símbolos, con una longitud mínima de 12 caracteres.

Para facilitar su gestión, puede recurrirse a administradores de contraseñas que almacenen de forma segura las credenciales y eviten su reutilización. También es esencial configurar contraseñas sólidas para la red Wi-Fi que da soporte al ecosistema IoT.

- **Cambiar el nombre del router**

Mantener el nombre de fábrica del router puede revelar información sobre su modelo o fabricante, facilitando los ataques automatizados. Es recomendable asignar un nombre personalizado, sin incluir datos personales como nombre o dirección, para dificultar su identificación.

- **Revisar los ajustes de privacidad y seguridad**

Los dispositivos IoT suelen incluir configuraciones de privacidad y seguridad predeterminadas. Es aconsejable revisar y ajustar estas opciones antes de comenzar a utilizarlos, así como consultar las políticas de privacidad para conocer cómo el proveedor gestiona los datos personales.

Si el dispositivo lo permite, se debe habilitar el registro de eventos (logs) para supervisar accesos, actualizaciones y posibles incidentes.

- **Activar y desactivar funciones en base a su uso**

Cada funcionalidad activa amplía la superficie de ataque. Por ello, se recomienda deshabilitar aquellas funciones que no se utilicen. Por ejemplo, si un dispositivo no requiere Bluetooth, NFC o activación por voz, es preferible mantenerlas desactivadas para reducir riesgos.

- **Implementar autenticación multifactor (MFA)**

Siempre que sea posible, debe activarse la autenticación multifactor, que requiere más de un método de verificación, como contraseña o código temporal. Aunque no todos los dispositivos IoT ofrecen esta opción, su uso añade una capa adicional de protección frente al acceso no autorizado.

- **Proteger el hardware**

En dispositivos situados en entornos accesibles o exteriores, la seguridad física es igualmente importante. Se deben proteger las conexiones, bloquear los puertos no utilizados, cifrar los datos almacenados localmente y, en caso necesario, optar por conexiones móviles seguras en lugar de redes Wi-Fi públicas o no controladas.

- **Fomentar la formación y concienciación**

La concienciación del usuario es la primera línea de defensa. Promover una cultura de ciberseguridad implica educar a los ciudadanos, empleados y responsables técnicos sobre el uso seguro de los dispositivos, la gestión responsable de contraseñas, la detección de correos fraudulentos y la importancia de aplicar buenas prácticas de forma continua.

Solo a través de una sociedad más informada y proactiva será posible reducir los riesgos y consolidar un entorno IoT verdaderamente seguro y sostenible.



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

# 13. Anexos

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

## 13.1. Listado de amenazas

A continuación, se presenta un listado de amenazas, organizadas por categoría, con una breve descripción de cada una y los activos afectados. Este listado permite una visión clara y estructurada de los riesgos técnicos, operativos, físicos y de privacidad, sirviendo como referencia para la evaluación, gestión y mitigación de los mismos dentro del entorno IoT y los sistemas asociados.

Antes de detallar las amenazas, es importante definir los valores de los activos considerados en el análisis, los cuales representan los elementos clave del ecosistema tecnológico que pueden verse comprometidos ante un incidente de seguridad:

- Dispositivos IoT: Sensores, actuadores, controladores y nodos conectados que recopilan o procesan información dentro de la infraestructura inteligente.
- Plataformas de gestión: Sistemas centralizados de administración, monitoreo y configuración de los dispositivos y servicios IoT.
- Sistemas Backend: Servidores, bases de datos y servicios de apoyo donde se almacenan, procesan o analizan los datos generados por los dispositivos.
- Aplicaciones y servicios: Interfaces de usuario, APIs y aplicaciones móviles o web que interactúan con los sistemas IoT y presentan la información al usuario final.
- Infraestructura: Componentes físicos y lógicos que sustentan la red (centros de datos, energía, cableado, routers, switches, etc.).
- Comunicaciones: Enlaces y protocolos de red que permiten la transmisión de datos entre dispositivos, servidores y usuarios.
- Otros dispositivos de la red IoT: Equipos conectados indirectamente o integrados con la red principal, susceptibles a ataques laterales o propagación de amenazas.

Con base en estos activos, el siguiente cuadro recoge las principales amenazas identificadas, clasificadas según su naturaleza y su posible impacto sobre el entorno IoT.



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

| Categoría | Amenaza | Descripción | Activos afectados |
|---|---|---|---|
| Amenazas Técnicas | Amenazas relacionadas con el software | Amenazas que explotan fallos en el código, librerías desactualizadas o errores de validación que permiten ejecución de código, acceso no autorizado o denegación de servicio. | – Dispositivos IoT,<br>– Plataformas de gestión<br>– Sistemas Backend |
| | Ataques sobre contraseñas y credenciales | Uso de contraseñas por defecto o débiles, ataques de fuerza bruta o phishing que comprometen la autenticación del sistema. | – Dispositivos IoT<br>– Plataformas de gestión<br>– Aplicaciones y servicios<br>– Sistemas Backend |
| | Amenazas derivadas de la exposición a Internet | Dispositivos o servicios accesibles públicamente (puertos abiertos, configuraciones inseguras) detectables mediante herramientas de exploración. | – Dispositivos IoT<br>– Infraestructura<br>– Comunicaciones |
| | Ataques de denegación de servicio (DDoS) | Saturación de servicios mediante redes de dispositivos comprometidos (botnets), afectando la disponibilidad de sistemas críticos urbanos. | – Infraestructura<br>– Comunicaciones,<br>– Plataformas de gestión<br>– Aplicaciones y servicios |
| | Integración con otras redes | Integración insegura entre la red IoT y otras redes corporativas o públicas que permite movimientos laterales o propagación de ataques. | – Infraestructura<br>– Comunicaciones<br>– Otros dispositivos de la red IoT |
| | Amenazas relacionadas con plataformas de administración | Explotación de debilidades en los paneles de control o herramientas de gestión remota (sin MFA, cifrado débil, API inseguras) que facilitan el acceso no autorizado. | – Plataformas de gestión<br>– Sistemas Backend<br>– Aplicaciones y servicios |

| Categoría | Amenaza | Descripción | Activos afectados |
|---|---|---|---|
| Amenazas Físicas | Acceso físico al dispositivo | Manipulación directa de sensores o nodos instalados en espacios públicos o industriales, posibilitando la alteración de firmware o extracción de datos. | – Dispositivos IoT<br>– Infraestructura |
| | Ataques basados en el hardware | Explotación de interfaces físicas (JTAG, UART, USB) o ingeniería inversa sobre el hardware para obtener información sensible o modificar el funcionamiento. | – Dispositivos IoT,<br>– Otros dispositivos de la red IoT |
| | Manipulación ambiental y sabotaje | Alteración intencionada de las condiciones físicas (temperatura, humedad, campos electromagnéticos) o sabotaje directo de equipos. | – Dispositivos IoT<br>– Infraestructura |
| | Robo o sustitución de dispositivos | Sustitución o sustracción de equipos legítimos por copias maliciosas que permiten el espionaje, manipulación o interrupción del servicio. | – Dispositivos IoT<br>– Infraestructura<br>– Comunicaciones |
| | Manipulación durante la cadena de suministro | Inserción de componentes falsificados o firmware comprometido durante la fabricación o distribución del dispositivo. | – Dispositivos IoT<br>– Plataformas de gestión<br>– Sistemas Backend |
| Amenazas de Privacidad | Malware y ransomware para IoT | Infección de dispositivos mediante software malicioso que roba información o bloquea el funcionamiento de los sistemas inteligentes. | – Dispositivos IoT<br>– Plataformas de gestión<br>– Sistemas Backend<br>– Aplicaciones y servicios |



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

| Categoría | Amenaza | Descripción | Activos afectados |
|---|---|---|---|
| | Intercepción de datos de tránsito | Captura o manipulación de datos transmitidos entre dispositivos y servidores mediante ataques Man-in-the-Middle o de replay. | – Dispositivos IoT<br>– Comunicaciones<br>– Plataformas de gestión<br>– Sistemas Backend |
| | Ataques sobre la privacidad de los datos | Acceso no autorizado o uso indebido de datos personales (localización, hábitos, biometría), vulnerando la confidencialidad y el cumplimiento normativo. | – Dispositivos IoT<br>– Plataformas de gestión<br>– Sistemas Backend<br>– Aplicaciones y servicios |

TABLA 8: LISTADO DE AMENAZAS IOT EN SMART CITIES



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

# 14. Referencias


1. America´s Cyber Defense Agency. (2023). *Cybersecurity Best Practices for Smart Cities*. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf

2. 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

3. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems.* https://doi.org/10.1016/j.future.2017.07.060

4. Editorial RA-MA. (2023). *Ciberseguridad IoT y su aplicación en Ciudades Inteligentes*. https://www.ra-ma.es/media/rama/files/book-attachment-7455.pdf

5. 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

6. European Union Agency for Cybersecurity (ENISA). (2025). *National Cyber Security Strategies*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

7. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025#contentList

8. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Cybersecurity Threat Landscape Methodology.* https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology

9. European Union Agency for Cybersecurity (ENISA). (2017). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

10. Instituto Nacional de Ciberseguridad (INCIBE). (2019). *La importancia de la seguridad en IoT. Principales amenazas.* https://www.incibe.es/incibe-cert/blog/importancia-seguridad-iot-principales-amenazas

11. Instituto Nacional de Ciberseguridad (INCIBE). (2017). *Riesgos y retos de ciberseguridad y privacidad en IoT*. https://www.incibe.es/incibe-cert/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

12. 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

13. IOActive. (2018). *Smart Cities Cyber Security Worries*. https://www.ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf

14. Ministry of Internal Affairs and Communications (MIAC). (2020). *Smart City Security Guidelines*. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf

15. National Institute of Standards and Technology (NIST). (2019). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. https://csrc.nist.gov/pubs/ir/8228/final

16. Nozomi Networks. (2025). *OT/IoT Tendencias e información sobre ciberseguridad*. https://es.nozominetworks.com/ot-iot-cybersecurity-trends-insights-july-2025

17. 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

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

19. Ranchordás S. y C. Goanta. (2020). *The New City Regulators: Platform and Public Values in Smart and Sharing Cities*. https://doi.org/10.1016/j.clsr.2019.105375

20. 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/

21. Soare, S. y J. Burton. (2020). *Smart Cities, Cyber Warfare and Social Disorder*. https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.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

22. Trapenberg, F. et al. (2021). *The Cybersecurity Risks of Smart City Technologies: What Do The Experts Think?* https://cltc.berkeley.edu/publication/smart-cities/

23. World Economic Forum (WEF). (2021). *Governing smart cities: policy benchmarks for ethical and responsible smart city development*. https://www.weforum.org/publications/governing-smart-cities-policy-benchmarks-for-ethical-and-responsible-smart-city-development/

# 15. 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.

## 15.1. Lista de materias tratadas en la guía

- Concepto y características de Smart Cities.
- Aplicaciones del Internet de las Cosas (IoT) en entornos urbanos.
- Arquitectura IoT urbana y capas funcionales.
- Puntos críticos de exposición y superficie de ataque en ciudades inteligentes.
- Riesgos asociados: técnicos, operativos y estratégicos.
- Amenazas de ciberseguridad: técnicas, físicas y de privacidad.
- Retos de ciberseguridad: estándares, escalabilidad, gobernanza y coordinación público-privada.
- Casos reales: filtración de datos, manipulación de sistemas e interrupción de servicios.
- Marco regulatorio actual y necesidades futuras en ciberseguridad IoT.
- Tendencias futuras y riesgos emergentes, incluyendo IA y Edge Computing.

## 15.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

## 15.3. 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

# Ciberseguridad IoT en Smart Cities: Retos y Amenazas

## Noviembre de 2025

## Versión 1.0

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia