12

Guía 12. Registros y archivos de registro generados automáticamente

Reglamento Europeo de Inteligencia Artificial

Empresas desarrollando cumplimiento de requisitos

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

Esta guía ha sido desarrollada en el marco del desarrollo del piloto español de sandbox regulatorio de IA, en colaboración entre los participantes, asistencias técnicas, potenciales autoridades nacionales competentes y el grupo asesor de expertos del sandbox.

La guía tiene como objetivo servir de apoyo introductorio a la normativa europea de Inteligencia Artificial y sus obligaciones aplicables. Si bien **no tiene carácter vinculante ni sustituye ni desarrolla la normativa aplicable, proporciona recomendaciones prácticas** alineadas con los requisitos regulatorios a la espera de que se aprueben las normas armonizadas de aplicación para todos los estados miembros.

El presente documento está sujeto a un **proceso permanente de evaluación y revisión**, con actualizaciones periódicas conforme al desarrollo de los estándares y las distintas directrices publicadas desde la Comisión Europea, y será actualizada una vez se apruebe el Ómnibus digital que modifica el Reglamento de Inteligencia Artificial.

Entre las referencias técnicas relevantes actualmente en desarrollo y aplicables, destacan las normas **ISO 15489-1:2016 "Information and documentation – Records management – Part 1: Concepts and principles"**, **ISO 31000:2018 "Risk management – Guidelines"**, **ISO/IEC 23894 "Information technology – Artificial intelligence – Guidance on risk management"**, **ISO/IEC 42001 "Information technology – Artificial intelligence – Management system"**, **prEN 18229-1 "AI Trustworthiness Framework - Part 1: Logging, Transparency and Human Oversight"** y **prEN ISO/IEC 24970 "AI System Logging"**, que servirán de base para el establecimiento de un marco común de gestión, registro, transparencia y supervisión de los sistemas de inteligencia artificial, integrando los principios de gestión documental, gestión del riesgo y gobernanza en el contexto del cumplimiento del Reglamento Europeo de Inteligencia Artificial.

Fecha de versión: 10 de diciembre de 2025

Contenido general

Índice detallado

1. Preámbulo

1.1. Objetivo del documento

En esta guía se presentan las **medidas** que servirán a proveedores y responsables de despliegue de sistemas de IA a **dar cumplimiento** a los **requisitos** del **Reglamento Europeo de la IA** referentes a la **generación y conservación de registros**, que todo sistema de IA de alto riesgo (HRAIS por sus siglas en inglés) debe incorporar.

El desarrollo de un adecuado **sistema de gestión de registros** no solo permitirá cumplir con las exigencias del Reglamento Europeo de la IA, sino también **facilitará** otras tareas como la **transparencia** y **rendición de cuentas** o **actividades de investigación** y **desarrollo basadas en pruebas**. Estos beneficios y algunos otros se verán más en detalle en el apartado 5.

1.2. ¿Cómo leer esta guía?

La estructura de esta guía presenta un **primer apartado** con el preámbulo

Un **segundo apartado** introductorio donde se define qué es un registro y se mencionan sus características principales.

Un **tercer apartado** centrado en el Reglamento de IA y en los artículos en torno a los registros. También se incluye una tabla con cada uno de estos artículos y sus referencias dentro de los apartados de la presente guía para facilitar su localización.

En el **cuarto apartado** se profundiza sobre los registros, incluyendo una descripción de los tipos de éstos, los aspectos que debe contener cada uno de ellos y, las obligaciones de los actores implicados en la conservación de los registros.

En el **quinto apartado** se describen los procesos que se deberán abordar para el desarrollo de una adecuada y completa gestión de registros.

El **sexto apartado** contempla la documentación técnica relacionada con los sistemas de registros y, el **apartado séptimo** incluye la referencia al cuestionario para facilitar la autoevaluación de los sistemas de IA.

Por último, los **apartados octavo y noveno** incluyen respectivamente un glosario de términos y, las referencias a normas y estándares que se han consultado para la realización de la presente guía.

1.3. ¿A quién está dirigido?

Es responsabilidad de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo implementar las medidas adecuadas para asegurar las obligaciones de conservación y mantenimiento de registros que se mencionan en el Reglamento de IA.

1.4. Casos de uso y ejemplos dispuestos a lo largo de la guía

Con el fin de **facilitar** la **comprensión de la guía**, se incorporan en ésta **diferentes ejemplos** que pretenden servir como **referencia** para la adecuación de los HRAIS para la **generación de registros** conforme a los requisitos del reglamento.

Estos ejemplos se desarrollan en base a los **casos de uso** descritos en la **Guía práctica y ejemplos para entender el Reglamento de IA**

Finalmente, cabe destacar que siempre que se ponga un ejemplo, se hará de manera ilustrativa. Proveedor y responsable del despliegue han de considerar la aplicación de todas las medidas indicadas en esta guía, según corresponda. Cada sistema de IA, siguiendo las directrices de esta guía, deberá identificar y aplicar las medidas más adecuadas según las características de su sistema de IA y su finalidad específica. Además, los ejemplos expuestos son específicos de los casos de uso.

Esto implica que las propuestas son específicas para los modelos considerados como ejemplo, y no una solución general para otros tipos de modelo, o incluso modelos de la misma tipología. Cada organización deberá, acorde a esta guía, establecer las medidas oportunas para su tipo de sistema de IA y su finalidad prevista.

Los ejemplos seleccionados a abordar en la presente Guía son:

- **Sistema de IA de promoción y ascenso**
- **Sistema de IA de administración de insulina**
- **Sistema de IA de reconocimiento biométrico en la asistencia al trabajo**

2. Introducción

2.1. ¿Qué es un registro?

En un sistema de IA, un registro es un archivo que almacena información sobre el comportamiento y desempeño del sistema durante su entrenamiento o uso en producción. El registro puede incluir elementos como, por ejemplo, información acerca los datos de entrada del sistema, las predicciones que realiza el sistema y cualquier error o anomalía que se produzca durante su ejecución.

Los registros son herramientas muy importantes para el análisis y la mejora continua del sistema de IA. Permite a los desarrolladores y operadores del sistema entender cómo se comporta en diferentes situaciones y cómo se puede optimizar para mejorar su precisión y eficiencia. También puede ayudar a detectar errores o sesgos en el sistema y a tomar medidas para corregirlos.

Además, los registros son activos de información que pueden actuar como evidencias de eventos del sistema de IA, permiten hacer un seguimiento de la ejecución y el comportamiento del sistema y ayudan a asegurar que el sistema opere conforme a su finalidad prevista.

2.2. ¿Qué es un sistema de gestión de registros?

En el contexto de la IA, un sistema de gestión de registros es un conjunto de procesos que se definen para recopilar, almacenar, analizar y gestionar los registros generados por un sistema de IA. Es fundamental para monitorear el rendimiento del sistema, detectar problemas y mejorar la precisión del modelo de IA.

Adicionalmente, es importante que el sistema cumpla con los requisitos de seguridad y privacidad de los datos, ya que los registros pueden contener información sensible y confidencial.

En el apartado 5 se analizará en detalle los procesos que comprenden un sistema de gestión de registros, de forma resumida éstos son:

- **Evaluación** de la necesidad para la creación de los registros y su **diseño**.
- **Captura, almacenamiento y control de acceso** sobre los registros garantizando su seguridad.
- **Retención** y **eliminación** de los registros.
- **Seguimiento y mejora continua** del sistema.

2.3. ¿Qué principios deberemos garantizar en la gestión de registros?

En la gestión de registros de los sistemas de IA es importante tratar de garantizar una serie de principios que ayuden a generar unos registros funcionales, válidos y fiables:

- **Confidencialidad**: los registros deben proteger la privacidad y la confidencialidad de los datos registrados, evitando su divulgación o acceso no autorizado.
- **Integridad**: los registros deben ser precisos y completos, sin cambios no autorizados, para asegurar la fiabilidad de los datos registrados.
- **Disponibilidad:** los registros deben estar disponibles cuando se necesiten, para que se puedan analizar, auditar o revisar si es necesario.
- **Autenticidad**: los registros deben ser auténticos, es decir, deben ser registrados por el sistema de forma legítima y no manipulados por usuarios no autorizados.
- **Accesibilidad y trazabilidad**: los registros deben ser accesibles y estar disponibles para su revisión y análisis, y deben estar acompañados de información de trazabilidad, para que se pueda identificar la fuente y el origen de la información registrada.
- **Responsabilidad**: los registros deben ser responsabilidad del propietario del sistema de IA y deben ser tratados de forma adecuada y segura.
- **Retención y eliminación**: los registros deben ser retenidos durante un período de tiempo adecuado, y luego eliminados de manera segura para garantizar que no se violen las normativas de protección de datos personales.

2.4. ¿Qué beneficios tiene una adecuada gestión de registros?

Como ya se ha comentado, el desarrollo de esta guía está enfocado en **ayudar al lector a cumplir con los requisitos del Reglamento Europeo de IA**. En este sentido, además del propio cumplimiento con lo establecido en dicho Reglamento, se considera relevante destacar que **una adecuada gestión de registros** de nuestro sistema de IA puede **aportar un valor diferencial** en diferentes horizontes pudiendo ayudar **en elementos como:**

- La transparencia y rendición de cuentas.
- Los procesos de toma de decisiones.
- Continuidad de negocio en caso de desastre o pérdida de información.
- La protección de los derechos y obligaciones de las organizaciones y los individuos
- Protección y soporte en litigios.
- La protección de la propiedad intelectual.
- Actividades de investigación y desarrollo basadas en pruebas.

3. Reglamento de Inteligencia Artificial

La puesta en servicio o la utilización de sistemas de IA de alto riesgo debe supeditarse al cumplimiento de determinados requisitos obligatorios, entre los cuales está el de registros. Estos requisitos tienen como objetivo garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuyos resultados de salida se utilicen en la Unión no representen riesgos inaceptables para intereses públicos importantes reconocidos y protegidos por el Derecho de la Unión.

En este apartado se incluye los artículos referentes a la generación de registros del Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento Europeo de Inteligencia Artificial) y se detalla en qué secciones de esta guía se abordan los diferentes elementos de dichos artículos.

3.1. Análisis previo y relación de los artículos

Las obligaciones sobre la generación de registros se encuentran principalmente en dos artículos del Reglamento Europeo de IA, artículo 12 *"Conservación de registros"* y artículo 19 *"Archivos de registro generados automáticamente"*. Adicionalmente, se debe atender a las obligaciones de los responsables del despliegue dispuestas en la sección 3 del capítulo III *"Obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y otras partes interesadas"*, artículo 26 *"Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo"*.

Por la naturaleza y contenido de estos artículos, se tratarán, en el caso concreto de esta guía, de forma conjunta. En este sentido:

- **Artículo Registros**: Establece que los HRAIS deberán incorporar las capacidades técnicas necesarias para la generación automática de registros. Además, señala una serie de condiciones que dichos registros deben cumplir.
- **Artículo Archivos de registros generados automáticamente:** Indica que los proveedores de los HRAIS deberán conservar los archivos de registro (referidos en el artículo "Registros") generados automáticamente por el sistema, siempre y cuando dichos archivos estén bajo su control.
- **Artículo Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo:** En lo referente a la conservación de registros (apartado 6), Indica que los responsables del despliegue de los HRAIS deberán conservar los archivos de registro (referidos en el artículo "Conservación de registros") generados automáticamente por el sistema, siempre y cuando dichos archivos estén bajo su control.

3.2. Contenido de los artículos en el Reglamento de IA

AI Act

Art.12 – Conservación de registros

1. Los sistemas de IA de alto riesgo **permitirán técnicamente el registro automático de acontecimientos** (en lo sucesivo, «archivos de registro») a lo largo de **todo el ciclo de vida del sistema.**

2. Para garantizar un nivel de trazabilidad del **funcionamiento del sistema** de IA de alto riesgo que resulte adecuado para la finalidad prevista del sistema, las **capacidades de registro** permitirán que se registren **acontecimientos pertinentes** para:

a) la **detección de situaciones** que puedan dar lugar a que el sistema de IA de alto riesgo presente un **riesgo** en el sentido del **artículo 79, apartado 1**, o a una modificación sustancial;

b) la **facilitación** de la **vigilancia poscomercialización** a que se refiere el **artículo 72**, y

c) la **vigilancia del funcionamiento** de los sistemas de IA de alto riesgo a que se refiere el **artículo 26, apartado 5.**

3. En el caso de los **sistemas** de IA de alto riesgo mencionados en el **anexo III, punto 1, letra a)**, las capacidades de registro incluirán, **como mínimo**:

a) un **registro del período de cada uso** del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso);

b) la **base de datos de referencia** con la que el sistema ha cotejado los datos de entrada;

c) los **datos de entrada** con los que la búsqueda ha arrojado una correspondencia;

d) la **identificación** de las **personas físicas implicadas** en la **verificación** de los **resultados** que se mencionan en el **artículo 14, apartado 5.**

AI Act

Art.19 - Archivos de registro generados automáticamente

1. Los **proveedores** de sistemas de IA de alto riesgo **conservarán los archivos de registro** a que se refiere el artículo 12, apartado 1, que los sistemas de IA de alto riesgo **generen automáticamente** en la **medida en que dichos archivos estén bajo su control.** Sin perjuicio del Derecho aplicable de la Unión o nacional, los archivos de registro se conservarán durante un **período de tiempo adecuado** para la finalidad prevista del sistema de IA de alto riesgo, de **al menos seis meses,** salvo que el Derecho de la Unión o nacional aplicable, en particular el Derecho de la Unión en materia de protección de datos personales, disponga otra cosa.

2. Los proveedores que sean **entidades financieras** sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros **mantendrán los archivos de registro generados automáticamente** por sus sistemas de IA de alto riesgo **como parte de la documentación** conservada en virtud del Derecho pertinente en materia de servicios financieros.

AI Act

Art.26.6 - Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo

Los **responsables del despliegue** de sistemas de IA de alto riesgo **conservarán los archivos de registro** que los sistemas de IA de alto riesgo **generen automáticamente** en la **medida en que dichos archivos** estén **bajo su control**, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de **al menos seis meses**, salvo que se disponga otra cosa en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

Los responsables del despliegue que sean **entidades financieras** sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros **mantendrán los archivos de registro como parte de la documentación conservada** en virtud del Derecho de la Unión en materia de servicios financieros.

3.3. Correspondencia del articulado con los apartados de la guía

En la tabla dispuesta a continuación se detalla en qué secciones de esta guía se abordan los diferentes elementos del articulado:

Artículo Reglamento	Requerimiento Reglamento	Sección guía
12.1	Archivos de registro a lo largo de todo el ciclo de vida del sistema	Apartado 2, apartado 4.2 y apartado 5
12.2.a	Detección de HRAIS que presenten un riesgo a escala nacional	Apartado 5.1.1
12.2.b	Facilitación vigilancia poscomercialización	Apartado 5.1.2
12.2.c	Vigilancia funcionamiento HRAIS	Apartado 5.1.3
12.3.a	Registros del periodo de cada uso del sistema de alto riesgo del Anexo III	Apartado 4.3
12.3.b	Base de datos con la que se ha cotejado el sistema de alto riesgo del Anexo III	
12.3.c	Datos de entrada que han arrojado correspondencia (sistemas de alto riesgo del Anexo III)	
12.3.d	Personas físicas implicadas en la verificación de resultados (sistemas de alto riesgo del Anexo III)	
19.1	Conservación de registros proveedores	Apartado 3.1 y apartado 4.1
19.2	Conservación de registros proveedores (entidades financieras)	
26.6	Conservación de registros responsables del despliegue	

4. Registros: actores y contenido

4.1. Agentes responsables de los registros

Las obligaciones asociadas a los sistemas de IA de alto riesgo en relación con la conservación de los registros, a los que se refiere el artículo 12, recaen tanto sobre el proveedor como sobre el responsable del despliegue del sistema de alto riesgo.

- Si soy el **proveedor** o el **responsable del despliegue** del sistema de IA de alto riesgo:
  a) Deberé encargarme de la **conservación** de los registros que genere mi sistema (ver apartado 5.3) siempre y cuando estos registros estén bajo mi control.
  b) Los deberé conservar durante un **periodo** de al menos **seis meses** salvo que se disponga lo contrario en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.
  c) Si soy una **entidad financiera** deberé mantener los registros como **parte** de la **documentación** conservada en virtud de la legislación pertinente en materia de servicios financieros.

En el apartado 3.2 se citan los artículos del Reglamento que especifican las obligaciones del proveedor y responsables del despliegue en relación con los requisitos en materia de registros.

4.2. ¿Qué información puede contener generalmente un registro?

Los registros deben representar la **información** que se haya identificado como **necesaria** tras el **proceso de evaluación** (ver apartado 5.1). Para dar una idea más detallada de la información que generalmente puede contener un registro de un sistema de IA, se adjunta a continuación los atributos más frecuentes:

a) Un identificador único del registro.
b) La identidad del usuario o el sistema que registró el evento.
c) Una descripción del contenido del registro.
d) La estructura del registro (por ejemplo, su forma y formato).
e) El contexto y finalidad en el que se crea, se recibe y se utiliza el registro.
f) Las acciones y eventos a lo largo de la existencia del registro.
g) Fecha y hora de cada acción realizada en el sistema.
h) Identificación del modelo o algoritmo de IA utilizado, incluyendo la versión y los parámetros de configuración utilizados.
i) Identificación de los datos de entrada utilizados por el sistema de IA.
j) Fuente de los datos de entrada utilizados por el sistema de IA.
k) El tipo de datos de entrada utilizados por el sistema de IA.

l) Resultados producidos por el sistema de IA, incluyendo la salida del modelo o algoritmo y cualquier información adicional generada por el sistema.
m) Métricas de calidad de los resultados (por ejemplo, la precisión).
n) Información de monitoreo de rendimiento y capacidad, como el uso de recursos (CPU, memoria, almacenamiento), el tiempo de respuesta y la tasa de errores.
o) Información de seguridad y privacidad, como la autenticación y autorización de usuarios, el cifrado de datos y la detección de intentos de acceso no autorizados.
p) Alertas o notificaciones generadas por el sistema, como advertencias de errores en los datos de entrada o fallas en el sistema.
q) Relaciones con otros registros.
r) Información que consideremos necesaria para cumplir la función de evidencia para la que se ha diseñado el registro (ver apartado 5.1).
s) Otra información necesaria para recuperar y presentar el registro (por ejemplo, la información de almacenamiento).

Ejemplo - Sistema de IA de promoción y ascenso

Tomando como ejemplo el **sistema de IA de promoción y ascenso** de los empleados, un ejemplo de un registro que se podría generar (en el apartado 5.1 se analiza en detalle cuando y porque interesará generar un registro) es aquel que recogiera la siguiente información:

- Fecha y hora de cada acción realizada en el sistema, como el envío de solicitudes de promoción o la revisión de perfiles de candidatos.
- Identificación del usuario o usuarios que realizaron cada acción, ya que esto permitiría una trazabilidad completa de las acciones en el sistema y una detección temprana de cualquier conducta discriminatoria.
- Perfil de los candidatos evaluados para cada puesto, incluyendo información relevante como la educación, experiencia laboral y habilidades requeridas para el puesto.
- Resultados de cada evaluación de candidatos, incluyendo puntuaciones, comentarios y notas realizadas por los evaluadores.
- Cualquier acción tomada en respuesta a las evaluaciones, como decisiones de contratación o promoción, y la justificación de dichas decisiones.
- Alertas o notificaciones generadas por el sistema en caso de detección de patrones discriminatorios, como la promoción frecuente de candidatos de un determinado género o etnia.

Ejemplo – Sistema de IA de administración de insulina

Tomando como ejemplo el **sistema de IA de administración de insulina**, un ejemplo de un registro que se podría generar (en el apartado 5.1 se analiza en detalle cuando y porque nos interesará generar un registro) es aquel que recogiera la siguiente información:

- Fecha y hora de cada administración de insulina.
- Tipo y cantidad de insulina administrada.
- Nivel de glucosa en sangre antes de la administración.
- Nivel de glucosa en sangre después de la administración.

- Alertas o notificaciones generadas por el sistema en caso de detección de patrones anormales o peligrosos, como niveles de glucosa demasiado bajos o altos, o administraciones frecuentes de insulina en un corto período de tiempo.
- Interacciones con otros medicamentos o tratamientos médicos del paciente.
- Cualquier otro evento relevante registrado por el sistema, como cambios en la dosis de insulina prescrita por el médico o cambios en la dieta del paciente.

4.3. ¿Qué información debe contener un registro de un sistema de identificación biométrica remota?

Un sistema de identificación biométrica remota es, según el Reglamento, *"un sistema de IA destinado a identificar a personas físicas generalmente a distancia, **sin su participación activa**, comparando sus datos biométricos con los que figuran en un repositorio de datos de referencia"*.

En este sentido, además de los elementos comunes de los registros de un sistema de IA, si el sistema es de identificación biométrica remota (sistemas de IA que figuran en el punto 1, letra a), del anexo III) deberá incorporar algunos elementos específicos, los cuales se indican en el apartado 3 del artículo:

AI Act

Art.12.3 - Registros

En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las capacidades de registro incluirán, como mínimo:

a) un registro del período de cada uso del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso);

b) la base de datos de referencia con la que el sistema ha cotejado los datos de entrada;

c) los datos de entrada con los que la búsqueda ha arrojado una correspondencia;

d) la identificación de las personas físicas implicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5 (el cual indica lo siguiente: En el caso de los sistemas de IA mencionados en **el anexo III, punto 1, letra a),** las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación. El requisito de la verificación separada por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando el

Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.)

En este contexto, lo que se deberá hacer si se ha desarrollado un sistema biométrico, es asegurarse de recabar en los registros esta información adicional.

A continuación, se dispone un ejemplo para un caso de uso de un sistema de IA de reconocimiento biométrico en la asistencia al trabajo:

Ejemplo – Sistema de IA de reconocimiento biométrico en la asistencia al trabajo

Tomando como ejemplo el **sistema de IA de reconocimiento biométrico en la asistencia al trabajo,** un ejemplo de un registro que se podría generar (en el apartado 5.1 se analiza en detalle cuando y porque nos interesará generar un registro) es aquel que recogiera la siguiente información:

- Fecha y hora de cada identificación realizada por el sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso).
- La base de datos de referencia con la que el sistema ha cotejado los datos de entrada.
- Una imagen de la cara que fue analizada (los datos de entrada con los que la búsqueda ha arrojado una correspondencia).
- La identificación de las dos o más personas físicas implicadas en la verificación de los resultados.
- Resultados de la identificación, incluyendo la persona identificada, si se realizó una coincidencia, el nivel de confianza de la identificación y cualquier error o anomalía detectada.
- Información sobre la cámara o dispositivo utilizado para capturar la imagen facial.
- Información sobre la ubicación y el contexto de la identificación, como el lugar donde se utilizó el sistema y la finalidad de la identificación (controlar el tiempo trabajado).
- Cualquier cambio en el sistema, como actualizaciones de software o hardware, que puedan afectar el comportamiento del sistema de IA.

La información recogida en estos tres ejemplos sobre los aspectos que debería contener un registro, se mencionará también en el capítulo 5, ya que se pretende ubicar este diseño de los registros en el proceso global de gestión y mantenimiento de registros.

5. ¿Qué elementos debo implantar y cómo debo hacerlo para desarrollar un adecuado sistema de gestión de registros?

En esta sección se describen los **procesos** que se deberán abordar para el **desarrollo** de una adecuada y completa **gestión de registros**, desde la evaluación de la necesidad para la creación de los registros hasta su disposición y eliminación:

5.1. Evaluación y diseño de los registros

¿Qué es?

La **evaluación** es el **proceso de análisis** mediante el cual **se determina** la **necesidad** de **generar registros** y los **requisitos** sobre estos registros. Esto ayudará a determinar qué **información** se debe **recabar** en los registros, estableciendo así qué registros debemos crear y capturar.

¿Cómo debo abordarlo?

En términos generales, esta primera fase consiste en analizar y determinar la necesidad de generar el registro, definir los objetivos específicos para la generación del registro y establecer su alcance. Además, en esta fase se diseñará el registro, mediante la identificación de los campos y categorías para la recopilación de información. Esta fase es crucial para establecer unos registros útiles y efectivos que cumplan con los objetivos del sistema de gestión de registros.

De este modo, podemos identificar los siguientes elementos dentro del proceso de evaluación y creación de los registros:

- **Identificación de la necesidad**: El primer paso es identificar la necesidad del registro. ¿Por qué se necesita el registro? ¿Cuáles son los objetivos del registro? Es importante definir claramente la necesidad para asegurar que el registro sea útil y relevante.
- **Identificación de los objetivos**: Una vez identificada la necesidad del registro, es necesario definir los objetivos específicos del registro. ¿Qué se espera lograr con el registro? ¿Cuáles son los resultados que se espera obtener? Es importante que los objetivos sean claros y específicos para que se pueda evaluar la efectividad del registro.
- **Definición del alcance**: El siguiente paso es definir el alcance del registro. ¿Qué tipo de información se registrará? ¿Cuánto tiempo se mantendrá el registro? Es importante establecer el alcance para evitar la recopilación de información innecesaria o irrelevante.
- **Diseño del registro**: Una vez definidos los objetivos y el alcance del registro, es necesario diseñar el registro. Esto implica definir los campos y categorías que se utilizarán para registrar la información, así como las herramientas y software que se utilizarán para capturar, almacenar y acceder a la información.
- **Identificación de los responsables**: Finalmente, es importante identificar a los responsables del registro. ¿Quién será el encargado de recopilar y mantener la información? ¿Quién será responsable de garantizar la precisión y la integridad del registro? Es importante definir claramente los roles y responsabilidades para garantizar la efectividad del registro.

Cada organización deberá determinar cuáles son sus necesidades para la generación de registros. No obstante, en el contexto del Reglamento Europeo de la IA, hay una serie de capacidades que los registros deben aportar al sistema de IA. En concreto, el texto del Reglamento expone lo siguiente:

AI Act

Art.12.2 - Registros

Para garantizar un nivel de **trazabilidad** del funcionamiento del sistema de IA de alto riesgo que resulte adecuado para la **finalidad prevista del sistema**, las **capacidades de registro** permitirán que se registren **acontecimientos pertinentes** para:

a) la **detección de situaciones** que puedan dar lugar a que el sistema de IA de alto riesgo presente un **riesgo** en el sentido del **artículo 79, apartado 1**, o a una modificación sustancial;

b) la **facilitación** de la **vigilancia poscomercialización** a que se refiere el **artículo 72**, y

c) la **vigilancia** del **funcionamiento** de los sistemas de IA de alto riesgo a que se refiere el **artículo 26, apartado 5.**

En este sentido, el proceso de evaluación consistirá en analizar estos tres elementos y determinar qué registros deben crearse y capturarse. A continuación, se entra más en detalle en cada uno de estos tres focos.

5.1.1. Situaciones de riesgo

Antes de poder abordar este punto se deberán **haber implementado** las **medidas** detalladas en la **guía** que describe el sistema de **gestión de riesgos** (consultar guía asociada al artículo del sistema de gestión de riesgos).

Una vez abordada la guía del sistema de gestión de riesgos, se dispondrá de un **inventario** con las **medidas de tratamiento** de los riesgos identificados y analizados. Como se detalla en dicha guía, el foco principal es la gestión de aquellos riesgos que puedan afectar a la **salud, seguridad o derechos fundamentales de las personas.**

El siguiente paso será **analizar y decidir para cada una de estas medidas** si se considera **necesario o no evidenciar** un determinado suceso, y consecuentemente **generar un registro con los requisitos y contenidos que se establezca.** Esta decisión y en su caso la especificación de los sucesos y registros asociados deberá incorporarse como proceda documentalmente como parte de las medidas de tratamiento de los riesgos asociados.

A continuación, se dispone un ejemplo detallado para el desarrollo de los diferentes elementos que componen la **fase de evaluación y diseño de los registros** en el contexto de la detección de situaciones que puedan dar lugar a que el sistema de IA presente un riesgo para la **salud, seguridad o derechos fundamentales de las personas.**

Ejemplo – Sistema de IA de reconocimiento biométrico en la asistencia al trabajo

En el ejemplo del **sistema de IA de reconocimiento biométrico en la asistencia al trabajo**, las fases para la evaluación de la necesidad y diseño del registro enfocado en **garantizar un proceso no discriminatorio** con el fin de **mitigar riesgos** relacionados con una posible violación del **derecho fundamental a la no discriminación** se centrarían en lo siguiente:

- **Identificación de la necesidad**: En esta fase, se identificaría la necesidad de contar con unos registros que permitan garantizar un proceso no discriminatorio en el sistema de IA de reconocimiento biométrico utilizado en la asistencia al trabajo. Esta necesidad se basaría en la preocupación por garantizar la igualdad de oportunidades y evitar la discriminación por cualquier motivo, como la raza, género, orientación sexual, religión, etc.
- **Identificación de los objetivos**: En esta fase, se definirían los objetivos específicos del registro para el sistema de IA de reconocimiento biométrico. Por ejemplo, se podrían establecer objetivos como: garantizar que el sistema no discrimine por motivos de raza, género u otros factores, asegurar que la precisión del sistema sea equitativa para todos los empleados, etc.
- **Definición del alcance**: En esta fase, se establecería el alcance del registro. En el caso de un Sistema de IA de reconocimiento biométrico en la asistencia al trabajo, se definirían los aspectos técnicos del sistema, como los algoritmos de reconocimiento biométrico utilizados, la forma en que se capturan y procesan las características biométricas de los empleados, etc.

- **Diseño del registro**: En esta fase, se diseñaría el registro para el Sistema de IA de reconocimiento biométrico en la asistencia al trabajo. Se definirían los campos y categorías para la recopilación de información, la forma en que se almacenaría la información, y las herramientas y software que se utilizarían para capturar, almacenar y acceder a la información. Algunos ejemplos de datos que podrían recabarse serían:
    - Fecha y hora de cada identificación realizada por el sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso).
    - La base de datos de referencia con la que el sistema ha cotejado los datos de entrada.
    - Una imagen de la cara que fue analizada (los datos de entrada con los que la búsqueda ha arrojado una correspondencia).
    - La identificación de las dos o más personas físicas implicadas en la verificación de los resultados.
    - Resultados de la identificación, incluyendo la persona identificada, si se realizó una coincidencia, el nivel de confianza de la identificación y cualquier error o anomalía detectada.
    - Información sobre la cámara o dispositivo utilizado para capturar la imagen facial.
    - Información sobre la ubicación y el contexto de la identificación, como el lugar donde se utilizó el sistema y la finalidad de la identificación (controlar el tiempo trabajado).
    - Cualquier cambio en el sistema, como actualizaciones de software o hardware, que puedan afectar el comportamiento del sistema de IA.
- **Identificación de los responsables**: Finalmente, se identificarían a los responsables de la gestión del registro. En este caso, se podría asignar la responsabilidad de recopilar y mantener la información a un equipo específico encargado de la gestión de los registros, y la responsabilidad de garantizar la precisión y la integridad del registro a los desarrolladores del Sistema de IA de reconocimiento biométrico.

Todo ello con el objetivo de garantizar la no violación del derecho fundamental a la no discriminación y evitar, por tanto, la discriminación en el proceso de asistencia al trabajo mediante el uso del Sistema de IA de reconocimiento biométrico.

5.1.2. Vigilancia poscomercialización

Del mismo modo que se indicaba en la sección anterior, antes de poder abordar este punto se deberán **haber implementado** las **medidas** detalladas en la **guía** que describe el sistema de **vigilancia poscomercialización** (consultar guía asociada al artículo del sistema de vigilancia poscomercialización).

Una vez abordada la guía que describe el sistema de vigilancia poscomercialización, se atiende a lo detallado en el apartado 2 del artículo 72:

AI Act

Art.72.2 - Vigilancia poscomercialización por parte de los proveedores y plan de vigilancia poscomercialización para sistemas de IA de alto riesgo

El sistema de vigilancia poscomercialización **recopilará, documentará y analizará de manera activa y sistemática los datos pertinentes** que pueden facilitar los responsables del despliegue o que pueden recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y que permiten al proveedor evaluar el cumplimiento permanente de los requisitos establecidos en el capítulo III, sección 2, por parte de los sistemas de IA. Cuando proceda, la vigilancia poscomercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue que sean autoridades garantes del cumplimiento del Derecho.

En este contexto, el primer paso que se deberá llevar a cabo es determinar qué información y qué datos del sistema de IA se necesitarán recabar tras su comercialización. Esto se habrá abordado al implementar las medidas establecidas en la guía que describe el sistema de **vigilancia poscomercialización**. Una vez definida esta información, se deberá diseñar los registros necesarios para recoger dicha información.

A continuación, se dispone un ejemplo detallado para el desarrollo de los diferentes elementos que componen la **fase de evaluación y diseño de los registros** en el contexto de la **recopilación de datos** para facilitar la **vigilancia poscomercialización**. Siempre poniendo especial atención a la detección de situaciones que puedan dar lugar a que el sistema de IA presente un riesgo para la **salud, seguridad o derechos fundamentales de las personas.**

Ejemplo – Sistema de IA de promoción y ascenso

En el ejemplo del **sistema de IA utilizado para la evaluación y promoción de empleados**, las fases para la evaluación de la necesidad y diseño del registro enfocado en **garantizar un proceso no discriminatorio** con el fin de **mitigar riesgos** relacionados con una posible violación del **derecho fundamental a la no discriminación** se centrarían en lo siguiente:

- **Identificación de la necesidad**: En esta fase, se identificaría la necesidad de contar con un registro que permita garantizar que el sistema de IA utilizado para la evaluación y promoción de empleados no discrimine a ningún empleado en base a características personales, como edad, género, origen étnico, orientación

sexual, religión, entre otras. Esta necesidad se basaría en la preocupación por garantizar un proceso justo y no discriminatorio, que valore las competencias y habilidades de los empleados de manera objetiva.

- **Identificación de los objetivos:** En esta fase, se definirían los objetivos específicos del registro para el sistema de IA utilizado para la evaluación y promoción de empleados. Por ejemplo, se podrían establecer objetivos como: detectar posibles sesgos en el sistema de IA, garantizar que las decisiones de evaluación y promoción estén basadas únicamente en criterios objetivos y relevantes para el puesto, monitorizar el uso del sistema de IA por parte del equipo de recursos humanos, entre otros.
- **Definición del alcance**: En esta fase, se establecería el alcance del registro. En el caso de un sistema de IA utilizado para la evaluación y promoción de empleados, se definirían los aspectos técnicos del sistema, como los criterios de evaluación, las métricas utilizadas para medir el desempeño de los empleados, los parámetros de ajuste del modelo de IA, entre otros.
- **Diseño del registro**: En esta fase, se diseñaría el registro para el sistema de IA utilizado para la evaluación y promoción de empleados. Se definirían los campos y categorías para la recopilación de información, la forma en que se almacenaría la información, y las herramientas y software que se utilizarían para capturar, almacenar y acceder a la información. Algunos ejemplos de datos que podrían recabarse serían:
    - Fecha y hora de cada acción realizada en el sistema, como el envío de solicitudes de promoción o la revisión de perfiles de candidatos
    - Identificación del usuario o usuarios que realizaron cada acción, ya que esto permitiría una trazabilidad completa de las acciones en el sistema y una detección temprana de cualquier conducta discriminatoria
    - Perfil de los candidatos evaluados para cada puesto, incluyendo información relevante como la educación, experiencia laboral y habilidades requeridas para el puesto
    - Resultados de cada evaluación de candidatos, incluyendo puntuaciones, comentarios y notas realizadas por los evaluadores.
    - Cualquier acción tomada en respuesta a las evaluaciones, como decisiones de contratación o promoción, y la justificación de dichas decisiones.
    - Alertas o notificaciones generadas por el sistema en caso de detección de patrones discriminatorios, como la promoción frecuente de candidatos de un determinado género o etnia.
- **Identificación de los responsables**: Finalmente, se identificarían a los responsables de la gestión del registro. En este caso, se podría asignar la responsabilidad de recopilar y mantener la información a un equipo específico encargado de la gestión de los registros, y la responsabilidad de garantizar que el sistema de IA utilizado para la evaluación y promoción de empleados sea justo y no discriminatorio a los desarrolladores del sistema.

Todo ello con el objetivo de garantizar que el sistema de IA utilizado para la evaluación y promoción de empleados sea justo y no discrimine a ningún empleado en base a características personales.

5.1.3. Vigilancia humana

Del mismo modo que se indicaba en las secciones anteriores, antes de poder abordar este punto se deberá **haber implementado** las **medidas** detalladas en la **guía** que describe el sistema de **vigilancia humana** (consultar guía asociada al artículo del sistema de vigilancia humana).

Una vez implementadas estas medidas, se habrá identificado la información que se considera necesaria para que el sistema de IA nos provea para cumplir con las necesidades de vigilancia humana. Más concretamente el apartado 5 del artículo *"Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo"* hace referencia a la necesidad de **identificar incidentes graves en el sistema de IA** durante su uso para poder **informar al proveedor e interrumpir su funcionamiento.**

En este contexto, una vez implementadas las medidas establecidas en la guía de vigilancia humana, se deberá prestar especial atención a la información que el sistema de IA deberá facilitarnos. Con ello, de igual modo que se ha hecho en las secciones anteriores, se deberán diseñar los registros necesarios para recoger dicha información.

A continuación, se dispone un ejemplo detallado para el desarrollo de los diferentes elementos que componen la **fase de evaluación y diseño de los registros** en el contexto de la **identificación de incidentes graves en el sistema de IA** durante su uso. Para con ello, **informar al proveedor e interrumpir su funcionamiento**. Siempre poniendo especial atención a la detección de situaciones que puedan dar lugar a que el sistema de IA presente un riesgo para la **salud, seguridad o derechos fundamentales de las personas.**

Ejemplo - Sistema de IA de administración de insulina

En el ejemplo del **sistema de IA de administración inteligente de insulina** para pacientes diabéticos, las fases para la evaluación de la necesidad y diseño del registro donde la finalidad es **detectar cualquier elemento que pudiera poner en riesgo la vida del paciente**, se centrarían en lo siguiente:

- **Identificación de la necesidad**: En esta fase, se identificaría la necesidad de contar con un registro que permita detectar cualquier elemento que pudiera poner en riesgo la vida del paciente diabético en el uso del sistema de administración inteligente de insulina. Esta necesidad se basaría en la preocupación por garantizar la seguridad y evitar posibles complicaciones graves en la salud del paciente, como una hipoglucemia o una hiperglucemia.
- **Identificación de los objetivos**: En esta fase, se definirían los objetivos específicos del registro para el sistema de IA de administración inteligente de insulina. Por ejemplo, se podrían establecer objetivos como: detectar cualquier cambio significativo en los niveles de glucosa del paciente, prevenir posibles episodios de hipoglucemia o hiperglucemia, monitorizar la actividad física del paciente, etc.
- **Definición del alcance**: En esta fase, se establecería el alcance del registro. En el caso de un sistema de administración inteligente de insulina para pacientes diabéticos, se definirían los aspectos técnicos del sistema, como la forma en que se mide y administra la insulina, la forma en que se capturan y procesan los niveles de glucosa del paciente, etc.

- **Diseño del registro**: En esta fase, se diseñaría el registro para el sistema de IA de administración inteligente de insulina. Se definirían los campos y categorías para la recopilación de información, la forma en que se almacenaría la información, y las herramientas y software que se utilizarían para capturar, almacenar y acceder a la información. Algunos ejemplos de datos que podrían recabarse serían:
    - Fecha y hora de cada administración de insulina
    - Tipo y cantidad de insulina administrada
    - Nivel de glucosa en sangre antes de la administración
    - Nivel de glucosa en sangre después de la administración
    - Alertas o notificaciones generadas por el sistema en caso de detección de patrones anormales o peligrosos, como niveles de glucosa demasiado bajos o altos, o administraciones frecuentes de insulina en un corto período de tiempo
    - Interacciones con otros medicamentos o tratamientos médicos del paciente
    - Cualquier otro evento relevante registrado por el sistema, como cambios en la dosis de insulina prescrita por el médico o cambios en la dieta del paciente
- **Identificación de los responsables**: Finalmente, se identificarían a los responsables de la gestión del registro. En este caso, se podría asignar la responsabilidad de recopilar y mantener la información a un equipo específico encargado de la gestión de los registros, y la responsabilidad de garantizar la precisión y la integridad del registro a los desarrolladores del sistema de IA de administración inteligente de insulina.

Todo ello con el objetivo de garantizar la seguridad y evitar posibles complicaciones graves en la salud del paciente diabético mediante el uso del sistema de IA de administración inteligente de insulina.

Finalmente, todo este proceso de evaluación y diseño de los registros deberá abordarse de forma recurrente, con la periodicidad que consideremos oportuna, en función de la frecuencia de actualización o variación de los elementos mencionados. Por ejemplo, si hay un cambio en el contexto del sistema de IA, esto afectará al análisis de riesgos (ver guía correspondiente al artículo del sistema de gestión de riesgos) y, por consiguiente, se deberá reevaluar si hay nuevos requisitos para los registros.

5.2. Captura, almacenamiento y control de acceso

¿Qué es?

Es el proceso consistente en **capturar**, **almacenar** y **conservar** los **registros definidos** en la fase precedente **garantizando su protección** frente a accesos no autorizados, modificaciones indeseadas, pérdidas o destrucción.

¿Cómo debo abordarlo?

Lo que se debe hacer en esta fase es guardar los registros de forma que se pueda garantizar su protección frente a accesos no autorizados, modificaciones indeseadas, pérdidas o destrucción. Para lograr este objetivo, deberemos:

a) Recabar la información en los registros según los criterios establecidos en la fase de diseño (esto dependerá de la naturaleza del sistema, donde esté implementado, el lenguaje de programación, etc.).
b) Seleccionar los medios de almacenamiento y materiales de protección adecuados (por ejemplo, en lugar de almacenar toda la información de los registros en un único servidor, disponer de servidores redundantes).
c) Implementar las medidas de ciberseguridad y control de acceso adecuadas para garantizar la seguridad de los registros (consultar guía de ciberseguridad).
d) Desarrollar y definir roles y responsabilidades sobre la gestión de los registros.
e) Garantizar la adecuada formación y capacitación del personal involucrado en la gestión de los registros (por ejemplo, definiendo cursos obligatorios para dicho personal, pues deben conocer los medios de almacenamiento seleccionados, las medidas de ciberseguridad que les apliquen y las medidas de control de acceso).
f) Considerar otras normativas o leyes aplicables como la normativa de protección de datos (GDPR).
g) Supervisar y revisar de forma recurrente los medios de almacenamiento y las medidas de ciberseguridad y control de acceso implementadas (por ejemplo, definiendo periodos de revisión y asignando un responsable de garantizar que estas revisiones se lleven a cabo).

Los registros deberán incluir la información de almacenamiento y control de acceso adecuada para garantizar la localización y monitorización de la seguridad de estos (por ejemplo, identificación de usuario que ha accedido, nivel de permiso que disponía, ubicación geográfica desde la cual se ha accedido y fecha y hora de acceso).

Adicionalmente, los sistemas de registros deben diseñarse para facilitar el uso de los registros mientras estos se conservan, es decir, no solo nos debe preocupar recabar y almacenar los registros sino también diseñar el sistema para que éstos sean accesibles y utilizables. Para ello, por ejemplo, se podrá crear copias en una ubicación alternativa para su acceso, de forma que no se ponga en riesgo la integridad y seguridad de los registros en su lugar de almacenamiento principal.

5.3. Retención y eliminación de los registros

¿Qué es?

Es el procedimiento mediante el cual se deberá establecer y recoger las necesidades de **conservación y destrucción** de los registros creados, capturados y almacenados.

¿Cómo debo abordarlo?

A la hora de establecer los procesos de retención y eliminación de los registros, se debe tener en consideración que éstos estarán determinados fundamentalmente por dos factores:

a) Por un lado, las necesidades de conservar los registros identificados en el proceso de evaluación, por ejemplo, en el escenario descrito en el apartado 5.1.1 se dispone de registros para garantizar un proceso no discriminatorio con el fin de mitigar riesgos relacionados con una posible violación del derecho fundamental a la no discriminación. Se deberá conservar este registro mientras sea necesario para garantizar dicho proceso, es posible que se necesite analizar en un momento dado algunas decisiones que haya podido tomar el sistema.
b) En segundo lugar, se deberá considerar los requisitos regulatorios o normativos aplicables, por ejemplo, la ley de protección de datos o GDPR si nuestros registros incluyen datos personales.

La destrucción de los registros es un proceso que debe siempre ser autorizado y documentado y debe llevarse a cabo cumpliendo las medidas de seguridad y acceso implementadas. Además, los registros involucrados en algún tipo de proceso legal no podrán ser destruidos hasta que se autorice su eliminación.

5.4. Seguimiento y mejora continua

Su finalidad es asegurar y mejorar la calidad y la eficacia del sistema de gestión de registros. Es imprescindible desarrollar un seguimiento y establecer unos periodos determinados de revisión y actualización del sistema de gestión de registros. Se pueden diferenciar las siguientes fases como parte de este proceso:

- **Monitorización e identificación de posibles errores**: El primer paso es identificar posibles errores que puedan estar afectando al sistema. Esto puede incluir errores en los datos registrados, problemas de rendimiento, problemas de seguridad, entre otros.
- **Análisis de los datos registrados:** Una vez identificados estos errores, es necesario analizar los datos registrados para determinar su causa. Esto puede implicar la revisión de los registros para encontrar patrones o correlaciones entre los datos.
- **Implementación de mejoras:** Una vez que se han identificado las causas de los errores, es necesario implementar mejoras en el sistema para corregirlos. Esto puede incluir la actualización del software, la mejora de los procedimientos de registro de datos o la capacitación del personal.
- **Evaluación de las mejoras:** Después de implementar las mejoras, es necesario evaluar su efectividad en la solución de los problemas identificados. Esto puede

implicar la comparación de los datos antes y después de las mejoras para determinar si se ha producido una mejora en el sistema.

- **Ciclo de mejora continua:** Finalmente, es importante establecer un ciclo de mejora continua para mantener el sistema actualizado y mejorar continuamente su rendimiento. Esto implica la repetición de los pasos anteriores para identificar nuevos posibles errores y mejorar el sistema de forma continua.

En definitiva, para la adecuada implementación del seguimiento y la mejora continua en un sistema de gestión de registros deberemos prestar especial atención a la identificación de posibles errores, analizar los datos registrados, implementar mejoras y evaluar su efectividad para mantener el sistema actualizado y mejorar su rendimiento continuamente.

5.5. ¿Quién debe responsabilizarse de la gestión de los registros?

Se deben establecer las responsabilidades y autorizaciones para la gestión de los registros, considerando todos los procesos de diseño, captura, almacenamiento, controles de acceso y retención y eliminación. Las responsabilidades deben asignarse a todo el personal involucrado en alguno de estos procesos y deberá reflejarse y documentarse en descripciones de puestos de trabajo y declaraciones similares, cuando corresponda. Además, las responsabilidades asignadas deberán quedar bien documentadas y reflejadas el documento desarrollado para recoger el proceso de gestión de los registros.

Ejemplo - Sistema de IA de promoción y ascenso

A continuación, se dispone un ejemplo de una posible distribución de responsabilidades en una organización:

a) Se asigna un responsable encargado de llevar a cabo los procesos de evaluación para identificar las necesidades de generación de registros (por ejemplo, puede ser el propio responsable del sistema de IA).
b) Se asigna un responsable encargado del diseño de los registros, en función de los requisitos del proceso de evaluación (por ejemplo, puede ser el mismo responsable que el encargado de la evaluación).
c) Se asigna un responsable encargado del proceso de captura de los registros (por ejemplo, podemos asignar esta tarea a un profesional independiente ajeno al desarrollo del sistema de IA o a su administración).
d) Se asigna un responsable encargado de garantizar el funcionamiento continuo y fiable de los sistemas de registros bajo su control y de garantizar que toda la documentación de los sistemas de gestión de registros esté completa y actualizada (por ejemplo, el administrador de sistemas).
e) Se asigna un responsable encargado de la gestión del almacenamiento de los registros (por ejemplo, este rol puede ser ostentado también por el administrador de sistemas).
f) Se asigna un responsable encargado de garantizar la seguridad de los registros mediante la implementación de las medidas de ciberseguridad y control de acceso (por ejemplo, este rol podría estar ostentado por un profesional de la oficina de seguridad de la información).
g) Se asigna un responsable encargado de garantizar la adecuada formación y capacitación del personal involucrado en la gestión de los registros (por ejemplo,

este rol lo podrían ostentar de forma compartida los profesionales de los dos puntos anteriores).

h) Se asigna un responsable encargado de los procesos de retención y eliminación de los registros (por ejemplo, el responsable de la evaluación podría encargarse de la definición de los periodos de retención y eliminación y el responsable de la captura de los registros podría encargarse de su ejecución).

i) Se asigna un responsable encargado de garantizar el correcto funcionamiento del sistema de gestión de registros, supervisando la adecuada ejecución de las tareas asignadas en los apartados anteriores (por ejemplo, un profesional de la gerencia de la organización).

5.6. Entidades sujetas a legislación sectorial

Aquellos proveedores de sistemas de IA que sean **entidades financieras** sujetas a requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la Unión en materia de servicios financieros **mantendrán los archivos de registro generados automáticamente** por sus sistemas de IA de alto riesgo **como parte de la documentación** conservada.

6. Documentación técnica

La obligación de mantener registros conforme a los artículos 12 y 19 del reglamento tiene un carácter transversal, ya que los mecanismos de registro deben integrarse en múltiples fases del ciclo de vida del sistema de IA: desde el desarrollo y las pruebas, hasta la operación y la vigilancia poscomercialización. En consecuencia, podría considerarse que cada apartado técnico del Anexo IV que documenta procesos, medidas o controles debería incorporar su propio subapartado de registro (por ejemplo, registrando actividades de diseño, gestión de riesgos o supervisión humana). No obstante, los únicos puntos del Anexo IV que se relacionan directamente y de forma explícita con la obligación de registros son los siguientes:

- 2(g) – Los procedimientos de validación y prueba utilizados, incluidos los archivos de registro de las pruebas y los informes de las pruebas fechados y firmados por las personas responsables.
- 9 – La descripción detallada del sistema establecido para evaluar el funcionamiento del sistema de IA en la fase posterior a la comercialización, incluido el plan de vigilancia poscomercialización.

Estos dos puntos, por sí solos, podrían considerarse suficientes para cubrir los requisitos documentales esenciales del reglamento en materia de registros, al abarcar tanto la generación y conservación de logs durante el desarrollo como su mantenimiento durante la fase operativa. Sin embargo, se considera una buena práctica ampliar la documentación incorporando y justificando además los siguientes aspectos complementarios:

a) El proceso de evaluación y diseño de los registros abordado, detallando los elementos analizados, la necesidad identificada, los objetivos, el alcance, los detalles del diseño y los responsables identificados.

b) El proceso de captura de registros desarrollado, identificando toda la información relevante del proceso.

c) El detalle de medios de almacenamiento donde se guardarán y conservarán los registros.

d) Las medidas de seguridad, ciberseguridad y control de acceso implementadas para garantizar la seguridad de los registros.

e) Los roles y responsabilidades definidos y establecidos sobre los procesos de gestión de registros, identificando la formación y capacitación de cada uno de los responsables en caso de ser necesario.

f) Los periodos establecidos de revisión y supervisión de los medios de almacenamiento y las medidas de ciberseguridad y control de acceso implementadas.

g) Las necesidades de conservación de los registros y los periodos de retención establecidos.

h) Las normas o regulaciones aplicables (por ejemplo, la ley de retención de datos o GDPR).

Esta documentación deberá ser difundida y conocida por todos los actores involucrados y se deberá revisar periódicamente para garantizar que quedan recogidas todas las actualizaciones o modificaciones que haya sufrido el proceso de gestión de los registros.

7. Cuestionario de autoevaluación

Para realizar una autoevaluación del cumplimiento de los requisitos del Reglamento de Inteligencia Artificial referidos en esta guía, se ha generado un cuestionario de autoevaluación global con una serie de preguntas con los puntos clave a tener en cuenta respecto a las obligaciones que dictaminan los artículos del Reglamento de IA mencionados en esta guía.

Será necesario referirse a ese documento para realizar el apartado del cuestionario de autoevaluación correspondiente a esta guía.

8. Anexos

8.1. Anexo A – Glosario de términos

Esta guía se ha desarrollado con un enfoque que trata de explicar cada concepto presente en la guía cuando se expone, no obstante, se han recogido ciertos términos específicos en esta sección como aclaración adicional:

1. **Acceso al registro:** derecho, oportunidad, medios para encontrar, utilizar o recuperar información.
2. **Agente:** individuo, grupo de trabajo u organización responsable o involucrado en los procesos de creación, captura y/o gestión de registros.
3. **Sistema de clasificación de empresas:** herramienta para vincular registros al contexto de su creación.
4. **Clasificación:** identificación sistemática y/o disposición de actividades y/o registros comerciales en categorías de acuerdo con convenciones, métodos y reglas de procedimiento lógicamente estructurados.
5. **Conversión:** proceso de cambio de registros de un formato a otro.
6. **Destrucción:** proceso de eliminación o eliminación de un registro, más allá de cualquier posible reconstrucción.
7. **Disposición:** gama de procesos asociados con la implementación de la retención de registros, destrucción o decisiones de transferencia documentadas en autoridades de disposición u otros instrumentos.
8. **Autoridad de disposición:** instrumento que define la disposición acciones autorizadas para registros especificados.
9. **Evidencia:** documentación de una transacción.
10. **Función:** grupo de actividades que cumplen con las principales responsabilidades para lograr los objetivos estratégicos de una entidad comercial.
11. **Migración:** proceso de mover registros de una configuración de hardware o software a otra sin cambiar el formato.
12. **Registro(s):** información creada, recibida y mantenida como evidencia y como un activo por una organización o persona, en cumplimiento de obligaciones legales o en la transacción de negocios.
13. **Gestión de registros:** campo de gestión responsable del control eficiente y sistemático de la creación, recepción, mantenimiento, uso y disposición de registros, incluidos los procesos de captura y mantenimiento evidencia de las actividades empresariales y la información sobre ellas y Transacciones en forma de registros.
14. **Sistema de registros:** sistema de información que captura, gestiona y proporciona acceso a registros a lo largo del tiempo.
15. **Transacción:** unidad más pequeña de un Proceso de trabajo consistente en un intercambio entre dos o más participantes o sistemas.
16. **Proceso de trabajo:** una o más secuencias de acciones necesarias para producir un resultado que cumpla con las reglas de gobierno.

9. Referencias, estándares y normas

Para el desarrollo de esta guía se han consultado y utilizado especialmente las normas y estándares siguientes. Algunos de estos estándares han sido ya publicados, mientras que otros se encuentran actualmente en desarrollo o revisión:

- ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles.
- ISO 31000:2018 - Risk management – Guidelines.
- ISO/IEC 23894 - Information technology – Artificial intelligence – Guidance on risk management.
- ISO/IEC 42001 Information technology – Artificial intelligence – Management system.
- prEN 18229-1 AI trustworthiness framework – Part 1: Logging, transparency and human oversight
- prEN ISO/IEC 24970 AI System Logging

Adicionalmente, se han consultado de forma accesoria otras normas y estándares como:

- ISO/IEC 27001:2022 - Information security, cybersecurity, and privacy protection – Information security management systems – Requirements.
- ISO/IEC 22989:2022 - Information technology – Artificial intelligence – Artificial intelligence concepts and terminology.
- ISO/IEC 23053:2022 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).
- ISO/IEC 5259-1 - Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples.
- ISO/IEC TR 24027:2021, Information technology – Artificial intelligence (AI) – Bias in AI systems and AI aided decision making.
- ISO/IEC AWI TS 12791 - Information technology – Artificial intelligence – Treatment of unwanted bias in classification and regression machine learning tasks.
- NIST - AI Risk Management Framework.

La presente guía toma como referencia el Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento Europeo de 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 DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de
Recuperación,
Transformación
y Resiliencia

España | digital 2026