

Uso responsable y seguro de sistemas de IA en Smart Cities para usuarios finales

Noviembre de 2025

Versión 1.0



Junta de Andalucía

Objeto del Expediente:

**“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IA PARA ENTORNOS DE SMART CITIES Y SALUD”
(CONTR 2024 829535).**

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

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 11/11/2025

Fecha de última actualización: 9/12/2025

ÍNDICE DE CONTENIDOS

1.	Introducción.....	6
2.	Objetivo y alcance.....	7
2.1.	Objetivo	7
2.2.	Alcance.....	7
3.	Referencias normativas.....	8
4.	Definiciones	11
5.	Sistemas de IA en los Smart Cities	13
5.1.	Funcionamiento general y tipos de sistemas de IA utilizados en Smart Cities.....	13
5.2.	Ámbitos de uso de la IA en Smart Cities y recomendaciones específicas	15
5.2.1.	Movilidad inteligente y transporte	15
5.2.2.	Energía, agua y medio ambiente urbano.....	16
5.2.3.	Seguridad urbana y gestión de emergencias.....	16
5.2.4.	Atención ciudadana digital y tramitación administrativa.....	17
5.2.5.	Participación ciudadana digital y plataformas municipales.....	17
5.2.6.	Turismo inteligente y servicios culturales digitales	17
6.	Riesgos y desafíos de la IA en Smart Cities para la ciudadanía.....	19
6.1.	Complejidad y falta de visibilidad del ecosistema urbano digital	19
6.2.	Privacidad y el uso intensivo de datos personales	20
6.3.	Seguridad digital y exposición a incidentes.....	21
6.4.	Riesgos derivados del funcionamiento de la IA	21
6.5.	Desinformación, manipulación digital y contenidos sintéticos	22
6.6.	Accesibilidad, inclusión y brecha digital	23
6.7.	Impacto en la experiencia ciudadana	23
7.	Principios de IA de uso responsable y seguro en Smart Cities.....	25
7.1.	Respeto y garantía de los derechos fundamentales.....	25
7.2.	Gestión del riesgo y calidad de los sistemas de IA	25
7.3.	Privacidad y protección de datos personales	26
7.4.	Transparencia, trazabilidad y explicabilidad de los sistemas	26
7.5.	Ciberseguridad orientada al usuario final.....	26
7.6.	Equidad, accesibilidad universal e inclusión	27
7.7.	Supervisión y control humano significativo.....	27
7.8.	Responsabilidad institucional y rendición de cuentas	27

7.9.	Sostenibilidad social y ambiental y fomento de la confianza pública	27
8.	Interacción segura con sistemas de IA urbanos	28
8.1.	Identificación de servicios y aplicaciones que utilizan IA	28
8.1.1.	Identificación de asistentes virtuales y modelos conversacionales	29
8.2.	Comprensión de avisos, permisos y condiciones de uso	30
8.2.1.	Comprensión de la toma de decisiones automatizadas	31
8.3.	Buenas prácticas en el uso seguro de la IA.....	31
8.3.1.	Interacción segura con asistentes virtuales.....	32
8.4.	Detección de señales de alerta y actuación ante incidencias	33
8.5.	Casos prácticos.....	34
9.	Medidas de autoprotección del usuario final	37
9.1.	Protección de la privacidad y de la información personal	37
9.2.	Seguridad digital y prevención del fraude	37
9.3.	Identificación de posibles sesgos o decisiones inapropiadas	38
9.4.	Verificación de contenidos sintéticos y prevención de la desinformación.....	38
9.5.	Accesibilidad y reducción de barreras digitales.....	39
10.	Derechos y garantías de la ciudadanía en el uso de sistemas de IA en Smart Cities	40
10.1.	Derechos derivados del RGPD y la LOPDGDD.....	40
10.2.	Garantías en el marco del Reglamento Europeo de Inteligencia Artificial (RIA).....	40
10.3.	Garantías en materia de ciberseguridad (NIS2 y ENS)	42
10.3.1.	Garantías derivadas del Esquema Nacional de Seguridad (ENS)	42
10.3.2.	Garantías derivadas de la Directiva NIS2.....	42
10.4.	Canales para ejercer derechos.....	43
11.	Referencias.....	45
12.	Otras referencias de interés	47
12.1.	Lista de materias tratadas en la guía.....	47
12.2.	Lista de productos mencionados en la guía.....	47
12.3.	Lista de servicios mencionados en la guía	47

ÍNDICE DE TABLAS

Tabla 1: Definiciones empleadas.	12
Tabla 2: Escenarios habituales en los que interviene IA	29
Tabla 3: Señales de que una respuesta proviene de IA	30
Tabla 4: Ejemplos de permisos y su implicación	31
Tabla 5: Ejemplos de uso seguro en situaciones comunes	32
Tabla 6: Interacciones que requieren precaución	33
Tabla 7: Escenarios de alerta y posible interpretación	33

1. Introducción

La integración de sistemas de Inteligencia Artificial (IA) en los servicios públicos urbanos representa un cambio estructural en la forma en que las ciudades gestionan sus recursos, planifican sus procesos y atienden a la ciudadanía. Estos sistemas contribuyen a optimizar operaciones en ámbitos como la movilidad, la energía, la gestión ambiental, la seguridad y la atención ciudadana, permitiendo analizar datos en tiempo real, automatizar tareas y apoyar decisiones administrativas con mayor precisión.

Este avance tecnológico, si bien ofrece beneficios contrastados, introduce también nuevos desafíos relacionados con la transparencia, la protección de datos personales, la supervisión humana, la calidad de los modelos y la seguridad digital. La complejidad inherente a los sistemas basados en IA puede dificultar su comprensión por parte de la ciudadanía, especialmente cuando operan de manera integrada en infraestructuras urbanas o en procesos administrativos no visibles para el usuario final.

Con el fin de garantizar un uso adecuado, seguro y respetuoso con los derechos fundamentales, la Unión Europea ha establecido un marco normativo robusto encabezado por el Reglamento (UE) 2024/1689, conocido como AI Act, que regula el desarrollo, despliegue y utilización de sistemas de IA. Este marco se complementa con el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), que regulan el tratamiento de datos personales, y con los requisitos de seguridad y resiliencia establecidos en la Directiva (UE) 2022/2555 (NIS2) y el Esquema Nacional de Seguridad (ENS), aplicables a las administraciones públicas y a sus proveedores tecnológicos.

Asimismo, normas internacionales como ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 27001, así como normas UNE del marco de Smart City (UNE 178104, UNE 178108, UNE 178301), proporcionan criterios técnicos que orientan la gobernanza, la gestión del riesgo, la calidad del dato y la seguridad en sistemas que integran IA.

En este contexto, resulta necesario disponer de una guía dirigida a la ciudadanía que facilite la comprensión del funcionamiento de los sistemas de IA presentes en el entorno urbano, identificar posibles riesgos, actuar de forma segura y ejercer sus derechos con claridad.

Esta guía no sustituye a la normativa aplicable ni a los procedimientos administrativos vigentes, sino que tiene carácter informativo y orientativo para facilitar una comprensión general del uso de la inteligencia artificial en los servicios urbanos.

2. Objetivo y alcance

2.1. Objetivo

La presente guía tiene como finalidad ofrecer a la ciudadanía un marco claro, accesible y práctico para comprender y utilizar de manera segura los servicios urbanos que incorporan Inteligencia Artificial. A través de criterios operativos, recomendaciones y explicaciones adaptadas al ámbito municipal, la guía busca:

- Facilitar la comprensión del papel de la IA en los diferentes servicios públicos urbanos y su influencia en la vida cotidiana.
- Proporcionar información clara sobre los riesgos y desafíos asociados al uso de tecnologías automatizadas en entornos de Smart Cities, incluyendo aspectos de privacidad, seguridad digital, transparencia, accesibilidad y fiabilidad de los sistemas.
- Promover un uso responsable, informado y seguro de las aplicaciones y plataformas municipales que integran IA, reforzando la autonomía de la ciudadanía.
- Garantizar que la ciudadanía conozca sus derechos en relación con el tratamiento de datos personales y la toma de decisiones automatizadas, así como las vías para ejercerlos eficazmente.
- Aclarar las obligaciones de las administraciones públicas y de sus proveedores tecnológicos, con arreglo al marco regulatorio europeo, nacional y municipal vigente.
- Contribuir a generar confianza pública en el despliegue de la IA en las ciudades mediante la divulgación de información rigurosa, comprensible y alineada con los principios de transparencia, seguridad y respeto a los derechos fundamentales.

En conjunto, la guía pretende fortalecer la capacidad de la ciudadanía para interactuar de forma consciente, crítica y segura con los servicios inteligentes de la ciudad, garantizando un uso adecuado y responsable de las tecnologías basadas en IA en el entorno urbano.

2.2. Alcance

Este documento se dirige a la ciudadanía que utiliza servicios municipales o plataformas digitales vinculadas al entorno urbano que emplean funciones basadas en IA. Las recomendaciones son aplicables a ámbitos como la movilidad inteligente, la atención ciudadana automatizada, la supervisión ambiental, la gestión energética, la información urbana en tiempo real, la seguridad y otros servicios propios de una Smart City.

La guía se centra en el uso desde la perspectiva del usuario final, sin entrar en aspectos de diseño, desarrollo o certificación técnica de los sistemas. Complementa las obligaciones legales y las políticas municipales ya existentes, y resulta aplicable independientemente de que el servicio se preste directamente por la administración o por entidades públicas y privadas que operan en el ecosistema urbano. Su alcance incluye servicios en funcionamiento y aquellos de futura implantación, siempre que supongan interacción con la ciudadanía.

3. Referencias normativas

Las referencias incluidas en este apartado se presentan con carácter informativo y orientativo, con el fin de ofrecer a la ciudadanía un contexto general sobre los marcos normativos y técnicos que regulan el uso de la inteligencia artificial en los servicios urbanos. Su inclusión no implica que la persona usuaria deba conocer o aplicar directamente estas normas, sino comprender que los servicios municipales basados en IA están sujetos a obligaciones legales, técnicas y de seguridad específicas.

- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, Reglamento de Inteligencia Artificial (RIA):** Establece un marco jurídico armonizado para el desarrollo y uso de sistemas de inteligencia artificial en la Unión Europea. Introduce un enfoque basado en el riesgo y obligaciones específicas para los sistemas de alto riesgo, incluidos los empleados en la seguridad pública y gestión de infraestructuras urbanas críticas. Refuerza los principios de transparencia, trazabilidad, supervisión humana y rendición de cuentas.
- **Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD):** Garantiza la protección de las personas físicas en lo relativo al tratamiento de datos personales. Resulta directamente aplicable al tratamiento automatizado de datos mediante inteligencia artificial, especialmente cuando involucra datos biométricos, de imagen o de voz.
- **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Desarrolla y complementa el RGPD en el ordenamiento español, incorporando derechos digitales y estableciendo obligaciones de transparencia, supervisión y rendición de cuentas aplicables también a sistemas basados en inteligencia artificial.
- **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, Directiva NIS2:** Refuerza las medidas para garantizar un nivel elevado de ciberseguridad en la Unión Europea. Afecta a entidades esenciales e importantes, incluidas administraciones públicas, servicios sanitarios, operadores de infraestructuras críticas y proveedores tecnológicos que prestan servicios relacionados con las Smart Cities.
- **Esquema Nacional de Seguridad (ENS):** Define los principios y requisitos mínimos de seguridad aplicables a los sistemas de información del sector público español y de los proveedores tecnológicos. Es fundamental para garantizar la protección de la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información procesada por sistemas de IA utilizados en el sector público.
- **Data Governance Act, Reglamento (UE) 2022/868:** Regula la gobernanza y la reutilización segura de datos en la Unión Europea, fomentando el intercambio seguro y confiable de información y la protección de los datos sensibles, incluidos los de carácter sanitario.
- **Digital Services Act, Reglamento (UE) 2022/2065:** Establece obligaciones de transparencia, trazabilidad y diligencia debida para prestadores de servicios digitales y plataformas en línea, aplicables a la gestión de contenidos sintéticos generados mediante IA.

- **Carta de Derechos Digitales (Gobierno de España, 2021):** Reconoce los derechos fundamentales en el entorno digital, incluyendo identidad, veracidad informativa, protección frente a la manipulación algorítmica y garantías de transparencia en el uso de tecnologías basadas en inteligencia artificial.
- **ISO/IEC 42001:2023 – Sistemas de gestión de la inteligencia artificial:** Establece requisitos para implantar y mantener un sistema de gestión de IA que garantice un uso seguro, responsable y trazable de los algoritmos. Su aplicación refuerza la gobernanza, la transparencia y el control en sistemas generativos utilizados en entornos urbanos y sanitarios.
- **ISO/IEC 23894:2023 – Gestión del riesgo en la inteligencia artificial:** Define un marco estructurado para identificar, evaluar y mitigar los riesgos derivados del desarrollo y uso de la IA, incluyendo los relacionados con la generación de contenidos sintéticos y su impacto en la integridad de la información.
- **ISO/IEC 38507:2022 – Gobernanza de la inteligencia artificial:** Proporciona directrices para integrar la IA en los sistemas de gobernanza organizacional, asignando responsabilidades, supervisión de la alta dirección y control del riesgo en la toma de decisiones automatizada.
- **ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad:** Establece requisitos para gestionar la seguridad de la información en organizaciones que operan con IA, asegurando la confidencialidad, integridad, disponibilidad y autenticidad de los datos procesados.
- **ISO 31000:2018 – Gestión del riesgo:** Ofrece principios y directrices generales para establecer un marco eficaz de gestión del riesgo organizativo, aplicable a los riesgos tecnológicos y algorítmicos en los sistemas inteligentes de Smart Cities y salud.
- **ISO/IEC 30111:2019 – Gestión de vulnerabilidades:** Describe procesos para la recepción, análisis y coordinación de vulnerabilidades en software y sistemas de IA, esenciales para prevenir incidentes que afecten la integridad de los modelos y de los datos.
- **NIST AI Risk Management Framework 1.0 (2023):** Proporciona un marco de referencia para gestionar los riesgos de la IA en todo su ciclo de vida, promoviendo la transparencia, la responsabilidad y la mitigación de sesgos en sistemas automatizados y generativos.
- **UNE 178104:2017 – Ciudades inteligentes. Interoperabilidad de plataformas de ciudad inteligente:** Norma del marco español de Smart Cities que establece los requisitos y modelos de interoperabilidad necesarios entre plataformas urbanas, sistemas municipales y servicios digitales. Resulta esencial para garantizar que los sistemas basados en IA puedan integrarse de forma segura, coherente y trazable con la infraestructura digital urbana, asegurando la continuidad del servicio y la correcta gestión del dato municipal.

- **UNE 178108:2017 – Ciudades inteligentes. Gestión inteligente de activos urbanos:** Define los principios, requisitos y procedimientos para la gestión digitalizada de activos urbanos mediante tecnologías avanzadas, incluyendo sensores, IoT e inteligencia artificial. Su inclusión es clave para asegurar que los sistemas de IA que interactúan con mobiliario urbano, alumbrado, redes energéticas o hidráulicas operen bajo criterios homogéneos de mantenimiento, seguridad y trazabilidad.
- **UNE 178301:2015 – Ciudades inteligentes. Sistema de indicadores y métricas:** Establece un marco común de indicadores urbanos que permite evaluar, monitorizar y comparar el rendimiento de los servicios inteligentes. Es relevante en el contexto de IA porque facilita la medición de impacto, la evaluación del desempeño algorítmico y el seguimiento de resultados que afectan directamente a los usuarios finales.
- **UNE 178503:2019 – Destinos turísticos inteligentes. Requisitos:** Aunque orientada a destinos turísticos, esta norma se considera aplicable a servicios urbanos con fuerte componente turístico dentro de Smart Cities. Incluye requisitos de accesibilidad, interoperabilidad, gobernanza del dato y sostenibilidad, todos ellos esenciales en sistemas de IA que interactúan con visitantes y residentes en áreas urbanas de interés turístico.
- **UNE-EN 301549:2022 – Accesibilidad de los productos y servicios TIC:** Norma armonizada que establece los requisitos de accesibilidad aplicables a productos, servicios digitales y plataformas públicas, incluyendo interfaces basadas en IA. Su incorporación es imprescindible para garantizar que los sistemas de IA urbanos sean accesibles para personas mayores, personas con discapacidad y colectivos en riesgo de exclusión digital.
- **ISO/IEC 25012:2014 – Modelo de calidad de datos:** Norma internacional que define las características de calidad del dato, incluyendo precisión, integridad, disponibilidad, trazabilidad y consistencia. Es fundamental para asegurar que los sistemas de IA urbanos se alimenten de datos fiables, especialmente en movilidad, gestión energética, seguridad urbana y servicios automatizados dirigidos al ciudadano.
- **ISO 37120 / ISO 37122 / ISO 37123 – Indicadores para ciudades sostenibles e inteligentes:** Conjunto de normas internacionales que establecen indicadores avanzados para la gestión inteligente y sostenible de las ciudades. Su adopción ofrece un marco metodológico sólido para integrar IA en la planificación urbana y evaluar su impacto sobre la ciudadanía, reforzando la transparencia, la comparabilidad y la toma de decisiones basada en datos.

4. Definiciones

Este capítulo recopilará los conceptos clave y acrónimos utilizados a lo largo de la guía. Incluirá una tabla con definiciones de términos como inteligencia artificial, sistema automatizado, contenido sintético, datos personales, supervisión humana, ciberseguridad, accesibilidad digital, sesgo algorítmico, entre otros.

Término/Acrónimo	Definición
Inteligencia Artificial (IA)	Conjunto de sistemas informáticos que, a partir del análisis de datos y con distintos niveles de autonomía, generan resultados como predicciones, recomendaciones, clasificaciones, contenidos o decisiones que influyen en entornos físicos o digitales.
Sistema de Inteligencia Artificial (Sistema de IA)	Sistema informático que utiliza técnicas de inteligencia artificial para procesar información y generar resultados automáticos, como respuestas, clasificaciones, predicciones o recomendaciones, en el contexto de un servicio o proceso.
Sistema automatizado	Sistema que ejecuta acciones o produce resultados sin intervención humana directa en cada operación, pudiendo basarse en inteligencia artificial o en reglas previamente definidas.
Decisión automatizada	Resultado generado por un sistema informático sin intervención humana directa en el momento de la decisión, que puede afectar a una persona o a un procedimiento administrativo.
Toma de decisiones automatizadas	Proceso mediante el cual un sistema automatizado clasifica, prioriza o resuelve solicitudes o situaciones utilizando reglas o modelos algorítmicos.
Supervisión humana	Capacidad de personas responsables para revisar, interpretar, corregir o detener el funcionamiento de un sistema automatizado cuando sea necesario.
Control humano significativo	Forma de supervisión humana en la que la intervención de una persona es real y efectiva, y no meramente formal, especialmente cuando una decisión automatizada puede tener impacto relevante sobre la ciudadanía.
Datos personales	Cualquier información que identifica o puede identificar a una persona física, como nombre, imagen, voz, ubicación u otros datos de contacto o identificación.
Datos sensibles	Datos personales que requieren una protección reforzada por su especial naturaleza, como datos biométricos, datos de salud o información que permita identificar de manera inequívoca a una persona.
Datos biométricos	Datos personales obtenidos a partir de características físicas, fisiológicas o conductuales de una persona, como el rostro, la voz o la huella dactilar.

Término/Acrónimo	Definición
Identificación biométrica	Uso de datos biométricos para identificar de manera única a una persona, especialmente en servicios digitales o espacios públicos, sujeto a requisitos legales específicos.
Perfilado	Tratamiento automatizado de datos personales destinado a analizar o predecir aspectos relacionados con una persona, como su comportamiento, preferencias o patrones de uso de servicios.
Contenido sintético	Texto, imagen, audio o vídeo generado o modificado mediante sistemas de inteligencia artificial, que puede aparentar ser real.
Deepfake	Tipo de contenido sintético generado mediante inteligencia artificial que imita de forma realista la imagen o la voz de una persona y puede inducir a error.
Sesgo algorítmico	Situación en la que un sistema de IA produce resultados injustos o desiguales debido a datos poco representativos, errores de diseño o limitaciones en su funcionamiento.
Calidad del dato	Grado en que los datos utilizados por un sistema son adecuados, precisos, completos y actualizados en relación con la finalidad del servicio.
Transparencia	Principio por el cual la ciudadanía debe ser informada de forma clara cuando interactúa con sistemas de inteligencia artificial y sobre su finalidad y funcionamiento general.
Explicabilidad	Capacidad de un sistema de IA para ofrecer explicaciones comprensibles sobre cómo y por qué se ha generado un determinado resultado.
Trazabilidad	Capacidad de reconstruir el funcionamiento de un sistema de IA y los datos utilizados para generar un resultado, con el fin de facilitar su supervisión, revisión y auditoría.
Ciberseguridad	Conjunto de medidas técnicas y organizativas destinadas a proteger sistemas digitales, datos y servicios frente a accesos no autorizados, fallos o ataques.
Incidente de seguridad	Evento que compromete o puede comprometer la confidencialidad, integridad, disponibilidad o autenticidad de un sistema o de los datos que trata.
Smart City	Ciudad inteligente: Entorno urbano que utiliza tecnologías digitales, sistemas de información y análisis de datos para mejorar la gestión de los servicios públicos y la calidad de vida de la ciudadanía.
Asistente virtual / chatbot	Sistema, habitualmente basado en inteligencia artificial, que interactúa con las personas mediante texto o voz para ofrecer información o guiar trámites de forma automatizada.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Sistemas de IA en los Smart Cities

Las ciudades inteligentes (Smart Cities) utilizan de forma creciente sistemas de inteligencia artificial (IA) para mejorar la gestión de los servicios públicos urbanos y facilitar la relación entre la ciudadanía y la administración. Estos sistemas se emplean para analizar información, anticipar necesidades, automatizar determinadas tareas y apoyar la toma de decisiones en ámbitos clave de la vida urbana.

En algunos casos, la presencia de la IA es visible para la ciudadanía, como cuando se interactúa con un asistente virtual municipal o se recibe una recomendación a través de una aplicación. En otros casos, los sistemas de inteligencia artificial actúan de manera menos perceptible, por ejemplo, ajustando automáticamente los tiempos de los semáforos, priorizando incidencias ciudadanas o detectando cambios en la calidad ambiental sin que la persona usuaria tenga que realizar ninguna acción.

Comprender qué es un sistema de IA, cómo se utiliza en el entorno urbano y cuáles son sus límites permite a la ciudadanía interpretar mejor la información que recibe, utilizar los servicios públicos con mayor seguridad y confianza, y saber cuándo resulta necesario solicitar aclaraciones o intervención humana.

5.1. Funcionamiento general y tipos de sistemas de IA utilizados en Smart Cities

Un sistema de inteligencia artificial es un sistema informático diseñado para analizar información y generar resultados automáticos que apoyan el funcionamiento de un servicio, un proceso o una decisión. A partir de datos, textos, imágenes, señales procedentes de sensores u otra información disponible, estos sistemas pueden producir resultados como clasificaciones, predicciones, estimaciones, recomendaciones, detecciones, respuestas automáticas o avisos.

En el entorno de las Smart Cities, los sistemas de IA pueden operar de forma automatizada o semiautónoma y se utilizan para gestionar servicios urbanos, apoyar la atención ciudadana, analizar el estado del entorno urbano o facilitar información relevante a la ciudadanía. Su finalidad es mejorar la eficiencia, la capacidad de respuesta y la planificación de los servicios públicos, sin sustituir el control ni la responsabilidad humana.

A diferencia de los programas informáticos tradicionales, que funcionan siguiendo instrucciones fijas definidas previamente, muchos sistemas de IA generan sus resultados a partir del análisis de grandes volúmenes de información y de la identificación de patrones o relaciones entre los datos. Esto les permite adaptarse a contextos cambiantes, como variaciones en la movilidad, incidencias imprevistas o cambios en las condiciones ambientales. Al mismo tiempo, implica que sus resultados pueden verse afectados por la calidad de los datos disponibles, por situaciones poco habituales o por cambios en el entorno urbano, por lo que no deben considerarse infalibles.

En función del tipo de tarea que realizan y del resultado que generan, en las Smart Cities se emplean distintos tipos funcionales de algoritmos de inteligencia artificial, entre los que destacan los siguientes:

- I. **Clasificación:** Analizan la información que reciben y determinan a qué categoría pertenece según patrones identificados a partir de datos previos. En el ámbito urbano, se utilizan para identificar el tipo de incidencia comunicada por la ciudadanía, clasificar solicitudes administrativas, distinguir entre distintos tipos de consultas o reconocer elementos básicos en imágenes o textos. Funcionan dentro de las categorías para las que han sido configurados, por lo que pueden cometer errores cuando se enfrentan a información ambigua, incompleta o a situaciones no previstas. **Ejemplo:** un sistema municipal que identifica automáticamente si una incidencia corresponde a alumbrado, limpieza, tráfico o ruido para derivarla al área competente.
- II. **Regresión:** Generan estimaciones numéricas aproximadas a partir del análisis de datos históricos y actuales, con el objetivo de anticipar valores futuros o desconocidos. Se emplean para prever la demanda energética, estimar tiempos de llegada del transporte público o anticipar niveles de ocupación de determinados servicios. Sus resultados tienen carácter orientativo y pueden variar si cambian las condiciones reales, como el tráfico, la meteorología o la aparición de incidencias imprevistas. **Ejemplo:** la estimación del tiempo de llegada de un autobús que se actualiza en función de atascos o desvíos.
- III. **Agrupamiento (clustering):** Analizan grandes volúmenes de datos para identificar similitudes y formar grupos de información con comportamientos parecidos, sin partir necesariamente de categorías predefinidas. En las Smart Cities se utilizan para detectar patrones de movilidad, zonas con incidencias recurrentes o comportamientos similares en el uso de servicios públicos. Estos resultados sirven de apoyo al análisis y a la planificación urbana, pero requieren interpretación humana para evitar conclusiones incorrectas o simplificadas. **Ejemplo:** el análisis de datos de llenado de contenedores de residuos que permite agrupar zonas de la ciudad con patrones similares de generación de basura y ajustar las rutas y frecuencias de recogida.
- IV. **Procesamiento del Lenguaje Natural (PLN):** Permiten a los sistemas entender y generar lenguaje humano, tanto en texto como en voz. Se utilizan en asistentes virtuales y chatbots municipales para responder consultas, guiar trámites o proporcionar información básica sobre servicios urbanos. Aunque facilitan el acceso a la información, pueden ofrecer respuestas incompletas, desactualizadas o poco ajustadas cuando la consulta es compleja, por lo que deben coexistir con canales claros de atención humana. **Ejemplo:** un chatbot municipal que responde preguntas frecuentes sobre citas, documentación o plazos administrativos.
- V. **Visión por computador:** Analizan imágenes o secuencias de vídeo para extraer información relevante sobre el entorno. En el ámbito urbano pueden emplearse para detectar incidencias en la vía pública, identificar situaciones que requieren revisión o apoyar la gestión de emergencias. Su funcionamiento puede verse afectado por factores como la iluminación, las condiciones meteorológicas o la calidad de las imágenes, y su uso está sujeto a requisitos legales estrictos cuando pueden aparecer personas o datos sensibles. **Ejemplo:** un sistema que detecta un vehículo detenido en un carril reservado para alertar a los servicios municipales.
- VI. **Aprendizaje por refuerzo:** Ajustan su comportamiento mediante la interacción con el entorno, evaluando los resultados de sus acciones para mejorar progresivamente un objetivo definido.

En las Smart Cities pueden utilizarse para optimizar procesos dinámicos que requieren ajustes continuos. Dado que sus decisiones pueden cambiar con el tiempo y el contexto, requieren supervisión continua para evitar impactos no deseados sobre la ciudadanía. **Ejemplo:** un sistema que ajusta la sincronización de semáforos en función de la fluidez real del tráfico.

- VII. **Sistemas basados en reglas expertas:** este tipo de sistemas automatizan decisiones aplicando condiciones definidas previamente por personal experto y criterios claros y verificables. Se utilizan cuando la administración establece reglas concretas para actuar ante determinadas situaciones, sin que el sistema tenga capacidad de aprendizaje autónomo. Aunque ofrecen un comportamiento previsible y fácil de supervisar, pueden no contemplar excepciones o cambios imprevistos, por lo que deben revisarse y actualizarse periódicamente para adaptarse a la evolución del entorno urbano. **Ejemplo:** un sistema que comprueba automáticamente si una solicitud de bonificación municipal cumple los requisitos establecidos (edad, empadronamiento y nivel de renta) y genera un aviso de concesión o denegación siguiendo exclusivamente las reglas fijadas por la normativa vigente.

Todos estos tipos de sistemas presentan límites. Pueden cometer errores, no contemplar situaciones excepcionales o generar resultados que no se ajusten plenamente a un caso concreto. Por ello, la inteligencia artificial debe entenderse como una herramienta de apoyo al servicio público y no como una decisión automática incuestionable. La ciudadanía tiene derecho a saber cuándo un servicio utiliza sistemas automatizados y a solicitar aclaraciones o revisión humana cuando un resultado no sea claro o tenga consecuencias relevantes. Aunque el ciudadano no necesite conocer el nombre técnico del algoritmo utilizado, sí debe saber si está interactuando con un sistema automatizado y qué impacto puede tener sobre sus derechos o decisiones.

5.2. Ámbitos de uso de la IA en Smart Cities y recomendaciones específicas

Los sistemas de inteligencia artificial se utilizan en distintos servicios urbanos para apoyar la gestión municipal y mejorar la prestación de servicios a la ciudadanía. Aunque los principios generales de uso responsable y seguro son comunes, la forma concreta en que la IA interviene, el tipo de información que utiliza y el impacto que puede tener sobre las personas varían según el ámbito de aplicación.

Este apartado describe los principales contextos en los que la ciudadanía se encuentra con sistemas de IA en una Smart City y ofrece orientaciones prácticas para comprender su funcionamiento y utilizarlos de forma informada.

5.2.1. Movilidad inteligente y transporte

En el ámbito de la movilidad, la IA se utiliza para gestionar semáforos en tiempo real, calcular tiempos de llegada del transporte público, proponer rutas alternativas, gestionar servicios de bicicleta o patinete compartido y analizar patrones de tráfico. Estas funcionalidades contribuyen a mejorar la eficiencia y a reducir tiempos de desplazamiento.

Para la ciudadanía, es importante entender que:

- Las estimaciones ofrecidas por aplicaciones de movilidad son aproximaciones basadas en datos y modelos, y pueden verse afectadas por incidencias imprevistas.
- El uso continuado de datos de geolocalización puede implicar la elaboración de perfiles de desplazamiento, por lo que resulta recomendable desactivar la ubicación cuando no sea necesaria o utilizar opciones de “solo mientras se usa la aplicación”.

Las decisiones relacionadas con seguridad vial deben basarse siempre en la observación directa de las condiciones del entorno y en el respeto a las normas de circulación, y no únicamente en las indicaciones de sistemas automatizados.

5.2.2. Energía, agua y medio ambiente urbano

La IA puede contribuir a la gestión inteligente del alumbrado público, al control de consumos energéticos, al funcionamiento de redes de agua y al seguimiento de indicadores ambientales como la calidad del aire o el ruido. Estos sistemas generan avisos y recomendaciones dirigidas tanto a la administración como, en algunos casos, directamente a la ciudadanía.

Las personas usuarias deben considerar que:

- Determinadas alertas ambientales se basan en datos en tiempo real, pero otras tienen un componente predictivo, por lo que conviene contrastar su contenido con la información oficial publicada por el Ayuntamiento u organismos competentes.
- La instalación de contadores inteligentes o aplicaciones de monitorización del consumo puede conllevar el tratamiento de datos que reflejan hábitos de vida. Es recomendable revisar la información ofrecida sobre estos tratamientos y ejercer los derechos de protección de datos cuando se considere oportuno.

5.2.3. Seguridad urbana y gestión de emergencias

En materia de seguridad y emergencias, la IA puede utilizarse para detectar patrones anómalos, ayudar a la gestión de recursos en tiempo real, analizar imágenes de cámaras públicas o enviar avisos a la población en caso de riesgo. El uso de estas tecnologías se encuentra sujeto a normas estrictas, dada su especial sensibilidad.

Para la ciudadanía, resulta esencial:

- Verificar siempre la autenticidad de los avisos de emergencia y seguir únicamente las indicaciones ofrecidas por canales institucionales reconocibles.
- Evitar difundir por redes sociales contenidos no verificados que puedan generar alarmas injustificadas o confusión.

Tomar conciencia de que el uso de cámaras y sensores en espacios públicos debe estar limitado por la normativa, y que ante dudas sobre tratamientos de imágenes o datos biométricos pueden ejercerse derechos de protección de datos o consultarse las autoridades competentes.

5.2.4. Atención ciudadana digital y tramitación administrativa

Los servicios de atención ciudadana incorporan cada vez con mayor frecuencia asistentes virtuales, chatbots, sistemas de clasificación automática de solicitudes y plataformas de tramitación electrónica guiadas por IA. Estas herramientas pueden facilitar la relación con la administración, pero no suprimen los canales tradicionales ni el derecho a la atención humana.

En este ámbito, la ciudadanía debería:

- Utilizar preferiblemente los canales oficiales publicados en las sedes electrónicas y portales municipales.
- Leer con atención los resúmenes de trámite y los datos incorporados automáticamente antes de confirmar una solicitud o un registro.

Solicitar atención personal (presencial, telefónica o en línea) cuando la respuesta automatizada no resulte comprensible, resulte contraria a la situación real o tenga consecuencias significativas.

5.2.5. Participación ciudadana digital y plataformas municipales

La IA puede emplearse en plataformas de participación y consulta pública para agrupar propuestas, detectar temas recurrentes o moderar contenidos. Aunque estos sistemas persiguen facilitar la gestión de grandes volúmenes de información, no deben sustituir el criterio humano en la toma de decisiones políticas o en la valoración de las aportaciones ciudadanas.

La persona usuaria puede:

- Revisar las condiciones de uso de las plataformas de participación, incluyendo los criterios de moderación automatizada.
- Pedir revisión de decisiones de moderación cuando considere que se han eliminado o alterado contenidos de forma injustificada.
- Verificar que las convocatorias y consultas en las que participa proceden realmente de fuentes institucionales legítimas.

5.2.6. Turismo inteligente y servicios culturales digitales

En el ámbito turístico y cultural, la IA se utiliza para generar rutas personalizadas, ofrecer contenidos interpretativos sobre el patrimonio, recomendar actividades o incluso crear experiencias inmersivas mediante contenidos sintéticos. Estas funcionalidades pueden enriquecer la experiencia urbana, pero también presentar riesgos de desinformación o de tratamiento excesivo de datos de preferencias personales.

La ciudadanía, tanto residente como visitante, puede:

- Verificar los contenidos informativos consultando fuentes oficiales (portales turísticos municipales, museos, oficinas de información).
- Limitar la cantidad de datos personales (por ejemplo, historial de desplazamientos o preferencias muy detalladas) proporcionados a aplicaciones culturales, especialmente si no son necesarios.

- Ser consciente de que determinadas recreaciones digitales pueden no corresponder exactamente con la realidad histórica o patrimonial, y utilizarlas como complemento, no como única fuente de conocimiento.

6. Riesgos y desafíos de la IA en Smart Cities para la ciudadanía

La integración de sistemas de Inteligencia Artificial en los servicios urbanos transforma la forma en que la ciudadanía se relaciona con su entorno, accede a los servicios municipales y participa en la vida pública. Esta transformación ofrece beneficios notables en eficiencia, rapidez, capacidad de anticipación y personalización, pero también introduce riesgos complejos que pueden afectar directamente a derechos fundamentales, a la privacidad, a la equidad, a la seguridad digital y a la confianza en las instituciones públicas.

El propósito de este capítulo es describir de manera completa y accesible los principales riesgos asociados al uso de sistemas de IA en las Smart Cities. Se estructura en secciones que analizan las causas, implicaciones y escenarios representativos de cada riesgo, con el fin de proporcionar a la ciudadanía un marco sólido para comprender el funcionamiento de estos sistemas y detectar situaciones en las que conviene solicitar información adicional, solicitar intervención humana, ejercer derechos y/o adoptar medidas de precaución.

6.1. Complejidad y falta de visibilidad del ecosistema urbano digital

Las Smart Cities se basan en una infraestructura digital extensa e interconectada formada por sensores, cámaras, plataformas de datos, redes de comunicaciones y modelos de IA. Buena parte de este funcionamiento resulta invisible para la ciudadanía, lo que puede dificultar la comprensión del servicio y generar incertidumbre sobre cómo se producen los resultados.

La falta de visibilidad sobre cómo se articula el entorno digital urbano puede generar las siguientes dificultades principales para la experiencia cotidiana de las personas usuarias:

- **Dificultad para saber cuándo interviene la IA:** Muchas personas usuarias desconocen cuándo un servicio incorpora IA. Por ejemplo, recomendaciones de movilidad, clasificación de incidencias o respuestas automatizadas pueden generarse mediante modelos de IA sin que el sistema lo indique de forma clara. La falta de información reduce la capacidad de interpretar la fiabilidad y explicabilidad del resultado.
- **Incertidumbre sobre quién gestiona los datos o toma decisiones:** Como los servicios pueden implicar a varias áreas municipales y empresas proveedoras, la ciudadanía puede no saber con claridad quién es responsable del tratamiento de sus datos o del funcionamiento del servicio.
- **Percepción de arbitrariedad o falta de justificación:** Si un sistema de inteligencia artificial modifica una ruta prevista, prioriza una incidencia o interpreta una solicitud de manera inesperada y no se explican los criterios aplicados, la ciudadanía puede sentir desconfianza o falta de transparencia.

El Reglamento europeo de inteligencia artificial exige que la ciudadanía sea informada siempre que interactúe con sistemas de IA y que las decisiones automatizadas relevantes cuenten con supervisión humana y explicaciones adecuadas. Por ello, cualquier servicio urbano basado en IA debe comunicar de forma clara que utiliza inteligencia artificial y explicar su funcionamiento básico. Cuando esta información no se proporciona, se produce un riesgo de falta de transparencia por lo que es

recomendable que las personas usuarias interpreten los resultados con cautela y soliciten información adicional o pidan una revisión humana.

6.2. Privacidad y el uso intensivo de datos personales

Muchos servicios basados en IA requieren grandes cantidades de datos personales para funcionar correctamente. Estos datos pueden reflejar desplazamientos, hábitos cotidianos, actividad digital o interacciones con servicios municipales. Una gestión inadecuada puede comprometer la privacidad y afectar derechos fundamentales, lo que puede manifestarse en situaciones como las siguientes:

- **Seguimiento implícito de hábitos y desplazamientos:** Los servicios de movilidad, sensores urbanos o aplicaciones municipales pueden proporcionar información continua sobre la ubicación y la actividad cotidiana, incluso cuando la persona usuaria no es plenamente consciente de ello.
- **Tratamiento de datos sensibles:** Algunos sistemas utilizan datos especialmente sensibles como la biometría, la voz o la imagen, que permiten identificar a una persona de manera inequívoca. Cuando estos datos se emplean para identificar o verificar a personas en espacios públicos mediante sistemas de IA, el Reglamento Europeo de Inteligencia Artificial los considera parte de sistemas de identificación biométrica remota. Este tipo de sistemas de IA se clasifican como alto riesgo según el RIA y, además, están prohibidos cuando funcionan en tiempo real en espacios públicos salvo la existencia de una habilitación legal específica y estricta. Estas garantías tienen como objetivo proteger los derechos fundamentales de la ciudadanía y evitar usos indebidos o desproporcionados.
- **Dificultad para conocer el destino de los datos:** La ciudadanía puede desconocer si los datos que facilita en un servicio concreto se utilizan solo para ese servicio o si se unen con información procedente de otros sistemas municipales, como aplicaciones de movilidad, plataformas de atención ciudadana o redes de sensores. Cuando los datos se combinan de esta forma, aumenta la cantidad de información que puede inferirse sobre la vida de una persona y se incrementan los riesgos para su privacidad si no existe una justificación clara y transparente.

De acuerdo con el RGPD, la LOPDGDD y el Reglamento Europeo de Inteligencia Artificial, el tratamiento de datos personales en servicios urbanos basados en IA debe realizarse con transparencia, proporcionalidad y una finalidad claramente definida. La ciudadanía tiene derecho a conocer qué datos se recogen, con qué finalidad se utilizan, quién accede a ellos y durante cuánto tiempo se conservarán, así como a solicitar aclaraciones cuando el tratamiento resulte poco claro. Estos derechos y garantías, junto con la posibilidad de oponerse a ciertos tratamientos, solicitar la supresión de datos o pedir la revisión de decisiones automatizadas, se describen con mayor detalle en el apartado 10 de esta guía. Contar con esta información permite a la ciudadanía mantener un mayor control sobre sus datos personales y reducir los riesgos asociados al uso excesivo de información en el entorno urbano.

6.3. Seguridad digital y exposición a incidentes

El funcionamiento de una Smart City depende de múltiples dispositivos conectados, servicios digitales y sistemas de inteligencia artificial, lo que incrementa la posibilidad de incidentes que afectan a la seguridad digital y pueden tener un impacto directo en la ciudadanía. Estos incidentes pueden alterar la información que reciben las personas usuarias, interferir en su interacción con los servicios públicos o comprometer la protección de sus datos personales. Entre los escenarios más habituales se encuentran los siguientes:

- **Accesos no autorizados mediante vulnerabilidades en servicios o aplicaciones municipales:** Un fallo de seguridad en una aplicación o plataforma digital basada en IA puede permitir que terceros accedan a información personal o modifiquen el funcionamiento del servicio sin consentimiento de la persona usuaria.
- **Difusión de información incorrecta por manipulación de sistemas digitales:** Un servicio municipal basado en IA que haya sido comprometido puede mostrar datos inexactos, generar recomendaciones erróneas o emitir avisos alterados, lo que afecta directamente la toma de decisiones cotidianas.
- **Recepción de comunicaciones falsas que imitan canales oficiales.** Las tecnologías generativas permiten crear mensajes, imágenes o audios que reproducen la apariencia de comunicaciones municipales reales. Esto puede inducir a la ciudadanía a interactuar con contenidos fraudulentos que soliciten datos personales o redirijan a servicios no legítimos.

El Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y el Reglamento Europeo de Inteligencia Artificial (RIA) establecen obligaciones para que los sistemas públicos basados en IA cuenten con medidas de protección, gestión de vulnerabilidades y detección temprana de incidentes. Ante cualquier duda, resulta recomendable que la persona usuaria acceda exclusivamente a canales oficiales, verifique la autenticidad de los mensajes recibidos y contrastar las comunicaciones con otros fuentes y medios oficiales.

6.4. Riesgos derivados del funcionamiento de la IA

Los sistemas de inteligencia artificial funcionan analizando grandes cantidades de datos para generar recomendaciones, clasificaciones o respuestas. Aunque pueden resultar útiles para mejorar la gestión urbana, su funcionamiento depende de la calidad de los datos disponibles y de las reglas establecidas durante su diseño. Esta dependencia puede generar resultados que no reflejen adecuadamente la situación real o que no se ajusten a las necesidades concretas de cada persona usuaria.

Estas limitaciones pueden afectar a la ciudadanía en distintas situaciones. Entre las más habituales se encuentran las siguientes:

- **Resultados imprecisos o poco ajustados a la realidad personal:** Cuando los datos empleados por el sistema están incompletos o no coinciden con la situación actual, pueden producirse respuestas incorrectas. Esto puede observarse cuando un sistema asigna una cita en un horario que no se corresponde con la disponibilidad real, cuando un trámite presentado en línea se

deriva a un departamento que no corresponde o cuando una solicitud aparece marcada como incompleta pese a haber aportado toda la documentación.

- **Tratamientos desiguales derivados de datos poco representativos:** Cuando los sistemas de IA se entrenan con información insuficiente o poco diversa, algunas personas pueden recibir resultados menos precisos, experimentando diferencias en la calidad del servicio que reciben.
- **Dificultad para comprender cómo se ha generado un resultado automatizado:** Al no explicarse siempre los criterios utilizados por el sistema, la ciudadanía puede desconocer el motivo de un determinado resultado, lo que dificulta identificar errores o solicitar una aclaración.
- **Cambios inesperados debidos a ajustes o actualizaciones del sistema:** Los sistemas de IA se actualizan periódicamente para mejorar su funcionamiento. En algunos casos, estas actualizaciones pueden modificar la forma en que se ordenan las solicitudes, se priorizan las incidencias o se presentan las recomendaciones, sin que la ciudadanía reciba una explicación clara de estos cambios.

El Reglamento Europeo de Inteligencia Artificial establece que los sistemas con impacto social relevante deben utilizar datos de calidad, aplicar medidas para reducir los sesgos, incorporar supervisión humana significativa y ofrecer explicaciones generales comprensibles sobre su funcionamiento. Estas garantías tienen por finalidad mejorar la fiabilidad de los sistemas y reforzar la confianza de la ciudadanía.

Cuando los resultados de un sistema de IA no se ajustan a la situación real, generan dudas razonables o condicionan decisiones relevantes, la persona usuaria puede solicitar una revisión humana y pedir información adicional sobre los criterios que han intervenido en la decisión automatizada. Esta posibilidad constituye una garantía esencial para asegurar un uso adecuado y transparente de la inteligencia artificial en los servicios urbanos.

6.5. Desinformación, manipulación digital y contenidos sintéticos

El uso de herramientas generativas basadas en inteligencia artificial permite crear textos, imágenes, audios y vídeos de apariencia realista que pueden confundirse con comunicaciones legítimas. La creación de este tipo de contenidos plantea riesgos específicos relacionados con la fiabilidad de la información que recibe la ciudadanía, que pueden aparecer en situaciones como las siguientes:

- **Mensajes falsos elaborados con apariencia institucional:** Los contenidos generados automáticamente pueden reproducir logotipos, estilos y formatos municipales, dificultando distinguir si un aviso, recomendación o notificación procede realmente de la administración pública.
- **Difusión de imágenes, audios o vídeos alterados que inducen a interpretaciones erróneas:** Los contenidos sintéticos pueden presentar situaciones inexistentes, modificar eventos o alterar información relevante sobre servicios públicos, generando confusión o alarma injustificada.

- **Dificultad creciente para verificar la autenticidad de la información digital:** El realismo de los contenidos generados por IA obliga a un mayor nivel de prudencia al interpretar mensajes digitales relacionados con decisiones, servicios o avisos municipales.

De acuerdo con el Reglamento Europeo de Inteligencia Artificial (RIA), el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y los principios de transparencia aplicables al sector público, la administración debe ofrecer información clara sobre el uso de los sistemas de IA, explicar su finalidad y garantizar la disponibilidad de atención humana cuando los resultados generen dudas o puedan tener un impacto relevante en la ciudadanía.

Asimismo, para un análisis más detallado de los riesgos, técnicas de detección y medidas de prevención asociadas a contenidos sintéticos y deepfakes generados mediante inteligencia artificial, se recomienda consultar la *Guía de detección y prevención de deepfakes generados por IA en los entornos de Smart Cities y Salud*.

6.6. Accesibilidad, inclusión y brecha digital

La digitalización de los servicios urbanos mediante el uso de IA puede mejorar significativamente la atención ciudadana, pero también puede generar dificultades para colectivos con menor acceso a la tecnología o con necesidades específicas de accesibilidad. Estos riesgos se manifiestan con frecuencia en los siguientes escenarios:

- **Dificultades para personas con discapacidad o con competencias digitales limitadas:** Interfaces no adaptadas, instrucciones complejas o procesos digitales rígidos pueden impedir que ciertas personas utilicen los servicios públicos de manera autónoma.
- **Ausencia de alternativas no digitales:** Cuando un trámite solo puede realizarse en línea o mediante una aplicación móvil, quienes no disponen de los medios necesarios pueden quedar excluidos del servicio.
- **Dependencia creciente de herramientas tecnológicas:** La automatización de gestiones cotidianas puede obligar a utilizar sistemas digitales que no siempre se ajustan a las capacidades o necesidades de todas las personas usuarias

El Reglamento Europeo de Inteligencia Artificial refuerza la obligación de garantizar accesibilidad adecuada, mitigar sesgos y mantener supervisión humana en sistemas con impacto social. Para favorecer un uso inclusivo, es recomendable que la ciudadanía emplee los recursos de accesibilidad disponibles y solicite asistencia cuando encuentre dificultades, y que la administración proporcione canales alternativos, descritos en el capítulo 10, cuando el uso de herramientas digitales no resulte adecuado.

6.7. Impacto en la experiencia ciudadana

La presencia continua de sistemas automatizados y dispositivos inteligentes en el espacio urbano puede influir en la percepción que la ciudadanía tiene de los servicios públicos, del entorno y de la propia administración. Estos efectos pueden aparecer en situaciones como las siguientes:

- **Sensación de vigilancia constante en el espacio público:** La presencia de cámaras, sensores y otros dispositivos puede generar inquietud sobre el nivel de seguimiento existente. El Reglamento Europeo de Inteligencia Artificial prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos salvo habilitación legal específica, lo que constituye una garantía relevante para los derechos de la ciudadanía.
- **Desconfianza derivada de una comunicación insuficiente:** La falta de información clara y accesible sobre qué sistemas de inteligencia artificial se utilizan, con qué finalidad y qué impacto pueden tener en la persona usuaria puede generar una percepción de opacidad institucional y disminuir la confianza en los servicios públicos.
- **Sobrecarga de avisos o notificaciones automatizadas:** La recepción frecuente de recomendaciones, alertas o actualizaciones digitales puede resultar difícil de gestionar y provocar saturación informativa, especialmente si los mensajes no son relevantes o no están bien contextualizados.
- **Dependencia excesiva de resultados automatizados:** El uso continuado de recomendaciones o clasificaciones generadas por sistemas de inteligencia artificial puede llevar a que la ciudadanía confíe en ellas sin valorar otras fuentes de información. Esto puede influir en decisiones cotidianas, sobre todo cuando no se explican bien sus limitaciones o no se recuerda que estos sistemas ofrecen un apoyo orientativo, pero no sustituyen el criterio personal ni la valoración humana

La administración debe ofrecer información clara sobre el uso de los sistemas de inteligencia artificial, explicar su finalidad de manera comprensible y garantizar la disponibilidad de atención humana cuando los resultados generados por estos sistemas produzcan dudas o puedan tener un impacto relevante en la ciudadanía, de acuerdo con el Reglamento Europeo de Inteligencia Artificial (RIA), el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y los principios de transparencia y buena administración aplicables al sector público. Estas medidas contribuyen a reforzar la confianza pública y a favorecer una experiencia más equilibrada en entornos urbanos digitalizados.

En conjunto, los riesgos descritos muestran que la incorporación de sistemas de inteligencia artificial en los servicios urbanos aporta beneficios relevantes, pero también introduce aspectos que la ciudadanía debe conocer para utilizar los servicios digitales con mayor seguridad y confianza. Comprender cómo funcionan estos sistemas, qué limitaciones presentan y en qué situaciones conviene solicitar información adicional o una revisión humana ayuda a interpretar correctamente los resultados y a detectar posibles incidencias.

7. Principios de IA de uso responsable y seguro en Smart Cities

La presencia de la Inteligencia Artificial en los servicios urbanos exige que tanto las administraciones públicas como la ciudadanía dispongan de criterios claros que orienten su utilización de manera segura, respetuosa y coherente con los derechos fundamentales. Este capítulo presenta los principios que deben guiar el funcionamiento de los sistemas de IA en la ciudad y la interacción de las personas usuarias con ellos. Su propósito es ofrecer un marco de referencia accesible que facilite la comprensión de cómo deben diseñarse, gestionarse y supervisarse estos sistemas, y qué pueden esperar las personas ciudadanas al utilizarlos en su vida cotidiana.

Los principios se alinean con el Reglamento Europeo de Inteligencia Artificial (RIA), el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), el Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y las normas de accesibilidad y gestión del dato aplicables al sector público.

7.1. Respeto y garantía de los derechos fundamentales

Los sistemas de inteligencia artificial utilizados en el entorno urbano deben operar en todo momento conforme al marco constitucional y legal que protege los derechos fundamentales de las personas. El uso de la IA en los servicios públicos no puede limitar el acceso a servicios esenciales, generar discriminaciones injustificadas ni producir efectos que comprometan libertades individuales o derechos reconocidos por el ordenamiento jurídico.

La ciudadanía debe ser informada de manera clara y comprensible cuando un servicio incorpora funciones basadas en inteligencia artificial. Esta información debe incluir, como mínimo, la finalidad del sistema, el tipo de datos tratados, la existencia de procesos de toma de decisiones automatizadas, los criterios generales que intervienen en su funcionamiento y los plazos de conservación de los datos personales, de conformidad con lo establecido en el RGPD y la LOPDGDD.

Asimismo, las personas usuarias deben disponer de mecanismos accesibles para solicitar aclaraciones sobre el funcionamiento del servicio, ejercer los derechos reconocidos en materia de protección de datos personales y solicitar la intervención o revisión humana de decisiones automatizadas que tengan un impacto relevante en su situación personal. Estas garantías se aplican en coherencia con el artículo 22 del RGPD y con los requisitos de supervisión humana establecidos por el Reglamento Europeo de Inteligencia Artificial.

7.2. Gestión del riesgo y calidad de los sistemas de IA

Los servicios municipales que incorporen IA deben someterse a procesos continuos de evaluación, supervisión y mejora para garantizar su fiabilidad y seguridad. Esto incluye el uso de datos adecuados y actualizados, la aplicación de controles que reduzcan la posibilidad de errores significativos y la actualización periódica de los sistemas para adaptarlos a nuevas necesidades urbanas.

La calidad del funcionamiento de los sistemas de IA contribuye directamente a la confianza ciudadana, por lo que resulta esencial que las administraciones adopten prácticas de gestión del riesgo alineadas con el RIA y con estándares internacionales como ISO/IEC 42001 e ISO/IEC 23894.

7.3. Privacidad y protección de datos personales

El tratamiento de datos personales en servicios basados en IA debe respetar estrictamente los principios de licitud, minimización, transparencia y seguridad establecidos en el RGPD y la LOPDGDD. Los datos utilizados deben ser únicamente los necesarios para la prestación del servicio, evitando la recopilación excesiva o el tratamiento incompatible con la finalidad comunicada.

Cuando los sistemas utilicen información sensible, como datos biométricos o imágenes, deben aplicarse salvaguardas reforzadas, informar de manera clara a las personas usuarias e incorporar medidas de seguridad acordes con el ENS y la Directiva NIS2. Las personas usuarias conservan en todo momento su derecho a obtener información sobre el tratamiento, así como a solicitar acceso, rectificación, supresión, oposición o revisión humana a través de los canales proporcionados en el capítulo 10.

7.4. Transparencia, trazabilidad y explicabilidad de los sistemas

Los sistemas de IA utilizados en Smart Cities que interactúan con personas deben ofrecer un nivel adecuado de transparencia que permita comprender sus funciones básicas, su finalidad y la forma en que contribuyen al servicio.

Las administraciones tienen la responsabilidad de proporcionar información clara sobre los criterios generales utilizados por los sistemas automatizados y garantizar que las decisiones relevantes puedan ser revisadas o explicadas de manera comprensible, conforme a las obligaciones de transparencia del RIA. Asimismo, deben mantenerse registros que permitan reconstruir los procesos técnicos y los datos utilizados en la generación de los resultados. Esta trazabilidad facilita la supervisión, la auditoría y la revisión de decisiones que puedan afectar a las personas usuarias, especialmente en servicios clasificados como de alto riesgo por el RIA.

7.5. Ciberseguridad orientada al usuario final

Los sistemas de IA deben estar protegidos frente a accesos no autorizados, manipulaciones y fallos que puedan comprometer la integridad, disponibilidad o autenticidad del servicio. Las administraciones deben asegurar la aplicación de medidas de seguridad acordes con el ENS y con los requisitos reforzados de gestión de vulnerabilidades y respuesta a incidentes establecidos por la Directiva NIS2.

La ciudadanía, por su parte, debe disponer de canales seguros para acceder a aplicaciones y servicios municipales y recibir pautas claras que reduzcan riesgos derivados de interacciones inseguras, intentos de fraude digital o comunicaciones falsas que imiten mensajes institucionales.

7.6. Equidad, accesibilidad universal e inclusión

La ciudad debe garantizar que los servicios basados en IA sean accesibles para todas las personas, con independencia de su edad, nivel de competencias digitales o situación física o cognitiva. Esto implica diseñar sistemas que cumplan los requisitos de accesibilidad digital, ofrecer instrucciones claras y proporcionar alternativas no digitales cuando el acceso electrónico no resulte viable para determinados colectivos.

Asimismo, los sistemas de IA deben evaluarse de manera periódica para evitar que introduzcan sesgos que afecten de forma desigual a diferentes grupos sociales, en coherencia con las obligaciones del RIA relativas a calidad del dato y supervisión.

7.7. Supervisión y control humano significativo

Aunque la IA puede automatizar muchos procesos, el control humano sigue siendo imprescindible, especialmente en aquellos casos en los que las decisiones tengan impacto relevante sobre la ciudadanía.

Debe existir siempre la posibilidad de intervención, supervisión o revisión por parte de personal municipal capacitado, y las decisiones automatizadas que puedan afectar a derechos o servicios esenciales deben estar sometidas a mecanismos claros de supervisión y evaluación.

7.8. Responsabilidad institucional y rendición de cuentas

Cada servicio municipal que utilice IA debe contar con responsables claramente definidos para su gestión, supervisión y resolución de incidencias. Las administraciones deben revisar periódicamente los resultados, documentar las decisiones relevantes, los criterios de funcionamiento y las medidas aplicadas para garantizar la seguridad, la calidad y la trazabilidad del sistema.

Asimismo, deben habilitar canales accesibles para que la ciudadanía pueda presentar consultas, reclamaciones, solicitar revisiones humanas o comunicar problemas relacionados con los resultados generados por servicios públicos que incorporen IA, en coherencia con los principios de buena administración y con los mecanismos de supervisión contemplados en el RIA.

7.9. Sostenibilidad social y ambiental y fomento de la confianza pública

La IA debe contribuir al desarrollo sostenible de la ciudad, promoviendo el uso eficiente de recursos, mejorando la gestión de infraestructuras y reduciendo el impacto ambiental asociado a los servicios públicos.

Del mismo modo, la confianza pública debe reforzarse mediante información clara sobre los beneficios, limitaciones y alcances de los sistemas utilizados. Una ciudadanía informada constituye un elemento esencial para asegurar la aceptación y el uso responsable de estas tecnologías en los Smart Cities.

8. Interacción segura con sistemas de IA urbanos

El uso cotidiano de servicios urbanos basados en Inteligencia Artificial implica una relación constante entre la ciudadanía y sistemas automatizados que procesan información, adaptan contenidos y generan recomendaciones. Aunque estos servicios pueden mejorar la eficiencia y la accesibilidad, también exigen atención a aspectos como la protección de datos, la autenticidad de los mensajes, la verificación de permisos y la detección temprana de comportamientos anómalos.

Desde el punto de vista del uso ciudadano, esta interacción con sistemas de IA debe entenderse como una relación continuada y dinámica, en la que los resultados ofrecidos por el servicio pueden variar en función de múltiples factores: datos disponibles, contexto urbano, cambios operativos del sistema o ajustes derivados de su mantenimiento y actualización. Por ello, los resultados automatizados no deben interpretarse como verdades absolutas, sino como apoyos funcionales al servicio público que pueden requerir contraste, validación adicional o intervención humana, especialmente cuando afectan a trámites, prioridades o derechos de la persona usuaria.

El presente capítulo proporciona una guía detallada para identificar, comprender y utilizar de forma segura los servicios municipales que incorporan IA. Incluye orientaciones prácticas, ejemplos habituales y escenarios ilustrativos que ayudan a interpretar correctamente el funcionamiento de estos servicios y a detectar posibles riesgos.

8.1. Identificación de servicios y aplicaciones que utilizan IA

En muchos servicios urbanos la presencia de IA no es evidente. La interfaz puede parecer tradicional, aunque en segundo plano intervengan algoritmos que clasifican información, generan predicciones o automatizan procesos identificados en el capítulo 5. Comprender cuándo se está interactuando con un sistema de este tipo resulta esencial para interpretar sus resultados de manera adecuada.

Desde la perspectiva de la ciudadanía, los sistemas de IA utilizados en entornos de Smart Cities suelen basarse en distintos tipos de algoritmos o técnicas, entre los que destacan:

- **Algoritmos de clasificación**, que ordenan solicitudes, incidencias o contenidos en función de determinados criterios, como prioridad, urgencia o tipología del servicio.
- **Algoritmos predictivos**, que estiman situaciones futuras a partir de datos históricos o en tiempo real, como tiempos de desplazamiento, demanda de servicios o evolución de consumos.
- **Sistemas de recomendación**, que proponen rutas, servicios, contenidos o alternativas personalizadas en función de patrones detectados.
- **Sistemas de análisis de imagen, audio o vídeo**, utilizados para detectar incidencias, eventos o patrones en el espacio urbano mediante cámaras, sensores u otros dispositivos.
- **Modelos conversacionales o asistentes virtuales**, que generan respuestas automáticas en servicios de atención ciudadana, tramitación administrativa o información urbana.

La utilización de uno u otro tipo de sistema determina el tipo de datos tratados, el grado de automatización y el impacto potencial sobre la persona usuaria, por lo que su identificación permite valorar adecuadamente la fiabilidad de los resultados ofrecidos y saber cuándo resulta conveniente solicitar información adicional o una revisión humana.

Indicadores de intervención de IA en servicios municipales:

- El servicio genera recomendaciones personalizadas (rutas, tiempos estimados, prioridades o propuestas automáticas).
- La respuesta del sistema se adapta en función de patrones detectados, horarios, ubicaciones o comportamientos previos.
- La aplicación incorpora asistentes virtuales, chatbots o sistemas de atención automatizada.
- Se analizan imágenes, audio o vídeos para detectar situaciones, vehículos, incidencias o comportamiento en la vía pública.
- El servicio indica la utilización de modelos predictivos, análisis en tiempo real o clasificación automatizada.
- La aplicación solicita permisos que permiten tratamiento continuo de datos (ubicación permanente, acceso a cámara o micrófono).
- El servicio muestra mensajes que incluyen expresiones como “procesamiento automatizado”, “modelo”, “predicción”, “clasificación” o “estimación”.

La siguiente tabla plantea los **escenarios habituales** en los que intervienen la IA:

Servicio urbano	Indicador de IA	Cómo detectarlo la ciudadanía
Aplicaciones de movilidad	Predicción de tiempos, rutas adaptadas	Cambios instantáneos en recomendaciones según tráfico o meteorología
Atención ciudadana digital	Chatbots y asistentes virtuales	Respuestas generadas de forma inmediata y estructurada
Gestión de aparcamientos	Análisis de imágenes	Notificaciones sobre disponibilidad sin intervención humana
Supervisión ambiental	Indicadores automáticos	Avisos generados por sistemas que analizan sensores en tiempo real
Información urbana	Alertas automáticas	Mensajes basados en modelos que analizan datos agregados

TABLA 2: ESCENARIOS HABITUALES EN LOS QUE INTERVIENE IA

8.1.1. Identificación de asistentes virtuales y modelos conversacionales

Los asistentes virtuales son cada vez más comunes en la atención ciudadana. La ciudadanía puede reconocerlos por características como:

- Respuestas inmediatas, sin pausas naturales.
- Estructuras de respuesta homogéneas o repetitivas.
- Dificultad para comprender matices o situaciones particulares.
- Uso de mensajes de tipo “¿Desea ampliar esta información?” o “Seleccione una opción”.

Estos sistemas están diseñados principalmente para resolver consultas frecuentes y estandarizadas. Cuando la consulta plantea situaciones excepcionales, requiere interpretación normativa o afecta de forma significativa a la persona usuaria, la respuesta automatizada debe entenderse como orientativa, siendo aconsejable recurrir a canales de atención humana para obtener una valoración más precisa.

La siguiente tabla demuestra **distintas señales** de que una respuesta proviene de IA:

Indicador	Ejemplo visible	Significado
Respuesta idéntica a preguntas distintas	“Consulte la sede electrónica para más información”	Falta de comprensión del contexto
No responde a preguntas abiertas	Repite el mismo texto	Limitación del sistema
Genera opciones predefinidas	Botones de selección	Proceso automatizado

TABLA 3: SEÑALES DE QUE UNA RESPUESTA PROVIENE DE IA

8.2. Comprensión de avisos, permisos y condiciones de uso

Los servicios basados en IA suelen requerir permisos y mostrar avisos relacionados con el tratamiento de datos, el acceso a sensores del dispositivo y la activación de funciones adicionales. Una correcta interpretación de estos elementos permite utilizar el servicio con mayor seguridad y reducir la exposición a riesgos.

Asimismo, datos recogidos mediante permisos de estos servicios pueden utilizarse no solo para la prestación directa del servicio, sino también para análisis automatizados, clasificaciones o predicciones. Esto puede dar lugar a inferencias adicionales sobre hábitos o patrones de uso, lo que refuerza la importancia de evaluar cuidadosamente cada permiso concedido.

Elementos que requieren especial atención por parte de la ciudadanía

- Permisos de geolocalización, especialmente cuando se solicitan de manera permanente.
- Permisos de cámara, micrófono y sensores del dispositivo, que pueden implicar tratamiento de datos sensibles.
- Solicitudes de activar notificaciones push que pueden incluir recomendaciones automatizadas.
- Avisos sobre toma de decisiones automatizadas, clasificación de solicitudes o priorización automática. Indicaciones sobre reutilización de datos, análisis estadístico o uso de modelos predictivos.

La siguiente tabla presenta ejemplos de permisos y sus implicaciones:

Permiso solicitado	Uso legítimo habitual	Riesgos asociados si se activa sin necesidad
Ubicación “siempre activa”	Estimación continua del transporte	Seguimiento constante de desplazamientos
Acceso a cámara	Lectura de códigos, validación de documentos	Captura accidental de imágenes o datos
Acceso a micrófono	Atención ciudadana por voz	Riesgo de registrar audio involuntario
Notificaciones	Avisos municipales	Exposición a mensajes engañosas si se confunden con avisos falsos.

TABLA 4: EJEMPLOS DE PERMISOS Y SU IMPLICACIÓN

Se recomienda las siguientes buenas prácticas al aceptar permisos:

- Activar únicamente los permisos estrictamente necesarios.
- Revisar periódicamente los permisos activos en el dispositivo.
- Comprobar si existe una opción de “solo durante el uso de la aplicación”.
- Consultar las políticas de privacidad para conocer el destino de los datos.
- Desactivar notificaciones cuando resulten excesivas o irrelevantes.

8.2.1. Comprensión de la toma de decisiones automatizadas

Algunos servicios municipales clasifican solicitudes o priorizan avisos mediante IA por lo que la ciudadanía debe prestar atención a:

- Si la aplicación indica que una respuesta ha sido generada automáticamente.
- Si la decisión tiene impacto relevante (trámites, reclamaciones, tiempos de respuesta).
- Si existen vías visibles para solicitar revisión humana.

Cuando una decisión automatizada produce efectos relevantes sobre la persona usuaria, como la asignación de prioridades, la modificación de plazos o la denegación de un trámite, la ciudadanía tiene derecho a solicitar información adicional y a que la decisión sea revisada por personal humano competente, de acuerdo con las garantías descritas en el capítulo 10.

8.3. Buenas prácticas en el uso seguro de la IA

El uso cotidiano de servicios municipales basados en IA puede gestionarse de manera segura mediante hábitos simples. Estas prácticas complementan, pero no sustituyen, las obligaciones de seguridad y protección que corresponden a las administraciones públicas y a sus proveedores tecnológicos. Su adopción contribuye a reducir riesgos derivados de errores automatizados, incidentes de seguridad o intentos de fraude digital.

Prácticas recomendadas:

- Descargar aplicaciones únicamente desde tiendas oficiales para evitar versiones manipuladas.
- Mantener los dispositivos actualizados para corregir vulnerabilidades de seguridad.
- Comprobar que el servicio dispone de un canal oficial asociado (sede electrónica, web municipal o app certificada).
- Evitar facilitar más datos personales de los necesarios para el funcionamiento del servicio.
- Revisar la coherencia de las respuestas automatizadas antes de actuar en función de ellas.
- Confirmar la información relevante mediante fuentes institucionales independientes cuando existan dudas.
- Configurar las notificaciones de forma que solo se reciban avisos esenciales.

Situación	Acción recomendada	Motivo
La aplicación pide ubicación permanente	Seleccionar “solo al usar la app”	Evita seguimiento continuo no necesario
El chatbot municipal da una respuesta incoherente	Revisar la información en la web oficial	Evita actuar en base a un error automatizado
Se recibe un aviso extraño sobre tráfico o emergencias	Contrastar con la web o redes oficiales	Evita caer en avisos falsos generados por IA
La app instala una actualización inesperada	Revisar la tienda oficial	Previene instalar modificaciones fraudulentas

TABLA 5: EJEMPLOS DE USO SEGURO EN SITUACIONES COMUNES

8.3.1. Interacción segura con asistentes virtuales

Los asistentes virtuales pueden resolver consultas, pero es conveniente tomar en consideración:

- Que su información puede no estar actualizada al minuto.
- Que pueden interpretar de forma literal algunas consultas.
- Que no deberían gestionarse a través de ellos trámites complejos.

La siguiente tabla señala las interacciones que requieren precaución por parte de la ciudadanía:

Tipo de consulta	Riesgo	Recomendación
Trámites sensibles	Respuesta incompleta o errónea	Solicitar atención humana

Tipo de consulta	Riesgo	Recomendación
Problemas urgentes	Retrasos del sistema	Acceder a teléfonos oficiales
Información contradictoria	Error del modelo	Confirmar en portal municipal

TABLA 6: INTERACCIONES QUE REQUIEREN PRECAUCIÓN

8.4. Detección de señales de alerta y actuación ante incidencias

La ciudadanía puede detectar indicios de funcionamiento anómalo, intentos de fraude o manipulación en aplicaciones que integran IA. Cuando las señales de alerta afectan a datos personales, a la autenticidad de comunicaciones institucionales o al acceso a servicios esenciales, resulta aconsejable no limitarse a la cautela individual, sino activar los canales de verificación y notificación previstos por la administración.

Las señales de alerta más frecuentes incluyen:

- Mensajes o notificaciones que simulan ser oficiales, pero presentan errores tipográficos, tonalidades atípicas o enlaces para acceder a una página web externa.
- Resultados automatizados que no se corresponden con la realidad o muestran contradicciones evidentes.
- Cambios bruscos en la aplicación que no han sido comunicados por canales oficiales.
- Solicitudes inesperadas de datos personales, comprobación de cuentas o permisos adicionales.
- Recomendaciones que generan presión, urgencia o instrucciones poco razonables.

La siguiente tabla plantea los distintos escenarios de alerta y posible interacción:

Señal de alerta	Posible causa	Interpretación recomendada
Aviso urgente pidiendo datos personales	Intento de fraude digital	Ignorar y verificar en canal oficial
Cambio repentino en la interfaz	Actualización no legítima	Cerrar app y verificar proveedor
Estimaciones absurdas o contradictorias	Error del sistema de IA	Solicitar revisión o consultar al servicio
Enlaces a páginas similares, pero no oficiales	Suplantación	Acceder manualmente a la web del ayuntamiento

TABLA 7: ESCENARIOS DE ALERTA Y POSIBLE INTERPRETACIÓN

Cómo actuar ante una incidencia:

- Verificar la información en canales oficiales: web del ayuntamiento, sede electrónica o teléfono de atención ciudadana.
- Interrumpir el uso de la aplicación si persisten los comportamientos sospechosos.
- Notificar la incidencia a los servicios municipales responsables.
- Evitar compartir información personal o pulsar enlaces incluidos en mensajes dudosos.
- Documentar la incidencia mediante capturas o anotaciones.

8.5. Casos prácticos

Estos casos prácticos tienen un carácter ilustrativo y muestran cómo situaciones cotidianas pueden implicar la intervención de sistemas de IA. Ante escenarios no contemplados expresamente, se recomienda aplicar los criterios generales expuestos en este capítulo y recurrir a los canales oficiales descritos en el capítulo 10.

I. Caso 1: Mensaje que solicita datos personales por mensajería instantánea

Una persona recibe un mensaje a través de una aplicación de mensajería instantánea que incluye el logotipo del ayuntamiento y solicita el envío del documento nacional de identidad para verificar un supuesto trámite administrativo pendiente.

Este tipo de comunicaciones suele corresponder a intentos de fraude o suplantación de identidad, en los que se imita deliberadamente la apariencia de mensajes institucionales legítimos. En muchos casos, estos mensajes utilizan contenidos generados o adaptados mediante herramientas de inteligencia artificial para reproducir con mayor realismo el lenguaje, el formato y los elementos visuales empleados por las administraciones públicas.

El riesgo para la ciudadanía es elevado, ya que la cesión de datos personales sensibles, como documentos de identidad, puede dar lugar a situaciones de robo de identidad, acceso indebido a servicios digitales, apertura fraudulenta de trámites administrativos o uso ilícito de la información en otros contextos. Este tipo de fraudes suele aprovechar la urgencia aparente del mensaje y la confianza que generan los símbolos institucionales.

Como actuar:

- La persona usuaria no debe responder al mensaje ni facilitar datos personales, documentos o credenciales a través de aplicaciones de mensajería instantánea no verificadas.
- Debe evitar pulsar enlaces incluidos en la comunicación, ya que pueden redirigir a sitios web fraudulentos diseñados para recopilar información personal.
- Resulta recomendable acceder siempre por iniciativa propia a la web oficial del ayuntamiento o a la sede electrónica para comprobar si existe realmente algún aviso o trámite pendiente.
- Como alternativa segura, la persona usuaria puede contactar directamente con los servicios de atención ciudadana del ayuntamiento por teléfono o acudir de forma presencial a una oficina municipal para verificar la situación del trámite con personal autorizado.
- En caso de duda o sospecha, la persona usuaria debe comunicar el intento de fraude a los servicios municipales correspondientes o a los organismos de ciberseguridad competentes, como INCIBE, con el fin de facilitar su detección y prevención.

II. Caso 2: Asistente virtual que repite respuestas genéricas

Una persona usuaria accede al servicio de atención ciudadana digital del ayuntamiento para realizar una consulta sobre un trámite administrativo concreto que presenta una circunstancia particular. El asistente virtual responde con un mensaje estándar que remite a información general. Tras reformular la consulta para aclarar el caso específico, el sistema ofrece exactamente la misma respuesta, sin incorporar matices ni adaptarse a la situación descrita.

Este tipo de comportamiento suele producirse cuando el asistente virtual está diseñado para resolver únicamente consultas frecuentes o altamente estandarizadas y no dispone de capacidad para interpretar excepciones normativas, situaciones personales complejas o combinaciones de requisitos no habituales. En estos casos, el sistema aplica patrones predefinidos y devuelve respuestas genéricas, aunque no resulten útiles para el caso planteado.

El principal riesgo para la ciudadanía es interpretar la respuesta automatizada como definitiva o vinculante, lo que puede dar lugar a errores en la tramitación, a la presentación incorrecta de documentación o al abandono del procedimiento por frustración. También existe el riesgo de que la persona usuaria retrase innecesariamente un trámite relevante al confiar en una respuesta que no refleja adecuadamente su situación.

Cómo actuar:

- La persona usuaria debe evitar insistir de forma reiterada en el asistente virtual cuando la respuesta no varía ni se adapta tras reformular la consulta.
- Debe contrastar la información recibida con la publicada en la sede electrónica, las bases reguladoras del trámite o la documentación oficial disponible en los canales municipales.
- Cuando el trámite tenga consecuencias relevantes o implique situaciones personales específicas, resulta recomendable contactar con los servicios de atención ciudadana para solicitar atención humana, ya sea por vía telefónica, telemática o presencial.
- En caso de persistir la duda, la persona usuaria debe priorizar siempre la información facilitada por personal municipal autorizado frente a la respuesta generada por el sistema automatizado.

Este caso pone de manifiesto que los asistentes virtuales son herramientas útiles para orientar y agilizar consultas básicas, pero no sustituyen la atención humana ni el análisis individualizado necesario en trámites administrativos que presentan particularidades o impacto significativo para la ciudadanía.

III. Caso 3: Notificación municipal con enlace a una plataforma aparentemente oficial

Una persona usuaria recibe un correo electrónico o una notificación digital que aparenta proceder de un servicio municipal y que le invita a acceder a una plataforma en línea para consultar una notificación, actualizar datos o completar un trámite pendiente. El mensaje utiliza un lenguaje formal, incluye referencias a servicios municipales reales y contiene un enlace que dirige a una página web visualmente similar a la sede electrónica del ayuntamiento.

Al acceder al enlace, la página solicita introducir credenciales, datos personales o información de identificación para continuar con el proceso.

Este tipo de situaciones puede corresponder a campañas de suplantación digital en las que se recrea de forma muy precisa la apariencia de plataformas institucionales legítimas. En muchos casos, se utilizan

técnicas avanzadas de diseño y contenidos generados o ajustados mediante herramientas de inteligencia artificial para reproducir textos, logotipos y estructuras habituales de los servicios públicos digitales.

El riesgo para la ciudadanía es significativo, ya que la introducción de credenciales o datos personales en estas plataformas falsas puede permitir a terceros acceder a cuentas reales, iniciar trámites sin consentimiento, modificar información personal o utilizar los datos obtenidos para fraudes posteriores. Además, este tipo de ataques suele dirigirse de forma masiva y selectiva, aprovechando momentos de alta actividad administrativa.

Cómo actuar:

- La persona usuaria debe evitar acceder a enlaces incluidos en mensajes o notificaciones digitales cuando no haya iniciado previamente ningún trámite o cuando existan dudas razonables sobre su autenticidad.
- Debe comprobar cuidadosamente la dirección web antes de introducir cualquier dato, verificando que corresponde exactamente al dominio oficial del ayuntamiento o de la sede electrónica.
- Como medida preventiva, se recomienda acceder siempre a los servicios municipales escribiendo manualmente la dirección web oficial en el navegador, en lugar de utilizar enlaces recibidos por correo o mensajería.
- Si ya se han introducido datos por error, la persona usuaria debe cambiar inmediatamente sus credenciales y contactar con el servicio municipal correspondiente para informar de la posible incidencia.
- En caso de sospecha, debe comunicarse el intento de suplantación a los servicios municipales y a los organismos de ciberseguridad competentes, con el fin de facilitar la detección y protección de otras personas usuarias.

Este caso pone de relieve la importancia de extremar las precauciones en el acceso a servicios digitales municipales y de no confiar únicamente en la apariencia visual de una plataforma, ya que las técnicas de suplantación digital pueden reproducir con gran fidelidad los entornos oficiales.

9. Medidas de autoprotección del usuario final

El uso de servicios urbanos que incorporan Inteligencia Artificial puede gestionarse de forma mucho más segura si la ciudadanía adopta ciertas pautas sencillas y constantes. Estas medidas no requieren conocimientos técnicos avanzados, pero sí una actitud atenta ante el funcionamiento de las aplicaciones y ante el tipo de información que se comparte en los entornos digitales municipales. El objetivo de este capítulo es ofrecer un conjunto de recomendaciones prácticas que ayuden a proteger la privacidad, reducir la exposición a incidentes de seguridad, identificar posibles errores automatizados y evitar la difusión de contenidos falsos o manipulados.

9.1. Protección de la privacidad y de la información personal

La privacidad es uno de los elementos más sensibles en los servicios que integran IA, ya que su funcionamiento suele basarse en el análisis de datos. La ciudadanía puede reforzar su protección mediante las siguientes prácticas:

- ✓ Revisar con regularidad los permisos que tienen las aplicaciones instaladas en el dispositivo, en especial aquellos vinculados a la geolocalización, la cámara, el micrófono o el acceso a archivos. Muchos servicios funcionan correctamente con permisos mínimos.
- ✓ Comprobar si una aplicación necesita realmente acceso constante a la ubicación. Cuando sea posible, resulta aconsejable seleccionar la opción de permitir la localización únicamente durante el uso del servicio.
- ✓ Evitar introducir información personal en campos que no son obligatorios. En muchos casos, los formularios de servicios digitales admiten completar el trámite sin proporcionar datos adicionales.
- ✓ Consultar las políticas de privacidad de los servicios municipales y, cuando exista duda sobre el tratamiento de datos, solicitar información a través de los canales oficiales o al Delegado de Protección de Datos.
- ✓ Eliminar periódicamente las aplicaciones que ya no se utilizan, reducir el número de cuentas activas y revisar los historiales almacenados en las plataformas municipales.

Estas pautas contribuyen a minimizar la cantidad de datos expuestos y a mantener un mayor control sobre la información personal que utilizan los sistemas de IA.

9.2. Seguridad digital y prevención del fraude

El uso seguro de los servicios urbanos requiere adoptar medidas básicas de protección del dispositivo y de precaución ante intentos de fraude o suplantación de identidades. Entre las recomendaciones más relevantes se encuentran:

- ✓ Mantener el dispositivo actualizado con las últimas versiones del sistema operativo y de las aplicaciones instaladas. Las actualizaciones suelen corregir vulnerabilidades que pueden ser explotadas.

- ✓ Descargar las aplicaciones únicamente desde tiendas oficiales y comprobar que el proveedor es legítimo. Esto reduce el riesgo de instalar aplicaciones fraudulentas.
- ✓ Utilizar contraseñas seguras y diferentes para los distintos servicios, así como activar la verificación en dos pasos cuando esté disponible.
- ✓ Evitar pulsar enlaces incluidos en mensajes inesperados, aunque aparenten proceder del ayuntamiento. Cuando la duda sea razonable, acceder directamente a la web municipal sin utilizar el enlace recibido.
- ✓ Verificar siempre la autenticidad de los perfiles de redes sociales que difunden información municipal, ya que algunos intentos de fraude utilizan nombres, logotipos o estilos visuales similares a los oficiales.

Estas medidas permiten reducir significativamente la probabilidad de que la persona usuaria sea víctima de una suplantación, un acceso indebido o una manipulación de información.

9.3. Identificación de posibles sesgos o decisiones inapropiadas

Los sistemas de IA pueden ofrecer resultados que no se ajustan adecuadamente a la realidad de la persona usuaria. Aunque la ciudadanía no tiene obligación de conocer los detalles técnicos de estos sistemas, sí puede identificar indicios de posibles errores o desviaciones.

Entre los signos que pueden sugerir un funcionamiento incorrecto se encuentran:

- ✓ Recomendaciones o respuestas que parecen incoherentes con la situación real o que contradicen información fiable disponible por otras vías.
- ✓ Solicitudes clasificadas de manera inesperada, especialmente cuando tengan repercusiones en la atención prioritaria o en la tramitación de procedimientos.
- ✓ Resultados que parecen repetirse o asignarse de manera idéntica a situaciones diferentes, lo que podría indicar una falta de adaptación del sistema.
- ✓ Percepción de un trato desigual que no encuentra explicación en la normativa o en las reglas del servicio.

Ante estos casos, se recomienda solicitar una revisión humana del trámite o plantear una consulta al servicio responsable para que se compruebe el funcionamiento del sistema. La administración está obligada a atender estas solicitudes y a revisar cualquier resultado que pueda haber sido generado de forma inadecuada.

9.4. Verificación de contenidos sintéticos y prevención de la desinformación

La proliferación de contenidos generados mediante IA, especialmente aquellos que imitan comunicaciones institucionales, exige nuevas precauciones por parte de la ciudadanía. Para evitar la difusión de desinformación, pueden adoptarse las siguientes medidas:

- ✓ Comprobar que los avisos, imágenes o vídeos proceden de canales oficiales. Los servicios municipales suelen publicar la misma información en su web, aplicaciones oficiales o perfiles verificados.

- ✓ Evitar difundir mensajes que generen alarma sin haber contrastado previamente su autenticidad.
- ✓ Revisar el lenguaje, el formato y la dirección web vinculada al contenido. Los mensajes falsos suelen contener detalles que difieren de los comunicados oficiales.
- ✓ Consultar diversos medios institucionales cuando la información tenga impacto relevante, como en situaciones de emergencia, cortes de servicios o recomendaciones de seguridad.

Esta verificación inicial ayuda a limitar la propagación de contenidos falsos y contribuye a mantener un entorno informativo más seguro.

9.5. Accesibilidad y reducción de barreras digitales

El uso de la IA puede facilitar el acceso a la información urbana, pero también puede generar dificultades para determinadas personas. Para garantizar un uso adecuado, se recomienda:

- ✓ Utilizar las funciones de accesibilidad del dispositivo, como el aumento de texto, la lectura en voz alta o los contrastes de color, que pueden mejorar la experiencia en aplicaciones municipales.
- ✓ Solicitar asistencia presencial en oficinas municipales cuando el uso de una aplicación resulte complejo, especialmente en trámites que requieran precisión o documentos específicos.
- ✓ Consultar las guías públicas sobre competencias digitales o servicios de apoyo ofrecidos por administraciones locales o autonómicas.
- ✓ Elegir canales no digitales cuando existan dificultades persistentes con los servicios automatizados. La administración debe garantizar vías alternativas.

Estas medidas permiten que un mayor número de personas pueda utilizar los servicios urbanos de forma autónoma y segura.

10. Derechos y garantías de la ciudadanía en el uso de sistemas de IA en Smart Cities

Este capítulo presentará, de manera clara, accesible y alineada con el marco normativo europeo y nacional, los derechos de las personas cuando interactúan, directa o indirectamente, con sistemas de inteligencia artificial en entornos urbanos. Su objetivo es que las personas usuarias conozcan qué pueden exigir, cómo puede defender sus derechos, qué garantías existen y qué obligaciones tienen las administraciones y proveedores tecnológicos para asegurar un uso responsable, seguro y transparente de los sistemas de inteligencia artificial.

Los derechos recogidos se derivan principalmente del Reglamento Europeo de Inteligencia Artificial (Reglamento (UE) 2024/1689), el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 (LOPDGDD), el Esquema Nacional de Seguridad (ENS), la Directiva NIS2 y la Carta de Derechos Digitales en España.

10.1. Derechos derivados del RGPD y la LOPDGDD

Las personas usuarias mantienen plenamente sus derechos sobre el tratamiento de sus datos personales cuando estos son procesados por sistemas de IA urbanos, incluyendo:

- Derecho de información: conocer quién trata los datos, con qué finalidad, durante cuánto tiempo y qué bases jurídicas legitiman el tratamiento.
- Derecho de acceso: solicitar qué datos personales se están tratando el sistema de IA, de dónde proceden, con qué fines y quiénes pueden recibirlos.
- Derecho de rectificación: solicitar la corrección de datos inexactos o incompletos.
- Derecho de supresión (“derecho al olvido”), cuando proceda según el artículo 17 del RGPD
- Derecho de oposición al tratamiento de los datos personales, especialmente cuando se base en intereses públicos o intereses legítimos.
- Derecho a no ser objeto de decisiones individuales automatizadas sin las debidas garantías, conforme al artículo 22 del RGPD.
- Derecho a la portabilidad de los datos, cuando el tratamiento se base en el consentimiento o en un contrato y se realice por medios automatizados.
- Derecho a solicitar intervención humana en decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente a la persona

Estos derechos son obligatorios y exigibles para cualquier responsable o encargado del tratamiento que utilice datos personales en servicios urbanos apoyados en sistemas de inteligencia artificial.

10.2. Garantías en el marco del Reglamento Europeo de Inteligencia Artificial (RIA)

El Reglamento Europeo de Inteligencia Artificial (AI Act) establece obligaciones para los proveedores y usuarios de sistemas de IA, que se traducen en garantías y salvaguardas para las personas afectadas.

Entre estas garantías destacan:

- **Transparencia al interactuar con sistemas de IA**

Las personas deben ser informadas de forma clara cuando interactúan con un sistema de inteligencia artificial, especialmente en asistentes virtuales, sistemas conversacionales o servicios automatizados.

- **Identificación de contenidos generados o manipulados mediante IA**

Se debe indicar de forma clara cuando un contenido (texto, audio, imagen o vídeo) ha sido generado o manipulado por IA, y cuando se utilicen sistemas de detección biométrica, según los requisitos de transparencia establecidos en el AI Act.

- **Explicaciones adecuadas sobre sistemas de alto riesgo**

Las personas tienen la garantía de recibir explicaciones adecuadas y comprensibles sobre el funcionamiento de sistemas de IA clasificados como de alto riesgo que les afecten, conforme a lo establecido en los artículos 13 y 50 del Reglamento.

- **Supervisión humana significativa y posibilidad de revisión**

En sistemas de alto riesgo, debe existir supervisión humana significativa. Las personas pueden solicitar revisión cuando una decisión automatizada produzca efectos jurídicos o afecte de manera relevante a su situación.

- **Información sobre los riesgos y limitaciones de los sistemas**

Cuando se empleen sistemas de IA de alto riesgo, las personas tienen derecho a recibir información relevante sobre los riesgos conocidos del sistema, sus limitaciones y las salvaguardas aplicadas.

- **Protección frente al uso de sistemas prohibidos**

Las administraciones públicas y proveedores municipales no pueden desplegar sistemas de IA prohibidos, como el reconocimiento biométrico en tiempo real en espacios públicos sin la habilitación legal expresa que exige el Reglamento.

- **Cumplimiento de requisitos mínimos de seguridad y gobernanza**

Las personas usuarias tienen la garantía de que los sistemas de IA utilizados en servicios urbanos cumplen los requisitos mínimos de seguridad, gobernanza, supervisión, gestión de riesgos y calidad establecidos en el AI Act.

10.3. Garantías en materia de ciberseguridad (NIS2 y ENS)

Los ciudadanos también están protegidos por los marcos de ciberseguridad aplicables al sector público y a los servicios esenciales.

10.3.1. Garantías derivadas del Esquema Nacional de Seguridad (ENS)

El ENS, de obligatorio cumplimiento en todas las administraciones públicas españolas y en sus proveedores tecnológicos, establece medidas que protegen los sistemas de información que soportan los servicios digitales municipales.

- **Garantía de integridad, disponibilidad y autenticidad de los servicios digitales**

Los servicios municipales basados en IA deben mantenerse operativos, fiables y protegidos frente a accesos o alteraciones indebidas.

- **Garantía de confidencialidad y protección de los datos**

Las administraciones y proveedores deben aplicar controles para evitar accesos no autorizados y asegurar que los datos se gestionan de manera segura en todo su ciclo de vida.

- **Garantía de trazabilidad y registro de actividad**

El Esquema Nacional de Seguridad exige la conservación de registros de las operaciones relevantes de los sistemas de información, incluidos aquellos que incorporan inteligencia artificial, con el fin de permitir la detección de incidentes, la investigación de accesos indebidos y la supervisión y revisión efectiva de los servicios digitales.

- **Gestión rápida y diligente de incidentes de seguridad**

Las entidades públicas deben detectar, comunicar y corregir incidentes de seguridad de forma coordinada, reduciendo al mínimo el impacto sobre la ciudadanía.

10.3.2. Garantías derivadas de la Directiva NIS2

La Directiva NIS2 refuerza los requisitos de seguridad en operadores de servicios esenciales y administraciones públicas, muchos de los cuales se integran en el funcionamiento de una Smart City.

Para las personas usuarias, esto implica:

- **Garantía de que los operadores aplican medidas avanzadas de ciberseguridad**

Incluyen gestión de vulnerabilidades, análisis de riesgos, medidas de protección de redes y continuidad de negocio.

- **Notificación proporcionada de incidentes relevantes**

Cuando un incidente afecta o puede afectar a la disponibilidad, integridad o continuidad de un servicio esencial, las entidades deben comunicarlo de manera adecuada y ofrecer recomendaciones a la ciudadanía cuando sea necesario.

- **Garantía de ciberresiliencia y recuperación ante ataques**

Las organizaciones cubiertas por NIS2 deben disponer de capacidades para recuperar la normalidad y garantizar la continuidad de los servicios urbanos tras un incidente o ataque.

10.4. Canales para ejercer derechos

Para que la ciudadanía pueda ejercer sus derechos o resolver dudas relacionadas con el uso de sistemas de inteligencia artificial en servicios urbanos, es esencial disponer de canales claros, accesibles y oficiales. Estos canales permiten gestionar reclamaciones, solicitar información, ejercer derechos de protección de datos o recibir asistencia ante incidentes de seguridad.

Los canales disponibles son los siguientes:

- **Delegado o delegada de Protección de Datos del Ayuntamiento (DPD)**

Es el punto de contacto para ejercer derechos reconocidos por el RGPD y la LOPDGDD:

- Acceso, rectificación, supresión, oposición y portabilidad;
- Consulta sobre tratamientos de datos realizados mediante sistemas de ia;
- Reclamaciones relacionadas con el uso de datos personales en servicios municipales.

El DPD debe responder de forma clara y en los plazos establecidos por la normativa.

- **Ayuntamiento o entidad titular del servicio digital**

Para cuestiones relacionadas con:

- El funcionamiento de un sistema de IA municipal,
- Dudas sobre permisos, decisiones automatizadas o procesos digitales,
- Incidencias relacionadas con el acceso o uso del servicio digital.

Este canal permite resolver cuestiones prácticas o realizar reclamaciones directamente con el responsable del servicio.

- **Autoridad Española de Protección de Datos (AEPD)**

Es la autoridad encargada de supervisar y garantizar los derechos en materia de protección de datos. La ciudadanía puede acudir a la AEPD para:

- Presentar una reclamación cuando considere vulnerados sus derechos;
- Informar sobre tratamientos indebidos de datos personales;

- Recibir orientación para el ejercicio de derechos rgpd.
- Este canal es complementario y no sustituye al dpd municipal.

- **AESIA (Agencia Española de Supervisión de la Inteligencia Artificial)**

Cuando esté plenamente operativa, AESIA será responsable de:

- Supervisar el cumplimiento del AI Act en España,
- Atender consultas sobre sistemas de inteligencia artificial de alto riesgo,
- Recoger información o denuncias sobre el uso indebido de IA en administraciones o empresas.

El alcance detallado de sus funciones se desplegará progresivamente conforme avance la implantación del Reglamento Europeo de IA.

- **INCIBE y organismos autonómicos de ciberseguridad**

La ciudadanía puede dirigirse a INCIBE-CERT o a los centros autonómicos de ciberseguridad para:

- Obtener asistencia ante incidentes que afecten a dispositivos personales,
- Reportar fraudes digitales, suplantaciones o intentos de phishing,
- Recibir recomendaciones para mejorar la seguridad digital en el uso de servicios urbanos.

Además, INCIBE ofrece atención telefónica a través del número 017 y/o soporte online.

- **Oficinas municipales de atención ciudadana**

Para garantizar la accesibilidad y evitar la exclusión digital, las personas usuarias pueden realizar consultas o ejercer derechos de manera presencial. Estas oficinas permiten:

- Tramitar solicitudes cuando la persona no tiene acceso a medios digitales,
- Obtener asistencia para el uso de servicios electrónicos o aplicaciones municipales,
- Facilitar el ejercicio de derechos para colectivos con dificultades tecnológicas.

11. Referencias

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act).
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>
- Reglamento (UE) 2016/679 (RGPD), de 27 de abril de 2016, relativo a la protección de datos personales.
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Directiva (UE) 2022/2555 (NIS2), relativa al nivel elevado común de ciberseguridad en la Unión.
<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- Reglamento (UE) 2022/868 (Data Governance Act) sobre la gobernanza europea de datos.
<https://eur-lex.europa.eu/eli/reg/2022/868/oj>
- Reglamento (UE) 2022/2065 (Digital Services Act – DSA) sobre servicios digitales.
<https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- Ley Orgánica 3/2018 (LOPDGDD), de Protección de Datos Personales y garantía de los derechos digitales.
<https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>
- Esquema Nacional de Seguridad (ENS) – Real Decreto 311/2022, de 3 de mayo.
<https://www.boe.es/eli/es/rd/2022/05/03/311>
- Carta de Derechos Digitales (Gobierno de España, 2021).
https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/Carta_Derechos_Digitales.pdf
- NIST AI Risk Management Framework 1.0 (2023).
<https://www.nist.gov/itl/ai-risk-management-framework>
- ISO/IEC 42001:2023 – AI Management System.
<https://www.iso.org/standard/81230.html>
- ISO/IEC 23894:2023 – AI Risk Management.
<https://www.iso.org/standard/77304.html>
- ISO/IEC 38507:2022 – Governance implications of AI.
<https://www.iso.org/standard/80382.html>
- ISO/IEC 27001:2022 – Information security management systems.

<https://www.iso.org/standard/82875.html>

- ISO 31000:2018 – Risk management guidelines.
<https://www.iso.org/standard/65694.html>
- ISO/IEC 30111:2019 – Vulnerability handling processes.
<https://www.iso.org/standard/69725.html>
- ISO/IEC 25012:2014 – Data quality model.
<https://www.iso.org/standard/35736.html>
- ISO 37120 / 37122 / 37123 – Sustainable and smart cities indicators.
<https://www.iso.org/committee/656906.html>
- UNE 178104:2017 – Interoperabilidad de plataformas de ciudad inteligente.
<https://www.aenor.com/norma-une-178104-2017-n0058578>
- UNE 178108:2017 – Gestión inteligente de activos urbanos.
<https://www.aenor.com/norma-une-178108-2017-n0058579>
- UNE 178301:2015 – Sistema de indicadores y métricas para ciudades inteligentes.
<https://www.aenor.com/norma-une-178301-2015-n0056687>
- UNE 178503:2019 – Destinos turísticos inteligentes.
<https://www.aenor.com/norma-une-178503-2019-n0060196>
- UNE-EN 301549:2022 – Accesibilidad de productos y servicios TIC.
<https://www.aenor.com/norma-une-en-301549-2022-n0062490>

12. 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.

12.1. Lista de materias tratadas en la guía

- Uso de sistemas de Inteligencia Artificial en los servicios públicos urbanos y en el entorno de las Smart Cities.
- Funcionamiento general de los sistemas de IA y sus principales tipos desde una perspectiva orientada a la ciudadanía.
- Los marcos normativos aplicables a la inteligencia artificial, la protección de datos personales y la ciberseguridad en el ámbito del sector público y estándares internacionales de uso responsable de Inteligencia artificial.
- Ámbitos de aplicación de la IA en movilidad, energía, medio ambiente urbano, seguridad, atención ciudadana, participación digital y turismo inteligente.
- Riesgos y desafíos asociados al uso de sistemas de IA para la ciudadanía, incluyendo privacidad, seguridad digital, sesgos algorítmicos, transparencia, explicabilidad y accesibilidad.
- Principios de uso responsable, seguro y respetuoso con los derechos fundamentales en los servicios urbanos basados en IA.
- Interacción segura de la ciudadanía con sistemas automatizados y plataformas digitales municipales que incorporen o emplean el uso de inteligencia artificial.
- Identificación de señales de alerta, detección de intentos de fraude digital y actuación ante incidencias relacionadas con sistemas de IA.
- Medidas de autoprotección del usuario final en materia de privacidad, ciberseguridad, verificación de información y uso responsable de servicios digitales.
- Derechos y garantías de la ciudadanía en relación con el tratamiento de datos personales, la toma de decisiones automatizadas y la supervisión humana.
- Canales institucionales disponibles para el ejercicio de derechos, la solicitud de información y la comunicación de incidencias.

12.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

12.3. Lista de servicios mencionados en la guía

- Servicios municipales de movilidad y transporte inteligente.
- Plataformas de atención ciudadana digital y tramitación administrativa electrónica.
- Servicios de gestión energética, agua y medio ambiente urbano.
- Sistemas de seguridad urbana y gestión de emergencias.
- Plataformas de participación ciudadana y consulta pública.
- Servicios de turismo inteligente y contenidos culturales digitales.

Uso responsable y seguro de sistemas de IA en Smart Cities para usuarios finales

Noviembre de 2025

Versión 1.0



Junta de Andalucía