RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Modelo de gobierno de Inteligencia Artificial en los entornos de Salud y Smart Cities

Octubre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea
NextGenerationEU

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

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD 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: 08/10/2025

Fecha de última actualización: 06/11/2025

ÍNDICE DE CONTENIDOS

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

ÍNDICE DE TABLAS

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

1. Introducción

La adopción de la Inteligencia Artificial (IA) en los sectores de Salud y de las Ciudades Inteligentes (Smart Cities) está transformando la prestación de servicios esenciales y la gestión de infraestructuras críticas. En hospitales, centros de investigación, administraciones locales y empresas públicas, los sistemas de IA ya intervienen en diagnóstico clínico, análisis de datos sanitarios, planificación terapéutica, movilidad urbana, seguridad, gestión energética y atención ciudadana.

Este avance genera nuevas capacidades institucionales, pero también introduce riesgos significativos derivados de la autonomía y opacidad de los sistemas, la posibilidad de sesgos no detectados, la dependencia de datos sensibles y las vulnerabilidades frente a incidentes de ciberseguridad. Garantizar un uso seguro, ético y conforme al marco jurídico vigente convierte la gobernanza de la IA, entendida como el conjunto de estructuras, procesos y responsabilidades que dirigen y controlan su utilización, en un elemento estratégico para las organizaciones que operan en estos entornos.

En el ámbito de la Salud, la implantación de IA está sujeta al Reglamento (UE) 2017/745 relativo a los productos sanitarios (MDR) y al Reglamento (UE) 2017/746 relativo a los productos sanitarios para diagnóstico in vitro (IVDR), que no regulan exclusivamente los sistemas de IA, pero resultan aplicables cuando estos se utilizan como dispositivos médicos o como parte de ellos. De igual modo, tanto en el sector sanitario como en las Smart Cities, el tratamiento de datos personales se rige por el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), que adapta el RGPD al ordenamiento jurídico español y resulta de aplicación complementaria en todo tratamiento de datos vinculado a la IA.

En el contexto urbano, la utilización de la IA debe alinearse con las políticas de protección de infraestructuras críticas, ciberseguridad, interoperabilidad, sostenibilidad ambiental y ética pública. La gobernanza institucional de la IA debe integrar estos marcos normativos y de riesgo, garantizando la protección de los derechos de las personas, la resiliencia organizativa y la transparencia en las decisiones automatizadas o asistidas por IA.

La presente guía establece un modelo de gobernanza de la Inteligencia Artificial, específicamente diseñado para los sectores de Salud y Smart Cities. Su propósito es dotar a las organizaciones de un marco institucional y operativo que regule la toma de decisiones sobre los sistemas de IA, defina responsabilidades claras y establezca indicadores de eficacia, seguridad, trazabilidad y transparencia, integrando la gestión del riesgo y la ciberseguridad como componentes esenciales.

El modelo se fundamenta en los principios recogidos en el Reglamento (UE) 2024/1689 (en adelante, el Reglamento europeo de Inteligencia Artificial o RIA), en la Norma Internacional ISO/IEC 42001:2023 sobre sistemas de gestión de la IA, en la Norma Internacional ISO/IEC 38507:2022 sobre gobernanza de las tecnologías de la información, en la Norma ISO 31000:2018 sobre gestión del riesgo, y en la Norma Internacional ISO/IEC 23894:2023 sobre gestión del riesgo en sistemas de IA, así como en las Directrices Éticas de la OMS (2021) para la gobernanza de la IA en la asistencia sanitaria. Con ello se consolida un marco de referencia común, basado en la gestión del riesgo y orientado a la ciberseguridad, que permite a las instituciones públicas y privadas implantar una IA fiable, auditada, segura, ciberresiliente y plenamente orientada al servicio del interés público.

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 objetivo de esta guía es proporcionar a las organizaciones públicas y privadas un marco de gobernanza de la IA centrado en la gestión de riesgos de IA y la ciberseguridad. El modelo establece principios, roles y procesos que permiten asegurar que la IA se desarrolle, implante y utilice de forma ética, segura, transparente y conforme a la legislación vigente.

La guía orienta las decisiones institucionales en materia de IA hacia la prevención y mitigación de riesgos técnicos, éticos, operativos y de ciberseguridad, promoviendo una gestión basada en la evidencia y la responsabilidad. Integra las obligaciones del Reglamento (UE) 2024/1689 (RIA), del Reglamento (UE) 2016/679 (RGPD) y de la LOPDGDD, así como las exigencias de la Directiva (UE) 2022/2555 (NIS2) y de los Reglamentos MDR e IVDR cuando resulten de aplicación. Se basa también en los estándares ISO/IEC 42001:2023, ISO/IEC 38507:2022, ISO/IEC 23894:2023, ISO 31000:2018 e ISO/IEC 27001:2022, que proporcionan las directrices técnicas para los sistemas de gestión y para la evaluación del riesgo de IA.

El propósito final es reforzar la confianza en el uso de la IA por parte de las instituciones públicas y privadas, garantizando la protección de los derechos fundamentales, la resiliencia organizativa y la rendición de cuentas ante la ciudadanía y las autoridades competentes.

2.2. Alcance

La presente guía es aplicable a todas las entidades públicas, privadas o mixtas que participen en el desarrollo, adquisición, despliegue, operación o supervisión de sistemas de IA en los sectores de Salud y Smart Cities, independientemente de su tamaño o madurez tecnológica. El ámbito de aplicación incluye, entre otros, los sistemas de IA utilizados en diagnóstico, tratamiento, gestión de pacientes o soporte clínico; las aplicaciones de IA en gestión urbana, movilidad, seguridad, energía, planificación o interacción ciudadana; y los proyectos de investigación, pilotos o soluciones en desarrollo con impacto sanitario o social.

El modelo cubre todas las fases del ciclo de vida de la IA, desde la planificación estratégica hasta la retirada del sistema, e incorpora la gestión del riesgo, la ciberseguridad y la mejora continua como principios transversales. Su diseño es escalable y adaptable a organizaciones de distinta naturaleza, complejidad o nivel de madurez tecnológica, permitiendo una implantación proporcional y eficiente de las estructuras de gobernanza requeridas por la Ley de Inteligencia Artificial (AI Act) y las normas internacionales ISO/IEC 42001, ISO/IEC 23894 y ISO/IEC 38507.

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

El presente modelo de gobernanza se fundamenta en un conjunto de normas jurídicas y estándares internacionales que establecen las obligaciones, principios y buenas prácticas que establecen los principios de seguridad, transparencia, responsabilidad y control humano:

- **Reglamento (Unión Europea) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento de Inteligencia Artificial o RIA):** Establece un marco jurídico armonizado sobre la Inteligencia Artificial en la Unión Europea. Introduce un enfoque basado en el riesgo, define obligaciones específicas para los sistemas de alto riesgo, incluidos los utilizados en el sector sanitario y en las infraestructuras críticas urbanas, y refuerza los principios de transparencia, supervisión humana y rendición de cuentas.

- **Reglamento (Unión Europea) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos – RGPD):** Reglamento 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. Aplica a todos los tratamientos de datos personales, incluidos los realizados mediante sistemas de Inteligencia Artificial.

- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Desarrolla y adapta el RGPD al ordenamiento jurídico español, estableciendo disposiciones complementarias sobre derechos digitales, transparencia en el tratamiento automatizado y supervisión de sistemas basados en IA.

- **Reglamento (Unión Europea) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios (MDR):** Regula la seguridad, validación clínica, evaluación de conformidad y seguimiento de los productos sanitarios, incluidos los sistemas de IA que actúan como dispositivos médicos o como parte de ellos.

- **Reglamento (Unión Europea) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios para diagnóstico in vitro (IVDR):** Establece los requisitos para la validación clínica, trazabilidad, conformidad y supervisión de los dispositivos de diagnóstico in vitro, incluidos aquellos que incorporan funciones de Inteligencia Artificial.

- **Directiva (Unión Europea) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022 (Directiva NIS2):** Directiva sobre medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión Europea. Aplica a entidades esenciales e importantes, incluidas infraestructuras críticas de Smart Cities y servicios sanitarios digitales.

- **ISO/IEC 42001:2023 – Sistemas de gestión de la Inteligencia Artificial:** Norma internacional que establece los requisitos para implantar, mantener y mejorar un sistema de gestión de IA, garantizando su uso responsable, seguro, transparente y conforme a los principios éticos y legales 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

- **ISO/IEC 38507:2022 – Gobernanza de las Tecnologías de la Información – Orientación para la gobernanza de la Inteligencia Artificial:** Define directrices para la integración de la IA en las estructuras de decisión corporativa, asegurando rendición de cuentas, gestión del riesgo y supervisión por parte de la alta dirección.

- **ISO/IEC 23894:2023 – Gestión del riesgo de la Inteligencia Artificial:** Proporciona un enfoque estructurado para la identificación y mitigación de los riesgos específicos derivados del desarrollo, despliegue y uso de sistemas de IA.

- **ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad**: establece los requisitos para un sistema de gestión de la seguridad de la información, aplicable a entornos de IA y sistemas digitales críticos.

- **ISO 31000:2018 – Gestión del riesgo**: ofrece principios y directrices generales para establecer un marco eficaz de gestión del riesgo organizativo, aplicable a la gestión del riesgo algorítmico y tecnológico.

- **ISO 13485:2016 – Sistemas de gestión de la calidad para productos sanitarios**: especifica los requisitos de un sistema de gestión de la calidad aplicable a la fabricación, validación y control de dispositivos médicos, incluidos los sistemas de IA que actúan como productos sanitarios o forman parte de ellos.

- **ISO 19011:2018 – Directrices para auditorías de sistemas de gestión**: proporciona principios, requisitos y orientaciones para planificar y realizar auditorías internas o externas de sistemas de gestión, incluyendo los aplicables a la gobernanza de la IA y a la calidad de productos sanitarios.

- **ISO 14001:2015 – Sistemas de gestión ambiental**: establece los requisitos para implantar y mantener un sistema de gestión ambiental que promueva la eficiencia energética, la reducción de impactos ambientales y la sostenibilidad de los sistemas de IA en entornos urbanos.

- **Directrices Éticas para una IA Confiable (Comisión Europea, 2019):** Establecen los principios de transparencia, explicabilidad, equidad, responsabilidad y supervisión humana como pilares de una Inteligencia Artificial confiable.

- **Guía de la Organización Mundial de la Salud (OMS, 2021) sobre ética y gobernanza de la IA para la asistencia sanitaria:** Define principios éticos y de rendición de cuentas aplicables al uso de sistemas de IA en salud pública, priorizando la seguridad del paciente, la equidad y la protección de los datos sanitarios.

La aplicación de este modelo deberá realizarse respetando la jerarquía normativa, otorgando prevalencia a los instrumentos jurídicos de la Unión Europea y a la legislación nacional, e integrando los estándares internacionales como marcos técnicos de referencia y apoyo a la demostración del cumplimiento regulatorio.

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

4. Definiciones

Acrónimos/Términos	Definición
RIA	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 (Ley de Inteligencia Artificial o AI Act). Introduce un enfoque basado en el riesgo, define obligaciones para proveedores, responsables de despliegue y usuarios, y establece requisitos específicos para los sistemas de IA de alto riesgo.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos. Establece los principios de licitud, lealtad, transparencia y seguridad aplicables al tratamiento de datos, incluidos los realizados mediante sistemas de IA.
LOPDGDD	Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, que adapta el RGPD al ordenamiento jurídico español y desarrolla disposiciones complementarias sobre derechos digitales y tratamientos automatizados de datos personales.
MDR / IVDR	Reglamentos (UE) 2017/745 y 2017/746 del Parlamento Europeo y del Consejo, ambos de 5 de abril de 2017, relativos a los productos sanitarios y a los productos sanitarios para diagnóstico in vitro. Establecen los requisitos de seguridad, rendimiento, trazabilidad y evaluación clínica aplicables a los dispositivos médicos y al software que actúa como producto sanitario, incluidos los que incorporan funciones de Inteligencia Artificial.
NIS2	Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas destinadas a garantizar un nivel elevado común de ciberseguridad en la Unión Europea. Amplía las obligaciones de gestión de riesgos y notificación de incidentes para entidades esenciales e importantes, incluidas las del ámbito sanitario y de las Smart Cities.
ISO / IEC	International Organization for Standardization (ISO) y International Electrotechnical Commission (IEC). Organismos internacionales de normalización responsables de elaborar estándares técnicos, entre ellos la ISO/IEC 42001:2023 (gestión de la IA), ISO/IEC 38507:2022 (gobernanza de TI e IA), ISO 31000:2018 (gestión del riesgo) y ISO/IEC 27001:2022 (seguridad de la información).
CISO	Chief Information Security Officer. Directivo responsable de la seguridad de la información y de la ciberseguridad institucional, incluyendo la protección de los sistemas de IA frente a amenazas y 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
CAIO	Chief Artificial Intelligence Officer. Responsable ejecutivo de la gestión operativa de la Inteligencia Artificial dentro de la organización. Coordina políticas, riesgos, auditorías y la conformidad normativa y ética de los sistemas de IA.
CRO	Chief Risk Officer. Responsable de coordinar y mantener el marco institucional de gestión del riesgo, incluyendo los riesgos técnicos, regulatorios y operativos asociados a la Inteligencia Artificial.
CDO	Chief Data Officer. Responsable de la gobernanza de los datos institucionales, garantizando su calidad, integridad, disponibilidad y uso conforme a la normativa aplicable.
CIO	Chief Information Officer. Responsable de la infraestructura tecnológica, la gestión de sistemas de información y la integración de la IA en la arquitectura digital de la organización.
DPO	Data Protection Officer o delegado de Protección de Datos, figura establecida por el RGPD y la LOPDGDD para supervisar el cumplimiento de la normativa de protección de datos y actuar como punto de contacto con la autoridad de control.
Sistema de IA	Sistema de software que utiliza una o varias técnicas de Inteligencia Artificial y que, con distintos grados de autonomía, genera resultados como predicciones, clasificaciones o decisiones que influyen en procesos, servicios o personas.
Modelo de IA	Representación matemática o estadística entrenada mediante datos que permite a un sistema de IA realizar inferencias, análisis o predicciones. Constituye el núcleo técnico del sistema.
Datos de salud	Datos personales relativos a la salud física o mental de una persona, incluidos los derivados de diagnósticos, tratamientos o prestación de servicios sanitarios. Están sujetos a un régimen reforzado de protección conforme al RGPD y la LOPDGDD.
Ciclo de vida de la IA	Conjunto de fases que abarcan la planificación, diseño, desarrollo, validación, despliegue, operación, supervisión, mantenimiento y retirada de un sistema de IA.
Trazabilidad	Capacidad para registrar, seguir y reconstruir las operaciones, datos, decisiones y configuraciones de un sistema de IA durante todo su ciclo de vida, garantizando transparencia y responsabilidad.
Auditoría de IA	Proceso sistemático, independiente y documentado que evalúa el grado de conformidad de un sistema de IA con los requisitos legales, técnicos, éticos y de seguridad establecidos.

Acrónimos/Términos	Definición
Evaluación de Impacto en Protección de Datos (EIPD / DPIA)	Evaluación exigida por el artículo 35 del RGPD para identificar y mitigar los riesgos que un tratamiento de datos personales, especialmente automatizado o basado en IA, puede representar para los derechos y libertades de las personas físicas.
Evaluación de Impacto en Derechos Fundamentales (EIDF)	Evaluación establecida en el AI Act para analizar el impacto potencial de un sistema de IA sobre los derechos fundamentales, la no discriminación, la transparencia y la seguridad de las personas.
Comité de Gobernanza de IA	Órgano colegiado interno responsable de supervisar la aplicación del modelo institucional de gobernanza de la IA, aprobar políticas y procedimientos, revisar evaluaciones de riesgo y autorizar la puesta en servicio de sistemas de alto riesgo.
Responsable Sectorial (Salud / Smart Cities)	Persona o unidad encargada de aplicar el modelo de gobernanza de IA dentro de su ámbito específico, garantizando el cumplimiento normativo, técnico y ético de los sistemas desplegados.
Órgano Promotor	Unidad organizativa que propone, impulsa y justifica el desarrollo o adquisición de un sistema de IA, evaluando su viabilidad técnica, su alineación estratégica y su conformidad regulatoria.
Producto sanitario	Cualquier instrumento, aparato, software o material destinado por el fabricante a ser utilizado con fines médicos específicos de diagnóstico, prevención, control o tratamiento de enfermedades, conforme al Reglamento (UE) 2017/745 (MDR).
Software as a Medical Device (SaMD)	Software destinado a cumplir una función médica específica que, por sí solo, cumple los criterios de producto sanitario establecidos en el MDR o el IVDR. Está sujeto a evaluación de conformidad y validación clínica.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Principios de la gobernanza de IA

Los principios que conforman el modelo de gobernanza de la Inteligencia Artificial (IA) definen el marco rector mediante el cual las organizaciones dirigen, controlan y evalúan el uso de sistemas de IA en los sectores de Salud y Smart Cities, basándose en un enfoque de gestión del riesgo y de ciberseguridad institucional.

Cada principio establece cómo se toman las decisiones sobre los sistemas de IA, qué responsabilidades corresponden a cada órgano y rol, y qué métricas o mecanismos de validación aseguran su correcto funcionamiento. El objetivo es garantizar que toda decisión automatizada o asistida por IA cuente con un responsable humano identificable, que los procesos sean auditables y que la tecnología se mantenga alineada con la legalidad, la ética y el interés público.

5.1. Principios generales

I. Legalidad y cumplimiento normativo.

Toda actividad vinculada al desarrollo, adquisición o utilización de sistemas de IA deberá ajustarse estrictamente al marco jurídico aplicable, incluyendo el Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial o AI Act), el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos – RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y las normativas sectoriales específicas, como los Reglamentos (UE) 2017/745 (MDR) y 2017/746 (IVDR).

La organización establecerá un proceso permanente de supervisión regulatoria y de adaptación proactiva a los cambios normativos, designará responsables de conformidad y exigirá la autorización previa del Comité de Gobernanza de IA antes de la puesta en producción de cualquier sistema, tras la verificación documental de su adecuación legal, técnica y ética.

II. Ética, derechos fundamentales y supervisión humana.

La Inteligencia Artificial debe desarrollarse y utilizarse de manera que respete la dignidad humana, la autonomía individual y los derechos fundamentales reconocidos por la Constitución Española y la Carta de Derechos Fundamentales de la Unión Europea. Toda decisión automatizada o asistida por IA que pueda tener un impacto significativo sobre las personas deberá estar sujeta a supervisión humana efectiva y ser explicable en términos comprensibles.

La organización definirá, aprobará e implementará salvaguardas de control humano proporcionadas al nivel de riesgo del sistema, incluyendo límites de uso, umbrales de confianza, protocolos de intervención y mecanismos de reversión.

III. Transparencia, trazabilidad y explicabilidad.

Las organizaciones deberán garantizar la transparencia de los sistemas de IA mediante la documentación completa y actualizada de su diseño, propósito, fuentes de datos, limitaciones y procesos de validación. Los resultados generados deberán ser comprensibles para los usuarios y

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

supervisores humanos, asegurando la posibilidad de auditar los procesos y reconstruir su lógica de decisión.

Cada organización deberá mantener un inventario institucional actualizado de todos los sistemas de IA, documentando su propósito, alcance, responsable, datos utilizados, métricas de desempeño y controles de supervisión. El responsable de inteligencia artificial o también conocido como el Chief Artificial Intelligence Officer (CAIO) será responsable de mantener dicho inventario y garantizar que los usuarios, auditores y órganos de control comprendan la lógica esencial y las limitaciones de los sistemas desplegados.

IV. Responsabilidad institucional y rendición de cuentas.

Cada sistema de IA deberá contar con un responsable claramente identificado dentro de la organización. Las responsabilidades deberán estar definidas y documentadas en la Matriz de Responsabilidades (RACI), que reflejará qué unidades ejecutan, aprueban, consultan o informan en cada proceso. La rendición de cuentas se reforzará mediante registros verificables de decisiones, revisiones periódicas y auditorías internas o externas que evalúen el cumplimiento y la eficacia de los controles establecidos.

V. Seguridad, fiabilidad y protección de datos desde el diseño.

Los sistemas de Inteligencia Artificial deberán ser seguros frente a errores, manipulaciones o ataques. Las medidas de seguridad de la información y de protección de datos personales deberán integrarse desde la fase de diseño y mantenerse durante todo el ciclo de vida del sistema, aplicando los principios de privacidad y seguridad desde el diseño y por defecto (“privacy and security by design and by default”).

La organización garantizará la integridad, disponibilidad y confidencialidad de los datos y modelos, así como la ciberresiliencia frente a amenazas o incidentes, en coherencia con la Directiva NIS2, y de conformidad con las normas ISO/IEC 27001, ISO/IEC 42001, ISO/IEC 23894 e ISO 31000, así como con las Directrices de ENISA sobre Ciberseguridad en la Inteligencia Artificial (2023).

VI. Sostenibilidad y mejora continua.

Las organizaciones deberán evaluar de forma sistemática el impacto social, ambiental y económico del uso de la Inteligencia Artificial, asegurando que esta contribuya al desarrollo sostenible, la eficiencia institucional y el bienestar ciudadano.

El modelo de gobernanza deberá incorporar mecanismos de revisión, aprendizaje y mejora continua basados en auditorías, análisis de incidentes, evaluaciones periódicas de desempeño, avances tecnológicos y cambios normativos. Estas revisiones deberán alinearse con los principios de responsabilidad y sostenibilidad definidos en la Agenda 2030, así como con los estándares ISO/IEC 42001, ISO 31000 y ISO/IEC 23894, garantizando la actualización constante del marco de control, de las políticas institucionales de IA y de los procesos de gestión de riesgos de IA y ciberseguridad.

5.2. Principios específicos del sector de Salud

Los principios específicos para el sector de la Salud complementan los principios generales del modelo de gobernanza y reflejan las obligaciones éticas, regulatorias y clínicas que rigen la aplicación de la IA en entornos sanitarios. Su propósito es garantizar que la tecnología refuerce la seguridad, la calidad asistencial y la protección de los derechos de los pacientes.

I. Primacía de la seguridad del paciente.

La seguridad del paciente constituye el eje rector de todo sistema de IA aplicado en el ámbito clínico. Los algoritmos deberán diseñarse, validarse y operarse bajo el principio de no maleficencia, asegurando que cualquier decisión automatizada o asistida por IA que pueda afectar a la salud de una persona esté sujeta a revisión médica significativa.

Se implementarán salvaguardas clínicas predefinidas y protocolos automáticos de alerta y revisión que permitan la intervención inmediata de un profesional en caso de resultados anómalos o contradictorios, de conformidad con los Reglamentos (UE) 2017/745 (MDR) y (UE) 2017/746 (IVDR), así como con las directrices técnicas de la Organización Mundial de la Salud (OMS) sobre seguridad del paciente y ética en IA.

II. Validación clínica y científica obligatoria.

Todo sistema de IA que intervenga en procesos de diagnóstico, tratamiento o soporte clínico deberá someterse a validación científica y clínica previa, conforme a los requisitos establecidos por los Reglamentos (UE) 2017/745 (MDR) y (UE) 2017/746 (IVDR).

Las pruebas de validación deberán documentarse, incluir revisiones por especialistas de la disciplina correspondiente y demostrar la seguridad, eficacia y desempeño del modelo antes de su autorización por el Comité de Gobernanza de IA. Asimismo, deberá garantizarse la trazabilidad metodológica de la validación conforme a las buenas prácticas establecidas en la ISO/IEC 42001 y la ISO/IEC 23894.

III. Supervisión médica y responsabilidad profesional.

La decisión clínica final corresponderá siempre a un profesional sanitario habilitado. El uso de sistemas de IA no exime de responsabilidad al facultativo ni a la entidad prestadora del servicio. La organización deberá establecer límites de uso, mecanismos de aprobación y umbrales de confianza que definan cuándo y cómo la IA puede ofrecer recomendaciones diagnósticas o terapéuticas, garantizando un control humano efectivo y documentado, en coherencia con los principios de supervisión humana del Reglamento europeo de inteligencia artificial.

IV. Calidad, trazabilidad y auditoría clínica.

Los sistemas deberán registrar de forma segura todas las interacciones, resultados y decisiones generadas, a fin de permitir auditorías médicas y regulatorias. Esta trazabilidad formará parte del expediente técnico del sistema, conforme a lo dispuesto en los Reglamentos (UE) 2017/745 (MDR) y (UE)

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

2017/746 (IVDR), y deberá conservarse durante todo el ciclo de vida del producto o servicio. Por otro lado, el sistema de auditoría se desarrollará en coherencia con las normas ISO 13485, ISO 19011, ISO/IEC 42001 e ISO/IEC 23894.

V. Equidad y no discriminación algorítmica.

Los datos clínicos utilizados en el entrenamiento de modelos deberán ser representativos, actualizados y libres de sesgos que puedan generar desigualdad diagnóstica o terapéutica. La organización establecerá revisiones periódicas de sesgos y adoptará medidas correctoras documentadas, de acuerdo con las directrices del RIA y las recomendaciones de la OMS.

VI. Protección reforzada de datos de salud.

Los datos de salud, considerados de categoría especial por el Reglamento (UE) 2016/679 (RGPD) en el artículo 9, requerirán medidas de seguridad reforzadas, anonimización y protocolos de acceso restringido.

Todo tratamiento deberá ampararse en una base jurídica válida y documentada, conforme al RGPD y a la Ley Orgánica 3/2018 (LOPDGDD), garantizando la confidencialidad, integridad y respeto de los derechos de los pacientes. Además, las medidas de seguridad deberán alinearse con la Directiva (UE) 2022/2555 (NIS2) y las normas ISO/IEC 27001:2022 e ISO/IEC 42001:2023, asegurando una protección integral de la información sanitaria.

5.3. Principios específicos del sector de Smart Cities

La aplicación de la Inteligencia Artificial en el entorno urbano exige un equilibrio entre innovación tecnológica, sostenibilidad ambiental y protección de los derechos digitales de la ciudadanía. Los principios siguientes establecen las bases para un uso ético y responsable de la IA en la gestión de Smart Cities.

I. Sostenibilidad ambiental y eficiencia energética.

La Inteligencia Artificial aplicada a la gestión urbana deberá contribuir activamente a los objetivos de sostenibilidad y neutralidad climática, optimizando el consumo energético y reduciendo la huella ambiental de las infraestructuras tecnológicas. Los sistemas de IA deberán diseñarse y operarse bajo criterios de eficiencia energética, uso responsable de los recursos y economía circular, priorizando modelos de despliegue sostenibles y centros de datos con bajas emisiones.

Las entidades responsables establecerán indicadores de desempeño ambiental y procedimientos de seguimiento que permitan evaluar el impacto ambiental de los sistemas de IA, en coherencia con los Objetivos de Desarrollo Sostenible (ODS), las políticas municipales de transición ecológica y los requisitos de la norma ISO 14001:2015 sobre gestión ambiental. Estas métricas deberán integrarse en el sistema de gestión de la IA conforme a la norma ISO/IEC 42001:2023, garantizando la trazabilidad y mejora continua de las prácticas de sostenibilidad durante todo el ciclo de vida de los sistemas.

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

II. Equidad digital y accesibilidad.

El uso de la IA en los servicios urbanos deberá garantizar la igualdad de acceso a la tecnología y a los servicios públicos digitales, evitando cualquier forma de discriminación directa o indirecta. Las soluciones basadas en IA deberán desarrollarse conforme a principios de accesibilidad universal, interoperabilidad y estandarización de datos, asegurando que ningún colectivo quede excluido del uso o beneficio de la tecnología.

Las entidades municipales o empresas operadoras deberán aplicar criterios de diseño inclusivo y de accesibilidad digital desde la fase de concepción de los sistemas, conforme a los principios de datos abiertos y a la norma UNE 178104, que regula la gestión inteligente de las ciudades. Los algoritmos empleados en la prestación de servicios públicos se someterán a revisiones periódicas y auditorías de sesgos, conforme a las buenas prácticas del AI Act y a las recomendaciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en materia de IA confiable y segura.

III. Seguridad pública y resiliencia.

Los sistemas de IA que intervengan en la gestión del tráfico, infraestructuras críticas, energía o seguridad ciudadana se deberán diseñarse conforme a los principios de ciberresiliencia, redundancia y continuidad operativa. La protección de estos sistemas es prioritaria, dado su papel en la estabilidad y seguridad urbana.

Las organizaciones responsables deberán incorporar la gestión del riesgo y la ciberseguridad en todas las fases del ciclo de vida del sistema, incorporando medidas de redundancia, protocolos de continuidad operativa y auditorías técnicas periódicas, en coherencia con la Directiva (UE) 2022/2555 (NIS2) y las normas ISO/IEC 22301, ISO/IEC 27001:2022, ISO/IEC 42001:2023 e ISO/IEC 23894:2023.

IV. Transparencia y participación ciudadana.

La transparencia constituye un principio esencial del modelo de gobernanza de la Inteligencia Artificial y un requisito explícito del Reglamento (UE) 2024/1689 (AI Act). Las administraciones públicas y las entidades operadoras deberán garantizar que la ciudadanía disponga de información clara, accesible y verificable sobre los sistemas de IA en funcionamiento, su finalidad, nivel de autonomía, datos utilizados, medidas de supervisión humana y resultados de las evaluaciones de riesgo.

La transparencia se materializará mediante la publicación institucional de registros actualizados de los sistemas de IA operativos, con indicación de su propósito, área responsable y nivel de riesgo, conforme a las disposiciones del AI Act. Asimismo, se fomentará la participación pública a través de portales digitales accesibles y canales de comunicación que permitan a la ciudadanía presentar observaciones, reclamaciones o solicitudes de información sobre el uso de la IA en los servicios urbanos, promoviendo la confianza y la rendición de cuentas en la gestión tecnológica.

V. Ética pública y rendición de cuentas.

El uso de la Inteligencia Artificial en la gestión urbana deberá regirse por los principios de integridad, proporcionalidad, equidad y responsabilidad pública. Las entidades deberán disponer de mecanismos

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

de rendición de cuentas que permitan demostrar la conformidad ética, técnica y legal de sus sistemas de IA ante los órganos de control y la ciudadanía.

Estas obligaciones deberán alinearse con la Carta de Derechos Digitales y con los principios del AI Act, que establecen la supervisión humana, la explicabilidad y la trazabilidad como elementos esenciales de una IA confiable. La rendición de cuentas incluirá la elaboración periódica de informes de evaluación ética y de impacto, los cuales deberán ser accesibles públicamente y formar parte del registro institucional 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

6. Estructura organizativa y de gobernanza

La estructura organizativa del modelo de gobernanza de la Inteligencia Artificial tiene como finalidad garantizar que las funciones de dirección, gestión, supervisión y control de los sistemas se ejerzan de manera coordinada, transparente y verificable. Este marco permite asignar responsabilidades precisas, asegurar la trazabilidad de las decisiones y reforzar la rendición de cuentas institucional ante los órganos directivos, las autoridades competentes y la ciudadanía.

El modelo se articula en tres niveles funcionales interdependientes, orientados a la gestión integral del riesgo y la ciberseguridad de los sistemas de IA:

- **Nivel estratégico**: define las políticas, aprueba el marco normativo, supervisa el cumplimiento global y evalúa los riesgos institucionales.
- **Nivel táctico:** coordina la gestión operativa de riesgos, aplica controles y asegura la coherencia de las políticas aprobadas.
- **Nivel operativo**: ejecuta la validación técnica, mantenimiento, seguridad y mejora continua de los sistemas de IA, garantizando trazabilidad y resiliencia.

Cada nivel cumple funciones específicas y complementarias, asegurando una interacción que refuerce el control interno y la coherencia del modelo tanto en el sector Salud, conforme a los Reglamentos (UE) 2017/745 (MDR) y 2017/746 (IVDR), como en el sector Smart Cities, conforme a la norma UNE 178104 y las directrices de equidad y sostenibilidad digital.

Además, la estructura organizativa deberá aplicarse con criterios de proporcionalidad, adaptándose al tamaño, complejidad y nivel de madurez tecnológica de cada entidad. Las organizaciones de menor escala podrán concentrar funciones bajo una misma figura, siempre que se preserve la independencia funcional y la trazabilidad de decisiones. En entidades de gran tamaño o con sistemas de IA de alto riesgo, las funciones deberán segregarse de forma clara y documentada.

6.1. Establecimiento Formal del Comité de Gobernanza de IA

La creación del Comité de Gobernanza de IA constituye el acto fundacional del modelo de gobierno de IA institucional. Este proceso debe formalizarse mediante un acto administrativo de la máxima dirección de la organización que otorgue la legitimidad y autoridad necesarias para el ejercicio de sus funciones.

6.1.1. Proceso de Creación y Mandato

La creación formal del Comité se realizará mediante la emisión de una resolución o acuerdo equivalente de la Alta Dirección. Dicho instrumento jurídico-interno contendrá, como mínimo, los siguientes elementos:

- ✓ **Base legal y justificación**: Referencia expresa al Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial), a las normativas sectoriales aplicables (MDR, IVDR, NIS2) y a la presente guía como marco de referencia.

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

- ✓ **Objetivo y finalidad**: Delimitación clara del ámbito competencial del Comité, especificando su naturaleza asesora, de supervisión y de decisión en materia de gobierno de IA.

- ✓ **Composición y nombramientos:** Designación formal de los miembros titulares y suplentes, indicando el cargo institucional que representan. Se establecerá un mecanismo para la renovación periódica de sus componentes.

- ✓ **Régimen de funcionamiento:** Determinación de la periodicidad de las reuniones ordinarias (mínimo trimestral), procedimiento para convocatorias extraordinarias, y quórum de constitución y adopción de acuerdos.

- ✓ **Atribuciones y facultades:** Enumeración exhaustiva de las competencias decisorias, entre las que se incluirán expresamente la aprobación de la Política Institucional de IA, la autorización de despliegue de sistemas de alto riesgo, y la asignación de recursos para la implementación del modelo de gobierno de IA dentro de la organización.

- ✓ **Dotación de recursos**: Previsión expresa de los medios personales, materiales y presupuestarios necesarios para el adecuado desempeño de las funciones encomendadas.

6.1.2. Composición del Comité

El Comité de Gobernanza de IA estará integrado por representantes de la Alta Dirección y responsables de las áreas funcionales críticas para la gestión del riesgo y ciberseguridad de la IA. La composición mínima obligatoria será la siguiente:

- **Presidencia o Alta Dirección:** ejerce la presidencia del Comité y asume la rendición de cuentas final ante los órganos de gobierno y las autoridades competentes.

- **Responsable de Inteligencia Artificial (Chief Artificial Intelligence Officer – CAIO):** coordina el inventario institucional de sistemas, las evaluaciones de impacto y la coherencia documental del modelo.

- **Responsable de Tecnología de la Información (Chief Information Officer – CIO):** encargado de la infraestructura tecnológica, interoperabilidad y seguridad operacional.

- **Responsable de Datos (Chief Data Officer – CDO):** garantiza la calidad, integridad y gobernanza de los datos.

- **Delegado de Protección de Datos (Data Protection Officer – DPO):** asegura el cumplimiento del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos – RGPD) y de la normativa nacional aplicable.

- **Responsable de Riesgos de Inteligencia Artificial (Chief Risk Officer – CRO):** encargado de la gestión de riesgos algorítmicos, éticos, técnicos y operativos.

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

- **Responsable de Seguridad de la Información (Chief Information Security Officer – CISO):** responsable de la ciberseguridad institucional conforme a la norma ISO/IEC 27001:2022.

- **Responsable de Ética y Derechos Fundamentales:** encargado de la revisión ética, del control de sesgos y de la protección de los derechos individuales.

- **Responsable Sectorial (Sanidad o Smart Cities):** aporta la perspectiva técnica y de política pública específica del ámbito en el que se despliega la IA.

- **Secretaría Técnica:** responsable de la gestión administrativa, la custodia documental y la elaboración de actas y dictámenes.

- **Responsable de Cumplimiento Normativo (Chief Compliance Officer – CCO):** figura recomendada pero no obligatoria para organizaciones de gran tamaño o con sistemas de alto riesgo, con el fin de supervisar la alineación del modelo de gobernanza de la IA con el marco regulatorio vigente y los principios de ética pública, integridad y transparencia institucional. Participará en la revisión de las políticas internas, en la evaluación de cumplimiento transversal y en la prevención de incumplimientos legales o éticos. En entidades de menor tamaño o con baja exposición regulatoria, podrá actuar como figura asesora o invitado permanente.

La composición del Comité deberá reflejar equilibrio entre perfiles técnicos, jurídicos y éticos, así como independencia funcional. Podrán incorporarse expertos externos o representantes de otras entidades públicas o privadas cuando la materia lo requiera.

El Comité se reunirá con carácter ordinario al menos una vez por trimestre y con carácter extraordinario ante incidentes graves, cambios regulatorios relevantes o revisiones del modelo. Las convocatorias se realizarán con antelación suficiente e incluirán el orden del día, la documentación de soporte y las propuestas de resolución y todas las decisiones se documentarán en actas oficiales, firmadas por la presidencia y la secretaría, que se incorporarán al Registro Institucional de Gobernanza.

En cuanto a sus **funciones principales**, el Comité desempeñará, entre otras, las siguientes funciones:

I. Aprobación de políticas y directrices

Aprobar la Política Institucional de IA, las normas internas y las directrices sobre transparencia, supervisión humana y gestión de datos.

II. Evaluación y supervisión de riesgos

Analizar los informes presentados por el CAIO, el responsable de Riesgos de IA y el DPO, y adoptar decisiones sobre mitigación, suspensión o mejora de sistemas cuando sea necesario.

III. Autorización de sistemas de alto riesgo

Validar, antes de su puesta en funcionamiento, los sistemas clasificados como de alto riesgo según el AI Act, basándose en las evaluaciones técnicas, éticas y de protección de datos.

IV. Seguimiento del cumplimiento y desempeño

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

Revisar los indicadores institucionales de desempeño y riesgo, evaluar el grado de cumplimiento normativo y promover acciones correctoras o preventivas.

V. Gestión ética y resolución de controversias

Analizar los dilemas éticos o conflictos de interés relacionados con la IA y emitir resoluciones motivadas, registradas formalmente.

VI. Informe anual de gobernanza

Elaborar y presentar ante la Alta Dirección un informe consolidado sobre cumplimiento, riesgos y auditorías, que sirva como base para la revisión estratégica y la mejora continua.

6.2. Roles y responsabilidades

La organización definirá y aprobará formalmente la designación de las funciones que intervienen en el gobierno de la Inteligencia Artificial. El responsable de Inteligencia Artificial (Chief Artificial Intelligence Officer, CAIO) elaborará la propuesta de roles y responsabilidades, que será revisada y aprobada por el Comité de Gobernanza de IA. Cada rol deberá disponer de autoridad suficiente, líneas de reporte claras y actividades expresas de cumplimiento. Las responsabilidades asignadas deberán integrarse en los estatutos, reglamentos internos o políticas institucionales correspondientes.

La efectividad del gobierno de la inteligencia artificial exige el establecimiento de una estructura organizativa formal con roles, responsabilidades y cadenas de reporte claramente definidas. Se establecen los siguientes roles como mínimos indispensables:

6.2.1. Roles a nivel estratégico

El nivel estratégico agrupa las funciones de dirección, supervisión y control general del modelo de gobernanza de la Inteligencia Artificial. Desde este nivel se establecen las políticas institucionales, se definen las prioridades estratégicas y se garantizan los mecanismos de rendición de cuentas ante los órganos de gobierno y las autoridades competentes. Su función esencial es asegurar que la gestión de la IA se integre en la estrategia organizativa, que los riesgos sean adecuadamente evaluados y que el uso de la tecnología responda a criterios de legalidad, seguridad, transparencia y beneficio público.

El nivel estratégico proporciona el marco de decisión dentro del cual se desarrollan las actuaciones tácticas y operativas. Establece las líneas maestras de actuación, asigna los recursos necesarios y supervisa el cumplimiento de las normas internas, de la legislación aplicable y de los principios éticos que orientan el modelo. De esta manera, garantiza que la Inteligencia Artificial se emplee de forma responsable, conforme al Reglamento (UE) 2024/1689 y a las normativas sectoriales y nacionales relacionadas.

Dentro de este nivel se incluyen dos actores principales:

- **Comité de Gobernanza de IA:** Órgano colegiado responsable de la dirección estratégica y del control general del modelo de gobierno de IA. Entre sus funciones destacan la aprobación de la política Institucional de IA, la definición del umbral de riesgo organizacional, la autorización del despliegue de sistemas IA de alto riesgo, y la evaluación periódica de la eficacia de los controles

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

internos. Asimismo, supervisa la correcta aplicación de las medidas de seguridad, ética y protección de datos, revisa los informes elaborados por los responsables técnicos y promueve la mejora continua del modelo de gobernanza. Sus decisiones garantizan la coherencia institucional y la rendición de cuentas ante la Alta Dirección y los organismos reguladores.

- **Alta Dirección**: Asume la responsabilidad final sobre el uso de la Inteligencia Artificial en la organización. Le corresponde refrendar las políticas y decisiones estratégicas aprobadas por el Comité, dotar de legitimidad y recursos al modelo, e integrar la gobernanza de la IA en la planificación institucional. También es responsable de la coherencia de las decisiones generadas por los sistemas de IA con los valores de la organización y con las políticas de sostenibilidad, equidad y protección de los derechos fundamentales.

6.2.2. Roles a nivel táctico

El nivel táctico tiene como objetivo transformar las directrices estratégicas en acciones concretas de gestión, coordinación y control. Este nivel garantiza la implementación coherente de las políticas aprobadas y supervisa la operativa técnica y organizativa de los sistemas de IA.

- **Responsable de Inteligencia Artificial (Chief Artificial Intelligence Officer – CAIO):** ejecutivo responsable de la gestión operativa del portafolio de sistemas de IA. Sus funciones incluyen la coordinación centralizada de todas las iniciativas, el mantenimiento del inventario institucional, la dirección de las evaluaciones de impacto y la supervisión de la integración de los principios de gobernanza en el ciclo de vida de los sistemas. Actúa como enlace permanente entre el Comité de Gobernanza de IA y las unidades operativas, elaborando los informes periódicos de seguimiento.

- **Responsable de Ciberseguridad (Chief Information Security Officer – CISO):** titular de la seguridad de la información y la ciberresiliencia institucional. Le corresponde la evaluación de vulnerabilidades en modelos y entornos de IA, la definición de arquitecturas seguras, la coordinación de la respuesta a incidentes y la validación técnica de los controles de seguridad antes del despliegue en producción. Dispone de autoridad funcional para suspender preventivamente la operación de sistemas que presenten vulnerabilidades críticas.

- **Delegado de Protección de Datos (Data Protection Officer – DPO):** supervisor del cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la normativa nacional aplicable. Ejerce funciones de consulta y aprobación previa en las Evaluaciones de Impacto en Protección de Datos, garantiza el ejercicio de los derechos de los interesados y actúa como punto de contacto con la autoridad de control.

- **Responsable de Riesgos de Inteligencia Artificial (Chief Risk Officer – CRO**): encargado del marco metodológico de gestión de riesgos de la organización aplicado a la IA. Desarrolla y mantiene los procedimientos para la identificación, evaluación y tratamiento de los riesgos técnicos, éticos, legales, operativos y de ciberseguridad asociados a los sistemas de IA. Elabora

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 mapa institucional de riesgos y emite dictámenes preceptivos sobre el perfil de riesgo de cada sistema antes de su autorización por el Comité.

- **Responsable de Datos (Chief Data Officer – CDO):** encargado de garantizar la calidad, integridad y gobernanza de los datos utilizados en los sistemas de IA. Define políticas de gestión de datos, valida la representatividad de los conjuntos de entrenamiento y vela por la interoperabilidad y trazabilidad de la información.

- **Responsable de Ética y Derechos Fundamentales:** figura encargada de promover la equidad, transparencia y respeto a los derechos fundamentales en el diseño y uso de la IA. Evalúa la existencia de sesgos, emite recomendaciones correctoras y supervisa la integración de los principios éticos en el ciclo de vida de los sistemas.

- **Responsable de Cumplimiento Normativo (Chief Compliance Officer – CCO):** figura no obligatoria encargada de garantizar la coherencia normativa y la alineación del modelo de gobernanza de la IA con el resto del marco regulatorio aplicable (protección de datos, seguridad, ética pública, contratación, transparencia y derechos digitales). Supervisa el cumplimiento transversal de las obligaciones legales y éticas, emite dictámenes de conformidad y colabora con el DPO, el CAIO y el responsable de Ética en la detección y mitigación de incumplimientos. En organizaciones de gran tamaño o con sistemas de alto riesgo, formará parte permanente del Comité de Gobernanza de IA; en entidades de menor tamaño, puede actuar como asesor o invitado permanente.

6.2.3. Roles a nivel operativo

El nivel operativo constituye la base de ejecución del modelo de gobernanza de la Inteligencia Artificial. Desde este nivel se materializan las directrices establecidas por los niveles estratégico y táctico, asegurando la correcta implementación técnica, la seguridad, la calidad y la trazabilidad de los sistemas de IA durante todo su ciclo de vida.

Su finalidad es garantizar que el desarrollo, el despliegue y la operación diaria de los sistemas se realicen conforme a los principios de legalidad, seguridad, ética, transparencia y mejora continua, bajo la supervisión y validación del nivel táctico.

Dentro de este nivel se establecen los siguientes roles y funciones esenciales:

- **Órgano Promotor:** Unidad organizativa o área funcional que identifica la necesidad de un sistema de IA, justifica su alineación con los objetivos institucionales y asume la responsabilidad principal sobre los resultados e impactos derivados de su uso. Participa en la definición de requisitos funcionales, en la validación de resultados y en la supervisión de la correcta aplicación del sistema dentro de su ámbito de competencia.

- **Equipos de Desarrollo de IA:** Responsables del diseño, entrenamiento, validación y documentación de los modelos de IA. Aplican los principios de ethics by design y security by design, garantizan la calidad, integridad y representatividad de los datos de entrenamiento, documentan las decisiones técnicas adoptadas y aseguran la trazabilidad completa del proceso

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

de desarrollo. Todas las versiones, ajustes y evaluaciones deberán registrarse en los repositorios institucionales de gobernanza.

- **Equipos de Implementación y Operaciones:** Encargados del despliegue técnico en entornos de producción, la integración con los sistemas existentes, la monitorización del funcionamiento y el mantenimiento preventivo y correctivo de los sistemas de IA. Ejecutan las actualizaciones de software, aplican parches de seguridad, gestionan incidentes técnicos y reportan periódicamente al responsable de Inteligencia Artificial (CAIO), al responsable de Ciberseguridad (CISO) y al delegado de Protección de Datos (DPO) sobre cualquier desviación, anomalía o vulnerabilidad detectada. También son responsables de mantener los registros de operación y evidencias de cumplimiento para auditorías internas o externas.

La actuación del nivel operativo deberá regirse por procedimientos documentados que definan responsabilidades, flujos de información, requisitos de validación y mecanismos de control. Toda acción o decisión técnica deberá quedar registrada en un repositorio Institucional de gobernanza de IA, asegurando la trazabilidad, verificabilidad y conservación de la evidencia.

En los sistemas clasificados como de alto riesgo, ninguna implementación, modificación o mantenimiento sustancial podrá realizarse sin la validación formal del Comité de Gobernanza de IA, conforme a los dictámenes preceptivos emitidos por el CAIO, el CRO, el CISO y el DPO.

6.2.4. Roles específicos del sector Salud

En el ámbito sanitario, la gobernanza de la Inteligencia Artificial debe garantizar la seguridad del paciente, la eficacia clínica y la conformidad con los Reglamentos (UE) 2017/745 (MDR), 2017/746 (IVDR) y 2024/1689 (Ley de Inteligencia Artificial), así como con las normas internacionales ISO 13485, IEC 62304 e ISO 14971.

Por ello, las organizaciones del sector Salud deberán incorporar los siguientes roles, diferenciando entre los obligatorios y los condicionales, conforme al tipo de sistema de IA, su nivel de riesgo y la naturaleza de la entidad (fabricante, desarrollador, operador o usuario).

Roles obligatorios:

- **Responsable Clínico de Validación de IA:** Profesional sanitario designado por la dirección médica o la gerencia, con autoridad formal para aprobar y supervisar el uso clínico de los sistemas de Inteligencia Artificial antes de su implantación. Es responsable de verificar la seguridad del paciente, la validez científica de los resultados y la conformidad del sistema con los requisitos de rendimiento, documentación técnica y vigilancia post comercialización establecidos en los Reglamentos MDR e IVDR. Este rol es obligatorio en toda organización que utilice IA en procesos de diagnóstico, tratamiento, monitorización o toma de decisiones clínicas, o que opere sistemas clasificados como de alto riesgo conforme al AI Act.

- **Coordinador de Seguridad del Paciente y Vigilancia de IA:** Figura responsable de la detección, notificación y gestión de incidentes o desviaciones relacionados con el funcionamiento de los sistemas de IA que puedan afectar la seguridad clínica. Supervisa la trazabilidad de los eventos adversos, la implementación de medidas correctoras y la comunicación con las autoridades

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

sanitarias competentes. Es obligatorio en todas las organizaciones que desplieguen sistemas de IA que influyan en decisiones clínicas o en la seguridad de pacientes, de conformidad con las obligaciones de vigilancia y gestión de riesgos del MDR y IVDR.

Roles condicionales:

- **Comité Médico de Evaluación de IA:** Órgano multidisciplinar que integra perfiles clínicos, técnicos y éticos, encargado de evaluar la idoneidad, eficacia, riesgos y beneficios de los sistemas de IA.

  Su establecimiento es obligatorio cuando la entidad:

  ✓ desarrolla, fabrica o integra sistemas de IA clasificados como de alto riesgo bajo el AI Act, o
  ✓ despliega IA que interviene directamente en decisiones diagnósticas, terapéuticas o de investigación clínica.

  En organizaciones que únicamente sean usuarias de sistemas certificados de bajo riesgo o de apoyo administrativo, este comité podrá sustituirse por un comité ético o de innovación existente que asuma formalmente sus funciones de revisión técnica y ética.

6.2.5. Roles específicos del sector Smart Cities

En el ámbito de las Smart Cities, la gobernanza de la Inteligencia Artificial debe garantizar la transparencia, la equidad, la sostenibilidad y la rendición de cuentas, en coherencia con el Reglamento (UE) 2024/1689 (Ley de IA), la Directiva (UE) 2022/2555 (NIS2), la norma UNE 178104:2017 sobre gestión inteligente de la ciudad y las normas ISO 37120 e ISO 37122 sobre servicios urbanos sostenibles y resilientes.

Las administraciones públicas, organismos locales y operadores de servicios inteligentes deberán integrar en su estructura los siguientes roles.

Roles obligatorios:

- Responsable de Impacto en el Servicio Público: Profesional con competencias en políticas urbanas, sostenibilidad y equidad digital, encargado de evaluar los impactos sociales, éticos, económicos y ambientales derivados del uso de sistemas de IA en la gestión urbana. Este rol es obligatorio en toda entidad pública o concesionaria que utilice IA en la prestación de servicios públicos o en procesos administrativos que afecten derechos ciudadanos (movilidad, energía, gestión ambiental, seguridad, planificación urbana, etc.). Debe elaborar un Informe Anual de Impacto Algorítmico, remitido al CAIO y al Comité de Gobernanza de IA, que documente resultados, riesgos y medidas mitigadoras.

- **Coordinador de Datos Urbanos e Interoperabilidad**: Responsable de asegurar la calidad, integridad, interoperabilidad, seguridad y apertura de los datos utilizados en los sistemas de IA urbanos. Coordina con el CDO y el CISO las políticas de gobernanza de los datos establecidas en la norma UNE 178104 y la Directiva (UE) 2019/1024 sobre datos abiertos. Su designación es obligatoria en cualquier organización que gestione infraestructuras inteligentes, redes interconectadas o datos urbanos críticos para la prestación de servicios.

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

- Responsable de Participación Ciudadana y Transparencia Algorítmica: Figura institucional encargada de garantizar la transparencia activa, la comunicación pública y la rendición de cuentas sobre el uso de IA. Supervisa la publicación en portales de transparencia o datos abiertos de información sobre los sistemas de IA operativos —su finalidad, nivel de autonomía, criterios de decisión y salvaguardas de supervisión humana— conforme al artículo 52 del AI Act y a la UNE 178104. Gestiona canales de participación, consultas y reclamaciones ciudadanas, y promueve la confianza pública en el uso de IA. Este rol es obligatorio en todas las entidades públicas o mixtas cuyo uso de IA tenga impacto directo en la ciudadanía o en la gestión de recursos públicos.

6.3. Modelos de relación y coordinación

La gobernanza efectiva de la Inteligencia Artificial requiere una coordinación continua y verificable entre los distintos actores internos y externos involucrados en su ciclo de vida. Esta coordinación se articula a través de mecanismos formales que garanticen la coherencia entre las políticas institucionales, los procesos técnicos y los criterios éticos, permitiendo una gestión integrada de riesgos, cumplimiento y calidad.

El modelo define dos ámbitos de coordinación: la relación interna, que regula las interacciones entre las unidades de la organización, y la relación externa, que abarca la cooperación con terceros, autoridades, entidades colaboradoras y ciudadanía.

6.3.1. Relación interna

La relación interna tiene como objetivo asegurar que todas las áreas funcionales implicadas en el uso de la IA actúen bajo principios de cooperación, transparencia y rendición de cuentas. Cada fase del ciclo de vida de los sistemas de IA deberá ser gestionada con claridad en cuanto a las competencias y dependencias jerárquicas, evitando duplicidades o vacíos de control.

La organización deberá establecer una Matriz de Responsabilidades (RACI), que determinará para cada proceso quién es responsable de su ejecución (Responsible), quién aprueba y asume la rendición de cuentas (Accountable), quién debe ser consultado (Consulted) y quién informado (Informed). La matriz RACI se encuentra incluida en el **Anexo A** de esta guía, donde se detallan las responsabilidades aplicables a la gestión del riesgo de IA en las distintas fases del ciclo de vida de los sistemas.

Cada entidad podrá adaptar o ampliar dicha matriz para cubrir otros procesos o ámbitos del ciclo de vida (diseño, desarrollo, validación, despliegue, operación o retirada), manteniendo su coherencia metodológica y siempre bajo custodia del CAIO y aprobación del Comité de Gobernanza de IA.

Sin embargo, es necesario asegurar que las interacciones entre las áreas de tecnología, datos, ética, legal, seguridad y negocio se regirán por protocolos formales que contemplen los siguientes aspectos:

- **Flujos de información:** deberán establecerse canales claros, direccionales y documentados para la transmisión de decisiones, incidentes y resultados de evaluación. Esta comunicación estructurada permite asegurar la coherencia institucional y evitar solapamientos o vacíos de responsabilidad.

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

- **Aprobaciones cruzadas**: toda modificación significativa de algoritmos, conjuntos de datos, modelos de entrenamiento o criterios de uso requerirá la validación formal del Comité de Gobernanza de IA antes de su implementación.

- **Coordinación operativa:** los equipos de desarrollo, validación y explotación deberán colaborar bajo la supervisión del CAIO, garantizando que las medidas de seguridad, privacidad y ética se integren desde el diseño.

- **Trazabilidad documental:** las deliberaciones, validaciones y aprobaciones deberán quedar reflejadas en informes de conformidad o actas internas, conservadas en el registro institucional de gobernanza.

La relación interna se apoyará además en reuniones de coordinación periódicas entre el CAIO, el responsable de Ciberseguridad, el DPO y el responsable de Riesgos, a fin de revisar los incidentes registrados, las no conformidades y los indicadores de desempeño de los sistemas activos.

6.3.2. Relación externa

La relación externa del modelo de gobernanza abarca las interacciones con todas las entidades y partes interesadas fuera de la organización que puedan tener impacto en el desarrollo, suministro, supervisión o uso de sistemas de IA. Estas relaciones deberán formalizarse mediante contratos, convenios o acuerdos marco que incluyan cláusulas específicas de cumplimiento normativo y ético.

Los ámbitos principales de relación externa son los siguientes:

- **Proveedores tecnológicos:**
  Los contratos con proveedores de soluciones o componentes de IA deberán incorporar cláusulas que obliguen al cumplimiento de este modelo de gobernanza, a la transparencia en la documentación técnica y a la colaboración en auditorías. Deberá garantizarse el acceso a información sobre los algoritmos, datos de entrenamiento, métricas de validación y límites de uso. Los proveedores serán responsables de los incumplimientos o desviaciones detectadas en sus productos o servicios. En el sector sanitario, estos contratos deberán contemplar expresamente las obligaciones derivadas de los Reglamentos (UE) 2017/745 (MDR) y (UE) 2017/746 (IVDR), así como las certificaciones clínicas o de calidad requeridas. En el ámbito de Smart Cities, se exigirá el cumplimiento de la norma UNE 178104 y de las directrices municipales sobre interoperabilidad y seguridad urbana.

- **Entidades colaboradoras:**
  Las relaciones con universidades, centros de investigación, startups o instituciones sanitarias se regularán mediante acuerdos de colaboración que definan de manera explícita los derechos de propiedad intelectual, el régimen de uso de los datos, los principios éticos aplicables y las obligaciones de confidencialidad. Toda cooperación estará sujeta a evaluación previa del Comité de Gobernanza de IA, que verificará su alineación con las políticas institucionales y la normativa 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

- **Autoridades competentes y organismos reguladores:**
  La organización mantendrá comunicación activa y transparente con las autoridades competentes en materia de sanidad, protección de datos, ciberseguridad e inteligencia artificial. Deberán establecerse protocolos de notificación inmediata de incidentes graves, vulneraciones de seguridad o incumplimientos que afecten a sistemas de alto riesgo, conforme a lo previsto en el Reglamento (Unión Europea) 2024/1689 y el Reglamento (Unión Europea) 2016/679. Asimismo, la organización cooperará en procesos de supervisión, inspección o auditoría requeridos por organismos nacionales o europeos.

- **Ciudadanía y usuarios finales:**
  En el caso de los sistemas de IA que interactúan directamente con la población, la organización deberá garantizar la transparencia y accesibilidad de la información sobre su uso. Se habilitarán mecanismos para que los ciudadanos puedan conocer la finalidad y funcionamiento general de los sistemas, así como canales seguros y accesibles para la presentación de reclamaciones, incidencias o solicitudes de información, en coherencia con los principios de transparencia activa y la Carta de Derechos Digitales. En Smart Cities, esta transparencia podrá materializarse mediante portales de datos abiertos o paneles digitales. En Salud, deberá expresarse mediante información dirigida a pacientes y profesionales, en lenguaje claro y no técnico.

Toda la documentación y trazabilidad derivada de estas relaciones se conservará en un repositorio institucional de gobernanza de IA.

6.3.3. Flujos de información y coordinación

Los flujos de información y mecanismos de coordinación constituyen el soporte operativo del modelo de gobernanza de la Inteligencia Artificial. Su propósito es garantizar que las decisiones, informes y actuaciones derivadas del ciclo de vida de los sistemas de IA se comuniquen de forma oportuna, verificable y bidireccional entre todos los niveles organizativos.

Entre os principios generales se encuentra:

- **Trazabilidad y registro**: Toda comunicación o intercambio de información relacionado con la gestión de sistemas de IA deberá quedar documentado en el Repositorio Institucional de Gobernanza, garantizando integridad, autenticidad y conservación.

- **Comunicación vertical y horizontal:** La información circulará ascendente y descendentemente entre los niveles estratégico, táctico y operativo, y transversalmente entre las áreas técnicas, jurídicas, éticas y de negocio. En el sector salud, esta comunicación incluirá la remisión periódica de informes clínicos o de seguridad a los comités asistenciales. En Smart Cities, se articularán canales de coordinación con las áreas municipales responsables de datos urbanos, movilidad y 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

- **Periodicidad y documentación:** Se establecerá un calendario formal de reuniones de coordinación interdepartamental. Las actas reflejarán acuerdos, incidentes, medidas correctoras y responsables designados, y se conservarán en el registro institucional.

- **Escalamiento de incidencias:** Cualquier desviación significativa o incidente crítico deberá comunicarse de inmediato al Comité de Gobernanza de IA, que evaluará las medidas preventivas o suspensiones temporales necesarias. En el ámbito sanitario, esto incluye incidentes de seguridad del paciente o de rendimiento clínico. En entornos de Smart Cities, incluye fallos que afecten a la seguridad pública o a la calidad de los servicios inteligentes.

- **Retroalimentación y mejora continua:** Los resultados de auditorías, evaluaciones y revisiones técnicas se comunicarán sistemáticamente a las unidades responsables, integrándose en los planes de mejora institucional y en los informes previstos en el apartado 6.4.

Los flujos definidos en este apartado se aplicarán conforme a la Matriz RACI incluida en el Anexo A, que determina las funciones Responsible, Accountable, Consulted e Informed para las actividades vinculadas a la gestión del riesgo de IA. Cada entidad podrá ampliar o adaptar esta matriz a otros procesos del ciclo de vida, manteniendo su coherencia metodológica y siempre con la validación formal del Comité de Gobernanza de IA. De esta forma se garantiza que cada decisión, comunicación o actuación operativa disponga de un responsable identificable y de evidencia documental verificable, tanto en el ámbito general como en los sectores específicos de Salud y Smart Cities.

Asimismo, los flujos de información y coordinación aquí descritos se complementan con los mecanismos de reporte institucional, comunicación y transparencia establecidos en el *apartado 6.4*, que desarrollan los procedimientos formales de documentación y rendición de cuentas.

6.4. Mecanismos de reporte, comunicación y transparencia

El correcto funcionamiento del modelo de gobernanza de la Inteligencia Artificial (IA) depende de que la información fluya de manera ordenada, verificable y oportuna entre todos los actores implicados.

La comunicación y el reporte institucional no son tareas accesorias, sino los instrumentos que garantizan la trazabilidad de las decisiones, la transparencia ante la ciudadanía y la rendición de cuentas frente a las autoridades competentes. Este apartado describe los mecanismos mediante los cuales la organización debe registrar, comunicar y divulgar la información relevante sobre el desempeño, los riesgos y el cumplimiento normativo de los sistemas de IA.

- **Comunicación interna**

La comunicación interna tiene como finalidad asegurar que todos los órganos, responsables y unidades implicadas en la gestión de la IA dispongan de información oportuna, veraz y verificable sobre el desempeño de los sistemas, los riesgos emergentes y el grado de cumplimiento normativo.

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

La organización debe establecer canales formales y estandarizados de comunicación entre las áreas técnicas, jurídicas, éticas y directivas. Estos canales pueden adoptar la forma de plataformas internas de gestión, actas digitales o repositorios documentales con control de acceso. Toda la información debe almacenarse de modo que pueda reconstruirse la secuencia de decisiones y verificarse quién intervino en cada fase del ciclo de vida de la IA.

El **Chief AI Officer (CAIO)** es responsable de centralizar la información operativa y de garantizar que los reportes sean coherentes, completos y comparables en el tiempo.

Deberá elaborar informes trimestrales dirigidos al Comité de Gobernanza de IA, que incluyan como mínimo:

- Una descripción detallada del estado de los sistemas de IA en producción y de los proyectos en desarrollo.
- Los resultados de las auditorías internas y de las revisiones técnicas o éticas efectuadas durante el periodo correspondiente.
- Los incidentes de seguridad, privacidad, calidad de datos o funcionamiento detectados, junto con las acciones correctivas o preventivas aplicadas.
- Los indicadores clave de desempeño (KPI) y los indicadores clave de riesgo (KRI), con especial atención a los vinculados a seguridad del paciente, protección de datos, fiabilidad técnica y equidad algorítmica.
- Las recomendaciones de mejora propuestas para el siguiente periodo de revisión.

El **Comité de Gobernanza de IA** consolidará la información recibida, elaborando un informe anual de cumplimiento y riesgo, que será remitido a la Alta Dirección. Este informe servirá como base para la revisión estratégica del modelo, la priorización de inversiones y la adopción de medidas de mejora institucional.

Toda la documentación generada deberá **conservarse en el Repositorio Institucional de Gobernanza**, garantizando su integridad, autenticidad y trazabilidad. El acceso a dicho repositorio estará limitado a las funciones autorizadas, conforme a los principios de necesidad y proporcionalidad establecidos por el Reglamento (Unión Europea) 2016/679 (RGPD).

- **Comunicación externa**

La comunicación externa tiene como finalidad garantizar la transparencia y la responsabilidad pública de las organizaciones que operan sistemas de IA en sectores de alta sensibilidad, así como facilitar la cooperación con autoridades, organismos reguladores y ciudadanos.

Las entidades deberán establecer protocolos de notificación y comunicación externa que contemplen:

I. Notificación de incidentes y vulneraciones

Cualquier evento que afecte a la seguridad, privacidad o continuidad de un sistema de IA deberá comunicarse de manera inmediata al CAIO, al DPO y al responsable de Ciberseguridad. Cuando el incidente sea grave o pueda comprometer derechos

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

fundamentales, la organización notificará sin demora a la autoridad competente, de acuerdo con los plazos establecidos por el RGPD y la Ley de Inteligencia Artificial (RIA), y cuando proceda, la Directiva (UE) 2022/2555 (NIS2). En el sector sanitario, esta obligación incluye incidentes clínicos, errores en sistemas de soporte a la decisión médica o vulneraciones de datos de pacientes. En Smart Cities, se extenderá a fallos que afecten la prestación de servicios públicos, la seguridad ciudadana o la integridad de los datos urbanos.

II. Comunicación con autoridades reguladoras.

Las entidades deben mantener una relación de cooperación activa con los organismos competentes en materia de sanidad, protección de datos, ciberseguridad o innovación digital. Esto implica atender los requerimientos de información, colaborar en auditorías oficiales y remitir los informes periódicos que demuestren el cumplimiento de las obligaciones legales y éticas.

III. Transparencia hacia la ciudadanía.

La transparencia institucional constituye una obligación de carácter proactivo orientada a garantizar que la ciudadanía disponga de información verificable sobre los sistemas de IA utilizados. En los sectores de Salud y Smart Cities, esta transparencia deberá permitir conocer los sistemas activos y su finalidad, el nivel de autonomía y supervisión humana, las medidas de seguridad y privacidad adoptadas, así como los mecanismos de control y las salvaguardas aplicadas. La difusión de esta información se realizará mediante portales institucionales, informes públicos o paneles digitales accesibles. En el ámbito sanitario, la entidad elaborará documentación específica dirigida a pacientes y profesionales, redactada en lenguaje comprensible y no técnico. En el contexto urbano, la información se presentará en portales o plataformas de datos abiertos que permitan conocer el propósito y los resultados de los sistemas de IA implantados.

IV. Atención y participación ciudadana.

La participación ciudadana complementa la transparencia activa mediante mecanismos que garantizan la comunicación bidireccional entre la organización y las personas potencialmente afectadas por el uso de sistemas de IA. La entidad deberá habilitar canales seguros, accesibles y verificables para presentar reclamaciones, solicitar información o formular observaciones. Todas las solicitudes se registrarán, clasificarán y atenderán dentro de los plazos institucionalmente establecidos. El CAIO es responsable de supervisar la coherencia, trazabilidad y documentación de las respuestas, asegurando su alineación con la política de transparencia y la normativa vigente. En el ámbito de las Smart Cities, dichos canales podrán integrarse en plataformas digitales participativas o portales municipales de datos abiertos. En el sector Salud, se articularán a través de los mecanismos de atención al paciente y de los servicios de información sanitaria, garantizando una respuesta adecuada, verificable y conforme a los derechos de los interesados.

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

- **Frecuencia y formato de reportes**

Los procesos de reporte deberán realizarse con una frecuencia y un formato homogéneos, definidos en la política Interna de Gobernanza de la IA y aprobados por el Comité de Gobernanza de IA.

El objetivo es asegurar que toda la información generada pueda ser interpretada, auditada y comparada de manera consistente a lo largo del tiempo, y que se disponga de evidencia documental suficiente para demostrar el cumplimiento de las obligaciones legales, éticas y técnicas.

Se establecen las siguientes pautas mínimas:

a) **Informes trimestrales del CAIO:** documento operativo que consolida la información técnica y organizativa sobre todos los sistemas de IA en producción y desarrollo. Debe incluir la descripción del estado de los sistemas, los incidentes detectados, las acciones correctivas aplicadas, los resultados de auditorías internas o revisiones técnicas, así como los indicadores clave de desempeño (KPI) y de riesgo (KRI).

b) **Informe anual consolidado del Comité de Gobernanza de IA:** documento estratégico que presenta una evaluación global del modelo de gobernanza, el grado de cumplimiento de las políticas y normas aplicables, la evolución de los riesgos institucionales y el plan anual de mejora. Este informe deberá remitirse a la Alta Dirección y servirá de base para la revisión de prioridades, la asignación de recursos y la actualización de la Política Institucional de IA.

c) **Reportes extraordinarios:** documentos emitidos de manera inmediata ante la aparición de incidentes graves, cambios regulatorios relevantes o hallazgos críticos derivados de auditorías internas o externas. Su finalidad es permitir una reacción temprana y documentada frente a situaciones que puedan comprometer la integridad, seguridad o conformidad del modelo.

Cada informe deberá incluir, como mínimo, los siguientes elementos:

- ✓ Un resumen ejecutivo claro y conciso.
- ✓ La descripción de los hallazgos más relevantes.
- ✓ El estado de cumplimiento frente a los marcos legales y estándares aplicables.
- ✓ Los incidentes detectados y las medidas adoptadas.
- ✓ Los indicadores KPI y KRI actualizados.
- ✓ Las recomendaciones y el plan de mejora.

Todos los documentos se archivarán en el Repositorio Institucional de Gobernanza, con registro de versiones y política de conservación conforme a la legislación vigente. El formato será uniforme en toda la organización y estará respaldado por plantillas oficiales aprobadas por el Comité de Gobernanza de IA y la versión final de cada reporte deberá incluir la fecha y estar firmada electrónicamente por el responsable emisor, garantizando su autenticidad e integridad.

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

6.5. Proporcionalidad y escalabilidad

La aplicación del modelo de gobernanza de la Inteligencia Artificial deberá regirse por los principios de proporcionalidad y escalabilidad, garantizando que las obligaciones, controles y procesos se ajusten al nivel de riesgo de los sistemas, al tamaño de la entidad y a su grado de madurez tecnológica.

Este principio, establecido en el Reglamento (UE) 2024/1689 (RIA) y desarrollado en las normas ISO/IEC 42001:2023 e ISO 31000:2018, permite adaptar la gobernanza y la gestión del riesgo a las capacidades reales de cada organización, manteniendo siempre los valores esenciales de legalidad, trazabilidad, seguridad y rendición de cuentas.

I. Proporcionalidad según el nivel de riesgo del sistema.

El modelo de gobernanza deberá modular la intensidad de los controles y mecanismos de supervisión en función de la clasificación de riesgo atribuida a cada sistema de Inteligencia Artificial. Esta proporcionalidad se traduce en un ajuste progresivo de las exigencias de validación, seguimiento y trazabilidad conforme aumenta o disminuye el nivel de riesgo reconocido, garantizando que los recursos de gestión se apliquen de manera eficiente y alineada con los requisitos normativos y éticos aplicables. De este modo, el modelo asegura una correspondencia coherente entre la naturaleza del sistema, su potencial impacto y el grado de control institucional requerido, preservando en todos los casos los principios de legalidad, transparencia y rendición de cuentas.

II. Proporcionalidad según la naturaleza y tamaño de la organización.

Las entidades deberán ajustar la estructura de gobernanza de IA a su dimensión, complejidad y exposición regulatoria, garantizando la independencia funcional y la trazabilidad de las decisiones.

- Organizaciones pequeñas: podrán acumular funciones en una misma persona o unidad (por ejemplo, el responsable de inteligencia artificial (CAIO) podrá asumir también la gestión de riesgos), siempre que se preserve una independencia mínima. En ningún caso el delegado de Protección de Datos (DPO) podrá auditarse a sí mismo ni asumir funciones de supervisión ética o de ciberseguridad que comprometan su imparcialidad.

- Organizaciones medianas: las funciones de riesgo, ética y cumplimiento podrán agruparse en un órgano colegiado, siempre que el CAIO, el DPO y el CISO mantengan autonomía funcional y capacidad de reporte directo al Comité de Gobernanza de IA.

- Organizaciones grandes o con sistemas de alto riesgo: las funciones deberán segregarse y documentarse de forma explícita, estableciendo líneas de reporte independientes, controles internos y auditorías externas o mixtas. Será obligatoria la existencia de un Comité de Gobernanza de IA formalmente constituido, con actas, quórum y procedimientos internos aprobados.

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

III. Proporcionalidad en la documentación y auditoría.

La extensión de la documentación técnica y la frecuencia de las auditorías se graduarán conforme al riesgo, la criticidad y el impacto potencial del sistema. Los sistemas de alto riesgo deberán conservar expedientes técnicos completos, evaluaciones de impacto y evidencias de conformidad con los estándares aplicables (ISO/IEC 42001, ISO/IEC 23894, ISO 31000, ISO/IEC 27001). Los sistemas de bajo riesgo podrán mantener registros resumidos que aseguren la trazabilidad básica, la transparencia y la capacidad de demostrar el cumplimiento normativo y ético ante las autoridades competentes.

Estos principios garantizarán una implantación coherente, verificable y sostenible del modelo de gobierno de IA, evitando cargas desproporcionadas y reforzando la responsabilidad institucional en el uso de la Inteligencia Artificial.

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. Funciones por líneas de defensa

El modelo de tres líneas de defensa se adopta como marco estructural para la gestión integrada de riesgos, cumplimiento y auditoría dentro del sistema de gobernanza de la Inteligencia Artificial. Su finalidad es garantizar la independencia funcional, la trazabilidad de las decisiones y la coherencia entre las actividades de desarrollo, control y verificación, asegurando que las decisiones automatizadas o asistidas por IA se gestionan con el mismo rigor, transparencia y rendición de cuentas que las decisiones humanas de alto impacto.

Cada línea de defensa desempeña funciones diferenciadas pero complementarias, cuya coordinación se articula bajo la supervisión del Comité de Gobernanza de IA y del responsable de IA (CAIO). La adecuada interacción entre estas tres líneas constituye la base del control interno y del ciclo de mejora continua del modelo de gobierno de IA.

7.1. Primera línea: gestión operativa

La primera línea corresponde a las áreas responsables del diseño, desarrollo, validación y operación de los sistemas de Inteligencia Artificial. Su función principal es asegurar la calidad técnica, la seguridad, la privacidad y la conformidad ética del sistema desde su concepción hasta su operación en producción. Esta primera línea es, por tanto, el nivel de ejecución operativa y de control inicial, donde se generan las evidencias que permiten verificar el cumplimiento de los procedimientos y la eficacia de los controles.

En esta línea el CAIO interviene de manera limitada como figura de enlace, asegurando la coherencia documental y la conexión entre la operación diaria y los mecanismos de supervisión. No obstante, su función principal de control, evaluación y reporte se ejerce desde la segunda línea.

RESPONSABLE DE IA (CAIO)
El responsable de IA coordina y supervisa el desarrollo, implementación y operación de los sistemas de IA en este nivel. Garantiza su alineación con los objetivos institucionales, el marco ético-legal y los requisitos técnicos de calidad y seguridad. Es responsable de coordinar la implantación práctica y verificar la trazabilidad y garantizar comunicación entre las áreas técnicas y el Comité de Gobernanza de IA.
Tareas
Individuales: 1. Aprobar y priorizar los casos de uso de IA, en coordinación con la Dirección Estratégica y el Comité de Gobernanza de IA. 2. Planificar y supervisar el ciclo de vida completo de los sistemas de IA. 3. Validar la robustez, explicabilidad y fiabilidad técnica de los modelos en cumplimiento con las políticas de calidad, seguridad, privacidad y ética de la organización. 4. Mantener actualizado el inventario institucional de sistemas de IA y su clasificación de riesgo, garantizando la trazabilidad técnica de los modelos.

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

5. Verificar la aplicación de los principios de *privacy by design*, *security by design* y *ethics by design* en las fases de desarrollo e implementación.
6. Validar los indicadores operativos de rendimiento (KPI) y riesgo (KRI) remitidos por los equipos técnicos.
7. Supervisar que las medidas correctivas derivadas de revisiones técnicas, incidentes o auditorías sean implementadas de manera efectiva.

Compartidas:

8. Asesorar a la Alta Dirección en decisiones estratégicas sobre adopción, escalabilidad y uso ético de la IA.
9. Coordinar con el Órgano Promotor y los Desarrolladores de Sistemas de IA la correcta ejecución de los casos de uso aprobados, asegurando su alineación técnica y operativa.
10. Colaborar con el Equipo de Implementación para garantizar la correcta transición de los modelos a entornos productivos y su monitorización continua.
11. Mantener comunicación constante con el delegado de Protección de Datos (DPO), el responsable de Ciberseguridad (CISO) y el responsable de Ética, a fin de garantizar la coherencia entre los controles técnicos, de privacidad y de derechos fundamentales.
12. Apoyar al responsable de Riesgos (CRO) en la detección y documentación de riesgos operativos emergentes.
13. Facilitar la información y documentación técnica solicitada durante las auditorías internas o revisiones convocadas por el Comité de Gobernanza de IA.

Órgano Promotor
El órgano promotor identifica, justifica y promueve los casos de uso de IA, evaluando su alineación con la estratégica institucional. Lidera la fase inicial de definición y colabora en la validación técnica y ética previa al despliegue.
Tareas

Individuales:

1. Definir los objetivos, alcance y beneficios esperados de cada caso de uso.
2. Evaluar la viabilidad técnica, organizativa y presupuestaria del proyecto.
3. Garantizar la disponibilidad de recursos y responsables durante el ciclo de vida del sistema.
4. Preparar y presentar la documentación inicial para la propuesta formal ante el Comité de Gobernanza de IA para su evaluación y aprobación.
5. Mantener la coherencia de la documentación del caso de uso con la política institucional de IA y con los criterios de clasificación de riesgo establecidos.

Compartidas:

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. Coordinar con el CAIO la priorización de casos de uso y su planificación en el portafolio institucional de sistemas de IA.
7. Colaborar con el DPO y el responsable de Ética en la identificación de los requisitos legales y éticos desde la fase de diseño.
8. Participar junto al responsable de Riesgos (CRO) en la valoración inicial de riesgos estratégicos, operativos y/o reputacionales.
9. Cooperar con el Equipo de Desarrollo y el Equipo de Implementación durante la validación previa al despliegue.
10. Contribuir al seguimiento de resultados e impactos, aportando información para la mejora continua del sistema.

Desarrolladores de Sistemas de IA
Los desarrolladores de sistemas de IA diseñan, entrenan, validan y documentan los modelos algorítmicos, asegurando su integridad técnica, transparencia y cumplimiento con los requisitos de explicabilidad y seguridad establecidos por la organización y las normativas vigentes.
Tareas

Individuales:

1. Diseñar los modelos de IA aplicando los principios de ¨ethics by design¨, ¨privacy by design¨ y ¨security by design¨.
2. Seleccionar y documentar los conjuntos de datos utilizados, asegurando su representatividad, calidad y licitud.
3. Implementar metodologías de entrenamiento y validación reproducibles, dejando trazabilidad de versiones, parámetros y resultados.
4. Evaluar la robustez, fiabilidad y estabilidad de los modelos antes de su puesta en producción.
5. Identificar y documentar posibles sesgos o limitaciones del modelo, evaluar su impacto y proponer medidas correctoras.
6. Mantener actualizada la documentación técnica y los repositorios de código y datos, conforme a los procedimientos internos de control.

Compartidas:

7. Colaborar con el responsable de IA (CAIO) y responsable de ciberseguridad (CISO) en la revisión técnica y coordinar la validación de entornos seguros del modelo antes de su despliegue.
8. Coordinar con el DPO la entrega de información necesaria para las Evaluaciones de Impacto en Protección de Datos (EIPD).
9. Trabajar con el responsable de Ética en la detección y mitigación de sesgos algorítmicos y en la aplicación de principios de equidad y no discriminación.
10. Cooperar con el responsable de Ciberseguridad en la aplicación de medidas de seguridad de software, datos y entornos de desarrollo.

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

11. Asistir al Equipo de Implementación durante la transición del modelo desde el entorno de desarrollo al entorno operativo.
12. Participar activamente en auditorías técnicas y revisiones internas, aportando documentación y evidencias verificables.

Equipo de Implementación de Sistemas de IA
El equipo de implementación integra los sistemas de IA en la infraestructura institucional, asegurando su funcionamiento estable, seguro y conforme a las especificaciones aprobadas por el Comité de Gobernanza de IA.

Tareas

Individuales:

1. Configurar los entornos de ejecución y acceso conforme a las políticas de seguridad establecidas.
2. Implementar herramientas de monitorización continua de rendimiento, sesgo, *data drift* y *concept drift*, registrando resultados y anomalías.
3. Registrar y conservar los logs, métricas e incidencias operativas con trazabilidad verificable.
4. Ejecutar actualizaciones, parches y revisiones programadas, conforme al ciclo de mantenimiento aprobado.
5. Aplicar protocolos de continuidad operativa y recuperación ante fallos.

Compartidas:

6. Coordinar con el CISO y el CAIO la validación técnica y de seguridad de los entornos de ejecución y la gestión de vulnerabilidades.
7. Colaborar con los Desarrolladores durante la fase de transición a producción, verificando la consistencia funcional del sistema.
8. Informar al CAIO de desviaciones o alertas detectadas durante la operación.
9. Cooperar con el DPO y el responsable de Ética en la revisión periódica del comportamiento y resultados del sistema en producción.
10. Proporcionar la documentación técnica y de monitorización necesaria para auditorías y revisiones convocadas por el Comité de Gobernanza de IA.

7.2. Segunda línea: gestión de riesgos y cumplimiento

La segunda línea integra las unidades transversales de gestión de riesgos, cumplimiento normativo, ética, protección de datos y ciberseguridad, que establecen marcos, políticas y procedimientos, supervisan la eficacia de los controles de la primera línea y verifican la adecuación legal y ética de los sistemas. La segunda línea reporta al Comité de Gobernanza de IA, emite dictámenes preceptivos para la autorización de despliegues y tiene facultad de requerir acciones correctivas o suspensiones preventivas cuando detecte incumplimientos graves.

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 la segunda línea, el CAIO asume la dirección técnica y estratégica del sistema institucional de gobernanza de la Inteligencia Artificial. En esta línea sus responsabilidades se centran en consolidar la información institucional sobre el desempeño, los riesgos y el cumplimiento normativo de los sistemas de IA, informando al Comité de Gobernanza de IA y a la Alta Dirección, y promoviendo la mejora continua del modelo.

RESPONSABLE DE IA (CAIO)
El responsable de IA diseña, implementa y mantiene el marco metodológico que regula el desarrollo, uso y supervisión de los sistemas de IA en la organización. El CAIO garantiza la coherencia institucional, la rendición de cuentas y la alineación con los marcos normativos internacionales, coordinando los responsables de Riesgo (CRO), cumplimiento, ética, protección de datos (DPO) y ciberseguridad (CISO).
Tareas

Individuales:

1. Aprobar y priorizar los casos de uso de IA, en coordinación con la Alta Dirección y el Comité de Gobernanza de IA, evaluando su viabilidad técnica, ética y regulatoria.
2. Supervisar la correcta aplicación de las políticas, metodologías y controles definidos por la segunda línea en toda la organización.
3. Centralizar el inventario de sistemas y mantener la clasificación actualizada de riesgos, estado operativo y controles aplicados.
4. Consolidar la información operativa y los resultados remitidos por la primera línea, garantizando su integridad, coherencia y trazabilidad documental.
5. Consolidar indicadores de rendimiento (KPI) y riesgo (KRI), garantizando la coherencia y comparabilidad de los informes remitidos al Comité.
6. Elaborar informes trimestrales y un informe anual consolidado sobre el estado de los sistemas de IA, incidentes, riesgos, cumplimiento y acciones de mejora.
7. Mantener actualizado el Repositorio Institucional de Gobernanza, asegurando la conservación, autenticidad y disponibilidad controlada de los documentos.
8. Coordinar la implementación de las recomendaciones y medidas aprobadas por el Comité de Gobernanza de IA, haciendo seguimiento de su cumplimiento.
9. Promover la mejora continua y la capacitación del personal en materia de IA responsable.

Compartidas:

10. Coordinar con el responsable de Riesgos (CRO), el delegado de Protección de Datos (DPO), el responsable de Ciberseguridad (CISO), el responsable de Ética y el responsable Sectorial las evaluaciones conjuntas de impacto, los dictámenes de conformidad y las acciones preventivas.
11. Asesorar a la Alta Dirección y al Comité de Gobernanza de IA sobre la adopción, ampliación o retirada de sistemas de IA, en función de su nivel de riesgo, resultados y desempeño ético-técnico.

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

12. Coordinar con el Órgano Promotor y los Desarrolladores de Sistemas de IA la validación técnica y regulatoria de los casos de uso aprobados, asegurando su alineación con los objetivos institucionales y los criterios de control establecidos.
13. Colaborar con el Equipo de Implementación en la supervisión de la transición de los modelos a entornos productivos, verificando la implantación de los mecanismos de monitorización y la correcta gestión de incidencias.
14. Mantener comunicación constante con el delegado de Protección de Datos (DPO), el responsable de Ciberseguridad (CISO) y el responsable de Ética, a fin de garantizar la coherencia entre los controles técnicos, de privacidad y de derechos fundamentales.
15. Supervisar la integración transversal de los controles de privacidad, seguridad y ética en todas las fases del ciclo de vida de los sistemas, en coordinación con el DPO, el CISO y el responsable de Ética.
16. Apoyar al responsable de Riesgos (CRO) en la detección y documentación de riesgos operativos emergentes.
17. Facilitar la información y documentación técnica solicitada durante las auditorías internas o revisiones convocadas por el Comité de Gobernanza de IA.
18. Representar a la organización ante autoridades competentes, organismos reguladores, redes sectoriales y foros nacionales o internacionales en materia de gobernanza de IA.
19. Promover la formación y sensibilización institucional sobre el uso ético, responsable y seguro de la Inteligencia Artificial.
20. Impulsar la mejora continua del modelo de gobernanza, integrando los resultados de auditorías, incidentes, evaluaciones de desempeño y revisiones estratégicas, y coordinando su actualización con el Comité de Gobernanza de IA.

Responsable de Riesgos de IA (CRO)
El responsable de riesgos de IA define y mantiene el marco institucional de gestión de riesgos algorítmicos, asegurando la identificación, evaluación y mitigación de los riesgos técnicos, éticos y operativos asociados a la IA.
Tareas

Individuales:

1. Elaborar y actualizar el mapa institucional de riesgos de IA y su metodología de evaluación.
2. Establecer niveles de tolerancia y criterios de mitigación.
3. Emitir dictámenes de riesgo antes del despliegue de cada sistema.
4. Supervisar la implementación de medidas correctivas y registrar los incidentes significativos.
5. Integrar los riesgos de IA en el sistema general de gestión de riesgos corporativo.

Compartidas:

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. Coordinar con el CAIO la identificación y priorización de riesgos emergentes.
7. Colaborar con el DPO y el CISO en la gestión de riesgos combinados de privacidad y ciberseguridad.
8. Participar en la elaboración de informes periódicos al Comité de Gobernanza de IA y en auditorías internas.

Delegado de Protección de Datos (DPO)
El delegado de protección de datos supervisa el cumplimiento del Reglamento (UE) 2016/679 (RGPD) y la normativa nacional aplicable, garantizando la licitud, transparencia y proporcionalidad de los tratamientos realizados por sistemas de IA.
Tareas

Individuales:

1. Revisar y aprobar las Evaluaciones de Impacto en Protección de Datos (EIPD).
2. Verificar la base jurídica, minimización y legitimidad de los tratamientos.
3. Supervisar la aplicación de medidas de anonimización, seudonimización y control de acceso.
4. Gestionar notificaciones de incidentes de privacidad ante las autoridades competentes.
5. Asesorar a las áreas implicadas sobre buenas prácticas en protección de datos.

Compartidas:

6. Colaborar con el CAIO, el CISO y el responsable de Ética en evaluaciones conjuntas.
7. Participar con el responsable de Riesgos en la evaluación de impactos combinados.
8. Intervenir en el Comité de Gobernanza de IA para la revisión y aprobación de sistemas de alto riesgo.

Responsable de Ciberseguridad
El responsable de ciberseguridad asegura la integración de los sistemas de IA en el Sistema de Gestión de Seguridad de la Información y protege los modelos, datos y entornos frente a vulnerabilidades o accesos indebidos.
Tareas

Individuales:

1. Evaluar riesgos de ciberseguridad en modelos y entornos de IA.
2. Implementar controles técnicos y procedimientos de gestión de vulnerabilidades.
3. Realizar pruebas de penetración y auditorías de seguridad periódicas.
4. Coordinar la respuesta ante incidentes 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

5. Mantener actualizada la documentación del sistema de gestión de seguridad.

Compartidas:

6. Colaborar con el CAIO y el Equipo de Implementación en la validación de entornos seguros.
7. Coordinar con el responsable de Riesgos la integración de riesgos de ciberseguridad en el mapa global.
8. Participar junto al DPO en la gestión de incidentes que afecten a datos personales.

Responsable de Ética y Derechos Fundamentales
El responsable de ética evalúa la conformidad de los sistemas de IA con los principios de equidad, transparencia y respeto de los derechos fundamentales, promoviendo una cultura de IA responsable.

Tareas

Individuales:

1. Revisar el diseño y funcionamiento de los sistemas desde una perspectiva ética.
2. Analizar sesgos y proponer medidas de corrección y mejora.
3. Elaborar informes éticos y recomendaciones para el Comité de Gobernanza de IA.
4. Promover la formación y sensibilización en ética de IA dentro de la organización.

Compartidas:

1. Coordinar con el CAIO, el DPO y el responsable de Riesgos las evaluaciones éticas y de impacto en derechos fundamentales.
2. Colaborar en la resolución de dilemas éticos y controversias.
3. Participar en la elaboración de informes de transparencia institucional.

Responsable Sectorial (Salud o Smart Cities)
El responsable sectorial asegura la aplicación del modelo de gobernanza de la Inteligencia Artificial en su ámbito específico, garantizando que los sistemas cumplan los requisitos técnicos, regulatorios y éticos propios del sector y se alineen con los objetivos institucionales y de servicio público.

Tareas

Individuales:

1. Interpretar y aplicar la normativa sectorial relevante (p. ej. MDR/IVDR en salud; normativa sobre infraestructuras críticas, datos abiertos o sostenibilidad en Smart Cities).
2. Asesorar a las áreas operativas y al CAIO sobre requisitos técnicos, funcionales o de calidad propios del sector.

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. Validar la adecuación funcional y regulatoria de los sistemas de IA antes de su presentación al Comité de Gobernanza de IA.
4. Identificar riesgos o impactos específicos del sector que puedan requerir controles adicionales o medidas preventivas.
5. Promover la alineación del uso de IA con las políticas públicas, los objetivos de servicio y la protección de los derechos de las personas.
6. Representar a la organización en foros técnicos o institucionales de su ámbito, promoviendo la coherencia sectorial y el intercambio de buenas prácticas.

Compartidas:

7. Colaborar con el CAIO en la revisión sectorial de proyectos, asegurando su coherencia con la estrategia y prioridades institucionales.
8. Coordinar con el DPO y el responsable de Ética la aplicación de salvaguardas adecuadas en materia de privacidad y derechos fundamentales.
9. Participar con el responsable de Riesgos en la identificación de riesgos operativos o de cumplimiento específicos del sector
10. Asistir al Comité de Gobernanza de IA en la evaluación de casos de uso de alto impacto o sensibilidad sectorial.
11. Contribuir, junto con el CAIO y el Comité, al diseño de indicadores sectoriales de desempeño e impacto (por ejemplo, seguridad del paciente, sostenibilidad o equidad digital).

Comité de gobernanza de IA
El Comité de Gobernanza de la Inteligencia Artificial coordina y supervisa la aplicación del modelo institucional de IA, garantizando que su desarrollo, uso y control se realicen de manera ética, segura y conforme a la legislación vigente.
Tareas

Individuales:

1. Aprobar las políticas, directrices y normas internas de gobernanza de la IA.
2. Analizar los informes del CAIO, DPO, responsable de Riesgos y Auditor Interno.
3. Autorizar la puesta en marcha de los sistemas clasificados como de alto riesgo.
4. Evaluar los indicadores institucionales de desempeño y cumplimiento.
5. Emitir resoluciones o recomendaciones ante dilemas éticos o incidentes relevantes.

Compartidas:

6. Coordinar con la Alta Dirección la revisión estratégica del modelo de gobernanza.
7. Colaborar con el CAIO y los responsables funcionales en la priorización de mejoras.
8. Participar con el Auditor Interno en la validación del plan anual de auditorías.
9. Comunicar a las autoridades competentes los informes consolidados de cumplimiento y riesgo.

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

10. Promover la formación, sensibilización y cultura organizativa sobre el uso responsable de la IA.

7.3. Tercera línea: auditoría interna

La tercera línea es la función de auditoría interna o externa independiente, que proporciona garantía objetiva sobre la eficacia del sistema de gobernanza, la gestión de riesgos y los controles internos. La auditoría evalúa el diseño y la ejecución de los procesos, la integridad de la documentación y la efectividad de la mejora continua, y eleva sus conclusiones a la alta dirección y, cuando proceda, al órgano de control institucional.

Auditor interno
El auditor interno evalúa de forma independiente la eficacia y conformidad del modelo de gobernanza de la Inteligencia Artificial, verificando que los controles y procesos cumplan con la normativa, las políticas institucionales y los estándares internacionales aplicables.
Tareas
Individuales: 1. Elaborar y ejecutar el plan anual de auditoría de IA, basado en riesgos y aprobado por la alta dirección. 2. Revisar la eficacia de los controles aplicados por las dos primeras líneas de defensa. 3. Comprobar la trazabilidad y completitud de la documentación de los sistemas de IA. 4. Identificar deficiencias o áreas de mejora y emitir recomendaciones objetivas. 5. Verificar la implementación de las acciones correctivas aprobadas. **Compartidas:** 6. Coordinar con el CAIO y el Comité de Gobernanza de IA el alcance y calendario de las auditorías. 7. Colaborar con el DPO y el responsable de Ciberseguridad en la verificación de controles de privacidad y seguridad. 8. Informar al Comité de Gobernanza de IA de los hallazgos y conclusiones de cada auditoría. 9. Participar en las reuniones de seguimiento de mejoras. 10. Facilitar información a las autoridades o auditores externos cuando sea requerido.

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. Seguimiento, auditoría y mejora continua

El sistema de gobernanza de la Inteligencia Artificial deberá incorporar mecanismos permanentes de supervisión, verificación y mejora continua, que aseguren su eficacia, coherencia y alineación con el marco normativo y ético vigente.

El objetivo de esta sección es establecer un proceso estructurado de revisión periódica y adaptación del modelo, garantizando que las decisiones institucionales se fundamenten en evidencia, evaluación y aprendizaje organizativo.

8.1. Supervisión y evaluación periódica

La organización deberá establecer mecanismos estables de seguimiento y control del modelo de gobernanza de la Inteligencia Artificial, con el fin de asegurar su eficacia, coherencia y cumplimiento continuado.

El **Comité de Gobernanza de IA** será el órgano responsable de supervisar su aplicación práctica, revisando periódicamente los informes elaborados por el responsable de Inteligencia artificial (CAIO) y por las unidades encargadas de riesgos, protección de datos, ciberseguridad y ética.

Estas revisiones permitirán comprobar que las políticas y procedimientos se aplican correctamente, que los controles implantados son eficaces y que los incidentes o desviaciones se gestionan con rapidez y transparencia.

La supervisión incluirá tanto la **evaluación de los resultados técnicos** y **operativos** de los sistemas de IA como el **grado de cumplimiento normativo**, **ético y organizativo** alcanzado por la entidad.

Los resultados del seguimiento deberán **documentarse en informes formales** presentados ante la alta dirección, que recojan los avances logrados, las áreas de mejora y las recomendaciones de ajuste.

En función de dichas conclusiones, el Comité podrá aprobar un **Plan de Acción** que incorpore las **medidas correctivas** o preventivas necesarias, designando responsables, plazos y recursos para su ejecución.

8.2. Mejora continua y revisión estratégica

El modelo de gobernanza deberá concebirse como un sistema dinámico y adaptable. La organización promoverá una cultura de aprendizaje y mejora continua, integrando las lecciones obtenidas de auditorías, evaluaciones, revisiones éticas y resultados operativos. Este enfoque permitirá actualizar las políticas internas, reforzar los mecanismos de control y ajustar los procedimientos conforme a la evolución normativa, tecnológica y social.

Al menos cada dos años, o cuando se produzcan cambios significativos en la legislación o en la estructura institucional, se llevará a cabo una revisión estratégica integral del modelo. Esta revisión será liderada por el **Comité de Gobernanza de IA**, con apoyo del CAIO y de las unidades transversales, y sus conclusiones se elevarán a la alta dirección para su aprobación formal.

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 resultado de dicha revisión servirá como base para la actualización de la Política Institucional de Gobernanza de la Inteligencia Artificial, asegurando que el modelo siga siendo eficaz, transparente y alineado con los valores y objetivos de la organización.

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. Anexos

9.1. Anexo A: RACI

Tareas asociadas con la Gestión del Riesgo IA			Roles asociados a Gestión del Riesgo IA							
			1º LDD Gestión operativa				2º LDD Gestión de riesgos y cumplimiento			
Fase del Ciclo de Vida	**Subfases**	**Actividades**	***Desarrolladores de Sistemas IA***	***Equipo de Implementación de Sistemas IA***	**Responsable de IA (CIA)**	***Órgano Promotor***	**Responsable de Ética de IA**	***Delegado/a de Protección de Datos (DPD)***	**Responsable de Riesgos IA (CIA)**	**Responsable Sectorial (Salud/Smart Cities)**
Identificación y evaluación de Casos de Uso	Identificación	1. Identificación caso de uso	C	I	A	R	C	C	C	C
		2. Clasificación riesgo	I	I	R	C	C	C	A	C
		3. Elaboración del informe de viabilidad	R	C	A	C	C	C	C	I
	Evaluación de casos de uso	4. Evaluación preliminar de protección de datos	C	I	R	I	C	AR	C	C
		5. Actualización inicial del inventario	C	I	A	R	I	I	C	I
		6. Aprobación del caso de uso	I	I	AR	R	C	C	C	C
Diseño, Desarrollo e Implementación de Casos de Uso	Diseño	7. Planificación del sistema de IA	R	I	A	C	C	C	C	I
		8. Evaluación y decisión sobre la externalización de proveedores	I	I	A	R	C	C	C	C
		9. Diseño del sistema IA	R	C	A	C	C	C	C	I
		10. Evaluación de impacto derechos fundamentales	C	I	R	I	A	C	C	C
		11. Evaluación de protección de datos	C	I	R	I	C	A	C	C
		12. Elaboración de documentación de protección de datos	C	I	R	I	C	A	C	C
	Desarrollo	13. Preparación y limpieza de datos	R	C	A	I	C	C	C	C
		14. Validación sectorial previa al despliegue	I	I	R	C	C	C	C	A
		15. Desarrollo y entrenamiento del modelo	R	C	A	I	C	C	C	C
		16. Evaluación de sesgos	R	I	C	I	A	C	C	C

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

Tareas asociadas con la Gestión del Riesgo IA			Roles asociados a Gestión del Riesgo IA							
			1º LDD Gestión operativa				2º LDD Gestión de riesgos y cumplimiento			
Fase del Ciclo de Vida	**Subfases**	**Actividades**	***Desarrolladores de Sistemas IA***	***Equipo de Implementación de Sistemas IA***	**Responsable de IA (CIA)**	***Órgano Promotor***	**Responsable de Ética de IA**	***Delegado/a de Protección de Datos (DPD)***	**Responsable de Riesgos IA (CIA)**	**Responsable Sectorial (Salud/Smart Cities)**
		17. Pruebas funcionales y técnicas de sistema IA	R	C	A	I	C	C	C	C
	Implementación	18. Informe ético del sistema IA	C	I	C	I	AR	C	C	C
		19. Control de explicabilidad del sistema IA	R	I	AR	C	C	C	C	C
		20. Control de robustez del sistema IA	R	I	A	C	C	C	C	C
		21. Pruebas de rendimiento del modelo IA	R	C	A	C	I	I	C	C
		22. Validación de seguridad de entornos	C	R	A	I	I	I	C	C
		23. Validación del sistema IA para paso a producción	R	R	A	AR	C	C	C	A
		24. Puesta en producción del sistema IA	I	I	AR	C	C	C	C	C
		25. Despliegue e implementación de los mecanismos de monitorización para el sistema de IA en producción	C	R	A	C	I	I	C	C
		26. Actualización del Inventario post producción	C	R	A	R	I	C	C	C
Supervisión y monitorización de Casos de Uso	Supervisión	27. Gestión de Riesgos	I	C	A	C	C	C	R	C
		28. Cumplimiento normativo y regulatorio	I	I	AR	C	R	R	R	C
		29. Evaluación Ética	C	I	C	I	AR	C	C	C
	Monitorización	30. Control de KPIs de rendimiento	C	R	AR	C	C	I	C	C
		31. Control de data drift y concept drift	C	R	AR	C	C	I	C	C
		32. Control de explicabilidad en producción	C	R	AR	C	C	I	C	C

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

10. Referencias

1. Unión Europea. (2024). 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 (Ley de Inteligencia Artificial). [AI Act].
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

2. Unión Europea. (2017). Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios (MDR).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R0745

3. Unión Europea. (2017). Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro (IVDR).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R0746

4. Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos (Reglamento General de Protección de Datos – RGPD).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679

5. Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas destinadas a garantizar un nivel elevado común de ciberseguridad en la Unión Europea (Directiva NIS2).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555

6. España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).* Boletín Oficial del Estado (BOE), núm. 294, de 6 de diciembre de 2018.
https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

7. Comisión Europea. (2024). Oficina Europea de Inteligencia Artificial (AI Office) – Estructura de gobernanza y funciones.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202401459

8. Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC). (2023). ISO/IEC 42001:2023 – Tecnologías de la información – Inteligencia artificial – Sistema de gestión.
https://www.iso.org/standard/81230.html

9. Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC). (2023). ISO/IEC 23894:2023 – Inteligencia artificial – Directrices para la gestión del riesgo.
https://www.iso.org/standard/77608.html

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

10. Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC). (2022). ISO/IEC 38507:2022 – Gobernanza de las Tecnologías de la Información – Orientación para la gobernanza de la Inteligencia Artificial.
https://www.iso.org/standard/56641.html

11. Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC). (2022). ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad – Requisitos.
https://www.iso.org/standard/82875.html

12. Organización Internacional de Normalización (ISO). (2018). ISO 31000:2018 – Gestión del riesgo – Directrices.
https://www.iso.org/standard/65694.html

13. Organización Internacional de Normalización (ISO). (2016). ISO 13485:2016 – Productos sanitarios – Sistemas de gestión de la calidad – Requisitos para fines reglamentarios.
https://www.iso.org/standard/59752.html

14. Organización Internacional de Normalización (ISO). (2018). ISO 19011:2018 – Directrices para auditorías de sistemas de gestión.
https://www.iso.org/standard/70017.html

15. Organización Internacional de Normalización (ISO). (2015). ISO 14001:2015 – Sistemas de gestión ambiental – Requisitos con orientación para su uso.
https://www.iso.org/standard/60857.html

16. Comisión Europea. (2019). Directrices Éticas para una IA Confiable.
https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

17. Organización Mundial de la Salud (OMS). (2021). Ética y gobernanza de la inteligencia artificial para la salud.
https://www.who.int/es/publications/i/item/9789240037403

18. Instituto Nacional de Estándares y Tecnología (NIST). (2023). AI Risk Management Framework 1.0 – Marco de gestión de riesgos de inteligencia artificial.
https://www.nist.gov/itl/ai-risk-management-framework

19. Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2023). Guidelines on AI Cybersecurity.
https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20of%20AI%20and%20Standardisation.pdf

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

11. 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.

11.1. Lista de materias tratadas en la guía

La guía aborda, de forma estructurada y conforme a la normativa vigente, las siguientes materias:

- Gobernanza institucional de la Inteligencia Artificial y estructura organizativa.
- Gestión de riesgos algorítmicos y principios de proporcionalidad.
- Protección de datos personales y derechos digitales (RGPD y LOPDGDD).
- Ciberseguridad, integridad técnica y gestión de incidentes (ISO/IEC 27001 y Directiva NIS2).
- Ética, derechos fundamentales y equidad algorítmica.
- Transparencia, rendición de cuentas y mecanismos de reporte institucional.
- Coordinación interinstitucional y relaciones sectoriales (Salud y Smart Cities).
- Auditoría interna, mejora continua y revisión estratégica.
- Cumplimiento normativo y trazabilidad documental.
- Adaptación al Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial) y a los estándares ISO/IEC 42001 y 23894.

11.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

11.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

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

Modelo de gobierno en IA en los entornos de Salud y Smart Cities

Octubre de 2025

Versión 1.0

Financiado por la Unión Europea NextGenerationEU