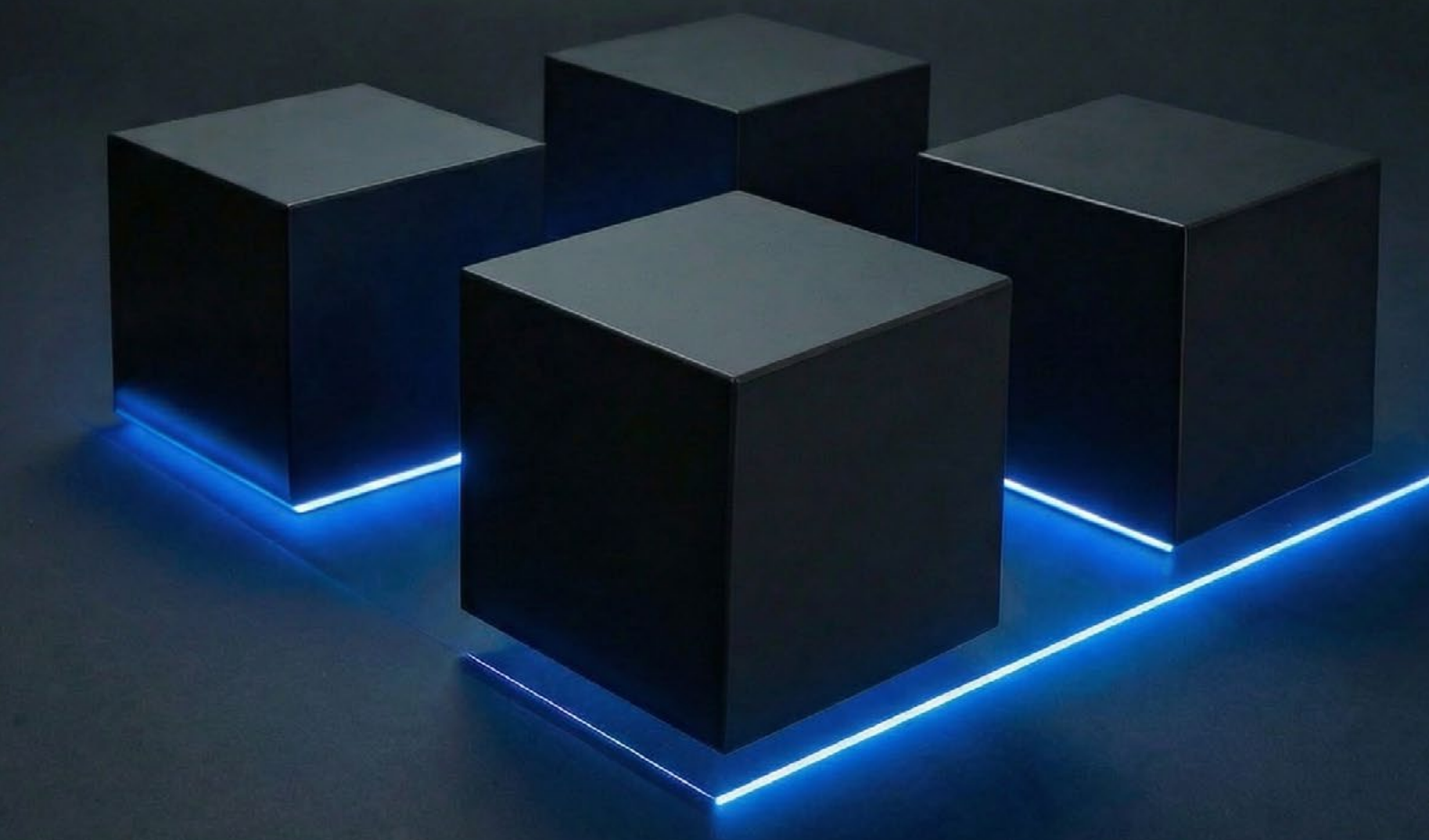
GIA | GRUPO DE INTELIGENCIA ARTIFICIAL

isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

INVENTARIO DE SISTEMAS Y SERVICIOS DE IA



AUTORES

COORDINADORES

David Moreno
Enrique Cervantes

COAUTORES

Antonio Antúnez
Antonio Béjar
Anxo Martínez
Carlos Casal
Daniel Panadero
Diana Aleo
Esther García
Gary Robertson
Gisela Reverter
Gonzalo Vilela
Héctor de Pedro
Jesús Abascal
Juan Antonio González
Juan Carlos Gómez
Juan Luis Meléndez
Lorena Jurado
Lorena Rosende
Paola Rojas
Roberto Hernández
Saúl Menduiña
Victor Armesto

COORDINACIÓN DE PROYECTO Y EDICIÓN

Beatriz García

DISEÑO Y MAQUETACIÓN

Susana Marín

CONTENIDO

01.

FUNDAMENTOS DEL INVENTARIO DE IA

1.1. Propósito: el inventario como mapa de riesgos activo

El **inventario de Servicios y Sistemas de inteligencia Artificial** constituye el pilar fundamental de una gobernanza responsable de la IA dentro de cualquier organización. Más allá de ser un simple registro técnico, su propósito principal es constituirse en un mapa integral de activos y riesgos, permitiendo a la organización conocer con precisión y referencia qué sistemas de IA utiliza, con qué fin, en qué condiciones, así como los impactos potenciales.

Desde la perspectiva de los **activos**, el inventario identifica y clasifica los sistemas de IA en función de su criticidad, ámbito de uso, grado de automatización, dependencia de datos y valor estratégico para el negocio. Esta visibilidad facilita la toma de decisiones en base a un conocimiento, la asignación de responsabilidades y la optimización de recursos tecnológicos.

En cuanto a los **riesgos**, el inventario actúa como un instrumento de detección temprana. Permite identificar riesgos éticos, legales, operativos y reputacionales asociados al uso de IA, como riesgos para la privacidad, impacto en los derechos fundamentales o sesgos vinculados a los mismos algoritmos, entre otros. Al centralizar esta información, el inventario se convierte en la base para la evaluación, priorización y mitigación de riesgos a lo largo de todo el ciclo de vida del sistema/servicio de IA.

En definitiva, un inventario correctamente implementado y diseñado transforma la gestión de la IA de un enfoque reactivo a uno proactivo y preventivo, alineado con los principios de responsabilidad, transparencia y control.

El inventario no se limita al cumplimiento: alinea la IA con los objetivos de negocio y los valores corporativos, acelera la confianza con clientes, reguladores y sociedad. Nos permite ver la diferencia entre inventario de “activos con IA” y la “IA como activo”.
Como beneficios clave del inventario, podríamos enumerar:

- Visibilidad integral del ecosistema de IA
- Activos internos.
- Soluciones de terceros.
- Priorización de riesgos y asignación clara de responsabilidades (propietario o responsable funcional, responsable técnico y del dato).
- Trazabilidad y evidencia para los procesos internos organizativos, auditorías internas y externas.
- Soporte a las decisiones corporativas y de negocio a nivel de inversión, implantación operativa a nivel de servicio, redundancia operativa, y retirada y/o sustitución del servicio.

1.2. Contexto Regulatorio: Reglamento de Inteligencia Artificial (RIA) y la Diligencia Debida

El RIA establece un enfoque basado en cuatro niveles de riesgo:

- Inaceptable.
- Alto.
- Limitado.
- Mínimo.

El inventario es imprescindible para identificar la categoría de cada sistema o servicio, su finalidad y las salvaguardas implementadas. Sin un inventario de sistemas en las organizaciones resulta inviable demostrar conformidad o avalarlo mediante procesos de auditoría. El RIA exige a las organizaciones identificar qué sistemas utilizan, su finalidad, su nivel de riesgo y las respuestas implementadas.

La **diligencia debida** requiere evidenciar que la organización ha identificado, prevenido y mitigado los impactos negativos del uso de la IA. El inventario permite concretar referencias a expedientes técnicos y evaluaciones de impacto (por ejemplo DPIA /FRIA) controles de seguridad y privacidad y resultados de pruebas de robustez.

Además, el inventario facilita el vínculo entre requisitos regulatorios y operación; transparencia interna y al usuario, supervisión adecuada, gestión y clasificación de incidentes, registro y mantenimiento supervisado.

Acudiendo a los pronunciamientos de los diversos organismos supervisores españoles o europeos podemos concluir que recomiendan e instan a su adopción como práctica esencial para garantizar el cumplimiento normativo y la gobernanza responsable de la IA. En este sentido, la **Agencia Española de Protección de Datos (AEPD)**, en su *Guía sobre Auditorías de Tratamientos que incluyen IA* ya en 2021 establecía, dentro del primer grupo de objetivos de control “Identificación y transparencia del componente”, como primer objetivo el “inventario del componente IA auditado”, señalando que “en cumplimiento de la responsabilidad proactiva debe existir trazabilidad, y para ello, una correcta identificación del componente IA parte del tratamiento auditado”. Concreta la AEPD en está guía (que actualmente se encuentra en revisión) que este objetivo de control se podría concretar en los controles siguientes:

- El componente IA está identificado en la documentación con un nombre o código, la identificación de la versión y la fecha de creación.
- Tanto el código como cualquier archivo adicional que defina la versión dispondrá de una firma digital de todo el conjunto que garantice su integridad.
- Existe y está documentado un historial de versiones de la evolución del componente IA utilizado, incluyendo los parámetros usados en el entrenamiento del componente y de todo aquello que asegure la trazabilidad de la evolución/cambios en el componente.

El **Supervisor Europeo de Protección de Datos (EDPS)**, en noviembre de 2025, en su *Guía sobre gestión de riesgos en sistemas de IA*, subraya que el principio de responsabilidad proactiva exige a las instituciones identificar y mitigar los riesgos derivados del uso de IA, así como demostrar las medidas adoptadas para garantizar el cumplimiento del **Reglamento (UE) 2018/1725** y, por extensión, del **RIA**.

La **Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)**, publicaba en diciembre de 2025, las guías desarrolladas en el marco del desarrollo del piloto de sandbox regulatorio de la IA como apoyo para la implementación y el cumplimiento del **RIA**. Revisadas las mismas, si bien no se dedica ninguna de ellas en concreto al inventario de la IA, las mismas incluyen referencias al inventario. Así, por ejemplo, en la ***Guía de Gestión de Riesgos*** se indica: *"Lo que haremos en esta fase será inventariar en un documento (una hoja Excel, por ejemplo) aquellos elementos del contexto que pudiesen impactar al análisis de riesgos"*[1] o en la ***Guía de Ciberseguridad*** establece que *"El proveedor deberá mantener actualizados los inventarios"*[2]. La guía incluso aconseja centralizar esta información en una herramienta corporativa, de modo que exista un **registro unificado, vigente y accesible** de todos los elementos críticos del sistema.

El inventario, por lo tanto, no solo apoya el cumplimiento legal, sino que refuerza la seguridad jurídica y la rendición de cuentas, reduciendo la exposición a sanciones, litigios y daños reputacionales.

El **RIA** no incluye conceptos como la diligencia debida o la accountability como hacen otras normas como el **RGPD**. Ahora bien, dado que su enfoque es de producto pero basado en el riesgo del sistema sí que establece y modula en función del mencionado riesgo las obligaciones de los actores de la cadena de suministro de la IA. Además, configura las obligaciones en las que sí subyacen los criterios de gestión de riesgos y por tanto de mejora continua. Veamos algunos ejemplos:

- **Sistema de gestión de riesgos iterativo (art. 9):** el proveedor debe establecer un proceso continuo de identificación, análisis y mitigación de riesgos vinculados al sistema de IA, planificado y actualizado durante todo su ciclo de vida.
- **Calidad y gobernanza de datos (art. 10):** se deben usar conjuntos de datos de alta calidad para el entrenamiento, validación y prueba de la IA. El Reglamento obliga a verificar que los datos sean pertinentes, representativos, completos y, en lo posible, libres de errores y sesgos.
- **Documentación técnica y registros (arts. 11-12):** por cada sistema de IA de alto riesgo, el proveedor debe elaborar un expediente técnico exhaustivo que permita evaluar la conformidad y asegurar la trazabilidad del desarrollo y funcionamiento del sistema. Esta documentación incluirá información detallada sobre el modelo, sus datos utilizados, proceso de diseño, pruebas, validaciones y medidas de control de riesgo aplicadas, redactada de forma clara y completa.
- **Transparencia e información al usuario desplegador (art. 13):** antes de comercializarse o ponerse en servicio, el sistema de IA de alto riesgo debe ir acompañado de instrucciones de uso e información clara para quien vaya a desplegarlo (por ejemplo, una empresa cliente). Estas instrucciones deben describir de forma comprensible las características, capacidades y limitaciones del sistema, las condiciones conocidas en las que su rendimiento puede verse afectado, así como los supuestos de uso previsto y usos prohibidos o no recomendados.
- **Supervisión humana (art. 14):** el proveedor debe diseñar el sistema con salvaguardas que permitan la supervisión e intervención humana efectiva. Debe definir, antes del despliegue, qué medidas de control humano son necesarias: por ejemplo, límites operativos incorporados que impidan a la IA tomar ciertas acciones sin aprobación humana, requerir confirmación humana en determinadas decisiones, o facilitar interfaces que hagan entendibles las salidas al operador.
- **Robustez, precisión y ciberseguridad (art. 15):** la IA de alto riesgo debe mantener durante todo su ciclo de vida un nivel adecuado de exactitud en sus resultados, resiliencia a fallos y seguridad frente a ataques. El proveedor ha de diseñar el sistema para funcionar de modo consistente con su finalidad declarada y según el estado del arte. Debe declarar en las instrucciones las prestaciones esperadas (por ej., margen de error) y asegurarse de no hacer afirmaciones engañosas sobre ellas.
- **Sistema de gestión de calidad y vigilancia postcomercialización (arts. 17 y 61):** los proveedores de IA de alto riesgo deben integrar estas acciones en un sistema de gestión de la calidad (SGC) interno.

Alineación con Marcos de Gestión (NIST AI RMF, ISO 42001)

1.3.

Para que un **Inventario de Sistemas y Servicios de la IA** sea realmente efectivo, debe alinearse con marcos de gestión reconocidos internacionalmente, que proporcionen una estructura coherente y basada en buenas prácticas.

El **NIST AI Risk Management Framework (NIST AI RMF)** propone un enfoque cíclico basado en gobernar, mapear, medir y gestionar los riesgos y activos de la IA. Dentro de este marco, el inventario cumple un rol central en la fase de identificar sistemas de IA en el contexto organizativo, su uso, vinculado con cada *stakeholder* y sus posibles impactos. Sin un inventario sólido, el resto del marco pierde consistencia

Por otro lado, **la ISO 42001,** norma específica para sistemas de Gestión de la IA, refuerza la necesidad de mantener la información documentada sobre sistemas de IA desplegados, su aplicación y objetivos, riesgos y controles. El inventario actúa como un repositorio estructurado que soporta el sistema de gestión, facilitando revisiones internas y externas, auditorías dentro de un marco de mejora continua

Cuando el **Inventario de Sistemas y Servicios de la IA** está alineado con el **NIST AI RMF** y la I**SO 42001**, permite que deje de ser un elemento aislado para integrarse en la arquitectura global de gobernanza corporativa, conectando la gestión de la IA con la gestión de riesgos, la seguridad de la información, la privacidad y el cumplimiento normativo.

[1] Agencia Española de Protección de Datos. (2021). Guía de gestión del riesgo y evaluación de impacto en tratamientos de datos personales. *https://www.aepd.es*

[2] Agencia Española de Protección de Datos & INCIBE. (2016). Guía de privacidad y seguridad en Internet. *https://www.incibe.es/ciudadania/formacion/guias/guia-de-privacidad-y-seguridad-en-internet*

1.4. Propósito: más allá del RIA

El **Inventario de Sistemas y Servicios de la IA** debe configurarse como una herramienta que, además de cumplir las obligaciones derivadas del RIA, sirva también como instrumento de apoyo para el cumplimiento de otras normativas (especialmente el **RGPD**). Desde la perspectiva del gobierno de la protección de datos, el inventario constituye una extensión natural del Registro de Actividades de Tratamiento (RAT), puesto que los sistemas de IA que tratan datos personales forman parte del conjunto de activos utilizados en dichos tratamientos. Por ello, como ya hemos señalado en guías anteriores, resulta esencial que ambos instrumentos (el RAT y el inventario de IA) estén plenamente coordinados y se retroalimenten.

Con frecuencia, la información recogida en el inventario permitirá identificar la existencia de operaciones de perfilado, decisiones automatizadas o la necesidad de articular mecanismos de oposición. Asimismo, la explicabilidad y la transparencia de los sistemas de IA serán elementos clave para elaborar los textos informativos dirigidos a los titulares de los datos conforme a los **artículos 13 y 14 del RGPD.**

Por último, la integración del inventario con otros registros corporativos no solo contribuye a la coherencia documental, sino que facilita el cumplimiento de obligaciones adicionales (como las derivadas del **artículo 64.4 del Estatuto de los Trabajadores**), particularmente en lo relativo al uso de sistemas automatizados en el ámbito laboral.

02.

GOBERNANZA Y PREPARACIÓN

2.1. El Equipo Multidisciplinar: Roles y Responsabilidades

Cada vez más, las organizaciones operan en un contexto en el que los sistemas de inteligencia artificial forman parte de procesos necesarios para la prestación de servicios, la toma de decisiones y la optimización de operaciones. La creciente presencia de estas tecnologías exige estructuras sólidas de gobernanza que permitan comprender de forma integral sus implicaciones técnicas, jurídicas, éticas y operativas. En este marco, resulta conveniente contar con un equipo multidisciplinar que reúna las funciones necesarias para analizar cada sistema desde distintos puntos de vista y asegurar que se cumplen las obligaciones establecidas por el RIA.

El propósito principal de este equipo es garantizar que las organizaciones integran, de forma coordinada, el conocimiento técnico, operativo y jurídico necesario para comprender y gestionar adecuadamente los sistemas de IA. No se trata de disponer de una estructura compleja o de múltiples departamentos, sino de garantizar que las funciones relevantes están representadas, independientemente de cómo se organicen internamente. Esto implica que las áreas tecnológicas y las áreas de negocio participen de forma activa en la identificación y análisis del sistema, y que las funciones jurídicas, ya sean de cumplimiento, asesoría jurídica, protección de datos u otras figuras equivalentes, aporten la interpretación normativa y las garantías necesarias.

Así, la participación de las **áreas responsables de tecnología** aporta una comprensión detallada de la arquitectura técnica del sistema, los modelos que incorpora, su funcionamiento interno y sus requisitos de integración con otros sistemas corporativos. Su participación permite valorar aspectos como la calidad del diseño, la robustez, la ciberseguridad o la capacidad de supervisión del sistema. Además, estas áreas permiten prever necesidades operativas, determinar limitaciones técnicas y establecer los requisitos mínimos para asegurar el mantenimiento y la actualización de cada solución.

Las **áreas de negocio** desempeñan un papel igualmente relevante, ya que son quienes aportan el contexto de uso y el propósito del sistema de IA. Comprender cómo se utilizará la tecnología, qué problema pretende resolver y qué impacto generará sobre procesos, personas o servicios es especialmente relevante para su correcta clasificación en el Inventario. Estas áreas permiten identificar quiénes serán las personas usuarias principales, qué decisiones podrán verse influidas por el sistema y en qué medida la IA contribuye a la consecución de los objetivos estratégicos de la organización. Este análisis facilita, además, anticipar riesgos derivados del uso del sistema en entornos reales.

Por otro lado, las **áreas jurídicas y de cumplimiento,** que en algunas organizaciones incluyen también la gestión de riesgos y la protección de datos, aportan una visión normativa para garantizar el uso adecuado de los sistemas de IA, interpretando las obligaciones del RIA y de otras normativas aplicables, y traduciendo estos requisitos en prácticas concretas para su funcionamiento dentro del marco regulatorio.

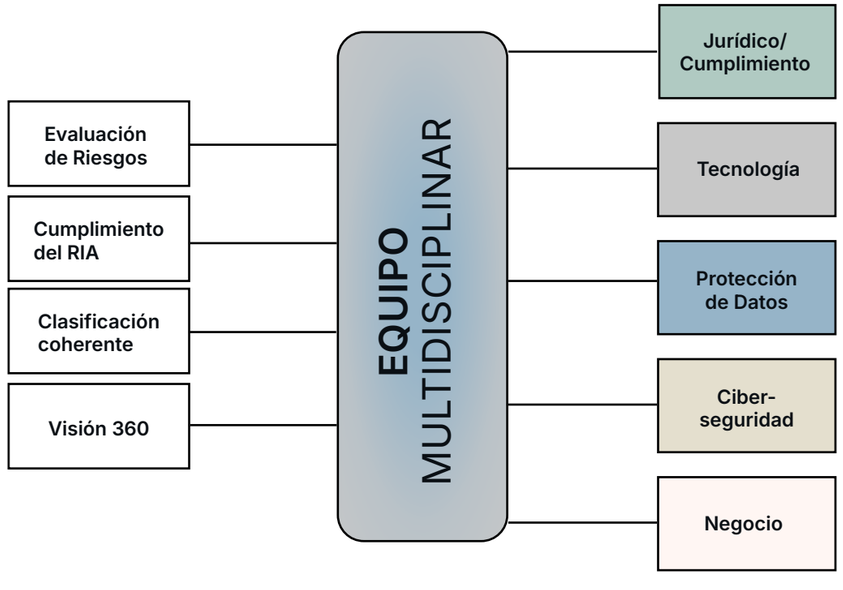
Estas áreas analizan los acuerdos, licencias, términos de servicio y garantías proporcionados por terceros, e identifican los compromisos que las organizaciones deben exigir para asegurar la transparencia, la trazabilidad y la responsabilidad asociada al uso de la IA. Esta labor garantiza que los contratos reflejen las obligaciones derivadas del RIA y que los proveedores cumplen estándares adecuados de calidad y seguridad.

Adicionalmente, las **áreas responsables de protección de datos** examinan con detalle los tratamientos de información personal asociados al funcionamiento del sistema. Esta revisión permite evaluar riesgos vinculados con la privacidad, la proporcionalidad del tratamiento o la existencia de categorías especiales de datos. Su participación refuerza la protección de los derechos de las personas y añade garantías adicionales que, en muchos casos, repercuten en la clasificación del sistema dentro del inventario. Estas áreas colaboran, asimismo, en la definición de controles asociados al acceso, la calidad y la gobernanza de los datos.

En conjunto, este enfoque permite aplicar criterios comunes y definir responsabilidades de manera clara, con el fin de cumplir los requisitos normativos: las áreas tecnológicas contribuyen con una comprensión detallada de la arquitectura del sistema, su funcionamiento y sus limitaciones; las áreas de negocio ofrecen el conocimiento del propósito, del uso esperado y del posible impacto sobre servicios y personas; y las funciones jurídicas aseguran la correcta interpretación de las obligaciones regulatorias, analizan los contratos con proveedores y verifican que los sistemas cuentan con las garantías necesarias. La combinación de estas perspectivas facilita la toma de decisiones informada y coherente.

El funcionamiento conjunto ofrece un mecanismo eficaz para identificar, documentar y clasificar los sistemas de IA y para aplicar los requisitos asociados a su ciclo de vida, desde la definición del propósito hasta la supervisión del uso, facilitando la aplicación de criterios homogéneos, evitando inconsistencias en la evaluación y reduciendo la posibilidad de que ciertos riesgos permanezcan sin identificar. Además, promueve un uso responsable de la tecnología y refuerza la confianza en los procesos internos asociados a la IA.

La labor del equipo multidisciplinar también sienta las bases para procesos como la clasificación del nivel de riesgo, la definición de mecanismos de supervisión humana, la elaboración de evaluaciones de impacto y el establecimiento de controles operativos. Cada uno de estos procesos requiere una comprensión transversal que no podría alcanzarse desde un único ámbito de conocimiento.



2.2. Definición del Alcance del Inventario

Visión Estratégica: El Inventario como Herramienta de Gestión Operativa

Una adecuada definición del alcance del Inventario de Sistemas de Inteligencia Artificial en una compañía es fundamental para que no se conciba únicamente como un registro estático o una mera obligación de cumplimiento, sino como una herramienta de trabajo dinámica y que pueda ser utilizada por todos los intervinientes en el marco de gobierno de la Inteligencia Artificial definido. El objetivo es que este repositorio sea el punto único de referencia para identificar, de forma clara y visual, todos los sistemas de Inteligencia Artificial que se utilizan y están validados por la compañía, así como los principales riesgos y medidas que se deben tener en cuenta.

Para lograr este objetivo, y a diferencia de los inventarios tradicionales de activos de IT, este repositorio se puede configurar de manera que actúe como eje central de validación de las herramientas. Su propósito es:

- **Centralizar el flujo de aprobación:** Reflejar los análisis de todas las áreas implicadas (Legal, Ciberseguridad, Ética, Protección de Datos y Negocio).
- **Trazabilidad del Ciclo de Vida de los Sistemas de IA:** Realizar el seguimiento desde la fase de ideación o adquisición hasta la retirada.
- **Monitorización de Riesgos:** Vincular cada sistema con los análisis de riesgos realizados, las medidas mitigadoras y evaluaciones de impacto asociadas (DPIA, FRIA).

Integración con Sistemas ya existentes en la compañía

En línea con la idea de aprovechar otros marcos de gobierno definidos en las organizaciones, como es el caso de Privacidad, y para evitar duplicidades optimizando la carga administrativa, la definición del alcance del inventario debe realizarse tratando de aprovechar las estructuras ya existentes. En este sentido, siempre que sea posible se recomienda la integración del Inventario de Sistemas de IA con:

- **Inventarios de Activos IT de la Compañía.**
- **Registros de Actividades de Tratamiento (RAT):** Sincronizando la información de las actividades de tratamiento de datos para evitar discrepancias.
- **Procesos de Compras y análisis de riesgos de terceros:** Capturando la entrada de sistemas de terceros desde el momento de la contratación.

Definición de la información a incluir en el Inventario

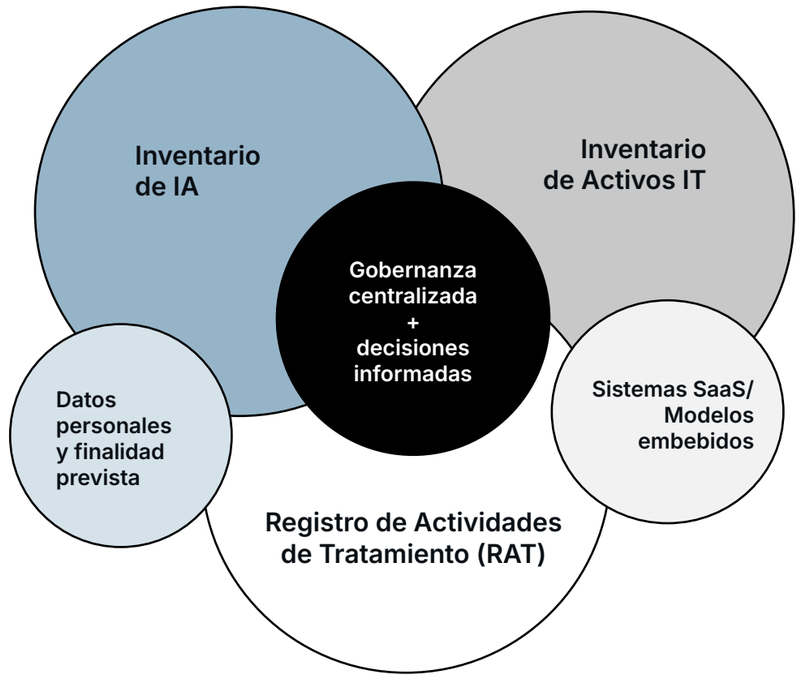
En primer lugar, se deben identificar los sistemas a incluir en el inventario. Se definen como objeto de este inventario todos los sistemas de software desarrollados internamente o adquiridos a terceros que utilicen técnicas de IA para generar resultados como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúan.

Específicamente, el alcance incluye:

- Modelos de Aprendizaje Automático (*Machine Learning* o ML).
- IA Generativa y Modelos Fundacionales.
- Sistemas de Lógica Basada en Conocimiento.
- IA Embebida en Software de Terceros (*SaaS*).

Para garantizar que el registro es manejable y evitar el exceso de información innecesaria, se deberían excluir del análisis los siguientes sistemas:

- **Software basado en reglas tradicionales:** programación lineal sin capacidad de aprendizaje.
- **Automatización Robótica de Procesos (RPA) simple:** scripts que replican clics humanos sin componentes cognitivos.
- **Herramientas de Análisis Estadístico Básico:** uso de hojas de cálculo.



Datos a Registrar y Granularidad

Una adecuada definición del alcance del inventario requiere encontrar el equilibrio entre la exhaustividad técnica y la agilidad operativa. La propuesta es dividir la información a registrar en el Inventario en tres **grandes bloques:**

A. Identificación y Contexto (Información Básica)

- ID y Nombre del Sistema: Identificador único del sistema y nombre comercial/interno.
- Intervinientes: Proveedor o propietario del sistema, responsable del despliegue, persona de referencia de negocio y responsable técnico.
- Finalidad Prevista: Descripción clara de para qué se va a utilizar el sistema. Esta información es fundamental a efectos de la clasificación de riesgo según el RIA.
- Estado: (En desarrollo / En pruebas / Producción / Retirado).

B. Análisis de Validación Multidisciplinar

Con el objetivo de que el inventario sirva como herramienta de análisis de riesgos y validación de los sistemas, debe configurarse de manera que sirva como evidencia de que el sistema ha pasado por las validaciones de todos los equipos intervinientes en el proceso. Para ello, se debe configurar de modo que refleje el resultado del análisis de cada una de las áreas (aprobado, aprobado con medidas, denegado):

- **Validación Técnica: r**obustez, precisión y rendimiento.
- **Validación Legal/Privacidad:** cumplimiento de RGPD y RIA
- **Validación Ética:** análisis de sesgos y equidad.
- **Validación de Ciberseguridad:** resiliencia ante ataques adversarios.
- **Validación de Propiedad Intelectual.**

C. Medidas de mitigación de los riesgos identificados

Como última entrada del inventario, se propone identificar las medidas necesarias para la adecuada implementación y uso de los sistemas de IA registrados.

Ámbito Organizativo y Aplicación Territorial

El alcance del inventario se debe extender a todas las áreas de negocio y filiales de la compañía (o el grupo, en su caso), independientemente de su ubicación geográfica, siempre que la organización tenga alguna implicación o pueda derivarse alguna responsabilidad por el uso de los sistemas.

Adicionalmente, se recomienda incluir todos los sistemas utilizados con independencia de la fase del ciclo de vida en la que se encuentren. De este modo, se mantiene la trazabilidad y evidencia de los sistemas utilizados en el paso.

Conceptos Clave: Sistemas, Modelos y *Fine-Tuning* de modelos fundacionales

2.3.

Este apartado ofrece una explicación sencilla y ordenada sobre los elementos principales que forman un sistema de Inteligencia Artificial. Su objetivo es ayudar a cualquier organización a diferenciar entre un sistema de IA, un modelo, un modelo fundacional y las tareas de ajuste que pueden modificar su comportamiento. Estos conceptos sirven de base para comprender qué se debe registrar en el inventario y qué responsabilidades conlleva cada tipo de componente.

Sistema de Inteligencia Artificial

Un sistema de Inteligencia Artificial, en adelante, “sistema de IA”, es el elemento central que se registra en el inventario. La organización debe entenderlo como el conjunto completo de piezas que permiten que una solución basada en IA funcione en la práctica.

Un sistema de IA es un producto o servicio que utiliza técnicas automatizadas para analizar información y generar una salida. Esta salida puede ser una predicción, una recomendación, un contenido o una decisión que influye en un entorno digital o físico. El sistema se compone de varios elementos: el o los modelos de IA, las interfaces que utilizan las personas, los datos que entran y salen, los procesos de preparación y revisión de esa información y la infraestructura donde funciona (por ejemplo, servidores, aplicaciones o servicios en la nube).

El RIA establece que se considera sistema de IA a cualquier solución que cumpla varios elementos básicos: está basada en técnicas automatizadas, analiza información, genera una salida y tiene capacidad para influir en su entorno. Estos elementos deben evaluarse durante todo el ciclo de vida: diseño, desarrollo, uso y mantenimiento.

Para cada sistema de IA, la organización registra información esencial, como:

- Propósito y uso previsto.
- Descripción del entorno donde funciona.
- Interfaces disponibles para las personas usuarias.
- Dependencias con otros sistemas o servicios.
- Categoría de riesgo según la normativa.
- Responsables del sistema dentro de la organización.
- Evidencia de pruebas realizadas, incluidas las orientadas a seguridad y comportamiento.

Modelo de Inteligencia Artificial

Mientras el sistema de IA representa todo el conjunto, el modelo de Inteligencia Artificial, en adelante, “modelo de IA”, es el componente que realiza las operaciones de análisis dentro del sistema.

Un modelo de IA es una estructura matemática creada para transformar unos datos de entrada en un resultado. Existen muchos tipos de modelos, como redes neuronales, árboles de decisión o sistemas basados en reglas; el modelo aprende a partir de datos. El comportamiento final depende tanto de este aprendizaje como de cómo se integra en el sistema, incluyendo políticas de uso, filtros de seguridad y otras configuraciones. Es la “inteligencia” dentro del sistema.

Además, un sistema de IA puede incluir varios modelos: uno principal para realizar la tarea, otros para detectar errores, supervisar el comportamiento o ayudar a explicar resultados.

Cada modelo que forme parte de un sistema se registra como un componente con:

- Tipo de modelo y finalidad.
- Origen o proveedor.
- Licencia y posibles restricciones.
- Versión y huella digital o identificador.
- Documentación asociada (“*model card*” u otras guías).
- Métricas básicas de funcionamiento.
- Referencia a los conjuntos de datos utilizados para entrenamiento y pruebas.

Modelos Fundacionales

Los modelos fundacionales ocupan un lugar especial dentro del inventario, ya que actúan como modelos de propósito general que pueden adaptarse a muchas tareas distintas.

Un modelo fundacional es un modelo entrenado con grandes cantidades de información variada. Gracias a su tamaño y complejidad, puede utilizarse en tareas muy diversas, como análisis de texto, imágenes, sonido o combinaciones de varios formatos. Estos modelos tienen capacidades amplias, pero también presentan riesgos que deben evaluarse. Algunos ejemplos son la generación de información incorrecta, la aparición de respuestas inapropiadas o riesgos sistémicos como: alucinaciones, *prompt injection*[3], fuga de datos o uso indebido.

Cuando un sistema utiliza un modelo fundacional, la organización registra:

- La relación entre el modelo base y el sistema que lo emplea.
- Documentación proporcionada por el proveedor.
- Límites de uso indicados por el proveedor.
- Evidencias de pruebas realizadas en materia de seguridad y comportamiento.
- Detalles sobre cómo se integra en el sistema final.

Ajuste de modelos fundacionales

El ajuste de modelos fundacionales, en adelante, *“fine tuning”* consiste en adaptar un modelo fundacional para que realice una tarea concreta o se comporte siguiendo unas directrices determinadas.

El ajuste es un proceso que modifica parte del modelo original para especializarlo. Puede realizarse con diferentes técnicas. Algunas requieren entrenamiento adicional con ejemplos específicos, y otras utilizan métodos que ajustan únicamente una parte del modelo para reducir recursos y costes. El resultado del ajuste es un modelo derivado que se comporta de manera distinta al modelo original. Por este motivo, este modelo derivado debe tratarse como un nuevo componente dentro del inventario.

Incluso pequeñas modificaciones, como plantillas de instrucciones o configuraciones internas, pueden generar cambios importantes en el comportamiento del sistema. Por ello, estas modificaciones deben registrarse y mantenerse versionadas.

La organización incorpora información clara sobre:

- El modelo base utilizado.
- Los datos empleados para el ajuste y su base jurídica.
- Configuraciones aplicadas durante el proceso.
- Resultados de validación y pruebas.
- Relación entre el modelo ajustado y el sistema donde se integra.

[3] Técnica de manipulación del comportamiento previsto de un sistema de IA basado en lenguaje, provocando que genere respuestas distintas a las establecidas por sus reglas o controles.

03.

VISIÓN GENERAL DE LAS FASES DEL INVENTARIADO

3.1. Introducción al Proceso Iterativo

Objetivo del Proceso Iterativo

El **Inventario de Servicios y Sistemas de IA** se concibe como un proceso dinámico, recurrente e iterativo, y no como un ejercicio estático de un solo evento. Esta aproximación es fundamental para garantizar que el inventario se mantenga como una fuente precisa y relevante a lo largo del ciclo de vida de todos los sistemas de IA de la organización.

El carácter iterativo del proceso responde precisamente a la naturaleza evolutiva de la tecnología de IA y al cambiante panorama regulatorio. Un sistema de IA que hoy se considera de riesgo limitado, mañana puede incorporar nuevas funcionalidades o desplegarse en un nuevo contexto que eleva el riesgo inicialmente asignado, incluye o modifica su clasificación a alto riesgo, de acuerdo con los criterios del RIA. Por lo tanto, el inventariado exige una vigilancia y actualización continua.

Alineación con Marcos de Referencia

La metodología para la creación y el mantenimiento del inventario se alinea estrechamente con los marcos de gestión de riesgo de IA más reconocidos, lo que asegura su robustez y su utilidad práctica, concretamente:

- **RIA:** el Inventario de Servicios y Sistemas de IA de permite la identificación temprana de sistemas que caen en las categorías de riesgo inaceptable, alto, limitado o mínimo, un requisito crucial para determinar las obligaciones de conformidad, así como permite la detección temprana en cualquier característica del servicio o sistema que puedan provocar una recalibración sobre el riesgo inicialmente identificado.
- **NIST AI Risk Management Framework (NIST AI RMF):** el proceso iterativo del inventario satisface los principios de Gobernanza, Mapeo, Medición y Gestión propuestos por el NIST. El inventario mapea los activos, mide el riesgo a través de la clasificación, y establece una base para la gestión continua de dichos riesgos.
- **ISO-IEC 42001 (Gestión de sistemas de IA o AIMS por sus siglas en inglés):** el Inventario de Servicios y Sistemas de IA constituye un componente esencial del AIMS, proporcionando la lista de activos de IA que deben ser gestionados y documentados. El proceso iterativo garantiza que la gestión de la IA sea continua y esté integrada en los procesos de negocio.

El proceso iterativo establece un vínculo directo y necesario entre el registro del servicio o sistema en el inventario y el cumplimiento regulatorio, especialmente en lo que respecta a:

- **Documentación Técnica:** el inventario actúa como el índice maestro que referencia la ubicación de la Documentación Técnica para cada sistema
- **Informes de auditorías de sesgo y pruebas de calidad:** la ficha del inventario registra la existencia, fecha y resultado de las auditorías de sesgo, las pruebas de calidad de los datos y los resultados en las métricas correspondientes.
- **Evaluaciones de Impacto sobre Derechos Fundamentales:** para los sistemas de IA de alto riesgo, el inventario debe señalar que se ha completado las evaluaciones correspondientes, tal como lo requiere el artículo 27 del RIA.

Mantenimiento Continuo y Clasificación de Riesgo Dinámica

El proceso de inventariado incorpora mecanismos de revisión periódica y desencadenantes de actualización, como pueden ser:

- Cambio en el propósito o alcance previsto.
- Actualización de algoritmos dentro del modelo.
- Modificación del conjunto de datos de entrenamiento.
- Vencimiento de certificaciones.
- Incidentes y reclamaciones.
- Detección de fallos críticos o sesgos.
- Revisiones periódicas programadas.
- Retirada del servicio o sistema.

Cualquiera de los puntos previamente mencionados desencadenará el procedimiento al que se hace referencia en el apartado 7.1 Asimismo, la detección de cualquier incidente o fallo activará adicionalmente el apartado 7.2.

Finalmente se ha de destacar que la clave del correcto funcionamiento de este inventario, para el aporte de valor, reside en su mantenimiento proactivo. Se trata de un registro vivo que requiere una gestión constante a través de la Fase 4[4]. El Inventario de Sistemas y Servicios de ISMS Forum funciona como un bucle de retroalimentación continuo que facilita la gestión del riesgo de IA y transforma las obligaciones de cumplimiento regulatorio en un activo estratégico para la organización.

[4] Monitorización y Mantenimiento

3.2. Resumen de la *Fase 1*: Mapeo e Identificación

El proceso de descubrimiento, mapeo e identificación de sistemas de Inteligencia Artificial dentro de una organización constituye uno de los pilares fundamentales para garantizar un gobierno tecnológico sólido, seguro y alineado con los marcos regulatorios actuales y emergentes. Desde una perspectiva de ciberseguridad y gestión del servicio, este proceso no se limita únicamente a identificar qué activos de IA existen en el entorno corporativo; implica comprender su uso real, su criticidad, su impacto operativo y los riesgos asociados tanto a nivel técnico como funcional.

Esta primera fase, mapeo e identificación, debe arrancar con una definición clara del alcance. Sin un perímetro bien delimitado (ya sean unidades de negocio, áreas funcionales, entornos operativos o infraestructuras tecnológicas) el inventario resultante será inconsistente y carecerá de valor para los equipos de seguridad, cumplimiento o gobierno del dato. A partir de este marco inicial, la organización debe establecer un modelo de gobierno específico para la IA que fije responsabilidades, líneas de supervisión, políticas internas y criterios de evaluación. Sin este modelo, cualquier intento de catalogar o controlar sistemas de IA termina generando fragmentación, duplicidad y, en última instancia, riesgos no gestionados.

Este proceso debe combinar enfoques manuales y automatizados. Un **enfoque híbrido** es esencial para detectar tanto los activos con implementación de soluciones IA típicas, como aquellos que quedan fuera del control habitual (*shadow AI*). El objetivo final será consolidar toda la información en un primer borrador del inventario oficial de sistemas y activos de IA. Este inventario no es un simple listado sino una herramienta estratégica que permite habilitar procesos de Gobierno, supervisión, auditoría y gestión de riesgos. A partir de su existencia, pueden desplegarse mecanismos de mejora continua, mediante revisiones periódicas y actualizaciones alineadas con el ciclo de vida de los sistemas.

El descubrimiento de sistemas y servicios IA es un proceso transversal que exige madurez operativa, disciplina metodológica y una integración estrecha entre ciberseguridad, gobierno del dato, TI y las áreas funcionales. Su correcta ejecución es la base para garantizar que el uso de la inteligencia artificial en la organización sea seguro, transparente, regulado y alineado con las mejores prácticas de Gestión del Servicio.

3.3. Resumen de la *Fase 2*: Clasificación y Evaluación de Riesgos

Esta fase constituye la primera capa de análisis estructurado dentro del proceso de inventariado de servicios y sistemas de IA. Su función es determinar, de manera preliminar, qué tipo de riesgo representa cada caso de uso, qué obligaciones regulatorias pueden aplicar y qué nivel de revisión será necesario antes de su desarrollo o despliegue. Esta fase actúa como una intersección crítica entre el descubrimiento inicial y la documentación y registro formal, sentando las bases del triaje, clasificación normativa y evaluación de impacto que serán desarrollados en profundidad en el Capítulo 5.

El objetivo principal de esta fase no es resolver todos los aspectos del riesgo, sino establecer una categorización inicial suficientemente robusta que permita activar los procedimientos adecuados en las fases posteriores. Para ello, este ejercicio combina elementos de validación conceptual, análisis normativo y detección temprana de alertas que permiten identificar si un caso de uso debe ser descartado, aceptado bajo condiciones o escalarse hacia evaluaciones especializadas.

Objetivos

1. Determinar el tipo y naturaleza del sistema de IA

Se identifican elementos como:

- **Tipo de IA:** *machine learning* tradicional, modelos predictivos, modelos generativos, modelos GPAI y GPAI con riesgo sistémico, IA embebida, herramientas de terceros, etc.
- **Finalidad del sistema:** soporte a decisiones, automatización, interacción conversacional, análisis de comportamiento, detección de anomalías, etc.
- **Relación con procesos organizativos y nivel de autonomía.**

2. Evaluar el riesgo inherente y contextual

La categorización debe responder a los criterios regulatorios del Reglamento Europeo de IA según su taxonomía oficial:

- Riesgo prohibido / no aceptable.
- Alto riesgo (incluyendo GPAI (Sistema de IA de propósito general) de riesgo sistémico).
- Riesgo limitado con obligaciones de transparencia.
- Riesgo mínimo (sin requisitos adicionales).

3. Conectar el nivel de riesgo con obligaciones concretas

La clasificación es el paso previo esencial para determinar:

- Nivel de documentación requerido.
- Necesidad de realizar evaluaciones adicionales.
- Supervisión humana obligatoria
- Requisitos de robustez, transparencia, testing o monitorización.
- Inclusión en registros oficiales o internos.

4. Preparar los elementos de entrada para el inventario documental

Toda información estructurada en esta fase se trasladará a la Fase 3 (Documentación y Registro), facilitando la creación del expediente técnico del sistema.

Como propósito general de esta fase, se quiere contar con una metodología que nos permita:

- Aplicar un triaje preciso del caso de uso.
- Identificar si incurre en actividades prohibidas por el RIA.
- Determinar si el sistema está vinculado a supuestos de alto riesgo.
- Evaluar posibles riesgos reputacionales, regulatorios o de impacto social.
- Analizar si será necesario llevar a cabo una Evaluación de Impacto sobre Derechos Fundamentales (FRIA).
- Definir el nivel de revisión y documentación necesarios.

Metodología

La metodología de clasificación y evaluación de riesgos abarca una serie de pasos:

1. Validación inicial.

Una de las aportaciones esenciales de esta fase es la realización de un triaje inicial, cuyo detalle metodológico se desarrolla de forma completa en la sección 5.1.

Este triaje permite:

- Validar que el caso de uso no incurre en actividades prohibidas.
- Identificar si pudiera situarse en una categoría de alto riesgo.
- Detectar riesgos reputacionales, regulatorios o sociales que exigen cautela.
- Determinar si el caso de uso debe avanzar, debe reformularse o debe descartarse.

Este punto ofrece, por tanto, la justificación conceptual para la existencia del proceso detallado que se describe posteriormente en el Capítulo 5, donde cada una de estas verificaciones iniciales se transforma en preguntas concretas, listas de control y secuencias de decisión.

2. Clasificación preliminar según el RIA

El Reglamento Europeo de IA introduce una taxonomía de riesgos que guía todo el ciclo de evaluación. Aquí podemos ver una estructura inicial:

- Prácticas prohibidas.
- Sistemas de alto riesgo (especialmente aquellos vinculados a empleo, servicios esenciales, biometría, seguridad, infraestructuras críticas o asistencia pública).
- Sistemas de riesgo limitado, con obligaciones de transparencia.
- Sistemas de riesgo mínimo.

El Capítulo 5 desarrollará en detalle estos criterios, proporcionando:

- Listas completas de supuestos.
- Ejemplos.
- Distinciones por contexto.
- Implicaciones para la documentación.
- Rutas metodológicas específicas para cada categoría.

3. Identificación temprana de condiciones de alerta

El análisis inicial también integra elementos que, aun no siendo prohibidos ni necesariamente de alto riesgo, pueden incrementar significativamente la complejidad del caso de uso y su exposición regulatoria.

Estas condiciones incluyen, entre otras:

- Participación de datos personales sensibles o de categoría especial.
- Uso de grandes modelos generativos o agentes autónomos.
- Integración con sistemas productivos críticos.
- Impacto potencial sobre colectivos vulnerables.
- Exposición pública de contenidos generados.
- Posibilidad de generar deepfakes o manipulación de información.
- Dependencia tecnológica externa o ausencia de datos representativos.

Más adelante se desarrollará cada una de estas condiciones en forma de preguntas específicas que permiten objetivar la decisión sobre si un caso de uso requiere una evaluación reforzada o una FRIA previa al despliegue.

3.4. Resumen de la Fase 3: Documentación y Registro

La Fase 3 del proceso de inventariado constituye la columna vertebral del gobierno documental de los sistemas de IA. Su propósito es asegurar que cada sistema, caso de uso o modelo tenga una trazabilidad completa, un expediente técnico estructurado, y una integración directa con las obligaciones regulatorias, presentes o futuras.

A diferencia de las fases anteriores (centradas en descubrir y clasificar) la Fase 3 se orienta a consolidar evidencias, formalizar la información y establecer un mecanismo permanente de actualización, de modo que la organización pueda demostrar, ante auditorías internas o externas, que la IA se gestiona de forma responsable, segura y conforme con la normativa.

Objetivos

La Fase 3 persigue tres metas principales:

1. Garantizar la disponibilidad de un registro único, actualizado y gobernado

El inventario debe evolucionar hacia un repositorio centralizado y estructurado que consolide la información esencial de cada sistema: identificación, propósito, arquitectura, fuentes de datos, criterios de evaluación del riesgo, controles implementados y métricas de desempeño. Este repositorio debe constituirse como el punto único de referencia para los comités de gobierno, auditores, responsables técnicos y funcionales, así como para las áreas de Operaciones, Negocio y Cumplimiento.

Asimismo, la información contenida en el inventario debe ser transversal y estar plenamente integrada con el inventario de activos y los repositorios de cumplimiento normativo, garantizando la coherencia, trazabilidad y reutilización de la información a lo largo de todo el ciclo de vida del sistema y de los procesos de control.

2. Proveer evidencias de cumplimiento y responsabilidad

La fase exige la elaboración de una documentación mínima obligatoria, alineada con marcos como el Reglamento Europeo de IA, ISO/IEC 42001 o el NIST AI RMF. Esta documentación soporta la evaluación del riesgo, la explicabilidad, la supervisión humana, la transparencia, la seguridad y la robustez del sistema.

3. Establecer los cimientos del ciclo de vida de gobierno

El registro y la documentación no son estáticos: deben permitir la monitorización, la revisión continua y la generación de indicadores que faciliten decisiones informadas sobre mantenimiento, mejora o retirada del sistema.

Componentes esenciales

Esta fase se articula en tres bloques, que más adelante serán desarrollados en el Capítulo 6:

1. Consolidación en una base de datos centralizada

El inventario debe componerse de un conjunto de campos normalizados, que permitan describir la iniciativa desde lo técnico, lo organizativo y lo regulatorio. Entre los campos típicos se incluyen:

- Identificación del sistema y responsable funcional.
- Finalidad y contexto de uso.
- Naturaleza del modelo (tradicional, ML, generativo, modelo fundacional...).
- Datos utilizados y procedencia.
- Nivel de riesgo según el marco de referencia adoptado (RIA, ISO/IEC 42001, criterios internos).
- Controles aplicados y medidas de mitigación.
- Evidencias disponibles y enlaces a documentación asociada.

Además, el inventario debe permitir control de versiones, registro de cambios, gestión de permisos, y mecanismos de consulta y auditoría.

2. Vinculación con la documentación de cumplimiento

La Fase 3 no se limita a registrar datos: exige construir el expediente documental asociado a cada sistema, que permite demostrar su conformidad.

Entre la documentación necesaria, se encuentran:

- **Expediente técnico:** descripción completa del sistema, su comportamiento esperado, arquitectura, datos, métricas de rendimiento, riesgos identificados y controles implantados.
- **Evaluaciones de impacto** (p. ej., evaluación de impacto en derechos fundamentales o evaluación ética, cuando apliquen por normativa o política interna).
- **Evidencias de validación:** resultados de pruebas, evaluaciones de robustez, explicabilidad, auditorías internas y revisiones de seguridad.
- **Políticas y normas aplicables:** principios de IA responsable, políticas de datos, políticas de seguridad, estándares éticos, etc.
- **Registros operativos:** bitácoras, logs de eventos significativos, incidencias detectadas, acciones correctivas y resultados de monitorización continua.

La documentación debe cumplir criterios de claridad, accesibilidad, integridad y trazabilidad, de manera que los distintos roles de la organización (CISO, responsables de negocio, auditores, comité de IA) puedan encontrar fácilmente lo necesario.

3. Conexión con obligaciones regulatorias y registros oficiales

En organizaciones sujetas a regulaciones específicas (por ejemplo, el RIA cuando entre en plena aplicación), la Fase 3 también comprende:

- Preparar el sistema para su registro en bases oficiales, cuando aplique (p. ej., para sistemas clasificados como de alto riesgo).
- Incorporar los requisitos documentales obligatorios, como plan de monitorización post-despliegue, obligaciones de transparencia o registros automáticos de eventos.
- Establecer los flujos de comunicación necesarios para el reporte de incidentes, especialmente cuando puedan tener impacto significativo en seguridad, derechos o infraestructuras críticas.

Esta fase debe diseñarse de forma lo suficientemente flexible y modular como para incorporar nuevas obligaciones sin rediseñar el inventario entero.

Roles y responsabilidades en la fase

La fase requiere la participación de distintos perfiles:

- **Responsables de negocio:** validan propósito, alcance, beneficios y uso adecuado del sistema.
- **Equipos técnicos:** mantienen el expediente técnico, describen arquitectura, integraciones, datos y métricas.
- **Equipos de seguridad y cumplimiento:** verifican requisitos éticos, regulatorios, de seguridad, de privacidad y de riesgo.
- **Comité de IA o estructura de gobernanza:** revisa, aprueba y supervisa la documentación y los cambios relevantes.
- **Auditoría interna o externa:** valida completitud y consistencia del registro y la documentación asociada.

La definición formal de estos roles garantiza que la información no dependa de personas concretas, sino de funciones institucionalizadas.

3.5. Resumen de la Fase 4: Monitorización y Mantenimiento

En esta fase, la operativa vinculada al inventario de sistemas y servicios de Inteligencia Artificial se establece como un control continuo y transversal para asegurar la Gobernanza efectiva además de la Gestión de Riesgos y el Cumplimiento Normativo. El propósito es que la información documentada refleje siempre la realidad operativa de los sistemas de IA; qué activos existen, para qué sirven, qué nivel de criticidad tiene para la organización, y qué controles aplicamos.

Este enfoque deberá estar alineado con el **RIA, la ISO/42001: 2023 y el NIST AI RMF.** En la práctica, convierte al inventario en un sistema vivo de trazabilidad, ayudando a anticipar, detectar y absorber cambios tecnológicos, regulatorios y de negocio.

Podemos subdividir esta fase en tres apartados.

Procedimientos de actualización del Inventario

El objetivo principal es mantener un modelo preciso y auditable de los Sistemas y servicios de la IA. Permitiendo exponer la realidad de los sistemas en la organización y que permita una trazabilidad completa. Como parte de este un proceso iterativo podemos destacar diferentes hitos en el procedimiento de actualización.

- **Detección e incorporación de nuevos sistemas.** El proceso se inicia con identificar todos los procesos de IA, desde un enfoque en dos ámbitos; a nivel funcional (*Top-Down*) o a nivel técnico (*Bottom-Up*). Esta identificación se realizará mediante cuestionarios, y mecanismos de descubrimiento.
- **Una revisión periódica planificada.** Hay que tener en cuenta que estos procesos están en constante evolución y este proceso deberá ir acompañado de una planificación y registro, vinculando para sistema de mayor riesgo, revisiones con un plazo más corto, ampliándose el plazo entre revisiones, ante sistemas con riesgo menor. En función del contexto de riesgo, la evolución de la frecuencia de análisis cambiará; aplicando para sistemas de alto riesgo, un periodo con un plazo de revisión menor. A medida que el riesgo sea de menor valor, el plazo de la revisión puede incrementarse, procurando no exceder el límite de no realizar revisiones por un periodo de doce meses. El propietario del servicio deberá verificar la exactitud del análisis y el conjunto y estado de las acciones.
- **Actualización por cambios significativos.** Estos desencadenantes se analizan de forma homogénea obligando a la revisión del inventario. Aquí podemos encontrar diversos cambios, como nuevas versiones de los modelos de IA aplicados, nuevas fuentes de datos, cambio del proveedor, deterioro del rendimiento y, por supuesto, cambios normativos o de políticas internas. Todo ello deberá garantizar un ciclo de vida real del sistema y del riesgo asociado.
- Por último, encontramos la **verificación, trazabilidad y mejora continua.** Este modelo de control de la calidad debe ser auditable y verificable. Para ello identificaremos, la verificación de los responsables y flujos de aprobación, histórico de cambios, vinculación de evidencias (DPIA/FRIA) y revisión periódica de eficacia y eficiencia del propio mantenimiento.

La sostenibilidad del mantenimiento depende del encaje operativo con procesos existentes a nivel corporativo como la Gestión de cambio, la Gestión de Riesgos y Cumplimiento, Gobierno del dato y seguridad de la Información y Comunicación incorporando la formación y sensibilización en la organización, así como las responsabilidades de mantener actualizado el inventario. La finalidad de esta integración será evitar duplicidades, reducción de carga y garantizar una visión holística del inventario.

Sistema de Registro de Incidentes y Fallos

El registro de incidentes es el eslabón de unión de la operativa diaria y la gobernanza. Cubriendo degradaciones del rendimiento, indisponibilidad y comportamientos anómalos, así como los errores recurrentes e impactos no previstos.

Los principios que deben regir estos registros son:

- **La trazabilidad completa.** Con registro de momento de la incidencia, así como la causa raíz y el impacto, mitigaciones, notificaciones, evidencias y lecciones aprendidas.
- Un **flujo estándar de detección y registro** que permita una priorización y, de paso, a un análisis con aplicación de medidas correctivas y de verificación; y por último de cierre.
- **Establecer la Responsabilidad del propietario del sistema** que lidere la coordinación con tecnología, seguridad y cumplimiento.
- **Relación con el inventario:** cada incidente actualiza la ficha y si se identifica un cambio relevante, actúe como desencadenante formal.

Estos modelos, cuando dependen de proveedores o componentes externos implicarán exigir contractualmente un sistema de registro con acceso seguro, SLA de notificación de incidentes críticos con detalle técnico planes de corrección, y conservación de evidencias por el tiempo requerido. Así, el registro convierte eventos operativos en inteligencias gestionable y comparable entre sistemas.

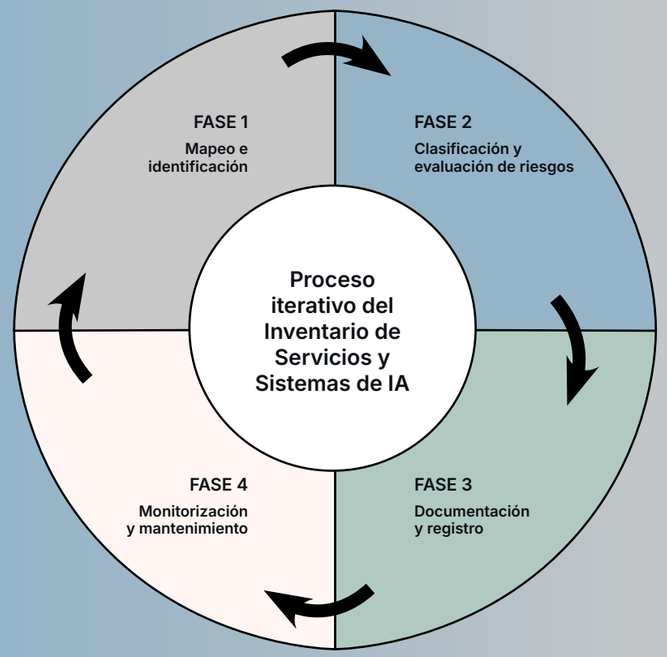
Seguimiento de la evolución normativa

Dado el dinamismo regulatorio en los sistemas y servicios de Inteligencia Artificial se deberá establecer una vigilancia recurrente, coordinada por cumplimiento y asesoría legal, con apoyo de tecnología, riesgos y seguridad.

Este proceso de seguimiento será mediante:

- **Fuentes externas:** nuevas normas, guías, criterios interpretativas y directrices que afecten a la clasificación de riesgos y obligaciones.
- **Señales internas:** basándose sobre todo en políticas corporativas, así como cambios en el organigrama, cambios en los proveedores de la organización y ámbitos de uso o resultados de evaluaciones.

Ante un cambio, se realiza un análisis de aplicabilidad al inventario, identificando qué sistemas son impactados, el cambio de categorías u obligaciones, así como la revisión documental y de control que deberán ser nuevamente ajustadas. La actualización queda evidenciada, en referencia al cambio, fecha y acciones, sosteniendo evidencias para auditorías y coherencias en la operación el riesgo y el cumplimiento.



04.

DESARROLLO DE LA FASE 1: MAPEO E IDENTIFICACIÓN

4.1. Técnicas de Descubrimiento de Sistemas de IA

Las técnicas de descubrimiento de sistemas de IA se refieren a métodos y procedimientos utilizados para identificar, mapear y analizar sistemas de IA presentes en una organización tanto en entorno de desarrollo como en producción. El objetivo de dicho descubrimiento se resume en tres principales aspectos:

- **Cumplimiento normativo:** garantizar que todos los sistemas de IA estén identificados para cumplir con regulaciones como el RIA de la UE.
- **Gestión de riesgos:** evaluar el impacto y los riesgos asociados a cada sistema de IA, y gestionar de forma proactiva cualquier riesgo identificado.
- **Transparencia y gobernanza:** facilitar la supervisión y el control sobre el uso de IA en la organización, como así también la alineación con la estrategia.

Como primer paso es recomendable implementar un proceso de descubrimiento que puede contemplar las siguientes fases:

1. Definir el alcance

- Identificar las áreas, departamentos y sistemas (en producción, desarrollo o pruebas) objeto de la revisión.

2. Crear grupo de trabajo y modelo de gobierno

- Crear un grupo de trabajo multidisciplinar con perfiles de TI, seguridad, legal, cumplimiento y negocio.
- Definir un modelo de gobierno del proceso de descubrimiento con designación de responsables para cada fase.

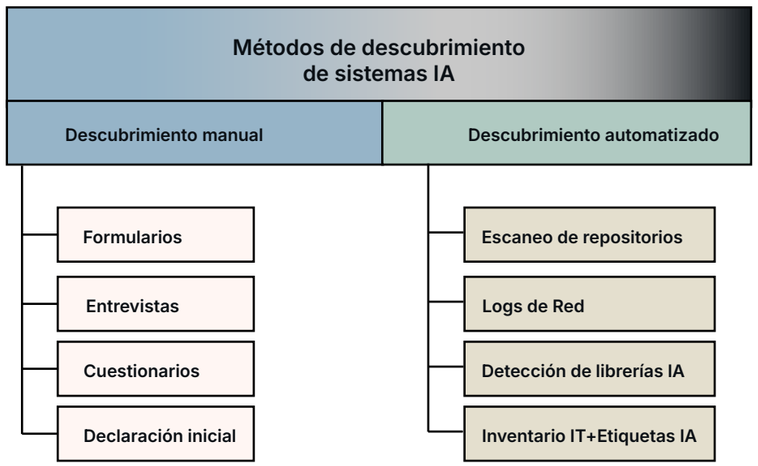
3. Definir los métodos descubrimiento

- Identificar los roles y procesos que puedan aportar información para realizar un mapeo manual de sistemas IA.
  - » Mediante entrevistas y encuestas internas se pueden identificar iniciativas, proyectos o herramientas IA que incluso no están catalogadas como tales.
  - » Otra opción puede ser el análisis de contratos con proveedores y servicios ya que muchas soluciones externas integran capacidades de IA que pueden pasar inadvertidas.

Si bien no es un método tan eficiente como el que se comentará a continuación, el uso de cuestionarios estructurados y plantillas de recolección de información, adaptados a las particularidades y necesidades de la organización, contribuye a sistematizar el proceso de identificación.

- Uso de herramientas que permitan realizar un mapeo automatizado.
  - » Herramientas de inventario y gestión de activos tecnológicos.
  - » Escanear repositorios de código para detectar librerías de IA.
  - » Uso de herramientas de análisis de logs y tráfico de aplicaciones para detectar patrones de IA.
  - » Otro grupo de herramientas que pueden ser de ayuda son las de descubrimiento de datos sensibles que permiten identificar datos que pueden ser utilizados para entrenar sistemas de IA, pueden ayudar no solo en la fase de descubrimiento sino en tomar decisiones informadas sobre la gestión y control de sus sistemas de IA gracias a los informes detallados que generan.

4. Registro



- Crear un inventario centralizado con los siguientes atributos:
  - » Descripción del sistema.
  - » Propósito y uso.
  - » Datos que procesa.
  - » Responsables.
  - » Nivel de Riesgo (alto, limitado, mínimo) conforme a la RIA.
  - » Posibles medidas adicionales de gestión.

5. Despliegue

- Capacitar a los equipos sobre la importancia del descubrimiento de IA y las obligaciones regulatorias.
- Comunicar los resultados y el inventario a las partes interesadas relevantes.

6. Mantenimiento

- Establecer un programa de revisiones periódicas, siempre que sea posible de forma automática, para mantener actualizado el inventario.
- Integrar el proceso de inventariado en los ciclos de desarrollo y adquisición de tecnología.

4.2. Proceso de Recopilación Inicial de Datos

Una vez definidos el alcance y las técnicas de descubrimiento en el epígrafe anterior, es necesario operativizar la ingesta de información. A diferencia del registro formal, que se tratará en la fase 3, esta etapa es puramente de investigación y descubrimiento, donde la finalidad es disponer de un "pre-inventario" o una lista de información en bruto (respuestas de encuestas, listados de proveedores, entrevistas...) que permita segregar qué herramientas son meros automatismos y cuáles constituyen un sistema de IA sujeto a la aplicación del Reglamento IA.

Desde una perspectiva normativa, la falta de conocimiento sobre la existencia de un activo que utilice IA no exime a la organización de responsabilidad, por lo que es imprescindible establecer un proceso de recopilación que combine dos enfoques de forma concurrente: el institucional y el operativo/forense.

A continuación, se detallan las fases y requisitos para la recopilación de la información:

1. Instrumentación de la recogida de información

Para garantizar la homogeneidad de la información obtenida a través de los canales definidos en el punto 4.1, se establecerán dos mecanismos de entrada estandarizados:

- **Descubrimiento manual:** dado que muchos responsables de negocio (u otro personal que forme parte de la plantilla de la organización) puede no ser consciente de que su software contiene IA, se habilitará un formulario de declaración inicial simplificado.

  En un primer momento, se deberá lanzar una campaña de identificación dirigida a los propietarios de procesos clave o susceptibles de utilizar herramientas de IA.

  A diferencia de la ficha registro final, este formulario debe centrarse en la funcionalidad del activo y debe tener un enfoque simple, es decir, debe contener preguntas como ¿Usas herramientas que ayuden a tomar decisiones de forma automatizada, generen texto/imágenes o clasifiquen datos automáticamente? y no preguntas de índole técnica.

- **Descubrimiento automatizado:** se deberá obtener reportes de herramientas de escaneo, segregando los activos por su naturaleza (librerías, APIs externas, Software SaaS, etc.).

  Además, en coordinación con las áreas correspondientes, se podrá analizar la actividad de red para identificar el acceso a dominios de IA públicos.

  De igual manera, si la organización dispone de un inventario de los activos tecnológicos, se podrá incorporar la etiqueta de IA a ese listado para que los responsables de tecnología de cada uno de los activos puedan cumplimentarlo en las futuras revisiones.

2. Triaje y validación

Una vez detectada una herramienta que sea susceptible de utilizar IA y de ser categorizada como un sistema IA, se debe realizar una calificación preliminar antes de iniciar el proceso completo de alta en la base de datos centralizada.

Este triaje deberá contener, como mínimo, las siguientes cuatro preguntas para determinar la necesidad de inventariarlo en la base de datos centralizada y si debe comunicarse su uso y funcionalidad a otras áreas interesadas:

- **¿Es IA según la definición establecida en el RIA?**
- **¿Existe tratamiento de datos de carácter personal en los términos establecidos en el Reglamento General de Protección de Datos?**
- **¿Existe tratamiento de información corporativa confidencial?**
- **¿Es un sistema IA tradicional o generativo?**

Una vez obtenida la información anterior, se excluirán del inventario de IA aquellos sistemas basados en automatismos simples que no cumplan la definición del RIA. Igualmente, deberá atenderse a la definición establecida por la Comisión Europea en sus directrices sobre la definición de sistemas de IA.

Asimismo, se debe distinguir entre una "librería" de código y el propio sistema IA funcional que la utiliza. El inventario debe registrar este último, no cada uno de sus componentes individuales.

3. Gestión de los activos ocultos o Shadow AI

Durante el proceso de recopilación inicial, es posible que surjan discrepancias entre lo declarado por las áreas de negocio y lo detectado por herramientas técnicas.

La detección de Shadow AI (sistemas de IA no autorizados o fuera del inventario oficial) representa un desafío crítico para la seguridad y el cumplimiento. El descubrimiento de estos activos ya sea mediante el análisis de logs de red, escaneo de librerías o reportes de proveedores, debe activar un protocolo de respuesta inmediata para evitar la exposición a riesgos de Riesgo Prohibido o brechas de datos personales.

Para regularizar los casos anteriores, se procederá de la siguiente manera:

1. Verificación: se debe confirmar que el tráfico corresponde a un proceso de negocio recurrente y no a usos personales o pruebas puntuales.

2. Responsabilidad Técnica del bloqueo urgente o preventivo: el CISO (o Responsable de Seguridad de la Información) tiene la autoridad técnica delegada para ejecutar el bloqueo cautelar de forma inmediata cuando se detecte un flujo de datos hacia sistemas de IA externos que no cuenten con un contrato de confidencialidad validado o que presenten riesgos.

3. Responsabilidad de Gobierno: el Comité de IA (o la estructura de gobernanza definida en la fase 3) es el órgano que ratifica o levanta dicho bloqueo tras un análisis de impacto rápido.

4. Criterio de Intervención: El bloqueo se aplicará por defecto si el sistema detectado interactúa con datos de categoría especial o información corporativa restringida sin supervisión humana documentada. Una vez identificada la herramienta a través del triaje preliminar, se aplicará una de las siguientes medidas en función de la criticidad detectada:

- **Bloqueo Total Inmediato:** aplicable a herramientas que incurran en Prácticas Prohibidas (ej. puntuación social, categorización biométrica no autorizada) o sistemas GenAI que no permitan el filtrado de datos confidenciales.
- **Supervisión Reforzada (*Shadow Watching*):** si la herramienta es valiosa para el negocio y el riesgo es moderado, se permite su uso temporal bajo monitorización estricta del tráfico, mientras el responsable del departamento inicia el proceso de alta formal.
- **Regularización Acelerada:** para sistemas de Riesgo Mínimo (p. ej. correctores gramaticales), se omitirá el bloqueo y se procederá directamente a la inscripción de oficio en el inventario provisional.

5. Regularización: para convertir un activo oculto en uno gestionado, se propone este ciclo:

- **Identificación del Propietario:** se localizará al responsable del área que ha implementado el uso para asignarle el rol de Responsable de Negocio en el inventario.
- **Evaluación Retroactiva:** el responsable deberá cumplimentar la Plantilla de Recolección y, si el sistema se clasifica como de Alto Riesgo, se deberá ejecutar un FRIA y un Expediente Técnico de forma prioritaria antes de retirar el bloqueo cautelar.
- **Decisión Final:** si el sistema vulnera las políticas de IA Responsable de la organización o no ofrece garantías de transparencia (**Art. 50 RIA**), el Comité de IA decretará la prohibición formal y el bloqueo técnico definitivo.

4. Consolidación de la información

El resultado final de este proceso será la obtención de un “pre-inventario” validado. Este documento contendrá únicamente los sistemas que han superado los filtros indicados anteriormente y que podrán ser sometidos a las evaluaciones de riesgos correspondientes y su posterior registro definitivo.

Herramientas y Plantillas para la Recolección

4.3.

Para garantizar la integridad y la calidad jurídica de la información recabada, además de reducir el riesgo de errores en la posterior clasificación de riesgo, resulta imprescindible estandarizar los instrumentos de captura de datos.

Con esta misión, se propone la utilización de una plantilla estandarizada diseñada para ser cumplimentada por usuarios de negocio sin perfil técnico. En cuanto a la estructura de la plantilla, se recomienda incluir los siguientes bloques de información:

1. Bloque funcional

Este epígrafe permitirá obtener la información necesaria para conocer qué hace y para qué se utiliza la herramienta.

En particular, se deberá registrar:

- Descripción de los datos de entrada (*input*) y del resultado generado (*output*)
- Nivel de autonomía (el sistema ofrece una recomendación o ejecuta una acción directamente)

2. Bloque de datos/información

En este bloque se deberá incluir los datos personales que son utilizados (identificativos y de contacto, económicos, etc.), así como los colectivos afectados (clientes, empleados, etc.).

Además, también se deberá indicar si existe utilización de información confidencial o restringida o sujeta a derechos de propiedad intelectual o industrial.

3. Bloque de origen

Se deberá incorporar información relativa al origen de la herramienta de IA, esto es, si se trata de una aplicación interna o externa.

En caso de tratarse de una aplicación externa deberá identificarse también al proveedor y el rol que tiene.

Toda la información obtenida deberá volcarse en un repositorio único (base de datos provisional) antes de pasarse al inventario oficial. Para ello, la plantilla de recolección deberá contar con los siguientes datos identificativos (además de la información identificada anteriormente):

Campo	Descripción	Objetivo
ID	Código único temporal	Trazabilidad del expediente
Fuente	Entrevista con el departamento responsable / Factura de la compra del proveedor / Escaneo de red	Evidencia de la diligencia debida
Nombre de la herramienta	Nombre comercial o del desarrollo interno	Identificación del activo
Estado del triaje	Pendiente / Descartado (No IA) / Confirmado (Pasar a Fase 2) / Bloqueado	Gestión del flujo de trabajo
Observaciones de Riesgo	Notas preliminares (p. ej., posible transferencia int. de datos").	Alertas tempranas para el DPO u otros departamentos afectados

05.

DESARROLLO DE LA FASE 2: CLASIFICACIÓN Y EVALUACIÓN DE RIESGOS

5.1. Proceso de “Triaje” para Nuevos Casos de Uso

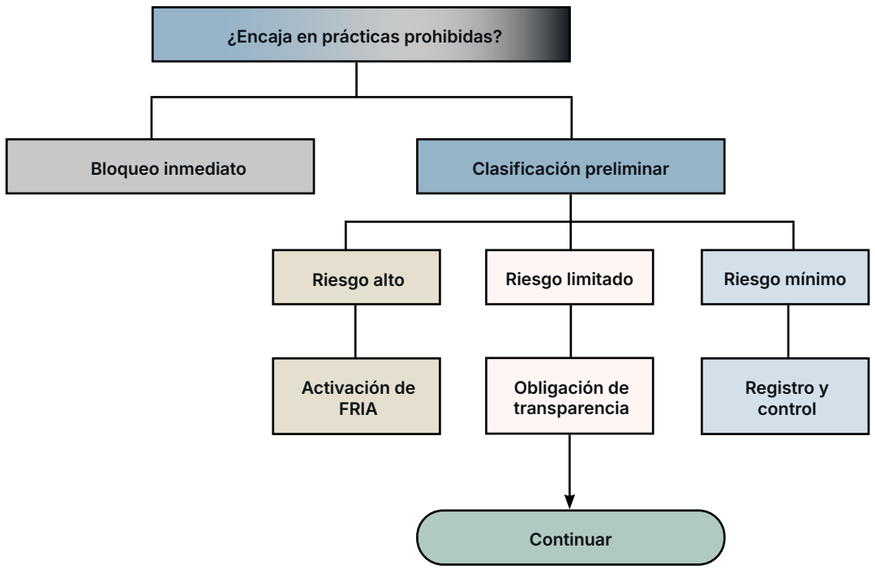
Ante la aparición de nuevos casos de uso es necesario realizar una clasificación rápida o triaje de dicho elemento, con el fin de evaluar si realmente se trata de un activo de IA o no para, en caso afirmativo, proceder a su clasificación.

A continuación, hay que confirmar que el caso de uso está alineado con la estrategia corporativa y no entra en actividades prohibidas por el RIA.

Finalmente, se fijará un nivel de riesgo, los cuales veremos en el siguiente apartado, que son los que realmente establecen los mecanismos de control necesarios.

En el anexo III se puede consultar un ejemplo de preguntas que podemos hacernos durante dicha fase, de cara a sistematizar la evaluación de riesgos.

Proceso de “Triaje”



5.2. Criterios de Clasificación de Riesgo según el RIA

Niveles de Clasificación

Tras el proceso de triaje detallado en el apartado 5.1, cada sistema se clasificará en uno de los cuatro niveles de riesgo definidos por la normativa europea:

- **Riesgo Prohibido:** sistemas que incurren en prácticas inaceptables, como la manipulación subliminal, la puntuación social o la categorización biométrica por atributos sensibles. Estos sistemas no pueden ser desplegados en ninguna circunstancia.
- **Alto Riesgo:** sistemas destinados a áreas críticas como la educación, el empleo (selección y supervisión de trabajadores), el acceso a servicios esenciales (bancarios, sanitarios) o infraestructuras críticas. Estos sistemas requieren obligatoriamente la Evaluación de Impacto sobre los Derechos Fundamentales (FRIA) descrita en el apartado 5.3. Se recomienda registrar en el inventario el cumplimiento de los requerimientos del RIA u otras normativas asociadas para los sistemas de alto riesgo, incluyendo el enlace a la Evaluación de Impacto sobre los Derechos Fundamentales.
- **Riesgo Limitado:** sistemas con obligaciones específicas de transparencia (p. ej. IA generativa, chatbots, deepfakes). Estos sistemas deben informar al usuario que está interactuando con una IA.
- **Riesgo Mínimo o Nulo:** aplicaciones que no presentan riesgos significativos para los derechos o la seguridad (p. ej. filtros de spam, juegos). No tienen obligaciones legales adicionales, aunque se recomienda seguir códigos de conducta voluntarios.

Adicionalmente, con el objetivo de que el inventario sirva como una herramienta de control y gestión de riesgos clara y visual, se pueden añadir otras clasificaciones:

- **Sistemas de Propósito General (GPAI):** se rigen por el Capítulo V **(Artículos 51 a 56)**. Si el sistema utiliza modelos como LLMs.
- **Sistemas de Inteligencia Artificial Generativa:** en determinadas compañías, el uso de estos sistemas está ampliamente extendido y su clasificación independiente en el Inventario puede ser muy útil para identificar, a nivel visual, las obligaciones asociadas y eventuales duplicidades en las funciones que llevan a cabo las herramientas.

¿Qué información incorporar en el registro en relación con esta clasificación?

Para que el inventario sea útil sin resultar burocrático, se recomienda registrar, en cada caso, la referencia al nivel de riesgo asociado a la normativa en el Inventario. Adicionalmente, en el caso en el que existan obligaciones adicionales asociadas a la implementación de determinados sistemas, también se recomienda mantener y registrar la evidencia de cumplimiento (por ejemplo, enlace al FRIA o a la EIPD correspondiente).

5.3. Evaluación de Impacto para Sistemas de Alto Riesgo

La Evaluación de Impacto para Sistemas de Alto Riesgo (“FRIA”, por sus siglas en inglés), que se recoge en el art. 27 del Reglamento, es un instrumento de control previo que permite comprender, antes del primer uso, cómo un sistema de IA puede afectar a las personas y qué medidas se aplicarán para reducir riesgos. En el marco del RIA, esta evaluación se vincula a la protección de los derechos fundamentales y se integra con otras obligaciones del ciclo de vida del sistema (por ejemplo, supervisión humana, gobernanza de datos, registros y transparencia).

Cuándo se exige y a quién aplica

El RIA establece la obligación de realizar una evaluación de impacto sobre derechos fundamentales antes del despliegue de determinados sistemas de IA de alto riesgo. En términos prácticos, el requisito se activa cuando concurren dos elementos:

- El tipo de responsable de despliegue (deployer): la obligación recae, con carácter general, sobre entidades públicas y sobre entidades privadas que prestan servicios públicos.
- El tipo de sistema de alto riesgo: la obligación se aplica a sistemas de alto riesgo en el sentido del RIA (art. 6.2), con dos matices relevantes:
  - » Existe una excepción para los sistemas de alto riesgo destinados a utilizarse en el ámbito de infraestructuras críticas (punto 2 del Anexo III).
  - » La obligación se aplica también, con independencia de ser o no entidad pública o prestadora de servicios públicos, a los responsables de despliegue de sistemas de alto riesgo en el ámbito de empleo, gestión de trabajadores y acceso al autoempleo en los supuestos previstos en los puntos 5(b) y 5(c) del Anexo III.

Este planteamiento refleja que el impacto en derechos fundamentales depende tanto de qué sistema se usa como de en qué contexto se usa y con qué efectos sobre decisiones y colectivos.

Qué debe incluir la evaluación	Elementos
El RIA enumera los elementos mínimos que deben recogerse, que se pueden estructurar como un relato breve apoyado por evidencias y anexos:	**Descripción del proceso en el que se usará el sistema conforme a su finalidad prevista:** qué fase del servicio o decisión afecta, qué entradas recibe, qué salidas produce y cómo se integran esas salidas en el procedimiento.
	Periodo y frecuencia de uso: desde cuándo se usará, con qué cadencia (continuo, por lotes, por demanda), y si el uso se limita a pilotos, campañas o situaciones concretas.
	Categorías de personas y grupos potencialmente afectados: no solo usuarios directos, también terceros que puedan verse influidos por una decisión o por una priorización, y colectivos que requieran atención específica (por ejemplo, por situación de vulnerabilidad).
	Riesgos específicos de perjuicio para esos grupos, teniendo en cuenta la información que facilita el proveedor (por ejemplo, instrucciones de uso y limitaciones conocidas).
	Cómo se implementa la supervisión humana: quién supervisa, en qué momentos, con qué información y con qué capacidad real de intervención.
	Medidas en caso de materialización del riesgo, incluyendo: • mecanismos de gobernanza interna (responsables, escalado, aprobación de cambios); • procedimientos de respuesta (suspensión, corrección, revisión de decisiones); • mecanismos de reclamación o canal para que las personas afectadas puedan plantear incidencias.

La evaluación debe ser operativa: describir el uso real del sistema y traducir los riesgos en medidas concretas. Adicionalmente, es útil reservar los detalles técnicos (métricas, umbrales, evidencias de prueba) para anexos o fichas del inventario.

Cómo llevarla a la práctica: una metodología en tres fases

Aunque el RIA fija un contenido mínimo, la práctica de las autoridades y proyectos piloto apunta a trabajar con una metodología de evaluación de riesgos que sea repetible y comparable. Un enfoque útil es organizar la evaluación en tres fases, de manera similar a metodologías de gestión de riesgos aplicadas a derechos fundamentales:

1. Planificación y alcance

En esta fase se concreta el “caso de uso” y se delimita el análisis:

- qué decisión o proceso se ve afectado.
- qué partes intervienen (equipo técnico, negocio/operación, área jurídica y de cumplimiento).
- qué documentación existe (ficha del sistema, información del proveedor, procedimientos internos, pruebas realizadas).
- qué versiones y configuraciones se evaluarán (por ejemplo, modelo, parámetros, conjunto de datos, reglas de negocio).

La finalidad no es describir toda la tecnología, sino fijar el perímetro para evitar una evaluación genérica.

2. Identificación y análisis de riesgos sobre derechos fundamentales

El análisis debe partir de los derechos potencialmente afectados en el contexto concreto (por ejemplo, no discriminación, privacidad, protección de datos, dignidad, libertad de información, derechos laborales). Dos criterios, alineados con metodologías públicas de evaluación de impacto en derechos fundamentales, ayudan a que el ejercicio sea consistente:

- **Analizar derechos de forma individual:** el impacto no se promedia. Un impacto relevante en un derecho no queda compensado por impactos menores en otros.
- **Relacionar cada riesgo con un escenario:** qué puede ocurrir, a quién afecta, con qué probabilidad y con qué gravedad, dejando constancia del motivo (evidencias, pruebas, histórico o experiencia del contexto).

En esta fase también se revisan elementos que suelen estar en el origen de los riesgos: calidad y representatividad de datos, sesgos, trazabilidad, límites de validez, dependencia de terceros, uso fuera del contexto previsto o cambios de finalidad.

3. Gestión y seguimiento de medidas

Una vez identificados los riesgos, se definen y verifican medidas de control, siguiendo un enfoque proporcionado al contexto de uso del sistema e incorporando mecanismos de supervisión humana, controles técnicos y organizativos y procedimientos de revisión[5].

En general, las medidas se reparten entre tres capas:

- **Diseño y configuración:** ajustes de umbrales, validaciones, restricciones de uso, controles de calidad de datos, explicaciones y registros.
- **Operación y supervisión:** puntos de control humano, formación de usuarios, procedimientos de revisión, pruebas periódicas, auditorías internas, gestión de incidencias.
- **Medidas para personas afectadas: i**nformación y transparencia en el punto de contacto, mecanismos de reclamación, revisión de decisiones cuando sea aplicable y medidas correctoras.

La evaluación se cierra con un plan de seguimiento: qué indicadores se revisarán, con qué frecuencia, quién aprueba cambios y qué desencadena una reevaluación.

[5] AESIA, *Guía de gestión de riesgos*; AESIA, *Guía de vigilancia humana*

Relación con la EIPD y otras evaluaciones

En muchos despliegues, la evaluación de impacto sobre derechos fundamentales se relaciona con la **Evaluación de Impacto en Protección de Datos (EIPD/DPIA)**. El RIA prevé expresamente que, si parte de las obligaciones ya se cumple mediante una EIPD, la evaluación de derechos fundamentales **la complementa**, evitando duplicidades, pero asegurando que el análisis no se limite a privacidad y protección de datos.

En la práctica, esto permite:

- reutilizar descripciones de procesos, mapas de datos, medidas de seguridad y roles;
- ampliar el análisis a otros derechos (por ejemplo, igualdad, libertad de información, derechos laborales) y a escenarios que no dependen del uso de datos personales;
- alinear decisiones de mitigación para que no haya medidas contradictorias.

Documentación, actualización y comunicación de resultados

La evaluación debe conservarse vinculada al inventario del sistema (o integrada en él) y mantenerse en versión controlada. No es un documento “de una sola vez”. Si cambian elementos relevantes o dejan de estar actualizados, el responsable de despliegue debe actualizar la evaluación.

Como regla práctica, conviene revisarla cuando se produzca alguno de estos cambios:

- modificación sustancial del modelo, del proveedor o de la configuración;
- ampliación de finalidad o cambio de contexto (por ejemplo, otro colectivo, otro servicio);
- cambios en los datos de entrada o en su procedencia;
- incidentes, quejas o patrones de error detectados;
- nuevas guías o especificaciones aplicables.

Por último, una vez realizada la evaluación, el artículo 27 prevé la notificación de sus resultados a la autoridad de vigilancia del mercado mediante el cuestionario o plantilla que desarrollará la AI Office. El propio artículo contempla que, en el supuesto previsto en el artículo 46(1), los responsables de despliegue pueden quedar exentos de la notificación.

En resumen, la evaluación de impacto para sistemas de alto riesgo permite pasar de una clasificación normativa a un análisis práctico del uso: qué derechos pueden verse afectados, qué escenarios hay que evitar y qué controles deben sostenerse durante toda la vida del sistema.

06.

DESARROLLO DE LA FASE 3: DOCUMENTACIÓN Y REGISTRO

6.1. Consolidación en una Base de Datos Centralizada

El **Inventario de Sistemas y Servicios de IA** es el instrumento jurídico de rendición de cuentas (*accountability*) de la organización. Por ello, una base de datos centralizada debe actuar como fuente única de información sobre los sistemas desarrollados, utilizados e implementados.

Su arquitectura debe estar diseñada de tal forma que pueda responder (en tiempo real y con evidencia documental) a preguntas como: ¿cuántos sistemas IA están operativos en la infraestructura de la organización?, ¿cuál es su finalidad exacta? y ¿quién es el responsable interno de su supervisión y control? Para alcanzar este fin, su alimentación debe ser sistémica y estar vinculada con el ciclo de vida del desarrollo de sistemas IA.

De esta manera, la base de datos permitiría demostrar ante auditores, reguladores y las demás partes interesadas que la organización ejerce un control efectivo y diligente sobre sus sistemas IA, conociendo toda la información relevante y necesaria para asegurar el cumplimiento normativo.

La creación de este registro centralizado está fundamentada en los siguientes principios y/o requisitos legales:

- **Transparencia y trazabilidad:** es fundamental para gestionar las obligaciones aplicables a los sistemas y demostrar que la organización conoce el uso previsto y las limitaciones de sus herramientas.
- **Gestión de riesgos:** el primer paso para gestionar los posibles riesgos asociados es establecer el contexto y mapear el sistema, sus actores e impactos. Por tanto, la base de datos es el soporte de un sistema de gestión de riesgos de inteligencia artificial confiable.
- **Conexión con otras normativas:** el inventario debe estar conectado, en su caso, con otras normativas como el Reglamento General de Protección de Datos (RGPD), de tal forma que permita relacionar la finalidad del sistema con la actividad de tratamiento recogida en el Registro de Actividades de Tratamiento (RAT).

Es fundamental que el sistema IA esté vinculado con sus componentes críticos y estos estén identificados en un mismo registro: el/los modelos subyacentes, los conjuntos de datos de entrenamiento/validación y los casos de uso de negocio asociados a cada uno de ellos.

Para garantizar la integridad de este registro, la base de datos se debe estructurar en torno a tres (3) pilares fundamentales: identidad del sistema, taxonomía del riesgo y ciclo de vida.

1. Campos críticos de identificación

Cuando se requiera incorporar un nuevo registro en el inventario (o modificar uno existente), se debe cumplimentar obligatoriamente una "Ficha registro" sobre el sistema IA que contenga la información básica y esencial. La ausencia de la información en esta ficha debe impedir el paso del sistema a una fase de producción.

A continuación, se detalla la información mínima imprescindible que debería contener:

- **Identificación:**
  - » Identificador único del sistema (ID): se asignará un código alfanumérico inmutable a cada sistema. Esto es vital para diferenciar entre sistemas similares y mantener la trazabilidad a lo largo del tiempo, especialmente cuando los nombres comerciales cambian.
  - » Nombre del sistema
  - » Versión
  - » Interno/Externo. En caso de ser externo, identificar el proveedor.
- **Finalidad y alcance:**
  - » Uso previsto del sistema: desde una perspectiva del Reglamento, este es uno de los campos más críticos del inventario ya que la clasificación de riesgo del sistema depende casi exclusivamente de la finalidad del mismo.

    Este campo debe ser lo suficientemente específico para que sea posible clasificar el sistema en los distintos niveles de riesgo del Reglamento IA, por lo que se deben evitar generalidades como "mejorar la eficiencia".
  - » Áreas de negocio que lo utilizan
- **Clasificación del riesgo:**
  - » Nivel de riesgo con base en el Reglamento IA
  - » Nivel de criticidad interna
- **Gobernanza:**
  - » Rol de la organización: se debe marcar claramente si se actúa como proveedor o responsable del despliegue, importador o distribuidor.
  - » Responsable técnico del sistema
  - » Responsable de negocio
- **Estado del ciclo de vida:** el inventario debe permitir registrar hallazgos en estados previos a la aprobación, por ejemplo: "detectado" (investigación), "en evaluación" (FRIA en curso), "aprobado" (piloto), "en producción" o "retirado".

2. Taxonomía de clasificación de riesgos

Para operacionalizar el cumplimiento, todo sistema que conste en la BBDD debe ser etiquetado bajo una de las categorías de riesgo que haya definido la organización. Esta clasificación disparará automáticamente los flujos de trabajo de cumplimiento requeridos.

3. Gobernanza, trazabilidad y accountability

La naturaleza evolutiva de la IA requiere disponer de un proceso de actualización procedimentado.

- **IA por diseño** (***AI by design***) (alta del sistema): ningún sistema debería entrar en producción sin haber completado su ficha en la BBDD centralizada y haber obtenido el visto bueno de los departamentos afectados.

  Asimismo, si un sistema sufre una modificación sustancial (p. ej., un cambio en la arquitectura, cambio de finalidad, etc.) el inventario debería generar una nueva versión del sistema y, en caso de ser necesario, reevaluar el mismo.
- **Mantenimiento:** debería establecerse una serie de disparadores para la actualización obligatoria de la BBDD, por ejemplo: ante cambios sustanciales en el algoritmo, el uso de nuevos sets de datos, o el cambio en la finalidad del sistema IA.
- **Auditorías periódicas:** los roles de cumplimiento deben realizar un muestreo aleatorio y periódico para verificar que lo registrado en la BBDD coincide con el uso real que le está dando negocio.

En relación con lo anterior, el inventario también debería incorporar un registro de *logs* indicando dónde se almacenan los logs automáticos de actividad del sistema, pues son la prueba forense que permitirá a la organización reconstruir la "decisión" de la IA en caso de litigio, demostrando trazabilidad.

6.2. Vinculación con Documentación de Cumplimiento (FRIA, Expediente Técnico)

El propósito de la vinculación documental consiste en asegurar que cada sistema de inteligencia artificial inventariado se relaciona de forma clara y verificable con los documentos requeridos para el cumplimiento normativo. Esto facilita la trazabilidad y la supervisión de las obligaciones legales y técnicas de los sistemas, permitiendo una gestión transparente y eficiente.

Formulario de Revisión de Impacto de Riesgos de la IA (FRIA)

El FRIA, o Formulario de Revisión de Impacto en Derechos Fundamentales, es una herramienta clave para garantizar que los sistemas de inteligencia artificial no vulneren los derechos y libertades de las personas que los utilizan o se ven afectados por ellos. Este procedimiento examina de forma sistemática los riesgos que puede presentar un sistema de IA, prestando especial atención a cuestiones como los derechos fundamentales, la existencia de sesgos, el impacto social, la seguridad y la fiabilidad.

El proceso FRIA, de acuerdo con el RIA y sus guías, debe abarcar varios puntos esenciales: describir para qué se va a utilizar el sistema, identificar los grupos de personas que pueden verse afectados, analizar los posibles escenarios de riesgo, estimar la probabilidad y gravedad de los posibles daños, y detallar las medidas para mitigar esos riesgos y el riesgo residual que permanece tras aplicar las medidas.

Todo este análisis se registra en el inventario de sistemas de IA, que facilita la gestión del cumplimiento normativo al guardar el estado de la FRIA (por ejemplo, en curso, finalizada o pendiente) y vincularla con la versión correspondiente del expediente técnico. De esta manera, cualquier responsable de supervisión puede acceder fácilmente a la documentación, comprobar el grado de cumplimiento y asegurarse de que se están siguiendo las obligaciones legales y procedimientos internos.

El FRIA es fundamental para identificar y valorar los riesgos que los sistemas de IA pueden suponer para los derechos fundamentales. Permite definir quiénes pueden verse afectados, en qué escenarios hay mayor riesgo y qué medidas deben tomarse para reducirlo al mínimo posible. Junto con el expediente técnico, que recoge toda la información sobre diseño, funcionamiento y seguridad del sistema, y el inventario, que mantiene todo actualizado y accesible, el FRIA ayuda a asegurar una gestión responsable y transparente de los sistemas de IA en la organización.

Ejemplo resumido:

Un sistema de IA para selección de personal se clasifica como de alto riesgo y se somete a un FRIA, que identifica posibles sesgos por género o nacionalidad, evalúa el impacto en el acceso al empleo y documenta medidas como ajustes en los datos, métricas de equidad y revisión humana obligatoria de las decisiones. Otro ejemplo, un sistema de recomendación de contenidos implementado por una entidad educativa queda registrado en el inventario. se adjunta la FRIA finalizada, que detalla las medidas adoptadas para proteger la privacidad de estudiantes, y se enlaza el expediente técnico actualizado, que incluye una descripción de los algoritmos y conjuntos de datos empleados. Este modelo permite revisar fácilmente el historial de cumplimiento y las acciones tomadas.

Expediente Técnico

El expediente técnico es el conjunto documental que recoge toda la información esencial sobre cada sistema de inteligencia artificial. Su objetivo es garantizar que el sistema cumple con las normativas y estándares, especialmente el RIA, proporcionando evidencia clara de cómo ha sido diseñado, entrenado, probado y gestionado. En este expediente se incluyen detalles sobre el propósito del sistema, su arquitectura técnica, los datos utilizados y su gobernanza, los procesos de entrenamiento y validación, el control de riesgos, la supervisión humana, las medidas de seguridad y ciberseguridad, la gestión de cambios, así como la documentación complementaria. Así, el expediente técnico facilita la evaluación, seguimiento y supervisión del sistema, asegurando transparencia y trazabilidad en todas las fases de su ciclo de vida.

En resumen, este documento sirve para demostrar que el sistema de IA ha sido desarrollado y operado de manera responsable, transparente y conforme a la regulación vigente, permitiendo a los responsables de cumplimiento y supervisión acceder fácilmente a toda la información relevante para tomar decisiones y garantizar la seguridad y fiabilidad del sistema.

Ejemplo resumido:

En un sistema de diagnóstico médico basado en IA, el expediente técnico documenta la arquitectura del modelo, los conjuntos de datos médicos anonimizados, las métricas de rendimiento, las pruebas de robustez y la supervisión clínica, todo enlazado al registro del sistema en el inventario.

Documentación complementaria

Además de FRIA y Expediente Técnico, se recomienda vincular:

- **Actas del comité ético o de cumplimiento.**
- **Informes de auditoría y revisiones regulatorias.**
- **Políticas de transparencia, explicabilidad y gestión de incidentes.**
- **Registros de supervisión humana, monitorización continua y planes de mejora.**

Ejemplo de tabla de inventario de IA

ID Sistema	Descripción	Clasificación (RIA)	Documentación asociada	Responsable	Estado
IA-001	Diagnóstico radiológico basado en redes neuro-nales	Alto riesgo	FRIA-001, ExpTec-001, Auditoría-2025	Dpto. IA Clínica	Activo
IA-002	Chatbot de atención al cliente	Riesgo limitado	FRIA-002, ExpTec-002	Cumplimiento Digital	En revisión
IA-003	Motor de recomendación web	Riesgo alto	FRIA-003, ExpTec-003, Comité Ético-2025	Tecnología y Legal	Validado

Esta estructura es coherente con buenas prácticas de plantillas de documentación técnica y kits de cumplimiento AI/ISO publicados por terceros especializados.

Procedimiento interno de uso del inventario

En el documento se podría añadir un apartado tipo “Procedimiento” con pasos como:

- Identificación de nuevo sistema de IA.
- Registro inicial en el inventario con un ID único.
- Elaboración del FRIA y del Expediente Técnico.
- Revisión y aprobación por comité interno.
- Actualización del inventario ante cambios significativos o nuevas versiones.

Este flujo se inspira en guías prácticas de documentación y gestión del ciclo de vida de IA para cumplimiento del RIA.

6.3. Conexión con Registros Oficiales y Obligaciones Regulatorias

El inventario debe garantizar un alineamiento normativo de los servicios y sistemas de IA con los registros oficiales y las obligaciones del RIA.

- **Registro en la UE (Art. 71):** los sistemas clasificados como alto riesgo se registrarán en la base de datos europea antes de su puesta en el mercado o en servicio. La ficha del sistema incluirá el EU AI Database Registration ID, fecha, versión y enlace al expediente técnico.
- **Vigilancia e incidentes (Art. 72):** se mantendrá un sistema de vigilancia postcomercialización, con indicadores, umbrales y canal de reporte de incidentes graves a la autoridad competente/AI Office. Las notificaciones quedarán enlazadas a la ficha del inventario.
- **FRIA (Art. 27):** cuando la organización actúe como deployer público o prestador de servicios públicos, o en los supuestos del Anexo III, se realizará antes del primer uso una Evaluación de Impacto en Derechos Fundamentales, registrando en la ficha su estado, riesgos y medidas.
- **Transparencia (Arts. 13 y 50):** cada ficha documentará los avisos a usuarios/personas expuestas, el marcado de contenidos sintéticos y los materiales de uso seguro proporcionados por el proveedor.
- **Modelos GPAI y de riesgo sistémico:** cuando aplique, la ficha reflejará las obligaciones de transparencia y seguridad reforzada, y utilizará la plantilla de “incidente grave GPAI” publicada por la Comisión. Estrategia Digital Europea
- **Coordinación con NIS2:** si un incidente afecta a la continuidad/seguridad de servicios esenciales/importantes, se activará la notificación NIS2 al CSIRT/ autoridad en los plazos establecidos, además de las obligaciones del RIA.

La conexión con registros oficiales y obligaciones regulatorias garantiza que cada sistema o servicio de inteligencia artificial inventariado cumple las exigencias establecidas por el RIA y, cuando corresponda, por otras normas europeas como NIS2. Este apartado permite mantener una trazabilidad completa entre el sistema interno y sus obligaciones regulatorias externas, incluyendo registros públicos, evaluaciones obligatorias, notificaciones de incidentes y controles de transparencia.

En primer lugar, debe identificarse si el sistema entra dentro de la definición legal de “sistema de IA” del RIA, registrando en el inventario tanto el veredicto (Sí/No) como la justificación técnica y funcional basándose en las directrices emitidas por la Comisión Europea. A continuación, el sistema debe clasificarse en la categoría regulatoria correspondiente: no regulado, IA de riesgo limitado, IA de alto riesgo, o Modelo de Propósito General (GPAI), incluyendo si corresponde a un modelo de riesgo sistémico. Esta clasificación determina si existen obligaciones adicionales de registro, transparencia o vigilancia.

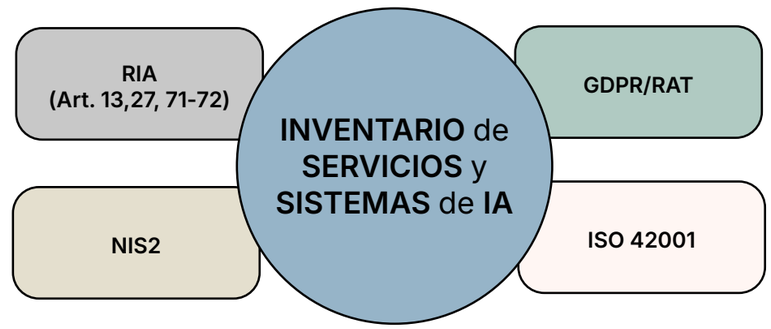
Cuando el sistema se clasifique como alto riesgo, debe cumplirse la obligación de registro en la Base de Datos Europea de IA (Art. 71 del RIA). En el inventario debe consignarse el EU AI Database Registration ID, el estado del registro (borrador, enviado, aprobado), la fecha de presentación y la referencia al expediente técnico presentado. Este identificador actúa como enlace oficial entre el sistema interno y su huella regulatoria en la Unión Europea.

Asimismo, los sistemas de alto riesgo deben contar con un mecanismo de vigilancia post-comercialización conforme al Artículo 72. El inventario debe reflejar el esquema de monitorización, los indicadores utilizados, los umbrales, la fecha de la última revisión y el área responsable del seguimiento continuo. Cualquier incidente grave relacionado con el funcionamiento del sistema debe quedar documentado, indicando el número de referencia del incidente notificado a la autoridad competente, la fecha de envío, el estado del expediente y las medidas correctivas adoptadas. Si el sistema es un modelo GPAI o un modelo con “riesgo sistémico”, el inventario debe indicar también si se ha utilizado la plantilla y directrices de reporte de incidentes específicas para GPAI publicadas por la Comisión.

Para los casos en los que la organización actúa como deployer y está sujeta al Artículo 27 (por ser una entidad pública o una entidad privada que presta servicios públicos), es obligatorio realizar una Evaluación de Impacto en Derechos Fundamentales (FRIA) antes del primer uso del sistema. En el inventario debe registrarse si la FRIA es requerida, su estado, los riesgos identificados, las medidas de mitigación previstas y la ubicación documental del informe.

El inventario también debe recoger todas las obligaciones de transparencia de los Artículos 13 y 50 del RIA, indicando qué información se proporciona a usuarios y personas expuestas, si el sistema genera contenido sintético y cómo se marca, así como el manual o instrucciones de uso seguro proporcionado por el proveedor para garantizar un uso conforme.

Cuando el sistema forme parte de servicios cubiertos por la Directiva NIS2, cualquier incidente de ciberseguridad relevante debe notificarse tanto por la vía NIS2 como, cuando proceda, por la vía del RIA. El inventario debe reflejar esta conexión incluyendo si el sistema es crítico para servicios esenciales o importantes, el CSIRT competente, los plazos aplicables a la notificación y el número de referencia del incidente registrado bajo NIS2.



07.

DESARROLLO DE LA FASE 4: MONITORIZACIÓN Y MANTENIMIENTO

7.1. Procedimientos para la Actualización del Inventario

Mantener un inventario de sistemas y servicios de inteligencia artificial actualizado es un elemento esencial para una adecuada gestión de riesgos dentro de las organizaciones y para el cumplimiento normativo. En la práctica, se trata de una acción básica alineada con marcos como el Reglamento (UE) 2024/1689 (Ley Europea de Inteligencia Artificial), la norma ISO/IEC 42001:2023 y el NIST AI Risk Management Framework.

El procedimiento de mantenimiento del inventario de inteligencia artificial es transversal y aplicable a organizaciones de cualquier sector. Su principal objetivo es garantizar que la información documentada refleje en todo momento la realidad de los sistemas de IA utilizados por la organización, de modo que exista una trazabilidad completa que permita conocer qué sistemas de IA existen, cuál es su propósito, qué criticidad tienen para el negocio y qué controles se aplican.

Etapas del proceso de actualización del inventario

A continuación, se describe cada una de las fases, los eventos que desencadenan la actualización, la frecuencia de las revisiones y la integración con otros procesos dentro de la organización.

Detección e incorporación de nuevos sistemas

Esta fase tiene como objetivo identificar y registrar los sistemas de IA existentes en la organización, incluyendo aquellos que no figuran de forma formal. La identificación de estos sistemas es indispensable para mantener un inventario actualizado. Para llevar a cabo esta identificación, se puede utilizar un enfoque descendente (top-down), un enfoque ascendente (bottom-up) o una combinación de ambos para obtener una visión completa. Por un lado, el enfoque descendente consulta a las unidades de negocio con el objetivo de identificar usos de IA. Por otro lado, el enfoque ascendente analiza infraestructuras tecnológicas y componentes para detectar servicios o soluciones que incorporen IA. Además, se alinean los procesos de adquisición de software y servicios con el inventario; en algunas organizaciones, la detección se refuerza incluyendo apartados específicos sobre uso de IA en formularios o cuestionarios de seguridad dirigidos a proveedores. Como medida complementaria, y para reducir el riesgo de usos no inventariados, puede apoyarse la identificación con mecanismos internos de descubrimiento y revisión de activos/servicios. Una vez identificados, cada sistema se registra en el inventario si todavía no se encuentra incluido, creando una ficha con la información descrita en los capítulos anteriores.

Revisión periódica planificada

El inventario requiere revisiones periódicas, ya que el contexto de los sistemas de IA evoluciona constantemente en el tiempo. Por este motivo, se define una frecuencia de revisión para cada sistema registrado. En las organizaciones, es habitual ajustar esa frecuencia en función del nivel de riesgo de cada sistema y de los recursos disponibles:

- **Sistemas de IA de alto riesgo:** revisión trimestral.
- **Sistemas de IA de riesgo limitado:** revisión semestral.
- **Sistemas de IA de riesgo mínimo:** revisión anual, evitando que un sistema relevante pase más de un año sin revisión formal.

Adicionalmente, antes de una modificación significativa en un sistema de IA, se realiza una revisión específica para asegurar que la información del inventario se encuentra actualizada. Durante cada revisión periódica, la persona responsable del sistema actualiza y comprueba que la información del inventario es correcta y verifica el estado de las acciones definidas en revisiones anteriores.

Actualización por cambios significativos

Además de las revisiones planificadas, el inventario se actualiza cuando se producen determinados eventos. Estos eventos, denominados desencadenantes de actualización, se definen previamente con el objetivo de asegurar una aplicación homogénea. De acuerdo con las prácticas habituales, se consideran desencadenantes de actualización los siguientes:

- **Reentrenamiento o nuevas versiones del modelo**: cuando un sistema de IA se reentrena con nuevos datos o se sustituye por una nueva versión; cada versión se trata como una evolución relevante del sistema y requiere actualizar la información del modelo.
- **Incorporación de nuevas fuentes de datos:** cuando el sistema comienza a utilizar datos adicionales o diferentes; se actualiza la información relativa a los datos tratados y a las implicaciones normativas asociadas, incluyendo posibles cambios en la clasificación de datos y el riesgo del sistema.
- **Extensión a nuevas geografías o colectivos de uso:** cuando un sistema amplía su ámbito de uso a nuevas ubicaciones geográficas o a nuevos grupos de usuarios; se actualiza la información relacionada con la normativa aplicable.
- **Cambio de proveedor o componentes externos:** cuando el sistema depende de servicios externos y se produce un cambio de proveedor, de condiciones contractuales o de componentes tecnológicos; se actualiza la información del sistema de IA.
- **Deterioro de rendimiento o detección de incidentes:** cuando la supervisión identifica una degradación relevante del rendimiento o la aparición de incidentes recurrentes; la situación se registra y, una vez aplicadas medidas de mitigación o correctoras, la información se actualiza nuevamente.
- **Cambios normativos o en políticas internas:** cuando entra en vigor una nueva normativa o se aprueban políticas internas que afectan a los sistemas de IA; la información se actualiza para reflejar dichos cambios.
- **Deriva del Modelo (*Model Drift*):** Más allá de la degradación súbita del rendimiento, la organización debe monitorizar y registrar la deriva de modelo como un desencadenante crítico de actualización del inventario. La deriva representa una pérdida de alineación entre la lógica interna del sistema y la realidad de los datos de producción, lo que puede transformar un sistema de "Riesgo Mínimo" en un generador de sesgos o errores imprevistos. Esta deriva puede darse de dos formas principalmente:
  - **Deriva de Concepto (*Concept Drift*):** Se produce cuando las propiedades estadísticas de la variable objetivo cambian. Si el contexto en el que se basa la "decisión" de la IA evoluciona, el Expediente Técnico original deja de ser representativo del funcionamiento real.
  - **Deriva de Datos (Data Drift / Covariate Shift):** Ocurre cuando la distribución de los datos de entrada en producción difiere significativamente de los datos utilizados durante el entrenamiento o la validación. Esto requiere una actualización inmediata en la ficha de Trazabilidad y Monitorización.

La identificación de estos desencadenantes permite que el inventario refleje la situación actual de los sistemas de IA, reduciendo el riesgo de información desactualizada y reforzando la gestión permanente a lo largo del ciclo de vida del sistema.

Sistema de Registro de Incidentes y Fallos

7.2.

Mantener un sistema de registro de incidentes y fallos asociado a los sistemas de inteligencia artificial es un elemento esencial para sostener la monitorización y el mantenimiento del inventario en el tiempo. En la práctica, este registro permite disponer de trazabilidad sobre eventos relevantes, facilitar el análisis posterior y asegurar que, una vez aplicadas medidas de mitigación o corrección, la información del inventario se actualiza para reflejar la situación real del sistema.

En este contexto, se consideran incidentes o fallos aquellos sucesos que derivan en una degradación apreciable del rendimiento, comportamientos anómalos, indisponibilidades, errores recurrentes o impactos no previstos en el servicio. Además, cuando un incidente, evidencia cambios relevantes en el sistema, en los datos o en el contexto de uso, su registro se convierte en un desencadenante de actualización del inventario, manteniendo coherencia con el procedimiento descrito en el apartado 7.1 (actualización por cambios significativos).

Para que el proceso sea eficaz y sostenible, el registro de incidentes se integra con los procesos corporativos ya existentes, especialmente con la gestión de cambios, la gestión de riesgos y el gobierno de datos y seguridad de la información. De este modo, los eventos relevantes asociados a un sistema de IA quedan documentados y enlazados con su ficha en el inventario, evitando que el seguimiento dependa de canales informales o quede disperso entre equipos.

Con carácter general, cada registro debe aportar información suficiente para reconstruir el suceso y facilitar su seguimiento. Alineado con las necesidades de trazabilidad y monitorización, resulta habitual incluir al menos: fecha y hora, impacto, análisis de causa raíz, medidas de mitigación, notificación a terceros o regulador cuando proceda, y lecciones aprendidas. Esta información se vincula a evidencias disponibles (por ejemplo, tickets, registros operativos, informes o métricas) para facilitar la verificación posterior y reforzar la trazabilidad del inventario.

En cuanto al tratamiento operativo, el registro se apoya en un flujo sencillo y repetible: detección y registro del evento, triaje y priorización, análisis, aplicación de medidas correctivas y verificación, y cierre. La persona responsable del sistema lidera el seguimiento, coordinándose con los equipos técnicos, de seguridad y de cumplimiento cuando el impacto lo requiera. Una vez controlado el incidente y aplicadas las medidas correctoras, se actualiza la ficha del sistema en el inventario, de forma que la información refleje el estado actual del sistema y las acciones adoptadas.

Cuando el sistema dependa de un proveedor o componente externo, el registro se complementa con compromisos que aseguren la disponibilidad de evidencias y la notificación diligente. En particular, resulta relevante exigir:

- un sistema de registro de eventos con trazabilidad y acceso seguro para la organización.
- conservación de registros durante periodos prolongados cuando aplique.
- notificación de incidentes de seguridad o fallos críticos en plazos definidos, incluyendo detalle del incidente y medidas correctivas.

En definitiva, el sistema de registro de incidentes y fallos convierte eventos operativos en información gestionable y comparable entre sistemas, refuerza la supervisión y facilita que las actualizaciones del inventario se ejecuten de forma homogénea y verificable a lo largo del ciclo de vida del sistema.

Verificación, trazabilidad y mejora continua

Cada vez que se realiza una actualización del inventario, ya sea como resultado de una revisión planificada o de un desencadenante específico, se asegura la calidad y la trazabilidad de la información registrada. Esta etapa engloba, al menos, las siguientes prácticas:

- **Verificación de la información actualizada:** se comprueba que la actualización se ha realizado de forma completa y coherente; cuando procede, pueden incorporarse flujos de aprobación con validación por responsables de cumplimiento o gestión de riesgos.
- **Mantenimiento de un registro histórico de cambios:** la trazabilidad requiere conocer qué información se ha modificado, en qué momento y por quién; resulta relevante en auditorías al permitir demostrar la evolución controlada de los sistemas de IA.
- **Vinculación de evidencias y documentación:** cada entrada del inventario actúa como punto de acceso a información más detallada; por ello, se incorporan referencias a documentos relacionados (por ejemplo, registros de incidentes, evaluaciones y políticas aplicables) para facilitar la verificación.
- **Mejora continua del proceso:** de forma periódica, la organización revisa la eficiencia del proceso de mantenimiento del inventario, ajustándolo con base en la experiencia acumulada.

En síntesis, estas prácticas sostienen el ciclo de vida de la información del inventario: registro inicial, mantenimiento periódico, actualización ante cambios relevantes y mejora continua.

Integración con procesos existentes

Para que el proceso de actualización resulte eficaz y sostenible, se integra con los procesos corporativos ya existentes. Este enfoque evita duplicidades, reduce la carga operativa y facilita que el mantenimiento del inventario forme parte de la operativa habitual de la organización. Entre los principales procesos se incluyen los siguientes:

- **Gestión de cambios de TI:** el inventario se incorpora al ciclo de vida de desarrollo y despliegue; en los procesos de gestión de cambios se incluye una verificación específica para identificar si el cambio afecta a un sistema de IA y si la información del inventario requiere actualización.
- **Gestión de riesgos y cumplimiento:** el inventario actúa como fuente confiable de información y punto de enlace con estos procesos; una vez identificado el sistema de IA, su nivel de riesgo se evalúa manteniendo alineados el inventario y las evaluaciones de riesgo.
- **Gobierno de datos y seguridad de la información:** el inventario se conecta con los inventarios de datos existentes; en el ámbito de seguridad de la información, cualquier hallazgo relevante o incidente relacionado con un sistema de IA se documenta en el inventario.
- **Comunicación y cultura organizativa:** la importancia del inventario se refuerza con sensibilización y formación; en actividades de uso ético de la IA, cumplimiento o uso responsable y seguro de tecnologías, se incluye el propósito del inventario y la forma de colaborar en su mantenimiento.

7.3. Seguimiento de la Evolución Normativa

El contexto regulatorio asociado a los sistemas de inteligencia artificial evoluciona de forma constante, por lo que el mantenimiento del inventario incorpora un seguimiento específico de la evolución normativa para sostener la gestión del riesgo y el cumplimiento a lo largo del tiempo. En la práctica, esta vigilancia permite identificar cambios que afectan a los sistemas inventariados y activar la actualización de la información cuando entra en vigor una nueva norma, se aprueban políticas internas o se publican criterios interpretativos relevantes.

El seguimiento se articula como un proceso recurrente coordinado entre las funciones de cumplimiento y asesoría legal, con participación de tecnología, gestión de riesgos y seguridad de la información cuando el cambio requiere adaptación técnica u operativa. Este enfoque se integra con los procedimientos de mantenimiento del inventario descritos en el apartado 7.1, de forma que los cambios normativos se tratan como un desencadenante de actualización y se reflejan en la ficha del sistema cuando impactan en su contexto de uso o en sus obligaciones aplicables.

A nivel general, la vigilancia normativa se apoya en dos tipos de señales, combinando fuentes externas e internas para asegurar que el inventario se mantiene alineado con el marco aplicable:

- **Fuentes externas:** nuevas disposiciones, guías, directrices o criterios emitidos por organismos competentes que modifican o aclaran la interpretación del marco regulatorio y pueden afectar a la clasificación del riesgo o a las obligaciones exigibles.
- **Señales internas:** actualizaciones de políticas corporativas, decisiones de gobierno y cambios organizativos u operativos (por ejemplo, cambios de proveedor, cambios en el contexto de uso o resultados de evaluaciones de riesgo) que introducen nuevas obligaciones o ajustan el enfoque de control.

Cuando se identifica un cambio normativo o un criterio interpretativo relevante, la organización realiza un análisis de aplicabilidad orientado al inventario. Este análisis determina qué sistemas pueden verse afectados, si existe variación en la categoría regulatoria o en el nivel de riesgo, y si aparecen obligaciones adicionales en materia de documentación, transparencia, vigilancia posterior al despliegue o notificación. A partir de ese punto, se actualizan las fichas afectadas para mantener la trazabilidad entre el sistema y las obligaciones aplicables, incorporando, cuando proceda, revisiones en la documentación vinculada y en los controles o medidas de supervisión.

Para sostener la trazabilidad, cada actualización motivada por evolución normativa se documenta como evidencia del propio mantenimiento: se conserva la referencia al cambio identificado, la fecha de evaluación, la decisión sobre aplicabilidad y las acciones derivadas (actualización de campos, revisión de documentación, ajustes en el plan de monitorización o en los controles aplicados). Con ello, el inventario mantiene su papel como punto de enlace entre la gestión de riesgos, el cumplimiento normativo y la operación real de los sistemas de IA, permitiendo explicar de forma ordenada por qué una ficha cambia y qué evidencia sustenta el cambio.

De esta forma, la vigilancia normativa se integra en el ciclo de vida del inventario como un mecanismo de actualización continua: permite anticipar cambios, evaluar su aplicabilidad, reflejar su impacto en las fichas afectadas y conservar evidencia verificable de las decisiones y acciones adoptadas.

08.

ESTRUCTURA Y CAMPOS DE LA PLANTILLA DEL INVENTARIO

8.1. Sección A: Identificación y Propiedad

Item	Objetivo	Razonamiento	Información Esperada
ID del Sistema	Identificar de manera única cada sistema presente en la organización	Es necesario trazar correctamente cada sistema y evitar errores o ambigüedades cuando existen sistemas con nombres similares (ejemplo: Copilot Chat / Copilot Studio)	Código único interno, estructurado según el estándar que defina la organización
Nombre del Sistema	Facilitar una identificación más comprensible	El nombre comercial es más fácil de manejar en contextos distintos al de la pura gestión del inventario o CMDB, como por ejemplo en comités o con perfiles que utilicen el sistema	Denominación interna del sistema, preferiblemente la denominación comercial que todos los usuarios conocen
Versión	Identificar la versión concreta del sistema inventariado	Los cambios de versión pueden implicar modificaciones en cuanto a funcionalidades y, por tanto, riesgos presentes, requiriéndose nueva evaluación	Número/código de la versión (v.1.2) y/o referencia a la licencia bajo la cual se ha contratado el sistema (licencia de uso concreta que ha otorgado el proveedor)
Fecha de Alta	Registrar el momento en el que el sistema se incorpora formalmente al inventario	Permite demostrar control temporal del inventario y facilita la planificación de revisiones y/o auditorías	Fecha en la que el sistema se ha incorporado al sistema
Estado	Conocer la situación del sistema en cuanto a su ciclo de vida	Permite determinar el nivel de exigencia de controles y evaluaciones, en función de la fase en que se encuentre	Determinación de si se encuentra en estado de Diseño / Desarrollo / Pruebas – piloto / Producción / Retirado
Área propietaria del sistema	Identificar al responsable funcional del sistema	Permite asignación de responsabilidades y vinculación con la matriz RACI que, en su caso, se haya definido	Identificación del área responsable (ejemplo: Innovación)
Responsable del sistema	Identificar al responsable en última instancia del sistema	Permite asignación de responsabilidades y vinculación con la matriz RACI que, en su caso, se haya definido	Identificación del rol o persona que actúa como owner del sistema
Proveedor del sistema	Identificar quién ha desarrollado y provee el sistema	Permite obtener la información necesaria para enfocar el cumplimiento de las obligaciones que resulten aplicables y gestionar las relaciones contractuales	Especificación de si se trata de un sistema desarrollado y contratado a un tercero, o de un sistema desarrollado internamente por la organización (en este caso deberá identificarse qué mercantil concreta del grupo lo ha desarrollado, para poder identificar correctamente los licenciamientos intra-grupo
Descripción funcional y finalidad prevista por el proveedor	Conocer la finalidad del sistema conforme a su diseño y conceptualización	Es clave para conocer si el uso real y práctico del sistema encaja con la finalidad prevista por su proveedor, evitando situaciones de desfase que deriven en la asunción de más responsabilidades legales de las esperables (conversión al rol de “proveedor”, bajo la regulación que fija el Reglamento de IA)	Descripción de las finalidades y funcionalidades conforme a la información comercial del proveedor

8.2. Sección B: Uso y Alcance

Item	Objetivo	Razonamiento	Información Esperada
Interacción con personas físicas	Conocer si el sistema interactúa con personas	En caso de que exista dicha interacción, se activa una obligación de transparencia para el proveedor del sistema, conforme al Reglamento de IA	Respuesta SÍ / NO
Generación de contenido multimedia	Conocer si el sistema genera contenido de texto, audio, vídeo o imagen	En caso afirmativo, se activan determinadas obligaciones de transparencia conforme al Reglamento de IA	Respuesta SÍ / NO, especificando la clase de contenido que se genera
Países en los que se desplegará	Identificar el alcance geográfico del sistema	Pueden existir obligaciones distintas en función del alcance geográfico, al existir distintas legislaciones y autoridades de vigilancia del mercado	Lista de países o regiones en las que se utilizará el sistema
Modelos de IA subyacentes	Conocer los modelos que integra el sistema.	Un mismo sistema puede integrar varios modelos, cada uno de ellos con riesgos y características diferentes	Denominación de los modelos que se integran en el sistema, especificando si se tratan de modelos de uso específico o modelos de IA de uso general
Proveedor del modelo subyacente (si aplica)	Conocer quién ha desarrollado o provee cada modelo subyacente	Es necesario para conocer si se asumen obligaciones adicionales conforme a la legislación aplicable, a la vez que permite asegurar que se ha regularizado toda la esfera contractual del sistema de forma debida (revisión de los términos que regulan no solo el uso del sistema, sino también el uso de los modelos subyacentes)	Denominación de los modelos que se integran en el sistema, especificando si se tratan de modelos de uso específico o modelos de IA de uso general

8.3. Sección C: Riesgo y Cumplimiento

Item	Objetivo	Razonamiento	Información Esperada
Caso de uso asociado	Identificar de manera única cada sistema presente en la organización	Un mismo sistema puede utilizarse para más de un caso de uso, siendo ésta información la que permite conocer el nivel de riesgo normativo que tiene el sistema en su conjunto	Lista de todos los casos de uso asociados. Cada caso de uso se ha de consignar en una fila específica del inventario
Descripción del caso de uso asociado	Describir el uso en la práctica del sistema por parte de la organización	Es necesario describir en detalle el uso real que se hace del sistema en el marco de cada proceso/caso de uso, para verificar que encaja con las finalidades previstas que ha declarado, para ese sistema, su proveedor. En caso contrario, cabe el riesgo de asumir el rol de proveedor de un sistema desarrollado por terceros, junto con todas las obligaciones reservadas a dicho rol	Descripción detallada del caso de uso
Sociedad usuaria	Identificar la sociedad (mercantil) que implementa el caso de uso	Es necesario identificar qué sociedad (o sociedades) en concreto, dentro del grupo, implementa cada uno de los casos de uso (la mercantil es el sujeto obligado de la regulación)	Listado de sociedades en las que aplica el caso de uso registrado
Nivel de riesgo normativo	Identificar el nivel de riesgo normativo del caso de uso	Es preciso contar con una visual de los niveles de riesgo asociados, conforme a la normativa, a los casos de uso que se persiguen con cada sistema de ia. El nivel de riesgo asociado al caso de uso es el que delimita el riesgo normativo del sistema (y por tanto sus obligaciones legales)	Resultado del triaje normativo de la ia (riesgo inaceptable, alto, limitado o mínimo)
Nivel de riesgo	Identificar el nivel de riesgo del caso de uso	Al margen del nivel de riesgo que etiquete la normativa (inaceptable, alto, limitado o mínimo), es preciso en algunos casos, y recomendable en otros, realizar un análisis de los riesgos que presenta el caso de uso (principalmente riesgos para la seguridad, salud y derechos fundamentales, pero que se puede extender a otras materias como el riesgo operacional, la privacidad, etc.)	Nivel de riesgo inherente y/o residual (en función del grado de detalle que se desee mostrar) que se ha alcanzado tras hacer el análisis de riesgos, expresado en términos cualitativos o cuantitativos
Tratamiento de datos	Conocer si el caso de uso registrado conlleva el tratamiento de datos personales	Es preciso vincular el gobierno de la ia con las acciones de cumplimiento en materia de protección de datos, asociando casos de uso de ia a actividades documentadas en el registro de actividades de tratamiento. La inclusión de una marca de “datos personales” en el inventario de ia puede servir como disparador del privacy by design y/o como capa de refuerzo para la actualización de los tratamientos previamente analizados	Respuesta SÍ / NO e indicación expresa de las categorías de datos empleadas en el caso de uso

09.

EJEMPLO PRÁCTICO DE UN INVENTARIO CUMPLIMENTADO

Para complementar el marco conceptual y procedimental descrito en los capítulos anteriores, se pone a disposición un ejemplo completo de **Inventario de Sistemas y Servicios de IA**, que refleja el nivel de granularidad y estructura recomendados para una gestión efectiva del ciclo de vida de estos sistemas.

El documento ejemplifica la integración de los distintos bloques de información exigidos por las buenas prácticas de gobernanza de IA:

- Identificación del sistema y roles implicados.
- Finalidad declarada y correspondencia con la clasificación regulatoria.
- Evaluación del nivel de riesgo y evidencia de las medidas de mitigación aplicadas.
- Relación con documentación obligatoria (FRIA, expediente técnico, auditorías, logs operativos).
- Estado del sistema dentro del proceso iterativo de supervisión y mantenimiento.

Este recurso permite observar cómo el inventario actúa como registro único, auditable y trazable, sustentando las obligaciones de transparencia, supervisión humana y gestión de riesgos definidas por el RIA y los marcos internacionales de referencia.

1. Identificación y propiedad del sistema

ID del sistema	Nombre del sistema	Versión	Fecha de alta en inventario	Estado	Área propietaria del sistema	Responsable del sistema	Proveedor del sistema
AI-HR-001	Eightfold AI	Eightfold Talent Intelligence Platform – release SaaS	03/03/2026	Producción	RR.HH	Responsable de selección de personal	Eightfold AI
AI-LR-001	Microsoft Copilot Studio	Servicio SaaS (Microsoft Copilot Studio)	07/11/2024	Producción	Atención al cliente	Responsable de atención al cliente	Microsoft
AI-MR-001	Proofpoint Email Protection	Licencia: Proofpoint Email Protection – suscripción SaaS	04/05/2025	Producción	Seguridad de la información	Responsable de Seguridad de la Información	Proofpoint

2. Uso y alcance del sistema

Descrición funcional y finalidad prevista por el proveedor	Interacción con personas físicas	Generación de contenido multimedia	Países en los que se desplegará	Modelos de IA subyacentes	Proveedor del modelo subyacente (si aplica)
Sistema para apoyar procesos de selección, realizando cribado y priorización de candidaturas y recomendaciones para la fase de entrevista.	Sí	Sí	España	Modelos de clasificación: ID- XY20	N/A
Plataforma para crear y desplegar asistentes conversacionales para resolver consultas frecuentes, guiar gestiones y derivar a atención humana cuando corresponda.	Sí	Sí	España	Modelos de lenguaje y recuperación de información documental: ID-ZK30	Microsoft
Filtrado automatizado para detectar y bloquear correo no deseado, intentos de suplantación y mensajes maliciosos.	No	No	España	Modelos de clasificación/ detección automática de amenazas	Proofpoint

3. Riesgo y cumplimiento

Caso de uso asociado (nombre)	Descripción del caso de uso	Sociedad usuaria	Rol (RIA) asumido por la organización	Nivel de riesgo normativo	Nivel de riesgo	¿Tratamiento de datos personales?
Cribado y priorización de candidaturas	Analiza currículos y perfiles, identifica competencias, ordena candidaturas por adecuación al puesto y propone una lista priorizada para revisión por personal de RR. HH.	ISMS FORUM SPAIN	Responsable del despliegue	ALTO	Inherente Alto	Sí
Asistencia automatizada a los clientes en canales digitales	Responde preguntas, apoya trámites y genera respuestas en lenguaje natural; informa al usuario de que está interactuando con un sistema de IA y permite derivación a agente humano.	ISMS FORUM SPAIN	Responsable del despliegue	LIMITADO	Inherente Medio	Sí, en caso de que se gestionen cuentas o incidencias
Filtrado automático de amenazas en el correo corporativo	Clasifica correos entrantes, los etiqueta o pone en cuarentena; el equipo de TI puede liberar falsos positivos y revisar registros.	ISMS FORUM SPAIN	Responsable del despliegue	MÍNIMO	Inherente Bajo	Sí

10.

EL INVENTARIO EN LA ARQUITECTURA DE GOBERNANZA ORGANIZATIVA

El **Inventario de Servicios y Sistemas de IA** no es un apéndice administrativo, sino un control primario de gobierno y riesgo. Convertirlo en registro único, versionado y auditable habilita la diligencia debida, la trazabilidad y la rendición de cuentas a lo largo de todo el ciclo de vida, enlazando finalidad prevista, clasificación regulatoria, controles técnicos y evidencias. Esta arquitectura documental es, además, la condición para acreditar conformidad con el RIA y mantener coherencia con marcos como ISO/IEC 42001 y NIST AI RMF.

El enfoque por fases, descubrimiento y mapeo, clasificación y evaluación de riesgos, documentación y registro, monitorización y mantenimiento, permite gestionar el inventario como un proceso iterativo, no estático. De este modo se reduce la ceguera operativa y se establece una recalibración continua del riesgo ante cambios en el propósito, el modelo, los datos, el contexto de uso o el marco normativo, con disparadores claros de revisión y control de versiones.

Desde la perspectiva técnica, el inventario opera como una CMDB especializada en IA que consolida arquitectura, modelos, datos, métricas y dependencias. Esta visibilidad integral facilita controles preventivos frente a implementaciones no autorizadas o no gobernadas, endurece el perímetro contractual con terceros y refuerza las defensas ante vectores específicos de IA, envenenado de datos, *prompt injection*, extracción de modelos, apoyándose en evidencias de robustez, auditorías de sesgo y resultados de pruebas.

En materia de cumplimiento, el inventario actúa como índice maestro del expediente técnico y de las evaluaciones de impacto en derechos fundamentales, y, cuando aplica, como base para los registros oficiales exigidos. La clasificación temprana en riesgo prohibido, alto, limitado o mínimo activa flujos de control diferenciados, determina obligaciones de transparencia y sostiene la vigilancia posterior al despliegue. La vinculación de cada ficha con su documentación de soporte garantiza consistencia entre lo declarado y lo efectivamente desplegado, minimiza lagunas y materializa el principio de *accountability*.

Operativamente, la fase de monitorización y mantenimiento dota de mecanismos para gobernar la deriva de datos y de concepto, la degradación del rendimiento y los vencimientos de certificaciones. El sistema de registro de incidentes unifica la narrativa técnica (impacto, causa raíz, medidas) con la narrativa regulatoria (notificaciones, evidencias y lecciones aprendidas), cerrando el bucle que actualiza la ficha del sistema, ajusta controles y, cuando procede, recalibra su clasificación. El resultado es una reducción efectiva de tiempos de detección y resolución, así como una base comparativa para decidir continuidad, mejora, retirada o sustitución.

El verdadero valor estratégico emerge al integrar el inventario con procesos corporativos existentes: gestión de cambios, gobierno del dato, compras y evaluación de terceros, gestión de riesgos y privacidad. Establecer el alta en el inventario como prerrequisito de paso a producción consolida el *"AI by design"*, evita desbordes tecnológicos y asegura que cada versión en servicio conserva una huella documental que refleja su comportamiento real en producción y las responsabilidades asociadas.

En síntesis, el inventario permite operar la inteligencia artificial bajo una lógica de control continuo. Proporciona un plano único para priorizar esfuerzos en función del riesgo, verificar la eficacia de los controles, justificar inversiones y articular una interlocución informada entre tecnología, negocio, cumplimiento, protección de datos y el órgano de gobernanza de IA. Al transformar obligaciones regulatorias en capacidades operativas, trazabilidad, explicabilidad, supervisión humana, transparencia y gestión de incidentes, se consolida como un pilar de resiliencia organizativa frente a riesgos técnicos, regulatorios y reputacionales derivados del uso de la IA.

11.

ANEXOS

11.1. Formulario de revisión de impacto de riesgos de la IA (FRIA)

Campo	Descripción / Ejemplo
ID del sistema en el inventario	IA-001
Nombre del sistema	Motor de diagnóstico clínico automatizado
Departamento responsable	Innovación Médica
Proveedor o desarrollador	Interno / Externo
Clasificación de riesgo (RIA)	Alto riesgo (art. 6)
Finalidad del sistema	Analizar imágenes médicas y sugerir diagnósticos preliminares
Marco normativo aplicable	RIA, GDPR, ISO/IEC 42001, otras normas sectoriales
Grupos e individuos afectados	Pacientes, personal médico, organización sanitaria
Derechos en riesgo	No discriminación, protección de datos, integridad física y salud
Escenarios de riesgo	Diagnóstico erróneo, sesgo en determinados colectivos, uso fuera de contexto
Probabilidad / Gravedad	[Escala interna: baja/media/alta]
Nivel de riesgo inicial	[Bajo/Medio/Alto]
Medidas de mitigación	Supervisión humana, validación clínica, pruebas de sesgo, controles de acceso
Riesgo residual	[Describir]
Supervisión humana	Descripción de cómo se interviene y quién es responsable
Plan de monitorización	Frecuencia de revisión, indicadores clave, triggers de reevaluación
Auditorías / revisiones realizadas	Auditoría interna 2025, revisión comité ético
Responsable del seguimiento	[Nombre / rol]
Fecha de elaboración / última revisión	[Fecha]

Esta estructura es consistente con guías prácticas de FRIA para el RIA que incluyen identificación de derechos afectados, análisis de probabilidad y gravedad, y diseño de medidas de mitigación.

11.2. Expediente técnico del sistema de IA (Art. 11 RIA)

Sección	Contenido requerido	Ejemplo
1. Identificación del sistema	Nombre, ID, versión, responsable	IA-001, v3.1, Responsable de IA Clínica
2. Propósito y alcance	Uso previsto, usuarios, entorno, limitaciones	Apoyo diagnóstico en hospital, uso por radiólogos
3. Arquitectura y componentes	Diagrama funcional, módulos, interfaces, dependencias	CNN de clasificación, módulo de preprocesado de imagen
4. Datos y gobernanza	Origen de datos, calidad, representatividad, anonimización, sesgo	Dataset interno anoninizado, controles de calidad, evaluación de sesgo demográfico
5. Entrenamiento y validación	Metodología, métricas, resultados, set de prueba	Entrenamiento supervisado, validación cruzada, precisión 94%
6. Gestión de riesgos	Identificación de riesgos, relación con FRIA, medidas aplicadas	Referencia a FRIA-001, controles sobre uso indebido
7. Supervisión humana	Controles humanos, procedimientos de override	Revisión de resultados por radiólogo antes del informe
8. Seguridad y ciberseguridad	Controles de acceso, protección de modelos, gestión de incidentes	Autenticación fuerte, registro de accesos, plan de respuesta a incidentes
9. Desempeño y robustez	Pruebas de estrés, escenarios adversos, degradación	Pruebas con datos ruidosos, análisis de comportamiento en casos límite
10. Control de cambios	Historial de versiones, motivo de cambios, evaluación de impacto	v3.0 → v3.1 por ampliación de dataset y mejora de precisión
11. Documentos anexos	FRIA, auditorías, actas, políticas internas	FRIA-001, Auditoría-IA 2025, Política de uso responsable
12. Registro y aprobaciones	Firmas, registro interno / externo, fecha	Aprobado por Comité de IA, registrado en base interna

Estas secciones coinciden con las recogidas en plantillas de documentación técnica para el RIA que cubren diseño, datos, pruebas y control del sistema.

11.3. Proceso de triaje: Ejemplo práctico

¿El caso de uso o sus resultados están relacionados con alguna de las siguientes actividades que están prohibidas (salvo en algunas excepciones específicas) según el RIA de la UE?

- Implementar técnicas subliminales, manipuladoras o engañosas para distorsionar el comportamiento y perjudicar la toma de decisiones informadas, causando un daño significativo.
- Explotar vulnerabilidades relacionadas con la edad, discapacidad o circunstancias socioeconómicas para distorsionar el comportamiento, causando un daño significativo.
- Puntuación social (es decir, evaluar o clasificar a individuos o grupos en función de su comportamiento social o características personales).
- Evaluar el riesgo de que una persona cometa delitos únicamente basándose en perfiles o rasgos de personalidad.
- Compilar o ampliar bases de datos de reconocimiento facial mediante la recopilación indiscriminada de imágenes faciales de Internet o grabaciones de CCTV.
- Inferir emociones en lugares de trabajo o instituciones educativas.
- Sistemas de categorización biométrica que infieren atributos sensibles (por ejemplo, raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida u orientación sexuales).
- Identificación biométrica remota en tiempo real (RBI) en espacios públicos para fines de aplicación de la ley.

Clasificación Preliminar del Riesgo

Aplicar criterios de clasificación del riesgo (Alto, Limitado, Mínimo) según la RIA de la UE:

¿El caso de uso o sus resultados están relacionados con alguna de las siguientes actividades clasificadas como de Alto Riesgo según la RIA de la UE (salvo en algunas excepciones específicas)?

- Identificación o categorización biométrica (incluido el reconocimiento de emociones).
- Infraestructura crítica.
- Educación y formación profesional.
- Empleo, gestión de trabajadores y acceso al autoempleo (incluidos sistemas de IA en procesos de selección, como la segmentación, selección y evaluación de candidatos; la supervisión y evaluación del rendimiento laboral; y la asignación de tareas basadas en características y comportamiento).
- Acceso y disfrute de servicios privados esenciales y servicios y beneficios públicos esenciales (incluidos sistemas de IA para evaluar la elegibilidad para asistencia pública esencial y servicios (incluidos los sanitarios); evaluar crédito/solvencia; clasificar llamadas de emergencia y triaje sanitario de pacientes; y evaluaciones de riesgo y fijación de precios en seguros de vida o salud).
- Aplicación de la ley, administración de justicia y procesos democráticos.
- Gestión de migración, asilo o control fronterizo.
- Mecanismo de seguridad de un producto que ya esté sujeto a la "legislación de armonización de la Unión Europea" detallada en el Anexo I de la RIA de la UE (por ejemplo, dispositivos médicos, maquinaria industrial, aeronaves/coches/vehículos/sistemas ferroviarios, embarcaciones, juguetes, ascensores, equipos para atmósferas potencialmente explosivas, equipos de radio, instalaciones de teleféricos, equipos de protección personal, combustión de gases, equipos marinos).

¿Existe la posibilidad de que el caso de uso genere un escrutinio o interés público significativo? Es decir, podría el caso de uso potencialmente:

- Generar una cobertura mediática significativa sobre la participación o asociación con nuestra empresa.
- Involucrar clientes, sectores o tipos de servicio que puedan ser perjudiciales para la marca y reputación de nuestra empresa por nuestra implicación, asociación o percepción pública.
- Ser de interés significativo para el público.
- Conducir a una investigación regulatoria sobre nuestra empresa y/o nuestro cliente (esto podría amplificarse en combinación con todos los puntos anteriores).

¿Podría la operación del sistema GenAI amenazar la seguridad, el estilo de vida o los derechos de personas o grupos de personas?

¿Se aplica alguna de las siguientes condiciones en relación con los datos que desea utilizar? (responda "sí" a todas las que apliquen):

- ¿Su caso de uso requiere manejar, utilizar y/o almacenar datos confidenciales del cliente o datos personales dentro del entorno de nuestra empresa o de un tercero?
- ¿La aplicación/sistema IA generativa se integrará con otros sistemas que contengan datos de nuestra empresa, del cliente o datos personales?
- ¿Están en alcance datos confidenciales de alto riesgo?
- ¿Están en alcance datos personales sensibles o de categoría especial?
- ¿El caso de uso prevé combinar datos obtenidos de múltiples fuentes (clientes, proyectos, oportunidades, geografías u otras fuentes de terceros...)?
- ¿El caso de uso prevé reutilizar datos para un propósito secundario?
- ¿El caso de uso utiliza datos disponibles públicamente obtenidos mediante web scraping?
- ¿Existe potencialmente una falta de datos de entrenamiento de alta calidad que sean representativos de la población en producción?

¿Se aplica alguna de las siguientes condiciones? (seleccione todas las que correspondan):

- El sistema IA generativa o el caso de uso incluye el uso de Agentes de IA" que actuarán de forma autónoma utilizando métodos no deterministas (si la respuesta es "sí", responda a las siguientes preguntas):
  - » El sistema de IA está en un entorno aislado (sandbox).
  - » ¿El sistema de IA es una prueba de concepto (PoC)?
  - » El sistema de IA no está conectado a soluciones en producción.
  - » El sistema de IA no está conectado ni puede realizar acciones en otras aplicaciones donde el mal uso suponga un alto riesgo.
  - » El sistema de IA no se está desarrollando para un caso de uso donde la alta precisión sea importante y/o las consecuencias de errores sean graves.
  - » Estamos entrenando o ajustando un modelo de lenguaje grande (LLM).
  - » El sistema GenAI o la herramienta aprenderá de datos y/o entradas de prompts.
  - » El sistema de IA generativa o sus resultados serán visibles externa o públicamente.
  - » El caso de uso se dirige o aplica a grupos vulnerables.
  - » La tecnología se utilizará o podría utilizarse con fines militares o políticos.
  - » El cliente opera en una industria altamente regulada.
  - » El sistema IA generativa generará o manipulará contenido de imagen, audio o vídeo que constituya un deepfake.

REFERENCIAS

Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). (2024–2025). *Guías sobre gestión de riesgos y supervisión humana en sistemas de inteligencia artificial.* https://www.aesia.gob.es

ENISA. (2023). *Threat landscape for artificial intelligence.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Commission. (2024–2025). *AI Act: Guidelines, templates and implementation resources.* AI Office. https://digital-strategy.ec.europa.eu

European Data Protection Board. (2017). *Guidelines on data protection impact assessment (DPIA).* https://edpb.europa.eu

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 - Information security management systems - Requirements*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 - Information security risk management*. ISO.

International Organization for Standardization. (2023). *ISO/IEC 42001:2023 - Artificial intelligence management system (AIMS)*. ISO.

ISMS Forum Spain. (2024). *Guía de inteligencia artificial y ciberseguridad (con el soporte del CCN)*. ISMS Forum. https://www.ismsforum.es/ficheros/descargas/isms-gt-ia-021707141605.pdf

ISMS Forum Spain. (2025). *Gobierno de la inteligencia artificial.* ISMS Forum. https://www.ismsforum.es/ficheros/descargas/en---gobierno-de-la-ia1765878738.pdf

ISMS Forum Spain. (2025). *Handbook del Reglamento de Inteligencia Artificial (RIA)*. ISMS Forum. https://www.ismsforum.es/ficheros/descargas/handbook-ia-final-corregido-11721047763.pdf

MITRE Corporation. (2023). *MITRE ATLAS: Adversarial threat landscape for artificial-intelligence systems.* https://atlas.mitre.org

National Institute of Standards and Technology. (2023). *AI risk management framework (AI RMF 1.0)*. NIST. https://www.nist.gov

OECD. (2019/2024). *OECD principles on artificial intelligence*. Organisation for Economic Co-operation and Development. https://www.oecd.org

Open Worldwide Application Security Project. (2024). *OWASP top 10 for machine learning and agentic AI applications*. https://owasp.org

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)*. Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo de la Unión Europea. (2022). *Directiva (UE) 2022/2555 (NIS2) relativa a las medidas para un alto nivel común de ciberseguridad en la Unión.* Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)*. Diario Oficial de la Unión Europea.

GIA | GRUPO DE INTELIGENCIA ARTIFICIAL

isms forum | INTERNATIONAL INFORMATION SECURITY COMMUNITY

INVENTARIO DE SISTEMAS Y SERVICIOS DE IA