RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Desarrollo Seguro de Soluciones IoT en Smart Cities

Febrero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

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

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

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 26/02/2026

Fecha de última actualización: 26/02/2026

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

1. Introducción

El Internet de las Cosas (IoT) se ha convertido en un elemento clave en el desarrollo de las Smart Cities, al permitir la interconexión de sensores, dispositivos y plataformas distribuidas que soportan la operación y gestión de servicios urbanos como el alumbrado público, la movilidad, la gestión del agua, la energía o el medio ambiente.

Sin embargo, el despliegue de soluciones IoT en entornos urbanos plantea desafíos específicos que tienen un impacto directo en la seguridad. Estos sistemas suelen estar compuestos por dispositivos con recursos limitados, instalados en ubicaciones accesibles físicamente y conectados a arquitecturas distribuidas y heterogéneas, y muchos de los servicios que soportan tienen un carácter esencial para la ciudadanía. Esta combinación incrementa de forma significativa la superficie de ataque y amplifica el impacto potencial de vulnerabilidades derivadas de errores de diseño, desarrollo o configuración.

En este escenario, la ciberseguridad no puede abordarse como un elemento añadido ni como una medida reactiva ante incidentes. Por el contrario, debe integrarse de manera transversal y sistemática desde las fases iniciales de diseño y desarrollo de las soluciones IoT. La adopción de principios de desarrollo seguro, tales como el enfoque de seguridad por diseño, resulta imprescindible para garantizar la resiliencia de los sistemas desplegados.

La ausencia de criterios claros y metodologías de desarrollo seguro no solo dificulta la evolución y la gestión de las plataformas, sino que también puede derivar en vulnerabilidades, una exposición prolongada a amenazas y riesgos significativos para la integridad y disponibilidad de los servicios urbanos. Por ello, el desarrollo seguro no es una opción, sino una condición necesaria para asegurar la confianza de la ciudadanía en las infraestructuras digitales que sustentan las ciudades inteligentes.

2. Objetivo y alcance

2.1. Objetivo

El objetivo de esta guía es proporcionar un marco práctico y estructurado para el desarrollo seguro de soluciones IoT en Smart Cities, integrando la seguridad de forma transversal desde las fases iniciales de planificación y diseño hasta la operación y el mantenimiento.

La guía está orientada a apoyar a entidades, integradores y equipos técnicos en la identificación de riesgos, la definición de requisitos de seguridad y la adopción de criterios coherentes de arquitectura, desarrollo de software, verificación y gestión del ciclo de vida, con el fin de mejorar la resiliencia de los servicios urbanos basados en IoT.

2.2. Alcance

Esta guía se centra en la definición de criterios de ciberseguridad aplicables al diseño, desarrollo y mantenimiento de soluciones IoT en Smart Cities. El documento aborda los principales riesgos de seguridad asociados a estos entornos y proporciona orientaciones prácticas para su mitigación a lo largo del ciclo de vida de la solución.

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

Quedan fuera del alcance el diseño funcional de los servicios urbanos, la definición de modelos avanzados de analítica y la selección de productos o soluciones comerciales concretas. La guía no sustituye normativas, estándares o pliegos técnicos específicos, sino que actúa como documento de apoyo para la definición de requisitos y la toma de decisiones en fases de planificación, diseño, desarrollo y supervisión de soluciones IoT en Smart Cities.

La guía está orientada principalmente a administraciones públicas,

es técnicos, integradores y otros agentes implicados en el despliegue de soluciones IoT en Smart Cities, proporcionando un marco común que facilite evaluaciones comparables y alineadas con buenas prácticas de seguridad.

2.3. Metodología

El contenido de esta guía ha sido elaborado siguiendo una metodología estructurada que integra revisión normativa, análisis técnico y adaptación al contexto específico de las soluciones IoT en entornos Smart City. El enfoque adoptado garantiza coherencia con buenas prácticas internacionales y su aplicabilidad práctica en proyectos reales.

La metodología seguida se basa en las siguientes etapas:

1. Revisión técnica: análisis de marcos de referencia, estándares y buenas prácticas en materia de desarrollo seguro y seguridad en sistemas IoT, como OWASP o NIST, con el fin de identificar controles y recomendaciones.
2. Adaptación al contexto de Smart Cities: contextualización de los controles y recomendaciones al entorno urbano, teniendo en cuenta las características específicas del ecosistema.
3. Traducción a medidas concretas: transformación de los controles y recomendaciones identificadas en requisitos y medidas aplicables, redactados en términos claros, verificables y orientados a su implementación técnica en proyectos reales.
4. Estructuración por fases del ciclo de vida: organización del contenido atendiendo a las distintas etapas del ciclo de vida de una solución IoT, asegurando una visión integral y continua de la seguridad.

Esta metodología garantiza que la guía sea tecnológicamente neutral, aplicable a distintos proveedores y arquitecturas, y alineada con los principales marcos de referencia en seguridad. Asimismo, proporciona criterios claros y estructurados para la toma de decisiones y la gestión integral de proyectos de IoT en entornos urbanos.

3. Referencias normativas

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

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

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

- **Normativas:**
  - Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
  - Reglamento (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a las medidas para asegurar un alto nivel común de ciberseguridad en la UE (en adelante, NIS2).
  - Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD).
  - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).

- **Estándares:**
  - IEC 62443, Seguridad para sistemas de automatización y control industrial.
  - ISO/IEC 27400, Seguridad y privacidad en IoT.
  - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
  - ISO/IEC 25010, Gestión de la calidad en el software.
  - ISO/IEC 27001, Gestión de la seguridad de la información.
  - ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
  - ISO/IEC 27034, Seguridad en aplicaciones.
  - ISO/IEC/IEEE 29119, Análisis de software.
  - UNE 178107, Estándares para la gestión de infraestructuras en Ciudades Inteligentes.

- **Guías:**
  - CSA IoT Security Controls Framework.
  - ENISA, Guía para la securización de IoT.
  - ETSI EN 303 645, Requisitos de ciberseguridad para IoT.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - Guía NIST IR 8259, Medidas para fabricantes de dispositivos IoT.
  - Guía NIST SP 800-213, Requisitos de ciberseguridad para dispositivos IoT.
  - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
  - OWASP IoT Top 10.
  - OWASP ASVS/MASVS.

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

4. Definiciones

Acrónimos	Definición
Anonimización	Proceso mediante el cual los datos se transforman de forma irreversible para que no sea posible identificar a una persona.
API	Interfaz que permite la comunicación estructurada y controlada entre aplicaciones o servicios (del inglés, Application Programming Interface).
ASVS	Estándar de OWASP que define requisitos verificables de seguridad para aplicaciones web (del inglés, Application Security Verification Standard).
Backend	Parte de una aplicación que procesa la lógica de negocio, gestiona datos y expone servicios a otros componentes.
Binario	Archivo ejecutable o compilado que contiene el código máquina listo para su ejecución.
Borde	Entorno donde el procesamiento y análisis de datos se realiza lo más cerca posible de la fuente que los genera.
Bypass	Vulnerabilidad que permite saltarse los controles de autenticación o autorización y acceder a funciones o datos sin los permisos requeridos.
Bytecode	Código intermedio generado a partir del código fuente, ejecutado por una máquina virtual.
Código fuente	Conjunto de instrucciones legibles por humanos escritas en un lenguaje de programación.
Contenedor	Unidad ligera que empaqueta una aplicación con sus dependencias para ejecutarse de forma aislada.
CSA	Organización internacional dedicada a definir buenas prácticas, estándares y marcos de seguridad para la computación en la nube (del inglés, Cloud Security Alliance).
CVE	Sistema de identificación estándar que asigna un identificador único a vulnerabilidades de seguridad (del inglés, Common Vulnerabilities and Exposures).
CVSS	Estándar que asigna una puntuación de severidad técnica a una vulnerabilidad según su explotabilidad e impacto (del inglés, Common Vulnerability Scoring System).
DAST	Técnica de análisis de seguridad que evalúa una aplicación en ejecución desde el exterior (del inglés, Dynamic Application Security Testing).
Edge	Capa de procesamiento cercana al dispositivo IoT que reduce latencia y dependencia del backend central.
ETSI	Organismo europeo de normalización que define estándares técnicos, incluidos de IoT (del inglés, European Telecommunications Standards Institute).

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
Firmware	Software de bajo nivel embebido en un dispositivo que controla su funcionamiento básico.
Framework	Conjunto estructurado de normas, librerías o buenas prácticas que facilitan el desarrollo de software.
Hardening	Proceso de refuerzo de un sistema reduciendo su superficie de ataque mediante configuraciones seguras.
Librería	Conjunto reutilizable de funciones o componentes software usados por una aplicación.
Log	Registro de eventos, acciones o errores generado por sistemas y aplicaciones para trazabilidad y análisis.
MASVS	Estándar de OWASP que define requisitos de seguridad para aplicaciones móviles (del inglés, Mobile Application Security Verification Standard).
Middleware	Software intermedio que facilita la comunicación y gestión entre distintos componentes o servicios.
NIST	Instituto estadounidense que publica marcos y guías de referencia en ciberseguridad (del inglés, National Institute of Standards and Technology).
OWASP	Organización internacional que desarrolla guías, estándares y proyectos abiertos sobre seguridad del software (del inglés, Open Worldwide Application Security Project).
Pasarela	Componente hardware o software que actúa como punto de interconexión entre redes o sistemas, permitiendo la comunicación, traducción de protocolos y control del tráfico entre ellos.
Plan de contingencia	Conjunto de medidas y procedimientos predefinidos para garantizar la continuidad de las operaciones y minimizar el impacto ante incidentes, fallos o situaciones de emergencia.
Redundancia selectiva	Estrategia de resiliencia que consiste en duplicar únicamente los componentes, sistemas o servicios críticos, en función de su impacto y nivel de riesgo.
Reidentificación	Proceso mediante el cual datos previamente anonimizados o seudonimizados pueden volver a asociarse con una persona física.
Seudonimización	Técnica que sustituye identificadores directos por pseudónimos, permitiendo la reidentificación controlada.
SAST	Técnica de análisis de seguridad que examina el código fuente o bytecode sin ejecutar la aplicación (del inglés, Static Application Security Testing).
SBOM	Inventario estructurado de componentes software y dependencias que forman parte de una solución (del inglés, Software Bill of Materials).
SCA	Análisis de componentes de terceros para identificar vulnerabilidades y riesgos en dependencias (del inglés, Software Composition Analysis).

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

Acrónimos	Definición
Software	Conjunto de programas, datos y configuraciones que permiten el funcionamiento de sistemas digitales.
TIC	Tecnologías de la Información y las Comunicaciones utilizadas para procesar, almacenar y transmitir datos (del inglés, Information and Communications Technology).
VLAN	Segmentación lógica de red que separa dominios de tráfico para mejorar seguridad y control (del inglés, Virtual Local Area Network).
Vulnerabilidad	Debilidad en un sistema, diseño o implementación que puede ser explotada para comprometer la seguridad.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Estructura de la guía

La guía se organiza de forma progresiva desde un contexto inicial del ecosistema y los riesgos asociados, hasta los criterios técnicos necesarios y la verificación y comprobación de estos:

1. Ecosistema IoT en Smart Cities y principales retos

   Se describe el ecosistema IoT urbano y los retos de seguridad derivados de despliegues masivos, entornos distribuidos y servicios críticos.

2. Metodologías y marcos de referencia

   Se presentan los principales estándares y marcos utilizados como base que sirven para estructurar requisitos y controles.

3. Aplicación práctica de OWASP IoT Top 10 a Smart Cities

   Se contextualizan los riesgos del OWASP en escenarios urbanos, describiendo cómo se manifiestan y su impacto potencial en servicios municipales.

4. Arquitectura segura de soluciones IoT en Smart Cities

   Se recogen criterios de diseño arquitectónico seguro orientados a reducir la superficie de ataque y contener incidentes.

5. Desarrollo seguro de software IoT

   Se establecen principios y prácticas para integrar la seguridad en el ciclo de vida del software, incluyendo software embebido, plataformas, dependencias, pruebas y mantenimiento continuo.

6. Herramientas de seguridad

   Se describen categorías de herramientas para apoyar la implantación práctica de los controles.

7. Checklist de cumplimiento

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

Se aporta un checklist verificable con condiciones de cumplimiento y evidencias, para facilitar revisiones previas a producción y evaluaciones periódicas.

6. Ecosistema IoT en Smart Cities

El desarrollo de soluciones IoT constituye uno de los pilares fundamentales para la consolidación de las Smart Cities debido a que la incorporación de sensores, actuadores y sistemas distribuidos en el entorno urbano permite monitorizar, automatizar y optimizar servicios públicos críticos. Por ello, su diseño y despliegue deben realizarse de manera confiable, resiliente y con una visión integral de seguridad.

Estos componentes, integrados con infraestructuras de comunicaciones y plataformas de gestión, conforman un ecosistema complejo en el que la protección de la información es esencial. Desde una perspectiva de ciberseguridad, el IoT urbano no debe entenderse únicamente como un habilitador tecnológico, sino como un conjunto de activos críticos cuya protección debe garantizar la confidencialidad, integridad y disponibilidad de los datos que sustentan los servicios de la ciudad.

A diferencia de los sistemas TIC tradicionales, las soluciones IoT en entornos urbanos interactúan directamente con el mundo físico y con la ciudadanía, lo que amplifica el impacto potencial de cualquier fallo de seguridad. Los dispositivos suelen operar con recursos limitados, conectividad heterogénea, condiciones ambientales adversas y ciclos de vida prolongados, estas características condicionan tanto su diseño como su operación y requieren que la seguridad se integre desde etapas tempranas del desarrollo.

El ecosistema IoT en una Smart City se estructura en múltiples capas interdependientes, entre las que se encuentran dispositivos de campo, redes de comunicación, pasarelas o nodos de borde, y plataformas centrales de gestión y análisis de datos. Cada capa introduce riesgos específicos que, si no se gestionan adecuadamente, pueden propagarse y comprometer el sistema completo. Sobre estas capas se construyen las aplicaciones municipales que facilitan la automatización de procesos y la toma de decisiones basada en datos.

En este contexto, resulta imprescindible adoptar un enfoque integral de desarrollo seguro, alineado con las buenas prácticas del sector y la gestión de riesgos. Este enfoque debe garantizar que la seguridad se aplique de forma coherente, proporcional y transversal en todas las fases de diseño, desarrollo, despliegue y operación del ecosistema IoT urbano.

6.1. Principales retos

El desarrollo de soluciones IoT en el ámbito de las Smart Cities presenta una serie de retos específicos que condicionan de forma directa el diseño, la arquitectura y el ciclo de vida del software. A diferencia de otros entornos, las soluciones IoT urbanas se caracterizan por su gran escala, la heterogeneidad de dispositivos y plataformas, y la criticidad de los servicios que soportan, lo que incrementa significativamente la complejidad técnica y la superficie de ataque.

Desde la perspectiva del desarrollo seguro, estos factores obligan a integrar la seguridad como un requisito transversal desde las fases iniciales del diseño. La falta de consideración de estos retos en

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

etapas tempranas puede derivar en arquitecturas frágiles, dificultades en las tareas de mantenimiento y un aumento del riesgo operativo a lo largo de todo el ciclo de vida del sistema.

A continuación, se describen los principales retos que deben tenerse en cuenta durante el desarrollo de soluciones IoT para Smart Cities.

❖ Gestión de dispositivos y software embebido

Uno de los principales retos en el desarrollo de soluciones IoT es la gestión de dispositivos con recursos limitados y ciclos de vida prolongados. Estos dispositivos suelen operar con restricciones severas de procesamiento, memoria y energía, lo que limita la implementación de mecanismos de seguridad convencionales y condiciona las decisiones de diseño del software embebido.

Además, muchos dispositivos permanecen desplegados durante largos periodos de tiempo y en ubicaciones de difícil acceso, lo que refuerza la necesidad de diseñar desde el inicio mecanismos seguros de identificación, autenticación, provisión de credenciales y actualización remota de firmware. El desarrollo debe contemplar la seguridad del dispositivo a lo largo de todo su ciclo de vida, desde su fabricación y puesta en servicio hasta su mantenimiento y retirada.

❖ Seguridad de las comunicaciones y de las interfaces

Las soluciones IoT para Smart Cities hacen uso de múltiples tecnologías y protocolos de comunicación, así como de diversas interfaces entre dispositivos, plataformas, servicios y aplicaciones. Esta diversidad incrementa la complejidad del desarrollo y exige un diseño cuidadoso de los mecanismos de protección de las comunicaciones y de las APIs expuestas.

Desde el punto de vista del desarrollo, resulta esencial garantizar que las comunicaciones se diseñen de forma segura por defecto, incorporando mecanismos que aseguren la confidencialidad, integridad y autenticidad de los datos intercambiados. Asimismo, la definición de interfaces y servicios debe minimizar la exposición innecesaria, aplicar principios de segmentación y aislamiento, y facilitar la evolución segura de la arquitectura a lo largo del tiempo.

❖ Complejidad del ecosistema y dependencias de terceros

El desarrollo de soluciones IoT en Smart Cities se apoya habitualmente en un ecosistema amplio de componentes y servicios de terceros, incluyendo plataformas IoT, librerías de software, servicios en la nube y soluciones compartidas entre distintos actores. Esta dependencia introduce retos adicionales en materia de seguridad, especialmente en lo relativo a la gestión de vulnerabilidades, la trazabilidad de componentes y la coherencia de los controles de protección.

La reutilización de software y servicios puede acelerar el desarrollo, pero también amplía la superficie de ataque si no se gestionan adecuadamente las dependencias asociadas. Por ello, el desarrollo seguro debe incorporar criterios claros para la selección, integración y mantenimiento de componentes externos desde las fases iniciales del proyecto.

❖ Gobernanza de la seguridad en el desarrollo

La naturaleza colaborativa de las Smart Cities implica la participación de múltiples organizaciones a lo largo del ciclo de vida de la solución. Esta realidad introduce retos en la definición de responsabilidades

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 seguridad, especialmente cuando el desarrollo, la operación y el mantenimiento recaen en actores distintos.

Desde la perspectiva del desarrollo, es fundamental que los requisitos de seguridad estén claramente definidos y alineados entre todas las partes, y que se integren en los procesos de diseño, desarrollo y validación del software. La ausencia de una gobernanza clara puede traducirse en inconsistencias en la implementación de controles de seguridad y dificultades para gestionar riesgos de forma efectiva.

❖ **Gestión del ciclo de vida del dato**

Los datos generados y procesados por las soluciones IoT constituyen un elemento central de los servicios de Smart City. Desde el desarrollo de la solución, es necesario considerar de forma integral el ciclo de vida del dato, incluyendo su generación, transmisión, procesamiento, almacenamiento y eliminación.

El desarrollo seguro debe garantizar que los mecanismos de protección de la información se integren de forma coherente en todas las capas del sistema, evitando enfoques parciales o reactivos. La correcta gestión de accesos, la protección frente a manipulaciones y la resiliencia ante incidentes son aspectos clave que deben abordarse desde el diseño de las soluciones.

7. Metodologías y marcos de referencia

La adopción de metodologías y marcos de referencia reconocidos es un elemento esencial para garantizar un enfoque sistemático y coherente en el desarrollo seguro de soluciones IoT para Smart Cities. Dado que estos entornos combinan infraestructuras heterogéneas, dispositivos distribuidos, servicios críticos y múltiples actores involucrados, resulta insuficiente aplicar controles de seguridad aislados o de forma reactiva. En su lugar, es necesario apoyarse en modelos estructurados que permitan gestionar el riesgo, integrar la seguridad desde las primeras fases de diseño y mantenerla de manera continua a lo largo de todo el ciclo de vida de las soluciones.

En este ámbito, los marcos de referencia aportan un lenguaje común, criterios verificables y un conjunto de prácticas contrastadas que facilitan la toma de decisiones y la definición de requisitos proporcionales al impacto de cada solución IoT. Estos marcos pueden clasificarse en tres grandes categorías complementarias:

- **Marcos orientados a la gestión del riesgo**, que ayudan a identificar amenazas, analizar impactos y priorizar controles en función del contexto urbano y la criticidad del servicio.
- **Marcos basados en controles de seguridad**, que ofrecen catálogos de salvaguardas técnicas y organizativas para reforzar la protección en cada capa del ecosistema IoT.
- **Marcos centrados en el desarrollo seguro**, que integran la seguridad dentro de los procesos de diseño, implementación, validación y mantenimiento del software y del firmware asociado a las soluciones IoT.

Un aspecto clave en las Smart Cities es la necesidad de adaptar estos marcos, tradicionalmente concebidos para entornos TIC, al contexto operativo y a las particularidades del IoT urbano, como son los dispositivos con recursos limitados, la exposición física constante, la conectividad variable, los

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

despliegues masivos y los ciclos de vida prolongados. Estas características obligan a reinterpretar y ampliar los requisitos habituales de seguridad, priorizando principios como la seguridad desde el diseño y la seguridad por defecto.

Asimismo, la coexistencia de múltiples estándares, guías y metodologías exige un enfoque coordinado. En lugar de aplicar cada marco de forma independiente, es recomendable establecer correspondencias entre ellos, integrándolos según su propósito, identificación de riesgos, definición de requisitos de diseño, validación de arquitecturas o verificación del cumplimiento. Este enfoque evita duplicidades, reduce lagunas de seguridad y facilita una protección consistente en todo el ecosistema.

Finalmente, la selección y aplicación de estos marcos debe alinearse con las fases del ciclo de vida de las soluciones IoT en Smart Cities, desde la planificación y contratación, pasando por el diseño y el desarrollo seguro, hasta el despliegue, la operación y el mantenimiento. Su uso proporciona una base sólida y común para integrar la seguridad como un proceso continuo, garantizando la resiliencia y confiabilidad de los servicios urbanos conectados.

A continuación, se presentan los principales marcos seleccionados, junto con su papel en el desarrollo seguro de soluciones IoT en Smart Cities.

7.1. OWASP IoT Top 10

El OWASP IoT Top 10 es uno de los marcos más utilizados para identificar los **riesgos de ciberseguridad** más comunes en los **ecosistemas IoT**. Su enfoque, centrado en vulnerabilidades reales observadas en dispositivos y plataformas, lo convierte en una referencia especialmente útil en Smart Cities, donde la interconexión masiva y la criticidad de los servicios amplifican el impacto de cualquier fallo de seguridad.

Este marco destaca debilidades recurrentes como:

- Credenciales inseguras o por defecto.
- Autenticación y autorización insuficiente.
- Comunicaciones sin protección adecuada.
- Actualizaciones inseguras o inexistentes.
- Exposición innecesaria de interfaces y servicios.

En entornos urbanos, estas vulnerabilidades pueden derivar en accesos no autorizados, manipulación de datos o interrupciones de servicios esenciales, lo que refuerza la necesidad de abordarlas desde las fases iniciales del diseño y desarrollo.

El OWASP IoT Top 10 sirve como **punto de partida para el análisis de riesgos y la definición de requisitos de seguridad**, facilitando además un lenguaje común entre los diferentes actores implicados. En el contexto de esta guía, se utiliza como referencia base, complementándolo con otros estándares que aportan mayor nivel de detalle y cobertura a lo largo del ciclo de vida de las soluciones 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

7.2. OWASP ASVS/MASVS

Los estándares OWASP ASVS (del inglés, Application Security Verification Standard) y OWASP MASVS (del inglés, Mobile Application Security Verification Standard) proporcionan un **marco** estructurado para **definir y verificar requisitos de seguridad en aplicaciones web y móviles**. En el contexto de las Smart Cities, estos estándares son especialmente relevantes porque muchas soluciones IoT dependen de aplicaciones de gestión, supervisión o administración que actúan como interfaces críticas entre los dispositivos y servicios urbanos.

Ambos marcos ayudan a reforzar aspectos clave del software asociado al ecosistema IoT, como:

- Autenticación y autorización robusta.
- Gestión segura de accesos.
- Protección de datos en tránsito y en reposo.
- Seguridad en APIs y servicios expuestos.
- Buenas prácticas en el desarrollo y pruebas de seguridad.

Estos se estructuran en niveles de seguridad, lo que facilita su adaptación a distintos contextos y grados de criticidad. En el ámbito de las Smart Cities, esta característica permite definir requisitos proporcionales al impacto potencial de cada solución IoT, evitando enfoques homogéneos que no tengan en cuenta la diversidad de servicios urbanos y escenarios de uso. Asimismo, su estructura favorece la integración de la seguridad en los procesos de desarrollo, pruebas y adquisición de software, tanto propio como de terceros.

Cabe destacar que OWASP ASVS y MASVS no están orientados al desarrollo de firmware ni a la seguridad de los dispositivos IoT en sí mismos, sino a los componentes software de soporte que interactúan con ellos. En el marco de esta guía, estos estándares se consideran referencias complementarias al OWASP IoT Top 10, aportando un **nivel de detalle técnico y verificable para el desarrollo seguro de aplicaciones asociadas al ecosistema IoT urbano**. Su utilización conjunta contribuye a reforzar la seguridad global de las soluciones IoT desplegadas en Smart Cities.

7.3. NIST IR 8259/ SP 800-213

Las guías NIST IR 8259 y NIST SP 800-213 proporcionan un **marco de referencia** específico para la **seguridad de dispositivos IoT**, orientado a la definición de capacidades mínimas de ciberseguridad que deben integrarse desde las fases iniciales de diseño y desarrollo. Su enfoque resulta especialmente adecuado para el contexto de las Smart Cities, donde los dispositivos IoT se despliegan a gran escala, operan durante largos periodos y forman parte de servicios urbanos con distintos niveles de criticidad.

El **NIST IR 8259** establece un **conjunto de capacidades fundamentales que los dispositivos IoT** deben soportar, como la identificación y gestión de dispositivos, la protección de los datos, la configuración segura, la actualización de software y la gestión de eventos de seguridad. Estas capacidades permiten abordar riesgos habituales asociados a dispositivos con recursos limitados y elevada exposición, y facilitan la definición de requisitos de seguridad claros y verificables que deben incorporarse durante el desarrollo del firmware y de los componentes embebidos.

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

Por su parte, el **NIST SP 800-213** traduce estas capacidades en **recomendaciones prácticas** dirigidas a **fabricantes y desarrolladores**, proporcionando orientaciones sobre cómo implementar dichas funcionalidades de seguridad de manera efectiva. En entornos de Smart Cities, esta guía resulta especialmente útil para alinear los requisitos técnicos de los dispositivos con un enfoque de seguridad desde el diseño, favoreciendo soluciones más robustas, mantenibles y resilientes a lo largo de su ciclo de vida operativo.

En el marco de esta guía, las referencias del NIST se consideran un complemento clave a otros marcos de carácter más general, aportando una visión centrada en el dispositivo IoT como activo crítico dentro del ecosistema urbano. Su aplicación permite reforzar el desarrollo seguro de los dispositivos, mejorar la coherencia de los requisitos de seguridad y reducir los riesgos derivados de despliegues masivos de IoT en el ámbito de las Smart Cities.

7.4. ETSI EN 303 645

La norma ETSI EN 303 645 establece un **conjunto de requisitos y recomendaciones de seguridad orientados a reducir las vulnerabilidades más comunes en dispositivos IoT**. Aunque su ámbito original se centra en dispositivos de consumo, sus principios y controles resultan plenamente aplicables al desarrollo de soluciones IoT en el contexto de las Smart Cities, especialmente en despliegues que implican grandes volúmenes de dispositivos distribuidos y conectados a servicios urbanos.

El estándar define un conjunto estructurado de buenas prácticas que abordan aspectos esenciales del desarrollo seguro, como la eliminación de credenciales por defecto, el refuerzo de los mecanismos de autenticación, la protección de datos sensibles, la implementación de comunicaciones seguras y la capacidad de actualizar el software o firmware de forma fiable. Estos requisitos buscan mitigar vulnerabilidades frecuentes que aparecen tanto en dispositivos simples como en plataformas urbanas complejas, especialmente aquellas relacionadas con accesos no autorizados, compromisos del dispositivo o malas prácticas de configuración.

Uno de los elementos diferenciadores de ETSI EN 303 645 es su **enfoque práctico y orientado a asegurar un nivel básico de protección** aplicable de manera uniforme a una amplia variedad de dispositivos. Esto facilita su utilización como criterio en procesos de contratación, homologación o evaluación de proveedores, aportando un marco común para la definición de expectativas de seguridad en proyectos IoT urbanos.

No obstante, la norma debe entenderse como un punto de partida que proporciona un nivel mínimo de seguridad. En ecosistemas de Smart Cities, caracterizados por la diversidad tecnológica y la criticidad de algunos servicios, estos requisitos deben integrarse con otros marcos más específicos que abordan de manera detallada aspectos como la gestión del riesgo, el desarrollo seguro o la seguridad en plataformas y aplicaciones. Su valor, por tanto, reside en su capacidad para servir como base sólida sobre la que construir requisitos adicionales adaptados al contexto urbano.

En esta guía, ETSI EN 303 645 se adopta como referencia para asegurar que los dispositivos IoT empleados en Smart Cities cumplen con unas capacidades mínimas de seguridad desde el diseño. Su aplicación contribuye a fortalecer el ecosistema IoT urbano y a promover el despliegue de soluciones

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

más robustas, resilientes y alineadas con las buenas prácticas internacionales en materia de ciberseguridad.

7.5. ISO/IEC 27001

Las normas ISO/IEC 27001 e ISO/IEC 27002 proporcionan un marco consolidado para la gestión de la seguridad de la información, aplicable a las organizaciones que diseñan, desarrollan, operan o mantienen soluciones IoT en el ámbito de las Smart Cities. Aunque no están específicamente orientadas al desarrollo técnico de dispositivos o software IoT, su enfoque sistemático resulta fundamental para establecer una gobernanza adecuada que permita implantar y sostener prácticas de desarrollo seguro de forma coherente y controlada.

ISO/IEC 27001 define los **requisitos para implantar un sistema de gestión de la seguridad de la información** basado en la identificación y tratamiento de riesgos. En el contexto de las Smart Cities, este enfoque permite integrar el desarrollo seguro de soluciones IoT dentro de un marco organizativo más amplio, alineando los objetivos de seguridad con los servicios urbanos y garantizando la asignación clara de responsabilidades a lo largo del ciclo de vida de las soluciones. Por su parte, **ISO/IEC 27002** proporciona un **conjunto de controles de seguridad que sirven como referencia para apoyar la implementación de medidas técnicas y organizativas**.

La aplicación de estas normas facilita la gestión de riesgos transversales que afectan al desarrollo y operación de soluciones IoT, como la protección de la información, el control de accesos, la gestión de incidentes de seguridad o la continuidad de los servicios. Asimismo, contribuye a coordinar la seguridad entre los distintos actores implicados, incluidos proveedores y terceros, aspecto especialmente relevante en ecosistemas IoT urbanos caracterizados por la externalización y la dependencia de múltiples agentes.

En el marco de esta guía, ISO/IEC 27001 e ISO/IEC 27002 se consideran referencias complementarias a los marcos específicos de IoT y de desarrollo seguro. Estas normas no definen prácticas concretas de desarrollo de firmware o software IoT, pero proporcionan el marco organizativo necesario para que dichas prácticas se planifiquen, gobiernen y mantengan de forma consistente, reforzando la resiliencia global del ecosistema IoT en las Smart Cities.

7.6. CSA IoT Controls Framework

El CSA IoT Controls Framework, desarrollado por la Cloud Security Alliance, constituye un **marco integral de controles de seguridad** específicamente orientado a **ecosistemas IoT**. Su principal objetivo es ofrecer una visión estructurada que abarca todas las capas del entorno IoT, desde los dispositivos, las comunicaciones y las plataformas, hasta los procesos operativos y la gestión organizativa, lo que lo convierte en una referencia especialmente valiosa para las Smart Cities, donde la interoperabilidad, la complejidad y la participación de múltiples actores son elementos habituales.

El enfoque del CSA IoT Controls Framework destaca por combinar requisitos técnicos con consideraciones organizativas, proporcionando un equilibrio que facilita su aplicación tanto en fases de diseño y desarrollo como en procesos de despliegue, operación y mantenimiento. Su estructura permite identificar de forma clara qué controles deben aplicarse en cada componente del ecosistema 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

ayudando a traducir los riesgos identificados en medidas concretas y verificables. Esta capacidad resulta especialmente útil en entornos urbanos, donde los servicios pueden depender de múltiples proveedores y tecnologías, y donde la consistencia en la aplicación de medidas de seguridad es fundamental para evitar brechas o incoherencias en la protección.

Otro aspecto relevante del CSA IoT Controls Framework es su papel como puente entre marcos de gestión del riesgo y estándares más orientados al desarrollo técnico. Al integrar controles que abarcan desde la identidad de los dispositivos hasta la protección de datos, pasando por la monitorización continua o la seguridad en plataformas en la nube, el marco facilita la creación de un modelo de seguridad coherente y alineado con el ciclo de vida completo de las soluciones IoT.

En el contexto de esta guía, el CSA IoT Controls Framework se utiliza como una referencia complementaria que aporta granularidad y claridad en la definición y evaluación de controles específicos para IoT. Su adopción contribuye a reforzar la gobernanza de la seguridad, a mejorar la consistencia en la implementación de medidas de protección y a avanzar hacia un ecosistema IoT urbano más resiliente y alineado con buenas prácticas internacionales.

8. Aplicación práctica de OWASP IoT Top 10 a Smart Cities

El OWASP IoT Top 10 identifica un conjunto de áreas de riesgo recurrentes que afectan al diseño, desarrollo y operación de soluciones IoT. En el contexto de las Smart Cities, estas áreas de riesgo deben abordarse de forma sistemática durante el desarrollo seguro de las soluciones, teniendo en cuenta el despliegue masivo de dispositivos, la criticidad de los servicios urbanos y el impacto potencial de los incidentes de ciberseguridad.

A continuación, se describen los principales riesgos identificados en el OWASP IoT Top 10, adaptándolos al contexto del desarrollo seguro de soluciones IoT para Smart Cities.

8.1. I1 – Credenciales débiles o por defecto

El uso de credenciales débiles, por defecto o embebidas en dispositivos, firmware, plataformas o aplicaciones constituye uno de los riesgos más críticos en soluciones IoT. Este riesgo se produce cuando los sistemas utilizan contraseñas predeterminadas de fábrica, credenciales compartidas entre múltiples dispositivos, secretos codificados directamente en el software o mecanismos de autenticación insuficientemente robustos.

En el contexto de las Smart Cities, este riesgo se ve agravado por el despliegue masivo de dispositivos, la exposición física de muchos activos y la vida útil prolongada de las soluciones. Una debilidad en la gestión de credenciales puede replicarse de forma sistemática, permitiendo que el compromiso de un único componente derive rápidamente en el acceso no autorizado a un conjunto amplio de dispositivos y servicios urbanos.

El potencial impacto asociado a este riesgo podría ser:

- **Escalado masivo de ataques**: el uso de credenciales comunes o por defecto facilita que un atacante replique el acceso no autorizado sobre cientos o miles de dispositivos similares.

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

- **Suplantación de dispositivos y servicios**: posibilidad de que activos no legítimos se integren en la solución, enviando datos falsos o recibiendo instrucciones indebidas.
- **Manipulación de servicios urbanos**: alteración del funcionamiento de servicios críticos como alumbrado público, movilidad, gestión del agua o energía.
- **Pérdida de integridad y confianza**: modificación de datos operativos y pérdida de fiabilidad de la información utilizada para la toma de decisiones municipales.
- **Riesgos regulatorios y reputacionales**: acceso indebido a sistemas municipales o información sensible con impacto legal y de imagen pública.

8.2. I2 – Servicios de red inseguros

El riesgo de servicios de red inseguros se produce cuando los dispositivos IoT, pasarelas, plataformas o componentes intermedios exponen servicios de red innecesarios, mal configurados o desarrollados sin controles de seguridad adecuados. Este riesgo incluye la presencia de servicios abiertos sin autenticación, protocolos inseguros, puertos expuestos sin justificación funcional o interfaces de administración accesibles desde redes no confiables.

En entornos urbanos, se ve incrementado por la heterogeneidad tecnológica, la necesidad de interoperabilidad y la coexistencia de múltiples dominios de red. La exposición de servicios inseguros puede deberse a configuraciones por defecto, a decisiones de diseño inadecuadas o a la reutilización de componentes sin un análisis de su superficie de ataque. Dado el carácter distribuido de las soluciones IoT urbanas, estas debilidades pueden pasar desapercibidas durante largos periodos de tiempo.

El potencial impacto asociado a este riesgo podría ser:

- **Acceso no autorizado a dispositivos y plataformas**: explotación de servicios expuestos para obtener control parcial o total de activos IoT.
- **Ejecución de acciones indebidas**: posibilidad de enviar comandos no autorizados, modificar configuraciones o alterar el comportamiento de dispositivos y servicios.
- **Movimiento lateral dentro del sistema**: uso de servicios inseguros como punto de entrada para acceder a otros componentes de la arquitectura IoT o a sistemas municipales integrados.
- **Interrupción de servicios urbanos**: degradación o indisponibilidad de servicios críticos como alumbrado, tráfico, monitorización ambiental o gestión de infraestructuras.
- **Ampliación de la superficie de ataque**: incremento del número de vectores explotables, facilitando ataques automatizados y explotación masiva a gran escala.

8.3. I3 – Interfaces inseguras

El riesgo de interfaces de ecosistema inseguras se produce cuando las interfaces que conectan los distintos componentes de una solución IoT, como APIs, aplicaciones web, aplicaciones móviles, servicios cloud o paneles de gestión, presentan deficiencias en su diseño o implementación de seguridad. Estas deficiencias pueden incluir controles de autenticación o autorización insuficientes, validación

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

inadecuada de entradas, exposición excesiva de funcionalidades o una gestión incorrecta de sesiones y tokens.

En el contexto de las Smart Cities, las soluciones IoT suelen integrarse en ecosistemas complejos que involucran múltiples actores, plataformas compartidas y sistemas municipales. Esta necesidad de interoperabilidad incrementa el número de interfaces expuestas y amplía la superficie de ataque. Una debilidad en cualquiera de estas interfaces puede ser explotada para acceder de forma indebida a datos o servicios, incluso sin necesidad de comprometer directamente los dispositivos IoT.

El potencial impacto asociado a este riesgo podría ser:

- **Acceso no autorizado a plataformas y servicios**: explotación de APIs o interfaces de gestión para obtener acceso a funciones críticas o información sensible.
- **Manipulación de datos y servicios urbanos**: alteración de datos operativos, inyección de información falsa o modificación del comportamiento de servicios urbanos.
- **Compromiso transversal del ecosistema**: una interfaz insegura puede actuar como punto de entrada para afectar a múltiples sistemas integrados o a plataformas compartidas entre distintos servicios municipales.
- **Exposición de información sensible**: acceso indebido a datos operativos, información de configuración o datos potencialmente sensibles utilizados para la toma de decisiones.
- **Dependencia de terceros y pérdida de control**: vulnerabilidades en interfaces gestionadas por terceros pueden impactar directamente en la seguridad de la solución IoT urbana.

8.4. I4 – Ausencia de mecanismos de actualización segura

El riesgo de falta de mecanismos de actualización segura se produce cuando los dispositivos IoT, pasarelas (edge) o componentes de plataforma no disponen de un proceso fiable para distribuir, verificar e instalar actualizaciones de software/firmware de forma controlada. Esto incluye escenarios en los que no existe capacidad de actualización remota, el proceso no valida la autenticidad e integridad del paquete, o las actualizaciones dependen de intervenciones manuales difíciles de aplicar a gran escala.

En el contexto de las Smart Cities, este riesgo es especialmente relevante porque los despliegues IoT suelen tener ciclos de vida prolongados y operar durante años en producción. Si la solución no puede actualizarse de forma segura y sostenida, las vulnerabilidades descubiertas con posterioridad al despliegue inicial permanecen explotables, incrementando de manera progresiva la exposición al riesgo. Además, la heterogeneidad de dispositivos y proveedores puede dificultar la aplicación homogénea de correcciones si el mecanismo de actualización no está contemplado desde el diseño.

El potencial impacto asociado a este riesgo podría ser:

- **Exposición prolongada a vulnerabilidades conocidas**: imposibilidad de aplicar parches de seguridad a tiempo, manteniendo durante largos periodos puntos débiles explotables.
- **Compromiso gradual del ecosistema**: aumento acumulativo del riesgo a medida que aparecen nuevas vulnerabilidades en componentes que no pueden corregirse o actualizarse.

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

- **Interrupción de servicios urbanos**: fallos de seguridad o explotación de vulnerabilidades que pueden afectar a la disponibilidad de servicios críticos.
- **Dificultad de operación y mantenimiento**: dependencia de actualizaciones manuales o intervenciones en campo, poco viables en despliegues masivos, con aumento de costes y tiempos de respuesta.
- **Riesgo de actualización maliciosa**: si el proceso no verifica la autenticidad e integridad de los parches, un atacante puede intentar introducir software manipulado o no autorizado, comprometiendo dispositivos y plataformas.

8.5. I5 – Uso de componentes inseguros u obsoletos

El riesgo de uso de componentes inseguros u obsoletos se produce cuando una solución IoT incorpora software, librerías, frameworks, sistemas operativos, módulos, imágenes o firmware con vulnerabilidades conocidas, sin mantenimiento o fuera de soporte. Este riesgo afecta tanto al software embebido en dispositivos como a pasarelas, plataformas backend, aplicaciones y servicios de integración, y suele estar asociado a dependencias de terceros o a reutilización de componentes sin un control sistemático.

En el contexto de las Smart Cities, este riesgo se agrava por la larga vida útil de los despliegues y la dificultad de actualización de determinados activos en campo, provocando que componentes que en su momento eran válidos pueden quedar obsoletos con el tiempo si no existe un control de versiones y de vulnerabilidades.

El potencial impacto asociado a este riesgo podría ser:

- **Explotación de vulnerabilidades conocidas**: un atacante puede aprovechar fallos ya documentados en componentes obsoletos para comprometer el sistema.
- **Compromiso transversal del ecosistema**: una vulnerabilidad en un componente reutilizado puede afectar simultáneamente a múltiples servicios urbanos o instancias desplegadas.
- **Pérdida de integridad y fiabilidad**: manipulación de datos, inyección de información falsa o alteración del comportamiento de sistemas que soportan decisiones municipales.
- **Afectación a la disponibilidad**: interrupciones o degradación de servicios urbanos críticos debido a la explotación o fallos derivados de componentes sin soporte.
- **Dificultad de corrección y aumento de costes**: cuando un componente está fuera de soporte, aplicar mitigaciones o migrar a alternativas seguras requiere cambios mayores, con impacto en plazos, operación y sostenibilidad técnica del servicio.

8.6. I6 – Protección insuficiente de la privacidad

El riesgo de protección insuficiente de la privacidad se produce cuando una solución IoT recopila, procesa, almacena o comparte información sin aplicar controles adecuados para proteger los datos personales o potencialmente identificables. Este riesgo puede manifestarse por una recopilación

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

excesiva de datos, una falta de anonimización o pseudonimización, controles de acceso inadecuados, o una gestión ineficiente del ciclo de vida de la información.

En el contexto de las Smart Cities, muchas soluciones IoT gestionan datos que, de forma directa o indirecta, pueden asociarse a personas físicas, como información de movilidad, patrones de consumo, imágenes, identificadores de dispositivos o datos de localización. La combinación de múltiples fuentes de datos y su análisis conjunto incrementa el riesgo de reidentificación, incluso cuando los datos individuales parecen no ser sensibles.

El potencial impacto asociado a este riesgo podría ser:

- **Exposición de datos personales o sensibles**: acceso indebido a información que puede revelar hábitos, desplazamientos o comportamientos de la ciudadanía.
- **Riesgos legales y regulatorios**: incumplimiento de normativas de protección de datos, con posibles sanciones y obligaciones de notificación a autoridades y personas afectadas.
- **Pérdida de confianza de la ciudadanía**: percepción de uso indebido o poco transparente de los datos generados por servicios urbanos conectados.
- **Uso no autorizado de la información**: reutilización de datos para fines distintos a los previstos inicialmente o sin base legítima.
- **Impacto reputacional para la entidad**: deterioro de la imagen pública de las entidades responsables del servicio y cuestionamiento de la legitimidad de los proyectos urbanos.

8.7. I7 – Transferencia y almacenamiento inseguro de datos

El riesgo de transferencia y almacenamiento de datos inseguros se produce cuando la información generada, transmitida o almacenada por una solución IoT no está protegida adecuadamente frente a accesos no autorizados, manipulación o pérdida. Este riesgo puede manifestarse mediante el uso de canales de comunicación sin cifrar, mecanismos débiles de protección del almacenamiento, gestión inadecuada de claves criptográficas o configuraciones inseguras en dispositivos, pasarelas, plataformas y servicios asociados.

En el contexto de las Smart Cities, las soluciones IoT generan grandes volúmenes de datos operativos que circulan entre dispositivos distribuidos, componentes de borde, plataformas centrales y sistemas municipales. La diversidad de tecnologías, la heterogeneidad de entornos y la integración con múltiples servicios incrementan la probabilidad de que existan puntos débiles en el flujo o almacenamiento de la información. Una debilidad en cualquiera de estas etapas puede ser explotada para interceptar, modificar o extraer datos de forma indebida.

El potencial impacto asociado a este riesgo podría ser:

- **Intercepción y manipulación de datos**: captura de información en tránsito o alteración de datos operativos, afectando a la fiabilidad de los servicios urbanos.
- **Pérdida de integridad de la información**: introducción de datos falsos o modificación de registros que soportan procesos de decisión y operación municipal.

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 no autorizado a información sensible**: exposición de datos operativos, configuraciones internas o información potencialmente sensible almacenada en dispositivos o plataformas.
- **Impacto en la continuidad del servicio**: fallos operativos derivados de datos corruptos, incompletos o manipulados, con efectos sobre servicios críticos.
- **Riesgos legales y reputacionales**: posibles incumplimientos normativos y pérdida de confianza en la gestión de los datos urbanos por parte de las entidades.

8.8. I8 – Ausencia de gestión de dispositivos

El riesgo de falta de gestión de dispositivos se produce cuando una solución IoT no dispone de mecanismos adecuados para identificar, inventariar, supervisar y gestionar los dispositivos a lo largo de todo su ciclo de vida. Esto incluye situaciones en las que no existe un inventario fiable de activos, no se controla el estado de los dispositivos, no se gestionan correctamente altas y bajas, o no se dispone de capacidad para aislar o retirar dispositivos comprometidos.

En el contexto de las Smart Cities, donde los despliegues suelen ser masivos, distribuidos y heterogéneos, la ausencia de una gestión centralizada y estructurada de los dispositivos incrementa de forma significativa la superficie de ataque. Dispositivos olvidados, mal configurados o fuera de control pueden permanecer operativos durante largos periodos, actuando como puntos débiles dentro del ecosistema IoT urbano.

El potencial impacto asociado a este riesgo podría ser:

- **Pérdida de visibilidad del parque de dispositivos**: desconocimiento del número, ubicación, estado o versión de software de los activos desplegados.
- **Persistencia de dispositivos comprometidos**: incapacidad para detectar, aislar o retirar dispositivos que presentan comportamientos anómalos o han sido comprometidos.
- **Incremento del riesgo**: dispositivos no gestionados pueden ser utilizados como punto de entrada para atacar otros componentes de la solución o sistemas municipales integrados.
- **Dificultad de mantenimiento y actualización**: imposibilidad de aplicar actualizaciones, parches o cambios de configuración de forma homogénea y controlada.
- **Impacto en la continuidad del servicio**: fallos operativos o degradación de servicios urbanos críticos derivados de dispositivos defectuosos, obsoletos o fuera de control.

8.9. I9 – Configuración por defecto insegura

El riesgo de configuración por defecto insegura se produce cuando los dispositivos, pasarelas, plataformas o aplicaciones de una solución IoT se despliegan utilizando configuraciones predeterminadas que no han sido adaptadas al contexto operativo real. Estas configuraciones pueden incluir servicios innecesarios, puertos abiertos, parámetros de seguridad inadecuados o funcionalidades activadas que no son requeridas para el servicio.

En el contexto de las Smart Cities, este riesgo se ve amplificado por el despliegue masivo y repetitivo de componentes similares. Una configuración insegura aplicada por defecto puede replicarse

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

automáticamente en cientos o miles de activos, generando una exposición a gran escala y facilitando la explotación de la solución por parte de diferentes actores. Además, la presión por acelerar los despliegues puede llevar a mantener configuraciones iniciales sin una revisión de seguridad adecuada.

El potencial impacto asociado a este riesgo podría ser:

- **Ampliación de la superficie de ataque**: exposición de servicios, interfaces o funcionalidades que no son requeridas para la operación del servicio urbano.
- **Explotación automatizada a gran escala**: una configuración por defecto insegura puede ser explotada de forma masiva al repetirse en numerosos dispositivos.
- **Acceso no autorizado a sistemas y datos**: aprovechamiento de parámetros inseguros para obtener acceso indebido a dispositivos, plataformas o información operativa.
- **Degradación de la seguridad del ecosistema**: una debilidad común en la configuración puede comprometer la arquitectura completa, incluso si otros controles están correctamente implementados.
- **Impacto operativo y reputacional**: incidentes de seguridad derivados de configuraciones inseguras que afectan a la continuidad del servicio y a la confianza en los proyectos urbanos.

8.10. I10 – Falta de protección física

El riesgo de falta de protección física se produce cuando los dispositivos IoT y los componentes de borde se despliegan en ubicaciones accesibles sin contar con medidas adecuadas para prevenir manipulaciones, accesos no autorizados o sabotajes físicos. Este riesgo incluye la exposición de puertos físicos, interfaces de depuración, almacenamiento accesible, carcasas sin protección o la ausencia de mecanismos de detección de manipulación.

En el contexto de las Smart Cities, muchos dispositivos IoT se instalan en espacios públicos o semipúblicos, como farolas, semáforos, armarios urbanos, estaciones de medida o edificios municipales, donde el acceso físico por parte de terceros es factible. La falta de protección física adecuada puede permitir a un atacante manipular directamente el dispositivo, alterar su software o utilizarlo como punto de entrada para comprometer otros elementos del ecosistema IoT.

El potencial impacto asociado a este riesgo podría ser:

- **Manipulación directa de dispositivos**: alteración del comportamiento de sensores o actuadores mediante acceso físico, afectando a la operación de servicios urbanos.
- **Compromiso lógico a partir de acceso físico**: extracción de firmware, credenciales o claves que permitan ataques posteriores sobre plataformas y sistemas centrales.
- **Introducción de dispositivos maliciosos**: sustitución o modificación de equipos legítimos para enviar datos falsos o recibir instrucciones indebidas.
- **Interrupción o sabotaje de servicios**: degradación o indisponibilidad de servicios críticos como alumbrado, control de tráfico, monitorización ambiental o gestión de infraestructuras.

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

- **Dificultad de detección del incidente**: los ataques físicos pueden pasar desapercibidos durante largos periodos, especialmente en despliegues extensos y distribuidos.
- **Impacto reputacional y operativo**: incidentes visibles en el espacio público que afectan a la confianza en los proyectos de Smart City y generan costes de reposición y mantenimiento.

En conjunto, estos riesgos recogidos en el OWASP IoT Top 10, proporcionan una base sólida para orientar el desarrollo seguro de soluciones IoT en Smart Cities.

9. Arquitectura segura IoT

La arquitectura de una solución IoT en el ámbito de las Smart Cities constituye un elemento clave en los aspectos relacionados con la seguridad de la información, ya que establece cómo se organizan, e interconectan los distintos componentes a lo largo de todo su ciclo de vida. En entornos urbanos, donde coexisten dispositivos distribuidos, pasarelas, plataformas de gestión e integraciones con sistemas municipales, el diseño de la arquitectura condiciona de forma directa la superficie de ataque, la capacidad de respuesta ante incidentes y la viabilidad de aplicar controles de seguridad.

Los riesgos descritos en el capítulo anterior ponen de manifiesto que aspectos como la identidad y el control de acceso, la protección de las comunicaciones e interfaces, la configuración segura, la actualización del software, la protección de la información, la monitorización y la cadena de suministro no pueden abordarse eficazmente mediante medidas aisladas. Estos aspectos requieren una arquitectura que permita limitar el impacto de fallos, errores de configuración o compromisos parciales del sistema.

Con el fin de estructurar una arquitectura segura de soluciones IoT, esta guía adopta como referencia principal el CSA IoT Controls Framework, al tratarse de un marco orientado específicamente a entornos IoT y por organizar la seguridad en dominios alineados con una arquitectura multicapa. Este enfoque facilita la traducción de los riesgos en decisiones arquitectónicas concretas, favoreciendo diseños modulares, segmentados y resilientes, especialmente adecuados para despliegues a gran escala en Smart Cities.

En los apartados siguientes se presentan los principios y decisiones arquitectónicas exigibles para construir soluciones IoT seguras en el contexto urbano, estableciendo las bases que posteriormente se desarrollarán en el capítulo de desarrollo seguro de software IoT, donde estas decisiones se materializan en prácticas de implementación, verificación y mantenimiento continuo.

9.1. Arquitectura segmentada por dominios

El diseño arquitectónico de una solución IoT en el ámbito de las Smart Cities debe estructurarse en capas y dominios claramente diferenciados, evitando arquitecturas planas en las que todos los componentes comparten implícitamente el mismo nivel de confianza. La segmentación adecuada permite limitar la propagación de incidentes de seguridad, reducir la superficie de exposición y facilitar la aplicación de políticas de seguridad en entornos urbanos complejos y distribuidos.

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

Una arquitectura segmentada no solo organiza técnicamente el sistema, sino que establece fronteras explícitas entre dispositivos, infraestructuras de comunicación, componentes de borde, plataformas IoT y sistemas corporativos o municipales. Estas fronteras permiten definir relaciones de confianza controladas, aplicar mecanismos de aislamiento y reducir el impacto de los compromisos, evitando que una incidencia en un dominio se propague al resto de la solución.

Como decisiones arquitectónicas exigibles, deberán contemplarse, al menos, las siguientes:

- **Segmentación lógica**: separación clara entre dispositivos IoT, redes de comunicaciones, pasarelas o componentes de borde, plataformas de gestión y sistemas externos o municipales.
- **Dominios de confianza**: definición de niveles de confianza diferenciados entre componentes, evitando suposiciones implícitas sobre el comportamiento seguro de otros dominios.
- **Aislamiento funcional**: separación de servicios críticos respecto a servicios de menor impacto, reduciendo el alcance de posibles incidentes o errores de configuración.
- **Flujos controlados**: delimitación, documentación y justificación de los flujos de datos y control permitidos entre dominios.
- **Interconexiones reguladas**: establecimiento de puntos de acceso claramente definidos y controlados entre capas y sistemas municipales, evitando interconexiones directas no supervisadas.

Este enfoque deberá reflejarse en un **diagrama de arquitectura** que identifique de forma clara las capas del sistema, los dominios de seguridad y los puntos de interconexión existentes entre ellos. La documentación técnica asociada deberá describir de manera estructurada los flujos de información y de control entre componentes, así como justificar explícitamente las relaciones de confianza definidas.

9.2. Integración segura de dispositivos y componentes de borde

La integración de dispositivos IoT y componentes de borde debe abordarse como un elemento estructural de la arquitectura y no como una simple conexión técnica. Los dispositivos desplegados en campo y las pasarelas que los agregan constituyen el principal punto de entrada al sistema y, en muchos casos, operan en entornos expuestos o de difícil control físico. Por este motivo, su incorporación debe realizarse bajo un modelo de confianza y mecanismos arquitectónicos que eviten accesos directos e indiscriminados a las plataformas centrales.

En el contexto de las Smart Cities, los componentes de borde desempeñan un papel clave como capa intermedia de control, validación y aislamiento entre los dispositivos y los sistemas centrales. Una arquitectura bien diseñada debe evitar relaciones de confianza implícitas entre dispositivos de campo y plataformas de backend, delegando en los componentes de borde la aplicación de políticas, la validación del tráfico y la contención de posibles incidentes

Como decisiones arquitectónicas exigibles, deberán contemplarse, al menos, las siguientes:

- **Registro previo**: incorporación de dispositivos únicamente tras un proceso formal de alta, evitando la conexión de activos no autorizados.

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

- **Punto de agregación**: uso de pasarelas o nodos de borde como elemento intermedio obligatorio antes del acceso a la plataforma IoT, evitando conexiones directas desde dispositivos de campo.
- **Canales dedicados**: separación de las comunicaciones de los dispositivos y del edge respecto a redes corporativas generales u otros entornos no controlados.
- **Validación de tráfico**: control y filtrado del tipo de datos, comandos y frecuencias que pueden circular desde el edge hacia los sistemas centrales, reduciendo el riesgo de abusos o comportamientos anómalos.
- **Revocación estructurada**: capacidad de aislar, desactivar o excluir dispositivos comprometidos sin afectar al funcionamiento global del sistema.

Este planteamiento deberá quedar reflejado en la **documentación de integración de dispositivos y componentes de borde**, describiendo el proceso formal de alta, el modelo de confianza adoptado y la función concreta que desempeñan las pasarelas dentro de la arquitectura.

Asimismo, la configuración de red deberá evidenciar la **separación** efectiva entre el **dominio de dispositivos y los entornos corporativos o municipales**, garantizando que dicha segmentación no solo esté documentada, sino también implementada técnicamente

9.3. Plataformas y backend seguros

Las plataformas IoT y los servicios backend constituyen el núcleo lógico de la solución, al concentrar la gestión de dispositivos, el tratamiento y almacenamiento de datos, y la integración con otros sistemas municipales. Debido a su papel central, estos componentes operan en un dominio de alta criticidad y deben diseñarse de forma que se aplique el principio de mínimo privilegio y se limiten las dependencias entre funciones.

Una arquitectura bien definida debe establecer separaciones claras entre las funciones de administración, operación y explotación de la información, reduciendo el impacto de errores de configuración, accesos indebidos o compromisos parciales. Asimismo, debe facilitar la gobernanza técnica del sistema y permitir su evolución controlada sin degradar los niveles de seguridad establecidos

Como decisiones arquitectónicas exigibles, deberán contemplarse, al menos, las siguientes:

- **Separación de funciones**: diferenciación entre módulos de gestión de dispositivos, procesamiento de datos y exposición de información o servicios, evitando accesos transversales innecesarios.
- **Entornos diferenciados**: existencia de entornos claramente separados para desarrollo, preproducción y producción, con controles que impidan la propagación de configuraciones, datos o accesos entre ellos.
- **Control de integraciones**: definición formal y documentada de los puntos de conexión con otros sistemas municipales o servicios externos, evitando integraciones implícitas o no gobernadas.
- **Gestión de accesos privilegiados**: delimitación clara entre accesos administrativos y accesos operativos o de personas usuarias, aplicando controles específicos para funciones de alta criticidad.

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

- **Escalabilidad controlada**: diseño que permita la ampliación de capacidades y servicios sin introducir nuevos dominios de confianza ni alterar el modelo de seguridad definido.

Este enfoque deberá quedar reflejado de forma clara y verificable en la **documentación de arquitectura de la plataforma**, incluyendo esquemas de despliegue que identifiquen los distintos entornos, los módulos funcionales y las relaciones existentes entre ellos

Deberán definirse y describirse formalmente las **integraciones con sistemas externos**, asegurando que cada punto de conexión esté documentado, justificado y sujeto a mecanismos de control y supervisión.

Asimismo, deberá evidenciarse la **separación** efectiva **entre los accesos administrativos y los accesos operativos o de personas usuarias**, garantizando que las funciones de alta criticidad estén protegidas mediante controles específicos y diferenciados.

9.4. Operación y continuidad del servicio

La arquitectura de una solución IoT en el ámbito de las Smart Cities no debe limitarse a su diseño inicial, sino contemplar desde el inicio su operación continuada y su capacidad de adaptación ante incidentes, fallos parciales o cambios tecnológicos. Un diseño arquitectónico adecuado debe permitir mantener la continuidad de los servicios urbanos, aislar componentes comprometidos y evolucionar el sistema sin degradar los niveles de seguridad previamente definidos.

Desde una perspectiva arquitectónica, la operación segura y la resiliencia del sistema deben estar soportadas por decisiones estructurales que faciliten la supervisión, la contención de impactos y la recuperación controlada ante eventos adversos. En entornos urbanos complejos y distribuidos, estas capacidades no pueden depender exclusivamente de procedimientos operativos, sino que deben integrarse de forma explícita en el diseño de la solución.

Como decisiones arquitectónicas exigibles, deberán contemplarse, al menos, las siguientes:

- **Aislamiento de impacto**: diseño que permita contener incidentes dentro de un dominio o componente concreto, evitando su propagación al conjunto del sistema.
- **Supervisión integrada**: incorporación estructural de capacidades de monitorización y registro en las distintas capas de la arquitectura, proporcionando visibilidad sobre el estado y comportamiento del sistema.
- **Gestión del ciclo de vida**: previsión de mecanismos que permitan la actualización, sustitución o retirada de componentes sin requerir rediseños completos ni comprometer la seguridad global.
- **Redundancia selectiva**: identificación de los elementos críticos del sistema y definición de mecanismos de continuidad adecuados a su impacto operativo.
- **Plan de contingencia técnico**: definición de escenarios de fallo previsibles y de las estrategias arquitectónicas asociadas para su recuperación o degradación controlada del servicio.

La arquitectura deberá reflejar estos elementos en sus esquemas de despliegue, identificando claramente los **componentes críticos**, sus **dependencias** y los **mecanismos** previstos para su recuperación.

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, deberán existir referencias documentadas a las **capacidades de supervisión** integradas en la solución y a los **procedimientos técnicos** que describen la gestión de fallos, la sustitución de componentes y los mecanismos de degradación controlada del servicio.

En conjunto, la arquitectura segura de soluciones IoT en Smart Cities debe concebirse como un sistema modular, segmentado y gobernable, basado en dominios de seguridad claramente definidos y relaciones de confianza explícitas. El uso del CSA IoT Controls Framework como referencia principal permite estructurar esta arquitectura de forma coherente, alineando riesgos, decisiones arquitectónicas y componentes técnicos, y proporcionando una base sólida para el desarrollo seguro, la operación resiliente y la evolución sostenible de los servicios urbanos basados en IoT.

10. Desarrollo seguro de software IoT

El software constituye uno de los elementos más determinantes en la seguridad de las soluciones IoT desplegadas en entornos de Smart Cities. A diferencia de otros componentes más visibles, como los dispositivos físicos o las infraestructuras de comunicación, el software actúa como el elemento integrador que gobierna el funcionamiento del sistema, gestiona los datos, controla los dispositivos y habilita los servicios urbanos. Por este motivo, deficiencias en su diseño, desarrollo o mantenimiento pueden introducir riesgos significativos con impacto transversal sobre múltiples servicios municipales.

En una solución IoT, el software no se limita a un único componente, sino que se distribuye a lo largo de todo el ecosistema, incluyendo el software embebido en los dispositivos, los componentes que operan en pasarelas o nodos de borde, las plataformas centrales de gestión y análisis, así como las aplicaciones web y móviles utilizadas para la supervisión y operación de los servicios. La seguridad de la solución depende, por tanto, de la coherencia y solidez con la que se desarrollan, integran y mantienen todos estos elementos, y no únicamente de la aplicación de medidas aisladas en un punto concreto del sistema.

En el contexto de las Smart Cities, el papel del software adquiere una relevancia adicional debido a la escala y criticidad de los despliegues, ya que un fallo de seguridad en un componente software podría afectar simultáneamente a un gran número de dispositivos, comprometer la disponibilidad de servicios urbanos esenciales o permitir accesos no autorizados a sistemas municipales. Además, muchos de estos sistemas están diseñados para operar durante largos periodos de tiempo, lo que incrementa la exposición a vulnerabilidades descubiertas con posterioridad a su despliegue inicial y refuerza la necesidad de una gestión continua del riesgo.

Desde una perspectiva de desarrollo seguro, resulta fundamental entender que la seguridad del software no puede abordarse únicamente como una cuestión técnica o de implementación puntual, sino como el resultado de un conjunto de decisiones tomadas a lo largo de todo su ciclo de vida. En este sentido, aspectos como la definición de requisitos, el diseño alineado con la arquitectura de seguridad, la gestión de accesos, la protección de la información, la integración de dependencias o la capacidad de actualización y mantenimiento influyen de manera directa en el nivel de riesgo asumido por la solución 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

Este capítulo de la guía aborda el desarrollo seguro del software IoT desde un enfoque orientado a la gestión del riesgo y a la toma de decisiones informadas. Su objetivo es proporcionar criterios que permitan al personal técnico y no técnico comprender qué aspectos del software son críticos para la seguridad, qué capacidades deben exigirse a las soluciones IoT y cómo evaluar si el desarrollo del software contribuye de forma efectiva a la resiliencia de los servicios urbanos en el ámbito de las Smart Cities.

10.1. Principios generales de desarrollo seguro aplicables a IoT

El desarrollo de software en soluciones IoT deberá basarse en un conjunto de principios de seguridad que orienten las decisiones técnicas desde las fases iniciales del proyecto. La aplicación de estos principios permite reducir el riesgo, prevenir la introducción de vulnerabilidades y minimizar el coste asociado a su corrección una vez desplegada la solución.

En el contexto de las Smart Cities, donde los sistemas IoT operan de forma distribuida, a gran escala y durante largos periodos de tiempo, la aplicación de estos principios resulta esencial para garantizar la integridad, disponibilidad y confianza en los servicios urbanos.

- **Seguridad desde el diseño**: La seguridad deberá integrarse desde las fases iniciales de análisis y arquitectura, formando parte de las decisiones funcionales y técnicas. No podrá considerarse un elemento añadido posteriormente, sino un requisito estructural del sistema.
- **Mínimo privilegio**: Cada componente, proceso, servicio o cuenta de acceso deberá disponer únicamente de los permisos estrictamente necesarios para desempeñar su función, evitando privilegios excesivos que puedan incrementar el impacto de un compromiso. Se promoverá, además, la separación de responsabilidades para limitar dependencias críticas.
- **Defensa en profundidad**: La protección del sistema deberá apoyarse en múltiples capas de seguridad complementarias, evitando la dependencia de un único mecanismo de control. El diseño no deberá asumir confianza implícita entre componentes y deberá incorporar medidas adicionales frente a accesos no autorizados o comportamientos anómalos.
- **Segmentación**: La arquitectura del software deberá facilitar la separación lógica de funciones y componentes, reduciendo dependencias innecesarias y evitando accesos transversales no justificados. Este principio contribuye a limitar la propagación de incidentes dentro del sistema.
- **Gestión segura del ciclo de vida**: El desarrollo deberá contemplar la capacidad de actualizar, corregir, sustituir y retirar componentes sin comprometer la seguridad global. La evolución del sistema deberá realizarse de forma controlada y alineada con el modelo de seguridad definido.
- **Protección de datos por defecto**: El tratamiento de datos deberá incorporar mecanismos de confidencialidad, integridad y disponibilidad desde su generación, limitando su exposición y garantizando el acceso únicamente a entidades autorizadas. Se evitará la recopilación innecesaria de información.
- **Configuración segura por defecto**: Las configuraciones iniciales deberán ser restrictivas y coherentes con los requisitos de seguridad establecidos. El sistema no deberá depender de ajustes posteriores para alcanzar un nivel adecuado de protección.

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

- **Trazabilidad y registro**: El software deberá incorporar capacidades de registro y auditoría que permitan trazar acciones relevantes, accesos a funcionalidades críticas y cambios de configuración. La trazabilidad deberá considerarse un requisito de diseño.
- **Gestión formal de cambios**: Toda modificación relevante deberá someterse a un proceso estructurado de evaluación previa, incluyendo análisis de impacto sobre la seguridad, antes de su despliegue en entornos operativos.
- **Validación y pruebas de seguridad**: El sistema deberá someterse a pruebas de seguridad durante todo su ciclo de vida, con el fin de verificar el cumplimiento de los requisitos definidos y detectar vulnerabilidades de forma temprana.

10.2. Integración de la seguridad en el ciclo de vida del software IoT

La integración de la seguridad en el ciclo de vida del software IoT resulta esencial para garantizar que las soluciones desplegadas en entornos urbanos mantengan un nivel de protección adecuado a lo largo del tiempo.

Este enfoque permite reducir riesgos de forma temprana, facilitar la gestión de cambios y asegurar que las decisiones técnicas adoptadas durante el desarrollo sean coherentes con los requisitos de seguridad, arquitectura y operación definidos para la solución. En sistemas IoT urbanos, caracterizados por su gran escala, complejidad y larga vida útil, la integración de la seguridad en el ciclo de vida constituye un elemento clave para la resiliencia y fiabilidad de los servicios.

❖ Planificación y requisitos

En las fases iniciales del proyecto deberán **identificarse** los **activos críticos** de la solución, los posibles **escenarios de riesgo** y los **requisitos de seguridad** asociados. La definición de requisitos no debe limitarse a funcionalidades técnicas, sino incluir aspectos como la protección de datos, el control de accesos, la capacidad de actualización segura, la gestión de dependencias y las necesidades de registro y supervisión.

Esta fase debe contemplar explícitamente la realidad del despliegue, incluyendo los dispositivos de campo, componentes de borde, plataformas centrales y posibles integraciones con sistemas municipales.

Una identificación temprana y estructurada de estos requisitos permite orientar adecuadamente las decisiones de diseño y arquitectura, evitando dependencias posteriores de difícil corrección y reduciendo el riesgo de introducir debilidades estructurales en el sistema.

❖ Diseño y arquitectura

Durante el diseño del software deberán **aplicarse** los **principios** descritos en el apartado anterior, alineando las decisiones de desarrollo con la arquitectura de seguridad definida para la solución. En esta fase se deberá realizar un **análisis de riesgos** y, cuando resulte apropiado, ejercicios de **modelado de amenazas** que permitan identificar puntos críticos y definir mecanismos de mitigación desde el 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

El diseño debe asumir entornos distribuidos y relaciones de confianza limitadas entre componentes, evitando dependencias y considerando que no todos los activos podrán actualizarse con la misma frecuencia.

Esta etapa resulta clave para definir los mecanismos de autenticación y autorización, la segregación de componentes, la protección de los datos, la gestión de errores y las estrategias de actualización y mantenimiento. Las decisiones adoptadas condicionan de forma directa el nivel de exposición del sistema a lo largo de toda su vida útil.

❖ Desarrollo e implementación

En la fase de desarrollo e implementación deberán aplicarse prácticas de **codificación segura**, **revisiones técnicas** y **controles** que permitan detectar errores y debilidades antes de su incorporación a entornos operativos. El proceso de desarrollo debe facilitar la identificación temprana vulnerabilidades, evitando que se propaguen a lo largo del sistema.

Estas prácticas deben aplicarse tanto al software embebido como a las plataformas, APIs e interfaces de operación.

La integración de verificaciones automáticas y revisiones de código o seguridad dentro del proceso de desarrollo contribuye a mejorar la calidad del software y a reducir la probabilidad de introducir fallos con impacto en la seguridad de la solución IoT.

❖ Pruebas y validación

La verificación de la seguridad del software deberá realizarse de forma progresiva **a lo largo del ciclo de vida** y no limitarse a una revisión final previa al despliegue. Las pruebas deben permitir comprobar que los requisitos de seguridad definidos se han implementado correctamente y que el comportamiento del software es coherente con los niveles de riesgo asumidos.

La validación debe considerar la interacción entre componentes y los puntos de integración, dado que la mayoría de las vulnerabilidades aparecen entre los límites de las capas.

Estas pruebas deben generar evidencias técnicas trazables que respalden la toma de decisiones y faciliten la evaluación del cumplimiento de los requisitos de seguridad, tanto en fases previas al despliegue como ante cambios significativos del sistema.

❖ Despliegue, operación y mantenimiento

Una vez desplegado **en producción**, la seguridad del software debe mantenerse mediante **procedimientos de actualización**, **gestión de vulnerabilidades**, **supervisión** de eventos y **control de cambios**. El ciclo de vida seguro del software IoT no finaliza con la puesta en servicio, sino que se extiende durante todo el periodo de operación del sistema.

En soluciones IoT destinadas a operar durante largos periodos de tiempo en entornos urbanos, esta fase adquiere una relevancia especial, debido que la sustitución o actualización de los dispositivos puede ser costosa o limitada, y cualquier vulnerabilidad puede persistir si no existe una gestión continua del software.

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, garantizar la disponibilidad del servicio requiere adaptar la solución a nuevas amenazas y cambios tecnológicos sin degradar el nivel de seguridad alcanzado.

10.3. Seguridad del software embebido y componentes de borde

El software embebido en los dispositivos IoT, así como el que opera en pasarelas o componentes de borde constituye el punto de contacto directo entre el entorno físico y la infraestructura lógica de la solución. Esta capa concentra riesgos específicos derivados tanto de su exposición física como de su función de agregación, validación y transmisión de datos hacia las plataformas centrales.

En el contexto de las Smart Cities, estos componentes suelen desplegarse de forma masiva, en ubicaciones accesibles y con ciclos de vida prolongados. Un diseño inseguro del software puede permitir la manipulación de dispositivos, la inyección de datos falsos, la degradación de servicios urbanos o la incorporación de nodos no autorizados en la solución. Dado su papel como primera línea de defensa, la seguridad del software en esta capa debe abordarse como un elemento crítico del desarrollo seguro de soluciones IoT.

❖ Identidad y autenticación del dispositivo

Cada dispositivo IoT deberá disponer de una **identidad única y verificable** dentro del sistema. El software embebido deberá implementar mecanismos que impidan la suplantación, la clonación lógica o el registro no autorizado de nuevos nodos, evitando el uso de identidades compartidas o credenciales estáticas reutilizables.

En el caso de pasarelas y componentes de borde, deberán aplicarse controles adicionales que permitan autenticar de forma fiable a los dispositivos que agregan y validan la legitimidad de las comunicaciones entrantes. Esto resulta especialmente relevante en entornos urbanos, donde la incorporación de activos no autorizados puede pasar inadvertida si no existen mecanismos explícitos de validación en el borde.

❖ Configuración segura y reducción de superficie de exposición

El software embebido deberá operar con **configuraciones restrictivas por defecto**, **deshabilitando** en producción **interfaces**, **servicios**, **cuentas** o **funcionalidades** que **no** sean estrictamente **necesarias** para su funcionamiento. El desarrollo no debe asumir que estos ajustes se realizarán posteriormente de forma manual, sino proporcionar configuraciones iniciales seguras desde el primer despliegue.

En dispositivos desplegados en entornos físicamente accesibles, deberán contemplarse mecanismos que dificulten la modificación no autorizada de parámetros críticos o la extracción de información sensible almacenada localmente. La reducción de la superficie de exposición resulta esencial para limitar vectores de ataque en entornos IoT distribuidos, donde la explotación de un único dispositivo puede replicarse de forma masiva.

❖ Protección de comunicaciones y validación de datos

Las comunicaciones entre dispositivos, pasarelas y plataformas deberán incorporar **mecanismos** que garanticen la **autenticidad** e **integridad** de la **información intercambiada**, evitando la manipulación de datos o comandos en tránsito.

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 software embebido y de borde deberá validar de forma sistemática los datos recibidos antes de su procesamiento, almacenamiento o retransmisión. Esta validación debe impedir que entradas manipuladas, inconsistentes o fuera de rango se propaguen hacia capas superiores del sistema y afecten al funcionamiento global de la solución o a la toma de decisiones basada en datos urbanos.

❖ Actualización segura

El software embebido y los componentes de borde deberán incorporar **mecanismos** que permitan su **actualización de forma controlada** y **segura** a lo largo de todo su ciclo de vida. Estas actualizaciones deberán garantizar la autenticidad e integridad del código antes de su instalación y permitir la trazabilidad de las versiones desplegadas en cada activo.

La capacidad de actualización segura resulta especialmente relevante en soluciones IoT con largos periodos de operación, donde la corrección de vulnerabilidades descubiertas con posterioridad al despliegue inicial es un requisito esencial para mantener la seguridad del sistema.

❖ Gestión de errores

El **tratamiento de errores, excepciones y condiciones anómalas** deberá realizarse de forma controlada, evitando la exposición de información sensible, la ejecución de comportamientos inseguros o la entrada en estados no deseados que puedan ser explotados.

En el caso de pasarelas y componentes de borde, el diseño del software deberá contemplar la capacidad de continuar operando de forma degradada ante fallos de conectividad con la plataforma central, siempre que ello no comprometa la seguridad de la solución ni permita eludir los controles establecidos. Esta resiliencia local es clave para mantener la continuidad de los servicios urbanos ante incidencias parciales de red o infraestructura.

10.4. Seguridad del software de las plataformas, interfaces y aplicaciones

Las plataformas centrales, los servicios backend, las interfaces de integración y las aplicaciones de gestión constituyen el núcleo lógico de la solución IoT. En esta capa se concentran la administración de dispositivos, el tratamiento y explotación de los datos, la exposición de servicios y la interacción con personas usuarias internas y externas. Debido a su carácter centralizado, un diseño inseguro del software en esta capa puede permitir accesos indebidos a información sensible, la alteración de configuraciones críticas o la interrupción de servicios municipales de alto impacto.

En el contexto de las Smart Cities, estas plataformas suelen dar servicio a múltiples sistemas, actores y casos de uso, y en muchos casos operan como infraestructuras compartidas. Desde la perspectiva del desarrollo seguro, el software de las plataformas debe diseñarse de forma coherente con la arquitectura definida, evitando concentraciones excesivas de privilegios, dependencias implícitas entre componentes y exposiciones innecesarias de servicios. La seguridad en esta capa resulta determinante para preservar la integridad global del sistema, ya que cualquier compromiso puede tener efectos sistémicos sobre el conjunto de la solución IoT.

❖ Control de accesos y gestión de cuentas

El software de las plataformas deberá implementar **mecanismos robustos de autenticación y autorización**, diferenciando de forma clara los perfiles administrativos, operativos y de consulta. Los

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

accesos privilegiados deberán estar estrictamente **limitados** y sujetos a controles específicos, evitando configuraciones que otorguen permisos excesivos por defecto o accesos transversales no justificados.

Desde el desarrollo, deberán contemplarse aspectos como la gestión de sesiones, la caducidad y rotación de credenciales y la trazabilidad de las acciones relevantes realizadas por las personas usuarias y los servicios. En entornos urbanos con múltiples actores y responsabilidades compartidas, estas capacidades son esenciales para limitar el impacto de accesos indebidos y facilitar la supervisión y auditoría del sistema.

❖ Protección de interfaces e integraciones

Las **APIs y mecanismos de integración** con otros sistemas municipales o servicios externos deberán diseñarse bajo el **principio de mínima exposición**. Únicamente deberán habilitarse los endpoints y funcionalidades estrictamente necesarias para el funcionamiento de la solución, incorporando controles de autenticación, autorización y validación de entradas desde el diseño.

La correcta delimitación de responsabilidades entre sistemas, junto con una definición de los contratos de integración, reduce dependencias y evita que un incidente en un sistema se propague o amplifique a través de interfaces compartidas. Este aspecto es especialmente relevante en plataformas IoT que actúan como punto de convergencia de múltiples servicios urbanos.

❖ Gestión y protección de datos

El tratamiento de la información en las plataformas IoT deberá contemplar la **clasificación de los datos según su criticidad y uso previsto**, así como la aplicación de **controles de acceso** acordes a dicha clasificación. El software deberá evitar el almacenamiento de información innecesaria y garantizar que los datos se procesan, conservan y eliminan de forma coherente con los requisitos definidos en las fases de planificación y diseño.

Desde el desarrollo, deberán integrarse mecanismos que faciliten la aplicación consistente de políticas de protección de datos a lo largo de todo su ciclo de vida, reduciendo el riesgo de exposiciones indebidas, usos no previstos o acumulación de información sin valor operativo.

❖ Registro y supervisión de actividad

Las plataformas y aplicaciones deberán incorporar **mecanismos de registro** que permitan identificar **accesos**, **cambios de configuración** y **operaciones** relevantes sobre componentes y datos críticos. Estos registros deberán generarse de forma coherente entre los distintos servicios y conservarse de manera que posibiliten un análisis forense en caso de incidentes de seguridad.

La supervisión continua de eventos y comportamientos, integrada desde el diseño del software, facilita la detección temprana de actividades anómalas y refuerza la capacidad de respuesta ante incidentes, especialmente en plataformas que soportan servicios urbanos críticos y de alta disponibilidad.

❖ Escalabilidad y evolución controlada

Dado que las soluciones IoT en Smart Cities suelen crecer de forma progresiva en número de dispositivos, servicios e integraciones, el software de las plataformas deberá diseñarse para **permitir** la **ampliación de capacidades** sin alterar el modelo de seguridad establecido.

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

La incorporación de nuevos módulos, funcionalidades o integraciones deberá realizarse siguiendo los mismos principios, requisitos y criterios de seguridad definidos inicialmente, evitando introducir excepciones que degraden la coherencia del sistema o amplíen innecesariamente la superficie de ataque a lo largo del tiempo.

10.5. Gestión de dependencias y cadena de suministro

Las soluciones IoT incorporan habitualmente componentes desarrollados por terceros, incluyendo librerías de código abierto, frameworks, sistemas operativos embebidos, middleware, imágenes de contenedores y servicios externos. Estos elementos forman parte del software desplegado y, por tanto, influyen de forma directa en el nivel de seguridad de la solución. La falta de control sobre las dependencias puede introducir vulnerabilidades que no provienen del desarrollo propio, sino de la cadena de suministro tecnológica.

En el contexto de las Smart Cities, donde las soluciones IoT suelen tener una larga vida útil y desplegarse a gran escala, un incidente en la cadena de suministro puede replicarse de forma sistemática y afectar simultáneamente a un elevado número de dispositivos, plataformas y servicios. Desde la perspectiva del desarrollo seguro, la gestión de dependencias debe abordarse como un requisito dentro del ciclo de vida del software.

❖ Identificación e inventario de componentes

El desarrollo deberá contemplar la **identificación** y el **mantenimiento** de un **inventario** actualizado de **librerías, módulos y componentes externos** integrados en cada parte de la solución IoT. Este inventario deberá incluir información relevante como el origen del componente, su versión y su ámbito de uso dentro del sistema.

En soluciones IoT urbanas, donde pueden coexistir múltiples versiones de software en dispositivos, edge y plataformas, conocer con precisión qué dependencias están en uso resulta esencial para evaluar el impacto de vulnerabilidades publicadas, cambios en el soporte por parte de proveedores o la necesidad de aplicar actualizaciones de seguridad de forma selectiva.

❖ Evaluación de riesgos asociados

Antes de incorporar una dependencia al desarrollo, deberá **evaluarse** su **procedencia**, nivel de **mantenimiento**, **historial** de **vulnerabilidades** conocidas y **grado** de **adopción**. Esta evaluación permite reducir la probabilidad de integrar componentes obsoletos o con un soporte insuficiente, especialmente en soluciones IoT destinadas a operar durante largos periodos de tiempo.

Desde el desarrollo, esta valoración debe formar parte de las decisiones técnicas de diseño y arquitectura, y no limitarse a consideraciones funcionales o de conveniencia a corto plazo.

❖ Control de versiones y actualizaciones

Las dependencias deberán gestionarse de forma controlada, evitando actualizaciones automáticas no evaluadas en entornos críticos. Al mismo tiempo, deberá existir un **procedimiento** que permita aplicar **actualizaciones** cuando se identifiquen vulnerabilidades relevantes o riesgos significativos asociados a un componente.

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 soluciones IoT para Smart Cities, el proceso de actualización debe tener en cuenta las limitaciones de despliegue, la heterogeneidad de dispositivos y la posible imposibilidad de actualizar todos los activos de forma inmediata. Por ello, los cambios deberán evaluarse y validarse previamente, evitando efectos secundarios no previstos que puedan afectar a la estabilidad o seguridad del servicio.

❖ **Relación con proveedores y terceros**

Cuando la solución IoT dependa de proveedores externos para el mantenimiento, soporte o actualización de determinados componentes, deberán definirse de forma clara las responsabilidades en materia de seguridad. Esto incluye los tiempos de respuesta ante la **publicación de vulnerabilidades**, los **canales de comunicación** y las **obligaciones** de **notificación** de **incidencias** relevantes.

Esta coordinación resulta especialmente relevante en ecosistemas IoT urbanos, donde múltiples actores pueden compartir componentes o plataformas, y donde una vulnerabilidad en un elemento común puede tener impacto transversal sobre varios servicios municipales.

❖ **Reducción del riesgo estructural**

La **gestión sistemática de dependencias** contribuye a reducir riesgos estructurales derivados de la complejidad del ecosistema software IoT. La ausencia de este control puede generar situaciones en las que la organización desconozca qué componentes están expuestos a vulnerabilidades conocidas, dificultando la toma de decisiones informadas y la priorización de acciones correctivas.

Desde la perspectiva del desarrollo seguro, la visibilidad y el control sobre la cadena de suministro refuerzan la gobernanza del software y mejoran la capacidad de adaptación ante cambios en el entorno tecnológico y en el panorama de amenazas.

10.6. Pruebas y verificación de la seguridad del software

Las pruebas y actividades de verificación de la seguridad constituyen un elemento esencial para comprobar que los principios y requisitos definidos en fases anteriores del desarrollo se han implementado de forma efectiva. En soluciones IoT, donde intervienen múltiples componentes interconectados y distribuidos, la verificación no debe limitarse a un análisis puntual, sino integrarse como parte de un proceso estructurado y continuo que permita identificar vulnerabilidades antes de su explotación en entornos reales.

Desde la perspectiva del desarrollo seguro, las pruebas de seguridad no solo permiten detectar vulnerabilidades técnicas, sino también validar que el comportamiento del software es coherente con los niveles de riesgo asumidos y con la arquitectura de seguridad definida para la solución. En entornos urbanos, esta validación debe considerar además el impacto potencial sobre la continuidad del servicio y la posibilidad de que un fallo se replique a gran escala.

❖ **Verificación a lo largo del ciclo de vida**

Las **actividades de prueba y verificación** deberán integrarse en las **distintas fases del ciclo de vida** del software, evitando su realización exclusivamente en etapas finales previas al despliegue. La detección temprana de defectos de seguridad permite su corrección con menor un impacto técnico y económico, y reduce significativamente la probabilidad de que vulnerabilidades estructurales alcancen entornos de producción.

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 soluciones IoT, esta integración resulta especialmente relevante por la diversidad de componentes y por la dificultad de corregir fallos una vez desplegados en campo. Como evidencia de esta integración, deberán existir procedimientos documentados de pruebas, planificación de actividades de verificación por fase y registros que acrediten su ejecución antes de la puesta en producción y tras cambios relevantes en el sistema.

❖ Revisión de diseño e implementación

La verificación de la seguridad deberá incluir la **revisión de los requisitos de seguridad** definidos, la **coherencia del diseño** con la **arquitectura** establecida y la correcta **aplicación** de los **principios** descritos en el apartado 9.1. Estas revisiones permiten identificar vulnerabilidades de diseño que no siempre se manifiestan como fallos técnicos evidentes, especialmente en sistemas distribuidos donde los puntos críticos suelen encontrarse en los límites entre componentes y dominios de confianza.

Asimismo, deberán realizarse revisiones del código y comprobaciones orientadas a detectar errores de implementación, configuraciones inseguras o exposiciones indebidas de funcionalidades o datos. Deberán conservarse actas de revisión técnica, informes de análisis estático o dinámico cuando proceda, y trazabilidad entre los requisitos de seguridad y los controles implementados en el software.

❖ Pruebas funcionales de seguridad

Además de validar la funcionalidad del sistema, deberán ejecutarse **pruebas** específicas que permitan comprobar el **comportamiento del software** ante intentos de acceso no autorizado, entradas incorrectas, abusos de funcionalidades o situaciones imprevistas. Estas pruebas deben abarcar tanto **componentes individuales como la interacción entre ellos**, dado que muchas vulnerabilidades se manifiestan en los puntos de integración.

En entornos urbanos, también es relevante validar el comportamiento ante fallos parciales y escenarios de degradación controlada, siempre desde una perspectiva de seguridad. Los resultados deberán documentarse mediante informes detallados, registros de incidencias detectadas y evidencias de corrección, mitigación o aceptación formal del riesgo cuando corresponda.

❖ Evidencias y trazabilidad

Las actividades de prueba y verificación deberán **generar evidencias** que permitan demostrar que la seguridad ha sido evaluada de forma sistemática y repetible. Esta trazabilidad resulta fundamental para facilitar la supervisión, la auditoría y la toma de decisiones por parte de las personas responsables del sistema, especialmente en entornos urbanos donde la rendición de cuentas y la transparencia adquieren una relevancia especial.

Deberá existir un repositorio organizado de evidencias, vinculado a versiones concretas del software y a hitos de despliegue, que permita acreditar qué verificaciones se realizaron, en qué fase del ciclo de vida, con qué alcance y en qué condiciones.

❖ Limitaciones y riesgo residual

Las pruebas de seguridad no garantizan la ausencia total de vulnerabilidades, por este motivo, sus resultados deberán integrarse en un enfoque más amplio de gestión del riesgo, reconociendo la

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

existencia de riesgos residuales y complementando la verificación técnica con **medidas de supervisión**, **actualización** y **mantenimiento** continuo.

La aceptación de riesgos residuales deberá quedar debidamente documentada, incluyendo la justificación técnica correspondiente y, cuando proceda, la definición de medidas compensatorias orientadas a reducir su impacto y su probabilidad de explotación.

10.7. Gestión de vulnerabilidades y mantenimiento continuo

La seguridad del software IoT no finaliza con su despliegue en producción, dado que estas soluciones suelen operar durante largos periodos de tiempo y están expuestas a un entorno de amenazas en constante evolución, resulta imprescindible adoptar un enfoque continuo para la identificación, evaluación y mitigación de vulnerabilidades. La ausencia de una gestión estructurada puede convertir el paso del tiempo en un factor de riesgo acumulativo que afecte de forma progresiva a la resiliencia del sistema.

Los despliegues en los entornos urbanos son masivos y los servicios soportados pueden ser críticos, una vulnerabilidad no tratada puede replicarse en el ecosistema y afectar simultáneamente a un elevado número de activos. Además, las limitaciones de acceso físico a dispositivos y la coexistencia de múltiples proveedores hacen que la gestión de vulnerabilidades requiera planificación, coordinación y capacidad de ejecución sostenida

Desde la perspectiva del desarrollo seguro, la gestión de vulnerabilidades y el mantenimiento continuo deben considerarse una extensión natural del ciclo de vida del software, alineada con las decisiones de arquitectura, las prácticas de desarrollo y los mecanismos de verificación definidos en los apartados anteriores. Este enfoque debe permitir conocer el nivel de exposición del sistema en todo momento y actuar de forma proporcional al riesgo.

❖ Identificación y seguimiento de vulnerabilidades

Deben establecerse **mecanismos** que permitan **identificar vulnerabilidades** que afecten tanto al **software** desarrollado específicamente para la solución como a los **componentes de terceros** de los que depende. Esta identificación puede apoyarse en **fuentes públicas** de información, **comunicaciones** de **proveedores**, resultados de **pruebas internas** y **revisiones periódicas** de los sistemas.

En soluciones IoT urbanas es especialmente relevante mantener trazabilidad sobre qué activos y versiones están afectados, dado que puede existir heterogeneidad entre dispositivos, pasarelas y componentes de plataforma. Un seguimiento estructurado de las vulnerabilidades identificadas facilita la toma de decisiones informadas, evita que debilidades conocidas permanezcan sin tratamiento y permite mantener una visión actualizada del nivel de exposición al riesgo de la solución.

❖ Evaluación del impacto y priorización

No todas las vulnerabilidades presentan el mismo nivel de criticidad ni requieren la misma urgencia de actuación. Su **evaluación** debe considerar factores como el **tipo de servicio** afectado, el **alcance** potencial del incidente, la **probabilidad** de **explotación** y el **impacto** sobre la continuidad de los servicios urbanos.

La priorización debe incorporar además de número de activos afectados y la posibilidad de propagación entre dominios o servicios. Este análisis permite priorizar acciones correctivas de forma proporcional al riesgo, optimizando la asignación de recursos técnicos y evitando respuestas tardías ante vulnerabilidades relevantes.

❖ Gestión de actualizaciones y parches

La **aplicación de actualizaciones y parches de seguridad** constituye una de las principales medidas para reducir la exposición a vulnerabilidades conocidas. Este proceso deberá realizarse de forma controlada, garantizando que las correcciones aplicadas no introducen efectos no previstos ni comprometen la estabilidad del sistema o la continuidad del servicio.

En soluciones IoT con despliegues masivos y limitaciones de acceso físico, el mantenimiento requiere mecanismos que permitan planificar, validar y desplegar actualizaciones de manera coherente con la arquitectura y el ciclo de vida del software. Asimismo, deberá considerarse la necesidad de mantener una trazabilidad del estado de actualización del parque de activos y la gestión de situaciones en las que determinados componentes no puedan actualizarse de forma inmediata.

❖ Coordinación con proveedores y terceros

La participación de múltiples actores requiere una **coordinación** efectiva con **proveedores externos** y **terceros** para la gestión de vulnerabilidades. Deben definirse responsabilidades claras en materia de seguridad, establecer **canales** de **comunicación** adecuados y acordar **tiempos** de **respuesta** alineados con la criticidad de los servicios soportados.

Esta coordinación resulta especialmente relevante cuando las vulnerabilidades afectan a componentes compartidos o a elementos fuera del control directo del equipo de desarrollo, ya que la capacidad de respuesta dependerá en parte del soporte y las actualizaciones proporcionadas por dichos terceros.

❖ Gestión del riesgo residual y mejora continua

La corrección inmediata de una vulnerabilidad puede no resultar viable en determinados escenarios por razones técnicas, operativas o por el impacto potencial sobre el servicio. En estos casos, el **riesgo residual** deberá gestionarse de forma consciente, documentada y aprobada, adoptando **medidas compensatorias** cuando proceda y definiendo un **plan de tratamiento** con responsables y plazos.

La información derivada de incidentes, revisiones periódicas y lecciones aprendidas deberá integrarse en procesos de mejora continua, permitiendo ajustar prácticas de desarrollo, verificación y operación para reducir la probabilidad y el impacto de futuros incidentes.

11. Herramientas de análisis de vulnerabilidades

La integración de herramientas de análisis en el proceso de desarrollo de software IoT constituye un elemento esencial para detectar vulnerabilidades de forma temprana, reducir los costes operativos asociados a su corrección y mejorar la calidad y resiliencia de las soluciones desplegadas.

Estas herramientas permiten automatizar actividades de verificación que, de otro modo, dependerían exclusivamente de revisiones manuales o pruebas puntuales. No sustituyen al análisis técnico ni a las

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

pruebas de seguridad descritas en capítulos anteriores, sino que los complementan, proporcionando visibilidad continua sobre el estado de seguridad del software a lo largo de todo su ciclo de vida.

11.1. Herramientas SCA

Las herramientas de Software Composition Analysis (SCA) permiten **identificar**, **inventariar** y **analizar** los **componentes de terceros** utilizados en una solución software, como librerías, frameworks, paquetes, imágenes de contenedores y componentes embebidos, incluyendo firmware cuando resulte de aplicación. Su objetivo es reducir el riesgo asociado a la cadena de suministro, detectando vulnerabilidades conocidas y proporcionando visibilidad sobre qué componentes y versiones forman parte de cada entrega.

En soluciones IoT para entornos urbanos, donde el uso de componentes de terceros es habitual y los despliegues suelen tener una larga vida útil, SCA es especialmente relevante para evitar que vulnerabilidades conocidas permanezcan sin tratamiento durante años, y para permitir respuesta rápida ante nuevas vulnerabilidades identificadas por el CVE que afecten a dependencias ya desplegadas.

Estas herramientas deberán permitir, como mínimo:

- Identificar de forma automática dependencias utilizadas en cada versión del software.
- Detectar vulnerabilidades conocidas asociadas a componentes de terceros y asociarlas a versiones concretas.
- Generar y mantener inventarios actualizados de componentes (SBOM) por versión y por componente del sistema.
- Evaluar el estado de soporte y obsolescencia de dependencias críticas, identificando componentes obsoletos o fuera de soporte.
- Facilitar la priorización del tratamiento en función de criticidad, como entre un componente expuesto y uno interno, o por el impacto en un servicio urbano.

Las herramientas SCA deberán integrarse de forma temprana en el proceso de desarrollo y mantenerse activas durante todo el ciclo de vida del software. Su ejecución será obligatoria cuando se incorporen nuevas dependencias o se introduzcan nuevos componentes de terceros.

11.2. Herramientas SAST

Las herramientas de Static Application Security Testing (SAST) **analizan** el **código fuente**, bytecode o binarios **sin necesidad de ejecutar la aplicación**, con el objetivo de identificar patrones de programación inseguros, errores de implementación y vulnerabilidades potenciales.

En el desarrollo de soluciones IoT, estas herramientas resultan aplicables tanto al software embebido como a componentes de las plataformas, servicios backend, APIs e interfaces de acceso. Su valor es máximo cuando se utilizan para detectar fallos de forma temprana, antes de que se desplieguen en producción.

Estas herramientas deberán permitir, como mínimo:

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

- Detectar vulnerabilidades en fases tempranas del desarrollo, antes de su integración en el sistema.
- Identificar errores de codificación asociados a validación de entradas, gestión de errores, autenticación, autorización y control de accesos.
- Verificar el cumplimiento de los estándares y buenas prácticas de desarrollo seguro definidos por la organización.
- Permitir la gestión de falsos positivos mediante mecanismos de justificación y revisión.

Las herramientas SAST deberán utilizarse de forma recurrente durante la fase de desarrollo, integrándose en los flujos de trabajo de los equipos técnicos. Su ejecución será un **requisito** necesario para autorizar el **paso a producción** de nuevos desarrollos o evolutivos.

11.3. Herramientas DAST

Las herramientas de Dynamic Application Security Testing (DAST) evalúan la seguridad del software en ejecución, analizando el comportamiento de aplicaciones, servicios y APIs desde la perspectiva de un atacante externo. Complementan el análisis estático permitiendo identificar vulnerabilidades explotables durante la ejecución, configuraciones inseguras y exposiciones reales de interfaces.

En soluciones IoT para Smart Cities, estas herramientas son especialmente relevantes para validar la seguridad de plataformas de gestión, interfaces web, APIs expuestas y aplicaciones móviles, así como para comprobar que la exposición real en un entorno similar a producción es consistente con el diseño y la arquitectura definidos.

Estas herramientas deberán permitir, como mínimo:

- Identificar vulnerabilidades explotables en aplicaciones y servicios en ejecución.
- Evaluar la exposición real de interfaces y APIs.
- Detectar configuraciones inseguras o errores de implementación visibles en tiempo de ejecución.
- Complementar los análisis estáticos mediante pruebas dinámicas centradas en el comportamiento del sistema.

Las herramientas DAST deberán utilizarse únicamente sobre soluciones que ya se encuentran desplegadas, realizando las pruebas sobre entornos controlados que reproduzcan el entorno de producción o, adicionalmente en el propio entorno de producción solo cuando sea viable y controlado sin afectar a la disponibilidad del servicio.

11.4. Condiciones para paso a producción

La puesta en producción de una nueva versión o evolutivo de la solución IoT deberá estar condicionada a criterios objetivos que permitan controlar el riesgo de forma consistente. Estos criterios se aplicarán a los resultados de los análisis de seguridad realizados sobre el software y sus dependencias, incluyendo

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

SCA, SAST y DAST, y deberán ajustarse a la criticidad del componente afectado y del servicio urbano soportado.

A efectos de este apartado, se utilizará el CVSS como referencia para clasificar las vulnerabilidades, considerando los siguientes rangos de severidad:

- **Crítica**: CVSS 9.0–10.0
- **Alta**: CVSS 7.0–8.9
- **Media**: CVSS 4.0–6.9
- **Baja**: CVSS 0.1–3.9

Asimismo, se establecen tres categorías de criticidad de componente, que deberán definirse según el contexto de cada entidad:

- **C1 – Crítico**: componentes expuestos o con funciones de control/administración cuyo compromiso puede afectar directamente a la integridad, disponibilidad o control de un servicio urbano esencial. Incluye APIs públicas, paneles de operación/administración, componentes de control en el borde y servicios que ejecutan acciones sobre actuadores o configuraciones críticas.
- **C2 – Importante**: componentes no expuestos directamente a Internet, pero que procesan datos sensibles o soportan funciones relevantes para la operación. Su compromiso puede tener impacto significativo, aunque normalmente requiere acceso previo a redes internas o a otros componentes. Incluye servicios internos de las plataformas, módulos de gestión de dispositivos, bases de datos operativas o integraciones internas con sistemas municipales.
- **C3 – No crítico**: componentes auxiliares o de bajo impacto, sin exposición directa y sin funciones críticas ni tratamiento de datos sensibles. Su compromiso tiene impacto limitado y no permite, por sí mismo, afectar a servicios esenciales. Incluye procesos de soporte no críticos, utilidades internas o componentes de baja relevancia operativa.

11.4.1. Criterios generales de no aprobación

No se autorizará el paso a producción de una nueva versión o evolutivo cuando se cumpla cualquiera de las siguientes condiciones:

- Existencia de vulnerabilidades críticas abiertas en la solución analizada, salvo que exista una excepción formal documentada, aprobada conforme al procedimiento definido en este apartado.
- Existencia de vulnerabilidades explotables que permitan alguno de los siguientes escenarios, con independencia del número total de hallazgos o de su severidad agregada:
    - Bypass de mecanismos de autenticación o autorización.
    - Exposición de secretos, credenciales o material sensible de seguridad.
    - Ejecución remota de código o comandos no autorizados.
    - Acceso no autorizado a datos críticos o sensibles del sistema o del servicio urbano.

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

- Ausencia de trazabilidad entre los resultados de los análisis de seguridad realizados, la versión que se pretende desplegar y el tratamiento asignado a cada hallazgo, ya sea corrección, mitigación o aceptación formal del riesgo, de modo que no sea posible justificar de forma verificable la decisión de despliegue.

11.4.2. Umbrales de aceptación

Los umbrales se aplican a la versión de la solución analizada y deberán medirse sobre el conjunto de hallazgos confirmados y no mitigados.

❖ Análisis SCA

Los umbrales de SCA deberán considerar, además de la severidad de la vulnerabilidad, la capacidad de explotación y la existencia de corrección disponible.

	Criticidad componente		
Severidad	**C1 – Crítico**	**C2 – Importante**	**C3 – No crítico**
Crítica	0	0	0
Alta	0	≤ 1	≤ 2
Media	≤ 5	≤ 7	≤ 10
Baja	≤ 10	≤ 15	No bloqueante

TABLA 2: UMBRALES DE ACEPTACIÓN SCA.

❖ Análisis SAST

Aplicable a código fuente, bytecode o binarios de componentes desarrollados o mantenidos por la solución

	Criticidad componente		
Severidad	**C1 – Crítico**	**C2 – Importante**	**C3 – No crítico**
Crítica	0	0	0
Alta	≤ 1	≤ 3	≤ 5
Media	≤ 5	≤ 5	≤ 10
Baja	≤ 10	≤ 10	No bloqueante

TABLA 3: UMBRALES DE ACEPTACIÓN SAST.

❖ Análisis DAST

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

Aplicable a plataformas, servicios y APIs en ejecución. Se ejecutará en entornos controlados equivalentes a producción o, cuando proceda, en producción bajo control.

	Criticidad componente		
Severidad	**C1 – Crítico**	**C2 – Importante**	**C3 – No crítico**
Crítica	0	0	0
Alta	0	≤ 1	≤ 3
Media	≤ 3	≤ 5	≤ 10
Baja	≤ 10	≤ 10	No bloqueante

TABLA 4: UMBRALES DE ACEPTACIÓN DAST.

Los umbrales de aceptación establecidos constituyen valores propuestos para homogeneizar criterios de autorización del despliegue y facilitar la evaluación objetiva previa al paso a producción. Dichos umbrales podrán adaptarse por cada entidad de acuerdo con su análisis de riesgos, la criticidad del servicio urbano, la exposición del componente y las restricciones operativas del despliegue IoT.

No obstante, con independencia de los umbrales aplicables, todo hallazgo identificado deberá ser objeto de gestión y seguimiento, incluyendo registro en el sistema de seguimiento de vulnerabilidades, asignación de persona responsable, clasificación de severidad, decisión de tratamiento y definición de un plan y plazos de resolución.

La decisión final de despliegue deberá mantener trazabilidad entre los resultados del análisis, la versión candidata y el tratamiento asignado a cada hallazgo.

11.4.3. Gestión de excepciones y riesgo residual

Cuando no sea viable corregir una vulnerabilidad antes de la puesta en producción por razones técnicas u operativas, deberá aplicarse un proceso formal de excepción. La excepción solo podrá aprobarse si se cumplen todas las condiciones siguientes:

- Justificación técnica del riesgo residual, incluyendo el impacto, probabilidad, componente afectado y motivo de no corrección inmediata.
- Medidas compensatorias definidas y aplicadas cuando proceda, como limitación de exposición, controles adicionales o monitorización reforzada.
- Aprobación explícita por la persona responsable designada, ya sea las persona propietaria del servicio o una persona responsable de la entidad.
- Fecha límite de corrección y registro de seguimiento hasta cierre.

12. Checklist técnica de paso a producción

La presente checklist técnica tiene como objetivo verificar, de forma operativa y previa al despliegue, que una versión de la solución IoT cumple las condiciones mínimas de seguridad necesarias para su puesta en producción. Está orientada a su uso por equipos técnicos y de operación, y se aplica por versión candidata, teniendo en cuenta la criticidad del componente y los resultados de los análisis de seguridad realizados.

Dominio	Controles
Gestión de identidades y accesos	• No existen credenciales por defecto activas en dispositivos/pasarelas (muestra representativa). • No existen credenciales compartidas en componentes críticos. • Roles y permisos revisados y configurados conforme a mínimo privilegio. • Accesos privilegiados limitados y trazables (registro de acciones).
APIs e interfaces	• Inventario de APIs/endpoints actualizado. • Mínimos endpoints expuestos y justificados. • Autenticación y autorización verificadas en endpoints críticos (incluye prueba de acceso indebido). • Validación de entradas implementada en endpoints críticos (pruebas con inputs malformados/fuera de rango).
Cadena de suministro	• SBOM generada y asociada a la versión. • Dependencias críticas revisadas (soporte/obsolescencia). • No existen vulnerabilidades críticas explotables en dependencias (o están mitigadas/aceptadas formalmente). • Excepciones de SCA documentadas y aprobadas cuando aplique.
Análisis de código	• SAST ejecutado sobre la versión candidata. • Hallazgos críticos = 0 y umbrales cumplidos según criticidad (C1/C2/C3).

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

Dominio	Controles
	• Falsos positivos revisados y justificados de forma trazable. • Secretos no presentes en repositorios/artefactos de despliegue.
Análisis dinámico	• DAST ejecutado sobre entorno equivalente a producción (o producción bajo control). • Hallazgos críticos = 0 y umbrales cumplidos según criticidad (C1/C2/C3). • Endpoints no previstos/no inventariados revisados y cerrados o justificados
Monitorización	• Logs mínimos activos: accesos, cambios de configuración y operaciones críticas. • Trazabilidad por versión/entorno en logs (o mecanismo equivalente). • Alertas mínimas configuradas para eventos críticos (si aplica al servicio).
Gestión de excepciones	• Riesgos residuales aprobados formalmente cuando existan. • Medidas compensatorias definidas y verificadas cuando proceda. • Plan de tratamiento definido con fecha límite y seguimiento.

TABLA 5: CHECKLIST TÉCNICA DE PASO A PRODUCCIÓN.

13. Checklist de cumplimiento y auditoría

La presente checklist de cumplimiento tiene como finalidad evaluar, desde una perspectiva global, el grado de alineación de la solución IoT con los principios, controles y buenas prácticas de seguridad descritos en esta guía a lo largo de todo su ciclo de vida. Está orientada a procesos de revisión, auditoría y gobernanza, y no se limita a una versión concreta del software.

A diferencia de la checklist técnica de paso a producción, esta checklist consolida evidencias a nivel de arquitectura, desarrollo, operación y gestión, permitiendo verificar la aplicación sistemática de los criterios de seguridad definidos y facilitando su uso como apoyo a auditorías internas, revisiones de cumplimiento o procesos de contratación y supervisión. Ambas checklists son complementarias y deben utilizarse de forma coordinada.

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

Dominio	Control	Condición de cumplimiento	Evidencias
Gobernanza y gestión del riesgo	Requisitos de seguridad	Existen requisitos de seguridad documentados desde fases iniciales del desarrollo de la solución y están asociados a controles.	• Documento de requisitos de seguridad. • Matriz de requisitos – controles.
	Enfoque basado en riesgos	Se aplica un enfoque basado en riesgos proporcional a la criticidad del servicio asociado y se revisan periódicamente los riesgos identificados.	• Análisis de riesgos actualizado. • Evidencias de revisiones periódicas y decisiones de tratamiento o aceptación.
Arquitectura y diseño seguro	Arquitectura segmentada	Existe una arquitectura con separación entre capas, dominios y niveles de confianza.	• Diagrama de arquitectura. • Esquema de segmentación de red o equivalente.
	Aislamiento de componentes críticos	Los componentes críticos están segregados para limitar la propagación de incidentes y reducir dependencias innecesarias.	• Documento de diseño que identifique componentes críticos y dependencias. • Evidencia de segregación (zonas, VLAN, políticas).
	Reducción de superficie de exposición	Solo se exponen servicios e interfaces estrictamente necesarias para la operación.	• Inventario de servicios/puertos expuestos.
Dispositivos y componentes de borde	Identidad única del dispositivo	Cada dispositivo dispone de una identidad individual y verificable dentro del sistema, no existen identidades compartidas en componentes críticos.	• Inventario de dispositivos. • Evidencias de autenticación individual.

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

Dominio	Control	Condición de cumplimiento	Evidencias
	Configuración segura por defecto	Los dispositivos se despliegan con configuraciones seguras y sin credenciales por defecto.	• Guía de hardening aplicada. • Evidencia de eliminación/cambio de credenciales por defecto.
	Actualización segura del software	Existe un proceso de actualización controlado que verifica la autenticidad e integridad del firmware/software y mantiene trazabilidad de versiones.	• Procedimiento de gestión de vulnerabilidades y parches. • Registro de actualizaciones.
Plataformas, interfaces y aplicaciones	Control de accesos y privilegios	Existen mecanismos de autenticación y autorización acordes a los perfiles definidos y se aplica mínimo privilegio.	• Matriz de roles y permisos. • Evidencia de configuración de perfiles en la plataforma. • Registro de accesos privilegiados.
	Protección de interfaces y APIs	Las APIs e interfaces están autenticadas y autorizadas, y limitadas a los servicios necesarios.	• Inventario de APIs. • Políticas de seguridad APIs.
	Registro y trazabilidad de actividad	Se generan y conservan registros de accesos y operaciones relevantes sobre componentes y datos críticos.	• Política/procedimiento de gestión de registros de logs y auditoría. • Ejemplos de logs de acceso/cambio. • Repositorio de logs.
Desarrollo seguro y cadena de suministro	Principios de desarrollo seguro aplicados	El desarrollo aplica principios de mínimo privilegio, separación de funciones y seguridad por defecto.	• Especificaciones de diseño y criterios de seguridad. • Revisiones técnicas documentadas (diseño/código).

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

Dominio	Control	Condición de cumplimiento	Evidencias
	Gestión de dependencias	Se dispone de inventario y control de versiones de componentes de terceros integrados en la solución.	• SBOM o inventario de dependencias. • Registro de versiones.
	Evaluación de proveedores	Existen requisitos de seguridad definidos contractualmente para proveedores y terceros, incluyendo soporte y notificación de vulnerabilidades.	• Cláusulas de seguridad en contratos. • SLA/Acuerdos con requisitos de ciberseguridad. • Evaluaciones del riesgo proveedores.
Verificación, vulnerabilidades y mantenimiento	Pruebas de seguridad realizadas	Se han realizado pruebas de seguridad antes de la puesta en producción y tras cambios relevantes.	• Informes de pruebas. • Evidencias de validación y cierre de hallazgos.
	Gestión de vulnerabilidades	Existe un procedimiento estructurado para identificar, evaluar, priorizar y hacer seguimiento de vulnerabilidades.	• Procedimiento documentado. • Registro de vulnerabilidades y estado.
	Gestión de parches y mantenimiento continuo	Las actualizaciones de seguridad se aplican de forma controlada y con trazabilidad de versiones.	• Historial de versiones. • Registros de actualización.

TABLA 6: CHECKLIST DE CUMPLIMIENTO Y AUDITORÍA.

14. Conclusiones

Las soluciones IoT desplegadas en las Smart Cities soportan servicios urbanos cada vez más críticos, interconectados y expuestos, lo que convierte la ciberseguridad en un requisito estructural y no en un elemento accesorio. La experiencia demuestra que los incidentes más graves no suelen derivarse de fallos puntuales, sino de debilidades acumuladas en el diseño, desarrollo y operación de los sistemas.

Esta guía ha abordado la seguridad de las soluciones IoT desde una perspectiva integral, incorporando principios de seguridad desde el diseño, criterios de arquitectura segura, prácticas de desarrollo de software, mecanismos de verificación y herramientas de apoyo a la operación. El objetivo no es imponer soluciones concretas, sino proporcionar un marco coherente que permita reducir riesgos de forma sistemática y sostenible.

La adopción de un enfoque basado en el ciclo de vida resulta especialmente relevante en las Smart Cities, donde los sistemas IoT tienen una larga vida útil y evolucionan mediante integraciones, ampliaciones y cambios operativos. La seguridad debe mantenerse de forma continua, apoyándose en procesos, herramientas y responsabilidades claramente definidas.

Finalmente, esta guía debe entenderse como un marco de referencia práctico, adaptable a distintos contextos y niveles de madurez, y complementario a los estándares y normativas aplicables. Su aplicación contribuye a mejorar la resiliencia de los servicios urbanos, la confianza en las soluciones IoT y la capacidad de las organizaciones para gestionar los riesgos de ciberseguridad de forma proactiva.

15. Referencias y enlaces a información adicional

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

2. Centro Criptológico Nacional (CCN-CERT). (2023). *Buenas Prácticas BP/28 Recomendaciones sobre desarrollo seguro*. https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/6834-ccn-cert-bp-28-recomendaciones-sobre-desarrollo-seguro/file?format=html

3. Cloud Security Alliance (CSA). (2021). *CSA IoT Security Controls Framework v2*. https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2

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

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*.

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

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

6. European Union Agency for Cybersecurity. (2021). *Guidelines for Securing the Internet of Things*. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

7. European Union Agency for Cybersecurity. (2019). *Good Practices for Security of IoT - Secure Software Development Lifecycle*. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

8. European Telecommunications Standards Institute (ETSI). (2024). *ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.* https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

9. Instituto Nacional de Ciberseguridad (INCIBE). (2024). *Cómo construir software seguro para mi start-up*. https://www.incibe.es/emprendimiento/publicaciones/guias-y-estudios/estudios/como-construir-software-seguro-para-mi-startup

10. Instituto Nacional de Ciberseguridad (INCIBE). (2024). *Buenas prácticas de desarrollo seguro en control industrial.* https://www.incibe.es/incibe-cert/blog/buenas-practicas-de-desarrollo-seguro-en-control-industrial

11. 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

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

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

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

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

15. ISMS Forum. (2025). *DevSecOps: guía de seguridad integrada desde el diseño y por defecto*. https://www.ismsforum.es/ficheros/descargas/iiedicionguiadevsecopsv1746557372.pdf

16. ISMS Forum. (2023). *Guía de iniciación en la Seguridad aplicada al DevOps*. https://www.ismsforum.es/ficheros/descargas/guia-devsecops-v41690197585.pdf

17. National Institute of Standards and Technology (NIST). (2021). *NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. https://csrc.nist.gov/pubs/sp/800/213/final

18. National Institute of Standards and Technology (NIST). (2020). *NIST IR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers*. https://csrc.nist.gov/pubs/ir/8259/final

19. Open Worldwide Application Security Project (OWASP). *OWASP Mobile Application Security Verification Standard (MASVS)*. https://mas.owasp.org/MASVS/

20. Open Worldwide Application Security Project (OWASP). *OWASP Application Security Verification Standard (ASVS)*. https://owasp.org/www-project-application-security-verification-standard/

21. Open Worldwide Application Security Project (OWASP). (2018). *OWASP Internet of Things Project*. https://owasp.org/www-project-internet-of-things/

16. 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.

16.1. Lista de materias tratadas en la guía

- Ecosistema IoT en Smart Cities
- OWASP IoT Top 10
- Arquitectura segura de soluciones IoT
- Principios generales de desarrollo seguro IoT
- Ciclo de vida del software 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

- Desarrollo seguro de software IoT
- Herramientas de análisis de vulnerabilidades
- Checklist de cumplimiento en desarrollo seguro

16.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

16.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Desarrollo Seguro de Soluciones IoT en Smart Cities

Febrero de 2026

Versión 1.0

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