



Guía 4. Sistema de gestión de la calidad

Reglamento Europeo de
Inteligencia Artificial



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia

España | digital ²⁰²⁶

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

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

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

Entre las referencias técnicas relevantes actualmente en desarrollo, destaca el **prEN 18286 “Artificial Intelligence – Quality Management System for EU AI Act Regulatory Purposes”**, que establecerá el marco de gestión de la calidad aplicable a los sistemas de IA en el contexto del cumplimiento del Reglamento Europeo de Inteligencia Artificial.

Fecha de versión: 10 de diciembre de 2025

Contenido general

1. Preámbulo	4
2. Introducción	6
3. Reglamento de Inteligencia Artificial.....	7
4. ¿Qué elementos debo implantar y cómo debo hacerlo para desarrollar un adecuado sistema de gestión de la calidad?	12
5. Otros elementos a considerar	36
6. Cuestionario de autoevaluación	40
7. Referencias, estándares y normas.....	41

Índice detallado

1. Preámbulo	4
1.1 Objetivo del documento	4
1.2 Cómo leer esta guía	4
1.3 ¿A quién está dirigido?	5
1.4 Casos de uso y ejemplos dispuestos a lo largo de la guía	5
2. Introducción	6
2.1 ¿Qué es un sistema de gestión de la calidad?	6
3. Reglamento de Inteligencia Artificial.....	7
3.1 Análisis previo y relación de los artículos	7
3.2 Contenido de los artículos en el Reglamento de IA	8
3.3 Correspondencia del articulado con los apartados de la guía	10
4. ¿Qué elementos debo implantar y cómo debo hacerlo para desarrollar un adecuado sistema de gestión de la calidad?	12
4.1 Cumplimiento reglamentario, evaluación de conformidad y gestión de las modificaciones	12
4.2 Diseño, control y verificación del diseño	14
4.3 Desarrollo, control y aseguramiento de la calidad	16
4.4 Examen, prueba y validación	18
4.5 Especificaciones técnicas, normas y normas armonizadas	19
4.6 Sistemas y procedimientos de gestión de datos	21
4.7 Sistema de gestión de riesgos	22
4.8 Sistema de vigilancia poscomercialización	23
4.9 Notificación de incidentes graves	23
4.10 Comunicación.....	24
4.11 Documentación	25
4.12 Gestión de los recursos	26
4.13 Marco de rendición de cuentas	28
5. Otros elementos a considerar	36
5.1 Implementación del sistema de gestión de calidad proporcional al tamaño de la organización del proveedor	36
5.2 Entidades financieras y proveedores sujetos a legislación sectorial	38
6. Cuestionario de autoevaluación	40
7. Referencias, estándares y normas.....	41

1. Preámbulo

1.1 Objetivo del documento

En esta guía se presentan las medidas organizativas y técnicas que servirán a proveedores y responsables del despliegue para dar cumplimiento al artículo **“Sistema de gestión de la calidad”** establecido en el artículo 17 del Reglamento Europeo de la IA. Este artículo establece los requisitos de gestión de la calidad que deberá incorporar todo sistema de IA de alto riesgo (HRAIS) y ciertos sistemas de IA de propósito general (artículo *“Requisitos para sistemas IA de propósito general y obligaciones para proveedores de estos sistemas”*). En este sentido, a lo largo de la guía nos referiremos, generalmente, a estos sistemas como “sistema de IA” con el objetivo de simplificar el discurso.

1.2 Cómo leer esta guía

Esta sección se ha elaborado para **acompañar al lector** en la lectura de la guía y ayudarle a alcanzar una **comprensión** de los contenidos más **ágil y eficaz**.

Para ello, presentamos una breve explicación del contenido y relevancia de cada una de las secciones:

1. Preámbulo

- 1.1. **Objetivo del documento:** breve introducción a los contenidos y objetivo de la guía.
- 1.2. **Cómo leer esta guía:** facilita al lector la comprensión de la guía.
- 1.3. **¿A quién está dirigido?:** explicación de las obligaciones de proveedor y responsable del despliegue.
- 1.4. **Casos de uso:** ejemplos ilustrativos empleados a lo largo de la guía.
2. **Introducción:** sección de la guía en la que se detalla y describe que es un sistema de gestión de calidad en contexto general y en el contexto específico del Reglamento Europeo de la IA.
3. **Reglamento de Inteligencia Artificial:** se realiza análisis de los artículos en torno a los cuales se ha escrito esta guía y relación entre los apartados de dichos artículos y aquellos de la guía donde se abordan.
4. **¿Qué elementos debo implantar y cómo debo hacerlo para desarrollar un adecuado sistema de gestión de la calidad?:** sección principal de la guía en la que se analizan los elementos del artículo y se especifica cómo debe abordarse cada uno de ellos para su adecuado cumplimiento.
5. **Otros elementos por considerar:** en esta sección abordamos el resto de los elementos específicos del artículo (como el análisis de la implementación del sistema de gestión de calidad proporcional al tamaño de la organización del proveedor).
6. **Referencias, estándares y normas:** documentación referenciada a lo largo de la guía.

1.3 ¿A quién está dirigido?

Los requisitos descritos en el artículo “*Sistema de gestión de la calidad*” están orientados fundamentalmente al desarrollo del sistema, realizado por el proveedor. En dicho artículo, no se especifican requisitos para aquel que hace uso del sistema, es decir, el responsable del despliegue. En caso de que el responsable del despliegue, en una situación determinada, participase en el desarrollo del sistema, éste debería aplicar las medidas desarrolladas para el proveedor.

En este contexto, las medidas detalladas a lo largo de esta guía son medidas orientadas a servir como guía para el proveedor. Estas medidas son tanto de carácter organizativo como técnico.

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

Con el fin de facilitar la comprensión de la guía, se incorporan a lo largo de la misma una serie de ejemplos que pretenden servir como referencia para la adecuación de los HRAIS para la gestión de sistemas de calidad conforme a los requisitos del reglamento.

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

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

Con este fin y dado a lo transversal del tema tratado, se dispondrá de una empresa ficticia y se analizará punto por punto del reglamento cuáles podrían ser las implicaciones a tener en cuenta de los apartados descritos en el reglamento en la empresa.

2. Introducción

2.1 ¿Qué es un sistema de gestión de la calidad?

Un sistema de gestión de la calidad en términos generales, tal y como se entiende según el estándar de referencia ISO 9001, consiste en un conjunto de procesos diseñados para que una organización pueda mejorar continuamente su desempeño global, así como proporcionarle una base para un desarrollo sostenible.

En el contexto del Reglamento Europeo de la IA, donde el propósito general es garantizar **la salud, la seguridad y los derechos fundamentales de las personas** en el contexto del uso de los sistemas de IA, el sistema de gestión de calidad (según lo expuesto en el artículo “Sistema de gestión de la calidad”) es aquel que contendrá los elementos especificados en dicho artículo (*algunos de ellos son: una estrategia para el cumplimiento reglamentario, el sistema de gestión de riesgos de acuerdo con lo especificado en el artículo correspondiente, sistemas y procedimientos de gestión de datos*) y que cuya documentación quedará reflejada en políticas, procedimientos e instrucciones escritas.

Esta guía facilita la comprensión del artículo “Sistema de gestión de la calidad” y ayudar al lector en la implementación de las medidas oportunas que le permitan cumplir con lo que se especifica en dicho artículo. De este modo, en la siguiente sección analizaremos cada uno de los elementos especificados en el artículo y trataremos de explicar en detalle cómo deben abordarse y documentarse.

Antes de entrar en la siguiente sección es importante destacar que, como podrá verse, la gran mayoría de los elementos que se indica que debe contener un sistema de gestión de la calidad ya han sido desarrollados en alguna de las guías técnicas elaboradas. En este contexto, dichos elementos serán referenciados desde esta guía a la guía oportuna donde se hayan desarrollado, incorporando el contenido adicional necesario para facilitar el cumplimiento con el elemento en cuestión. Así, por ejemplo, el apartado g) especifica que el sistema de gestión de calidad deberá incluir “*el sistema de gestión de riesgos que se menciona en el artículo 9*”. En este caso, incorporaremos en el correspondiente apartado de esta guía (siguiente sección) una explicación de cómo se debe completar este elemento vinculándolo con el contenido correspondiente, en este caso, de la guía desarrollada para facilitar el cumplimiento con el artículo “Sistema de gestión de riesgos”.

El artículo establece que el sistema deberá documentarse de forma sistemática mediante políticas, procedimientos e instrucciones escritas.

Esta guía no prescribe un formato concreto, dejando su elección a cada organización (por ejemplo: políticas internas, procedimientos técnicos, anexos, etc.).

3. Reglamento de Inteligencia Artificial

3.1 Análisis previo y relación de los artículos

Las obligaciones sobre los sistemas de gestión de la calidad se encuentran principalmente en el artículo 17 del Reglamento Europeo de IA “*Sistema de gestión de la calidad*”.

En este sentido:

- **Artículo Sistema de gestión de la calidad** → establece las obligaciones de los proveedores de sistemas de IA de alto riesgo de implementar un sistema de gestión de calidad documentado que garantice el cumplimiento normativo. Este sistema debe incluir estrategias de cumplimiento, gestión de riesgos, control de diseño y desarrollo, pruebas, vigilancia poscomercialización, notificación de incidentes y comunicación con autoridades y partes interesadas. Su alcance debe ser proporcional al tamaño del proveedor y puede integrarse con sistemas existentes si cumplen normativas sectoriales de la UE. El artículo también incorpora consideraciones específicas para entidades financieras.

A modo de resumen visual, puede representarse de la siguiente forma:



3.2 Contenido de los artículos en el Reglamento de IA

AI Act

Art.17 – Sistema de gestión de la calidad

Los **proveedores** de sistemas de IA de alto riesgo **establecerán** un **sistema de gestión de la calidad** que garantice el **cumplimiento del presente Reglamento**. Dicho sistema deberá consignarse de manera sistemática y ordenada en documentación en la que se recojan las **políticas, los procedimientos y las instrucciones** e incluirá, al menos, los siguientes aspectos:

- a) una **estrategia para el cumplimiento de la normativa**, incluido el cumplimiento de los procedimientos de **evaluación de la conformidad** y de los procedimientos de **gestión de las modificaciones** de los sistemas de IA de alto riesgo;
- b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **diseño** y el **control** y la **verificación del diseño** del sistema de IA de alto riesgo;
- c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **desarrollo** del sistema de IA de alto riesgo y en el **control y el aseguramiento de la calidad** de este;
- d) los procedimientos de **examen, prueba y validación** que se llevarán a cabo **antes, durante y después** del **desarrollo** del sistema de IA de alto riesgo, así como la frecuencia con que se ejecutarán;
- e) las **especificaciones técnicas**, incluidas las **normas**, que se **aplicarán** y, cuando las **normas armonizadas** pertinentes no se **apliquen en su totalidad** o no cubran todos los requisitos pertinentes establecidos en la sección 2, los **medios** que se utilizarán para **velar** por que el sistema de IA de alto riesgo **cumpla dichos requisitos**;
- f) los **sistemas y procedimientos de gestión de datos**, lo que incluye su adquisición, recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con esa finalidad;
- g) el **sistema de gestión de riesgos** que se menciona en el artículo 9;
- h) el establecimiento, aplicación y mantenimiento de un **sistema de vigilancia poscomercialización** de conformidad con el artículo 72;
- i) los **procedimientos** asociados a la **notificación** de un **incidente grave** con arreglo al artículo 73;



j) la gestión de la **comunicación** con las **autoridades nacionales competentes**, otras autoridades pertinentes, incluidas las que permiten acceder a datos o facilitan el acceso a ellos, los **organismos notificados**, otros **operadores**, los **clientes** u otras **partes interesadas**;

k) los **sistemas y procedimientos** para llevar un **registro** de toda la **documentación e información pertinente**;

l) la **gestión de los recursos**, incluidas **medidas** relacionadas con la seguridad del suministro;

m) un **marco de rendición de cuentas** que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

2. La aplicación de los aspectos mencionados en el apartado 1 **será proporcional al tamaño de la organización del proveedor**. Los proveedores respetarán, en todo caso, el grado de rigor y el nivel de protección requerido para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.

3. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al Derecho sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicho Derecho.

4. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

3.3 Correspondencia del articulado con los apartados de la guía

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

Artículo Reglamento	Requerimiento Reglamento	Sección guía
17.1.a	Cumplimiento reglamentario, evaluación de conformidad y gestión de las modificaciones	Apartado 4.1
17.1.b	Diseño, control y verificación del diseño	Apartado 4.2
17.1.c	Desarrollo, control y aseguramiento de la calidad	Apartado 4.3
17.1.d	Examen, prueba y validación	Apartado 4.4
17.1.e	Especificaciones técnicas, normas y normas armonizadas	Apartado 4.5
17.1.f	Sistemas y procedimientos de gestión de datos.	Apartado 4.6
17.1.g	Sistema de gestión de riesgos	Apartado 4.7
17.1.h	Sistema de vigilancia poscomercialización	Apartado 4.8
17.1.i	Notificación de incidentes graves	Apartado 4.9
17.1.j	Comunicación	Apartado 4.10
17.1.k	Documentación	Apartado 4.11
17.1.l	Gestión de los recursos	Apartado 4.12
17.1.m	Marco de rendición de cuentas	Apartado 4.13
17.2	Implementación del sistema de gestión de calidad proporcional al tamaño de la organización del proveedor	Apartado 5.1
17.3	Entidades financieras y proveedores sujetos a legislación sectorial	Apartado 5.2
17.4	Entidades financieras y proveedores sujetos a legislación sectorial	Apartado 5.2

Esta correspondencia no sustituye otros requisitos del Reglamento (documentación técnica, evaluación de conformidad, obligaciones del capítulo III sección 2). Cada uno debe abordarse en su propia guía técnica.

4. ¿Qué elementos debo implantar y cómo debo hacerlo para desarrollar un adecuado sistema de gestión de la calidad?

El **primer apartado** del artículo consiste en un **listado de los elementos** que, como mínimo, **deberá contener** nuestro **sistema de gestión de la calidad**. Esta documentación quedará reflejada en **políticas, procedimientos e instrucciones escritas**.

En las siguientes subsecciones (4.1 a 4.13) se va a **fragmentar, analizar y describir** cada uno de los elementos expuestos en dicho listado y **facilitar la comprensión** de los **requisitos** que se describen.

El resto de los apartados del artículo (2, 3 y 4) recogen una serie de consideraciones adicionales que analizaremos en las subsecciones 5.1 y 5.2.

4.1 Cumplimiento reglamentario, evaluación de conformidad y gestión de las modificaciones

AI Act

Art.17.1a – Sistema de gestión de calidad

Una **estrategia para el cumplimiento reglamentario**, incluido el cumplimiento de los procedimientos de **evaluación de la conformidad** y de los procedimientos de **gestión de las modificaciones** de los sistemas de IA de alto riesgo.

El procedimiento de **evaluación de la conformidad** está integrado por toda una serie de procesos y fases a través del cual se verifica que un producto es conforme con los requisitos de la legislación de armonización exigidos para que tal producto se pueda poner en el mercado con ciertas garantías.

El proceso de evaluación de la conformidad se ha desarrollado en la guía “Guía de evaluación de la conformidad”. En dicha guía se describen los dos procedimientos de evaluación de la conformidad aplicables a los sistemas de IA, los cuales, están descritos en los Anexos VI y VII del Reglamento. Estos procedimientos son:

- La autoevaluación interna realizada por el propio proveedor
- El control externo realizado por un organismo notificado.

- Cada uno de estos procedimientos contemplan a su vez una serie de fases que han de alcanzarse para entender superada la evaluación de la conformidad.
- La elección de uno u otro procedimiento de evaluación de conformidad está vinculada al tipo de sistema de IA que desarrolle el proveedor conforme a lo indicado artículo “Evaluación de la conformidad” del Reglamento.

El sistema de gestión de calidad debe contener al menos una indicación del procedimiento de evaluación de la conformidad que resulta aplicable a su sistema de IA de alto riesgo tomando como referencia el apartado B) del punto 3 de la Guía de Evaluación de la Conformidad donde se explica la asignación del procedimiento según el tipo de sistema y su finalidad.

La guía de **Documentación técnica** establece como documentar las gestiones de las modificaciones del sistema de IA en las siguientes vertientes:

- Por un lado, se indica que debe mantenerse un listado tanto de software como de firmware, relacionado con el sistema de IA. Esto incluye la información de las versiones de librerías, componentes software, o elementos de terceros. Debe mantenerse un registro actualizado de versiones, incluyendo librerías, componentes y elementos de terceros, así como un histórico completo de cambios.
- Aquellos cambios predeterminados que estén establecidos en el ciclo de vida del producto deberán estar contemplados dentro del sistema de gestión de la calidad. La guía de documentación técnica establece los datos que son necesarios recopilar en la documentación de cara a la realización de los cambios predeterminados.
- La documentación de cada cambio realizado sobre el sistema de IA deberá de contener los mismos apartados que la documentación general del sistema de IA. Se deberán tener registros de haber superado con éxito los procedimientos de verificación y validación del mismo, para garantizar que el sistema de IA, conserva los parámetros de precisión, solidez y ciberseguridad definidos.
- Debe distinguirse entre cambios sustanciales, cambios no sustanciales y cambios predefinidos, tal como se establece en el artículo sobre modificaciones. Los cambios sustanciales pueden requerir repetir todo o parte del procedimiento de evaluación de conformidad.

En el [apartado 4.2](#) Diseño, control y verificación del diseño y en el [apartado 4.4](#) Examen, prueba y validación, se abordan aspectos relacionados con los aspectos de verificación y validación respectivamente que deben ser tenidos en cuenta a la hora de gestionar actualizaciones del sistema de IA.

El proveedor debe considerar que cada cambio realizado sobre el sistema de IA debe, en sí mismo, estar sujeto a los mismos tipos de controles de calidad aplicables a todo el conjunto. De esta manera, se establece un criterio de continuidad de la calidad, no solo aplicable al proceso de diseño, implementación y puesta en marcha, si no aplicable una vez puesto en marcha el sistema, a cualquier modificación que este pueda sufrir.

4.2 Diseño, control y verificación del diseño

AI Act

Art.17.1b - Sistema de gestión de calidad

Las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **diseño** y el **control** y la **verificación** del **diseño** del sistema de IA de alto riesgo.

El proveedor es responsable, durante el proceso de diseño del sistema de IA del procedimiento sistemático que permitirá la verificación de dicho diseño. El diseño debe basarse tanto en los requisitos técnicos y funcionales del sistema como en las medidas de mitigación del plan de gestión de riesgos.

Un aspecto fundamental que el proveedor debe considerar para el control y verificación del diseño es la relación entre los riesgos y el diseño, esto implica disponer de un seguimiento por parte de los equipos implicados de manera periódica.

Hay tres grandes conjuntos de aspectos de diseño del sistema de IA específicamente abordados por las guías que acompañan a esta y relacionadas con la ciberseguridad, precisión y solidez del sistema de IA.

Ciberseguridad

En la guía de ciberseguridad se establece el concepto de inventario del sistema de IA para que la ciberseguridad se aplique desde el diseño. En la fase de diseño, se deberán establecer los controles de seguridad necesarios, aplicados al inventario de activos y amenazas. Específicamente se debe considerar durante el diseño y relativo a la ciberseguridad (ver apartado La ciberseguridad para el sistema de inteligencia artificial del alto riesgo en la organización, de la guía de ciberseguridad):

- Implicar al delegado de protección de datos (DPD), desde el diseño del sistema de IA y para la planificación de la ciberseguridad, como interlocutor dentro del grupo de trabajo establecido para desarrollar la planificación estando presente en la toma de decisiones. No obstante, el DPD no debe asumir responsabilidades operativas de ciberseguridad, preservando su independencia.
- La relación de la ciberseguridad como establecimiento de controles de seguridad está directamente relacionada con el sistema de gestión de riesgos (ver guía de gestión de riesgos).
- Debe establecerse un cuadro de mando técnico para monitorizar los requisitos de precisión, solidez, ciberseguridad y riesgos definidos en la fase de diseño.

Como se indica en el apartado 3 de la guía de ciberseguridad, se deben realizar unos inventarios de actores y activos (ver el citado apartado para el detalle). El proveedor deberá mantener actualizados los inventarios, y establecer un responsable de que la información que estos reflejan este acorde a las definiciones establecidas en el diseño del sistema de IA.

Precisión

Durante el diseño del sistema de IA de alto riesgo, se establecen los criterios que definen la precisión adecuada para el modelo, con el objetivo de cubrir los requisitos establecidos en el artículo “Precisión, solidez y ciberseguridad” del Reglamento Europeo de IA (ver apartado Garantizando la precisión, en la guía de precisión). El control y la verificación de estos criterios de diseño debe ser realizado por el proveedor garantizando los siguientes aspectos:

- Las métricas seleccionadas, son las adecuadas para la medida de la precisión del modelo, acorde a su finalidad prevista y a la mitigación de los riesgos detectados para el modelo en el análisis de riesgos.
- Del mismo modo la función objetivo, se verificará que es adecuada para la finalidad y riesgos.
- El diseño incluye los mecanismos necesarios para la garantía de la precisión a lo largo del ciclo de vida del modelo.

La guía de precisión contiene las medidas técnicas que deben ser evaluadas en los criterios allí descritos para asegurar su calidad.

Solidez

La solidez de un sistema de IA debe ser verificada y analizada durante todo el ciclo de vida, pero su definición se establece en la fase de diseño. Se deben identificar características reconocidas del sistema y en las cuales deberá mostrar solidez. Estas características deben establecerse en la fase de diseño y deben provenir directamente de dos puntos principales:

- Se deben alinear con el plan de riesgos.
- Deben estar motivadas por la finalidad prevista.

Durante el diseño se deben disponer de evidencias de que el diseño de los criterios de solidez está alineado con los puntos indicados.

Desde el diseño del sistema de IA, el proveedor debe establecer una serie de propiedades para establecer el control de la calidad de la solidez. Estas propiedades son: **fiabilidad, estabilidad, sensibilidad, relevancia y alcanzabilidad**. Parte del proceso sistemático de control de calidad para la solidez, está directamente relacionado con el diseño de los experimentos, cuya realización se abordará en los apartados siguientes.

En la guía de solidez, se establecen los criterios de selección de las métricas propuestas (que pueden consultarse en el Anexo I del mismo documento). Estas métricas son establecidas por diseño para el sistema de IA y deberán tenerse en cuenta durante el proceso de gestión de la calidad para la fase de diseño.

4.3 Desarrollo, control y aseguramiento de la calidad

AI Act

Art.17.1c - Sistema de gestión de calidad

Las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **desarrollo y el control y el aseguramiento de la calidad** del sistema de IA de alto riesgo.

Del mismo modo que el diseño se propone procedimientos sistemáticos para los tres aspectos relacionados con los requerimientos técnicos relativos a ciberseguridad, precisión y solidez, es responsabilidad del proveedor extender dichos procedimientos al proceso de desarrollo del sistema de IA.

Para ello de manera general el proveedor deberá realizar un **seguimiento** de las especificaciones establecidas en el diseño, su traza y cumplimiento, acorde a los requerimientos que se deben cubrir, en relación con ciberseguridad, precisión y solidez. Este seguimiento puede realizarse con diversas herramientas de mercado (*open source* o comerciales) que permitan definir una operativa de ML-OPS que pueda seguir la traza de las acciones realizadas desde el diseño y su implementación durante el desarrollo de la solución.

Las acciones aquí descritas, deberán estar incluidas dentro de los procesos de ML-OPS del sistema de IA, de manera iterativa en cada paso del proceso de desarrollo y garantizando que se cumplen las especificaciones establecidas en el diseño del sistema.

Específico de cada uno de los elementos que hemos considerado en anteriores apartados se debe considerar lo siguiente.

Ciberseguridad

En la guía de ciberseguridad se establece que, durante la implementación del sistema de IA, se deben abordar la implementación de los controles de seguridad acorde a las vulnerabilidades identificadas.

Estos controles de seguridad van dirigidos a establecer salvaguardias sobre las vulnerabilidades relativas a los datos, los ataques adversarios y la explotación de fallos del sistema de IA.

Como medidas de aseguramiento de la calidad para la ciberseguridad durante el proceso de desarrollo en la guía de ciberseguridad se proponen al proveedor, entre otras, las siguientes acciones: mecánicas de equipo rojo/azul, pruebas específicas con test automáticos, SAST Y DAST continuos, análisis de vulnerabilidades conocidas tipo CVE/VWE y pruebas de penetración genéricas y específicas al sistema de IA sobre vectores de vulnerabilidad de AI (ataques adversarios o de penetración)

La calidad durante el desarrollo del sistema exige un análisis de los indicadores de ciberseguridad establecidos en el cuadro de mando para garantizar que durante todo el desarrollo estos se mantienen correctos. Las evidencias del seguimiento de los indicadores de ciberseguridad y su garantía de mantenimiento es una manera de ilustrar **cómo** se demuestran las acciones de calidad.

Precisión

El aseguramiento de la calidad de la precisión durante el desarrollo del sistema de IA se basa en la ejecución de pruebas automatizadas o manuales diseñadas para validar, en cada etapa del desarrollo del modelo, su relación con la precisión definida en el diseño. Por ello, estas pruebas automatizadas deberán tener en cuenta los siguientes puntos:

- El preprocesamiento de los datos (en la guía de precisión).
- Durante el proceso de desarrollo, debe evitarse el sobreaprendizaje, detallado en la guía de precisión).
- Los modelos de contraste o *baseline models* seleccionados, con los que se establece una comparación para el seguimiento del desarrollo y asegurar su control de calidad (ver apartado 4.1.3 de la guía de precisión).

El objetivo principal del control de calidad durante el desarrollo es asegurar que las métricas y sus valores definidos en el diseño se mantengan dentro de los rangos especificados, y que el sistema, en esta fase, funcione conforme a lo previsto o logre progresivamente el comportamiento esperado. Por lo tanto, es necesario conservar evidencia de todas las validaciones realizadas.

Solidez

El control de calidad de la solidez se establece en un procedimiento de dos pasos que se realizan durante todo el desarrollo del sistema de IA:

- Verificación: Entendida como la confirmación, con la provisión de evidencias de que los requisitos especificados en el diseño se cumplen tal y como fueron establecidos.
- Validación: Entendido como la confirmación de los requisitos establecidos sobre la finalidad prevista, y en relación con los criterios para la solidez que se han establecido en la fase de diseño.

Adicionalmente, en este proceso de verificación y validación se debe tener en consideración, como métricas asociadas a las ya seleccionadas, dos parámetros adicionales, cuyos valores deben ser establecidos en diseño y garantizados en desarrollo:

- Eficiencia: durante el desarrollo se deben generar en validación y en verificación evidencias de la eficiencia del sistema, como se detalla en la guía de solidez.
- Rendimiento: en la sección Rendimiento en sistemas de IA profundiza en el rendimiento relacionado con la solidez.

En el apartado Validación y Verificación, de la guía de solidez, se abordan estos dos aspectos. El proveedor durante el desarrollo del sistema deberá asegurarse que el sistema es verificado y validado, y que se registran evidencias del proceso.

4.4 Examen, prueba y validación

AI Act

Art.17.1d - Sistema de gestión de calidad

Los procedimientos de **examen, prueba y validación** que se llevarán a cabo **antes, durante y después del desarrollo** del sistema de IA de alto riesgo, así como la **frecuencia** con que tendrán lugar.

A lo largo de las guías relacionadas del sandbox relativas a ciberseguridad, precisión y solidez que acompañan a esta se han especificado las medidas de examen, prueba y validación que son de aplicación para los sistemas de IA, de acuerdo con el cumplimiento de los requerimientos establecidos en el Reglamento Europeo de IA.

Las pruebas necesarias dependerán del tipo de sistema y los riesgos identificados. Las acciones descritas a continuación combinan requisitos del Reglamento con buenas prácticas recomendadas para el sandbox.

El aseguramiento de la calidad de los controles de seguridad aplicados para mitigar las vulnerabilidades del sistema, son en sí mismos procedimientos de prueba adecuados para validar que dicha calidad se alcanza. En ese sentido, todas las pruebas realizadas en el apartado anterior, con el objetivo de garantizar la calidad durante el desarrollo deberían registrar como mínimo:

- La versión de los datos con las que se han realizado, junto con la versión del modelo.
- Los resultados esperados
- Los resultados obtenidos
- Si la prueba permite la validación del aspecto validado o no
- En caso de que no se valide, indicar la criticidad

Para el caso de que se esté corrigiendo pruebas no exitosas anteriores, se debe incluir al menos:

- La referencia de la batería de pruebas anterior en la que se registró el error
- La solución aplicada para corregirlo.

No todos los sistemas requerirán el mismo nivel de complejidad en las pruebas. El alcance deberá ser proporcional al riesgo y al diseño del sistema, según el artículo 17.2.

Ciberseguridad

En el caso de ciberseguridad, su aseguramiento es en sí mismo un proceso de examen, prueba y validación pues no puede entenderse la calidad en ciberseguridad, sin que esta se encuentre constantemente *tensionada* y puesta a prueba. Por ello los métodos descritos en el apartado anterior son considerados como mecanismos de examen y prueba. Para asegurar que se valida adecuadamente la ciberseguridad se seguirá el proceso de pruebas descrito en este apartado.

Precisión

Los procedimientos destinados al examen y prueba de la precisión son algo más específicos dada su naturaleza formal, aunque deberán registrarse y revisarse tal y como se indica en este apartado. Estos procedimientos pueden establecerse en dos grandes grupos:

- Test de significancia estadística (ver apartado 4.3.2 guía de precisión). Este tipo de test permiten dar validez estadística a la validación de la métrica de precisión seleccionada. El detalle de la tipología de tipos posibles y su realización puede verse en la guía de precisión.
- Benchmarks de bases de datos y modelos (ver apartado 4.3.3 de la guía de precisión). Los benchmarks dependen de la tarea y el estado del arte del campo; por tanto, deberán **actualizarse** conforme pasa el tiempo y los modelos y bases de datos **evolucionan**.

Solidez

Estas pruebas sirven para cuantificar que el sistema alcanza la solidez establecida por diseño, en todos los pasos del ciclo de vida, pero especialmente para la puesta en marcha de un sistema o la distribución de una aplicación. Estos experimentos se han de sumar a las operaciones de verificación y validación realizadas durante el desarrollo.

Los pasos en el proceso de experimentación para la solidez implican: planificar (ver Anexos de la guía de solidez), conducir los experimentos, analizar los resultados, interpretarlos y decidir sobre el resultado la acción a realizar. Durante todos estos pasos se han de dejar las evidencias necesarias de su actuación, que justifiquen el paso siguiente y las decisiones realizadas.

En el apartado 7.1.2, se aborda en detalle el proceso aquí indicado, para la realización de pruebas destinadas a garantizar la solidez del sistema acorde a los requisitos establecidos y al procedimiento de diseño referido. Es un control de calidad para la solidez del sistema que el proveedor debe implementar. Como se ha indicado han de registrarse adecuadamente los resultados de los experimentos.

4.5 Especificaciones técnicas, normas y normas armonizadas

AI Act

Art.17.1e - Sistema de gestión de calidad

Las **especificaciones técnicas**, incluidas las **normas**, que se **aplicarán** y, cuando las **normas armonizadas** pertinentes no se **apliquen en su totalidad** o no **cubran todos los requisitos** pertinentes establecidos en la sección 2, los **medios** que se utilizarán para velar por que el sistema de IA de alto riesgo **cumpla** dichos requisitos.

El sistema de gestión de calidad definido deberá incorporar en su documentación algunos de los siguientes elementos:

- Cuando las haya y se hayan utilizado por parte del proveedor, **listado de normas armonizadas** aplicadas junto con los requisitos del Reglamento que estas cubren.
- Cuando las haya y se hayan utilizado por parte del proveedor, **listado de especificaciones comunes** aplicadas junto con los requisitos del Reglamento que estas cubren.
- **Especificaciones técnicas aplicadas** junto con los requisitos del Reglamento que estas cubren. En el caso de que el proveedor haya cubierto todos los requisitos del Reglamento con la aplicación de normas armonizadas o especificaciones técnicas comunes, no será necesario indicar otras especificaciones técnicas y estándares nacionales e internacionales.

Para **documentar** este apartado recomendamos **lo siguiente**: el sistema de gestión de la calidad podría incorporar las normas armonizadas que cubren algunos o parte de los requisitos exigibles a los sistemas de IA y a su vez otra serie de normas y estándares internacionales que cubren el resto de los requisitos restantes.

Hoy en día no existen normas armonizadas aprobadas por los organismos europeos de normalización ni especificaciones comunes aprobadas por la Comisión Europea que cubran los requisitos que se exigen a los sistemas de IA por parte del Reglamento.

De cara al sandbox y mientras no existan normas armonizadas y especificaciones comunes no existan ni se apliquen por el proveedor, **el sistema de gestión de la calidad** habrá de contener aquellas especificaciones técnicas que se hayan aplicado por parte del proveedor para cubrir los requisitos del Reglamento, en este caso:

- **Las Guías Técnicas** que se han facilitado junto con los requisitos que cubren del Reglamento.
- Para aquellos casos en los que los proveedores hayan ido más allá de las Guía Técnicas facilitadas, las **especificaciones técnicas basadas en los estándares nacionales o internacionales** que se hayan podido utilizar junto con los requisitos que cubren del Reglamento.

La forma de documentar esta información podría tomar como referencia la siguiente tabla (**ejemplo no real**):

Requisito cubierto	Norma armonizada/especificación común/estándar
Artículo 12.2	Estándar nacional X
Artículos 14. Apartado 1 y 2	Norma armonizada X
Artículo 15. Apartados 1, 2 y 3.	Norma ISO X

La tabla es orientativa: no todos los requisitos del Reglamento deberán vincularse necesariamente a una norma o estándar.

Para más información consulte la Guía de Evaluación de la Conformidad y la Guía de Documentación Técnica.

4.6 Sistemas y procedimientos de gestión de datos

AI Act

Art.17.1f – Sistema de gestión de calidad

Los **sistemas y procedimientos de gestión de datos**, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin.

El sistema de gestión de calidad definido deberá incorporar en su documentación, los sistemas y procedimientos de gestión de datos descritos en este apartado. El artículo del Reglamento “Datos y gobernanza de datos” recoge un listado de requisitos más amplio que todo sistema de IA de alto riesgo debe cumplir. De forma resumida, los conjuntos de datos de entrenamiento, validación y prueba se someterán a las siguientes prácticas de gobernanza y gestión de datos:

- Elección de un **diseño adecuado**.
- **Procesos de recopilación** de datos.
- **Operaciones de tratamiento** para la **preparación** de los datos (*la anotación, el etiquetado, la depuración, el enriquecimiento y la agregación*).
- **Formulación de los supuestos** pertinentes con respecto a la **información de los datos que miden y representan**.
- **Evaluación previa de la disponibilidad, la cantidad y la adecuación** de los conjuntos de datos necesarios:
 - Serán pertinentes y representativos.
 - Estarán completos.
 - Tendrán las propiedades estadísticas adecuadas.
 - Tendrán en cuenta, en función de su finalidad prevista, las características o elementos particulares del contexto geográfico, conductual o funcional en el que se pretende utilizar el HRAIS.
- **Análisis de sesgos** (*atendiendo aquellos que puedan afectar a la salud y la seguridad de las personas o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión*).
- **Detección y remediación de lagunas o deficiencias** en los datos:
 - Carecerán de errores.

El proveedor deberá documentar en su SGC cómo se implementan estos procesos, indicando responsables, herramientas, evidencias y criterios de revisión. Estos requisitos

deberán aplicarse sin perjuicio de los principios y obligaciones del RGPD, incluyendo minimización, limitación de finalidad y evaluaciones de impacto cuando proceda

Además, en la medida en que sea **estrictamente necesario** para garantizar la **vigilancia, la detección y la corrección de los sesgos**, se podrán tratar las **categorías especiales de datos personales, ofreciendo siempre las salvaguardias adecuadas** para los **derechos y las libertades** fundamentales de las personas.

Para el adecuado cumplimiento de estos requisitos se ha desarrollado la “Guía de datos y gobernanza de datos”. En dicha guía se presentan las medidas que servirán a proveedores y responsables del despliegue para dar cumplimiento con el artículo “**Datos y gobernanza de datos**”. En la sección “Documentación técnica” de dicha guía se detalla cómo se deberá abordar la documentación de cada medida.

4.7 Sistema de gestión de riesgos

AI Act

Art.17.1g – Sistema de gestión de calidad.

El **sistema de gestión de riesgos** que se menciona en el artículo 9.

Un **sistema de gestión de riesgos** tiene por objetivo la **identificación y análisis de riesgos** y la **implementación de medidas mitigadoras**. Entendemos por riesgo, cualquier factor con una probabilidad de suceder y un impacto en caso de que suceda. De hecho, el riesgo se calcula como el producto de dichos factores, probabilidad e impacto.

En el contexto del Reglamento Europeo de la IA, el sistema de gestión de riesgos que se desarrolle deberá prestar especial atención a los **riesgos que puedan afectar a la salud, la seguridad y los derechos fundamentales de las personas**. En este sentido, se deberá poner el foco en la identificación y análisis de cualquier riesgo que pueda tener especial afectación en los elementos mencionados. Por consiguiente, se deberán implementar las medidas adecuadas que permitan mitigar los riesgos identificados y evaluados.

Para el adecuado cumplimiento de estos requisitos se ha desarrollado la “Guía de gestión de riesgos”. En dicha guía se presentan las medidas que servirán a proveedores y responsables del despliegue para dar cumplimiento con el artículo “**Sistema de gestión de riesgos**”. En la sección “Documentación técnica” de dicha guía se detalla cómo se deberá abordar la documentación de cada medida.

4.8 Sistema de vigilancia poscomercialización

Al Act

Art.17.1h – Sistema de gestión de calidad

El establecimiento, la implantación y el mantenimiento de un **sistema de vigilancia poscomercialización** con arreglo al artículo 72.

Un sistema de vigilancia poscomercialización de sistemas de IA de alto riesgo se concibe como un **conjunto de procesos y herramientas** orientados a recabar datos de un sistema para transformarlos en una serie de indicadores sobre su actividad con el objetivo de supervisar los sistemas de inteligencia artificial (IA) **después de su introducción en el mercado o puesta en servicio, según corresponda**. El objetivo es que el proveedor pueda evaluar si los sistemas de IA cumplen los requisitos establecidos en el capítulo III, sección 2, a lo largo de todo el ciclo de vida del sistema inteligente.

Para el adecuado cumplimiento de estos requisitos se ha desarrollado la “Guía de sistema de vigilancia poscomercialización”. En dicha guía se presentan las medidas que servirán a proveedores y responsables del despliegue para dar cumplimiento con el artículo “Vigilancia poscomercialización”. El sistema de vigilancia se articula principalmente a través del proveedor, sin perjuicio de las obligaciones de uso, supervisión y notificación que corresponden al responsable del despliegue. En la sección “Documentación técnica” de dicha guía se detalla cómo se deberá abordar la documentación de cada medida.

4.9 Notificación de incidentes graves

Al Act

Art.17.1i – Sistema de gestión de calidad

Los **procedimientos** asociados a la **notificación** de un **incidente grave** con arreglo al artículo 73.

La guía de gestión de incidentes establece en su apartado 4.1.1, cómo abordar los requisitos de notificación de incidentes graves acorde al Reglamento Europeo de IA. En dicho apartado se describe el procedimiento de notificación de incidentes graves, y las medidas que permiten abordar dicho procedimiento. Un aspecto importante de los procedimientos de notificación de incidentes es que también implican al responsable del despliegue, en la medida en la que este es responsable de notificar al proveedor del sistema de IA a través del canal establecido para ello. Especial atención requiere el apartado 4.1.1 de la citada guía que resume de manera visual el procedimiento de

notificación de incidentes graves, que debe ser incluido dentro del sistema de gestión de calidad.

El sistema de gestión de la calidad debe tener claramente documentado al menos:

- La cadena de responsabilidad de la notificación del incidente, que incluya la figura del DPD, así como otras figuras de relevancia a nivel de cumplimiento que sean de aplicación. La notificación a las autoridades deberá realizarse en los plazos establecidos por el Reglamento.
- El mecanismo de registro de incidentes que se utiliza, así como el mecanismo de generación y conservación de las evidencias.
- La cadena de resolución del incidente, con los responsables de aplicación de este. El proveedor es el principal sujeto obligado frente a las autoridades. El responsable del despliegue deberá informar al proveedor sin dilación a través del canal establecido.
- En el caso del proveedor, y que el incidente afecte a varios responsables de despliegue del sistema de IA (potencialmente a todos), la cadena de responsabilidad para la comunicación, el canal y el formato, en el que se deberán proporcionar instrucciones claras al responsable del despliegue de cómo proceder para ese incidente en particular y si deberán, en cualquier caso, los responsables del despliegue a su vez notificar a las autoridades, personas físicas afectadas por el incidente en sus propios sistemas.
- La notificación del incidente durante la utilización del sistema es un aspecto que podrá ser también responsabilidad del responsable del despliegue del sistema de IA, por lo que los aspectos indicados, se aplican a este también.

4.10 Comunicación

AI Act

Art.17.1j – Sistema de gestión de calidad

La gestión de la **comunicación** con las **autoridades nacionales competentes**; las autoridades competentes, **incluidas las sectoriales**, que permiten acceder a datos o facilitan el acceso a ellos; los **organismos notificados**; otros **operadores**; los **clientes**, u otras **partes interesadas**.

El Reglamento establece a lo largo de su articulado un conjunto de obligaciones que se exigen a los proveedores y responsables del despliegue de sistemas de IA con relación a las comunicaciones que estos han de desplegar con las autoridades nacionales competentes, organismos notificados, clientes, etc.

Sistema de gestión de calidad definido deberá incorporar en su documentación los distintos procedimientos de comunicación derivados de las obligaciones previamente indicadas, entre otros, estos procedimientos pueden abarcar:

- Se ha de **indicar y describir el canal o canales de comunicación** que se utilizarán para cada una de las comunicaciones que se derivan de las diferentes obligaciones descritas.
- Se ha de **contemplar el formato o formatos** en los que se facilitarán los documentos que en su caso se requieran.
- Se ha de **nombrar a la persona o personas responsables** que se encargarán de gestionar las diferentes comunicaciones.
- Se deben **implementar y describir las herramientas** que permitan el acceso a los datos, registros, código fuente y otras acciones que se deriven de estas obligaciones. Algunas de estas herramientas están mencionadas en la Guía de Documentación Técnica.
- El acceso a código fuente o datos solo deberá habilitarse cuando sea exigible conforme al procedimiento regulatorio aplicable.

Para más información, recuerde que las obligaciones que se derivan del Anexo VII del Reglamento sobre la evaluación por parte de un organismo notificado del sistema de gestión de la calidad y la documentación técnica también se analizan en la Guía de Documentación Técnica y en la Guía de Evaluación de la Conformidad.

4.11 Documentación

AI Act

Art.17.1k – Sistema de gestión de calidad

Los **sistemas y procedimientos** destinados a llevar un **registro** de toda la **documentación e información pertinente**.

La documentación del sistema de IA se ha articulado a lo largo de las guías que acompañan a esta y relativas al sandbox en dos vertientes.

Por un lado, cada guía, especialmente aquellas que tienen una vertiente más técnica y menos procedimental establecen los criterios de documentación necesarios para una correcta aplicación de las medidas. Así ocurre entre otras, con las guías de ciberseguridad, precisión, solidez y registros.

Por otro lado, de manera específica la guía de Documentación Técnica proporciona la estructura del contenido de la documentación técnica del sistema de IA de alto riesgo y los criterios de conservación de esta.

El proveedor deberá establecer una serie de medidas técnicas para mantener un registro de la documentación e información pertinente. La documentación deberá mantenerse durante todo el ciclo de vida del sistema, desde su diseño hasta su retirada, y deberá también conservarse durante los plazos exigidos por el Reglamento tras la retirada del sistema. Para ello con el objetivo de mantener la documentación actualizada, y mantener un registro de toda ella el proveedor debe al menos:

- Establecer, dentro de los procesos de gestión del sistema de inteligencia artificial, un **procedimiento de seguimiento de los cambios** que tenga su reflejo en la actualización de la documentación.
- Generar una **cadena de responsabilidad**, o establecer un responsable de la gestión del cambio sobre el sistema, que se encargue de actualizar la documentación acorde a los cambios.
- La documentación de los **cambios en el sistema** de inteligencia artificial debe tener el **nivel de completitud del resto** de la documentación técnica descrita en esta guía.
- **Establecer, definir y dimensionar** acorde un sistema de gestión documental, solución técnica equivalente, que le permita garantizar la conservación y cambios de esta. Esto puede materializarse en repositorios documentales, sistemas de gestión de calidad corporativos u otras soluciones equivalentes. El sistema debe garantizar la conservación de la documentación y la posibilidad de acceso al mismo por parte de organismos notificados para su evaluación. Igualmente, aquella documentación técnica que tenga como objetivo servir de instrucciones al responsable del despliegue, deberá estar accesible a este.

4.12 Gestión de los recursos

AI Act

Art.17.1I – Sistema de gestión de calidad

La **gestión de los recursos**, incluida la **seguridad** de las **medidas** relacionadas con el suministro.

Antes de abordar este apartado se recomienda al lector revisar la sección 1.2 donde se expone detalladamente la relación entre un sistema de gestión de calidad según se entiende en el estándar de referencia ISO 9001 y el desarrollado en el Reglamento Europeo de la IA.

Teniendo en consideración lo indicado en dicha sección 1.2, cabe destacar que la gestión de los recursos se ha vinculado que de forma más directa a lo expuesto en la ISO 9001. Estos recursos son esenciales para sostener el cumplimiento continuo del Reglamento durante todo el ciclo de vida del sistema. Así, en este apartado, vamos a tratar de guiar al lector detallando los elementos principales que han de considerarse en la gestión de los recursos:

Personas:

- **De acuerdo con la ISO 9001:** *“La organización debe determinar y proporcionar las personas necesarias para la implementación eficaz de un sistema de gestión de la calidad y para la operación y control de sus procesos”.*
- **Cómo enfocarlo:** Lo que debemos hacer en este caso es analizar detalladamente las personas y los perfiles que necesitaremos para poder abordar todos los elementos establecidos en el sistema de gestión de calidad del Reglamento de la

IA. Para ello debemos valorar estos elementos y la información facilitada para cada uno de ellos a lo largo de la presente guía con el fin de poder realizar una estimación lo más adecuada posible.

Infraestructura:

- **De acuerdo con la ISO 9001:** *“La organización debe determinar, proporcionar y mantener la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de los productos y servicios”.*
- **Cómo enfocarlo:** La ISO 9001 incluye en el apartado de infraestructura algunos elementos como los recursos de software y hardware o las tecnologías de la información y la comunicación. En el contexto del desarrollo del sistema de gestión de calidad del Reglamento Europeo que se ha analizado a lo largo de esta guía, los elementos relacionados con la infraestructura serían todos aquellos recursos técnicos y tecnológicos necesarios para el desarrollo de dicho sistema. Por ejemplo, para el desarrollo de los procedimientos de examen, prueba y validación del apartado “d)”, tal y como se indica en la sección 4.4 y como se detalla en las guías allí referenciadas de ciberseguridad, precisión y solidez, se deberá contar con la infraestructura necesaria para el desarrollo de dichas pruebas.

Ambiente para la operación de los procesos:

- **De acuerdo con la ISO 9001:** *“La organización debe determinar, proporcionar y mantener el ambiente necesario para la operación de sus procesos y para lograr la conformidad de los productos y servicios”.*
- **Cómo enfocarlo:** La ISO 9001 incluye en este apartado algunos elementos como factores humanos, físicos, sociales o psicológicos. En este contexto, la organización deberá determinar cuáles son los factores ideales en cada escenario (temperatura, iluminación, circulación de aire, ruido, prevención del estrés, etc.) para el adecuado desarrollo del sistema de gestión de calidad.

Recursos de seguimiento y medición:

- **De acuerdo con la ISO 9001:** *“La organización debe determinar y proporcionar los recursos necesarios para asegurarse de la validez y fiabilidad de los resultados cuando se realice el seguimiento o la medición para verificar la conformidad de los productos y servicios con los requisitos. La organización debe asegurarse de que los recursos proporcionados son apropiados para el tipo específico de actividades de seguimiento y medición realizadas y que se mantienen para asegurarse de la idoneidad continua para su propósito. Además, la organización debe conservar la información documentada apropiada como evidencia de que los recursos de seguimiento y medición son idóneos para su propósito”.*
- **Cómo enfocarlo:** Los sistemas de IA son artefactos software con una naturaleza muy especial, eso hace que su comportamiento a lo largo del tiempo pueda variar, no solo en aquellos casos en los que el sistema continúa aprendiendo con el tiempo, si no en general en todos los escenarios. La aparición de espacios de dominio no esperados en los datos de entrada, o incluso la existencia de errores o fallos no detectados que pueden afectar a la precisión, solidez, ciberseguridad (consultar guías correspondientes) o incluso a la finalidad prevista causando daño a las personas o afectar derechos y libertades, son aspectos que no pueden ser

descartados. Este tipo de monitorización encaja en el escenario de una monitorización poscomercialización (consultar dicha guía), en la que se realiza un seguimiento de los parámetros, métricas y controles técnicos que se establecieron en el diseño y con el objetivo de cubrir los riesgos encontrados en el plan de riesgos, especialmente aquellos relacionados con garantizar la salud, seguridad y derechos fundamentales de las personas. La monitorización deberá incluir también aspectos organizativos y humanos, como la supervisión de decisiones automatizadas.

Conocimientos de la organización:

- **De acuerdo con la ISO 9001:** *“La organización debe determinar los conocimientos necesarios para la operación de sus procesos y para lograr la conformidad de los productos y servicios. Estos conocimientos deben mantenerse y ponerse a disposición en la medida en que sea necesario. Cuando se abordan las necesidades y tendencias cambiantes, la organización debe considerar sus conocimientos actuales y determinar cómo adquirir o acceder a los conocimientos adicionales necesarios y a las actualizaciones requeridas”.*
- **Cómo enfocarlo:** La ISO 9001 incluye en este apartado los conocimientos adquiridos en base a la experiencia (por ejemplo, lecciones aprendidas de proyectos o resultados de las mejoras de procesos), mediante la consulta de fuentes internas (por ejemplo, propiedad intelectual o documentación interna generada a partir de proyectos y experiencias previas) y mediante la consulta de fuentes externas (por ejemplo, consulta de normas y estándares o recopilación de conocimientos provenientes de clientes o proveedores). En este contexto, con el objetivo de desarrollar el sistema de gestión de calidad del Reglamento Europeo de la IA, la organización deberá asegurarse de que dispone de los conocimientos necesarios y suficientes como para abordar cada uno de los aspectos exigidos por dicho Reglamento y analizados a lo largo de la presente guía.

4.13 Marco de rendición de cuentas

AI Act

Art.17.1m – Sistema de gestión de calidad

Un **marco de rendición de cuentas** que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

El objetivo de este marco de rendición de cuentas es establecer las responsabilidades y autorizaciones en torno a los diferentes elementos que componen el sistema de gestión de la calidad. Las responsabilidades deben asignarse a todo el personal involucrado en alguno de estos procesos y deberá reflejarse y documentarse en descripciones de puestos de trabajo y declaraciones similares, cuando corresponda. Además, las responsabilidades

asignadas deberán quedar bien documentadas y reflejadas en el documento desarrollado para recoger el sistema de gestión de calidad.

Así, en este apartado se van a recoger todos los elementos que se han abordado a lo largo de esta guía y disponer algunos ejemplos de cómo se podrían asignar las responsabilidades para cada uno de ellos, revisando cada uno de los apartados del artículo.

Ejemplo - Resumen visual de asignación de responsabilidades

A continuación, puede encontrarse una tabla a modo resumen visual de los siguientes del marco de rendición de cuentas que será analizado por apartado. Las funciones indicadas pueden repartirse entre varias personas o equipos según la estructura de la organización.:

Requisito	Propuesta de responsable
Estrategia para el cumplimiento de la normativa	Perfil legal
Técnicas sistemáticas que se utilizarán en el diseño	Miembro del equipo de diseño
Técnicas sistemáticas que se utilizarán en el desarrollo	Miembro del equipo de desarrollo
Procedimientos de examen, prueba y validación	Miembro del Red/blue team o del equipo de QA
Especificaciones técnicas, incluidas las normas, que se aplicarán	Perfil legal + perfil técnico
Sistemas y procedimientos de gestión de datos	CDO o responsable del sistema de IA
El sistema de gestión de riesgos	CRO o responsable del sistema de IA
Sistema de vigilancia poscomercialización	Miembro del equipo de QA
Procedimientos asociados a la notificación de incidentes graves	Responsable de calidad
Comunicación con las ANC	Departamento jurídico o cumplimiento; con participación del DPO cuando proceda.

Registro de documentación

Miembro del equipo de cumplimiento

Gestión de los recursos

Miembro de RRHH

AI Act

Art.17.1a – Sistema de gestión de calidad

Una **estrategia para el cumplimiento reglamentario**, incluido el cumplimiento de los procedimientos de **evaluación de la conformidad** y de los procedimientos de **gestión de las modificaciones** de los sistemas de IA de alto riesgo.

Ejemplo – Asignación de responsabilidad

Como regla general, los responsables de este apartado deberían ostentar un perfil legal. Si bien, y dada la estrecha relación del proceso de evaluación de conformidad con el proceso de diseño del sistema de IA, es recomendable que también estén presentes miembros del equipo responsable del diseño del sistema, así como aquellos a los que se asignen tareas de vigilancia poscomercialización.

AI Act

Art.17.1b – Sistema de gestión de calidad

Las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **diseño** y el **control** y la **verificación** del **diseño** del sistema de IA de alto riesgo.

Ejemplo – Asignación de responsabilidad

Los responsables de este apartado están identificados dentro del equipo que realiza el diseño, que tiene la responsabilidad de realizar el seguimiento de la calidad en el proceso del diseño, cuya labor es supervisada y validada por los responsables técnicos del proveedor. Así en una pyme o en una empresa de nueva creación podrán ser identificados dentro de los responsables de producto, y en compañías de mayor tamaño estar relacionados directamente o con la oficina del CTO.

AI Act

Art.17.1c – Sistema de gestión de calidad

Las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el **desarrollo y el control y el aseguramiento de la calidad** del sistema de IA de alto riesgo.

Ejemplo – Asignación de responsabilidad

Del mismo modo que en apartado anterior, la estructura del equipo de desarrollo será la responsable en toda su extensión del aseguramiento de la calidad durante el proceso de desarrollo. Esta asignación de responsabilidad debe ir dirigida desde las figuras equivalentes jefe de proyecto, jefes de equipo hasta las asociadas al equipo de desarrollo. Del mismo modo que en el anterior caso, estos deberán reportar dependiendo de la estructura del proveedor a la figura interna correspondiente y en compañías de mayor tamaño de nuevo relacionado con el CTO.

AI Act

Art.17.1d – Sistema de gestión de calidad

Los procedimientos de **examen, prueba y validación** que se llevarán a cabo **antes, durante y después del desarrollo** del sistema de IA de alto riesgo, así como la **frecuencia** con que tendrán lugar.

Ejemplo – Asignación de responsabilidad

La asignación de responsabilidad para los procedimientos de examen, prueba y validación está relacionada con la estructura que el equipo de aseguramiento de la calidad tenga dentro de la estructura del proveedor. Para todos los procedimientos asociados, deberá existir un equipo responsable de su realización, generación de evidencias y validación de resultados. Dependiendo del tamaño de la organización del proveedor, este equipo podrá tener diferente tamaño y estructura: desde pequeños equipos en formato equipo rojo/azul, hasta grandes equipos de QA y validación. Independientemente del tamaño se recomienda al proveedor que los equipos de diseño y desarrollo sean diferentes de los de pruebas.

AI Act

Art.17.1e – Sistema de gestión de calidad

Las **especificaciones técnicas**, incluidas las **normas**, que se **aplicarán** y, cuando las **normas armonizadas** pertinentes no se **apliquen en su totalidad**, los **medios** que se utilizarán para **velar** por que el sistema de IA de alto riesgo **cumpla los requisitos** establecidos en la sección 2 del presente capítulo.

Ejemplo – Asignación de responsabilidad

El perfil de los responsables de esta sección englobará a personas con conocimientos legales de la materia, así como perfiles más técnicos relacionados con las diferentes normas armonizadas y en su caso estándares internacionales que se pretendan aplicar. La distinción de estos perfiles obedece a la propia naturaleza de las especificaciones técnicas y normas armonizadas. Así, el perfil jurídico sobre todo valorará las consecuencias legales que tiene la no aplicación/aplicación parcial/ aplicación total de normas armonizadas/especificaciones comunes/estándares internacionales de cara al Reglamento de IA. Por su parte, los responsables que ostentan un perfil marcadamente técnico sobre todo se centrarán de valorar qué normas armonizadas/especificaciones comunes/ estándares internacionales aplican para el sistema de IA específico y cómo estás han de implementarse.

AI Act

Art.17.1f – Sistema de gestión de calidad

Los **sistemas y procedimientos de gestión de datos**, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin.

Ejemplo – Asignación de responsabilidad

Los sistemas y procedimientos de gestión de datos, tal y como se describen en la guía de datos y gobernanza de datos desarrollada para dar cumplimiento al artículo “Datos y gobernanza de datos” del Reglamento, deben ser coordinados y gestionados idealmente por una figura transversal a toda la organización (como un CDO en aquellas organizaciones que lo dispongan). Este responsable será el encargado de asegurar que se abordan todos los elementos descritos en la mencionada guía para el adecuado cumplimiento de los requisitos de datos y gobernanza de datos. Así como también de coordinar al resto de posibles figuras involucradas, por ejemplo, será necesario contar

con el apoyo del DPD para el adecuado cumplimiento con la normativa de protección de datos de carácter personal cuando resulte de aplicación ésta. En una organización más pequeña, como una pyme, es posible que este rol quede ostentado por el responsable del sistema de IA, si, por ejemplo, en este caso dicho responsable se está haciendo cargo del cumplimiento de todos los requisitos del Reglamento Europeo de la IA.

AI Act

Art.17.1g – Sistema de gestión de calidad

El **sistema de gestión de riesgos** que se menciona en el artículo 9.

Ejemplo – Asignación de responsabilidad

El sistema de gestión de riesgos, tal y como se describe en la guía de gestión de riesgos desarrollada para dar cumplimiento con el artículo “Sistema de gestión de riesgos” del Reglamento, debe ser coordinado y gestionado idealmente por una figura transversal a toda la organización (como un CRO en aquellas organizaciones que lo dispongan). Este responsable será el encargado de asegurar que se abordan todos los elementos descritos en la mencionada guía para el adecuado cumplimiento de los requisitos relacionados con la gestión de los riesgos. En una organización más pequeña, como una pyme, es posible que este rol quede ostentado por el responsable del sistema de IA, si, por ejemplo, en este caso dicho responsable se está haciendo cargo del cumplimiento de todos los requisitos del Reglamento Europeo de la IA.

AI Act

Art.17.1h – Sistema de gestión de calidad

El establecimiento, la implantación y el mantenimiento de un **sistema de vigilancia poscomercialización** con arreglo al artículo 72.

Ejemplo – Asignación de responsabilidad

Tal y como se detalla en la guía desarrollada para la implementación de un sistema de vigilancia poscomercialización, los requisitos descritos en el artículo indicado están enfocados en las medidas que debe de tomar el proveedor de servicio una vez el sistema inteligente se encuentra en producción. Por lo tanto, es responsabilidad del proveedor evaluar que durante todo el ciclo de vida se cumplen los requisitos expuestos en dicho artículo. La responsabilidad de la definición y coordinación de este sistema, en una organización de gran tamaño, podría recaer sobre los equipos encargados del aseguramiento de la calidad. De igual forma que se mencionaba en el apartado b), para

todos los procedimientos asociados, deberá existir un equipo responsable de su realización, generación de evidencias y validación de resultados. Dependiendo del tamaño de la organización del proveedor, este equipo podrá tener diferente tamaño y estructura. Independientemente del tamaño se recomienda al proveedor que los equipos de diseño y desarrollo sean diferentes de los de pruebas.

Al Act

Art.17.1i – Sistema de gestión de calidad

Los **procedimientos** asociados a la **notificación** de un **incidente grave** con arreglo al artículo 73.

Ejemplo – Asignación de responsabilidad

En el propio apartado se han indicado las cadenas de responsabilidad que deben tenerse en cuenta, y si estructura, que según el tamaño de la compañía deberán tener adecuarse a disponer de una responsabilidad clara. Es muy importante que el proveedor cuente con un canal de comunicación con los responsables del despliegue para el mecanismo de notificación de incidentes. Se remite al citado apartado para el detalle.

Al Act

Art.17.1j – Sistema de gestión de calidad

La gestión de la **comunicación** con las **autoridades nacionales competentes**; las autoridades competentes, **incluidas las sectoriales**, que permiten acceder a datos o facilitan el acceso a ellos; los **organismos notificados**; otros **operadores**; los **clientes**, u otras **partes interesadas**.

Ejemplo – Asignación de responsabilidad

En función del tipo de comunicación que esté contemplada, será conveniente identificar distintos responsables. Puede resultar interesante que exista un responsable central que aglutine todas y cada una de las comunicaciones posibles a las que hace mención el Reglamento y, a su vez, existan niveles inferiores específicos para la gestión de cada una de las comunicaciones. Por ejemplo, los proveedores están obligados a facilitar la documentación que requieran las autoridades en materia de protección de derechos fundamentales. Este precepto habilita a las autoridades de protección de datos a solicitar cierta documentación generada a raíz del cumplimiento del Reglamento de IA, esa comunicación, si bien puede estar centralizada en un responsable general, la gestión específica de la misma podría llevarse a cabo por una unidad específica, en este caso, el Delegado de Protección de Datos (si lo hay) o departamento jurídico correspondiente.

AI Act

Art.17.1k – Sistema de gestión de calidad

Los **sistemas y procedimientos** destinados a llevar un **registro** de toda la **documentación e información pertinente**.

Ejemplo – Asignación de responsabilidad

La guía de documentación técnica establece una serie de contenidos que deben de ser registrados e incorporados para el sistema de IA. Este tipo de información es muy vertical y extensa a lo largo de la empresa, y como se comenta en la indicada guía dependiendo del tamaño de la organización del proveedor puede ser llevada a cabo por diferentes equipos, o por equipos más multidisciplinares (para el caso de pyme y empresas de nueva creación). Dado este carácter vertical, es necesario que exista una figura responsable de la coordinación y aspectos generales del proceso (formato, repositorio), que en grandes empresas puede estar relacionado con los equipos de cumplimiento, y en pymes o empresas de nueva creación, depender de la estructura de dirección de esta.

AI Act

Art.17.1l – Sistema de gestión de calidad

La **gestión de los recursos**, incluida la **seguridad** de las **medidas** relacionadas con el suministro.

Ejemplo – Asignación de responsabilidad

La gestión de los recursos, abordada en esta misma guía, podría ser coordinada por una figura transversal a toda la organización como un departamento encargado del aseguramiento de la calidad. En todo caso, cada uno de los pilares descritos dentro de la gestión de los recursos probablemente sea apoyado desde departamentos diferentes. Así, por ejemplo, la gestión de los recursos relacionados con las personas y perfiles y los conocimientos necesarios sería responsabilidad del departamento de recursos humanos.

5. Otros elementos a considerar

5.1 Implementación del sistema de gestión de calidad proporcional al tamaño de la organización del proveedor

En esta sección se abordará lo especificado en el apartado 2 del artículo:

Al Act

Art.17.2 – Sistema de gestión de calidad

La inclusión de los aspectos mencionados en el apartado 1 será **proporcional al tamaño de la organización del proveedor**.

Adicionalmente, recogemos en esta sección lo indicado en el **Recital 146**:

Al Act

Recital 146

Además, habida cuenta del tamaño muy reducido de algunos operadores y con el fin de garantizar la proporcionalidad en lo que respecta a los costes de la innovación, conviene permitir a las microempresas cumplir una de las obligaciones más costosas, a saber, establecer un sistema de gestión de la calidad, de una manera simplificada que reduciría la carga administrativa y los costes para dichas empresas sin afectar al nivel de protección ni a la necesidad de cumplir los requisitos para los sistemas de IA de alto riesgo.

La Comisión debería elaborar directrices para especificar los elementos del sistema de gestión de la calidad que deben cumplir de esta manera simplificada las microempresas.

Este texto trata sobre la necesidad de **garantizar la proporcionalidad** en la aplicación del Reglamento considerando el **tamaño** de los operadores y los **costes** de innovación. Se propone **escalar las obligaciones** más costosas al **tamaño de la empresa**, minimizando los costes asociados para las microempresas al establecer el sistema de gestión de calidad tratado en esta guía, para **reducir la carga administrativa y los costos**. Al hacerlo, se busca proteger a las microempresas sin comprometer el nivel de protección de la IA ni la necesidad de cumplir con los requisitos aplicables a los sistemas de IA de alto riesgo. La proporcionalidad no exime del cumplimiento de los requisitos legales, sino que permite adaptar la forma de documentarlos y organizarlos al tamaño de la entidad. La condición de microempresa no excluye tampoco la aplicación del régimen de sistemas de IA de alto riesgo cuando el sistema cumpla los criterios del Reglamento.

En general, el objetivo de este texto es encontrar un equilibrio entre la aplicación del Reglamento y la necesidad de proteger a las microempresas que podrían tener dificultades para cumplir con todas las obligaciones regulatorias. La finalidad es promover la innovación y el crecimiento de las empresas, mientras se asegura la protección de los responsables del despliegue. La proporcionalidad es un principio clave en el Reglamento y este texto hace hincapié en la necesidad de aplicarlo correctamente para lograr estos objetivos.

5.2 Entidades financieras y proveedores sujetos a legislación sectorial

En esta sección se abordará lo especificado en el apartado 3 y 4 del artículo que establece:

AI Act

Art.17.3 – Sistema de gestión de calidad

Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al Derecho sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicho Derecho.

Este apartado hace referencia a la regulación de los proveedores de sistemas de inteligencia artificial de alto riesgo y cómo pueden cumplir con las obligaciones relativas a los sistemas de gestión de calidad. En concreto, se establece que en el caso de aquellos proveedores que ya están sujetos a obligaciones relacionadas con los sistemas de gestión de calidad según la legislación sectorial relevante de la Unión Europea, los aspectos descritos en el apartado 1 pueden formar parte de los sistemas de gestión de calidad existentes bajo esa legislación.

En otras palabras, el texto sugiere que en algunos casos los requisitos regulatorios específicos para la IA de alto riesgo podrían integrarse en los sistemas de gestión de calidad ya existentes que se aplican a los proveedores de sistemas de IA de alto riesgo, siempre y cuando dichos sistemas cumplan con las normativas sectoriales aplicables de la Unión Europea.

La finalidad de este texto es proporcionar claridad y coherencia en la regulación de la IA de alto riesgo, al tiempo que se evita duplicidad de requisitos y se facilita su cumplimiento. Esto también puede ayudar a mejorar la eficacia y eficiencia en la regulación de la IA de alto riesgo, ya que se aprovechan los sistemas de gestión de calidad existentes para cumplir con los nuevos requisitos regulatorios. En resumen, el objetivo del texto es garantizar la regulación de la IA de alto riesgo en la UE, reduciendo la carga administrativa y de costos para los proveedores, al mismo tiempo que se asegura la protección y seguridad del responsable del despliegue final.

AI Act

Art.17.4 – Sistema de gestión de calidad

En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

Este texto se refiere a la regulación de proveedores que son entidades financieras y cómo pueden cumplir con las obligaciones de establecer un sistema de gestión de calidad en el marco de la legislación de la Unión Europea en materia de servicios financieros. En particular, se establece que, si las entidades financieras ya cumplen con los requisitos relativos a sus sistemas o procesos de gobernanza interna en virtud de la legislación de la UE en materia de servicios financieros, se considerará que han cumplido con la obligación de establecer un sistema de gestión de calidad. No obstante, se especifica que en cualquier caso deberá cumplirse con lo establecido en los subapartados g) h) e i).

Este texto sugiere que las normas relativas a los sistemas o procesos de gobernanza interna pueden cumplir con las obligaciones de establecer un sistema de gestión de calidad. Además, se menciona que se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo “Normas armonizadas” del Reglamento en ese contexto.

La finalidad de este texto es promover la eficiencia y la simplificación en la regulación de los proveedores que son entidades financieras y que ya están sujetos a requisitos específicos de gobernanza interna en virtud de la legislación de la UE en materia de servicios financieros. Esto significa que no tendrán que cumplir con requisitos adicionales en relación con el sistema de gestión de calidad si ya cumplen con los requisitos de gobernanza interna (con la excepción de los subapartados g) h) e i)). El objetivo de este enfoque es evitar la duplicación de requisitos y reducir la carga administrativa para las entidades financieras. En resumen, el texto busca mejorar la eficacia y eficiencia de la regulación de los proveedores que son entidades financieras, al mismo tiempo que se garantiza la protección de los responsables del despliegue.

La presente guía toma como referencia el Reglamento 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento Europeo de Inteligencia Artificial).

6. Cuestionario de autoevaluación

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

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

El cuestionario tiene carácter orientativo y no sustituye en ningún caso los procedimientos formales de evaluación de la conformidad.

7. Referencias, estándares y normas

Para el desarrollo de esta guía se han consultado y utilizado especialmente las normas y estándares siguientes:

- [1] ISO-IEC 38505-1 - Information technology - Governance of IT - Governance of data. Part 1: Application of ISO/IEC 38500 to the governance of data
- [2] ISO-IEC 38507 - Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations
- [3] ISO-IEC 5338 - Information technology - Artificial intelligence - AI system life cycle processes
- [4] ISO-IEC 24027 - AI Algorithmic bias - Information technology - Artificial Intelligence (AI) - Bias in AI systems and AI-aided decision making
- [5] ISO-IEC 5259-1 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 1: Overview, terminology, and examples
- [6] ISO-IEC 5259-2 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 2: Data quality measures
- [7] ISO-IEC 5259-3 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 3: Data quality management requirements and guidelines
- [8] ISO-IEC 5259-4 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 4: Data quality process framework
- [9] ISO-IEC 5259-5 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 5: Data quality governance
- [10] ISO-IEC 8183 - Information technology – Artificial intelligence – Data life cycle framework
- [11] ISO-IEC 42001 - Information technology - Artificial intelligence - Management system
- [12] ISO-IEC 22989 - Information technology - Artificial intelligence - Artificial intelligence concepts and terminology
- [13] prEN 18286 Artificial intelligence - Quality management system for EU AI Act regulatory purposes
- [14] VERMA, Sahil and RUBIN, Julia, 2018. Fairness definitions explained. In: Proceedings of the International Workshop on Software Fairness - FairWare '18 [online]. Gothenburg, Sweden: ACM Press. 2018. p. 1-7. [Accessed 6 May 2019]. [Fairness definitions explained | Proceedings of the International Workshop on Software Fairness \(acm.org\)](#)

- [15] MITCHELL, Shira, POTASH, Eric, BAROCAS, Solon, D'AMOUR, Alexander and LUM, Kristian, 2020. Prediction-Based Decisions and Fairness: A Catalogue of Choices, Assumptions, and Definitions. arXiv:1811.07867 [stat] [online]. 24 April 2020. [\[1811.07867\] Prediction-Based Decisions and Fairness: A Catalogue of Choices, Assumptions, and Definitions \(arxiv.org\)](#)
- [16] GAJANE, Pratik and PECHENIZKIY, Mykola, 2018. On Formalizing Fairness in Prediction with Machine Learning. arXiv:1710.03184 [cs, stat] [online]. 28 May 2018. [Accessed 30 October 2020]. [\[1710.03184\] On Formalizing Fairness in Prediction with Machine Learning \(arxiv.org\)](#)
- [17] AGARWAL, Alekh, DUDÍK, Miroslav and WU, Zhiwei Steven, 2019. Fair Regression: Quantitative Definitions and Reduction-based Algorithms. arXiv:1905.12843 [cs, stat] [online]. 29 May 2019. [Accessed 30 October 2020]. [\[1905.12843\] Fair Regression: Quantitative Definitions and Reduction-based Algorithms \(arxiv.org\)](#)
- [18] Confusion matrix, 2020. Wikipedia [online]. [Accessed 30 October 2020].
- [19] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA
MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia

España | digital