RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Cláusulas de seguridad para contratación pública de tecnología de IA en el entorno de Smart Cities

Enero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

"ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD 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: 15/01/2026

Fecha de última actualización: 06/02/2026

ÍNDICE DE CONTENIDOS

1. Introducción 7
2. Objetivo y alcance 8
   2.1. Objetivo 8
   2.2. Alcance 8
3. Referencias normativas 10
4. Definiciones 12
5. Instrucciones de uso 16
6. Tipologías de proveedores de tecnologías de IA en Smart Cities 18
   6.1. Proveedores de soluciones de IA 18
   6.2. Proveedores de plataformas y servicios de IA 19
   6.3. Proveedores mixtos 20
   6.4. Prestadores de servicios de integración, operación y soporte de soluciones de IA 21
   6.5. Proveedores de datos y servicios de preparación de datos para IA 22
   6.6. Consideraciones generales sobre la tipología de proveedores 23
7. Cláusulas de seguridad, gobernanza y control para sistemas de IA en el entorno de Smart Cities 24
   7.1. D_01 Gobernanza del sistema de IA urbano 24
      7.1.1. C_01_01 Marco formal de responsabilidades 24
      7.1.2. C_01_02 Política de gobernanza del sistema de IA 25
      7.1.3. C_01_03 Mecanismo estructurado de supervisión 25
   7.2. D_02 Clasificación del sistema de IA y determinación del nivel de riesgo conforme al RIA 25
      7.2.1. C_02_01 Determinación y documentación de la clasificación en base al RIA 26
      7.2.2. C_02_02 Identificación de roles conforme al RIA 26
      7.2.3. C_02_03 Ajuste de obligaciones al nivel de riesgo y a los roles 26
      7.2.4. C_02_04 Verificación de ausencia de prácticas prohibidas 27
   7.3. D_03 Cumplimiento normativo y regulatorio 27
      7.3.1. C_03_01 Alineamiento con la normativa aplicable 27
      7.3.2. C_03_02 Evidencias de conformidad 28
      7.3.3. C_03_03 Gestión de la cadena de suministro y subcontratación 28
   7.4. D_04 Gestión documental y evidencias de cumplimiento 28
      7.4.1. C_04_01 Documentación técnica y funcional del sistema de IA 29

7.4.2. C_04_02 Registro de cambios y evidencias de pruebas 29
7.5. D_05 Gestión integral de riesgos del sistema de IA 29
7.5.1. C_05_01 Proceso de gestión de riesgos 30
7.6. D_06 Evaluación de impacto en derechos fundamentales 30
7.6.1. C_06_01 Colaboración en evaluaciones de impacto en derechos fundamentales 30
7.7. D_07 Gobernanza del dato urbano para IA 31
7.7.1. C_07_01 Marco de gobernanza del dato para el sistema de IA 31
7.7.2. C_07_02 Ciclo de vida de los datos utilizados por el sistema de IA 31
7.8. D_08 Calidad, representatividad y mitigación de sesgos en datos 32
7.8.1. C_08_01 Evaluación de calidad y representatividad de los datos 32
7.8.2. C_08_02 Identificación y mitigación de sesgos en los datos 32
7.9. D_09 Protección de datos personales y minimización 32
7.9.1. C_09_01 Principio de minimización y limitación de la finalidad 33
7.9.2. C_09_02 Seudonimización, anonimización y medidas de protección 33
7.9.3. C_09_03 Localización de datos y transferencias internacionales 33
7.10. D_10 Restricciones de uso, reutilización y reentrenamiento con datos municipales 34
7.10.1. C_10_01 Uso de los datos limitado al objeto del contrato 34
7.10.2. C_10_02 Condiciones para el reentrenamiento con datos municipales 34
7.11. D_11 Gestión de identidades, accesos y mantenimiento remoto 34
7.11.1. C_11_01 Control de acceso basado en roles y mínimo privilegio 35
7.11.2. C_11_02 Gestión del ciclo de vida de identidades y cuentas técnicas 35
7.11.3. C_11_03 Autenticación reforzada y acceso remoto de mantenimiento 35
7.12. D_12 Configuración segura y hardening de entornos de IA 36
7.12.1. C_12_01 Configuración inicial segura del sistema de IA 36
7.12.2. C_12_02 Desactivación de servicios, puertos y funciones innecesarias 36
7.13. D_13 Seguridad de comunicaciones, APIs y cifrado 36
7.13.1. C_13_01 Comunicaciones seguras entre el sistema de IA y otros sistemas 37
7.13.2. C_13_02 Protección de APIs y microservicios del sistema de IA 37
7.13.3. C_13_03 Gestión segura de claves, certificados y secretos 37
7.14. D_14 Gestión de vulnerabilidades y dependencias 37
7.14.1. C_14_01 Proceso de gestión de vulnerabilidades y dependencias 38
7.14.2. C_14_02 Aplicación de parches y mitigación de vulnerabilidades 38
7.15. D_15 Registro, auditoría y trazabilidad técnica 38

7.15.1. C_15_01 Generación y conservación de registros de actividad 38
7.15.2. C_15_02 Integridad y acceso a los registros 39
7.16. D_16 Continuidad operativa y modo degradado sin IA 39
7.16.1. C_16_01 Integración del sistema de IA en los planes de continuidad 39
7.16.2. C_16_02 Definición de modo degradado y operación sin IA 39
7.17. D_17 Seguridad en servicios cloud e IA como servicio 40
7.17.1. C_17_01 Requisitos de seguridad para servicios cloud e IAaaS 40
7.17.2. C_17_02 Monitorización y acceso a registros (logs) en entornos cloud 40
7.18. D_18 Gestión del ciclo de vida y versionado del modelo 40
7.18.1. C_18_01 Control de versiones de los modelos de IA 41
7.18.2. C_18_02 Mecanismos de reversión (rollback) de modelos 41
7.19. D_19 Validación previa al despliegue y tras cambios 41
7.19.1. C_19_01 Validación inicial antes de la puesta en producción 42
7.19.2. C_19_02 Validación tras cambios significativos o reentrenamientos 42
7.20. D_20 Monitorización del modelo en producción 42
7.20.1. C_20_01 Definición de métricas y umbrales de monitorización 42
7.20.2. C_20_02 Monitorización y reacción ante degradaciones 43
7.21. D_21 Gestión de cambios y reentrenamiento 43
7.21.1. C_21_01 Procedimientos para la gestión de cambios del modelo 43
7.21.2. C_21_02 Reentrenamiento con nuevos datos urbanos 43
7.22. D_22 Trazabilidad de inferencias y explicabilidad 44
7.22.1. C_22_01 Trazabilidad mínima de inferencias 44
7.22.2. C_22_02 Mecanismos de explicabilidad adaptados al personal de operación público . 44
7.23. D_23 Supervisión humana efectiva y límites de automatización 45
7.23.1. C_23_01 Definición de roles humanos y uso asistencial de la IA 45
7.23.2. C_23_02 Controles para evitar automatización acrítica de decisiones 45
7.24. D_24 Gestión de sesgos, equidad e incertidumbre 46
7.24.1. C_24_01 Evaluación de sesgos y equidad en el contexto urbano 46
7.24.2. C_24_02 Gestión de incertidumbre y políticas de abstención 46
7.25. D_25 Gestión de incidentes de ciberseguridad del sistema de IA 46
7.25.1. C_25_01 Procedimiento de gestión de incidentes de ciberseguridad del sistema de IA 47
7.25.2. C_25_02 Notificación de incidentes de ciberseguridad a la entidad contratante 48

7.25.3. C_25_03 Coordinación con los procedimientos de gestión de incidentes de la entidad contratante 48
7.26. D_26 Gestión de incidentes del modelo y daños potenciales 48
7.26.1. C_26_01 Procedimiento específico de gestión de incidentes del modelo 49
7.26.2. C_26_02 Notificación a la entidad contratante y coordinación de respuesta 49
7.27. D_27 Formación y competencias para uso seguro de IA en Smart Cities 49
7.27.1. C_27_01 Formación a personas usuarias y personal de operación del sistema de IA.... 50
7.27.2. C_27_02 Formación y concienciación para personal técnico del adjudicatario 50
7.28. D_28 Controles específicos para IA generativa en servicios urbanos 50
7.28.1. C_28_01 Delimitación de casos de uso y restricciones para IA generativa 51
7.28.2. C_28_02 Avisos, revisión humana y carácter no definitivo del contenido generado 51
7.29. D_29 Protección frente a abusos, exfiltración y manipulación en IA generativa y RAG 51
7.29.1. C_29_01 Controles frente a inyección de instrucciones y jailbreaking 51
7.29.2. C_29_02 Protección frente a fuga de información y uso de RAG sobre datos municipales 52
7.30. D_30 Reversibilidad, portabilidad y retirada del sistema de IA..... 52
7.30.1. C_30_01 Plan de reversibilidad y retirada del sistema de IA 52
7.30.2. C_30_02 Portabilidad, devolución y borrado de datos personales..... 53
8. Referencias..... 54
9. Otras referencias de interés 55
9.1. Lista de materias tratadas en la guía..... 55
9.2. Lista de productos mencionados en la guía..... 55
9.3. Lista de servicios mencionados en la guía 55

ÍNDICE DE TABLAS

Tabla 1: Definiciones empleadas. 15

1. Introducción

En los últimos años, las ciudades han incorporado de forma creciente soluciones basadas en Inteligencia Artificial (en adelante, IA) para apoyar la planificación, gestión y operación de servicios urbanos. Los modelos y sistemas de IA se utilizan en ámbitos tan diversos como la movilidad y el tráfico, la gestión energética y ambiental, la seguridad ciudadana, la gestión de incidencias en el espacio público, la comunicación con la ciudadanía y la optimización de recursos materiales y humanos.

La IA se integra en plataformas de ciudad inteligente, centros de control urbano y sistemas de información municipales, aportando capacidades de análisis avanzado sobre grandes volúmenes de datos urbanos, generación de predicciones, automatización de decisiones de baja complejidad y asistencia al personal de operación y a las personas responsables públicas. La promesa de estas tecnologías es mejorar la eficiencia de los servicios, reducir tiempos de respuesta, anticipar problemas antes de que se materialicen y facilitar una toma de decisiones más informada.

Al mismo tiempo, la adopción de IA en Smart Cities introduce riesgos específicos que deben ser gestionados de forma sistemática. Entre ellos destacan la exposición a nuevas superficies de ataque y dependencias tecnológicas en materia de ciberseguridad, el tratamiento intensivo de datos personales y de datos relativos a la movilidad o al comportamiento de las personas, la opacidad de determinados modelos, la posibilidad de decisiones o recomendaciones sesgadas y la necesidad de asegurar que siempre exista supervisión humana efectiva allí donde las salidas de la IA puedan afectar a derechos fundamentales o a servicios urbanos críticos.

Este documento recoge un conjunto de cláusulas de seguridad, gobernanza y cumplimiento normativo destinadas a ser incorporadas en procedimientos de contratación pública que contemplen el diseño, adquisición, integración, despliegue, operación, mantenimiento o externalización de soluciones de IA en el ámbito de las Smart Cities. El objetivo es que los modelos, plataformas y servicios de IA contratados se sujeten a obligaciones claras y verificables en términos de seguridad de la información, protección de datos personales, gestión de riesgos, transparencia y responsabilidad.

Las cláusulas que se describen a continuación están concebidas como referencia técnica para la redacción de pliegos y contratos relacionados con tecnologías de IA en la ciudad. Su aplicación por parte de las entidades contratantes pretende reforzar la seguridad y la resiliencia de los servicios urbanos que incorporan IA, mantener la confianza de la ciudadanía en el uso de datos y algoritmos en el espacio público y fomentar una cultura de diseño, despliegue y explotación de la IA que sea responsable, transparente y alineada con el marco jurídico vigente.

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

2. Objetivo y alcance

2.1. Objetivo

El propósito del presente documento es apoyar a los órganos de contratación en la incorporación de cláusulas de seguridad en los pliegos técnicos relacionados con soluciones, sistemas y servicios de Inteligencia Artificial (IA) en los entornos de Smart Cities. Mediante un enfoque estructurado por dominios, se pretende facilitar la selección de requisitos contractuales ajustados al tipo de solución, al perfil del proveedor y a la criticidad funcional del sistema de IA objeto del contrato.

Los objetivos que se presentan a continuación definen el propósito general del documento y orientan su uso práctico en los distintos procedimientos de contratación:

- Establecer un marco común y homogéneo de cláusulas técnicas de seguridad aplicables a la contratación de tecnologías de IA en entornos urbanos inteligentes, alineado con la normativa vigente y los principales estándares nacionales e internacionales en materia de protección de datos, seguridad de la información, ciberseguridad y gestión de riesgos tecnológicos.
- Facilitar a los órganos de contratación pública la inclusión de requisitos de seguridad, privacidad, robustez, transparencia, explicabilidad y supervisión humana adecuados, proporcionados y verificables, adaptados al tipo de solución de IA y a los servicios urbanos sobre los que actúa.
- Minimizar los riesgos derivados de la integración de tecnologías de IA en las infraestructuras y servicios urbanos, garantizando el cumplimiento de principios como la seguridad y la privacidad desde el diseño, la trazabilidad, la interoperabilidad segura y la resiliencia operativa.
- Impulsar la responsabilidad compartida en materia de seguridad y gobernanza de la IA en los entornos urbanos entre entidades públicas y adjudicatarios, incluyendo a los terceros que participen en la cadena de suministro de datos, modelos, plataformas o servicios.
- Favorecer el cumplimiento de las normativas y estándares aplicables a la IA y a la ciberseguridad en el contexto de Smart Cities, incluyendo, cuando proceda, el RIA, el CRA, NIS2, el RGPD, la LOPDGDD y el ENS.

2.2. Alcance

El clausulado incorporado en el presente documento es aplicable a todos los sistemas, soluciones y servicios relacionados con IA que se adquieran, desarrollen, integren, desplieguen o mantengan en el ámbito del sector urbano. Esto incluye, entre otros:

- Sistemas de IA utilizados para la gestión de la movilidad y el tráfico, la regulación de cruces, la priorización del transporte público, la gestión de aparcamientos o el análisis de patrones de desplazamiento.
- Soluciones de IA aplicadas a la gestión de infraestructuras y servicios urbanos, como alumbrado, redes de energía, agua, residuos, calidad del aire, mantenimiento predictivo y gestión de emergencias.

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

- Sistemas de análisis de vídeo, imagen, audio u otros datos procedentes de sensores urbanos que incorporan IA para seguridad ciudadana, gestión de incidentes, monitorización del espacio público o control de aforos.
- Soluciones de IA generativa, asistentes virtuales, chatbots y sistemas de recomendación empleados en la atención a la ciudadanía, la tramitación de solicitudes, la comunicación de avisos municipales o el apoyo al personal de operación de centros de control urbano.
- Plataformas de IA, servicios en la nube y componentes de orquestación de modelos (por ejemplo, plataformas MLOps, servicios de inferencia, IA como servicio) que formen parte de la cadena tecnológica y operativa del ecosistema de ciudad inteligente objeto de licitación.

La aplicación de las cláusulas de seguridad se adaptará al nivel de criticidad del sistema de IA y a la tipología del proveedor, de forma que las medidas resulten proporcionales al riesgo y coherentes con lo establecido en las regulaciones y normativas aplicables, debiendo quedar dicha adecuación documentada en el expediente de contratación.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

3. Referencias normativas

Las referencias incluidas en este apartado conforman el marco jurídico y técnico directamente aplicable al diseño, despliegue, operación y contratación de sistemas de Inteligencia Artificial (IA) en el entorno de las Smart Cities. Se integran normas europeas, nacionales e internacionales sobre inteligencia artificial, protección de datos, ciberseguridad y seguridad de los sistemas de información del sector público.

Las entidades contratantes deberán verificar en cada momento la vigencia de las normas citadas y podrán complementar este listado con otras disposiciones o estándares aplicables en su ámbito competencial.

- **Reglamento (UE) 2024/1689, Reglamento de Inteligencia Artificial (RIA):** Establece un marco jurídico armonizado para el desarrollo, la comercialización, la puesta en servicio y el uso de sistemas de IA en la Unión Europea. Introduce un enfoque basado en el riesgo y obligaciones específicas para distintos tipos de sistemas de IA, incluidos los empleados en servicios y aplicaciones en el ámbito de las Smart Cities, reforzando la gestión de riesgos, la gobernanza de datos, la documentación, la trazabilidad, la transparencia, la supervisión humana y la rendición de cuentas.

- **Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD):** Garantiza la protección de las personas físicas respecto al tratamiento de datos personales. Resulta plenamente aplicable al tratamiento de datos mediante sistemas de IA en entornos urbanos, especialmente cuando involucra datos de localización, imagen, audio u otros datos de categoría especial vinculados a servicios municipales.

- **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Desarrolla y complementa el RGPD en el ordenamiento jurídico español e incorpora un catálogo de derechos digitales y previsiones relevantes para determinados tratamientos automatizados y para el sector público, con impacto en el uso de sistemas de IA cuando impliquen tratamiento de datos personales.

- **Real Decreto 311/2022, por el que se regula el 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 que les prestan servicios. Resulta fundamental para la protección de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información procesada mediante sistemas de IA en el entorno urbano.

- **Directiva (UE) 2022/2555, relativa a medidas para un elevado nivel común de ciberseguridad en la Unión (Directiva NIS2):** Refuerza las obligaciones de gestión de riesgos, medidas técnicas y organizativas, notificación de incidentes y supervisión para entidades esenciales e importantes, incluidas, en los términos que establezca la normativa de transposición y el ámbito subjetivo aplicable, determinadas administraciones públicas y determinadas entidades tecnológicas.

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

- **Reglamento (UE) 2024/2847, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Cyber Resilience Act, CRA):** Establece requisitos de ciberseguridad para productos con elementos digitales, incluyendo dispositivos, componentes y software que puedan incorporar funcionalidades de IA y que formen parte de soluciones desplegadas en entornos urbanos inteligentes.

- **ISO/IEC 42001:2023, Information technology – Artificial intelligence – Management system:** Especifica los requisitos para implantar, mantener y mejorar un sistema de gestión de la IA, con el fin de garantizar un uso seguro, responsable y trazable de los sistemas de IA en las organizaciones.

- **ISO/IEC 23894:2023, Information technology – Artificial intelligence – Risk management:** Proporciona un marco estructurado para identificar, evaluar y tratar los riesgos asociados al desarrollo, despliegue y uso de la IA, incluyendo riesgos técnicos, organizativos, éticos y regulatorios relevantes para el ámbito de las Smart Cities.

- **ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements:** Establece los requisitos para implantar y mantener un sistema de gestión de la seguridad de la información, aplicable a las organizaciones que operan y explotan sistemas y servicios de IA.

- **Guías publicadas por la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA):** Documentos y recomendaciones en el ámbito de la inteligencia artificial fiable y la supervisión regulatoria, cuando resulten aplicables a sistemas de IA desplegados en servicios municipales o plataformas de ciudad inteligente.

- **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 transparencia, responsabilidad y mitigación de sesgos en sistemas automatizados y generativos. Se considera una referencia técnica complementaria cuando su utilización resulte compatible con el marco jurídico europeo.

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

4. Definiciones

Este capítulo proporciona una tabla clara y precisa de acrónimos y términos relevantes utilizados a lo largo del documento.

Acrónimos/Términos	Definición
API (Application Programming Interface)	Conjunto de reglas y especificaciones que permiten que distintas aplicaciones o sistemas de software se comuniquen entre sí, facilitando el intercambio estructurado de datos y la invocación de servicios.
Autenticación multifactor (MFA)	Mecanismo de autenticación que requiere más de un factor (por ejemplo, algo que se sabe, algo que se tiene, algo que se es) para verificar la identidad de una persona antes de conceder acceso.
Balanceo de datos	Conjunto de técnicas aplicadas sobre los datos de entrenamiento de un modelo de IA para corregir desequilibrios en la representación de distintas categorías, clases o grupos, con el fin de reducir el riesgo de que el modelo reproduzca o amplifique sesgos derivados de dicha distribución desigual. Puede incluir técnicas de sobremuestreo, submuestreo, generación de datos sintéticos u otras estrategias de ajuste.
Centro de Control Urbano (CCU)	Infraestructura operativa desde la que una entidad pública supervisa y coordina, de forma centralizada, servicios urbanos, tráfico, incidencias y otros procesos de ciudad inteligente, pudiendo integrar información y salidas de sistemas de IA.
Ciclo de vida del modelo de IA	Conjunto de etapas que recorre un modelo de IA desde su concepción y diseño inicial hasta su retirada, incluyendo desarrollo, entrenamiento, validación, despliegue, monitorización, reentrenamiento, versionado y retirada.
Continuidad de negocio	Capacidad de una organización para seguir prestando servicios esenciales a niveles aceptables durante o tras una interrupción grave, apoyándose en planes y procedimientos específicos.
CRA (Cyber Resilience Act)	Reglamento (UE) 2024/2847 que establece requisitos horizontales de ciberseguridad para productos con elementos digitales, incluyendo software y componentes que pueden integrar funcionalidades de IA.
CVEs (Common Vulnerabilities and Exposures)	Identificadores públicos y normalizados para vulnerabilidades de seguridad conocidas en productos de hardware y software, publicados en bases de datos como la mantenida por MITRE y utilizados como referencia común para describir y gestionar vulnerabilidades.

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

Acrónimos/Términos	Definición
Datos sintéticos	Datos generados artificialmente (por ejemplo, mediante modelos de IA) que imitan ciertas propiedades estadísticas de datos reales, con el objetivo de ser utilizados en entrenamiento, pruebas o validación, reduciendo en lo posible la exposición de datos reales.
Drift (deriva)	Cambio estadísticamente significativo en la distribución de los datos de entrada o en la relación entre entradas y salidas del modelo de IA, que puede provocar degradación del rendimiento o comportamientos no deseados si no se detecta y corrige.
Explicabilidad	Propiedad de un sistema de IA que permite a las personas usuarias comprender, en términos razonables, los factores principales que han influido en sus salidas (predicciones, recomendaciones o decisiones), sin necesidad de revelar toda la complejidad interna del modelo o secretos industriales.
Exfiltración	Extracción no autorizada de datos o información desde un sistema, red o entorno protegido hacia un destino externo controlado por un tercero o no previsto por la organización, ya sea mediante técnicas de ataque informático, abuso de funcionalidades legítimas del sistema o manipulación de las salidas de un modelo de IA.
GPAI (General Purpose AI Model / Modelo de propósito general)	Modelo de IA entrenado con grandes cantidades de datos y diseñado para ser capaz de realizar un amplio rango de tareas distintas, que puede integrarse posteriormente en múltiples sistemas o aplicaciones, conforme a la definición del RIA.
Hardening	Proceso de configuración y refuerzo de la seguridad de un sistema, plataforma o componente tecnológico mediante la eliminación o desactivación de servicios, puertos, funcionalidades y configuraciones innecesarias o inseguras, con el objetivo de reducir su superficie de ataque y limitar la exposición a amenazas.
IA (Inteligencia Artificial)	Sistema basado en máquinas diseñado para operar con distintos niveles de autonomía y que, a partir de datos de entrada, infiere cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales, conforme a la definición establecida en el Reglamento (UE) 2024/1689 (RIA).
IA generativa	Subconjunto de sistemas de IA capaces de generar contenido nuevo (texto, imagen, audio, vídeo u otros) a partir de datos de entrenamiento, incluyendo modelos de lenguaje, modelos de difusión y arquitecturas similares.

Acrónimos/Términos	Definición
IAaaS (IA como servicio)	Modelo de prestación de servicios en el que funcionalidades de IA (por ejemplo, inferencia de modelos, clasificación o generación de contenido) se ofrecen a través de la nube como servicio gestionado por un proveedor externo.
Inyección de instrucciones (prompt injection)	Técnica de ataque dirigida contra sistemas de IA generativa y modelos de lenguaje, consistente en la introducción de instrucciones maliciosas o manipuladas en las entradas del sistema (directamente o a través de datos externos que el modelo procesa) con el fin de alterar su comportamiento previsto, eludir restricciones de seguridad o provocar la generación de salidas no autorizadas.
Jailbreaking	Técnica de manipulación de las entradas de un sistema de IA generativa o de un modelo de lenguaje cuyo objetivo es eludir las restricciones, salvaguardas o políticas de uso establecidas por el proveedor o por la entidad contratante, provocando que el sistema genere contenidos o ejecute acciones que en condiciones normales estarían bloqueados o limitados.
Logs / Registros de actividad	Registros generados por sistemas y aplicaciones que recogen información sobre eventos relevantes (accesos, cambios de configuración, llamadas a APIs, errores, etc.), utilizados para trazabilidad, auditoría y análisis de incidentes.
Medidas compensatorias	Controles de seguridad alternativos o adicionales que se implantan cuando no es posible aplicar la medida de protección principal prevista (por ejemplo, un parche de seguridad) dentro del plazo o en las condiciones requeridas, con el fin de reducir el riesgo a un nivel aceptable hasta que pueda implementarse la solución definitiva.
Microservicio	Componente de software diseñado para realizar una función específica y delimitada dentro de una arquitectura de aplicación distribuida, que se ejecuta de forma independiente y se comunica con otros componentes a través de interfaces bien definidas (habitualmente APIs), facilitando el desarrollo, despliegue y escalado independiente de cada funcionalidad.
MLOps	Conjunto de prácticas, procesos y herramientas destinados a gestionar de forma controlada el ciclo de vida completo de los modelos de IA (desarrollo, entrenamiento, despliegue, monitorización, reentrenamiento, versionado y retirada), integrando equipos de datos, desarrollo y operaciones.
Plataforma de ciudad inteligente	Conjunto de sistemas, servicios y componentes tecnológicos que la entidad contratante utiliza para integrar, procesar y visualizar datos urbanos, coordinar servicios y, en su caso, consumir o integrar salidas de sistemas de IA.

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

Acrónimos/Términos	Definición
RAG (Retrieval Augmented Generation)	Enfoque que combina mecanismos de recuperación de información desde fuentes o repositorios (por ejemplo, bases de datos, documentos, registros municipales) con modelos de IA generativa, de manera que las salidas del modelo se apoyan en información externa actualizada o específica.
Reversión (rollback)	Procedimiento controlado mediante el cual se restaura un sistema, modelo de IA o componente tecnológico a una versión anterior estable y previamente validada, con el fin de revertir los efectos de un cambio, actualización o despliegue que haya provocado errores, degradación del rendimiento u otros efectos adversos en el servicio.
Responsable del despliegue (deployer)	Persona física o jurídica, autoridad pública u otro organismo que utiliza un sistema de IA bajo su autoridad en el ejercicio de una actividad profesional, conforme al RIA. Esta condición no depende por sí sola de quién haya desarrollado, integrado, mantenido o explotado técnicamente el sistema.
Sesgo (bias) en sistemas de IA	Tendencia sistemática de un modelo de IA a producir salidas que favorecen o perjudican de forma injustificada a determinados grupos, zonas o situaciones, a veces como consecuencia de sesgos presentes en los datos de entrenamiento o en el diseño del sistema.
Sistema de IA de alto riesgo	Sistema de IA clasificado como de alto riesgo conforme a los supuestos, categorías y condiciones establecidos en el RIA y sujeto, en consecuencia, a requisitos reforzados en materia de gestión de riesgos, gobernanza de datos, documentación técnica, trazabilidad, supervisión humana, exactitud, robustez y ciberseguridad.
Trazabilidad	Capacidad de reconstruir de forma fiable qué ha ocurrido en un sistema de IA o en su entorno técnico y operativo, incluyendo, cuando proceda, qué versión del modelo intervino, qué datos o fuentes se utilizaron, qué cambios se aplicaron, qué decisiones de configuración se adoptaron y en qué momento se produjeron, mediante registros y documentación adecuados.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Instrucciones de uso

El presente apartado tiene como finalidad proporcionar una guía clara y orientativa que permita realizar una selección coherente de cláusulas a las personas gestoras encargadas de redactar los pliegos de contratación pública relacionados con soluciones, sistemas y servicios de IA en el entorno de Smart Cities.

I. Identificación de la necesidad y del caso de uso de IA

Definir qué se quiere conseguir con la licitación y el caso de uso concreto de IA (gestión de tráfico, optimización de alumbrado, análisis de vídeo para seguridad, recomendaciones automáticas para ciudadanía, asistentes virtuales, modelos analíticos en la plataforma de ciudad, etc.), así como su impacto potencial en los servicios urbanos y en la ciudadanía.

II. Determinación de la tipología de proveedor y del modelo de prestación

Determinar la tipología de proveedor conforme al apartado 6 (soluciones de IA, plataformas y servicios de IA, proveedores mixtos, integración y soporte, datos y preparación de datos) y el modelo de prestación (on-premise, cloud, servicio gestionado, acceso por API), identificando también subcontratistas y proveedores de modelos de propósito general si los hubiera.

III. Asignación de roles y responsabilidades

Identificar los roles implicados (responsable y encargado del tratamiento según RGPD/LOPDGDD, proveedor y responsable del despliegue según RIA, personal de operación de plataformas urbanas o centros de control) y definir la distribución de responsabilidades a lo largo del ciclo de vida de la solución, incluida la cadena de suministro.

IV. Clasificación regulatoria y análisis de riesgos

Verificar la posible clasificación del sistema de IA según el RIA (alto riesgo u otras categorías), la aplicabilidad de otras normas (CRA, NIS2, normativa sectorial) y realizar un análisis preliminar de riesgos que considere seguridad de los servicios urbanos, protección de datos, continuidad operativa, ciberseguridad, sesgos y equidad.

V. Clasificación según el ENS

Clasificar el sistema de información que soporta la solución de IA conforme al Esquema Nacional de Seguridad (categoría básica, media o alta) y usar esta clasificación como referencia para la intensidad de las medidas de seguridad a exigir en el clausulado.

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

VI. Gobernanza del dato

Precisar qué datos urbanos se utilizarán (sensores, tráfico, imagen, datos personales, datos seudonimizados o anonimizados, etc.), su origen y calidad, la base jurídica del tratamiento y las restricciones de uso (incluido entrenamiento y reentrenamiento), así como las reglas de conservación, supresión y, en su caso, transferencias internacionales.

VII. Selección de dominios y cláusulas

En función de los pasos anteriores, seleccionar en el capítulo 7 los dominios de control (D_XX) y las cláusulas (C_XX_YY) que resulten aplicables al contrato, procurando que sean proporcionales a la criticidad del caso de uso y al impacto potencial de la IA sobre los servicios urbanos y la ciudadanía.

VIII. Definición de entregables y criterios de aceptación

Determinar qué evidencias y documentación deberá aportar el adjudicatario (informes de pruebas, documentación técnica, evidencias de cumplimiento, planes de gestión de riesgos, documentación de modelos, etc.) y fijar criterios de aceptación vinculados al cumplimiento de las cláusulas seleccionadas.

IX. Inclusión en pliegos y documentación del análisis

Incorporar las cláusulas elegidas en los pliegos técnicos y documentos contractuales, indicando su carácter obligatorio y consecuencias en caso de incumplimiento, y dejar constancia en el expediente de contratación del análisis realizado y de la justificación de la selección de dominios y cláusulas.

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

6. Tipologías de proveedores de tecnologías de IA en Smart Cities

El presente apartado tiene como finalidad identificar las principales tipologías de proveedores que pueden intervenir en la contratación pública de tecnologías de Inteligencia Artificial (IA) en el entorno de las Smart Cities. Las tipologías descritas tienen un carácter funcional y contractual y no se corresponden necesariamente, de forma directa, con los roles definidos en el Reglamento (UE) 2024/1689 (RIA), si bien pueden solaparse con ellos según el caso concreto.

Esta clasificación es útil para:

- Determinar las obligaciones de seguridad, protección de datos y gobernanza que corresponden a cada tipo de proveedor.
- Facilitar la selección proporcionada de dominios de control y cláusulas aplicables en cada contrato.
- Aclarar la distribución de responsabilidades a lo largo del ciclo de vida de las soluciones de IA (diseño, desarrollo, integración, despliegue, operación, mantenimiento, actualización y retirada).
- Una misma entidad adjudicataria puede encajar simultáneamente en más de una tipología, en función del alcance del contrato y del rol que asuma en la solución.

6.1. Proveedores de soluciones de IA

Se consideran proveedores de soluciones de IA aquellos adjudicatarios que diseñan, desarrollan, entrenan, validan y suministran sistemas de IA orientados a casos de uso concretos en el ámbito de las Smart Cities, pudiendo incluir, cuando así se establezca, su implantación inicial en los sistemas, plataformas urbanas o centros de control de la entidad contratante.

Entre las características habituales de esta tipología se encuentran:

- La entrega de una solución de IA con funcionalidades claramente definidas (por ejemplo, sistemas de apoyo a la gestión del tráfico, análisis de vídeo para seguridad ciudadana, modelos de predicción de demanda de servicios, optimización de alumbrado o energía, soluciones de IA generativa para atención a la ciudadanía).
- La inclusión de los modelos de IA, de los componentes software necesarios para su ejecución y, en su caso, de interfaces de usuario o módulos de integración básicos con las plataformas y sistemas urbanos existentes.
- La asunción de responsabilidades sobre el diseño, entrenamiento, validación y actualización de los modelos de IA durante el periodo de garantía y/o mantenimiento contratado.

Roles RIA habitualmente asociados:

En el sentido del RIA, esta tipología de entidad adjudicataria suele asumir el rol de proveedor del sistema de IA cuando desarrolla o manda desarrollar el sistema y lo pone en el mercado o en servicio bajo su nombre o marca. Cuando, además, utiliza el sistema para prestar servicios a la entidad contratante bajo

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

su propia responsabilidad, puede asumir también el rol de responsable del despliegue (deployer) para determinadas actividades, sin perjuicio de que la propia entidad contratante pueda asumir dicho rol cuando utilice el sistema en el ejercicio de sus competencias.

Estas entidades deberán garantizar, entre otros aspectos:

- Que la solución cumple la normativa aplicable, incluyendo, cuando proceda, el RIA, el Reglamento (UE) 2024/2847 (CRA), la Directiva (UE) 2022/2555 (NIS2), el RGPD, la LOPDGDD y el Esquema Nacional de Seguridad (ENS).
- Que se respetan las obligaciones reforzadas del RIA cuando la solución tenga la consideración de sistema de IA de alto riesgo, incluyendo la gestión de riesgos, la gobernanza de datos, la documentación técnica, la trazabilidad, la transparencia y la supervisión humana.
- Que se entrega a la entidad contratante la documentación técnica relevante sobre el sistema de IA, los datos utilizados para su entrenamiento y validación, la gestión de riesgos y las medidas de seguridad y supervisión implementadas, en los términos exigidos en el contrato.

6.2. Proveedores de plataformas y servicios de IA

Se consideran proveedores de plataformas y servicios de IA aquellos adjudicatarios que proporcionan infraestructuras, entornos y servicios técnicos que permiten desarrollar, entrenar, validar, desplegar, operar y monitorizar modelos de IA en el contexto urbano, ya sea por parte de la entidad contratante o de terceros designados por esta.

Dentro de esta tipología se incluyen, entre otros:

- Plataformas de desarrollo y operación de modelos de IA (por ejemplo, entornos MLOps, plataformas de ciencia de datos o soluciones específicas para entrenamiento, evaluación y despliegue de modelos).
- Servicios de IA en la nube, como APIs de modelos de IA, servicios de inferencia gestionada o capacidades de IA como servicio (IAaaS) que procesan datos urbanos o personales o influyen en procesos y servicios municipales.
- Servicios de infraestructura especializada para IA, como recursos de computación para entrenamiento e inferencia, servicios de almacenamiento de datos para IA y servicios de orquestación y monitorización de modelos integrados en la plataforma de ciudad inteligente.

Cuando el adjudicatario proporcione o integre modelos de propósito general (GPAI) en el sentido del RIA, deberá declarar expresamente esta circunstancia en el contrato y analizar las obligaciones específicas que le correspondan conforme a su posición en la cadena de valor, incluyendo, cuando proceda, su condición de proveedor del modelo GPAI, proveedor del sistema de IA que lo integra o responsable del despliegue del sistema resultante.

Roles RIA habitualmente asociados:

En el sentido del RIA, estas entidades pueden asumir distintos roles según su actividad concreta. Pueden actuar como proveedor en el sentido del RIA (provider) cuando desarrollan o ponen en el mercado un

sistema de IA bajo su nombre o marca; pueden intervenir respecto de modelos de propósito general (GPAI) cuando desarrollan, suministran o integran este tipo de modelos; y, en determinados escenarios, pueden asumir la condición de responsable del despliegue (deployer) cuando utilizan sistemas de IA bajo su autoridad para prestar servicios a la entidad contratante.

Estas entidades deberán garantizar, entre otros aspectos:

- Que la infraestructura y los servicios prestados cumplen, cuando proceda, con el ENS, el RIA, el RGPD, la LOPDGDD, la Directiva NIS2 y el CRA, cuando este último resulte material y temporalmente aplicable.
- Que informan a la entidad contratante sobre la localización de los datos, las condiciones de tratamiento y las medidas de seguridad técnicas y organizativas implementadas, incluyendo las relativas a cifrado, control de accesos, segregación de entornos, separación lógica respecto de otros clientes, monitorización y continuidad del servicio.
- Que la integración de la plataforma o servicio con los sistemas y plataformas urbanas de la entidad contratante se realiza de forma segura, respetando las políticas de seguridad, la segmentación de redes y la gestión de identidades definidas por la entidad.

6.3. Proveedores mixtos

Se consideran proveedores mixtos aquellos adjudicatarios que combinan funciones propias de los proveedores de soluciones de IA (apartado 6.1) y de los proveedores de plataformas y servicios de IA (apartado 6.2), asumiendo una responsabilidad amplia sobre la solución, la infraestructura y los servicios asociados.

Esta tipología de entidades adjudicatarias puede:

- Suministrar una o varias soluciones de IA para determinados servicios o procesos urbanos.
- Proporcionar la plataforma y los servicios necesarios para el entrenamiento, despliegue, operación, monitorización y actualización de los modelos de IA suministrados.
- Gestionar, en nombre de la entidad contratante y con el alcance definido en el contrato, parte o la totalidad del ciclo de vida de los modelos de IA, incluyendo reentrenamientos, ajustes de parámetros y despliegue de nuevas versiones.

Roles RIA habitualmente asociados:

En el sentido del RIA, estas entidades pueden asumir simultáneamente varios roles, según la configuración concreta del contrato y del servicio: proveedor en el sentido del RIA (provider), cuando diseñan y ponen en el mercado o en servicio sistemas de IA bajo su nombre o marca, responsable del despliegue (deployer), cuando utilizan dichos sistemas bajo su autoridad para prestar servicios; y, en su caso, una posición regulatoria relevante respecto de modelos de propósito general (GPAI), cuando desarrollan, suministran o integran este tipo de modelos en sus soluciones o plataformas.

En consecuencia, las entidades adjudicatarias de tipología mixta deberán:

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

- Cumplir las obligaciones aplicables a las tipologías descritas en los apartados 6.1 y 6.2, tanto en materia de producto como de servicios e infraestructura.
- Detallar, en la documentación contractual, cómo se reparten las responsabilidades en materia de seguridad, protección de datos, cumplimiento regulatorio, gestión de riesgos, supervisión humana, monitorización del rendimiento del modelo y gestión de incidentes.
- Coordinarse con otras entidades que intervengan en la solución (por ejemplo, integradores o proveedores de datos) para garantizar una gestión coherente de la cadena de suministro y de los riesgos asociados.

6.4. Prestadores de servicios de integración, operación y soporte de soluciones de IA

Se consideran prestadores de servicios de integración, operación y soporte de soluciones de IA aquellos adjudicatarios que, sin ser necesariamente responsables del desarrollo del modelo de IA ni de la plataforma subyacente, se encargan de implantar, configurar, integrar, operar y dar soporte a la solución de IA en los sistemas, plataformas urbanas e infraestructuras de la entidad contratante.

Entre sus funciones habituales se encuentran:

- Integrar la solución de IA con la plataforma de ciudad inteligente, los centros de control urbano y otros sistemas corporativos existentes.
- Configurar flujos de trabajo, interfaces de usuario y reglas de negocio para incorporar la IA en los procesos urbanos y organizativos de la entidad.
- Realizar pruebas de integración y seguridad, colaborar en la validación operativa de la solución y prestar servicios de operación, soporte y mantenimiento durante la vigencia del contrato.

Roles RIA habitualmente asociados:

En el sentido del RIA, estas entidades pueden asumir la condición de responsable del despliegue (deployer) cuando utilizan un sistema de IA bajo su autoridad para prestar servicios a la entidad contratante. En otros supuestos, podrán actuar como entidades que utilizan técnicamente un sistema de IA desplegado por la propia entidad contratante, sin que ello altere por sí solo la atribución de roles regulatorios, que deberá determinarse conforme a la configuración contractual y al uso efectivo del sistema.

Estas entidades deberán:

- Respetar las políticas de seguridad de la información, protección de datos, segmentación de redes y gestión de accesos definidas por la entidad contratante.
- Coordinarse con los proveedores de soluciones de IA y de plataformas y servicios de IA implicados, para que la integración, operación y soporte no introduzcan vulnerabilidades ni afecten negativamente a la seguridad de los servicios urbanos o a la protección de datos personales.

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

- Documentar las configuraciones, adaptaciones, interconexiones y cambios realizados en los sistemas de la entidad como consecuencia del despliegue, integración, operación y soporte de la solución de IA, y mantener actualizada dicha documentación.

6.5. Proveedores de datos y servicios de preparación de datos para IA

Se consideran proveedores de datos y servicios de preparación de datos para IA aquellos adjudicatarios que proporcionan datos urbanos y/o servicios de normalización, limpieza, enriquecimiento, etiquetado, anonimización, seudonimización o generación de datos sintéticos destinados a entrenar, validar o evaluar modelos de IA utilizados en Smart Cities.

Esta tipología incluye, entre otros:

- Proveedores de conjuntos de datos urbanos (movilidad, energía, medio ambiente, uso del espacio público, entre otros) destinados a proyectos de IA autorizados por la entidad contratante.
- Prestadores de servicios de transformación y preparación de datos específicos para IA: limpieza, estandarización, codificación, anonimización, seudonimización o generación de datos sintéticos.
- Organizaciones que actúan como intermediarias en el acceso a datos urbanos bajo marcos de gobernanza de datos definidos por la entidad contratante o por otras autoridades competentes.

Roles RIA habitualmente asociados:

En el sentido del RIA, estas entidades pueden asumir el rol de proveedor del sistema de IA cuando desarrollan o ponen en servicio herramientas de procesamiento de datos que constituyen en sí mismas sistemas de IA, o el rol de responsable del despliegue cuando utilizan sistemas de IA para prestar servicios de preparación de datos a la entidad contratante. En otros casos actuarán como proveedores de datos, sin que ello implique necesariamente la asunción de un rol específico en el RIA más allá de sus obligaciones en materia de protección de datos y seguridad de la información.

Estas entidades deberán:

- Cumplir estrictamente con la normativa de protección de datos personales, en particular cuando se trate de información relativa a la ciudadanía, y con las instrucciones del responsable del tratamiento designado por la entidad contratante.
- Garantizar, en la medida en que lo permita el alcance del servicio, la calidad, coherencia, representatividad y actualidad de los datos suministrados o transformados.
- Documentar los procesos de preparación de datos (transformación, etiquetado, anonimización, seudonimización, generación de datos sintéticos) y las limitaciones y riesgos residuales asociados a su uso en modelos de IA.

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

6.6. Consideraciones generales sobre la tipología de proveedores

La correcta identificación de la tipología o tipologías de entidades adjudicatarias presentes en cada contrato es un paso previo clave para:

- Aplicar de forma adecuada el clausulado recogido en el capítulo 7.
- Determinar el reparto de responsabilidades en materia de seguridad, cumplimiento regulatorio, protección de datos y gestión de riesgos a lo largo de la cadena de suministro.
- Justificar la selección de dominios y cláusulas en el expediente de contratación, en coherencia con el análisis de riesgos y con los principios de proporcionalidad y responsabilidad.

Cuando una misma entidad adjudicataria desempeñe simultáneamente varias de las tipologías descritas, la entidad contratante deberá aplicar de forma acumulativa las obligaciones correspondientes a cada una de ellas, modulando su intensidad en función del análisis de riesgos y de las características concretas del contrato, y dejando reflejada esta combinación de roles contractuales y, en su caso, de roles RIA en los pliegos y en la documentación contractual.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

7. Cláusulas de seguridad, gobernanza y control para sistemas de IA en el entorno de Smart Cities

El presente capítulo recoge un conjunto estructurado de cláusulas organizadas por dominios funcionales. Cada dominio incluye una definición y una o varias cláusulas destinadas a ser incorporadas, total o parcialmente, en los pliegos de contratación pública que contemplen soluciones de IA en el entorno urbano.

El objetivo de estas cláusulas es establecer requisitos claros y verificables en materia de seguridad, gobernanza, gestión de riesgos, protección de datos y cumplimiento normativo, adaptados a la realidad de las Smart Cities y al marco regulatorio aplicable, incluyendo el Reglamento (UE) 2024/1689 (RIA), el RGPD, la LOPDGDD, el ENS, la Directiva NIS2 y el CRA.

7.1. D_01 Gobernanza del sistema de IA urbano

- **Definición del dominio**

Conjunto de mecanismos, roles, políticas y procesos que el adjudicatario debe definir e implementar para asegurar una gestión clara, estructurada y responsable del sistema de IA contratado en el entorno urbano. Este dominio abarca la asignación de responsabilidades entre las partes implicadas, la existencia de políticas internas de gobernanza de IA, la supervisión periódica del sistema y la coordinación con la entidad contratante durante todo el ciclo de vida del sistema de IA.

- **Cláusulas aplicables**

7.1.1. C_01_01 Marco formal de responsabilidades

El adjudicatario deberá establecer y documentar un marco formal de responsabilidades específico para el sistema de IA objeto del contrato, en el que se identifiquen, como mínimo:

- Las personas o unidades responsables del diseño, configuración y operación técnica del sistema de IA.
- Las personas o unidades responsables de la seguridad de la información y la protección de datos personales en relación con dicho sistema.
- Las personas o unidades responsables del cumplimiento normativo y de la gestión de riesgos del sistema de IA.
- Un punto de contacto único para la entidad contratante respecto a cuestiones técnicas, de seguridad y de cumplimiento relacionadas con el sistema de IA.

Cualquier cambio relevante en la asignación de responsabilidades deberá ser notificado a la entidad contratante y reflejado en la documentación de gobernanza del sistema de IA.

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

7.1.2. C_01_02 Política de gobernanza del sistema de IA

El adjudicatario deberá disponer de una política de gobernanza del sistema de IA objeto del contrato, que podrá formar parte de un marco corporativo más amplio, siempre que contemple de manera específica dicho sistema. Esta política deberá:

- Describir los procesos internos de gestión del ciclo de vida del sistema de IA (diseño, desarrollo, entrenamiento, validación, despliegue, monitorización, actualización y retirada),
- Establecer las líneas de responsabilidad y los mecanismos de supervisión interna sobre el sistema de IA,
- Contemplar la integración de requisitos de seguridad, protección de datos, cumplimiento del RIA y gestión de riesgos desde las fases iniciales del proyecto,
- Definir los mecanismos de coordinación con la entidad contratante, incluyendo la comunicación de cambios relevantes y la atención a requerimientos de información.

La política deberá mantenerse actualizada durante toda la vigencia del contrato y ponerse a disposición de la entidad contratante cuando ésta lo solicite.

7.1.3. C_01_03 Mecanismo estructurado de supervisión

El adjudicatario deberá establecer un mecanismo formal de supervisión del sistema de IA, que podrá materializarse en un comité interno, un responsable designado o una estructura equivalente. Este mecanismo deberá:

- Revisar periódicamente el comportamiento y el rendimiento del sistema de IA,
- Supervisar la aplicación de las medidas de seguridad y de protección de datos definidas,
- Analizar incidentes y cambios relevantes en el sistema de IA y en su contexto de uso,
- Proponer y coordinar la implementación de medidas correctoras o de mejora.

Las reuniones y decisiones relevantes de este mecanismo de supervisión deberán quedar documentadas y dicha documentación estará disponible para la entidad contratante cuando así se requiera.

7.2. D_02 Clasificación del sistema de IA y determinación del nivel de riesgo conforme al RIA

- **Definición del dominio**

Conjunto de obligaciones destinadas a garantizar que el adjudicatario identifica y documenta, de forma justificada, la clasificación del sistema de IA conforme al Reglamento (UE) 2024/1689 (RIA), así como los roles que asume en dicho reglamento y las consecuencias de esta clasificación en términos de obligaciones técnicas, organizativas y documentales.

- **Cláusulas aplicables**

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

7.2.1. C_02_01 Determinación y documentación de la clasificación en base al RIA

Antes de la puesta en servicio del sistema de IA en el entorno urbano, el adjudicatario deberá determinar y documentar su clasificación conforme al RIA, indicando:

- Si el sistema de IA entra en alguna de las categorías de sistemas de IA de alto riesgo previstas en el reglamento, o si se trata de un sistema de otra categoría (por ejemplo, riesgo limitado o mínimo),
- La base utilizada para dicha clasificación (referencia a anexos, categorías o criterios del RIA),
- Si el sistema integra o utiliza modelos de propósito general (GPAI) y, en su caso, la información relevante sobre dichos modelos.

Esta clasificación formará parte de la documentación contractual y deberá revisarse cuando se produzcan cambios sustanciales en el sistema o en su uso que puedan afectar al nivel de riesgo.

7.2.2. C_02_02 Identificación de roles conforme al RIA

El adjudicatario deberá identificar expresamente, en el marco del contrato, los roles que asume conforme al RIA en relación con el sistema de IA objeto de la adjudicación, indicando al menos:

- Si actúa como proveedor del sistema de IA (provider) en el sentido del RIA,
- Si actúa como responsable del despliegue (deployer) al utilizar el sistema de IA para prestar servicios a la entidad contratante,
- Si interviene respecto de modelos de propósito general (GPAI), deberá identificarse expresamente si actúa como proveedor del modelo GPAI, como proveedor del sistema de IA que lo integra, como responsable del despliegue del sistema resultante o bajo cualquier otra condición regulatoria aplicable conforme al RIA.

Asimismo, deberá indicar cuándo la propia entidad contratante asume el rol de responsable del despliegue, en caso de utilizar el sistema de IA en el ejercicio de sus propias competencias. Esta identificación deberá vincularse a las obligaciones específicas que corresponden a cada rol conforme al RIA.

7.2.3. C_02_03 Ajuste de obligaciones al nivel de riesgo y a los roles

El adjudicatario deberá garantizar que las obligaciones técnicas, organizativas y documentales que asume en virtud del contrato son compatibles con la clasificación y los roles definidos conforme al RIA. Cuando se trate de un sistema de IA de alto riesgo, deberá asegurar que se encuentran implantados los elementos exigidos por el reglamento, incluyendo, entre otros:

- Un sistema de gestión de riesgos,
- Una gobernanza adecuada de los datos utilizados,
- La elaboración y mantenimiento de la documentación técnica,
- El registro de logs apropiados para la supervisión y el análisis de incidentes,
- Medidas que permitan una supervisión humana efectiva del sistema.

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

Cualquier cambio en la clasificación del sistema o en los roles asumidos que derive en nuevas obligaciones o en la modificación de las existentes deberá ser comunicado a la entidad contratante y reflejado en la documentación de cumplimiento.

7.2.4. C_02_04 Verificación de ausencia de prácticas prohibidas

El adjudicatario deberá verificar y declarar expresamente, antes de la puesta en servicio del sistema de IA, que la solución objeto del contrato no incurre en ninguna de las prácticas prohibidas por el Reglamento (UE) 2024/1689 (RIA), ni ha sido diseñada, configurada o destinada a usos que pudieran situarla materialmente en alguno de dichos supuestos.

A tal efecto, el adjudicatario deberá:

- Identificar y documentar los usos previstos del sistema de IA en el marco del contrato, así como las limitaciones y condiciones de uso relevantes para su encaje regulatorio,
- Analizar si el sistema, su configuración, sus finalidades o su contexto de despliegue podrían dar lugar, directa o indirectamente, a un uso prohibido conforme al RIA,
- Informar por escrito y sin demora indebida a la entidad contratante cuando existan dudas razonables sobre la licitud del caso de uso, sobre su clasificación regulatoria o sobre el riesgo de incurrir en una práctica prohibida,
- Abstenerse de poner en servicio, desplegar o mantener funcionalidades respecto de las cuales no exista una base regulatoria suficientemente clara o cuya compatibilidad con el RIA no haya sido adecuadamente analizada y documentada.

La entidad contratante podrá requerir al adjudicatario la aportación de la justificación técnica y regulatoria correspondiente, así como la adopción de limitaciones de uso, medidas de configuración o restricciones funcionales adicionales cuando resulte necesario para evitar riesgos de incumplimiento.

7.3. D_03 Cumplimiento normativo y regulatorio

- **Definición del dominio**

Conjunto de medidas y compromisos que el adjudicatario debe asumir para garantizar que el sistema de IA, su infraestructura asociada y los servicios prestados cumplen el marco normativo aplicable, incluyendo el RIA, el RGPD, la LOPDGDD, el ENS, la Directiva NIS2, el CRA y cualquier normativa sectorial relevante para los servicios urbanos afectados.

- **Cláusulas aplicables**

7.3.1. C_03_01 Alineamiento con la normativa aplicable

El adjudicatario será responsable de garantizar que el sistema de IA y los servicios asociados se ajustan a la normativa vigente en materia de inteligencia artificial, protección de datos personales, seguridad de la información y ciberseguridad, incluyendo, cuando proceda:

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

- El Reglamento (UE) 2024/1689 (RIA),
- El Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD),
- El Real Decreto 311/2022 (Esquema Nacional de Seguridad, ENS),
- La Directiva (UE) 2022/2555 (NIS2) y su normativa de trasposición aplicable,
- El Reglamento (UE) 2024/2847 (CRA) en lo que resulte aplicable,
- La normativa sectorial específica relacionada con el servicio urbano objeto del contrato.

7.3.2. C_03_02 Evidencias de conformidad

El adjudicatario deberá aportar, cuando proceda y a requerimiento de la entidad contratante, evidencias documentales que acrediten el cumplimiento de la normativa aplicable, tales como:

- Declaraciones de conformidad o documentación técnica elaborada en aplicación del RIA,
- Certificaciones o informes de evaluación emitidos por terceros independientes (por ejemplo, certificaciones ISO/IEC, ENS, evaluación de controles de seguridad o privacidad),
- Informes de auditoría interna o externa relativos a la seguridad de los sistemas utilizados para prestar el servicio,
- Documentación sobre medidas técnicas y organizativas implantadas para cumplir el RGPD, la LOPDGDD, el ENS y NIS2.

La entidad contratante podrá vincular la aceptación inicial del sistema o la continuidad del servicio a la recepción y revisión satisfactoria de estas evidencias.

7.3.3. C_03_03 Gestión de la cadena de suministro y subcontratación

El adjudicatario deberá informar a la entidad contratante sobre los subcontratistas y terceros que participen en la prestación del servicio o que tengan acceso a datos, modelos, plataformas o componentes del sistema de IA, indicando, al menos:

- La identidad del subcontratista y los servicios que presta,
- La localización desde la que presta sus servicios y, en su caso, la ubicación de los datos que trata,
- Las medidas de seguridad y protección de datos que el subcontratista tiene implantadas.

La incorporación de nuevos subcontratistas que intervengan en actividades relevantes para la seguridad, la protección de datos o el funcionamiento del sistema de IA requerirá la autorización previa y por escrito de la entidad contratante. El adjudicatario será responsable de que los subcontratistas cumplan obligaciones equivalentes a las asumidas en el contrato en materia de seguridad, protección de datos y cumplimiento normativo.

7.4. D_04 Gestión documental y evidencias de cumplimiento

- **Definición del dominio**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Conjunto de actividades dirigidas a asegurar que la documentación técnica, funcional, de seguridad y de cumplimiento asociada al sistema de IA se genera, mantiene, actualiza y pone a disposición de la entidad contratante de forma estructurada, accesible y trazable durante toda la vigencia del contrato.

- **Cláusulas aplicables**

7.4.1. C_04_01 Documentación técnica y funcional del sistema de IA

El adjudicatario deberá elaborar y mantener actualizada la documentación técnica y funcional necesaria para comprender, operar, integrar y supervisar el sistema de IA, incluyendo, al menos:

- Descripción funcional del sistema de IA y de sus casos de uso previstos,
- Arquitectura técnica e interfaces principales con otros sistemas urbanos,
- Información relevante sobre los modelos de IA empleados (tipo de modelo, tareas, versiones y principales parámetros),
- Requisitos técnicos de despliegue, operación, monitorización y seguridad,
- Limitaciones de uso y advertencias relevantes para el contexto urbano.

Esta documentación deberá entregarse a la entidad contratante en idioma español y en formato estructurado y reutilizable.

7.4.2. C_04_02 Registro de cambios y evidencias de pruebas

El adjudicatario deberá mantener un registro actualizado de los cambios relevantes en el sistema de IA (nuevas versiones de modelos, cambios de parámetros significativos, modificaciones de arquitectura, ampliaciones del ámbito de uso) y de las pruebas asociadas a dichos cambios. Este registro deberá incluir, al menos:

- La descripción del cambio,
- La fecha de implementación,
- El motivo del cambio,
- Las pruebas realizadas y sus resultados,
- El estado de aprobación o rechazo.

El registro deberá estar disponible para la entidad contratante cuando ésta lo solicite.

7.5. D_05 Gestión integral de riesgos del sistema de IA

- **Definición del dominio**

Conjunto de procesos que el adjudicatario debe establecer para identificar, analizar, evaluar, tratar y revisar los riesgos asociados al sistema de IA en el entorno de Smart Cities, incluyendo riesgos técnicos, operativos, de seguridad de la información, de protección de datos y de impacto sobre derechos fundamentales y servicios urbanos.

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

- **Cláusulas aplicables**

7.5.1. C_05_01 Proceso de gestión de riesgos

El adjudicatario deberá definir, documentar e implantar un proceso de gestión de riesgos específico para el sistema de IA objeto del contrato, que integre, al menos:

- La identificación de riesgos relevantes en las distintas fases del ciclo de vida del sistema, incluyendo, cuando la naturaleza del caso de uso lo justifique, riesgos derivados de ataques adversariales (como perturbaciones de entradas, envenenamiento de datos de entrenamiento o intentos de extracción del modelo),
- La evaluación de la probabilidad e impacto de dichos riesgos sobre los servicios urbanos y sobre las personas,
- La definición e implementación de medidas de mitigación y controles asociados,
- La revisión periódica del registro de riesgos y la actualización de las medidas cuando se produzcan cambios significativos o incidentes relevantes.

Este proceso deberá estar alineado con los requisitos del RIA para sistemas de IA de alto riesgo, cuando proceda, y con el enfoque de gestión de riesgos de la entidad contratante.

7.6. D_06 Evaluación de impacto en derechos fundamentales

- **Definición del dominio**

Conjunto de obligaciones orientadas a garantizar que, cuando el sistema de IA pueda afectar de manera significativa a derechos fundamentales o a colectivos vulnerables, se lleve a cabo una evaluación específica de impacto en derechos fundamentales, de acuerdo con lo previsto en el RIA y con cualquier requisito adicional establecido por la normativa nacional o por la entidad contratante.

- **Cláusulas aplicables**

7.6.1. C_06_01 Colaboración en evaluaciones de impacto en derechos fundamentales

Cuando, conforme al RIA o a las políticas de la entidad contratante, resulte necesaria una evaluación de impacto en derechos fundamentales relacionada con el sistema de IA objeto del contrato, el adjudicatario deberá colaborar activamente en su realización, aportando la información técnica, organizativa y de funcionamiento que le sea requerida.

Esta información incluirá, en su caso:

- La descripción del sistema de IA y de sus casos de uso,
- La caracterización de las personas y colectivos potencialmente afectados,
- Los riesgos identificados para derechos fundamentales y para la equidad en el contexto urbano,
- Las medidas de mitigación incorporadas al diseño y a la operación del sistema.

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

7.7. D_07 Gobernanza del dato urbano para IA

- **Definición del dominio**

Conjunto de principios, roles y procesos que regulan cómo se gestionan los datos utilizados por el sistema de IA en sus distintas fases (entrenamiento, validación, pruebas y operación) en el contexto de una Smart City. Incluye la identificación de tipos de datos, fuentes autorizadas, responsabilidades sobre su tratamiento, reglas de conservación y supresión y coordinación con la gobernanza del dato de la entidad contratante.

- **Cláusulas aplicables**

7.7.1. C_07_01 Marco de gobernanza del dato para el sistema de IA

El adjudicatario deberá definir y documentar un marco de gobernanza del dato específico para el sistema de IA objeto del contrato, que incluya, al menos:

- La identificación de los tipos de datos utilizados (por ejemplo, datos de sensores urbanos, datos de movilidad, datos ambientales, datos de imagen o vídeo, datos personales, datos seudonimizados, datos anonimizados, datos sintéticos),
- Las fuentes de datos autorizadas y las condiciones bajo las cuales pueden ser utilizadas,
- Los roles y responsabilidades relacionados con la gestión de estos datos en el ámbito del adjudicatario,
- La relación con la entidad contratante en materia de derechos de uso, acceso y tratamiento de los datos.

Este marco deberá estar alineado con las políticas de gobernanza de datos de la entidad contratante y ponerse a su disposición cuando lo solicite.

7.7.2. C_07_02 Ciclo de vida de los datos utilizados por el sistema de IA

El adjudicatario deberá describir y aplicar reglas claras para el ciclo de vida de los datos utilizados por el sistema de IA (recogida, ingestión, preprocesado, almacenamiento, uso, archivado y supresión), asegurando que:

- Únicamente se conservan durante el tiempo necesario para los fines previstos,
- Se documentan las ubicaciones y repositorios donde se almacenan,
- Se aplican las medidas de seguridad y protección de datos definidas contractualmente,
- Se contempla la supresión o devolución de datos a la entidad contratante al finalizar el contrato o cuando así se requiera.

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

7.8. D_08 Calidad, representatividad y mitigación de sesgos en datos

- **Definición del dominio**

Conjunto de medidas destinadas a garantizar que los datos urbanos utilizados por el sistema de IA tienen la calidad suficiente para los fines perseguidos, son representativos de los contextos de uso previstos y no introducen sesgos injustificados que puedan traducirse en resultados discriminatorios o inadecuados en servicios urbanos.

- **Cláusulas aplicables**

7.8.1. C_08_01 Evaluación de calidad y representatividad de los datos

El adjudicatario deberá evaluar la calidad y representatividad de los datos utilizados para entrenar, validar y operar el sistema de IA, analizando, entre otros aspectos:

- La integridad y coherencia de los datos,
- La cobertura territorial (por ejemplo, distintos barrios o zonas de la ciudad),
- La representación de distintos perfiles de uso, franjas horarias, eventos especiales o condiciones anómalas relevantes.

Las principales conclusiones de esta evaluación, incluidas las limitaciones conocidas, deberán documentarse y ponerse a disposición de la entidad contratante.

7.8.2. C_08_02 Identificación y mitigación de sesgos en los datos

El adjudicatario deberá analizar la existencia de sesgos relevantes en los datos utilizados por el sistema de IA (por ejemplo, sesgos geográficos, temporales o demográficos) y, cuando estos puedan afectar a la equidad o al trato igualitario de la ciudadanía, deberá:

- Documentar los sesgos identificados,
- Proponer y, cuando sea razonablemente posible, aplicar medidas de mitigación (reajustes de muestreo, balanceo de datos, reglas adicionales de negocio, etc.),
- Informar a la entidad contratante sobre los sesgos que no puedan eliminarse completamente, a fin de que puedan ser gestionados operativamente.

7.9. D_09 Protección de datos personales y minimización

- **Definición del dominio**

Conjunto de obligaciones orientadas a garantizar que el tratamiento de datos personales realizado por el sistema de IA cumple el RGPD, la LOPDGDD y las políticas de la entidad contratante, aplicando principios de minimización, limitación de la finalidad, seudonimización o anonimización cuando proceda y asegurando la confidencialidad de la información tratada.

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

- **Cláusulas aplicables**

7.9.1. C_09_01 Principio de minimización y limitación de la finalidad

El adjudicatario deberá garantizar que los datos personales tratados por el sistema de IA son los estrictamente necesarios para las finalidades legítimas definidas en el contrato y en la documentación de tratamiento correspondiente, y que:

- No se tratan categorías de datos que no sean imprescindibles,
- No se amplían las finalidades sin autorización expresa y por escrito de la entidad contratante,
- Se respetan los principios de licitud, lealtad y transparencia previstos en el RGPD.

Cualquier cambio en las finalidades o en los tipos de datos personales tratados deberá ser previamente autorizado por la entidad contratante.

7.9.2. C_09_02 Seudonimización, anonimización y medidas de protección

Cuando resulte apropiado para los fines perseguidos y técnicamente viable, el adjudicatario deberá aplicar técnicas de seudonimización o anonimización a los datos personales utilizados por el sistema de IA, particularmente en fases de desarrollo, pruebas y entrenamiento. En todo caso, deberá:

- Documentar las técnicas empleadas y su adecuación a los riesgos identificados,
- Evaluar los riesgos residuales de reidentificación y adoptar medidas adicionales cuando sea necesario,
- Garantizar la confidencialidad de los datos mediante controles de acceso y medidas de seguridad adecuadas conforme al RGPD, la LOPDGDD y el ENS.

7.9.3. C_09_03 Localización de datos y transferencias internacionales

El adjudicatario deberá informar a la entidad contratante sobre la localización geográfica de los datos personales tratados por el sistema de IA, incluyendo datos de entrenamiento, validación, operación y registros de actividad.

Cuando el tratamiento implique transferencias de datos personales fuera del Espacio Económico Europeo, el adjudicatario deberá:

- Informar previamente a la entidad contratante sobre los países de destino y los mecanismos de transferencia previstos,
- Garantizar que dichas transferencias se realizan al amparo de alguno de los mecanismos previstos en el capítulo V del RGPD (decisión de adecuación, cláusulas contractuales tipo, normas corporativas vinculantes u otras garantías adecuadas),
- Documentar las garantías aplicadas y ponerlas a disposición de la entidad contratante,
- No modificar la localización de los datos ni los mecanismos de transferencia sin autorización previa y por escrito de la entidad contratante.

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

En los casos en que la entidad contratante exija expresamente que los datos permanezcan dentro del Espacio Económico Europeo o dentro del territorio español, el adjudicatario deberá cumplir dicho requisito y acreditarlo con evidencia documental.

7.10. D_10 Restricciones de uso, reutilización y reentrenamiento con datos municipales

- **Definición del dominio**

Conjunto de restricciones contractuales y controles técnicos destinados a asegurar que los datos proporcionados por la entidad contratante sólo se utilizan para los fines autorizados en el contrato y que cualquier reutilización, incluida su utilización para el reentrenamiento de modelos, se realiza en las condiciones acordadas y conforme a la normativa aplicable.

- **Cláusulas aplicables**

7.10.1. C_10_01 Uso de los datos limitado al objeto del contrato

El adjudicatario se comprometerá a utilizar los datos proporcionados por la entidad contratante únicamente para la prestación de los servicios y el cumplimiento de las finalidades previstas en el contrato. Quedará expresamente prohibido el uso de estos datos para otros fines, incluyendo el entrenamiento general de otros productos o servicios del adjudicatario, salvo autorización previa, expresa y por escrito de la entidad contratante.

7.10.2. C_10_02 Condiciones para el reentrenamiento con datos municipales

Cuando se prevea el reentrenamiento del sistema de IA utilizando datos municipales proporcionados por la entidad contratante, el adjudicatario deberá:

- Obtener la autorización previa, expresa y por escrito de la entidad contratante,
- Garantizar el cumplimiento del RGPD, la LOPDGDD y las instrucciones del responsable del tratamiento,
- Documentar los datos utilizados, la justificación del reentrenamiento, los cambios introducidos en el modelo y los resultados de las pruebas realizadas,
- Poner esta documentación a disposición de la entidad contratante, especialmente cuando los cambios puedan tener impacto significativo en los servicios urbanos o en la ciudadanía.

7.11. D_11 Gestión de identidades, accesos y mantenimiento remoto

- **Definición del dominio**

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

Conjunto de controles destinados a garantizar que el acceso a plataformas de IA, consolas de administración, entornos MLOps, APIs, datos y servicios asociados al sistema de IA se limita a identidades autorizadas y se realiza bajo el principio de mínimo privilegio. Incluye tanto personas usuarias como cuentas técnicas, así como las condiciones para el acceso remoto de mantenimiento, que deberá ser autorizado, controlado y trazable.

- **Cláusulas aplicables**

7.11.1. C_11_01 Control de acceso basado en roles y mínimo privilegio

El adjudicatario deberá garantizar que el sistema de IA y sus componentes asociados soportan un modelo de control de acceso basado en roles, de forma que:

- Se diferencien claramente los perfiles de acceso (por ejemplo, administración, operación, soporte, monitorización, consulta),
- Cada cuenta disponga únicamente de los permisos estrictamente necesarios para el desempeño de sus funciones,
- Se revisen periódicamente los permisos asignados, ajustándolos cuando se produzcan cambios en el personal o en las funciones asignadas.

7.11.2. C_11_02 Gestión del ciclo de vida de identidades y cuentas técnicas

El adjudicatario deberá establecer procedimientos formales para la alta, modificación y baja de cuentas de persona usuaria y cuentas técnicas relacionadas con el sistema de IA, garantizando que:

- No se habilitan cuentas sin una solicitud y autorización previa,
- Las cuentas se desactivan o eliminan sin demora cuando dejan de ser necesarias (por cambio de funciones, salida del personal o fin del contrato),
- Las cuentas técnicas (por ejemplo, servicios, APIs, procesos automáticos) están inventariadas, asociadas a una función clara y a un responsable identificado.

7.11.3. C_11_03 Autenticación reforzada y acceso remoto de mantenimiento

El adjudicatario deberá implementar mecanismos de autenticación robusta (preferentemente autenticación multifactor) para accesos de administración, acceso remoto de mantenimiento y otros accesos con privilegios elevados. El acceso remoto al sistema de IA o a sus componentes solo podrá realizarse:

- Mediante canales y herramientas previamente autorizados por la entidad contratante,
- Con registro de la identidad de la persona usuaria, fecha, hora, origen de la conexión y acciones relevantes realizadas,
- Durante el tiempo estrictamente necesario para la actuación de mantenimiento o soporte.

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

7.12. D_12 Configuración segura y hardening de entornos de IA

- **Definición del dominio**

Conjunto de prácticas y configuraciones orientadas a que las plataformas, servicios y componentes sobre los que se despliega el sistema de IA se encuentren en un estado seguro, reduciendo al mínimo la superficie de ataque. Incluye la eliminación de configuraciones por defecto inseguras, la desactivación de servicios no necesarios y la aplicación de guías de hardening coherentes con las políticas de la entidad contratante.

- **Cláusulas aplicables**

7.12.1. C_12_01 Configuración inicial segura del sistema de IA

El adjudicatario deberá asegurar que, antes de la puesta en producción, las plataformas y servicios que soportan el sistema de IA:

- Se configuran siguiendo parámetros de seguridad recomendados por el fabricante y buenas prácticas reconocidas,
- No utilizan credenciales por defecto ni configuraciones preestablecidas inseguras,
- Se someten a una revisión básica de seguridad de configuración (por ejemplo, puertos abiertos, servicios activos, políticas de autenticación y registro).

7.12.2. C_12_02 Desactivación de servicios, puertos y funciones innecesarias

El adjudicatario deberá desactivar o limitar todos aquellos servicios, puertos y funcionalidades de las plataformas de IA que no sean imprescindibles para la prestación del servicio objeto del contrato, de manera que:

- Se reduzca la exposición del sistema a ataques externos o internos,
- Cualquier nuevo servicio que se necesite habilitar requiera justificación técnica y, cuando así se acuerde, autorización previa de la entidad contratante,
- Se mantenga documentación actualizada sobre los servicios y puertos habilitados.

7.13. D_13 Seguridad de comunicaciones, APIs y cifrado

- **Definición del dominio**

Conjunto de medidas orientadas a proteger las comunicaciones entre el sistema de IA y otros sistemas urbanos, así como las APIs y microservicios que se utilicen. Incluye el cifrado de comunicaciones, el uso de protocolos seguros, controles de autenticación y autorización en las APIs y la gestión segura de claves, certificados, tokens y otros secretos utilizados por el sistema de IA.

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

- **Cláusulas aplicables**

7.13.1. C_13_01 Comunicaciones seguras entre el sistema de IA y otros sistemas

El adjudicatario deberá garantizar que las comunicaciones entre el sistema de IA y otros sistemas o servicios urbanos:

- Se realizan mediante protocolos criptográficos actualizados y configuraciones seguras,
- Se restringen a los destinos, puertos y servicios necesarios para la prestación del servicio,
- No exponen interfaces de administración o depuración a redes no controladas o no autorizadas.

7.13.2. C_13_02 Protección de APIs y microservicios del sistema de IA

Cuando el sistema de IA exponga o consuma APIs o microservicios, el adjudicatario deberá:

- Implementar mecanismos de autenticación y autorización robustos,
- Aplicar validación de entradas, limitación de tasas y manejo controlado de errores para reducir riesgos de inyección y abusos,
- Documentar las APIs disponibles, sus usos previstos y las restricciones de seguridad asociadas, entregando esta documentación a la entidad contratante.

7.13.3. C_13_03 Gestión segura de claves, certificados y secretos

El adjudicatario deberá gestionar de forma segura las claves criptográficas, certificados, tokens, API keys y otros secretos relacionados con el sistema de IA, asegurando que:

- Se almacenan en repositorios de secretos o mecanismos equivalentes, con controles de acceso adecuados,
- Se establece y aplica una política de rotación periódica, así como rotaciones ad hoc cuando exista sospecha de compromiso,
- No se incluyen secretos en código fuente, scripts o documentación en claro.

7.14. D_14 Gestión de vulnerabilidades y dependencias

- **Definición del dominio**

Conjunto de procesos para identificar, evaluar y mitigar vulnerabilidades en las plataformas, servicios y componentes del sistema de IA, incluyendo vulnerabilidades derivadas de librerías, frameworks y otros elementos específicos de IA. El objetivo es mantener un nivel de exposición razonable y acorde con la criticidad de los servicios urbanos afectados.

- **Cláusulas aplicables**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

7.14.1. C_14_01 Proceso de gestión de vulnerabilidades y dependencias

El adjudicatario deberá disponer de un proceso documentado de gestión de vulnerabilidades que contemple:

- La consulta periódica de fuentes de información sobre vulnerabilidades (por ejemplo, bases de datos de CVEs),
- La identificación de vulnerabilidades que afecten a sistemas operativos, plataformas de IA, frameworks y librerías utilizadas por el sistema,
- La evaluación de la criticidad de dichas vulnerabilidades en función del impacto potencial sobre la seguridad y continuidad de los servicios urbanos.

7.14.2. C_14_02 Aplicación de parches y mitigación de vulnerabilidades

El adjudicatario deberá aplicar parches y medidas de mitigación de vulnerabilidades de forma planificada y acorde a su criticidad, garantizando que:

- Los parches se prueban en entornos no productivos cuando sea posible antes de su despliegue en producción,
- Las vulnerabilidades de alta criticidad se abordan dentro de plazos razonables compatibles con el nivel de riesgo,
- Cuando no sea posible aplicar un parche en plazo, se adoptan medidas compensatorias que reduzcan el riesgo a un nivel aceptable para la entidad contratante.

7.15. D_15 Registro, auditoría y trazabilidad técnica

- **Definición del dominio**

Conjunto de medidas destinadas a garantizar que el sistema de IA genera y conserva registros de actividad suficientes para permitir la auditoría técnica, el análisis forense y la trazabilidad de acciones relevantes, sin perjuicio de las obligaciones específicas de registro vinculadas al RIA u otras normas.

- **Cláusulas aplicables**

7.15.1. C_15_01 Generación y conservación de registros de actividad

El adjudicatario deberá asegurar que el sistema de IA y sus componentes asociados generan registros de actividad que recojan, al menos:

- Los accesos a plataformas de IA, consolas de administración y APIs sensibles,
- Los cambios de configuración relevantes, despliegues de nuevas versiones de modelos y ejecuciones de reentrenamiento,
- Los errores críticos y eventos de seguridad.

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

Estos registros deberán conservarse durante el tiempo que se acuerde contractualmente, respetando la normativa aplicable.

7.15.2. C_15_02 Integridad y acceso a los registros

El adjudicatario deberá proteger los registros de actividad frente a accesos no autorizados, modificaciones o borrados indebidos, y deberá:

- Implementar controles de acceso que limiten quién puede consultar y gestionar los registros (logs),
- Proporcionar mecanismos para exportar los registros a sistemas de monitorización y auditoría de la entidad contratante,
- Facilitar el acceso a dichos registros a la entidad contratante cuando ésta lo requiera para fines de auditoría, análisis de incidentes o comprobación de obligaciones contractuales.

7.16. D_16 Continuidad operativa y modo degradado sin IA

- **Definición del dominio**

Conjunto de medidas destinadas a garantizar que la entidad contratante puede mantener, en la medida de lo posible, la prestación de servicios urbanos cuando el sistema de IA sufra fallos, degradaciones graves o deba ser desactivado temporalmente, mediante mecanismos de continuidad, operación en modo degradado o procedimientos alternativos sin IA.

- **Cláusulas aplicables**

7.16.1. C_16_01 Integración del sistema de IA en los planes de continuidad

El adjudicatario deberá proporcionar a la entidad contratante la información necesaria para que el sistema de IA pueda integrarse en los planes de continuidad de negocio y recuperación ante desastres, incluyendo:

- Dependencias técnicas críticas del sistema,
- Requisitos de copias de seguridad de modelos, configuraciones y datos necesarios para su funcionamiento,
- Tiempos orientativos de restauración y recuperación tras incidentes.

7.16.2. C_16_02 Definición de modo degradado y operación sin IA

Cuando proceda, el adjudicatario deberá colaborar con la entidad contratante en la definición de:

- Mecanismos de operación en modo degradado (por ejemplo, con reglas simplificadas o modelos de menor complejidad) ante fallos o incidencias de la IA,

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

- Procedimientos para operar sin apoyo de IA en caso de desactivación prolongada del sistema, recurriendo a procesos manuales u otros medios que permitan mantener, al menos, un nivel básico de servicio.

Estos mecanismos y procedimientos deberán documentarse y revisarse periódicamente.

7.17. D_17 Seguridad en servicios cloud e IA como servicio

- **Definición del dominio**

Conjunto de requisitos y controles de seguridad aplicables cuando el sistema de IA se despliega total o parcialmente sobre servicios en la nube o se presta como IA como servicio (IAaaS), garantizando el cumplimiento de las obligaciones aplicables, la protección de datos, la segregación de entornos y la capacidad de supervisión por parte de la entidad contratante.

- **Cláusulas aplicables**

7.17.1. C_17_01 Requisitos de seguridad para servicios cloud e IAaaS

Cuando el sistema de IA se encuentre desplegado sobre servicios cloud o se ofrezca como IAaaS, el adjudicatario deberá garantizar que:

- Los servicios utilizados cumplen con los requisitos del ENS y, en su caso, con las obligaciones derivadas de NIS2,
- Existe una segregación adecuada de entornos (desarrollo, pruebas y producción) y una separación lógica suficiente respecto de otros clientes del proveedor,
- Se informa a la entidad contratante sobre la localización de los datos y las principales medidas de seguridad aplicadas por el proveedor cloud.

7.17.2. C_17_02 Monitorización y acceso a registros (logs) en entornos cloud

El adjudicatario deberá asegurar que los servicios cloud utilizados permiten:

- La generación y conservación de registros de actividad (logs) relevantes para la seguridad y el funcionamiento del sistema de IA,
- El acceso, por parte de la entidad contratante o del propio adjudicatario bajo sus instrucciones, a dichos registros (logs) para fines de supervisión, auditoría y gestión de incidentes,
- La integración de estos registros con los sistemas de monitorización y seguridad de la entidad contratante cuando ésta así lo requiera.

7.18. D_18 Gestión del ciclo de vida y versionado del modelo

- **Definición del dominio**

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

Conjunto de procesos y controles destinados a gestionar de forma estructurada el ciclo de vida de los modelos de IA utilizados en el sistema, desde su diseño y entrenamiento inicial hasta su retirada, incluyendo la identificación inequívoca de versiones, su documentación y la capacidad de revertir a versiones anteriores cuando resulte necesario.

- **Cláusulas aplicables**

7.18.1. C_18_01 Control de versiones de los modelos de IA

El adjudicatario deberá establecer y mantener un sistema de control de versiones para los modelos de IA utilizados en el marco del contrato, de modo que:

- Cada versión del modelo desplegada en entornos de la entidad contratante esté identificada de forma única,
- Se asocien a cada versión los datos básicos sobre su entrenamiento (fecha, conjunto de datos utilizado, principales parámetros, entorno de entrenamiento),
- Se mantenga un histórico de versiones, incluyendo fechas de despliegue y retirada, así como el motivo del cambio.

Esta información deberá ponerse a disposición de la entidad contratante cuando ésta lo solicite.

7.18.2. C_18_02 Mecanismos de reversión (rollback) de modelos

El adjudicatario deberá garantizar la existencia de mecanismos que permitan revertir, de manera controlada y segura, a una versión anterior del modelo en caso de:

- Detección de errores graves en la nueva versión,
- Degradación significativa del rendimiento respecto a criterios acordados,
- Impacto negativo no esperado sobre la prestación de servicios urbanos.

El procedimiento de reversión deberá estar documentado, haber sido probado previamente y poder ejecutarse sin comprometer la integridad de los datos ni la continuidad del servicio más allá de lo estrictamente necesario.

7.19. D_19 Validación previa al despliegue y tras cambios

- **Definición del dominio**

Conjunto de pruebas y revisiones que el adjudicatario debe realizar para asegurarse de que el sistema de IA cumple los requisitos técnicos, funcionales y de seguridad definidos antes de su despliegue en producción, así como tras cambios significativos o reentrenamientos del modelo.

- **Cláusulas aplicables**

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

7.19.1. C_19_01 Validación inicial antes de la puesta en producción

El adjudicatario deberá realizar, antes de la puesta en producción del sistema de IA, pruebas de validación que incluyan, al menos:

- Verificación del cumplimiento de los requisitos funcionales acordados,
- Pruebas de rendimiento y comportamiento del modelo con datos representativos del contexto urbano,
- Pruebas básicas de robustez frente a entradas anómalas o situaciones límite relevantes,
- Comprobación de que se cumplen los requisitos de seguridad definidos para el despliegue.

Los resultados de estas pruebas deberán documentarse y ponerse a disposición de la entidad contratante, que podrá condicionar la puesta en producción a su revisión y aceptación.

7.19.2. C_19_02 Validación tras cambios significativos o reentrenamientos

Tras cambios significativos en el sistema de IA, incluyendo reentrenamientos importantes del modelo, modificaciones relevantes de su arquitectura o ampliaciones del ámbito de uso, el adjudicatario deberá:

- Realizar pruebas de validación equivalentes en alcance a las de la fase inicial, adaptadas al cambio realizado,
- Documentar los resultados, indicando impacto en el rendimiento, en el comportamiento del sistema y en los riesgos identificados,
- No desplegar la nueva versión en entornos productivos hasta que las pruebas hayan sido satisfactorias y, en su caso, aceptadas por la entidad contratante.

7.20. D_20 Monitorización del modelo en producción

- **Definición del dominio**

Conjunto de medidas orientadas a supervisar de forma continua o periódica el comportamiento del modelo de IA una vez desplegado en producción, con el fin de detectar degradaciones de rendimiento, cambios en los datos de entrada (drift) y comportamientos anómalos que puedan afectar a la calidad o seguridad de los servicios urbanos.

- **Cláusulas aplicables**

7.20.1. C_20_01 Definición de métricas y umbrales de monitorización

El adjudicatario deberá definir, en coordinación con la entidad contratante cuando proceda, las métricas relevantes para la monitorización del modelo de IA en producción (por ejemplo, tasas de acierto, errores, tiempos de respuesta, tasas de rechazo) y los umbrales a partir de los cuales deba considerarse que

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

existe una degradación significativa o un comportamiento anómalo. Estas métricas y umbrales deberán documentarse y revisarse periódicamente.

7.20.2. C_20_02 Monitorización y reacción ante degradaciones

El adjudicatario deberá implementar mecanismos de monitorización que permitan:

- Recoger y analizar las métricas definidas,
- Detectar desviaciones relevantes respecto a los umbrales acordados, incluyendo fenómenos de drift en los datos de entrada o en la relación entre datos y salidas del modelo,
- Generar avisos o alertas cuando se superen dichos umbrales.

Ante la detección de una degradación significativa, el adjudicatario deberá evaluar la necesidad de aplicar medidas correctoras (reajuste, reentrenamiento, reversión de modelo) y comunicar a la entidad contratante las incidencias relevantes y las acciones propuestas.

7.21. D_21 Gestión de cambios y reentrenamiento

- **Definición del dominio**

Conjunto de procedimientos que regulan los cambios que afectan al sistema de IA y, en particular, al modelo o modelos utilizados (parámetros, arquitectura, datos de entrenamiento), así como el reentrenamiento con nuevos datos urbanos, asegurando que dichos cambios se gestionan de forma controlada y coherente con el análisis de riesgos y con la clasificación conforme al RIA.

- **Cláusulas aplicables**

7.21.1. C_21_01 Procedimientos para la gestión de cambios del modelo

El adjudicatario deberá establecer un procedimiento de gestión de cambios que contemple:

- La identificación y clasificación de los cambios (menores, mayores, sustanciales),
- La evaluación del impacto de cada cambio sobre el rendimiento, la seguridad, la protección de datos y la clasificación según el RIA del sistema, cuando proceda,
- La planificación y ejecución de pruebas asociadas al cambio, conforme al dominio D_19,
- La aprobación interna del cambio antes de su despliegue en entornos de la entidad contratante.

7.21.2. C_21_02 Reentrenamiento con nuevos datos urbanos

Cuando el sistema de IA sea objeto de reentrenamiento con nuevos datos urbanos, el adjudicatario deberá:

- Documentar los conjuntos de datos utilizados y su origen,

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

- Analizar posibles efectos del reentrenamiento sobre el rendimiento y sobre los sesgos del modelo,
- Actualizar, cuando corresponda, la documentación técnica, el análisis de riesgos y la clasificación del sistema conforme al RIA,
- Informar a la entidad contratante sobre los reentrenamientos relevantes y sus principales efectos antes de desplegar la nueva versión en producción.

7.22. D_22 Trazabilidad de inferencias y explicabilidad

- **Definición del dominio**

Conjunto de medidas orientadas a proporcionar, cuando sea necesario y conforme a la normativa aplicable, trazabilidad sobre las inferencias realizadas por el sistema de IA y mecanismos de explicabilidad que permitan al personal de operación y a las personas responsables públicas comprender, en términos adecuados, el comportamiento del sistema y las principales razones de sus recomendaciones o decisiones.

- **Cláusulas aplicables**

7.22.1. C_22_01 Trazabilidad mínima de inferencias

Cuando la naturaleza del sistema de IA y la normativa aplicable lo requieran, el adjudicatario deberá garantizar que el sistema permite registrar, al menos de forma parcial, información relevante sobre determinadas inferencias, como:

- Versión del modelo utilizado,
- Momento en que se realizó la inferencia,
- Tipo de entrada o contexto de decisión (en términos que no vulneren la protección de datos),
- Indicadores de confianza o calidad asociados, cuando existan.

Los detalles concretos de esta trazabilidad se definirán en función del caso de uso, buscando un equilibrio entre la utilidad para la supervisión y la minimización de datos personales.

7.22.2. C_22_02 Mecanismos de explicabilidad adaptados al personal de operación público

El adjudicatario deberá proporcionar mecanismos de explicabilidad, técnicos o de diseño de interfaz, que permitan al personal de operación y a las personas responsables públicas:

- Comprender, en términos comprensibles, los factores o variables que más influyen en las salidas del sistema,
- Identificar las limitaciones del modelo y los casos en los que su uso puede ser menos fiable,
- Evitar interpretaciones erróneas o una confianza injustificada en las recomendaciones generadas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Esta explicabilidad deberá diseñarse de forma proporcionada al tipo de sistema, al contexto urbano y al perfil y conocimientos de las personas usuarias previstas, sin revelar información que comprometa la seguridad o secretos industriales no necesarios para la supervisión del sistema.

7.23. D_23 Supervisión humana efectiva y límites de automatización

- **Definición del dominio**

Conjunto de medidas destinadas a garantizar que el sistema de IA se utiliza bajo una supervisión humana adecuada, manteniendo el control último de las decisiones en manos de personal competente de la entidad contratante, y evitando la automatización acrítica de decisiones que puedan afectar a la ciudadanía o a la prestación de servicios urbanos.

- **Cláusulas aplicables**

7.23.1. C_23_01 Definición de roles humanos y uso asistencial de la IA

El adjudicatario, en coordinación con la entidad contratante, deberá definir y documentar el rol que desempeñan las personas que utilizan o supervisan el sistema de IA, especificando:

- Que el sistema de IA actúa como herramienta de apoyo a la decisión o a la operación y no sustituye la responsabilidad última del personal de operación o de las personas responsables públicas, salvo que una norma específica disponga lo contrario,
- Qué tipos de decisiones o actuaciones deben ser siempre revisadas o validadas por personal humano antes de su ejecución,
- En qué casos el personal debe apartarse de la recomendación de la IA (por ejemplo, cuando la recomendación resulte contraria a la normativa, incoherente con la información disponible o injustificadamente perjudicial para un colectivo).

7.23.2. C_23_02 Controles para evitar automatización acrítica de decisiones

En la medida en que el diseño del sistema lo permita, el adjudicatario deberá implementar mecanismos que contribuyan a prevenir la automatización acrítica de decisiones, tales como:

- Requisitos de confirmación explícita por parte de la persona usuaria antes de ejecutar acciones críticas basadas en recomendaciones de la IA,
- Avisos o mensajes en la interfaz recordando las limitaciones del sistema y la necesidad de revisar las salidas en contextos sensibles,
- Restricciones para impedir que el sistema ejecute de forma completamente autónoma determinadas acciones cuando la entidad contratante exija supervisión humana.

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

7.24. D_24 Gestión de sesgos, equidad e incertidumbre

- **Definición del dominio**

Conjunto de medidas orientadas a identificar y gestionar los sesgos y desigualdades que puedan derivarse del uso de IA en servicios urbanos, así como a tratar adecuadamente la incertidumbre asociada a las salidas del sistema, fijando límites de uso y políticas de abstención cuando proceda.

- **Cláusulas aplicables**

7.24.1. C_24_01 Evaluación de sesgos y equidad en el contexto urbano

El adjudicatario deberá evaluar, con la periodicidad acordada y en colaboración con la entidad contratante cuando sea necesario, el comportamiento del sistema de IA en términos de equidad y posibles sesgos, analizando:

- Diferencias de rendimiento o de trato entre zonas geográficas, barrios o distritos,
- Impactos diferenciados en distintos colectivos de población según criterios relevantes para el uso (por ejemplo, franjas horarias, patrones de movilidad, uso de servicios),
- Posibles efectos no deseados que supongan un trato desigual injustificado en la prestación de servicios urbanos.

Los resultados de estas evaluaciones, junto con las medidas adoptadas o propuestas para mitigarlos, deberán documentarse y ponerse a disposición de la entidad contratante.

7.24.2. C_24_02 Gestión de incertidumbre y políticas de abstención

Cuando el diseño del sistema lo permita, el adjudicatario deberá incluir mecanismos que permitan:

- Estimar o indicar la confianza o calidad asociada a determinadas salidas del sistema, cuando dicho indicador sea útil para la interpretación,
- Configurar políticas de abstención o no emisión de recomendación en situaciones en las que los datos de entrada estén fuera del ámbito previsto o la incertidumbre sea excesiva para un uso seguro,
- Señalar a la persona usuaria aquellos resultados que, por su naturaleza o por el contexto, deban tratarse con especial cautela.

La entidad contratante podrá acordar, con apoyo del adjudicatario, los criterios concretos de abstención y de uso de avisos, en función del caso de uso y del impacto potencial sobre la ciudadanía.

7.25. D_25 Gestión de incidentes de ciberseguridad del sistema de IA

- **Definición del dominio**

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Conjunto de procesos, procedimientos y obligaciones de notificación destinados a garantizar la detección, contención, análisis, recuperación y comunicación de incidentes de ciberseguridad que afecten al sistema de IA, a sus componentes, a los datos que trata o a las infraestructuras sobre las que opera. Este dominio aborda amenazas como accesos no autorizados, exfiltración de datos, compromiso de componentes de la cadena de suministro, ataques de denegación de servicio, manipulación adversarial de datos o modelos y cualquier otra acción malintencionada o evento de seguridad que pueda comprometer la disponibilidad, integridad, confidencialidad o autenticidad del sistema de IA y de los servicios urbanos que dependen de él.

Este dominio es complementario al dominio D_26, que cubre los incidentes derivados del comportamiento propio del modelo de IA (errores sistemáticos, degradación del rendimiento, decisiones con impacto negativo). Ambos dominios pueden activarse de forma simultánea cuando un incidente de ciberseguridad provoque, además, un comportamiento anómalo del modelo.

- **Cláusulas aplicables**

7.25.1. C_25_01 Procedimiento de gestión de incidentes de ciberseguridad del sistema de IA

El adjudicatario deberá disponer de un procedimiento documentado de gestión de incidentes de ciberseguridad que contemple de forma específica el sistema de IA objeto del contrato. Este procedimiento deberá incluir, al menos:

- La detección y clasificación de incidentes de ciberseguridad que afecten al sistema de IA o a sus componentes (por ejemplo, accesos no autorizados a plataformas de IA o entornos MLOps, exfiltración de datos de entrenamiento o de operación, compromiso de APIs o servicios de inferencia, manipulación adversarial de datos de entrada o de modelos, ataques de denegación de servicio, compromiso de componentes de la cadena de suministro del sistema de IA),
- Los criterios para la asignación del nivel de severidad de los incidentes, teniendo en cuenta el impacto potencial sobre los servicios urbanos, la protección de datos personales y los derechos de las personas,
- Las actividades de contención, erradicación y recuperación del sistema, incluyendo, cuando proceda, la desactivación temporal del sistema de IA o su operación en modo degradado conforme al dominio D_16,
- El análisis de causa raíz y la definición, implantación y seguimiento de medidas correctoras y preventivas,
- El registro documentado de cada incidente, las acciones de respuesta adoptadas y las lecciones aprendidas.

Este procedimiento deberá estar alineado con los requisitos del ENS, la Directiva NIS2 y, cuando proceda, con las obligaciones de notificación de incidentes graves previstas en el RIA.

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

7.25.2. C_25_02 Notificación de incidentes de ciberseguridad a la entidad contratante

El adjudicatario deberá notificar a la entidad contratante los incidentes de ciberseguridad significativos que afecten al sistema de IA, con la celeridad necesaria para permitir a la entidad el cumplimiento de sus propias obligaciones de notificación conforme al RGPD, la Directiva NIS2, el RIA y demás normativa aplicable. La notificación deberá respetar, como mínimo, los siguientes criterios:

- Comunicación de una alerta temprana a la entidad contratante tan pronto como se tenga conocimiento razonable del incidente, sin demora indebida,
- Envío de una notificación más detallada en el plazo que se acuerde contractualmente, que incluya la descripción del incidente, su alcance conocido o estimado, los sistemas y datos potencialmente afectados, las medidas de contención adoptadas y el plan de análisis y recuperación previsto,
- Actualización periódica a la entidad contratante sobre la evolución del incidente hasta su resolución y cierre.

Los plazos concretos de notificación deberán definirse en el contrato y ser coherentes con los plazos establecidos por la normativa aplicable. Cuando el incidente afecte a datos personales, la notificación deberá incluir la información necesaria para que la entidad contratante pueda valorar la obligación de comunicación a la autoridad de control y, en su caso, a las personas afectadas, conforme al RGPD.

7.25.3. C_25_03 Coordinación con los procedimientos de gestión de incidentes de la entidad contratante

El adjudicatario deberá coordinar su procedimiento de gestión de incidentes de ciberseguridad con los procedimientos, equipos y herramientas de gestión de incidentes de la entidad contratante. A tal efecto, deberá:

- Designar una persona o equipo de contacto disponible para la coordinación de la respuesta a incidentes con la entidad contratante,
- Participar, cuando la entidad contratante lo requiera, en las actividades de análisis forense, contención y recuperación relacionadas con el incidente,
- Facilitar a la entidad contratante el acceso a los registros de actividad (logs), evidencias técnicas y cualquier otra información relevante para la investigación del incidente,
- Colaborar en la elaboración de los informes de incidentes que la entidad contratante deba remitir a autoridades de supervisión, equipos de respuesta a incidentes (CSIRT) o autoridades de protección de datos.

7.26. D_26 Gestión de incidentes del modelo y daños potenciales

- **Definición del dominio**

Conjunto de procesos específicos para la detección, notificación, análisis y tratamiento de incidentes relacionados con el comportamiento del modelo de IA, especialmente aquellos que se traduzcan en

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

errores sistemáticos, degradación relevante del rendimiento o decisiones con impacto negativo significativo sobre los servicios urbanos o las personas.

- **Cláusulas aplicables**

7.26.1. C_26_01 Procedimiento específico de gestión de incidentes del modelo

El adjudicatario deberá definir e implantar un procedimiento para la gestión de incidentes vinculados al modelo de IA, que incluya, como mínimo:

- Criterios para identificar qué eventos o comportamientos deben considerarse incidentes del modelo (por ejemplo, aumento súbito de errores, quejas recurrentes sobre salidas de la IA, efectos adversos en un servicio urbano),
- Canales para la notificación de estos incidentes por parte de la entidad contratante, del personal de operación o de otros terceros autorizados,
- Actividades de análisis de causa raíz (revisión de datos, configuración, cambios recientes, condiciones de uso),
- Definición, implantación y seguimiento de medidas correctoras y preventivas.

7.26.2. C_26_02 Notificación a la entidad contratante y coordinación de respuesta

El adjudicatario deberá notificar a la entidad contratante, con la mayor celeridad posible, los incidentes del modelo que puedan:

- Comprometer la calidad del servicio urbano en el que interviene la IA,
- Suponer un riesgo para la seguridad pública, la protección de datos personales o los derechos de las personas,
- Indicar un fallo relevante en el diseño, entrenamiento o configuración del sistema.

La notificación deberá incluir la descripción del incidente, su alcance potencial, las medidas provisionales adoptadas y el plan de análisis y corrección. Cuando resulte pertinente, la gestión de estos incidentes deberá coordinarse con los procedimientos generales de gestión de incidentes de seguridad de la entidad contratante.

7.27. D_27 Formación y competencias para uso seguro de IA en Smart Cities

- **Definición del dominio**

Conjunto de requisitos según el RIA orientados a asegurar que las personas que utilizan, administran o supervisan el sistema de IA cuentan con la formación y las competencias necesarias para hacerlo de forma segura, informada y alineada con las políticas de la entidad contratante.

- **Cláusulas aplicables**

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

7.27.1. C_27_01 Formación a personas usuarias y personal de operación del sistema de IA

El adjudicatario deberá proporcionar a la entidad contratante un plan de formación inicial y, cuando proceda, formación continua dirigida a las personas que utilicen o supervisen el sistema de IA, que cubra, al menos:

- La finalidad y el ámbito de uso del sistema de IA,
- Las principales funcionalidades y limitaciones del sistema,
- Las buenas prácticas para interpretar las salidas de la IA y para detectar comportamientos anómalos,
- Los procedimientos para notificar incidentes, errores o dudas relacionadas con el sistema.

La formación deberá impartirse, como mínimo, antes de la puesta en producción del sistema y cuando se introduzcan cambios significativos que afecten a su uso.

7.27.2. C_27_02 Formación y concienciación para personal técnico del adjudicatario

El adjudicatario deberá asegurar que su personal técnico implicado en el diseño, desarrollo, despliegue, operación, soporte o mantenimiento del sistema de IA dispone de formación adecuada y actualizada en:

- Ciberseguridad aplicada a sistemas y plataformas de IA,
- Protección de datos personales y obligaciones derivadas del RGPD y la LOPDGDD,
- Requisitos relevantes del RIA, del ENS y de otras normas aplicables al entorno urbano,
- Buenas prácticas de MLOps, gestión de cambios y respuesta a incidentes.

El adjudicatario deberá incluir, dentro de sus programas de concienciación interna, contenidos específicos sobre el impacto que las decisiones tecnológicas pueden tener en servicios urbanos y en la ciudadanía.

7.28. D_28 Controles específicos para IA generativa en servicios urbanos

- **Definición del dominio**

Conjunto de medidas orientadas a garantizar que el uso de sistemas de IA generativa y, en su caso, de modelos de propósito general (GPAI) en servicios municipales se realiza de forma controlada, delimitando casos de uso autorizados, evitando confusión entre contenido generado y contenido oficial y reduciendo riesgos de seguridad, privacidad y desinformación.

- **Cláusulas aplicables**

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

7.28.1. C_28_01 Delimitación de casos de uso y restricciones para IA generativa

Cuando el contrato incluya sistemas de IA generativa, el adjudicatario deberá definir y documentar, de acuerdo con la entidad contratante:

- Los casos de uso autorizados (por ejemplo, generación de borradores de comunicaciones, propuestas de textos informativos, asistencia al personal de operación en la redacción de respuestas),
- Los casos de uso expresamente no permitidos o que requieran una justificación adicional (por ejemplo, decisiones automatizadas sin supervisión, generación de contenido con efectos jurídicos directos),
- Las restricciones técnicas o procedimentales necesarias para evitar usos engañosos o inadecuados en el contexto urbano.

7.28.2. C_28_02 Avisos, revisión humana y carácter no definitivo del contenido generado

El adjudicatario deberá garantizar que las interfaces a través de las cuales se utilicen sistemas de IA generativa:

- Indican de forma clara cuándo el contenido mostrado ha sido generado o propuesto por la IA,
- Incluyen avisos adecuados recordando que el contenido generado puede requerir revisión y validación por parte de personal de la entidad contratante antes de su difusión o uso como información oficial,
- Permiten configurar flujos de revisión humana obligatoria para determinados tipos de contenido o comunicaciones sensibles.

7.29. D_29 Protección frente a abusos, exfiltración y manipulación en IA generativa y RAG

- **Definición del dominio**

Conjunto de medidas de seguridad orientadas a reducir los riesgos de uso malicioso o no deseado de sistemas de IA generativa y de soluciones que combinan IA con técnicas de recuperación aumentada (RAG) sobre datos municipales, incluyendo ataques de inyección de instrucciones, jailbreaking y fuga de información sensible.

- **Cláusulas aplicables**

7.29.1. C_29_01 Controles frente a inyección de instrucciones y jailbreaking

El adjudicatario deberá implantar, cuando proceda, controles razonables para reducir el riesgo de que:

- El sistema de IA generativa obedezca instrucciones maliciosas o contrarias a las políticas de la entidad contratante,

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

- Se eludan salvaguardas de seguridad mediante técnicas de jailbreaking u otras manipulaciones de las entradas.

Estos controles podrán incluir separación de instrucciones de sistema y de usuario, filtrado de entradas y salidas, y uso de configuraciones específicas para restringir comportamientos no deseados del modelo.

7.29.2. C_29_02 Protección frente a fuga de información y uso de RAG sobre datos municipales

Cuando el sistema de IA utilice datos municipales mediante técnicas de RAG u otros mecanismos de acceso a repositorios internos, el adjudicatario deberá garantizar que:

- El sistema no expone información confidencial o datos personales más allá de lo necesario y autorizado,
- Se aplican controles de acceso y registros adecuados sobre las fuentes de datos utilizadas,
- La entidad contratante puede conocer, al menos a nivel agregado, qué tipos de fuentes se utilizan como base para las respuestas generadas, cuando ello no comprometa la seguridad ni la protección de datos.

7.30. D_30 Reversibilidad, portabilidad y retirada del sistema de IA

- **Definición del dominio**

Conjunto de obligaciones destinadas a garantizar que, al finalizar el contrato o cuando la entidad contratante lo requiera, la retirada del sistema de IA y la transición a otro proveedor o solución se realizan de manera ordenada, preservando la continuidad de los servicios urbanos y asegurando la adecuada gestión de datos, modelos y configuraciones.

- **Cláusulas aplicables**

7.30.1. C_30_01 Plan de reversibilidad y retirada del sistema de IA

El adjudicatario deberá elaborar y acordar con la entidad contratante un plan de reversibilidad y retirada del sistema de IA, que incluya, al menos:

- Las actividades necesarias para detener el uso del sistema y desactivar sus componentes en los entornos de la entidad,
- Las condiciones y formatos de entrega de los datos municipales tratados, de las configuraciones relevantes y, cuando proceda, de los modelos y elementos necesarios para asegurar la continuidad operativa,
- Los plazos de ejecución y los recursos previstos para llevar a cabo la transición.

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

7.30.2. C_30_02 Portabilidad, devolución y borrado de datos personales

Al finalizar el contrato o cuando así lo requiera la entidad contratante, el adjudicatario deberá:

- Facilitar la portabilidad de los datos municipales y personales tratados por el sistema de IA en formatos estructurados y reutilizables acordados con la entidad contratante,
- Proceder a la devolución, borrado o, cuando se acuerde, seudonimización de los datos personales obrantes en sus sistemas o en los de terceros bajo su control, de acuerdo con las instrucciones de la entidad y la normativa de protección de datos,
- Aportar evidencia documental adecuada (por ejemplo, certificados de borrado o destrucción) que acredite el cumplimiento de las obligaciones de devolución, supresión, borrado o destrucción de los datos personales y demás soportes, repositorios, copias de trabajo y entornos donde dichos datos hubieran sido tratados, incluidos los de terceros bajo el control del adjudicatario, sin perjuicio de las obligaciones legales de conservación que resulten aplicables.

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

8. 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 (RIA). 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 las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. https://eur-lex.europa.eu/eli/reg/2016/679/oj

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

- Directiva (UE) 2022/2555 (NIS2), relativa a medidas para un elevado nivel común de ciberseguridad en la Unión. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). https://www.boe.es/eli/es/rd/2022/05/03/311

- Reglamento (UE) 2024/2847 (Cyber Resilience Act – CRA), relativo a los requisitos horizontales de ciberseguridad para productos con elementos digitales. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R2847

- ISO/IEC 42001:2023, Artificial Intelligence — Management system. https://www.iso.org/standard/81230.html

- ISO/IEC 23894:2023, Artificial intelligence — Risk management. https://www.iso.org/standard/77304.html

- ISO/IEC 27001:2022, Information security management systems — Requirements. https://www.iso.org/standard/82875.html

- NIST AI Risk Management Framework 1.0 (2023). https://www.nist.gov/itl/ai-risk-management-framework

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

9. 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.

9.1. Lista de materias tratadas en la guía

- Gobernanza y marco regulatorio de la IA en Smart Cities
- Clasificación de sistemas conforme al RIA y asignación de responsabilidades
- Gestión de riesgos y evaluación de impacto en derechos fundamentales
- Gobernanza y protección del dato urbano
- Seguridad técnica de sistemas y plataformas de IA
- Ciclo de vida del modelo: validación, monitorización y reentrenamiento
- Supervisión humana, explicabilidad y control de automatización
- Gestión de incidentes y continuidad operativa
- Seguridad en entornos cloud e IA generativa
- Reversibilidad y salida contractual del sistema de IA

9.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

9.3. Lista de servicios mencionados en la guía

No se mencionan productos específicos en la guía.

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

RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Cláusulas de seguridad para contratación pública de tecnología de IA en el entorno de Smart Cities

Enero de 2026

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía