RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Capacitación organizativa en ciberseguridad IA aplicada a las administraciones públicas en entornos de Smart Cities y Salud

Diciembre 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: 15/12/2025

Fecha de última actualización: 10/01/2026

ÍNDICE DE CONTENIDOS

1. Introducción 6
2. Objetivo y alcance 7
   2.1. Objetivo 7
   2.2. Alcance 7
3. Referencias normativas 9
4. Definiciones 12
5. Relación entre capacitación, gestión del riesgo y el gobierno de la IA 15
   5.1. La capacitación como medida exigible 15
   5.2. Vinculación con la gestión del riesgo de IA 16
   5.3. Capacitación y cumplimiento demostrable 16
6. Modelo organizativo de capacitación en ciberseguridad aplicada a la Inteligencia Artificial 17
   6.1. Principios rectores del modelo de capacitación 17
   6.2. Capacitación como sistema organizativo 18
   6.3. Articulación del modelo dentro de la organización 18
   6.4. Proporcionalidad y adaptabilidad del modelo 18
7. Perfiles organizativos y necesidades de capacitación 20
   7.1. Alta dirección y responsables políticos o directivos 20
   7.2. Responsables de gobierno del dato e IA 20
   7.3. Responsables de ciberseguridad y tecnologías de la información (CISO/CIO) 21
   7.4. Personal técnico y desarrolladores 21
   7.5. Personal funcional y operativo 22
   7.6. Personal jurídico, cumplimiento y control interno 22
   7.7. Proveedores y colaboradores cuando aplique 23
8. Plan de implantación del modelo de capacitación en ciberseguridad aplicada a la Inteligencia Artificial 24
   8.1. Metodología de implantación por fases y criterios de validación 24
      8.1.1. Fase 1: Diagnóstico institucional, descubrimiento de sistemas y análisis de brechas de competencia 24
      8.1.2. Fase 2: Diseño formal del sistema de capacitación y de los mecanismos de verificación 25
      8.1.3. Fase 3: Despliegue controlado, ejecución supervisada y generación de evidencia 27
      8.1.4. Fase 4: Integración plena en los sistemas de gestión y control permanente 28
9. Seguimiento, verificación y mejora continua del modelo de capacitación 29
   9.1. Seguimiento periódico de la capacitación como control organizativo 29

9.2. Verificación y evidencia: trazabilidad de competencias y registros de control 30
9.3. Indicadores de desempeño y eficacia de la capacitación 31
9.4. Actualización por cambios del sistema y por evolución del riesgo 31
9.5. Auditoría interna y revisión de eficacia 32
9.6. Cultura organizativa y gestión del cambio 33
10. Referencias 34
11. Otras referencias de interés 36
11.1. Lista de materias tratadas en la guía 36
11.2. Lista de productos mencionados en la guía 37
11.3. Lista de servicios mencionados en la guía 37

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

ÍNDICE DE TABLAS

Tabla 1: Definiciones empleadas. 14

1. Introducción

La adopción de sistemas de Inteligencia Artificial en las administraciones públicas se ha consolidado como un elemento estructural de los procesos de modernización del sector público, especialmente en ámbitos de elevada criticidad como las Smart Cities y la Salud. En estos contextos, la IA se utiliza para apoyar decisiones y optimizar procesos que inciden directamente en la continuidad de servicios esenciales, en la seguridad de las personas y, en numerosos casos, en el ejercicio de derechos fundamentales.

Esta evolución tecnológica no supone únicamente la incorporación de nuevas herramientas digitales. Implica la introducción de nuevos activos organizativos, como datos, modelos, configuraciones, integraciones y registros, así como nuevas dependencias respecto de proveedores, plataformas, servicios gestionados y terceros. Asimismo, los sistemas de IA incorporan comportamientos específicos que pueden manifestarse de forma incorrecta o no prevista a lo largo de su ciclo de vida, alterando de manera sustancial el perfil de riesgo institucional.

Los sistemas de IA operan con distintos grados de autonomía, se integran en flujos de decisión existentes y generan resultados que influyen en actuaciones administrativas, clínicas u operativas. En consecuencia, un uso indebido, una degradación progresiva del desempeño o una gestión inadecuada del sistema puede traducirse en la degradación de servicios públicos urbanos, en la afectación a la seguridad del paciente, en la exposición de datos de especial sensibilidad o en la adopción de decisiones que no resulten defendibles ante el control interno o ante autoridades competentes.

La experiencia operativa en el sector público pone de manifiesto que una parte significativa de los fallos y desviaciones asociados a proyectos de IA no responde a deficiencias técnicas aisladas, sino a factores organizativos, como el uso fuera del propósito previsto, la supervisión humana sin una aplicación práctica efectiva, la ausencia de criterios claros de actuación ante anomalías o una comprensión insuficiente de los límites y condiciones de uso seguro del sistema. Por este motivo, la seguridad y la conformidad normativa dependen no solo de controles técnicos, sino también de la competencia efectiva de las personas que participan en el diseño, adquisición, integración, despliegue, operación, supervisión y control de estos sistemas.

En este contexto, la capacitación organizativa adquiere una relevancia estructural. No puede abordarse como un elemento accesorio ni como una iniciativa voluntaria, sino como un componente necesario para garantizar que los sistemas de IA se utilizan de forma segura, conforme y controlada a lo largo de todo su ciclo de vida institucional.

La presente guía se integra en el conjunto de documentos del proyecto que establecen el modelo de gobierno de la IA, la metodología de gestión de riesgos, la clasificación de sistemas conforme al Reglamento europeo de IA y la definición de roles y responsabilidades asociadas. Esta guía no sustituye ni reproduce dichos contenidos. Su finalidad es complementaria y específica: establecer el marco organizativo de la capacitación en ciberseguridad aplicada a la Inteligencia Artificial, de modo que los principios, obligaciones y controles definidos en las guías de referencia puedan aplicarse de forma efectiva y defendible en la práctica.

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 establecer un marco organizativo, estructurado y auditable de capacitación en ciberseguridad aplicada a la Inteligencia Artificial, dirigido a las administraciones públicas que desarrollan, adquieren, integran, despliegan, operan o supervisan sistemas de IA en entornos de Smart Cities y Salud.

A efectos de esta guía, la capacitación se entiende como un control organizativo orientado a reducir riesgo real, y no como un catálogo de acciones formativas ni como una iniciativa genérica de concienciación. Desde esta perspectiva, la guía define cómo una organización debe asegurar que cada rol relevante dispone de las competencias necesarias para ejercer sus funciones de forma segura, conforme y controlada, con capacidad para:

- Aplicar la supervisión humana exigible cuando corresponda.
- Operar los sistemas conforme a su propósito previsto, a sus límites y a las condiciones de seguridad definidas.
- Detectar, gestionar y escalar anomalías e incidentes específicos de IA.
- Generar y conservar evidencia verificable de competencia, autorización y trazabilidad asociada a funciones críticas.

Este enfoque permite integrar la capacitación en los sistemas de gestión y control ya existentes, incluyendo el modelo de gobierno de la IA, la gestión del riesgo, la seguridad de la información y el cumplimiento normativo, y facilita demostrar su implantación mediante criterios objetivos ante órganos directivos, auditoría interna u otras instancias de control.

2.2. Alcance

Esta guía es aplicable a administraciones públicas y entidades del sector público institucional, así como a entidades colaboradoras o concesionarias cuando, por su papel operativo o de soporte, intervengan en sistemas de IA utilizados para la prestación de servicios urbanos o sanitarios.

El alcance comprende sistemas de IA en cualquier fase de su ciclo de vida institucional, incluyendo la planificación y aprobación del caso de uso, la adquisición o desarrollo, la validación, el despliegue, la operación, la modificación, la monitorización y la retirada.

La guía resulta de aplicación a sistemas de IA utilizados, entre otros, en servicios urbanos como movilidad, energía, gestión ambiental, seguridad, emergencias, atención ciudadana y operación de infraestructuras conectadas. En el ámbito de la salud, se aplica tanto a sistemas empleados en la gestión sanitaria y la salud pública como a aquellos que influyen en procesos asistenciales y tratan datos de salud u otras categorías especiales de datos personales.

La aplicación concreta de la guía deberá ajustarse por proporcionalidad en función del nivel de riesgo del sistema y de la criticidad del servicio afectado, utilizando los criterios de gestión de riesgo y clasificación establecidos en las guías del proyecto correspondientes.

A efectos operativos, se entiende que el programa de capacitación debe contemplar, como mínimo, a:

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

- Alta dirección y responsables políticos o directivos.
- Funciones de gobierno del dato e Inteligencia Artificial.
- Responsables de ciberseguridad y tecnologías de la información.
- Personal técnico y desarrolladores.
- Personal funcional y operativo.
- Funciones jurídicas, de cumplimiento y control interno.
- Proveedores y colaboradores externos, cuando aplique.

La definición detallada de necesidades de capacitación por perfil se desarrolla en capítulos posteriores, evitando duplicar las definiciones de roles, órganos y líneas de defensa ya establecidas en la guía de modelo de gobierno de la IA del proyecto.

3. Referencias normativas

Las referencias incluidas en este apartado se presentan con carácter informativo y orientativo, con el fin de ofrecer a las administraciones públicas un contexto general sobre los marcos normativos y técnicos que inciden en el uso de la inteligencia artificial en servicios urbanos y sanitarios. Su inclusión no implica que todos los perfiles deban conocer o aplicar directamente estas normas, sino situar la capacitación en el contexto de obligaciones legales, técnicas y de seguridad aplicables.

- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, Reglamento de Inteligencia Artificial (RIA):** Establece un marco jurídico armonizado para el desarrollo y uso de sistemas de inteligencia artificial en la Unión Europea. Introduce un enfoque basado en el riesgo y obligaciones específicas para los sistemas de alto riesgo, incluidos los empleados en la seguridad pública y gestión de infraestructuras urbanas críticas. Refuerza los principios de transparencia, trazabilidad, supervisión humana y rendición de cuentas.

- **Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD):** Garantiza la protección de las personas físicas en lo relativo al tratamiento de datos personales. Resulta directamente aplicable al tratamiento automatizado de datos mediante inteligencia artificial, especialmente cuando involucra datos biométricos, de imagen o de voz.

- **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Desarrolla y complementa el RGPD en el ordenamiento español, incorporando derechos digitales y estableciendo obligaciones de transparencia, supervisión y rendición de cuentas aplicables también a sistemas basados en inteligencia artificial.

- **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, Directiva NIS2:** Refuerza las medidas para garantizar un nivel elevado de ciberseguridad en la Unión Europea. Afecta a entidades esenciales e importantes, incluidas administraciones públicas, servicios sanitarios, operadores de infraestructuras críticas y proveedores tecnológicos que prestan servicios relacionados con las Smart Cities.

- **Esquema Nacional de Seguridad (ENS):** Define los principios y requisitos mínimos de seguridad aplicables a los sistemas de información del sector público español y de los proveedores tecnológicos. Es fundamental para garantizar la protección de la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de la información procesada por sistemas de IA utilizados en el sector público.

- **Data Governance Act, Reglamento (UE) 2022/868:** Regula la gobernanza y la reutilización segura de datos en la Unión Europea, fomentando el intercambio seguro y confiable de información y la protección de los datos sensibles, incluidos los de carácter sanitario.

- **Digital Services Act, Reglamento (UE) 2022/2065:** Establece obligaciones de transparencia, trazabilidad y diligencia debida para prestadores de servicios digitales y plataformas en línea, aplicables a la gestión de contenidos sintéticos generados mediante IA.

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

- **Carta de Derechos Digitales (Gobierno de España, 2021):** Reconoce los derechos fundamentales en el entorno digital, incluyendo identidad, veracidad informativa, protección frente a la manipulación algorítmica y garantías de transparencia en el uso de tecnologías basadas en inteligencia artificial.

- **ISO/IEC 42001:2023 – Sistemas de gestión de la inteligencia artificial:** Establece requisitos para implantar y mantener un sistema de gestión de IA que garantice un uso seguro, responsable y trazable de los algoritmos. Su aplicación refuerza la gobernanza, la transparencia y el control en sistemas generativos utilizados en entornos urbanos y sanitarios.

- **ISO/IEC 23894:2023 – Gestión del riesgo en la inteligencia artificial:** Define un marco estructurado para identificar, evaluar y mitigar los riesgos derivados del desarrollo y uso de la IA, incluyendo los relacionados con la generación de contenidos sintéticos y su impacto en la integridad de la información.

- **ISO/IEC 38507:2022 – Gobernanza de la inteligencia artificial:** Proporciona directrices para integrar la IA en los sistemas de gobernanza organizacional, asignando responsabilidades, supervisión de la alta dirección y control del riesgo en la toma de decisiones automatizada.

- **ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad:** Establece requisitos para gestionar la seguridad de la información en organizaciones que operan con IA, asegurando la confidencialidad, integridad, disponibilidad y autenticidad de los datos procesados.

- **ISO 31000:2018 – Gestión del riesgo**: Ofrece principios y directrices generales para establecer un marco eficaz de gestión del riesgo organizativo, aplicable a los riesgos tecnológicos y algorítmicos en los sistemas inteligentes de Smart Cities y salud.

- **ISO/IEC 30111:2019 – Gestión de vulnerabilidades:** Describe procesos para la recepción, análisis y coordinación de vulnerabilidades en software y sistemas de IA, esenciales para prevenir incidentes que afecten la integridad de los modelos y de los datos.

- **NIST AI Risk Management Framework 1.0 (2023):** Proporciona un marco de referencia para gestionar los riesgos de la IA en todo su ciclo de vida, promoviendo la transparencia, la responsabilidad y la mitigación de sesgos en sistemas automatizados y generativos.

- **UNE 178104:2017 – Ciudades inteligentes. Interoperabilidad de plataformas de ciudad inteligente:** Norma del marco español de Smart Cities que establece los requisitos y modelos de interoperabilidad necesarios entre plataformas urbanas, sistemas municipales y servicios digitales. Resulta esencial para garantizar que los sistemas basados en IA puedan integrarse de forma segura, coherente y trazable con la infraestructura digital urbana, asegurando la continuidad del servicio y la correcta gestión del dato municipal.

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

- **UNE 178108:2017 – Ciudades inteligentes. Gestión inteligente de activos urbanos:** Define los principios, requisitos y procedimientos para la gestión digitalizada de activos urbanos mediante tecnologías avanzadas, incluyendo sensores, IoT e inteligencia artificial. Su inclusión es clave para asegurar que los sistemas de IA que interactúan con mobiliario urbano, alumbrado, redes energéticas o hidráulicas operen bajo criterios homogéneos de mantenimiento, seguridad y trazabilidad.

- **UNE 178301:2015 – Ciudades inteligentes. Sistema de indicadores y métricas:** Establece un marco común de indicadores urbanos que permite evaluar, monitorizar y comparar el rendimiento de los servicios inteligentes. Es relevante en el contexto de IA porque facilita la medición de impacto, la evaluación del desempeño algorítmico y el seguimiento de resultados que afectan directamente a los usuarios finales.

- **UNE 178503:2019 – Destinos turísticos inteligentes. Requisitos:** Aunque orientada a destinos turísticos, esta norma se considera aplicable a servicios urbanos con fuerte componente turístico dentro de Smart Cities. Incluye requisitos de accesibilidad, interoperabilidad, gobernanza del dato y sostenibilidad, todos ellos esenciales en sistemas de IA que interactúan con visitantes y residentes en áreas urbanas de interés turístico.

- **UNE-EN 301549:2022 – Accesibilidad de los productos y servicios TIC:** Norma armonizada que establece los requisitos de accesibilidad aplicables a productos, servicios digitales y plataformas públicas, incluyendo interfaces basadas en IA. Su incorporación es imprescindible para garantizar que los sistemas de IA urbanos sean accesibles para personas mayores, personas con discapacidad y colectivos en riesgo de exclusión digital.

- **ISO/IEC 25012:2014 – Modelo de calidad de datos:** Norma internacional que define las características de calidad del dato, incluyendo precisión, integridad, disponibilidad, trazabilidad y consistencia. Es fundamental para asegurar que los sistemas de IA urbanos se alimenten de datos fiables, especialmente en movilidad, gestión energética, seguridad urbana y servicios automatizados dirigidos al ciudadano.

- **ISO 37120 / ISO 37122 / ISO 37123 – Indicadores para ciudades sostenibles e inteligentes:** Conjunto de normas internacionales que establecen indicadores avanzados para la gestión inteligente y sostenible de las ciudades. Su adopción ofrece un marco metodológico sólido para integrar IA en la planificación urbana y evaluar su impacto sobre la ciudadanía, reforzando la transparencia, la comparabilidad y la toma de decisiones basada en datos.

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

4. Definiciones

Este capítulo recopila los conceptos clave y acrónimos utilizados a lo largo de la guía.

Término/Acrónimo	Definición
Alucinación	Resultado generado por un sistema de Inteligencia Artificial, especialmente generativo, que parece correcto o plausible, pero es falso, inventado o no está fundamentado en los datos de entrada, en el entrenamiento del modelo o en el contexto proporcionado.
Automatización acrítica	Uso de los resultados de un sistema de IA sin aplicar validación, contraste o supervisión humana, incluso cuando el contexto, el impacto o las señales del sistema exigirían intervención.
Clasificación de riesgo de IA	Proceso mediante el cual un sistema de Inteligencia Artificial se categoriza en función del nivel de riesgo que puede generar para las personas, los servicios o los derechos, atendiendo a su finalidad, contexto de uso e impacto potencial.
Contenido sintético	Información generada total o parcialmente por un sistema de IA, como texto, imágenes, audio, vídeo o código, que no procede directamente de una fuente humana o de un registro real.
Control de cambios	Conjunto de procedimientos destinados a garantizar que cualquier modificación en un sistema de IA, incluidos datos, modelos, configuraciones o integraciones, se evalúa, autoriza, documenta y valida antes de su aplicación.
Data Poisoning (envenenamiento de datos)	Ataque o manipulación deliberada de los datos de entrenamiento o entrada de un sistema de IA con el objetivo de alterar su comportamiento, degradar su rendimiento o inducir resultados incorrectos.
Deriva del modelo (Model Drift)	Degradación o cambio significativo del rendimiento de un sistema de IA debido a variaciones en los datos de entrada, en el entorno operativo o en los patrones sobre los que fue entrenado.
Explicabilidad (XAI)	Capacidad de un sistema de IA para ofrecer información comprensible sobre cómo y por qué produce determinados resultados, de forma adecuada al contexto y a las personas usuarias.
IA generativa	Tipo de sistema de Inteligencia Artificial diseñado para generar nuevos contenidos, como texto, imágenes, audio o código, a partir de instrucciones o datos de entrada.

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

Término/Acrónimo	Definición
Impacto crítico	Consecuencia potencial de un fallo, uso indebido o mal funcionamiento de un sistema de IA que puede afectar gravemente a la seguridad, la salud, los derechos fundamentales o la continuidad de un servicio esencial.
Incidente de IA	Evento no deseado relacionado con el funcionamiento, uso o supervisión de un sistema de IA que puede generar impacto negativo en la organización, los servicios o las personas.
Prompt Injection (Inyección de prompts)	Técnica mediante la cual se introducen instrucciones manipuladas en un sistema de IA generativa para alterar su comportamiento, eludir controles o provocar respuestas no previstas.
Inteligencia Artificial (IA)	Conjunto de sistemas informáticos que, a partir del análisis de datos y con distintos niveles de autonomía, generan resultados como predicciones, recomendaciones, clasificaciones, contenidos o decisiones que influyen en entornos físicos o digitales.
Inventario de sistemas de IA	Registro estructurado y actualizado de los sistemas de Inteligencia Artificial utilizados por la organización, incluyendo su finalidad, estado, responsables, dependencias y nivel de riesgo.
Linaje de datos	Capacidad de identificar el origen, las transformaciones, el uso y el destino de los datos a lo largo de su ciclo de vida dentro de un sistema o proceso.
Logs (registros)	Registros automáticos que documentan eventos, accesos, decisiones o acciones realizadas por un sistema o por las personas usuarias, con fines de control, auditoría y análisis de incidentes.
MLOps	Conjunto de prácticas, procesos y herramientas destinadas a gestionar de forma controlada el ciclo de vida de los modelos de aprendizaje automático, desde su desarrollo hasta su operación y actualización.
Modelo fundacional	Modelo de IA entrenado con grandes volúmenes de datos generales, capaz de adaptarse a múltiples tareas distintas mediante ajustes o instrucciones adicionales.
Monitorización	Seguimiento continuo del comportamiento y rendimiento de un sistema de IA para detectar anomalías, degradaciones, desviaciones del propósito previsto o riesgos emergentes.
Propósito previsto	Finalidad, contexto de uso, población objetivo y límites operativos para los que un sistema de IA ha sido diseñado, validado y autorizado.

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

Término/Acrónimo	Definición
RAG (Retrieval-Augmented Generation)	Técnica empleada en sistemas de IA generativa que combina la recuperación de información desde fuentes externas con la generación de respuestas, de modo que el sistema consulta datos o documentos antes de producir el resultado.
Repositorio de evidencias	Sistema organizado para almacenar y conservar evidencias documentales de capacitación, control y cumplimiento, garantizando su integridad, trazabilidad y disponibilidad.
Riesgo residual	Nivel de riesgo que permanece tras aplicar las medidas de control y mitigación previstas.
Shadow AI	Uso de sistemas de Inteligencia Artificial dentro de una organización sin conocimiento, autorización o control formal por parte de los órganos responsables.
Supervisión humana efectiva	Capacidad real de personas autorizadas para comprender el funcionamiento del sistema de IA, detectar anomalías, intervenir, escalar, suspender o modificar su uso conforme a procedimientos definidos.
Trazabilidad	Capacidad de reconstruir de forma fiable las decisiones, acciones y cambios realizados en un sistema, incluyendo quién intervino, cuándo, cómo y con qué información.
Sistema de Gestión de Seguridad de la Información (SGSI)	Es un conjunto de políticas, procedimientos, procesos y controles cuya finalidad es proteger los activos de información de una organización.
Riesgo intrínseco	El nivel de riesgo que presenta un sistema, proceso o activo antes de aplicar cualquier medida de control.

TABLA 1: DEFINICIONES EMPLEADAS.

5. Relación entre capacitación, gestión del riesgo y el gobierno de la IA

La capacitación organizativa en ciberseguridad aplicada a la Inteligencia Artificial constituye un mecanismo estructural de control del riesgo integrado en el sistema de gobierno de la IA. En el contexto de las administraciones públicas que operan sistemas de IA en entornos de Smart Cities y Salud, su función es habilitar la aplicación efectiva de los controles de gobierno y gestión del riesgo definidos por la organización.

En ausencia de una capacitación estructurada y adecuada al riesgo, incluso modelos de gobierno formalmente correctos o arquitecturas técnicas robustas resultan insuficientes para garantizar un control efectivo. En estos casos, se producen deficiencias organizativas que afectan directamente a la capacidad de la entidad para gestionar riesgos y rendir cuentas.

En particular, pueden producirse, entre otros, los siguientes efectos:

- La no detección o el escalado tardío de riesgos y anomalías relevantes.
- La aplicación de carácter exclusivamente documental o incompleta de los controles definidos.
- La imposibilidad de demostrar diligencia debida y control efectivo ante auditorías, inspecciones o análisis de incidentes.

La capacitación no constituye, por tanto, un elemento accesorio del gobierno de la IA, sino una condición operativa necesaria para su funcionamiento efectivo.

5.1. La capacitación como medida exigible

El marco normativo europeo y nacional establece la obligación de que las organizaciones adopten medidas técnicas y organizativas adecuadas para garantizar un uso seguro, conforme y responsable de los sistemas digitales y, en particular, de los sistemas de Inteligencia Artificial. En este contexto, la capacitación del personal forma parte de dichas medidas organizativas exigibles, al mismo nivel que la definición de roles, la documentación de procesos o la implantación de controles técnicos.

El Reglamento (UE) 2024/1689 exige que los sistemas de IA, especialmente los clasificados como de alto riesgo, sean utilizados conforme a las instrucciones, limitaciones y salvaguardas previstas. Este requisito presupone necesariamente que las personas usuarias, supervisoras o responsables del sistema comprenden de manera efectiva:

- El propósito previsto del sistema.
- Sus límites funcionales y operativos.
- Los riesgos asociados a su utilización, incluidos los derivados de un uso fuera de propósito.
- Los procedimientos de actuación ante desviaciones, anomalías o incidentes.

De forma análoga, la Directiva (UE) 2022/2555 (NIS2) refuerza la responsabilidad de los órganos de dirección en materia de ciberseguridad, incluyendo la obligación de garantizar que el personal dispone de las competencias adecuadas para gestionar riesgos y responder a incidentes. En el sector público, este principio se ve reforzado por el Esquema Nacional de Seguridad, que reconoce la formación y la competencia como elementos esenciales del sistema de protección.

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

En este contexto, la capacitación organizativa en IA y ciberseguridad debe entenderse como:

- Una condición previa para el despliegue efectivo de determinados sistemas de IA, en particular los de alto riesgo.
- Un requisito para la continuidad operativa de servicios urbanos y sanitarios críticos.
- Un elemento de evidencia esencial para demostrar cumplimiento normativo y diligencia institucional ante autoridades competentes y órganos de control.

5.2. Vinculación con la gestión del riesgo de IA

La presente guía se apoya en la metodología de gestión del riesgo de IA definida en la correspondiente guía del proyecto, sin reproducirla ni modificarla. Su aportación específica consiste en establecer cómo la capacitación opera como control organizativo necesario para la eficacia real de dicha metodología.

En términos operativos, la capacitación permite que las personas que intervienen en el ciclo de vida del sistema:

- Identifiquen riesgos relevantes de forma temprana y coherente con el contexto operativo.
- Interpreten adecuadamente los resultados de las evaluaciones de riesgo y de impacto.
- Apliquen de manera consistente y sostenida las medidas de mitigación definidas, tanto técnicas como organizativas.

La profundidad, el alcance y el contenido de la capacitación deben ajustarse de forma proporcional al nivel de riesgo del sistema de IA, al impacto potencial de sus resultados y al grado de autonomía del sistema en la toma de decisiones. De este modo, la capacitación se integra como un control transversal presente en todas las fases del ciclo de vida de la IA, alineado con los principios establecidos en las normas ISO/IEC 23894 e ISO 31000.

5.3. Capacitación y cumplimiento demostrable

En el ámbito de la Inteligencia Artificial, el cumplimiento no se limita a la existencia formal de políticas o procedimientos, sino que requiere evidencias de que la organización es capaz de aplicarlos de forma efectiva en la práctica. La capacitación constituye un factor determinante de esta capacidad demostrable al contribuir a:

- Generar registros verificables de competencias adquiridas
- Asegurar la coherencia entre responsabilidades asignadas y capacidades reales
- Y reducir la probabilidad de errores humanos que deriven en incidentes de seguridad, vulneraciones de derechos o uso indebido de los sistemas

En ausencia de evidencia adecuada de capacitación, la organización no puede sostener de forma defendible la aplicación efectiva de sus controles de gobierno de la IA. Por ello, la capacitación organizativa debe integrarse en los mecanismos de control interno, auditoría y mejora continua definidos, actuando como elemento habilitador y verificable del sistema de gobierno de la IA.

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

6. Modelo organizativo de capacitación en ciberseguridad aplicada a la Inteligencia Artificial

La capacitación organizativa en ciberseguridad aplicada a la Inteligencia Artificial debe concebirse como un sistema estructural, permanente y gobernado, integrado en el modelo de control interno de la organización. Se concibe como un marco organizativo que garantiza que las personas que intervienen en el ciclo de vida de los sistemas de IA disponen, en todo momento, de las competencias necesarias para ejercer sus funciones de forma segura, conforme y controlada.

Este modelo se articula en coherencia con el modelo de gobierno de la IA definido por la organización y con los mecanismos de gestión del riesgo, sin duplicar estructuras ni redefinir responsabilidades. Mientras que el modelo de gobierno determina quién decide, quién supervisa y quién rinde cuentas, el modelo de capacitación establece cómo se asegura que dichas funciones se ejercen con capacidad real, conocimiento suficiente y criterios de actuación adecuados al riesgo.

La ausencia de un modelo organizativo de capacitación estructurado constituye un riesgo institucional en sí mismo, ya que impide aplicar de forma efectiva las obligaciones normativas, debilita la supervisión humana exigible y compromete la capacidad de demostrar diligencia debida ante auditorías, inspecciones o incidentes relacionados con el uso de sistemas de IA.

6.1. Principios rectores del modelo de capacitación

El modelo organizativo de capacitación se fundamenta en un conjunto de principios que garantizan su coherencia institucional, su eficacia operativa y su alineación con el marco normativo aplicable:

I. **Principio de adecuación al riesgo**
Las competencias exigidas a cada perfil se ajustan al nivel de riesgo del sistema de IA, al impacto potencial de sus resultados y al grado de autonomía del sistema. Este enfoque evita tanto la infraformación, ya que genera riesgos operativos, como la sobrecarga innecesaria en contextos de bajo riesgo.

II. **Principio de integración organizativa**
La capacitación se integra con la gestión del riesgo, la ciberseguridad, la protección de datos, el cumplimiento normativo y la auditoría interna. De este modo, la capacitación se convierte en un control transversal.

III. **Principio de continuidad y actualización**
Dado que los sistemas de IA evolucionan, se reentrenan, se amplían o se integran en nuevos procesos, las competencias requeridas no pueden considerarse estáticas. El modelo debe garantizar la actualización periódica de conocimientos, especialmente cuando se producen cambios relevantes en los sistemas, en el contexto normativo o en el perfil de amenazas.

IV. **Principio de verificabilidad**

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

Toda capacitación relevante debe generar evidencia documentada, trazable y auditable, de forma que la organización pueda demostrar, ante órganos de control internos o externos, que las personas que ejercen funciones críticas disponen de las competencias adecuadas.

6.2. Capacitación como sistema organizativo

El modelo de capacitación se concibe como un sistema organizativo completo y continuado. A tal efecto, la organización debe definir, documentar y mantener:

- Un marco común de competencias relacionadas con la IA y la ciberseguridad.
- Criterios formales para determinar qué competencias son exigibles a cada perfil organizativo.
- Mecanismos de planificación, ejecución, seguimiento y revisión de la capacitación.
- Responsabilidades explícitas sobre la gestión, supervisión y validación del modelo.

Este enfoque permite que la capacitación acompañe al sistema de IA durante todas las fases de su ciclo de vida institucional, desde la concepción y el diseño hasta su modificación sustancial o retirada, resultando especialmente crítico en entornos de Salud y de Smart Cities.

6.3. Articulación del modelo dentro de la organización

El modelo organizativo de capacitación debe integrarse formalmente en la estructura de la organización, con una asignación clara de responsabilidades y sin generar nuevas capas de gobierno innecesarias.

La responsabilidad sobre la existencia, adecuación y eficacia del modelo recae en la Alta dirección, en coherencia con las obligaciones de diligencia y supervisión establecidas en el marco normativo de ciberseguridad y de Inteligencia Artificial. Esta responsabilidad se ejerce a través de los órganos de gobierno ya definidos en el modelo de gobierno de la IA.

La coordinación operativa corresponde a las funciones responsables de la IA y de la gestión del riesgo, que deben asegurar la coherencia entre perfiles, riesgos identificados y competencias exigidas. La ejecución de las acciones de capacitación podrá apoyarse en unidades de formación, recursos humanos u otros servicios internos, garantizando siempre la alineación con los criterios técnicos, regulatorios y de seguridad definidos en esta guía.

6.4. Proporcionalidad y adaptabilidad del modelo

El modelo organizativo de capacitación se diseña para ser proporcional y adaptable a organizaciones de distinto tamaño, complejidad y nivel de madurez. En organizaciones de menor tamaño, podrá materializarse mediante estructuras simplificadas, siempre que se preserve la trazabilidad, la asignación clara de responsabilidades y la capacidad de demostrar cumplimiento.

En organizaciones de mayor tamaño o en aquellas que operan sistemas de IA de riesgo elevado o impacto crítico, el modelo deberá desplegarse de forma más estructurada, con planes formales, seguimiento periódico, mecanismos de revisión reforzados y generación sistemática de evidencia

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

auditable. La proporcionalidad determina la forma de aplicación del modelo, pero no exime del cumplimiento de sus principios básicos.

7. Perfiles organizativos y necesidades de capacitación

La implantación y operación segura de sistemas de Inteligencia Artificial en administraciones públicas que prestan servicios en entornos de Smart Cities y Salud depende de la competencia efectiva de las personas que intervienen en su ciclo de vida. En coherencia con lo establecido en los capítulos anteriores, este capítulo concreta las necesidades de capacitación por perfil organizativo, sin introducir nuevos roles ni modificar responsabilidades.

La finalidad de este capítulo no es describir funciones ni estructuras de gobierno, ya definidas en la guía de Modelo de gobierno de la IA del proyecto, sino especificar las competencias mínimas que deben estar garantizadas para que cada perfil pueda ejercer sus funciones sin introducir riesgos adicionales para la organización, los servicios públicos o los derechos de las personas.

7.1. Alta dirección y responsables políticos o directivos

La Alta dirección y los responsables políticos o directivos ostentan la responsabilidad institucional última sobre la adopción, continuidad, ampliación, suspensión o retirada de sistemas de IA. Sus decisiones determinan el nivel de riesgo aceptado por la organización, las condiciones de uso admisible y el grado de dependencia respecto de terceros.

La capacitación de este perfil no tiene carácter técnico, sino estratégico y decisional. Debe permitir comprender las implicaciones reales del uso de IA en servicios públicos críticos y exigir evidencias suficientes antes de autorizar decisiones relevantes.

La capacitación de este perfil debe garantizar que dispone, como mínimo, de capacidad para:

- Comprender el enfoque basado en riesgo del Reglamento (UE) 2024/1689 para asumir la responsabilidad final sobre el nivel de riesgo aceptado por la organización en servicios urbanos y sanitarios.
- Valorar la introducción, ampliación o retirada de sistemas de IA basándose en evaluaciones de impacto completas, que ponderen los riesgos operativos, jurídicos, reputacionales y sobre derechos fundamentales frente a los beneficios esperados.
- Exigir condiciones mínimas de supervisión humana, trazabilidad y control como condición previa y necesaria para la autorización de cualquier sistema que interactúe con servicios críticos o derechos de las personas.
- Solicitar y evaluar evidencias de cumplimiento y control con un enfoque crítico.

7.2. Responsables de gobierno del dato e IA

Las funciones de gobierno del dato e IA, incluyendo perfiles como CAIO o CDO cuando existan, garantizan la coherencia, trazabilidad y control del conjunto de sistemas de IA como activos organizativos. Su capacitación se orienta al control del ciclo de vida completo del sistema y de los riesgos asociados a datos, modelos y configuraciones.

Las competencias de este perfil deben asegurar, como mínimo, su capacidad para:

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

- Garantizar la existencia y fiabilidad de un inventario centralizado de sistemas de IA, datos y modelos, como activo de control indispensable para la gobernanza y la auditoría.
- Establecer y hacer cumplir políticas rigurosas de linaje de datos, versionado de modelos y gestión formal de cambios, para asegurar la reproducibilidad de las decisiones y la capacidad de investigación de incidentes.
- Definir y documentar formalmente los límites de uso, supuestos operativos y condiciones de explotación segura, asegurando que son comprendidos y aplicados por los equipos operativos.
- Actuar como nexo de coherencia entre los riesgos identificados en las evaluaciones, los controles definidos por las políticas y las evidencias generadas en la operación diaria.

7.3. Responsables de ciberseguridad y tecnologías de la información (CISO/CIO)

Los responsables de ciberseguridad y TI aseguran la integración segura y resiliente de los sistemas de IA en la arquitectura tecnológica de la organización. Su capacitación aborda riesgos específicos de la IA que no se cubren adecuadamente mediante controles tradicionales de seguridad de la información.

Este perfil deberá ser competente para, como mínimo:

- Identificar y clasificar los activos específicos de IA (modelos, datos de entrenamiento, pipelines) para aplicar controles de seguridad adecuados a su criticidad, más allá de la protección genérica de la infraestructura.
- Integrar los sistemas de IA en el marco del ENS y en el SGSI, evitando que se conviertan en "islas" no controladas dentro de la arquitectura de seguridad de la organización.
- Diferenciar entre una degradación funcional (ej. deriva del modelo) y un ataque deliberado (ej. envenenamiento de datos), ya que una respuesta incorrecta puede agravar el incidente o destruir evidencia forense.
- Diseñar y exigir la implementación de registros (logs) y evidencias que permitan una investigación forense efectiva de incidentes específicos de IA y cumplir con las obligaciones de notificación de la Directiva NIS2.

7.4. Personal técnico y desarrolladores

El personal técnico y los desarrolladores determinan la robustez, fiabilidad y controlabilidad efectiva de los sistemas de IA. Su capacitación combina prácticas de desarrollo seguro con gestión de riesgos específicos de datos y modelos para garantizar que los sistemas sean auditables y operables de forma segura.

Las exigencias de capacitación para este perfil se orientan a garantizar su capacidad para:

- Identificar y mitigar activamente riesgos asociados a sesgos, deriva del modelo, manipulación de entradas (prompt injection, data poisoning) y exposición de información sensible durante la inferencia.
- Aplicar un control de cambios y un versionado rigurosos de datos y modelos, con una validación formal previa a cualquier despliegue o modificación en entornos productivos.

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

- Implementar mitigaciones técnicas verificables para los riesgos identificados, conservando evidencia suficiente de su eficacia para procesos de auditoría.
- Documentar de forma clara e inequívoca el propósito previsto del sistema, sus límites operativos conocidos y las condiciones de uso seguro para los operadores.

7.5. Personal funcional y operativo

El personal funcional y operativo materializa la supervisión humana efectiva durante el uso diario de los sistemas de IA. Su capacitación se orienta a la operación segura, la detección de anomalías y la activación de procedimientos definidos para evitar la automatización acrítica.

Este perfil debe demostrar, como mínimo, las siguientes capacidades operativas:

- Comprender y respetar el propósito previsto y los límites del sistema que utiliza, reconociendo cuándo un resultado puede requerir validación humana adicional.
- Detectar resultados incoherentes, degradaciones de rendimiento o usos indebidos, actuando como primera línea de defensa ante el comportamiento anómalo del sistema.
- Aplicar sin demora los procedimientos definidos de escalado, suspensión del sistema o conmutación a modos de operación manual cuando proceda.
- Registrar de forma suficiente la interacción con el sistema y las decisiones de intervención humana, generando una traza de auditoría defendible.

7.6. Personal jurídico, cumplimiento y control interno

Las funciones jurídicas y de control traducen obligaciones normativas en exigencias organizativas, contractuales y procedimentales. Su capacitación garantiza que el cumplimiento sea exigible y verificable.

Se considera esencial que este perfil disponga de capacidad para, como mínimo:

- Interpretar las obligaciones del RIA y otras normativas aplicables para traducirlas en controles organizativos y técnicos concretos.
- Incorporar requisitos de trazabilidad, auditoría, responsabilidad y control en los pliegos de contratación pública y en los contratos con proveedores, convirtiéndolos en obligaciones contractuales exigibles.
- Evaluar los impactos jurídicos y la responsabilidad institucional derivada de incidentes de IA, cambios relevantes en los sistemas o reclamaciones de terceros.
- Verificar la validez de las evidencias de cumplimiento generadas por la organización, anticipando los requerimientos de auditorías e inspecciones.

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

7.7. Proveedores y colaboradores cuando aplique

Cuando terceros intervienen en sistemas de IA, la organización debe asegurar que actúan con competencias equivalentes a las exigidas internamente. La capacitación se materializa como exigencia contractual y como condición verificable de la prestación del servicio.

La organización debe asegurar, como mínimo:

- La verificación previa de las competencias del personal de terceros que vaya a desempeñar funciones críticas, exigiendo acreditaciones o certificaciones cuando sea proporcionado.
- La inclusión de obligaciones contractuales explícitas sobre control de cambios, generación de evidencias, respuesta a incidentes y cumplimiento de las políticas de seguridad de la organización.
- La reserva de una capacidad de auditoría efectiva sobre los procesos y sistemas del proveedor, garantizando el acceso a la información relevante para verificar el cumplimiento.
- La participación necesaria de personal clave de terceros en los ejercicios o simulacros de respuesta a incidentes que realice la organización, cuando su rol sea crítico.

8. Plan de implantación del modelo de capacitación en ciberseguridad aplicada a la Inteligencia Artificial

La implantación del modelo de capacitación definido en esta guía constituye, en sí misma, un proceso de control organizativo estructural que debe ejecutarse con el mismo rigor metodológico, jurídico y de gobernanza que la implantación de un sistema de información crítico o de un control clave de seguridad. No se trata de un proyecto formativo discreto, ni de una iniciativa de mejora voluntaria, sino del establecimiento de una capacidad institucional permanente, orientada a reducir, gestionar y demostrar el control del riesgo humano asociado al uso de sistemas de Inteligencia Artificial en entornos de Smart Cities y Salud.

Este capítulo establece un marco formal para la implantación del modelo, definiendo condiciones, fases, responsabilidades y criterios de validación que permiten asegurar que la capacitación opera como un control real, efectivo, verificable y defendible, y no como un conjunto de acciones formativas desvinculadas de la gestión del riesgo. La correcta implantación del modelo constituye una condición necesaria para poder sostener, ante auditoría interna, inspección externa o investigación de incidentes, que la organización ejerce una diligencia debida razonable en el uso de sistemas de IA.

El plan de implantación se rige por los principios de proporcionalidad basada en el riesgo, priorización de sistemas y funciones críticas, integración en los sistemas de gestión existentes y generación sistemática de evidencia auditable. En consecuencia, la ausencia de implantación efectiva, o su ejecución sin una verificación efectiva, deberá tratarse como un riesgo organizativo de primer nivel, sujeto a los procedimientos de gestión del riesgo institucional.

8.1. Metodología de implantación por fases y criterios de validación

La implantación del modelo de capacitación se estructura en un conjunto de fases secuenciales, cuya finalización debe ser validada formalmente antes de avanzar a la fase siguiente. Esta metodología no persigue rigidez administrativa, sino asegurar que el modelo se construye sobre bases sólidas, coherentes con el estado real de la organización y alineadas con el perfil de riesgo de los sistemas de IA en uso.

La duración concreta de cada fase podrá ajustarse en función del tamaño, complejidad y madurez de la organización, pero los objetivos, contenidos y resultados exigibles de cada fase no son opcionales.

8.1.1. Fase 1: Diagnóstico institucional, descubrimiento de sistemas y análisis de brechas de competencia

El objetivo de esta fase es establecer una línea base auditable del estado real de control de la organización en relación con la capacitación en IA. Esta fase es crítica, ya que cualquier deficiencia en su ejecución compromete la validez del conjunto del modelo. Esta fase incluye, como actuaciones mínimas siendo:

I. En primer lugar, la consolidación, validación y ampliación del inventario institucional de sistemas de IA, en coordinación con la función de gobierno de la IA. Este ejercicio no puede

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

limitarse a los sistemas formalmente declarados. La organización deberá adoptar medidas activas para identificar uso no declarado o parcialmente gestionado de IA (Shadow AI), incluyendo, cuando sea proporcionado, encuestas obligatorias a unidades organizativas, revisión de contratos y licencias de software con capacidades de IA embebidas, análisis de integraciones SaaS y revisión de prácticas habituales de uso de herramientas de IA generativa en el entorno laboral. El inventario resultante deberá incluir todos los sistemas en diseño, adquisición, prueba, producción u operación, reflejando su propósito, estado en el ciclo de vida, dependencias de terceros y clasificación formal de riesgo conforme al Reglamento (UE) 2024/1689 y a la metodología definida en las guías del proyecto.

II. En segundo lugar, el mapeo formal de roles, funciones y responsabilidades asociados a cada sistema de IA. Este mapeo deberá asignar personas o unidades organizativas concretas a los perfiles definidos en el Capítulo 7, reflejando la participación real en el ciclo de vida del sistema y no únicamente la estructura orgánica formal. Este registro constituye el documento de referencia para determinar qué personas están sujetas a qué exigencias de capacitación, y su ausencia o falta de precisión invalida la trazabilidad del modelo.

III. En tercer lugar, la ejecución de un análisis de brechas de competencia, basado en evidencias verificables y diseñado de forma escalable y proporcionada. En organizaciones de gran tamaño, la evaluación deberá articularse mediante un enfoque combinado, que podrá incluir autoevaluaciones estructuradas para una primera clasificación, complementadas con entrevistas, pruebas de diagnóstico o verificaciones específicas para los perfiles y sistemas de mayor criticidad. El objetivo no es la exhaustividad formal, sino la identificación fiable de déficits de capacidad que introducen riesgo real.

IV. Finalmente, los resultados del diagnóstico deberán traducirse en una priorización formal de actuaciones, basada en criterios de riesgo, integrando tanto el riesgo intrínseco como el residual en dicha priorización. Los sistemas de IA de alto riesgo en producción y los perfiles cuya actuación es crítica para la supervisión humana, la seguridad, la continuidad del servicio o la respuesta ante incidentes deberán constituir la prioridad. Esta priorización deberá ser aprobada por el órgano de gobernanza correspondiente y utilizada como base vinculante del plan de implantación.

La no realización de esta fase, o su ejecución superficial, invalida la implantación del modelo, ya que impide demostrar que las decisiones de capacitación responden a riesgos reales y no a criterios genéricos o declarativos.

8.1.2. Fase 2: Diseño formal del sistema de capacitación y de los mecanismos de verificación

La Fase 2 tiene como finalidad transformar los resultados del diagnóstico en un sistema de control organizativo definido, exigible y verificable, evitando que las necesidades de capacitación identificadas se diluyan en iniciativas formativas genéricas o desconectadas del riesgo real.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA 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 esta fase, la capacitación deja de ser una intención y pasa a configurarse como un estándar interno de competencia, equivalente a cualquier otro control clave de seguridad, cumplimiento o continuidad de servicio.

I. En primer lugar, la organización deberá definir y aprobar formalmente los itinerarios de competencia exigibles por perfil, de conformidad con los perfiles organizativos descritos en el Capítulo 7 y con la priorización basada en riesgo resultante de la Fase 1. Cada itinerario deberá especificar, de manera explícita y documentada:
   - Las competencias mínimas que deben acreditarse para ejercer una función determinada en relación con uno o varios sistemas de IA;
   - El nivel de profundidad requerido en función del tipo de sistema, su clasificación de riesgo y su grado de autonomía;
   - Las condiciones bajo las cuales una persona puede considerarse autorizada para operar, supervisar, validar o intervenir sobre un sistema de IA;
   - Los supuestos que obligan a la renovación, ampliación o actualización de la competencia acreditada. Estos itinerarios no constituyen programas formativos en sentido pedagógico, sino criterios normativos internos que determinan si una persona puede o no desempeñar una función crítica sin introducir un riesgo inaceptable. La inexistencia de un itinerario formal para un perfil relevante deberá considerarse una laguna de control.

II. En segundo lugar, la organización deberá desarrollar, adaptar o adquirir los activos formativos necesarios para dar soporte a dichos itinerarios. Todo material formativo deberá ser específico para el contexto de la organización y para los sistemas de IA efectivamente utilizados, evitando contenidos genéricos que no aborden riesgos reales, dependencias técnicas concretas o procedimientos institucionales.
   Cada activo formativo deberá someterse a un proceso formal de validación técnica y normativa, dejando evidencia de:
   - Su adecuación a los riesgos identificados al aplicar la guía de metodología de gestión de riesgos documentada
   - Su coherencia con el modelo de gobierno de la IA y con los procedimientos operativos existentes
   - Su alineación con las obligaciones regulatorias aplicables y documentadas en la guía de clasificación en base al reglamento europeo y, complementado por la guía de roles y obligaciones según la clasificación

   Cuando la organización no disponga internamente de capacidad suficiente para validar contenidos asociados a sistemas de riesgo medio o alto, deberá preverse de forma explícita la validación externa independiente, como parte integrante del diseño del sistema y no como medida excepcional.

III. En tercer lugar, y de forma inseparable, la organización deberá diseñar y aprobar los mecanismos de verificación de competencia, que constituyen el elemento central que diferencia una capacitación formal de un control real. Estos mecanismos deberán:
   - Estar diferenciados por perfil y por nivel de 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

- Verificar capacidad efectiva de actuación, y no solo adquisición teórica de conocimiento
- Generar evidencia objetiva, comparable y auditable En funciones críticas, especialmente aquellas relacionadas con supervisión humana, operación de sistemas de alto riesgo, control de cambios o respuesta ante incidentes, la asistencia a una formación no constituye evidencia suficiente.

En estos casos, deberán establecerse verificaciones prácticas, simulacros, ejercicios de toma de decisiones, revisiones de desempeño o combinaciones de las anteriores, con criterios de evaluación definidos y documentados. Finalmente, durante esta fase deberán definirse los indicadores de seguimiento y eficacia del sistema de capacitación, en coherencia con el Capítulo 9. Estos indicadores deberán permitir evaluar no solo cobertura formal, sino también calidad de la competencia y reducción efectiva del riesgo humano.

8.1.3. Fase 3: Despliegue controlado, ejecución supervisada y generación de evidencia

La Fase 3 corresponde a la puesta en operación inicial del sistema de capacitación, con un enfoque explícito en la generación de evidencia y en la validación práctica del modelo diseñado. Esta fase no debe concebirse como un despliegue masivo indiscriminado, sino como una ejecución estrictamente alineada con la priorización basada en riesgo.

La capacitación deberá desplegarse comenzando por:

- Sistemas de IA clasificados como de alto riesgo y ya en producción
- Perfiles cuya actuación condiciona directamente la supervisión humana efectiva, la seguridad, la continuidad del servicio o la capacidad de respuesta ante incidentes
- Funciones donde una actuación incorrecta pueda generar impactos irreversibles o difícilmente mitigables La ejecución de la capacitación deberá realizarse bajo supervisión activa, verificando que los contenidos se imparten conforme a lo diseñado y que los mecanismos de verificación se aplican de forma consistente.

Cualquier desviación detectada durante esta fase deberá documentarse y corregirse antes de ampliar el despliegue. De manera paralela, deberá ponerse en funcionamiento el repositorio institucional de evidencias de capacitación, integrado en el sistema documental de la organización y sujeto a los mismos principios de integridad, trazabilidad y conservación que el resto de las evidencias de control. Cada acción formativa y cada verificación realizada deberá generar un registro que permita reconstruir, a posteriori:

- Qué persona estaba capacitada para qué función
- Respecto de qué sistema de IA y en qué versión
- En qué periodo temporal
- Con arreglo a qué criterios de validez Esta fase tiene también un objetivo explícito de aprendizaje organizativo.

La organización deberá analizar las dificultades prácticas, resistencias, sobrecargas o incoherencias detectadas, utilizándolas como entrada formal para el ajuste del modelo antes de su consolidación.

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

8.1.4. Fase 4: Integración plena en los sistemas de gestión y control permanente

La Fase 4 formaliza la transición del modelo desde un plan de implantación a un sistema de control organizativo permanente, integrado en los procesos ordinarios de la organización y no dependiente de iniciativas puntuales. A partir de este momento, las exigencias de competencia definidas deberán incorporarse de forma explícita en:

- Las descripciones de puestos de trabajo críticos
- Los procesos de selección y provisión de puestos
- Los planes de acogida y formación inicial
- La gestión de la rotación, sustituciones y externalizaciones

Asimismo, deberán activarse los ciclos regulares de revisión y auditoría, conforme a lo establecido en el Capítulo 9, evaluando no solo la existencia de capacitación, sino su eficacia real como control del riesgo humano.

La auditoría deberá poder contrastar comportamiento efectivo, no únicamente documentación formal. Los resultados de auditorías, incidentes reales, simulacros, cambios relevantes en los sistemas de IA o en el marco normativo deberán canalizarse a través de un proceso formal de mejora continua, con responsables, plazos y evidencias de cierre definidos.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA 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. Seguimiento, verificación y mejora continua del modelo de capacitación

En entornos de Smart Cities y Salud, donde los sistemas de IA se integran en servicios esenciales y operan sobre datos de alta sensibilidad, la capacitación solo constituye un control real si se mantiene actualizada, si se aplica de forma consistente y si produce resultados verificables en la operación diaria, especialmente cuando se enfrentan anomalías, incidentes o cambios del sistema. Por ello, la organización debe establecer un conjunto de mecanismos de seguimiento y mejora continua que permitan demostrar, de manera auditable, que las competencias requeridas por perfil se mantienen vigentes, que el personal clave sabe actuar ante escenarios de riesgo y que la capacitación se adapta a la evolución tecnológica, normativa y operativa.

Este capítulo se alinea con el enfoque de mejora continua de los sistemas de gestión, en particular con los principios de ISO 31000 e ISO/IEC 42001, y se coordina con los mecanismos de seguimiento y auditoría definidos en la guía "Modelo de Gobierno de la IA", evitando duplicidades: dicha guía determina qué se supervisa del sistema de IA y con qué órganos; esta guía concreta cómo se verifica que las personas están capacitadas para ejecutar ese control.

9.1. Seguimiento periódico de la capacitación como control organizativo

El seguimiento de la capacitación debe integrarse en los ciclos ordinarios de control interno de la organización. Esto implica que la capacitación se planifica, se ejecuta, se revisa y se corrige con una periodicidad definida y con responsables claros, del mismo modo que se revisan los controles técnicos, los procedimientos operativos o las medidas de seguridad de la información.

El seguimiento debe cubrir, como mínimo, tres dimensiones:

I. En primer lugar, la cobertura por **perfil y función.** La organización debe poder demostrar que las personas que desempeñan roles relevantes para la IA, tal como se definen en el Modelo de Gobierno, han recibido la capacitación exigible para su función y que dicha capacitación se mantiene vigente. Esto incluye situaciones habituales en el sector público que generan riesgos invisibles si no se controlan, como rotación de personal, cambios de puesto, incorporación de personal temporal, reorganizaciones internas o externalización parcial de funciones.

II. En segundo lugar, la **adecuación al riesgo**. El seguimiento debe verificar que la profundidad de la capacitación se corresponde con el riesgo del sistema y la criticidad del servicio. No es aceptable mantener el mismo nivel de capacitación cuando un sistema pasa de piloto a operación en un servicio esencial, cuando se integra en nuevos procesos o cuando se amplía su nivel de autonomía. En términos prácticos, esto exige que la capacitación se revise como parte del control de cambios y del ciclo de vida del sistema: si el sistema cambia materialmente, la capacitación exigible también puede cambiar.

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. En tercer lugar, la **eficacia operativa.** La organización debe comprobar que la capacitación produce comportamientos y decisiones coherentes con los procedimientos de supervisión humana, gestión de incidentes y control del riesgo. Esta dimensión es la que diferencia un programa de existencia documental de un programa con eficacia demostrable. Un personal que ha "asistido" a una formación, pero no sabe intervenir, registrar evidencia o escalar una anomalía sigue siendo un riesgo operativo.

9.2. Verificación y evidencia: trazabilidad de competencias y registros de control

Para que la capacitación sea auditable, debe generar evidencia verificable y conservarse con criterios de integridad y trazabilidad. La evidencia no debe limitarse a certificados genéricos, sino reflejar que la persona ha adquirido competencias aplicables a su función y que dichas competencias se actualizan cuando cambian los sistemas, los riesgos o los procedimientos.

La organización deberá establecer un repositorio de evidencias de capacitación, integrado en su esquema documental institucional, que permita demostrar al menos los siguientes elementos recomendados:

- **La identificación del perfil y rol al que aplica la capacitación**, garantizando coherencia con los roles del Modelo de Gobierno de la IA y con las líneas de defensa. La evidencia debe permitir reconstruir qué rol ejercía la persona en el periodo relevante, ya que en el sector público es frecuente que una misma persona desempeñe funciones distintas a lo largo del tiempo.

- El **contenido formativo impartido y su relación con riesgos concretos**. En ámbito de la IA, la formación ha de relacionarse a escenarios como la supervisión humana, el control de cambios, la gestión de incidentes, el uso conforme al propósito, la trazabilidad y la respuesta ante anomalías. Si la evidencia disponible no permite entender con claridad qué se enseñó, la organización pierde capacidad de defensa ante una auditoría.

- La **evaluación o verificación de competencia**, al menos para perfiles críticos. En entornos de alto riesgo, es insuficiente acreditar asistencia. La organización debe establecer mecanismos de verificación proporcionados, que pueden incluir pruebas de comprensión, ejercicios guiados, simulacros de decisión o validación por desempeño en procedimientos. La proporcionalidad es clave: no se trata de imponer cargas iguales a todos, sino de asegurar que los perfiles donde un error puede escalar a incidente grave tienen verificación de competencia acorde.

- La **vigencia temporal y reglas de actualización**. La evidencia debe incorporar la fecha, la vigencia y el criterio de renovación, especialmente cuando existan cambios relevantes en el sistema, en el marco normativo o en el perfil de amenazas. En sistemas de IA operativos, la capacitación debe considerarse parte del mantenimiento del control, no un hito histórico.

Financiado por la Unión Europea NextGenerationEU

9.3. Indicadores de desempeño y eficacia de la capacitación

La mejora continua requiere medición. Sin indicadores, la organización solo puede afirmar que "ha formado", pero no puede demostrar que controla el riesgo humano asociado a la IA.

Los indicadores deben seleccionarse con prudencia para no incentivar conductas indeseadas ni convertirse en burocracia vacía. Deben ser comprensibles por la Alta dirección, útiles para el CAIO, el CISO y el CRO, y trazables para auditoría. Sin convertir este apartado en un catálogo rígido, la organización debería incorporar indicadores en cuatro categorías:

- Indicadores de cobertura y vigencia, orientados a verificar que los perfiles críticos mantienen la capacitación requerida y que no existen "zonas sin control" por rotación, reorganización o externalización.

- Indicadores de capacidad de supervisión humana, que permitan medir si el personal funcional y operativo aplica los criterios de contraste, intervención y escalado cuando corresponde, y si lo hace de forma documentada. En la práctica, la tasa y calidad de los registros de intervención humana y de escalado ante anomalías suele ser un indicador más valioso que un examen teórico.

- Indicadores de gestión de incidentes y anomalías relacionados con IA, orientados a medir si la organización detecta antes, responde mejor y conserva evidencia suficiente cuando aparecen fallos, degradaciones o ataques. En IA, el tiempo de detección y la capacidad de distinguir drift de manipulación son críticos y dependen directamente de competencias.

- Indicadores de calidad de la documentación y trazabilidad, especialmente para equipos técnicos, de datos y MLOps, ya que la ausencia de evidencia convierte cualquier respuesta institucional en frágil. Un sistema con logs incompletos, versiones no controladas o cambios no registrados es un sistema que expone a la organización, aunque "funcione".

Los indicadores deben revisarse periódicamente para asegurar que siguen midiendo lo importante y que no generan incentivos perversos, y deben integrarse en los informes regulares establecidos en la gobernanza de IA sin duplicar circuitos.

9.4. Actualización por cambios del sistema y por evolución del riesgo

En IA, el riesgo es dinámico. La capacitación debe actualizarse cuando cambian los sistemas, los datos, los modelos, las integraciones o los procedimientos. También debe actualizarse cuando el entorno cambia: nuevas obligaciones regulatorias, nuevas amenazas, nuevos patrones de uso o nuevas evidencias derivadas de incidentes internos o del sector. La organización deberá definir disparadores claros que obliguen a revisar la capacitación exigible. Entre los más relevantes se incluyen:

- Cambios materiales del sistema, incluyendo reentrenamientos, modificaciones de arquitectura, incorporación de nuevas fuentes de datos, cambios de proveedor, integración con nuevos procesos o aumento del nivel de autonomía.

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

- Cambios del contexto operativo, como el paso de piloto a producción, la extensión a nuevas unidades, el uso en decisiones de mayor impacto o la operación en escenarios de mayor criticidad, por ejemplo, en salud asistencial directa o en servicios urbanos esenciales.

- Cambios en el perfil de amenaza o incidentes relevantes. Si la organización detecta un patrón de fallos por automatización acrítica, por ausencia de escalado o por malas prácticas de control de cambios, la capacitación debe adaptarse como medida correctora, no limitarse a "recordatorios".

- Cambios normativos o de política institucional que modifiquen obligaciones de transparencia, supervisión, registro o respuesta ante incidentes. Este enfoque evita una de las fallas estructurales más habituales: mantener un programa de capacitación congelado mientras los sistemas evolucionan, lo que genera una apariencia de control sin control real.

9.5. Auditoría interna y revisión de eficacia

La capacitación, en tanto que control organizativo, debe ser auditada. La auditoría no debe centrarse únicamente en comprobar que existe un plan o que hay registros, sino en evaluar si la capacitación reduce riesgo real y habilita la ejecución efectiva de los procedimientos de gobernanza.

La auditoría interna, coordinada con las funciones de control definidas en el Modelo de Gobierno de la IA, debería evaluar al menos:

- La coherencia entre roles y competencias exigidas, verificando que los perfiles definidos en la gobernanza tienen capacitación alineada y que no existen vacíos, duplicidades o contradicciones.

- La trazabilidad de la evidencia, comprobando que los registros permiten reconstruir qué competencias existían en un periodo concreto, quién estaba autorizado para operar o supervisar, y qué formación aplicaba al sistema en esa versión.

- La eficacia mediante pruebas y evidencias operativas, incluyendo revisión de registros de intervención humana, gestión de incidentes, escalados y decisiones de conmutación, así como ejercicios de verificación cuando sea proporcionado. En sistemas de alto riesgo, una auditoría que no contrasta comportamiento real deja un vacío de control.

- La gestión de proveedores y terceros, cuando intervienen en funciones críticas, verificando que las exigencias de competencia se han incorporado a la contratación y que existen mecanismos de supervisión, conforme al capítulo 7.

Los hallazgos deben traducirse en planes de acción con responsables, plazos y evidencias de cierre, integrándose en la mejora continua del modelo y elevándose al órgano correspondiente según la estructura de gobernanza ya establecida.

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

9.6. Cultura organizativa y gestión del cambio

La capacitación técnica y procedimental no produce control efectivo si el entorno cultural penaliza el reporte de anomalías o favorece una confianza ciega en la automatización. En organizaciones públicas, esto puede verse reforzado por presiones operativas, falta de tiempo, jerarquías rígidas o miedo a atribuciones de responsabilidad.

Por ello, la organización debe asegurar que el modelo de capacitación se despliega en un contexto que favorezca la supervisión humana efectiva. Esto requiere integrar, de forma proporcionada, elementos de cultura de seguridad y gestión del cambio: promover prácticas de reporte sin represalias, reforzar que cuestionar un resultado algorítmico forma parte del control institucional, y evitar que la implantación de sistemas de IA en el uso diario se convierta en automatización acrítica.

En salud, este punto es especialmente crítico porque la presión asistencial puede empujar a aceptar recomendaciones por velocidad, y porque la supervisión humana es un requisito de seguridad del paciente, no un formalismo.

En Smart Cities, es crítico porque los sistemas se perciben como “objetivos” y pueden normalizar decisiones que afectan de manera desigual a territorios o colectivos si no existe cultura de contraste, revisión y transparencia.

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. Referencias

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (AI Act). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689

- Reglamento (UE) 2016/679 (RGPD), de 27 de abril de 2016, relativo a la protección de datos personales. https://eur-lex.europa.eu/eli/reg/2016/679/oj

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

- Reglamento (UE) 2022/868 (Data Governance Act) sobre la gobernanza europea de datos. https://eur-lex.europa.eu/eli/reg/2022/868/oj

- Reglamento (UE) 2022/2065 (Digital Services Act – DSA) sobre servicios digitales. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

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

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

- Carta de Derechos Digitales (Gobierno de España, 2021). https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/Carta_Derechos_Digitales.pdf

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

- ISO/IEC 42001:2023 – AI Management System. https://www.iso.org/standard/81230.html

- ISO/IEC 23894:2023 – AI Risk Management. https://www.iso.org/standard/77304.html

- ISO/IEC 38507:2022 – Governance implications of AI. https://www.iso.org/standard/80382.html

- ISO/IEC 27001:2022 – Information security management systems.

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

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

- ISO 31000:2018 – Risk management guidelines.
  https://www.iso.org/standard/65694.html

- ISO/IEC 30111:2019 – Vulnerability handling processes.
  https://www.iso.org/standard/69725.html

- ISO/IEC 25012:2014 – Data quality model.
  https://www.iso.org/standard/35736.html

- ISO 37120 / 37122 / 37123 – Sustainable and smart cities indicators.
  https://www.iso.org/committee/656906.html

- UNE 178104:2017 – Interoperabilidad de plataformas de ciudad inteligente.
  https://www.aenor.com/norma-une-178104-2017-n0058578

- UNE 178108:2017 – Gestión inteligente de activos urbanos.
  https://www.aenor.com/norma-une-178108-2017-n0058579

- UNE 178301:2015 – Sistema de indicadores y métricas para ciudades inteligentes.
  https://www.aenor.com/norma-une-178301-2015-n0056687

- UNE 178503:2019 – Destinos turísticos inteligentes.
  https://www.aenor.com/norma-une-178503-2019-n0060196

- UNE-EN 301549:2022 – Accesibilidad de productos y servicios TIC.
  https://www.aenor.com/norma-une-en-301549-2022-n0062490

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 sistemática las siguientes materias:

- Marco conceptual y estratégico de la capacitación organizativa en ciberseguridad aplicada a la Inteligencia Artificial en administraciones públicas.
- Relación entre capacitación, gobierno de la IA y gestión del riesgo algorítmico en entornos de Smart Cities y Salud.
- Marco normativo aplicable, incluyendo Reglamento (UE) 2024/1689, RGPD, NIS2, ENS y estándares ISO e UNE relevantes.
- Definiciones operativas vinculadas a IA, ciberseguridad, trazabilidad, supervisión humana, control de cambios y gestión de incidentes.
- Principios rectores del modelo organizativo de capacitación basados en adecuación al riesgo, integración organizativa, continuidad y verificabilidad.
- Diseño del modelo estructural de capacitación como sistema organizativo permanente y gobernado.
- Identificación de perfiles organizativos críticos y determinación de competencias mínimas exigibles por rol.
- Integración de la capacitación en el ciclo de vida institucional de los sistemas de IA.
- Metodología de implantación por fases con criterios de validación formal y generación de evidencia auditable.
- Mecanismos de seguimiento periódico, verificación de competencias y mantenimiento de evidencias documentales.
- Indicadores de desempeño orientados a medir cobertura, eficacia operativa y reducción del riesgo humano.
- Actualización del modelo ante cambios tecnológicos, normativos, organizativos o del perfil de amenaza.
- Auditoría interna de la capacitación como control organizativo crítico.
- Integración de la cultura organizativa de supervisión humana efectiva y gestión responsable de la automatización.
- Gestión de competencias de proveedores y terceros que intervienen en sistemas de IA en servicios públicos críticos.
- Vinculación entre capacitación, continuidad de servicio, seguridad del paciente y resiliencia urbana.

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

11.2. 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 productos específicos en la guía.

RETECH
Redes Territoriales de Especialización Tecnológica

RED ARGOS

Capacitación organizativa en ciberseguridad aplicada a la IA administraciones públicas en entornos de Smart Cities y Salud

Diciembre 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