CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

GIA GRUPO DE INTELIGENCIA ARTIFICIAL

Autores

Coordinadora:

Elena Mora

Participantes:

Ana García

Anna Boix

Carlos Lopez

Cristina Köhler

Diego Estévez

Eduardo Argüeso

Francisco Javier Carbayo

Inés Vázquez

Johanna Álvarez

Josep Bardallo

Lluis Sunyol

Montse Carrera

Ramon Baradat

Rodrigo López

Veronica Eguiron

Gestión de Proyecto:

Beatriz García

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Contenido

1. INTRODUCCIÓN 5
2. MOTIVACIÓN DE LA NECESIDAD DE CLAUSULAS CONTRACTUALES 5
3. TIPOLOGIA DE SISTEMAS Y SERVICIOS IA 6
   a) CONCEPTOS PRELIMINARES Y CONSIDERACIONES SOBRE EL ALCANCE 7
   b) ANALISIS DE TIPOLOGÍAS DE SISTEMAS Y SERVICIOS IA CONSIDERADOS 8
4. INVENTARIO DE ACTIVIDADES A REGULAR 11
5. IDENTIFICACION DE RIESGOS EN EL USO DE SISTEMAS DE IA Y GESTIÓN DE PROVEEDORES .. 26
   a. RIESGOS DE PRIVACIDAD 26

FASES DEL CICLO DE VIDA DEL PROVEEDOR 27

FASE 1. Selección de Proveedores y Contratación 28
1.1. Recogida y tratamiento de datos 28
1.2. Transparencia e información del funcionamiento de la IA 28
1.3. Gestión de derechos 28
1.4. Finalidad del tratamiento 28
1.5. Transferencias Internacionales 28
1.6. Almacenamiento de la información 29
1.7. Base de legitimación del tratamiento 29
FASE 2. Gestión de la privacidad durante el despliegue del sistema de IA 29
FASE 3. Monitorización y Seguimiento 30
3.1 Monitorización de Incidentes y Vulnerabilidades 30
3.2 Transparencia Continua en el Funcionamiento del Algoritmo 30
3.3. Plazos de Retención 30
3.4. Alto Riesgo y Evaluación de Impacto para los Derechos y Libertades 30
3.5. Subcontratación 30

FASE 4. Baja del Proveedor 31

4.1 Gestión de la Información al Finalizar la Relación Contractual 31

4.2 Transferencias de Datos a un Nuevo Proveedor 31

b. Otros riesgos 31

6. MODELOS DE CLAUSULAS 33

a. CLAUSULA GÉNERICA A INCLUIR EN CONTRATOS 33

b. CLAUSULA A INCLUIR EN CONTRATOS de sistemas / servicios de IA 34

7. PLAN DE IMPLANTACIÓN DE LAS CLAUSULAS de inteligencia artificial 41

8. OTRAS NORMATIVAS A CONSIDERAR 44

Protección de datos personales 44

Propiedad intelectual e industrial 44

Ciberseguridad y Seguridad de la información 45

Laboral 46

Secretos empresariales 46

Competencia 46

Responsabilidad civil 47

Consideraciones sectoriales, el ejemplo del sector salud 47

Cláusula de cierre 48

1. INTRODUCCIÓN

En la era digital actual, la inteligencia artificial (IA) se ha convertido en una herramienta esencial para mejorar la eficiencia y la innovación. Esta tecnología está transformando múltiples sectores, desde la salud y la educación hasta la industria y el entretenimiento. Ofrece grandes oportunidades para el desarrollo de sistemas y servicios innovadores que pueden mejorar la eficiencia, la precisión y la personalización de las soluciones. Sin embargo, la implementación de la IA también plantea importantes cuestiones legales, éticas y sociales que deben abordarse adecuadamente para evitar riesgos y garantizar un uso responsable y beneficioso de la tecnología.

Es crucial establecer un marco contractual robusto que regule las condiciones y responsabilidades de las partes implicadas en la contratación de sistemas y servicios de IA. Este marco resulta especialmente relevante para los sistemas de alto riesgo, que pueden tener un impacto significativo en la salud, la seguridad o los derechos fundamentales de las personas. La regulación adecuada de estos sistemas protege a los usuarios y asegura que la IA se utilice de manera ética y conforme a la ley.

Por este motivo, dentro del Comité Operativo GIA (del Grupo de Inteligencia Artificial) del ISMS, se vio la necesidad de crear un subgrupo específico que ahondara en esta necesidad. El presente documento refleja el resultado del arduo trabajo de dicho Grupo, que ha avanzado colaborativamente en el desarrollo de posibles cláusulas contractuales a incorporar.

Este documento comienza con un análisis detallado de la motivación detrás de la necesidad de estas cláusulas y prosigue identificando las principales tipologías de sistemas y servicios de IA que deben ser regulados, así como los requisitos esenciales que deben contemplarse contractualmente. A continuación, se profundiza en la identificación de riesgos en el uso de sistemas de IA y la gestión de proveedores, abordando tanto los riesgos de privacidad como las diferentes fases del ciclo de vida del proveedor.

Posteriormente, se identifican los modelos de cláusulas a utilizar y se describe el proceso seguido para la regularización necesaria de los contratos existentes en la organización. Aunque el foco principal de este documento es la regulación de los sistemas y servicios de IA ofrecidos por proveedores y los aspectos establecidos por el Reglamento de Inteligencia Artificial (RIA), como apartado final, se mencionan otras normativas y aspectos relevantes que deben ser considerados al redactar contratos correspondientes.

Esperamos que este documento sea de gran utilidad y sirva de base para que los responsables de esta materia en las organizaciones puedan adaptarlo a su realidad específica, su apetito al riesgo y las características del proveedor y servicio o sistema de IA contratado. Es fundamental recordar que este documento y las propuestas de cláusulas no constituyen un acuerdo contractual completo, ya que no incluyen condiciones relativas, por ejemplo, al pago, plazos de entrega, legislación aplicable o resolución de litigios. Se trata únicamente de cláusulas específicas asociadas al uso de sistemas y servicios de IA.

Finalmente, cabe destacar que este documento debe ser revisado por las áreas correspondientes de cada organización y adaptado a sus circunstancias particulares. Ni ISMS Forum ni las personas participantes en este proyecto se hacen responsables del uso que se haga del mismo ni de los posibles conflictos que de él se deriven.

2. MOTIVACIÓN DE LA NECESIDAD DE CLAUSULAS CONTRACTUALES

En los últimos años, la inteligencia artificial se está convirtiendo en un elemento central de la estrategia empresarial a nivel global, incluso en aquellos sectores de actividad que, inicialmente, se mostraban más reticentes a incorporar estas tecnologías a sus procesos productivos. La capacidad de la IA para procesar grandes volúmenes de datos y para automatizar la toma de decisiones complejas está transformando la productividad de las organizaciones, al permitirles mejorar las experiencias de los clientes y la eficiencia de sus procesos internos, lo que redunda, sin duda, en una ventaja competitiva.

A la vista de que, en este documento, trataremos diversos conceptos y aplicaciones prácticas relacionadas con la Inteligencia Artificial (en adelante, IA), como primer paso debemos entender a qué nos referimos con IA.

En términos generales, podríamos decir que los sistemas de IA son programas informáticos que, para un conjunto de objetivos definidos por el ser humano, puede generar resultados que normalmente requerirían de intervención humana (como predicciones, contenidos, recomendaciones o decisiones). Es decir, estos sistemas replican o imitan la inteligencia humana, entendiéndola como la capacidad de razonamiento, aprendizaje, percepción y toma de decisiones que asociamos a los seres humanos.

En este contexto, se ha puesto de manifiesto la necesidad de regular esas nuevas tecnologías. Como respuesta a dicha necesidad, y tras años de negociaciones, surge el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, más conocido como Reglamento de Inteligencia Artificial (en adelante, RIA).

Pese a esta nueva regulación, lo cierto es que la legislación vigente no proporciona unas directrices suficientemente claras para hacer frente a los desafíos que plantea la contratación de proveedores de IA. Por ello, en este documento, trataremos de establecer un clausulado tipo para las organizaciones que deseen adquirir modelos o sistemas de IA desarrollados por un proveedor externo.

Hemos de señalar que la incorporación de cláusulas contractuales relativas al uso de Inteligencia Artificial al suministrar productos y servicios tiene una doble vertiente:

Por un lado, la gestión de riesgos de proveedores es uno de los primeros procesos afectados por esta incorporación del clausulado. Es crucial identificar tempranamente el potencial uso de IA desde las etapas iniciales de la selección de un proveedor para asegurar que se ofrezcan garantías suficientes. Estas garantías pueden estar relacionadas con diversos aspectos, como la privacidad y el cumplimiento del Reglamento General de Protección de Datos (RGPD) cuando se trata de datos personales. En estos casos, el artículo 28.1 del RGPD establece que el responsable del tratamiento debe elegir a un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, asegurando así el cumplimiento del RGPD y la protección de los derechos del interesado. Además, incluso en el caso de proveedores que no utilicen datos personales, los protocolos habituales de compliance y due diligence exigen comprobar la idoneidad del proveedor como parte de la gestión de riesgos empresarial.

Por otro lado, dado que el uso de la Inteligencia Artificial se ha generalizado en mayor o menor medida progresivamente en los últimos años, es posible que los proveedores habituales ya estén prestando servicios o suministrando productos que incorporan IA sin que se haya incluido ningún clausulado específico más allá de las cláusulas habituales. Es posible por tanto que no se haya procedido a regular de forma específica este aspecto y que dicho clausulado no se haya adaptado a las previsiones del RIA una vez se ha producido su publicación. Es por ello por lo que cobra importancia la adaptación de los procesos y documentos a lo dispuesto en el RIA, mediante la actualización de los procesos de selección y gestión de proveedores de productos y servicios de IA a lo largo de su ciclo de vida, así como la identificación de aquellos proveedores existentes que ya están prestando servicios a través de un inventario de soluciones de IA en la empresa y la correspondiente actualización de las cláusulas contractuales.

No obstante, dicha revisión del clausulado al amparo del RIA debe abordarse de una manera integral, no quedando sólo afectada la cláusula de protección de datos sino otras áreas de Derecho como la normativa en materia de propiedad intelectual o industrial y de secretos empresariales, o de otros derechos fundamentales (igualdad, etc…), la seguridad de la información de la organización, y cualesquiera otras áreas del Derecho que pudieran requerir algún tipo de adaptación en el clausulado del contrato por el uso de IA.

3. TIPOLOGIA DE SISTEMAS Y SERVICIOS IA

La identificación de las distintas tipologías de sistemas y servicios de Inteligencia Artificial (IA) es fundamental para que las entidades puedan establecer adecuadamente los requisitos y controles necesarios. Cada tipo de sistema de IA presenta características y riesgos específicos que deben ser gestionados de manera adecuada para garantizar el cumplimiento de la normativa, la protección de los derechos fundamentales y la seguridad de la información. Por ello, el presente apartado tratará de identificar los principales sistemas y servicios de IA que pueden ser objeto de contratación para, en fases posteriores, proceder a identificar los requisitos específicos de cada uno de ellos que permitan minimizar los riesgos asociados.

A. CONCEPTOS PRELIMINARES Y CONSIDERACIONES SOBRE EL ALCANCE

Antes de comenzar con la identificación propiamente dicha, es necesario indicar que se considera un sistema IA (Inteligencia Artificial) como “aquella entidad que realiza comportamientos que una persona podría calificar razonablemente de inteligentes si un humano hiciera algo similar”, usando para ello la definición publicada por la guía introductoria “INTRODUCCIÓN A LA IA PARA PROFESIONALES DE SEGURIDAD DE LA INFORMACIÓN”, publicada por el ISMS Forum.

Por otra parte, no podemos perder de vista la definición que el propio Reglamento de Inteligencia Artificial establece como Sistema de IA : «”un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales”Dentro de esta familia de sistemas, los de **Aprendizaje Automático o ML**, por las siglas de **Machine Learning en inglés,** son el grupo de mayor nivel de adopción y atención actual en el mercado, y por ello son el tipo de sistemas que centran este análisis de tipologías. De forma muy sintética diremos que estos sistemas son capaces de aprender a procesar datos nuevos a partir del análisis previo de datos históricos, sin que sea necesario programar explícitamente estos procesamientos. El proceso de análisis previo de datos históricos se denomina entrenamiento (training en inglés).

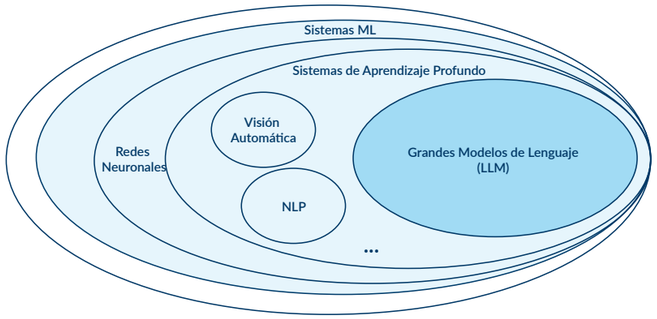
A su vez, dentro de los sistemas de Aprendizaje Automático, los **basados en Redes Neuronales** son los más habituales y profusos en el mercado, por lo que nos hemos centrado en esta categoría a la hora de identificar las tipologías objeto de este análisis. Estos sistemas efectúan un procesamiento que se asemeja a de las neuronas del cerebro humanos. Estas neuronas se disponen en capas, interconectándose de manera que la salida de una capa es la entrada de la siguiente.

Dentro de esta categoría de sistemas de Aprendizaje Automático basados en Redes Neuronales, los denominados de **Aprendizaje Profundo (Deep Learning en inglés)** son los que en los últimos años han experimentado una mayor demanda y desarrollo, tanto por su capacidad de aportar valor como por los avances tecnológicos en las capacidades que demandan, en términos de computación y técnicas de proceso de datos. Ambos aspectos están relacionados precisamente con su profundidad, entendida como el alto número de capas de neuronas, así como del número de neuronas por capa, del orden de centenas y centenas de miles respectivamente, lo que les confiere la potencia necesaria para tareas complejas. Dentro de estos sistemas se pueden identificar múltiples subcategorías, por ejemplo:

- **Visión automática (Computer Vision en inglés)**, usado para interpretar imágenes y reconocer objetos, se usan para reconocimiento facial o biométrico, para identificación de objetos en una foto o un video para, por ejemplo, hacer peritajes de daños en vehículos o viviendas, o para interpretar imágenes medicas
- **Procesamiento del lenguaje natural (NLP o Natural Language Processing en inglés)** para tareas como la identificación de información en textos, la traducción automática o la extracción del sentimiento de un texto
- **T**ext-to-Speech y Speech-to-text, traducción de texto a alocuciones y viceversa**.**
- **Soporte a la toma de decisiones, por ejemplo, determinar que producto del portfolio es el que tiene más opciones de ser adquirido por un client**e determinado y con qué nivel de confianza o asignar un nivel de interés o riesgo a un posible cliente a la hora de conceder un préstamo o contratar una póliza de seguro

Finalmente, dentro de estos sistemas de Aprendizaje Profundo, ha habido un área que ha experimentado un auge sin precedentes en los últimos tres o cuatro años. Se trata de los sistemas de **IA Generativa**, y dentro de estos los **Grandes Modelos de Lenguaje o LLM (por sus siglas en inglés, Large Language Models).** Estos sistemas son los que se usan en servicios como ChatGPT o Copilot, y están siendo adoptados para tareas cotidianas como sumarización o traducción de documentos, generación de documentos o chatbots interactivos conversacionales sobre cualquier temática, tanto por los usuarios particulares como por las empresas. Por este motivo y por contemplar algunos aspectos específicos de su implantación o explotación, y porque los modelos de propósito general (a los que los reguladores establecen requisitos específicos) generalmente son LLMhemos dedicado una categoría de tipología aparte, aun cuando son también sistemas de Aprendizaje Automático.

La siguiente figura recoge de forma esquemática este planteamiento de selección de tipologías, en la que resaltamos las dos categorías seleccionadas.



B. ANALISIS DE TIPOLOGÍAS DE SISTEMAS Y SERVICIOS IA CONSIDERADOS

Como se indicaba anteriormente, el análisis de tipologías de sistemas y servicios se ha centrado en los sistemas de Aprendizaje Profundo (ML) y, dentro de ellos, también se ha hecho un análisis específico para los Grandes Modelos de Lenguaje (LLM), dada su relevancia actual en el mercado.

Dentro de cada uno de estos grupos objetivo, el criterio de descomposición seleccionado para el análisis de implicaciones contractuales ha sido el de aprovisionamiento o contratación, es decir, por componentes del sistema o servicio potencialmente contratables por separado, a lo largo del ciclo de vida de los sistemas IA.

Este criterio de selección de tipologías es más útil para las empresas a la hora de considerar aspectos a regular en los contratos, ya que será el que aporte mayores diferencias en dichos aspectos contractuales.

También se consideró hacer el análisis diferencial de clausulado por tipo de sistema IA, es decir, por la solución tecnológica o algorítmica que usa (visión automática, procesamiento de lenguaje natural, clasificación, etc.). Sin embargo, esto parece menos útil por dos razones:

- el gran número de usos finales que la IA puede soportar, que además crece de forma constante
- que las diferencias en cuanto a los aspectos a regular en el contrato no van a venir tanto de la solución tecnológica o algorítmica específica del modelo sino del posicionamiento del componente en la cadena de aprovisionamiento y/o el tratamiento o caso de uso que se vaya a realizar

En la siguiente figura se representan los componentes susceptibles de ser adquiridos y contratados por separado de los sistemas y servicios objeto del análisis. Los componentes se han dispuesto de abajo a arriba, indicando la dependencia de los bloques superiores respecto de los inferiores.

Así, en la capa inferior se muestran las distintas formas de adquirir o contratar los modelos ML o LLM sobre los que se apoyan las aplicaciones, dispuestas en capas superiores, incluyéndose los servicios de afinado (o "fine tuning[1]") y generación aumentada por recuperación (RAG[2] , por Retrieval Augmented Generation, en inglés, para modelos LLM), que opcionalmente pudieran ser necesarios para soportar la aplicación.

Los modelos ML (no LLM) normalmente se aprovisionarán de dos maneras:

a. como modelo ML de uso general (según la definición del Reglamento de IA de la UE, RIA), adquirible de un proveedor especialista o como modelo open source, al que normalmente se le aplicará un procedimiento de afinado (fine tuning) con acopio y preparación de datos
b. como modelo ML desarrollado a medida por una especialista, lo que conllevará una etapa previa de acopio y preparación de datos para entrenar, validar y probar el modelo

[1] Fine tuning, o afinado, es el proceso de entrenamiento incremental de un modelo previamente entrenado, con información de una temática específica no cubierta, o no cubierta con suficiente profundidad, en el entrenamiento inicial.
[2] RAG, Retrieval Augmented Generation, es el proceso de incorporación de información específica como contexto de las preguntas dirigidas al LLM, para conseguir respuestas más precisas que las que proporcionaría el LLM según su entrenamiento de base.

Sistemas ML (no LLM)

Servicio SaaS basado en ML	
Mantenimiento del sistema (correc.&evolut.)	
Operación del sistema	
Aplicación basada en ML	
Fine tuning	Desarrollo modelo ML a medida
Modelo ML uso general	Prep de datos

Sistemas LLM

Servicio SaaS basado en LLM	
Mantenimiento del sistema (correc.&evolut.)	
Operación del sistema	
Implementación de Aplicación	
Generación Aumentada por Recuperación (RAG)	
Fine tuning	
Modelo LLM uso general privado	Servicio LLM uso general (SaaS)

A su vez, los modelos LLM también se aprovisionarán normalmente de dos maneras:

a. como modelo LLM de uso general (según definición RIA) desplegado para uso privado, adquirible de un proveedor especialista o como modelo open source
b. como servicio LLM de uso general, provisto (y con acceso controlado) como SaaS por un proveedor de estos servicios

Sobre los modelos LLM se podrá aplicar un procedimiento de afinado (fine tuning), con acopio y preparación de datos, y/o un proceso de generación aumentada por recuperación (RAG).

Sobre los componentes de modelo, posteriormente afinado y/o extendido por RAG, según el caso, se apoya la aplicación, que implementa la lógica del proceso de negocio en cuestión y la interacción con los usuarios y/o otros sistemas externos con los que deba interactuar. La aplicación usa los servicios expuestos por el modelo, normalmente sobre una API. La aplicación puede apoyarse sobre uno o varios modelos, por ejemplo, un modelo NLP para evaluar el sentimiento de los mensajes del usuario, y otro modelo NLP para calcular el grado de coherencia de las respuestas del LLM y el por último el propio LLM en sí.

Sobre la capa de aplicación, se disponen las capas de servicios de operación y evolución de la aplicación y los modelos subyacentes (denominado conjuntamente "sistema" en la figura).

Finalmente, en la figura también se representa la posibilidad de adquirir la aplicación en modo servicio SaaS, como una caja que engloba a todos los componentes.

Ilustraremos ahora todos estos conceptos con un ejemplo:

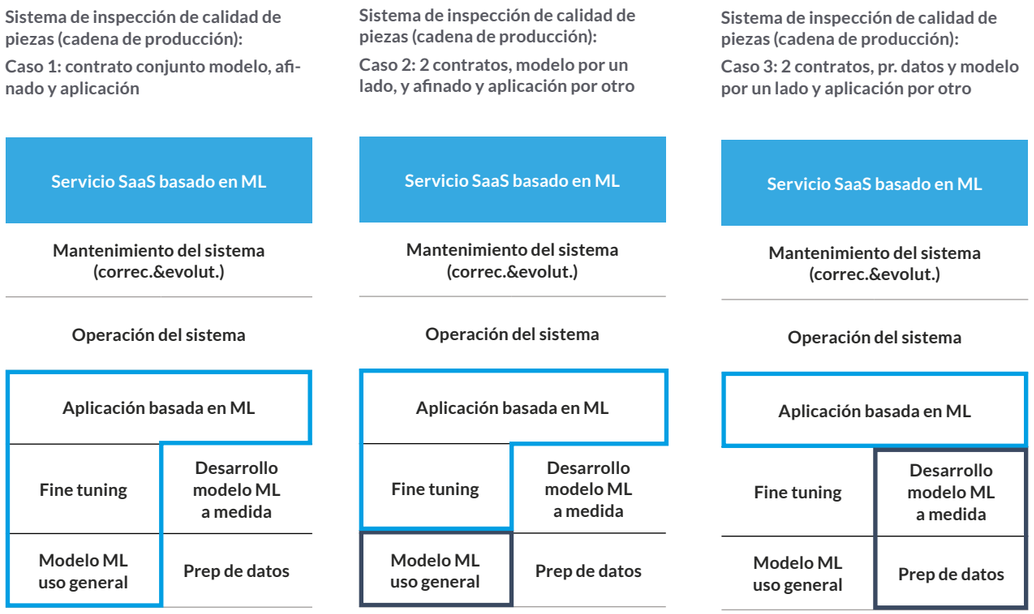
Consideremos un sistema basado en IA para la detección de productos defectuosos en el control de calidad de una cadena de producción industrial. Este sistema se basa en un modelo de visión automática, para la inspección de los productos producidos y la detección visual de fallos de fabricación en los mismos.

De forma esquemática, la aplicación controla el proceso de inspección de calidad, tomando datos de la cámara de control de la línea de producción, pasándole los datos al modelo para que evalue los posibles defectos, para a continuación disparar el desvío de la pieza fuera de la cadena, si estuviera defectuosa, o su continuación en la cadena hacia la siguiente fase, si no se han apreciado defectos.

La siguiente figura ilustra este caso:

En la figura se describen 3 formas de adquisición y contratación de dicho sistema:

1. **caso 1:** se contrata como un todo el modelo general, el afinado al caso de uso de la empresa de fabricación en cuestión y la implementación de la aplicación que implementa el proceso
2. **caso 2,** dos contratos, uno, enmarcado en naranja, para el modelo general, y otro, enmarcado en rojo, para el afinado del modelo al caso de uso de la empresa y la aplicación que implementa el proceso
3. **caso 3**, en este caso dos contratos. Uno enmarcado en naranja, para el desarrollo del modelo a medida en este caso, incluyendo la preparación de los datos de entrenamiento, validación y prueba. Y otro contrato, enmarcado



en rojo, para el desarrollo de la aplicación que implementa el proceso.

Cabe recordar que la taxonomía de componentes para la categoría genérica de Sistemas ML es la misma independientemente de las múltiples subcategorías (visión automática, procesamiento de lenguaje natural, clasificación, etc.) que apuntábamos anteriormente. Al fin y al cabo, todos estos sistemas son descomponibles en uno o varios modelos ML que soportan una aplicación, tan compleja como el sistema final requiera, de forma modular.

Si tomamos el coche autónomo como ejemplo, este no deja de ser una gran aplicación compuesta, conectada a diversos módulos de sensores que le aportan imágenes de la carretera y de las señales, datos de los elementos mecánicos del coche (velocidad, presión de los neumáticos, posición de la dirección, etc.), estado de los elementos de seguridad, etc.

Cada aplicación componente se apoya en uno o varios modelos ML, por ejemplo, uno de visión automática, para "ver" la carretera y el espacio adyacente, otro de control de los elementos de seguridad, otro del guiado general del coche, tomando datos del resto y gobernando la dirección, acelerador y freno, etc. Esta jerarquía de aplicaciones y modelos ML daría lugar a su vez a una jerarquía de contratos según se hiciera el aprovisionamiento y contratación de cada componente a una empresa especializada en cada en cada uno de ellos, con agrupaciones de los mismos análogas a las descritas en el caso del sistema de inspección de calidad descrito anteriormente.

Tipo	Descripción	Servicio/ Sistema	Principales características	Ejemplos
Modelo ML de uso general.	Compra de un modelo ML de uso general, como componente a integrar; normalmente requerirá fine tuning.	Sistema	Modelo de uso general, ya entrenado por el proveedor, listo para ser fine tuned o integrado con una aplicación una vez verificado su funcionamiento. El modelo ML dependerá fundamentalmente de los datos con los que se entrenó, validó y probó, y esto da lugar a implicaciones de contratación	Un modelo de reconocimiento de imágenes genérico, capaz de identificar objetos de diversa naturaleza. Análisis de facturas para extraer los datos necesarios a incluir en una Base de Datos.
Fine tuning de un modelo de uso general.	Contratación servicio de fine tuning (adaptación al caso de uso concreto) de un modelo ML de uso general a un proveedor de servicios	Servicio	Los datos de fine tuning pueden ser proporcionados por el proveedor del servicio o por el propio cliente. El fine tuning del modelo ML implica las siguientes actividades: - acopio y preparación de los datos de fine tuning - ejecución del fine tuning- prueba del modelo fine tuned	Una particularización del modelo de reconocimiento genérico anterior, que se especializa en un tipo de objetos específico, mediante un reentrenamiento con objetos de ese tipo en cuestión. Podría ser un clasificador de productos manufacturados correctos o defectuosos. Un modelo fine tuned para el reconocimiento facial o biométrico.
Preparación de datos de entrenamiento, validación o prueba para modelo ML (para modelo ML a medida).	Servicio de preparación de datos de entrenamiento, validación o prueba para modelo ML.	Servicio	A partir de datos en bruto, preparación de los datasets de entrenamiento/validación/ prueba para uno (o varios) modelo(s) ML.	Transformación de los datos en bruto, etiquetado, etc. Generación de datos sintéticos para los sets de validación, p.e. Mejora de la calidad de los datos para garantizar que los datos utilizados en el entrenamiento son adecuados.
Desarrollo de un Modelo ML a medida.	Desarrollo de un modelo ML a medida por un integrador / consultora.	Servicio	Desarrollo de un modelo ML a medida por un integrador / consultora. El modelo ML implica las siguientes actividades por parte del proveedor, con implicaciones contractuales: - acopio y preparación de los datos de entrenamiento, validación y prueba. - diseño del modelo ML. - entrenamiento y validación. - prueba del modelo entrenado.	Modelo de reconocimiento de imágenes que no se desarrolla a partir de un modelo de uso general por particularización, sino a medida desde el principio. Modelo de reconocimiento de imágenes desarrollado para el reconocimiento facial o biométrico.
Aplicación basada en modelo ML.	Contratación de desarrollo e integración de una aplicación basada en un modelo ML (ya sea adaptado a partir de un modelo de uso general o desarrollado a medida).	Servicio	Servicio de implementación e integración de una aplicación basada en un modelo ML. Esta aplicación cubrirá la interfaz con los usuarios y la lógica de negocio del proceso específico que cubra, integrándose con el modelo ML para que soporte la toma de decisiones para los datos de entrada basándose en la configuración resultante del entrenamiento del modelo.	Una aplicación que hace uso del modelo especializado de reconocimiento de objetos del caso anterior. Por ejemplo, en control de calidad de una línea de producción, para detectar defectos en los elementos producidos. Aplicación que usa un sistema de reconocimiento facial o biométrico para controlar el acceso a una dependencia de acceso restringido.
Operación de aplicación basada en ML.	Contratación de un servicio de soporte a operación de una aplicación basada en un modelo ML.	Servicio	Servicio de soporte a la operación y de una aplicación basada en un modelo ML, como la descrita en el apartado anterior.	Servicio de operación de la aplicación y el modelo subyacente descrito en los casos anteriores.
Evolución de aplicación basada en modelo ML.	Contratación de un servicio de evolución de una aplicación basada en un modelo ML, incluyendo reentrenamiento.	Servicio	Servicio de soporte a la evolución y reentrenamiento de una aplicación basada en un modelo ML, como la descrita en el apartado anterior.	Servicio de mantenimiento evolutivo de la aplicación y el modelo subyacente descritos en los casos anteriores.

Tipo	Descripción	Servicio/ Sistema	Principales características	Ejemplos
Servicio SaaS basado en modelo ML.	Contratación de una aplicación basada en modelo ML, como servicio SaaS.	Servicio	Servicio SaaS de una aplicación basada en modelo ML. Tanto la aplicación como el modelo ML que la sustenta están provisto en modo SaaS.	Un servicio SaaS de detección de defectos de los elementos producidos en una cadena de producción por análisis de imágenes.
Modelo LLM de uso general.	Compra de un modelo LLM de uso general como componente a integrar.	Sistema	Compra de modelo LLM de uso general, para ser desplegado sobre plataforma propia (ya sea Cloud Privada Virtual o ion-premise) como componente para soportar una aplicación basada en él (ver apartado “Aplicación basada en LLM”, más adelante.	Por ejemplo, Mistral.
Servicio LLM de uso general.	Contratación de un servicio LLM público, provisto como SaaS, normalmente acceso API, a integrar en una aplicación.	Servicio	Contratación de un servicio LLM público provisto como SaaS, accesible mediante API, para soportar una aplicación basada en él (ver apartado “Aplicación basada en LLM”, más adelante.	Por ejemplo, OpenAI GPT-4o, Claude Sonet o Gemini.
Fine tuning de modelo LLM.	Contratación de fine tuning un modelo LLM, privado o servicio como servicio público, como componente a integrar.	Servicio	Servicio de fine tunning de un modelo LLM de uso general a un proveedor de servicios: El fine tuning se puede hacer sobre un modelo LLM propietario o uno provisto en modo SaaS sobre un API por un prestador de servicio.	Un Integrador de Sistemas prepara datos y ejecuta la operación de fine tuning de un modelo de uso general, abierto servicio cerrado, para soportar un caso de uso específico del cliente que lo despliega. Por ejemplo, conocimiento (preguntas, respuestas) de un proceso de negocio concreto en base a la información proporcionada por el negocio.
Generación Aumentada por Recuperación.	Implementación de un esquema RAG para contextualización especializada.	Servicio	Sobre el caso anterior, se añade un esquema RAG para mejorar el contexto de los prompts y obtener respuestas más específicas y precisas	Ejemplo: Una empresa de marketing digital quiere utilizar un LLM combinado con RAG para ayudar a que su personal redacte contenido de alta calidad de manera más eficiente y precisa. El asistente puede generar borradores de artículos, publicaciones en blogs, descripciones de producto buscando información relevante de bases de datos y otras fuentes para enriquecer el contenido. Este servicio cubre la preparación de los fragmentos de documentos (chunks), su vectorización y carga en la base de datos vectorial, y las pruebas de validación.
Aplicación basada en LLM.	contratación de la implementación de una aplicación basada en servicio o modelo LLM.	Servicio	servicio de implementación (por un integrador de sistemas) de una aplicación basada en LLM. El LLM podría ser privado o un servicio LLM provisto por un proveedor público en modo SaaS.	Ejemplo: Asistente de redacción de contenidos para sugerir palabras clave y frases que mejoren la visibilidad del contenido en motores de búsqueda. Sistema de acceso o la admisión de personas físicas a centros educativos y de formación profesional que usa un LLM para sumarizar los expedientes históricos de los candidatos.

Tipo	Descripción	Servicio/ Sistema	Principales características	Ejemplos
Operación de aplicación basada en LLM.	contratación de un servicio de soporte a operación de una aplicación basada en un modelo LLM	Servicio	Servicio de soporte a la operación y de una aplicación basada en un modelo LLM.	OEperación de la aplicación descrita en el caso de aplicación basda en LLM.
Evolución de aplicación basada en modelo LLM.	contratación de un servicio de evolución de una aplicación basada en un modelo LLM, incluyendo re-fine tuning	Servicio	Servicio de evolución y reafinamiento de una aplicación basada en un modelo LLM	Evolución y reafinamiento en el caso de la aplicación basada en LLM.
Servicio SaaS de aplicación basada en modelo LLM.	contratación de una aplicación basada en modelo LLM, provista como servicio SaaS.	Servicio	Servicio SaaS de una aplicación basada en modelo ML.	Aplicación descrita en el caso de aplicación basada en LLM, provista como servicio SaaS.

4. INVENTARIO DE ACTIVIDADES A REGULAR

A partir del análisis de las distintas regulaciones y documentos de referencia, se ha procedido a identificar aquellas actividades que podrían tener que quedar reguladas contractualmente con el objetivo de que le sirvan al lector como punto de referencia a la hora de determinar los aspectos contractuales a considerar en la contratación de un sistema / servicio de IA. La elección de los requisitos dependerá, entre otras cosas, del sistema / servicio de IA que se encuentre afectado y del apetito al riesgo de la entidad contratante.

Actividad	Descripción	Origen	Imp[3]	Dif[4]	Requisito matizable[5]	Detalle[6]	Tipo de sistema
Sistema de gestión de riesgos.	Texto general: Se garantizará que durante todo el ciclo de vida del sistema se identifican, analizan, evalúan y tratan los riesgos conocidos y previsibles y otros que podrían surgir. Obligación del proveedor en sistemas de Alto riesgo.		Alta	Media	Sí, en función de los datos tratados en el sistema.	Texto modulado (para proveedores de sistemas más complejos o que empleen altos volúmenes de datos personales): El proveedor garantizará que, durante todo el ciclo de vida del siste-ma, se identifican, analizan, evalúan y tratan los riesgos conocidos y previsibles y otros que podrían surgir. Para ello, el proveedor acreditará que se ha empleado un procedimiento de ges-tión de riesgos fiable y que, en consecuencia, se han aplicado medidas y controles adecuados a los riesgos detectados. Las medidas y controles podrán ser validados aportando certificados tales como ISO 27001, ISO 31000, ISO/IEC 42001, entre otras. La adecuación del procedimiento empleado podrá acreditarse aportando otros certificados propios del sector de actividad o emitidos por un tercero, siempre que sean reconocidos por escrito por la otra parte. En caso de carecerse de certificados, como parte del proceso de homologación del proveedor, podrá solicitársele información adicional que acredite la metodología empleada para la gestión de riesgos, lo que puede incluir solicitud de documentación adicional, cumplimentación de cuestionarios, entrevistas, etc.	Obligatorio en sistemas de alto riesgo.
Calidad de los datos. Diseño, origen y preparación de los datos.	Texto general: Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad. Hay que tener en cuenta la normativa de protección de datos (si se usan datos personales), especialmente: PbD, principios del tratamiento y origen lícito (información/consentimientos interesados).	Art. 10 Reglamento IA / RGPD	Alta	Media	Sí, en función de los datos tratados en el sistema.	Texto modulado (cuando se traten datos personales): El proveedor garantizará que los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad del sistema de IA. Dichas prácticas deberán incluir, además de los requisitos legalmente establecidos en el RIA, procedimientos o normas internas para la regulación de la IA (tales como estrategia de IA de la compañía, evaluaciones del cumplimiento, registro del sistema, normativa interna dirigida al personal, procedimientos internos de notificación de incidentes, etc.), definición clara de roles y responsabilidades a nivel interno, así como acreditación de la formación recibida por el personal interno del proveedor que intervenga en el proyecto.	Obligatorio en sistemas de alto riesgo.
Calidad de los datos. Evitar sesgos.	Texto general: Se garantizará que el sistema está diseñado o cuenta con los controles suficiente que permitan evitar la existencia de sesgos. Matizar que evitar sesgos puede requerir el uso de categorías especiales de datos (art. 9 RGPD)	Art. 10 Reglamento IA / Art. 9 RGPD	Alta	Alta	Sí, en función del tipo de sesgo.	Texto modulado (cuando se trate de sesgos que impliquen uso de datos personales que, no siendo de categorías especiales, puedan provocar discriminación entre personas físicas, como el género o situación económica): Cuando el sistema de IA pueda implicar discriminación de personas físicas en base a datos personales, además de los requisitos legalmente establecidos en la normativa de protección de datos, inteligencia artificial y cualquier otra aplicable al presente contrato, se valorará especialmente que el proveedor haya implementado controles adicionales. Texto modulado (cuando se trate de sesgos que impliquen uso de datos personales de categorías especiales): Cuando sea estrictamente necesario para garantizar la detección y corrección de sesgos que el proveedor del sistema trate excepcionalmente categorías especiales de datos, además de los requisitos legalmente establecidos en la normativa de protección de datos, inteligencia artificial y cualquier otra aplicable al presente contrato, se valorará especialmente que el proveedor haya implementado controles adicionales. Texto modulado (común a los dos casos anteriores): En concreto, se tendrá en cuenta: -Pruebas. La realización periódica de pruebas de sesgo por el proveedor, a fin de asegurarse de que los datos de entrenamiento representan de forma justa a todos los colectivos afectados. -Auditorías de los algoritmos, a fin de comprender cómo toma decisiones el sistema y si el sesgo está influyendo de forma indebida en las decisiones. -Formación. Que el personal del proveedor que intervenga en el desarrollo del sistema de IA haya recibido formación en ética de la IA. -Diversidad del equipo de desarrollo. Se tomará en especial consideración que el equipo de desarrollo incluya criterios de diversidad (edad, raza, sexo, condición social, etc.), a fin de contribuir a identificar y mitigar posibles sesgos.	Obligatorio en sistemas de alto riesgo.

[3] Importancia
[4] Dificultad
[5] Requisito que pueda ser matizable en función de la casuística
[6] Detalle del requisito. Proporciona mayor detalle o información sobre el requisito, especialmente si el requisito puede ser matizable por algun motivo.

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Actividad	Descripción	Origen	Imp	Dif	Requisito matizable	Detalle	Tipo de sistema
Documentación técnica, Instrucciones de uso y Transparencia.	Texto general: El proveedor acreditará que ha redactado la documentación técnica pertinente para acreditar que el sistema cumple los requisitos de la normativa vigente. Los sistemas de IA se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. El proveedor proporcionará las instrucciones de uso correspondientes, en formato digital o de otro tipo que resulte adecuado, que deberán incluir información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para el responsable del despliegue. El responsable del despliegue deberá seguir las instrucciones proporcionadas.	Arts. 11, 13 y 26 Reglamento IA	Alta	Alta	Sí, en función de la complejidad del sistema.	Texto modulado (en sistemas de funcionamiento especialmente complejo o poco transparente): Para facilitar la comprensión por parte de su destinatario, la información podrá facilitarse en capas, debiendo contener la primera de ellas, necesariamente, la identidad del proveedor, la finalidad del sistema, nivel de precisión y una descripción básica de sus características, capacidades y limitaciones, los cambios en el sistema y su funcionamiento, las medidas de vigilancia humana, los recursos informáticos y de hardware necesarios, la descripción del mecanismo que permite recabar, almacenar e interpretar correctamente los archivos de registro y la forma de obtener o consultar la información completa.	Obligatorio en sistemas de alto riesgo.
Supervisión humana.	Texto general: El sistema permitirá la supervisión humana de manera efectiva mientras esté en uso, lo que implica que deberá incluir una interfaz humano-máquina adecuada. El responsable del despliegue la encomendará a personas con competencia, formación y autoridad necesarias.	Arts. 14 y 26 Reglamento	Alta	Media	Sí, en función de la complejidad del sistema o de sus consecuencias sobre las personas físicas.	Texto modulado (en sistemas de funcionamiento espe-cialmente complejo, poco transparente o que impli-quen graves consecuencias para las personas físicas): El sistema deberá incluir, además de los requisitos legalmente establecidos: -Sistema de alertas, sencillo y fácilmente accesible que alerte a los supervisores humanos cuando la IA tome ciertas decisiones que se desvíen de lo esperado. -Posibilidad de anulación manual de una determinada decisión del sistema. -Sensibilizaciones, ayudas o tutoriales para los supervi-sores humanos, a fin de que estén correctamente educados y sepan cómo funciona la IA, cómo interpre-tar sus decisiones y cuándo es necesario intervenir.	Obligatorio en sistemas de alto riesgo.
Archivos de registro.	Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de eventos («archivos de registro») a lo largo de todo su ciclo de vida.	Art. 12 Reglamento IA	Alta	Alta	No	-	Obligatorio en sistemas de alto riesgo.
Transparencia con destinatarios.	Texto general: Los sistemas de IA destinados a interactuar directamente con personas físicas deberán diseñarse y desarrollarse de forma que las personas físicas estén informadas de que están interactuando con un sistema de IA.	Art. 50 Reglamento IA	Alta	Baja	Sí, en función de la finalidad del sistema de IA, información tratada en el sistema, perfil de la persona física que interactúa con el sistema de IA.	Texto modulado (personas físicas destinadas a interac-tuar con el sistema pertenecen a colectivos vulnera-bles): La información deberá ser inteligible y de fácil acceso, y empleará un lenguaje claro y sencillo, evitando estructuras excesivamente complejas o remisiones a normativas, a otros textos legales o a condiciones generales del proveedor. La información proporcionada a las personas físicas que interactúan con el sistema deberá adaptarse a las circunstancias particulares de su destinatario, especialmente cuando se dirija a co-lectivos de personas especialmente vulnerables, incluyendo menores de edad. Texto modulado (finalidades complejas): La informa-ción deberá ser inteligible y de fácil acceso, y empleará un lenguaje claro y sencillo, evitando estructuras exce-sivamente complejas o remisiones a normativas. Para mejorar su comprensión, la información podrá propor-cionarse en capas, debiendo contener necesariamente la primera capa informativa un aviso de que se está interactuando con un sistema de IA, la identificación del proveedor, una descripción básica de su finalidad y de la información tratada en dicho sistema y la forma de obtener o consultar la información completa.	Para todos los sistemas destinados a interactuar con personas.
Obligación de explicar el funcionamiento del sistema de IA a escala individual.	Texto general: El proveedor está obligado a asistir a la organización para explicar cómo el sistema de IA llegó a una decisión o resultado concreto sobre las personas o el grupo de personas en relación con las cuales está previsto que se utilice el sistema de IA. Como mínimo, esta asistencia incluirá una indicación clara de los factores clave que llevaron al sistema de IA a obtener un resultado concreto y de los cambios que deben hacerse en los datos de entrada para que llegue a un resultado diferente. Esta obligación incluye el suministro a la organización de toda la información técnica y de otro tipo necesaria para explicar cómo el sistema de IA ha llegado a una decisión o un resultado concretos, así como para ofrecer a las personas o al grupo de personas con respecto a los que se utiliza o está previsto que se utilice el sistema de IA la oportunidad de verificar la manera en que el sistema de IA llega a una decisión o un resultado concretos. El proveedor concede a la organización el derecho a utilizar, compartir y divulgar esta información en la medida en que sea necesario para informar a las personas o grupos de personas con respecto a los que se utiliza o se prevé utilizar el sistema de IA acerca de su funcionamiento o en el marco de cualquier procedimiento judicial.	Art. 13 Reglamento IA	Alta	Alta	Sí, en función de la complejidad del sistema.	Texto modulado (por ejemplo en sistemas muy complejos a nivel técnico o que traten información especialmente sensible): Estas obligaciones incluyen, entre otros, el código fuente del sistema de IA, las especificaciones técnicas utilizadas en su desarrollo, los conjuntos de datos, la información técnica sobre el modo en que se han obtenido y editado los conjuntos de datos utilizados en el desarrollo del sistema de IA, información.	Obligatorio en sistemas de alto riesgo.

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Actividad	Descripción	Origen	Imp	Dif	Requisito matizable	Detalle	Tipo de sistema
Precisión, solidez y ciberseguridad.	Los sistemas de IA deben tener un nivel adecuado de precisión, solidez y ciberseguridad.	Art. 15 Reglamento IA	Alta	Media	Sí, en función de la finalidad del sistema de IA, información tratada en el sistema, sector de actividad, etc.	El texto modulado podría desarrollarse en Anexos. Deberán describirse los niveles de precisión requeridos y los que puede proporcionar el sistema de IA. Deberá facilitarse una descripción de las medidas técnicas y organizativas que debe adoptar el proveedor para garantizar un nivel adecuado de solidez, seguridad y ciberseguridad. Estas medidas deben garantizar que el sistema de IA será lo más resistente posible frente a errores, fallos e incoherencias que pueden surgir en los propios sistemas o en el entorno donde operan, en particular a causa de su interacción con personas físicas u otros sistemas. Los sistemas de IA serán resistentes a los intentos de terceros no autorizados de alterar su uso, comportamiento, resultados o funcionamiento aprovechando las vulnerabilidades del sistema. Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA podrán figurar, según corresponda, medidas para prevenir, detectar, responder a, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos») o los componentes preentrenados utilizados para el entrenamiento («envenenamiento de modelos»), los datos de entrada diseñados para hacer que el modelo cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo, que podrían traducirse en tomas de decisiones perjudiciales.	Obligatorio en sistemas de alto riesgo.
Evaluación de la conformidad.	El proveedor garantizará que el sistema de IA se someta al siguiente procedimiento de evaluación de la conformidad antes de su entrega: a. El proveedor verifica que el sistema de gestión de la calidad establecido cumple los requisitos legal y contractualmente establecidos. b. El proveedor examina la información presente en la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos legal y contractualmente establecidos. c. El proveedor también verifica que el proceso de diseño y desarrollo del sistema de IA sea coherente con la documentación técnica. El proveedor garantiza que el sistema de IA se someterá a un nuevo procedimiento de evaluación de la conformidad siempre que el proveedor modifique sustancialmente el sistema durante el período de vigencia del contrato.	Art. 11, 43 y concordantes Reglamento IA	Alta	Alta	Sí	En función del tipo de sistema, podrá establecerse la obligación del proveedor de realizar la evaluación de la conformidad de acuerdo con alguno de los procedimientos del art. 43 RIA.	
Ubicación.	Texto general: El proveedor del sistema deberá indicará, con carácter previo a la firma del contrato, dónde se encuentra ubicado el sistema y dónde se ubicará la información introducida por el responsable del despliegue. La citada información se podrá proporcionar mediante declaración responsable del proveedor. En sistemas que impliquen uso de datos personales, es importante determinar dónde se almacena la información recabada, para cumplir con las disposiciones relativas a transferencias internacionales del RGPD.	RGPD	Alta	Media	Sí, en función de si se tratan o no datos personales y de la ubicación del proveedor.	Texto modulado (cuando los sistemas impliquen uso de datos personales): El proveedor se compromete a tratar la información dentro de los estados miembros del EEE. La transferencia a terceros países u organizaciones requerirán la autorización previa y por escrito del responsable del despliegue. En este caso, el proveedor deberá incorporar al contrato las garantías adicionales que aseguren la protección adecuada de los datos personales de conformidad con la normativa vigente, tales como una decisión de adecuación, normas corporativas vinculantes o cláusulas contractuales tipo.	Obligatorio en sistemas que usen datos personales.
Implementación de políticas de uso de IA generativa	Desarrollar e implementar políticas internas para el uso responsable de herramientas de IA generativa.	Buenas prácticas recomendadas.	Media	Media			Para cualquier sistema.
Gestión de datos personales para entrenamiento de IA.	Garantizar que los datos utilizados para entrenar modelos de IA cumplan con las regulaciones de privacidad y derechos de autor.	RGPD	Alta	Media			Obligatorio en sistemas que usen datos personales.
Respeto de la propiedad intelectual en la IA.	Evaluar y asegurar que los sistemas de IA cumplan con las regulaciones de propiedad intelectual, evitando infracciones en el uso de datos protegidos por derechos de autor.	Normativa PI	Alta	Alta			Obligatorio en sistemas que puedan usar información protegida por derechos de autor.
Evaluación de impacto en derechos fundamentales	Realizar evaluaciones de impacto para identificar y mitigar los riesgos de los sistemas de IA en los derechos fundamentales de las personas.	Art. 27 Reglamento IA	Alta	Alta			Obligatorio en sistemas de alto riesgo.

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Actividad	Descripción	Origen	Imp	Dif	Requisito matizable	Detalle	Tipo de sistema
Responsabilidad / Indemnizaciones.	Regulación de la responsabilidad. Texto general: El proveedor indemnizará a la organización por cualesquiera reclamaciones presentadas por terceros, incluidos los supervisores, en relación con cualquier vulneración de sus derechos de propiedad intelectual, derechos a la intimidad o reclamaciones equivalentes relativas al conocimiento, la competencia ilícita, etc., con respecto a los conjuntos de datos del proveedor y los conjuntos de datos de terceros. La organización indemnizará al proveedor frente a cualesquiera reclamaciones presentadas por terceros, incluidos los supervisores, en relación con cualquier vulneración de sus derechos de propiedad intelectual, derechos a la intimidad o reclamaciones equivalentes relativas al conocimiento, la competencia ilícita, etc., con respecto a los conjuntos de datos de la organización.	Proyecto Directiva RC y PD; Directiva compraventa de bienes; Directiva contenidos y derechos digitales.	Alta	Media	Sí	Podrá modularse en función del tipo de sistema.	Para cualquier sistema.
Datos Personales.	Regulación uso datos personales sistemas IA.	RGPD	Alta	Media			Obligatorio en sistemas que usen datos personales.
Definiciones.	Incorporar definiciones al inicio del acuerdo.		Media	Media	Sí	Pueden añadirse definiciones adicionales si el sistema lo requiere.	Para cualquier sistema.
Descripción del sistema de IA y finalidad prevista.	El contrato debería incluir una descripción básica del sistema de IA y de la finalidad prevista, o remitirse a otro contrato, clausulado o documento donde se especifique.	Reglamento IA	Alta	Baja	Sí	Deberá personalizarse en función del sistema de IA.	Para cualquier sistema.
Conjuntos de datos.	El contrato debería describir los conjuntos de datos que se utilizarán para el entrenamiento (si procede), la validación y la prueba del sistema de IA. Debe hacerse la distinción entre conjuntos de datos de la organización, por un lado, y conjuntos de datos de proveedores y conjuntos de datos de terceros, por otro. En el caso de los conjuntos de datos de la organización, deben describirse las finalidades con las que el proveedor puede utilizar los conjuntos de datos (distintos de la ejecución del contrato) y si el proveedor está obligado a destruir el conjunto de datos al final del período de vigencia del contrato. En el caso de los conjuntos de datos del proveedor y los conjuntos de datos de terceros, se describirán las finalidades con las quela organización puede utilizar los conjuntos de datos y si el proveedor está obligado a entregarlos.	Art. 10 Reglamento IA / Buenas prácticas	Media	Media	Sí	Deberá personalizarse en función del sistema de IA.	Para cualquier sistema.
Proveedores.	Cadena de subcontratación. Texto general: El proveedor deberá identificar sus subcontratistas que intervengan en la entrega del sis-tema IA o, en todo caso, informar de los medios por los cuales el contratante podrá acceder a la relación de subcontratistas intervi-nientes en cada momento. En todo caso, el proveedor será responsable de que todos sus subcontratistas puedan cumplir y cumplan, como mínimo, todas las obligaciones que para el propio proveedor se estable-cen en el contrato, siendo pleno responsable de las consecuencias, de cualquier tipo, que se deriven de que cualquiera de sus subcontratis-tas no pueda cumplir o no cumpla dichas obligaciones.	Identificar roles y responsabilidades	Alta	Alta			Para cualquier sistema.
Propiedad Industrial.	Regulación sobre el uso de elementos susceptibles de Propiedad Industrial de los participantes o terceros.	Normativa P. Industrial	Media	Media			Obligatorio en sistemas que puedan usar información protegida por la P.I.
Sistema de gestión de la calidad en sistemas de alto riesgo	Ver artículo citado. Texto general: Antes de la entrega del sistema de IA, el proveedor establecerá un sistema de gestión de la calidad que garantice el cumplimiento de estas cláusulas. Dicho sistema se documentará de manera sistemática y ordenada mediante políticas, procedimientos e instrucciones escritas e incluirá, al menos, los extremos indicados en el art. 17.1 del Reglamento de Inteligencia Artificial.	Art. 17 Reglamento IA	Alta	Media	N/A	-	Obligatorio en sistemas de alto riesgo.

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Actividad	Descripción	Origen	Imp	Dif	Requisito matizable	Detalle	Tipo de sistema
Conservación de documentación en sistemas de alto riesgo.	Ver artículo citado.	Art. 18 Reglamento IA	Alta	Media			Obligatorio en sistemas de alto riesgo.
Generación de datos sintéticos.	Fuentes de datos de base y requisitos de resultados.	Buenas prácticas recomendadas	Baja	Baja			Para cualquier sistema.
Derechos relativos a conjuntos de datos de la organización.	Texto general: Todos los derechos, incluidos los derechos de propiedad intelectual, relacionados con los conjuntos de datos de la organización corresponden a la misma o a un tercero que este designe. El proveedor no tiene derecho a utilizar conjuntos de datos de la organización para fines distintos de la ejecución del contrato, salvo que se disponga lo contrario. Previo requerimiento de la organización, el proveedor deberá destruir los conjuntos de datos de la organización, salvo que se disponga otra cosa en las presentes cláusulas. Si la organización así lo solicita, el proveedor deberá aportar pruebas factibles de la destrucción de los conjuntos de datos indicados.	Art. 10 Reglamento IA / Buenas prácticas	Media	Alta	Sí	Podrán acordarse modificaciones por las partes.	Para cualquier sistema.
Derechos relativos a conjuntos de datos del proveedor y de terceros	Texto general: Todos los derechos, incluidos los derechos de propiedad intelectual, relativos a conjuntos de datos del proveedor y a conjuntos de datos de terceros corresponderán al proveedor o a un tercero. El proveedor concede a la organización un derecho no exclusivo a utilizar conjuntos de datos del proveedor y de terceros que, en cualquier caso, resulta suficiente para la ejecución de las disposiciones del contrato, incluidas las cláusulas, salvo disposición en contrario. Este derecho incluye el derecho a utilizar conjuntos de datos de proveedor y de terceros para el ulterior desarrollo del sistema de IA, en particular sus nuevas versiones, por parte de la organización o de un tercero.	Art. 10 Reglamento IA / Buenas prácticas	Media	Alta	Sí	Podrán acordarse modificaciones por las partes.	Para cualquier sistema.
Transmisión de los conjuntos de datos	Previo requerimiento de la organización, el proveedor transmitirá a la organización, o a un tercero designado por la misma, la versión más reciente de los conjuntos de datos de la organización, salvo disposición en contrario. Previo requerimiento de la organización, el proveedor transmitirá a la organización, o a un tercero designado por la misma, la versión más reciente de los conjuntos de datos del proveedor y de los conjuntos de datos de terceros, salvo disposición en contrario. El proveedor debe transmitir los conjuntos de datos a la organización en un formato estructurado, de uso común y lectura mecánica.	Art. 10 Reglamento IA / Buenas prácticas	Media	Alta	Sí	Podrán acordarse modificaciones por las partes.	Para cualquier sistema.
Mantenimiento (evolutivo, correctivo, adaptativo…)	Regular el posible mantenimiento sobre la IA contratada.	Normativa civil y mercantil	Media	Media			Para cualquier sistema.
Descripción de roles de participantes en contrato.	Establecer qué role tiene cada parte participante con relación a la establecidas en el Reglamento IA.	Reglamento IA	Alta	Alta			Para cualquier sistema.
Aprendizaje del sistema	Se debería regular cómo funciona el aprendizaje del sistema a partir de la información introducida y si tiene la capacidad de utilizar la información introducida por un responsable del despliegue en beneficio de otros.	Normativa de protección de datos, secretos empresariales y concordante	Alta	Media			Para cualquier sistema.
Registro de IA	Texto general: Previo requerimiento de la organización, el proveedor facilitará toda la información pertinente a los efectos de este contrato.	Código civil y normativa mercantil	Alta	Media	Sí	Texto modulado (por ejemplo en sistemas de alto riesgo o sobre materias que requieran registro): Previo requerimiento de la organización, el proveedor facilitará toda la información pertinente a los efectos de este contrato. La organización tendrá derecho a facilitar a terceros la información referida así como a revelarla, por ejemplo, en registros de sistemas de IA. Previo requerimiento de la organización, el proveedor ayudará a registrar los sistemas de IA en cualquier registro pertinente.	Para cualquier sistema.

CLAUSULAS CONTRACTUALES SISTEMAS / SERVICIOS DE IA

Actividad	Descripción	Origen	Imp	Dif	Requisito matizable	Detalle	Tipo de sistema
Cumplimiento y auditoría. Medidas correctoras.	Texto general: El proveedor debe garantizar que, desde la entrega del sistema de IA hasta el final del período de vigencia del contrato, el sistema de IA cumpla con estas cláusulas. Los proveedores deberán poner a disposición de la organización toda la información necesaria para demostrar el cumplimiento de las presentes cláusulas. La organización tendrá derecho a realizar, al menos, una auditoría anual. El proveedor está obligado a cooperar en las auditorías o inspecciones que realice la organización o un profesional u organización independiente en su nombre, con el fin de comprobar si el proveedor cumple con sus obligaciones. Si se determina que el proveedor no cumple las obligaciones establecidas en la presente cláusula, el proveedor estará obligado a subsanar las deficiencias detectadas en un plazo razonable. Si el proveedor no subsana las deficiencias detectadas en plazo, el proveedor incurrirá en incumplimiento del contrato. Si, durante el período de vigencia del contrato, el proveedor considera o tiene motivos para considerar que el sistema de IA no es conforme con las presentes cláusulas, adoptará inmediatamente las medidas correctoras necesarias para lograr su conformidad e informará a la organización al respecto.	Código civil y normativa mercantil	Alta	Media	Sí	Texto modulado (por ejemplo, en sistemas de alto riesgo): El proveedor debe garantizar que, desde la entrega del sistema de IA hasta el final del período de vigencia del contrato, el sistema de IA cumpla con estas cláusulas. Los proveedores deberán poner a disposición de la organización toda la información necesaria para demostrar el cumplimiento de las presentes cláusulas. La organización tendrá derecho a realizar, al menos, una auditoría anual. Adicionalmente, podrá realizar auditorías adicionales por causas sobrevenidas, tales como la modificación sustancial del sistema de IA. El proveedor está obligado a cooperar en las auditorías o inspecciones que realice la organización o un profesional u organización independiente en su nombre, con el fin de comprobar si el proveedor cumple con sus obligaciones. La organización elaborará o hará que se elabore un informe en el que se registrarán las conclusiones de la auditoría y donde el organismo público hará constar en qué medida el proveedor cumple las obligaciones derivadas del contrato. Si se determina que el proveedor no cumple las obligaciones establecidas en la presente cláusula, el proveedor estará obligado a subsanar las deficiencias detectadas en el plazo razonable que este establezca en el informe. Si el proveedor no subsana las deficiencias detectadas en plazo, el proveedor incurrirá en incumplimiento del contrato. Si, durante el período de vigencia del contrato, el proveedor considera o tiene motivos para considerar que el sistema de IA no es conforme con las presentes cláusulas, adoptará inmediatamente las medidas correctoras necesarias para lograr su conformidad e informará a la organización al respecto.	Para cualquier sistema.
Costes	Texto general: Salvo que las partes lleguen a otro acuerdo o que se disponga expresamente lo contrario en estas cláusulas, la organización no adeudará al proveedor ninguna tasa adicional por las labores necesarias para el cumplimiento de estas cláusulas.	Código civil y normativa mercantil	Baja	Media	Sí	Texto modulado: Se informa expresamente de que las siguientes actividades requeridas al proveedor para el cumplimiento de estas obligaciones podrían implicar costes adicionales: (especificar).	Para cualquier sistema.
Vigilancia postcomercialización	Texto general: El proveedor establecerá y documentará un sistema de vigilancia postcomercialización de forma proporcionada a la naturaleza de las tecnologías de IA y a los riesgos de los sistemas de IA de alto riesgo.	Art. 72 Reglamento IA	Alta	Alta	Sí, en función de la tecnología y el tipo de sistemas.	Deberá personalizarse en función del sistema de IA.	Alto riesgo.

5. IDENTIFICACION DE RIESGOS EN EL USO DE SISTEMAS DE IA Y GESTIÓN DE PROVEEDORES

La identificación de riesgos asociado al uso de sistemas de inteligencia artificial cobra una especial relevancia en la contratación de productos y servicios de IA con terceros, y debe iniciarse en las fases tempranas de selección de proveedores.

De este modo, ya en la fase de homologación es fundamental implementar determinados mecanismos que permitan detectar posibles factores de riesgo.

Este proceso de identificación no solo facilita la selección o exclusión de ciertos proveedores, sino que resulta esencial para redactar y estructurar las cláusulas que regirán la relación contractual.

A continuación procederemos a profundizar en la identificación y gestión de riesgos y cómo se han de gestionar en las distintas fases del ciclo de vida del proveedor. Para ello tomaremos de referencia el riesgo de privacidad que los sistemas y servicios de IA pueden tener asociado y daremos posteriormente unas pinceladas sobre otros riesgos que podrían tenerse en consideración.

A. RIESGOS DE PRIVACIDAD

Este proceso de identificación no solo facilita la selección o exclusión de ciertos proveedores, sino que resulta esencial para redactar y estructurar las cláusulas que regirán la relación contractual.

Cuando hay datos de carácter personal implicados, el Reglamento General de Protección de Datos en su artículo 28.1, ya establece que el responsable del tratamiento ha de elegir a un encargado del tratamiento de datos personales que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con el RGPD y garantice los derechos del interesado.

No obstante, no sólo la contratación implica riesgos para la privacidad, sino que también pueden converger riesgos de otros tantos ámbitos estrechamente relacionados con los sistemas de IA. Tales riesgos pueden surgir en la fase de implementación del producto o servicio, así como en cualquier momento de la prestación del servicio, incluyendo el cese del servicio o de la utilización del producto por diferentes motivos (finalización del contrato, etc.).

A continuación, se describen las principales fases del ciclo de vida de un proveedor desde el análisis inicial de aquellos proveedores que optan a la provisión de sistemas de inteligencia artificial y/o prestación del servicio como la selección final del proveedor en base a criterios de madurez y su contratación posterior; la fase del despliegue, que se puede considerar una especialidad específica de la contratación de sistemas de inteligencia artificial, hasta la monitorización periódica de proveedores y la baja final del proveedor. De esta forma, la gestión de riesgos es relevante y tiene sus propias particularidades en todas y cada una de las fases del ciclo de vida del proveedor.

FASES DEL CICLO DE VIDA DEL PROVEEDOR

FASE 1. Selección de Proveedores y Contratación

La selección de proveedores es una fase crucial en la que considerar varios factores para asegurar el cumplimiento de unos estándares de privacidad, seguridad.

Existe una serie de factores que pueden ser determinantes en la contratación con el proveedor y que pueden incidir en la toma de decisiones de un proveedor respecto de otro, dependiendo de los riesgos de privacidad derivados del tratamiento de datos por parte de los proveedores:

1.1. Recogida y tratamiento de datos

Antes de seleccionar un proveedor de IA, es fundamental identificar y evaluar los tipos de datos que el proveedor recopilará, almacenará y procesará. Esta evaluación debería detallar el volumen, naturaleza y procedencia de los datos, verificando si se trata de datos sensibles o especialmente protegidos. En esta fase, se deben establecer requisitos contractuales para asegurar que el proveedor cumpla con principios de minimización de datos y de adecuación, garantizando que solo se recojan datos estrictamente necesarios.

Igualmente será necesario conocer la información pertinente sobre los conjuntos de datos que hayan sido utilizados para el desarrollo del sistema, la cual, en su caso, deberá haber sido facilitada por el proveedor en la documentación técnica que acompañe al sistema de IA.

1.2. Transparencia e información del funcionamiento de la IA

La transparencia es uno de los principales requisitos a evaluar de cara a formalizar la contratación de un proveedor de IA, materializándose a través de dos vías: la explicabilidad del sistema y la información facilitada a los usuarios finales.

Respecto a la primera, en el contrato, debe incluirse una cláusula que obligue al proveedor a proporcionar una descripción comprensible de cómo su IA procesa los datos y llega a sus decisiones, así como de los factores que pueden influir en su rendimiento. Además, se recomienda exigir al proveedor un compromiso con prácticas de explainability, o explicabilidad, de modo que pueda entenderse y auditarse el sistema en caso de incidentes.

Por otro lado, la transparencia hacia los usuarios finales es fundamental para preservar su privacidad y derechos. Durante esta fase, debe solicitarse al proveedor que facilite la información que se proporcionará a los usuarios explicando cómo sus datos serán procesados por la IA. Los contratos deberían incluir compromisos del proveedor para garantizar la disponibilidad de esta información y adaptar su lenguaje a las normativas de privacidad vigentes.

1.3. Gestión de derechos

El proveedor deberá comprometerse a colaborar en la gestión de derechos de los interesados (acceso, rectificación, supresión, oposición, etc.). Debe incluirse una cláusula que especifique cómo se atenderán las solicitudes de los titulares de los datos y los plazos de respuesta, así como las responsabilidades del proveedor en la ejecución de los derechos. También deben establecerse los procedimientos y herramientas para garantizar la efectividad de esta gestión.

1.4. Finalidad del tratamiento

El contrato debe definir claramente las finalidades del tratamiento de datos y asegurarse de que el proveedor no realice tratamientos adicionales o incompatibles. Es recomendable añadir una cláusula en la que el proveedor se comprometa a no utilizar los datos personales para fines distintos a los estipulados contractualmente, limitando su uso exclusivamente al objeto de la contratación.

1.5. Transferencias Internacionales

Es común que los proveedores de IA operen en diversas jurisdicciones. Por lo tanto, es crucial incluir en el contrato los requisitos para el cumplimiento de la normativa sobre transferencias internacionales. Esto incluye estipular las salvaguardias ade cuadas, como el uso de cláusulas contractuales tipo (Standard Contractual Clauses), y evaluar los

riesgos inherentes en las transferencias de datos fuera del Espacio Económico Europeo (EEE), especialmente si el proveedor tiene servidores o centros de procesamiento en terceros países.

1.6. Almacenamiento de la información

El contrato debe especificar el lugar de almacenamiento de los datos personales y, si es necesario, los proveedores deben comprometerse a emplear servicios de almacenamiento en territorios que ofrezcan un nivel adecuado de protección.

Esta cláusula puede acompañarse de una obligación de realizar auditorías periódicas para confirmar el cumplimiento de las políticas de almacenamiento seguro.

1.7. Base de legitimación del tratamiento

Es fundamental que la base jurídica para el tratamiento de datos sea identificada y documentada con claridad. Dependiendo del caso, puede ser el consentimiento de los usuarios, la ejecución de un contrato, el interés legítimo o el cumplimiento de una obligación legal. El contrato debe reflejar la base de legitimación correspondiente y exigir al proveedor que no realice tratamientos sin esta legitimación.

FASE 2. Gestión de la privacidad durante el despliegue del sistema de IA

Aun después de haberse concluido la fase de homologación y contratación del proveedor, y de que el sistema de inteligencia artificial se haya integrado en las actividades del responsable de su despliegue, es esencial mantener un proceso constante de identificación y gestión de los riesgos potenciales para la privacidad que puedan surgir con el uso de dicho sistema.

Este seguimiento continuo permitirá anticipar y mitigar nuevas situaciones de riesgo que podrían no haber sido identificadas en las fases iniciales, o que, únicamente se manifestarán en relación con el uso que haga del sistema el responsable del despliegue.

Dentro de esos posibles factores de riesgo pueden identificarse los siguientes grupos o criterios:

- **Recogida de los datos personales** que será utilizada como input en el despliegue del sistema IA.
  - » Ausencia de base de legitimación adecuada para el tratamiento de los datos y, en su caso, ausencia de consentimiento informado.
  - » Ausencia de transparencia a la hora de recabar los datos para su tratamiento con Inteligencia Artificial.
  - » Ausencia de transparencia respecto al entrenamiento constante durante el despliegue.

- **Sesgos algorítmicos:**
  Si los datos de entrenamiento contienen sesgos, los resultados proporcionados por la IA también pueden estar sesgados, lo que puede llevar a decisiones injustas o discriminatorias.

- **Medidas de seguridad implementadas en el Sistema de Inteligencia Artificial:**
  - » Durante la fase de entrenamiento, prueba y validación.
  - » Implementadas para la ciberseguridad durante el despliegue.

- **Uso indebido de la información y los datos:** riesgo de que la información recopilada y procesada por la IA sea utilizada de forma inapropiada (ej.: para finalidades no informadas, utilizando datos más allá de los estrictamente necesarios, etc.).

- **Interrupción de operaciones:** Un fallo en la gestión de datos por parte de un proveedor puede interrumpir las operaciones de la empresa contratante, afectando la continuidad del negocio.

- **Multas y sanciones:** Las violaciones de privacidad pueden resultar en multas significativas y sanciones regulatorias, lo que puede tener un impacto financiero considerable.

- **Falta de asignación y distribución de responsabilidades:** riesgo de ausencia de claras responsabilidades ante una violación de la privacidad como consecuencia del uso de Inteligencia Artificial.

- **Incumplimiento de la confidencialidad:** clausulado que refuerce y garantice la confidencialidad del proveedor respecto a los datos y la información que sea tratada por el Sistema de IA durante el despliegue.

- **Problemas reputacionales:** Si un proveedor sufre un incidente de seguridad, esto puede afectar negativamente la reputación de la empresa contratante, especialmente si se asocia con la falta de diligencia en la selección del proveedor, si bien esto puede suceder en cualquier momento de la prestación del servicio por el proveedor.

FASE 3. Monitorización y Seguimiento

La fase de monitorización persigue asegurar que los terceros cumplan con los estándares de privacidad y seguridad establecidos. Esto incluye auditorías regulares, evaluaciones de riesgo y la implementación de controles continuos para detectar y mitigar posibles amenazas. Por tanto, además de la comprobación del cumplimiento de los requisitos de Privacidad que se identificaron en el momento de la contratación, hay algunos aspectos cuya comprobación es relevante en esta fase:

3.1. Monitorización de Incidentes y Vulnerabilidades

Dado el uso de IA, es posible que surjan vulnerabilidades o incidentes relacionados con el tratamiento de datos personales. El contrato debe exigir que el proveedor implemente sistemas de monitorización continua para detectar posibles vulnerabilidades de seguridad en sus algoritmos. También es recomendable exigir que el proveedor notifique cualquier incidente de seguridad en un plazo definido (por ejemplo, 24 horas), junto con un plan de acción inmediato para minimizar los daños.

3.2. Transparencia Continua en el Funcionamiento del Algoritmo

El proveedor debe comprometerse a mantener informada a la organización sobre cualquier cambio relevante en el funcionamiento del algoritmo que pueda afectar la privacidad de los usuarios. Estos cambios pueden incluir actualizaciones en el modelo, ajustes en el procesamiento o mejoras de seguridad. El contrato debe estipular que cualquier modificación del algoritmo sea documentada y comunicada para una revisión de conformidad.

3.3. Plazos de Retención

Es esencial acordar y documentar los plazos de retención de los datos personales, con cláusulas contractuales que obliguen al proveedor a eliminar o anonimizar los datos al final del periodo de retención. Se recomienda establecer auditorías periódicas para verificar el cumplimiento de estos plazos y garantizar la eliminación segura de los datos según lo estipulado.

3.4. Alto Riesgo y Evaluación de Impacto para los Derechos y Libertades

El uso de IA puede implicar un alto riesgo para los derechos y libertades de los interesados, especialmente si se trata de datos sensibles o si las decisiones automatizadas afectan significativamente a los individuos. En esta fase, debe requerirse que el proveedor realice una Evaluación de Impacto en la Protección de Datos (EIPD) para evaluar y mitigar los riesgos potenciales. El contrato puede incluir una cláusula de colaboración para realizar evaluaciones conjuntas cuando sea necesario y tomar medidas para minimizar los riesgos.

El proveedor debe realizar revisiones periódicas de los plazos de retención y de la EIPD, ya que los cambios en los procesos de IA pueden afectar el nivel de riesgo. El contrato debe incluir una cláusula que obligue al proveedor a actualizar sus evaluaciones de impacto y sus plazos de retención si se modifican significativamente los procesos o finalidades del tratamiento de datos.

3.5. Subcontratación

La subcontratación de proveedores para la prestación del servicio o para el desarrollo del producto requiere del cumplimiento de los mismos estándares de privacidad y seguridad, por lo que en esta fase debe requerirse la confirmación de las empresas subcontratadas, de la comprobación de las condiciones contractuales pactadas, así como la posible existencia de algún riesgo derivado de esta subcontratación que pueda comprometer la privacidad y la seguridad.

FASE 4. Baja del Proveedor

La implantación de un plan de baja bien estructurado es esencial para proteger los datos personales, minimizar los riesgos asociados a esta fase y asegurar una transición segura y controlada.

4.1. Gestión de la Información al Finalizar la Relación Contractual

Al finalizar la relación con el proveedor, se deben establecer procedimientos claros para la devolución, eliminación o anonimización de los datos. Es recomendable incluir en el contrato una cláusula que establezca la obligación del proveedor de eliminar todos los datos personales de sus sistemas de manera segura y documentar el proceso de eliminación. Además, se puede exigir que se emita una certificación que confirme la eliminación o anonimización de los datos, junto con el cumplimiento de las políticas de retención y borrado.

4.2. Transferencias de Datos a un Nuevo Proveedor

Si los datos personales deben transferirse a un nuevo proveedor, deben establecerse las medidas técnicas y organizativas necesarias para asegurar que la transferencia se realice de manera segura y conforme a la normativa aplicable. El contrato debe estipular las condiciones bajo las cuales se realizará esta transferencia, incluyendo las salvaguardias de seguridad para evitar pérdidas o accesos no autorizados durante el proceso.

B. OTROS RIESGOS

Adicionalmente a los riesgos contemplados en el epígrafe anterior hay otra serie de riesgos que han de tenerse en consideración a la hora de realizar esta evaluación del riesgo de un sistema de IA.

Para este compendio de **materias de riesgos de sistemas de IA,** se ha tomado de referencia tanto el **EU HLEG ALTAI**[7] como el **NIST AI RMF**[8]

Se complementa la tabla con el detalle de si cada materia de riesgo es generalmente exigible (exigible para cualquier sistema empresarial) o si es exigible en virtud del RIA.

Materias de Riesgo IA	Descripción	generalmente exigible?	exigible por AI Act?
Validez	Cumplimiento de su función prevista; puede medirse, por ejemplo, mediante métricas como exactitud, precisión, exhaustividad o coherencia y factualidad. Para ello será conveniente auditar el sistema periódicamente.	sí	Alto riesgo: artículo 8, 15
Fiabilidad	Validez sostenida, robustez del sistema durante su funcionamiento a lo largo el tiempo, incluso ante desviaciones respecto a su forma de uso esperada.	sí	Alto riesgo: artículo 15
Supervisión humana	Posibilidad de permitir la verificación de las salidas del sistema, incluso antes de que la misa sea tenida en cuenta y obre su efecto	depende del caso	Alto riesgo: artículo 14
Gobierno de datos	Gestión diligente de los datos en todo el ciclo de vida del sistema, desde entrenamiento, validación, pruebas e inferencia (uso). Si bien esta práctica es parte necesaria para garantizar la validez del sistema, se trata como una materia aparte dado que los sistemas de IA son extremadamente sensibles a los datos sobre los que trabajan y cualquier modificación no intencionada de los mismos (accidental o maliciosa) puede provocar comportamientos indeseados y difíciles de detectar y corregir de forma inmediata.	sí	Alto riesgo: artículo 10

[7] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[8] https://www.nist.gov/itl/ai-risk-management-framework

Materias de Riesgo IA	Descripción	generalmente exigible?	exigible por AI Act?
Seguridad (no causar daño)	No producir riesgo sobre la vida, salud, bienes o entorno, por ejemplo, evitando proporcionar información sobre actividades peligrosas, delictivas, incitadoras de odio o discriminación o proporcionando consejo sobre materias cuya correcta interpretación requiera capacitación de la audiencia superior a la esperable por defecto.	depende del caso	Alto riesgo: artículo 15
Ciberseguridad	Resistencia a ataques y fallos derivados de vulnerabilidades, específicas de sistemas IA o genéricas, que puedan comprometer la disponibilidad, integridad o disponibilidad del sistema o los datos manejados por el mismo.	sí	Alto riesgo: artículo 15 (al proveedor se le puede exigir información sobre vulnerabilidades y controles, si bien la aplicación de los controles será normalmente responsabilidad del implementador).
Resiliencia	Capacidad de mantener funcionamiento en circunstancias adversas, con a lo sumo degradación parcial de capacidad o con capacidad de degradación informada y ordenada.	sí	Alto riesgo: artículo 15
Responsabilidad	Hacer frente a las consecuencias derivadas del funcionamiento correcto del sistema, implantando las medidas necesarias para limitar o eliminar los efectos de su funcionamiento erróneo.	sí	Alto riesgo: artículo 12 (producción, mantenimiento o ambos, de los registros/trazas, según el sistema/servicio contratado).
Transparencia	Informar sobre el hecho de estar interactuando con un sistema basado en IA (en mayor o menor medida). Informar sobre el diseño, funcionamiento y parámetros relevantes del sistema, según el caso y la audiencia. Proporcionar trazas que permitan analizar a bajo nivel como el sistema ha llegado a la decisión. Poder responder a "¿Qué ha pasado?"	depende del caso	Artículo 50 (en los supuestos aplicables) Modelos de propósito general: artículo 53 Modelos de propósito genera de riesgo sistémico: artículo 55 Alto riesgo: artículo 11, 12, 13
Explicabilidad	Proporcionar información que permita entender razonablemente como se ha producido la respuesta del sistema. Para ello será conveniente monitorizar continuamente el sistema y probarlo/auditarlo periódicamente. Poder responder a "¿Cómo ha pasado?"	sí	Alto riesgo: artículo 11, 12, 13
Interpretabilidad	Proporcionar información que permita entender el significado de la respuesta del sistema en el contexto del uso específico del mismo. Poder responder a "¿Qué significa lo que ha pasado?"	sí	Alto riesgo: artículo 11, 12, 13
Privacidad	Tratamiento apropiado (según normativas de privacidad como RGPD) de datos privados, protección de los mismos durante el entrenamiento, pruebas y uso del sistema, evitando que datos privados puedan accederse por entes no autorizados (personas os sistemas), incluyendo la inferencia de los mismos a parir de las respuestas del sistema.	sí, si el sistema usa datos personales para entrenamiento o para su funcionamiento (RGPD)	Alto riesgo: artículo 10 (entrenamiento)
Equidad	Evitar el sesgo y la discriminación, especialmente en la toma de decisiones sobre personas, por ejemplo, evitando que determinados colectivos puedan verse perjudicados por una distribución desequilibrada de los datos de entrenamiento del modelo IA. El sesgo puede deberse a otros factores, como los algoritmos, además de la distribución de los datos de entrenamiento. La falta de equidad (o la presencia de sesgo en los datos de entrenamiento) no solo afecta a la toma de decisiones sobre personas. También puede afectar a cualquier toma de decisiones si los datos de entrenamiento o los algoritmos no son suficientemente equilibrados respecto a todas las casuísticas susceptibles de ser evaluadas.	sí	Alto riesgo: artículo 10

6. MODELOS DE CLAUSULAS

A. CLAUSULA GÉNERICA A INCLUIR EN CONTRATOS

Como hemos ido viendo, la inteligencia artificial ha irrumpido en el mercado de manera significativa, transformando diversos sectores y ofreciendo nuevas oportunidades para los proveedores. Gracias a esta tecnología avanzada, los proveedores pueden integrar la IA en sus actividades diarias, mejorando la eficiencia operativa, optimizando la gestión de recursos y proporcionando servicios más personalizados y de alta calidad a sus clientes.

Por eso, es más que probable que todo proveedor que se vaya a contratar o que ya esté contratado, proceda a utilizar sistemas de IA en su actividad diaria o incluso directamente en la prestación del servicio que proporciona a la entidad. Para controlar esta situación y el riesgo que esto puede tener asociado, se determina la necesidad de incluir una cláusula específica en todo contrato de proveedor que controle este tipo de situaciones.

Con esta cláusula además, se pretender ir controlando la IA Embebida que pueda existir en la organización. Entendiendo como IA Embebida aquella que se integra en dispositivos y/o sistemas ya existentes que no contaban en su inicio con este tipo de tecnologías y funcionalidades.

Incidir en que no se trata de una cláusula específica de IA ni únicamente para aquellos proveedores que ofrezcan específicamente sistemas o servicios de IA.

El objetivo de esta cláusula es disponer de un texto de carácter genérico para incorporar en los contratos de cualquier servicio que nos pueda prestar un proveedor para tratar de incorporar controles en caso de que este proveedor utilice para la prestación de dicho servicio sistemas de IA. Por ejemplo, en la contratación de un servicio de traducción automática en la nube (SAAS), que contratamos con un proveedor, podremos incluir esta cláusula de salvaguardia.

A continuación, trasladamos una propuesta de redacción de una cláusula contractual IA que podrá adaptar a sus concretas necesidades, y también a su específico apetitito del riesgo, para lo que se propone un sistema de autorización previa en función de la clasificación de sistemas IA del RIA.

BORRADOR CLÁUSULA GENÉRICA CONTRATOS IA

Si el Proveedor propone utilizar Inteligencia Artificial, (específicamente Inteligencia Artificial generativa) en la prestación del servicio y/o en la provisión de los entregables, el Proveedor debe informar siempre con carácter previo y por escrito a la organización/empresa, sin perjuicio que en función del riesgo que pueda suponer el tipo de IA utilizado, deba implicar también una autorización previa.

Concretamente, para determinar la necesidad de autorización de la organización, se atenderá a lo previsto en el siguiente cuadro:

SUPUESTO RIA	NIVEL DE RIESGO RIA	REQUIERE INFORMACION PREVIA	REQUIERE AUTORIZACION PREVIA
PROHIBIDO	INACEPTABLE	SI	NO CABE AUTORIZACION
EVALUACION DE CONFORMIDAD		SI	SI
OBLIGACION DE TRANSPARENCIA		SI	SI
SIN OBLIGACIONES		SI	NO ES NECESARIA

No obstante, en relación con aquellos productos y servicios que pudiesen presentar un riesgo limitado, también es posible adaptar el sistema propuesto más arriba mediante la pre-clasificación de algunos de los servicios o productos de IA más utilizados o de uso más previsible para cada concreta compañía, de modo que sin perjuicio de los correspondientes análisis de riesgo y privacidad por diseño y por defecto, los concretos productos o servicios como excepción se consideren aceptables para su contratación no quedando sujetos a autorización por disponer de una evaluación de conformidad previa.

El prestador del servicio del que es objeto el presente contrato declara expresamente que utiliza/no utiliza (tachar la que no aplique) tecnología de inteligencia artificial (en adelante IA) para la prestación del servicio.

En caso de proponer durante la prestación del servicio el uso de Inteligencia Artificial (especialmente Inteligencia Artificial generativa), el Proveedor deberá comunicarlo a la organización con una antelación previa de un mes por los medios designados al efecto en la cláusula de notificaciones y obtener la previa autorización escrita para proceder a su uso[9], de conformidad con lo establecido en el párrafo siguiente.

[SOLO INCLUIR PÁRRAFO A CONTINUACIÓN SI LA SOLUCIÓN USA IA]

En el cado de utilización de tecnología o sistemas de inteligencia artificial en la prestación del servicio, el prestador se compromete, bajo pena de nulidad contractual, expresamente a los siguientes extremos:

A obtener la correspondiente autorización por escrito sobre el concreto servicio y proveedor que le va a prestar el servicio. A estos efectos se presentará un informe en el que se declare que la solución de IA que va a utilizar cumple con los requerimientos del Reglamento General de Protección de Datos Personales[10] y demás normativa de aplicación en esta materia, así como con los requerimientos del Reglamento de IA[11] , los estándares de la OCDE para la clasificación de los sistemas de IA de 2022 y la ISO/IEC TR 24027:2021 y cualquier otro estándar que sean aplicables al servicio.

A explicar las técnicas y algoritmos que utilizará la solución de IA, así como las posibles limitaciones o sesgos inherentes a las técnicas y algoritmos.

A formalizar, cuando proceda, un contrato encargo de tratamiento de datos personales con el CLIENTE, de conformidad con lo previsto en el art. 28 RGPD, así como, en su caso, a formalizar un contrato de subencargado de tratamiento de datos personales con el proveedor de la solución IA. En este caso se deberá informar y autorizar de cualquier cambio en el proveedor del servicio de conformidad con el art. 28.2 RGPD.

A asumir la responsabilidad que se pueda derivar del uso de la solución IA como consecuencia de riegos tecnológicos, continuidad de negocio y ataques cibercriminales.

A asumir la responsabilidad derivada del incumplimiento por parte de la solución IA del Reglamento de IA y otra normativa sobre la responsabilidad civil extracontractual derivada del uso de la inteligencia artificial; así como la normativa en materia de propiedad intelectual o industrial y de secretos empresariales, de la normativa de protección de datos personales o de otros derechos fundamentales (igualdad, etc.), así como cualquier otra responsabilidad que afecte a la seguridad de la información de la organización o a otra normativa que pudiese ser de aplicación.

B. CLAUSULA A INCLUIR EN CONTRATOS de sistemas / servicios de IA

Cuando el contrato está relacionado directamente con la contratación de un sistema o servicio de IA, es importante incorporar un clausulado específico que recoja los distintos requisitos que se hayan considerado necesario en función del tipo de sistema o servicio objeto de la contratación.

[9] Esta autorización dependerá del apetito del riesgo de cada entidad, por lo que se podrá modular la autorización en función del umbral de riesgo o clasificación del sistema IA que utilice el proveedor según lo expuesto en la tabla.

[10] 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

[11] 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 y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

Como se ha visto anteriormente en el inventario de requisito, los requisitos puede ser de muy diversa tipología y lo importante es seleccionar aquellos que se consideren necesarios.

A continuación se muestra un borrador de Clausula a utilizar en este tipo de servicios. Borrador ya que se debería tomar como partida para completarlo o adaptarlo tanto a la realidad de la compañía contratante como al servicio / sistema contratado BORRADOR CLÁUSULA GENÉRICA PARA INCORPORAR EN CONTRATOS DE SISTEMA / SERVICIOS DE IA

El Proveedor reconoce que el uso de la IA es una parte integral del mismo, se compromete expresamente al cumplimiento de los siguientes requisitos:

1. Conformidad Normativa y Documentación

1.1 Cumplimiento Normativo

El Proveedor garantiza que el sistema de inteligencia artificial (en adelante, "IA") y sus servicios asociados cumplen con el Reglamento (UE) 2024/1689 sobre inteligencia artificial (en adelante, "RIA"), el Reglamento General de Protección de Datos (UE) 2016/679 (en adelante, "RGPD"), y demás normativas aplicables, incluyendo normas de protección de datos personales, propiedad intelectual, industrial, y buenas prácticas de la industria. En caso de tratarse de un sistema de alto riesgo, el Proveedor implementará todas las medidas adicionales que el RIA requiere para estos sistemas.

El proveedor asegurará que el sistema de IA cumpla con las disposiciones establecidas a continuación desde su entrega hasta el final del contrato.

1.2 Documentación de Conformidad

El Proveedor pondrá a disposición del Cliente, cuando este lo solicite y en todo caso cuando sea legalmente exigible, la documentación que acredite la conformidad del sistema con la normativa aplicable, y las presentes cláusulas. Esto incluirá una declaración de conformidad y, en su caso, la certificación emitida por un organismo notificado en la Unión Europea. La documentación incluirá los resultados de los procedimientos de evaluación de conformidad, pruebas y verificaciones.

1.3 Notificación de Cambios Regulatorios

El Proveedor notificará, de manera fehaciente, al Cliente cualquier cambio regulatorio que afecte al sistema de IA de inmediato, junto con las actualizaciones necesarias para mantener la conformidad con la normativa vigente, a través del siguiente canal: [identificar correo electrónico, teléfono…etc.], sin dilación indebida.

2. Gestión de Conjuntos de Datos y Mitigación de Sesgos

2.1 Calidad y Pertinencia de los Datos

El Proveedor garantiza que los datos utilizados en la IA serán pertinentes, representativos y libres de errores en la medida de lo posible, con propiedades adecuadas al contexto de uso. El Proveedor tomará medidas para detectar y mitigar sesgos en los datos de entrenamiento, validación y prueba, conforme a las buenas prácticas estadísticas y los requisitos del RIA.

2.2 Documentación y Transparencia de los Datos

El Proveedor documentará el origen, las características y el procesamiento de los datos utilizados, manteniendo registros detallados y accesibles para el Cliente. Esta documentación incluirá una evaluación de calidad de los datos, así como un análisis de los posibles sesgos y las medidas adoptadas para su mitigación.

2.3 Actualización de los Conjuntos de Datos

El Proveedor actualizará periódicamente los conjuntos de datos y la documentación correspondiente para asegurar su adecuación continua al propósito del sistema de IA.

3. Sistema de Gestión de Riesgos

3.1 Implementación de un Sistema de Gestión de Riesgos

El Proveedor ha implementado un sistema de gestión de riesgos conforme al RIA, que cubre la detección, estimación y mitigación de riesgos que puedan afectar la seguridad, los derechos fundamentales y el cumplimiento regulatorio.

3.2 Componentes del Sistema de Gestión de Riesgos

Este sistema incluye, entre otros, los siguientes elementos:

- **Detección y Evaluación de Riesgos:** Identificación de riesgos conocidos y previsibles, incluyendo aquellos derivados del uso indebido razonablemente previsible del sistema de IA.
- **Medidas de Mitigación y Control:** Adopción de acciones específicas para eliminar o reducir los riesgos detectados.
- **Monitoreo Continuo y Ajustes:** Establecimiento de un mecanismo de monitoreo constante para identificar y gestionar riesgos emergentes durante el ciclo de vida del sistema de IA.

3.3 Documentación y Auditorías de Riesgos

El Proveedor documentará los riesgos detectados, los controles implementados y las pruebas realizadas, y proporcionará esta documentación al Cliente antes de la entrega del sistema. Este sistema estará sujeto a auditorías externas si el Cliente lo requiere siempre con un preaviso de, al menos, 10 días.

4. Transparencia, Explicabilidad y Supervisión Humana

4.1 Transparencia del Sistema de IA

El sistema de IA está diseñado para ofrecer transparencia y permitir al Cliente comprender su lógica y funcionamiento. El Proveedor proporcionará documentación clara y soporte técnico para asegurar que el Cliente pueda supervisar y entender adecuadamente el sistema, especialmente en los siguientes aspectos:

- **Lógica y Toma de Decisiones:** Explicación de los principios y métodos utilizados por el sistema de IA para la toma de decisiones, así como de las posibles limitaciones que puedan afectar la precisión y confiabilidad de los resultados.
- **Interacción con Personas Físicas:** En caso de que el sistema interactúe con personas físicas, la información proporcionada será clara y comprensible, especialmente para colectivos vulnerables.
  La información relacionada con las medidas para garantizar la transparencia, se encuentran identificadas en el anexo A. El proveedor deberá proporcionar al Cliente la información necesaria para explicar las decisiones del sistema de IA a los usuarios con respecto a los que se utilice o está previsto que se utilice el sistema de IA. En caso de ser necesario, la información contendrá ejemplos ilustrativos que aborden las limitaciones, así como los usos previstos y excluidos del sistema de IA.

El proveedor deberá proporcionar al Cliente, a petición de este, la información correspondiente al registro del sistema de IA.

4.2 Supervisión Humana y Capacitación

El Proveedor implementará medidas para garantizar la supervisión humana adecuadas a los riesgos asociados, incluyendo mecanismos de intervención que permitan a los operadores detectar y mitigar posibles riesgos o anomalías en el funcionamiento del sistema. El personal del Cliente recibirá formación específica y acceso a instrucciones claras sobre cómo supervisar y controlar el sistema. Este detalle se encuentra identificado en el anexo B.

4.3 Notificación de Modificaciones en la Lógica del Sistema

En caso de modificaciones sustanciales en la lógica o los datos del sistema que puedan afectar la transparencia, el Proveedor notificará al Cliente y actualizará la documentación técnica en consecuencia.

5. Documentación Técnica y Conservación de Registros

5.1 Entrega de Documentación Técnica

El Proveedor entregará al Cliente la documentación técnica e instrucciones de uso necesarias, que incluirán al menos:

- Identificación del Proveedor, contacto y ubicación del sistema de IA.
- Descripción del sistema, su precisión, capacidades y limitaciones.
- Información sobre los datos procesados, recursos necesarios y mecanismos de supervisión humana.
- Especificaciones técnicas y métodos de desarrollo utilizados.
- Idioma de redacción de la documentación técnica y las instrucciones de uso.

La información de la documentación técnica se encuentra identificada de conformidad a lo dispuesto en el anexo C. El detalle de las instrucciones de uso se encuentra identificadas en el anexo D.

5.2 Registro de Eventos y Trazabilidad

El Proveedor implementará un sistema de registro de eventos durante el funcionamiento de la IA, asegurando trazabilidad y acceso seguro para el Cliente. En particular, los registros permitirán registrar sucesos para detectar situaciones que puedan:

a. Presentar un riesgo para la salud, la seguridad o los derechos fundamentales de las personas, o
b. Suponer una modificación sustancial.

Estos registros permitirán auditar el sistema y estarán disponibles durante al menos 10 años tras la finalización del contrato, en conformidad con el artículo 12 del RIA.El Proveedor conservará los archivos de registro generados automáticamente por el sistema de IA, en la medida en que dichos archivos se encuentren bajo su control en el marco del contrato durante el período de vigencia de este. Al final del período de vigencia del contrato, el proveedor facilitará estos registros al organismo público sin demora.

5.3 Notificación de Incidentes de Seguridad

En caso de incidente de seguridad o fallo crítico, el Proveedor notificará, de manera fehaciente, al Cliente en un plazo máximo de 48 horas, a través del siguiente canal: [identificar correo electrónico, teléfono…etc.], proporcionando detalles sobre el incidente y las medidas correctivas adoptadas.

6. Actualización y Mantenimiento de Conformidad

6.1 Compromiso de Actualización y Conformidad Continua

El Proveedor se compromete a mantener el sistema de IA en conformidad con los requisitos normativos durante toda la vigencia del contrato. Esto incluye realizar actualizaciones periódicas para mejorar la precisión, robustez y seguridad del sistema, e informar al Cliente de cualquier cambio que pueda afectar su funcionamiento.

6.2 Notificación y Evaluación de Conformidad de Actualizaciones

Cada actualización significativa será notificada previamente al Cliente, y se actualizará la evaluación de conformidad si el cambio afecta la seguridad o los resultados del sistema. Esta evaluación será documentada y proporcionada al Cliente.

7. Derechos sobre los Conjuntos de Datos

7.1 Derechos del Cliente sobre sus Conjuntos de Datos

El Cliente conservará la titularidad exclusiva de todos los derechos de propiedad intelectual sobre los conjuntos de datos que proporcione al Proveedor. Estos datos serán considerados propiedad exclusiva del Cliente, y el Proveedor los utilizará únicamente en el marco y para los fines estrictamente necesarios para la ejecución de este contrato, salvo autorización expresa del Cliente. El Cliente podrá solicitar, según corresponda que el Proveedor destruya los conjuntos de datos del Cliente, así como aportar evidencias de dicha destrucción a petición del Cliente.

7.2 Limitación de Uso y Confidencialidad

El Proveedor no obtendrá, por virtud de este contrato, ningún derecho de propiedad, licencia o uso sobre los conjuntos de datos proporcionados por el Cliente, salvo aquellos necesarios para la ejecución del contrato. A solicitud del Cliente, el Proveedor deberá devolver, destruir o eliminar permanentemente todos los datos al finalizar el contrato.

7.3 Derechos de Uso del Cliente sobre los Datos proporcionados por el Proveedor

El Cliente tendrá un derecho de uso no exclusivo, intransferible y limitado sobre los conjuntos de datos proporcionados por el Proveedor para la utilización del sistema de IA según los términos de este contrato.

El proveedor garantizar al Cliente que el conjunto de datos proporcionados por el Proveedor ha sido recopilado de conformidad a la normativa aplicable, especialmente habiendo cumplido con los requisitos de transparencia sobre el fin original de la recopilación de datos.

7.4 Comunicación de los conjuntos de datos

El Cliente podrá solicitar al Proveedor la transmisión de los conjuntos de datos, en su versión más reciente, en el formato designado por el Cliente [identificar formato de archivo]

8. Protección de Datos Personales

8.1 Cumplimiento de normativa de protección de datos personales

8.1.1 Ambas partes cumplirán con todas las disposiciones del RGPD y demás normativas aplicables en relación con la protección de datos personales. Según corresponda, el tratamiento de datos biométricos realizado mediante un sistema de IA para la identificación biométrica debe cumplir lo establecido en el artículo 10 de la Directiva (UE) 2016/680.

8.1.2. Los firmantes quedan informados sobre el tratamiento de datos, realizado por parte de Cliente y del Proveedor, respectivamente, que será el mantenimiento de la relación para la ejecución del presente servicio. Los firmantes, garantizan la exactitud y veracidad de los datos facilitados, comprometiéndose a comunicar a la contra parte cualquier modificación.

Si cualquiera de los firmantes facilita datos de terceras personas, garantiza a la contra parte haber informado a ésta de los términos y condiciones del tratamiento de los datos.

Para el solicitar el ejercicio de derecho por parte de los interesados, se detalla a continuación, los canales habilitados por cada una de las partes:

- Cliente: a través del siguiente canal: [identificar correo electrónico, teléfono…etc.], identificando en el asunto [identificar].
- Proveedor: a través del siguiente canal: [identificar correo electrónico, teléfono…etc.], identificando en el asunto [identificar].

8.2 Formalización del Acuerdo de Encargado de Tratamiento

Cuando el Proveedor actúe como encargado del tratamiento respecto a los datos personales proporcionados por el Cliente, ambas partes suscribirán un Acuerdo de Encargado de Tratamiento que incluya las instrucciones específicas del Cliente, conforme al artículo 28 del RGPD.

9. Responsabilidad y Suspensión del Servicio

9.1 Responsabilidad en Caso de Errores Operativos

En caso de que la IA produzca resultados erróneos que causen perjuicios, el Proveedor colaborará para mitigar los daños y realizar ajustes al sistema. El Proveedor no será responsable por daños indirectos, salvo en casos de negligencia grave.

9.2 Suspensión Temporal del Servicio

El Proveedor se reserva el derecho de suspender temporalmente el servicio de IA en caso de riesgos críticos que comprometan la seguridad o funcionalidad del sistema, notificando al Cliente de inmediato y tomando las medidas correctivas necesarias.

10. Confidencialidad

El Proveedor garantiza al Cliente la confidencialidad de toda la información (sea o no clasificada como tal) que, con motivo de la prestación del servicio o por otro medio pueda llegar a conocer, incluyendo cualesquiera secretos comerciales. Dicho deber de confidencialidad subsistirá incluso una vez finalizada la prestación de servicios.

Anexo A. Medidas para garantizar la transparencia

Facilítese aquí una descripción de las medidas técnicas y organizativas que debe adoptar el proveedor para garantizar la transparencia de conformidad con la cláusula 4.1.

Anexo B. Medidas para garantizar la supervisión humana

Facilítese aquí una descripción de las medidas técnicas y organizativas que debe adoptar el proveedor para garantizar la supervisión humana de conformidad con la cláusula 4.2.

Anexo C: Documentación técnica

La documentación técnica incluirá como mínimo la siguiente información aplicable al sistema IA:

1. Una descripción general del sistema de IA que incluya:
   1.1. su finalidad prevista, el nombre del proveedor, la fecha y la versión del sistema;
   1.2. la naturaleza de los datos que puedan o vayan a ser tratados por el sistema y, en el caso de los datos personales, las categorías de personas físicas y grupos que puedan o vayan a verse afectados;
   1.3. cómo el sistema de IA puede interactuar o utilizarse para interactuar con los soportes físicos o el software que no formen parte del propio sistema de IA, cuando proceda;
   1.4. las versiones de software y de firmware pertinentes y cualquier requisito relativo a la actualización de las versiones;
   1.5. la descripción de todas las formas en que el sistema de IA se ha introducido en el mercado o puesto en servicio;
   1.6. la descripción del soporte físico en el que se prevé que opere el sistema de IA;
   1.7. en caso de que el sistema de IA consista en un componente de productos, fotografías o ilustraciones de las características exteriores, el marcado y la configuración interna de dichos productos;
   1.8. una descripción detallada y fácilmente inteligible de los principales objetivos de optimización del sistema;
   1.9. una descripción detallada y fácilmente inteligible de los resultados esperados del sistema y de la calidad prevista de estos;
   1.10. instrucciones detalladas y fácilmente inteligibles para la interpretación de los resultados del sistema;
   1.11. ejemplos de situaciones en las que no debe utilizarse el sistema.

2. Una descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, en particular:
   2.1. los métodos y las medidas adoptados para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas previamente entrenados facilitados por terceros y cómo los ha utilizado, integrado o modificado el proveedor, especialmente una descripción de cualesquiera licencias u otros acuerdos contractuales relativos a dichos datos de entrada de terceros;
   2.2. las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA y de los algoritmos; las opciones clave de diseño, en particular, la justificación lógica y las hipótesis planteadas, también con respecto a las personas o grupos de personas en relación con los que se prevé utilizar el sistema; las principales opciones de clasificación; aquello que el sistema está diseñado para optimizar y la pertinencia de los diversos parámetros; las decisiones adoptadas acerca de cualquier posible efecto de compensación con respecto a las soluciones técnicas aplicadas para dar cumplimiento a los requisitos establecidos en las presentes cláusulas;
   2.3. la descripción de la arquitectura del sistema que detalle cómo se incorporan o enriquecen mutuamente los componentes del software, y cómo se integran en el procesamiento general; los recursos informáticos utilizados para el desarrollo, el entrenamiento, la prueba y la validación del sistema de IA;

2.4. cuando proceda, los requisitos sobre datos en forma de fichas técnicas que describan las metodologías y técnicas de entrenamiento, así como los conjuntos de datos de entrenamiento utilizados, incluida la información acerca de la procedencia de dichos conjuntos de datos, su alcance y sus características principales; cómo se obtuvieron y seleccionaron los datos; los procedimientos de etiquetado (p. ej., para el aprendizaje supervisado), las metodologías de depuración de datos (p. ej., la detección de valores atípicos);
2.5. en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su funcionamiento, junto con toda la información pertinente relativa a las soluciones técnicas adoptadas con el objetivo de garantizar que el sistema de IA cumpla de forma continua los requisitos pertinentes establecidos en estas cláusulas;
2.6. los procedimientos de validación y prueba utilizados, incluida la información acerca de los datos de validación y prueba empleados y sus características principales; los parámetros utilizados para medir la precisión, la solidez, la ciberseguridad y el cumplimiento de otros requisitos pertinentes dispuestos en estas cláusulas, así como los efectos potencialmente discriminatorios; los archivos de registro de las pruebas y todos los informes de las pruebas fechados y firmados por las personas responsables, en particular en lo que respecta a los cambios predeterminados a que se refiere la cláusula 2, epígrafe 5;
2.7. las medidas de ciberseguridad adoptadas.

Información detallada acerca del seguimiento, el funcionamiento y el control del sistema de IA, en particular con respecto a: sus capacidades y limitaciones de funcionamiento, incluidos los niveles de precisión para las personas o grupos de personas específicos con respecto a los que se prevé utilizar el sistema y el nivel de precisión general esperado en relación con su finalidad prevista; los resultados no deseados previsibles y las fuentes de riesgo para la salud y la seguridad, los derechos fundamentales y la discriminación en vista de la finalidad prevista del sistema de IA.

3. Una descripción detallada del sistema de gestión de riesgos con arreglo a la cláusula 2.
4. Una descripción de todo cambio pertinente que introduzca el proveedor en el sistema a lo largo de su ciclo de vida.

Anexo D: Instrucciones de uso

Las instrucciones de uso incluirán como mínimo la siguiente información, aplicable al sistema de IA:

1. la identidad y los datos de contacto del proveedor y, en su caso, de sus representantes autorizados;
2. las características, capacidades y limitaciones del funcionamiento del sistema de IA, especialmente y cuando corresponda:
   2.1. la finalidad prevista;
   2.2. el nivel de precisión, solidez y ciberseguridad mencionado en la cláusula 8 con respecto al cual se haya probado y validado el sistema de IA y que puede esperarse de este, así como las circunstancias claramente conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado;
   2.3. cualquier circunstancia claramente conocida o previsible, asociada a la utilización del sistema de IA conforme a su finalidad prevista o en condiciones de un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales;
   2.4. el grado en que el sistema de IA puede explicar las decisiones que toma;
   2.5. su funcionamiento en relación con las personas o los grupos de personas con respecto a los que se pretenda utilizar el sistema;
   2.6. la información pertinente acerca de las acciones de los usuarios que puedan influir en el funcionamiento del sistema, especialmente el tipo o la calidad de los datos de entrada o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA;
3. los cambios en el sistema de IA y su funcionamiento predeterminados por el proveedor, en su caso;
4. las medidas de vigilancia humana a que se hace referencia en la cláusula 7, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida del sistema de IA por parte del organismo público;
5. la vida útil prevista del sistema de IA, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a la actualización del software;
6. una descripción de los mecanismos incluidos en el sistema de IA que permiten a los usuarios recopilar, almacenar e interpretar adecuadamente los archivos de registro.

7. PLAN DE IMPLANTACIÓN DE LAS CLAUSULAS DE INTELIGENCIA ARTIFICIAL

El objetivo de disponer de un plan de implantación es proporcionar una guía detallada sobre los pasos necesarios para implantar las cláusulas de IA propuestas en esta guía. Al seguir este plan, las partes contratantes podrán garantizar una mayor seguridad jurídica, transparencia y confianza en sus acuerdos. Además, se garantizará el cumplimiento normativo y de los principios y requisitos esenciales de la IA, como la equidad, la transparencia, la responsabilidad y la protección de los derechos fundamentales. Este plan no solo aborda los aspectos legales, sino que también tiene en cuenta las implicaciones éticas y sociales del uso de la IA, y ofrece un enfoque integral para la gestión de riesgos y la promoción de prácticas responsables en el desarrollo y la implementación de sistemas de IA. Las fases del plan incluyen el análisis de tipologías de sistemas y servicios de IA, la selección de cláusulas contractuales adecuadas, la redacción e integración de las cláusulas, la revisión y validación finales, y la evaluación y mejora continua.

I Fases del plan

El plan se divide en las siguientes fases, cada una de las cuales es necesaria para garantizar una implementación efectiva y responsable de las cláusulas de IA:

1. ANÁLISIS DE TIPOLOGÍAS DE SISTEMAS Y SERVICIOS DE IA: esta fase inicial es fundamental para comprender el alcance y las características de los sistemas y servicios de IA que se pretenden contratar o proporcionar. Consiste en identificar y clasificar dichos sistemas según su nivel de riesgo, su forma de aprovisionamiento, sus componentes y su ciclo de vida. Para ello, se empleará un enfoque esquemático y un desglose de las tipologías más relevantes.

Este análisis permitirá determinar qué sistemas requieren una atención especial y qué medidas específicas deben implementarse para mitigar los riesgos asociados. Se tendrán en cuenta las actividades que deben regularse contractualmente en función del tipo de sistema o servicio de IA. Asimismo, otros factores a considerar para priorizar la revisión del contrato y la modificación de cláusulas es el estado actual de la relación comercial con el proveedor: es necesario contar con información sobre la duración del contrato, los períodos de renovación y la incorporación de nuevos productos o servicios que requieran una ampliación contractual. Estos aspectos deben consultarse con la persona o el área responsable del contrato que dispongan de dicha información. Este inventario garantizará que todas las actividades críticas estén debidamente cubiertas por las cláusulas contractuales.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

1.1 Identificación de sistemas y servicios de IA: identificación de los diferentes sistemas y servicios de IA que se pretenden contratar o proporcionar.
1.2 Clasificación según el nivel de riesgo: clasificar los sistemas y servicios de IA según su nivel de riesgo, teniendo en cuenta factores como el impacto potencial en la salud, la seguridad y los derechos fundamentales de las personas.
1.3 Análisis del ciclo de vida: análisis del ciclo de vida de los sistemas y servicios de IA, desde su desarrollo y despliegue hasta su operación y desmantelamiento.
1.4 Evaluación de componentes: evaluar los componentes de los sistemas y servicios de IA, incluidos el hardware, el software y los datos, para identificar posibles riesgos y medidas de mitigación.

2. SELECCIÓN DE CLÁUSULAS CONTRACTUALES DE IA: en esta fase, se seleccionarán las cláusulas contractuales de IA más adecuadas para cada tipología de sistema o servicio de IA, teniendo en cuenta el nivel de riesgo, las obligaciones y los derechos de las partes involucradas. Esta guía incluye textos modulados que permiten adaptar la cláusula a diferentes supuestos específicos. Estas cláusulas abordan aspectos cruciales como la documentación técnica, la transparencia, la evaluación de conformidad, la responsabilidad y la protección de datos. También se tendrán en cuenta los requisitos y las buenas prácticas para la gestión de riesgos, la calidad de los datos, la prevención de sesgos, la propiedad intelectual y la vigilancia poscomercialización, entre otros aspectos.

La selección cuidadosa de estas cláusulas garantiza que se aborden todos los aspectos relevantes y que las partes contratantes comprendan claramente sus derechos y responsabilidades.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

- **2.1** Revisión de documentos de referencia: revisión de los documentos de referencia para identificar las cláusulas contractuales relevantes.
- **2.2** Redacción y adaptación de cláusulas genéricas: adaptación de las cláusulas genéricas a las necesidades específicas de cada contrato mediante la utilización de textos modulados cuando sea necesario.

3. REDACCIÓN E INTEGRACIÓN DE LAS CLÁUSULAS CONTRACTUALES DE IA: en esta fase, se procederá a redactar e integrar en el contrato principal o en un anexo específico, según el caso, las cláusulas contractuales de IA seleccionadas. Para ello, se seguirán las recomendaciones y los modelos de cláusulas de IA para diferentes sectores y escenarios.

La redacción de las cláusulas debe ser clara y precisa para que todas las partes comprendan sus derechos y obligaciones. La integración de estas cláusulas en el contrato principal o en un anexo específico debe realizarse de manera coherente, garantizando que no haya contradicciones con otras disposiciones contractuales y que se mantenga la integridad del acuerdo.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

- **3.1** Revisión de coherencia: revisar las cláusulas redactadas para garantizar que no haya contradicciones con otras disposiciones contractuales.
- **3.2** Integración en el contrato: integrar las cláusulas redactadas en el contrato principal o en un anexo específico, según corresponda.

4. REVISIÓN Y VALIDACIÓN DE LAS CLÁUSULAS CONTRACTUALES DE IA: esta fase es necesaria para garantizar que las cláusulas redactadas e integradas sean coherentes, claras, legales y se ajusten a las expectativas y necesidades de las partes. Para ello, los equipos jurídicos y técnicos de cada parte realizarán una verificación interna exhaustiva. Dicha verificación incluirá una revisión detallada de cada cláusula para identificar posibles inconsistencias, ambigüedades o problemas legales. Además, se negociará entre las partes para llegar a un acuerdo mutuo sobre las cláusulas definitivas. Si es necesario o conveniente, se podrá recurrir a la asistencia de expertos externos o de organismos notificados para obtener una opinión independiente y garantizar que las cláusulas cumplen con todas las normativas aplicables.

La revisión y validación de las cláusulas es un paso esencial para garantizar que el contrato final sea sólido y que todas las partes estén protegidas y satisfechas con los términos acordados.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

- **4.1** Verificación interna: realizar una verificación interna exhaustiva por parte de los equipos jurídicos y técnicos de cada parte para identificar posibles inconsistencias, ambigüedades o problemas legales.
- **4.2** Negociación entre las partes: negociación entre las partes para llegar a un acuerdo mutuo sobre las cláusulas definitivas.
- **4.3** Asistencia de expertos externos: recurrir a la asistencia de expertos externos o de organismos notificados para obtener una opinión independiente y asegurar que las cláusulas cumplen con todas las normativas aplicables.
- **4.4** Validación final: validar las cláusulas contractuales con todas las partes involucradas para asegurar su conformidad y aceptación.
- **4.5** Alfabetización: para garantizar una implementación efectiva de las cláusulas de IA, todas las partes involucradas deben comprender plenamente sus derechos y responsabilidades. Para ello, es importante implementar programas de capacitación y concienciación para los empleados, proveedores y otros grupos de interés.

5. REVISIÓN PERIÓDICA DEL CUMPLIMIENTO Y ACTUALIZACIÓN DE LAS CLÁUSULAS: esta fase garantizará que las cláusulas contractuales de IA sigan siendo relevantes y efectivas a medida que evolucionan los servicios o el contexto en el que se utilizan. Incluye la evaluación continua del cumplimiento de las cláusulas, la recopilación de opiniones de las partes involucradas y la actualización de las cláusulas para reflejar cambios en la normativa, la tecnología o las mejores prácticas.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

- **5.1** Monitorización continua: establecer mecanismos de supervisión para garantizar el cumplimiento continuo de las cláusulas contractuales de IA como, por ejemplo, la obligación de realizar auditorías periódicas, revisiones de rendimiento y sistemas de informes para identificar y abordar cualquier incumplimiento o problema que surja.
- **5.2** Recopilación de feedback: recopilar la opinión de las partes involucradas para identificar posibles problemas y áreas de mejora.
- **5.3** Revisión de incidentes o eventualidades: revisión de incidentes y problemas surgidos para ajustar las cláusulas según sea necesario, así como la revisión cuando acontezcan otros eventos que afecten los sistemas o servicios de IA.
- **5.4** Actualización de cláusulas: actualizar las cláusulas para reflejar cambios en la normativa, la tecnología o las mejores prácticas.
- **5.5** Documentación de lecciones aprendidas: documentar lecciones aprendidas y estudios de caso para informar sobre futuras implementaciones.

6. PLAN DE ADAPTACIÓN DE CONTRATOS EXISTENTES: este apartado constituye un paso adicional a los anteriores y está dirigido especialmente a aquellas organizaciones que, antes de la entrada en aplicación del Reglamento (UE) de Inteligencia Artificial, ya trabajaban con proveedores que utilizaban tecnología de IA. La adaptación de los contratos existentes y la integración de las nuevas cláusulas de IA en los procesos de contratación son fundamentales para garantizar la coherencia con el marco regulatorio y contractual establecido, y para asegurar que los acuerdos previos se alineen con las nuevas exigencias.

Dado que muchos contratos vigentes no incluían disposiciones específicas sobre IA, es necesario diseñar un proceso de actualización que permita implementar esta tecnología de manera estructurada y priorizada, en función del nivel de riesgo de los sistemas y servicios involucrados. Para ello, es preciso identificar los proveedores afectados, evaluar los ajustes necesarios y comunicarse de manera efectiva con los responsables de las distintas áreas para coordinar la implementación de los cambios.

Las acciones específicas que se llevarán a cabo en esta fase son las siguientes:

- **6.1** Identificación de contratos vigentes: realización de un inventario de contratos con proveedores que emplean IA para determinar cuáles requieren adaptación.
- **6.2** Clasificación por nivel de riesgo: analizar el impacto y la criticidad de cada sistema o servicio de IA para establecer prioridades en la actualización contractual.
- **6.3** Revisión y modificación de cláusulas: actualización de los contratos existentes para incorporar las disposiciones necesarias que garanticen el cumplimiento del Reglamento de IA.
- **6.4** Comunicación con las partes involucradas: informar a los responsables de productos y servicios en la organización sobre los cambios necesarios y coordinar la validación del plan de acción.
- **6.5** Integración de cláusulas en nuevas contrataciones: se asegurará de que los responsables de productos y servicios en la organización dispongan del clausulado actualizado y lo apliquen en los nuevos acuerdos.
- **6.6** Supervisión y seguimiento: establecer mecanismos para evaluar el cumplimiento de las cláusulas adaptadas y realizar ajustes cuando sea necesario.

II Conclusión

La implementación de cláusulas contractuales de IA es un proceso complejo pero necesario para garantizar el uso responsable y ético de la IA. Este plan proporciona una guía para cada fase del proceso, desde el análisis inicial de tipologías de sistemas y servicios de IA, la selección de cláusulas contractuales adecuadas, la redacción e integración de las cláusulas, hasta la revisión y validación finales, y la evaluación y mejora continua.

Al seguir este plan, las organizaciones pueden garantizar que sus contratos de IA sean sólidos, claros y conformes con todas las normativas aplicables. Además, la capacitación y el seguimiento continuo fomentan una cultura de cumplimiento y responsabilidad. En última instancia, un enfoque bien planificado y ejecutado para la implementación de cláusulas de IA puede proporcionar mayor seguridad jurídica, transparencia y confianza a todas las partes involucradas, y promover el uso beneficioso y ético de la IA.

Asimismo, la correcta adaptación de los contratos existentes y la integración de las nuevas cláusulas en la contratación de proveedores garantizarán una transición ordenada y alineada con las exigencias regulatorias, minimizando riesgos y fortaleciendo la seguridad jurídica en el uso de la inteligencia artificial.

8. OTRAS NORMATIVAS A CONSIDERAR

La consideración de los aspectos normativos a la hora de "construir" un instrumento contractual cuyo objeto verse sobre Inteligencia artificial se focaliza lógicamente en las regulaciones específicas sobre la materia.

Sin negar, en absoluto, que ese enfoque es fundamental, la construcción de un marco contractual sobre la adquisición, desarrollo, uso, etc., de sistemas de Inteligencia Artificial no debe olvidar ni dejar de lado otras Normativas que serán muy relevantes, aunque no sean específicas de Inteligencia Artificial.

Algunas de estas Normativas han sido incorporadas, de uno u otro modo, en el Reglamento de Inteligencia Artificial, si bien en este apartado se pretende ir más allá del contenido de ese Reglamento. En concreto, se pretende proponer una relación, necesariamente no exhaustiva, de esas otras Normativas a considerar cuando enfrentamos la configuración de un instrumento contractual cuyo objeto, dicho en sentido amplio, se refiere a Inteligencia Artificial.

Protección de datos personales

Cuando hablamos de IA, hay una cierta tendencia a considerar que, de manera automática, van a surgir implicaciones en materia de Protección de datos personales, entre otras razones por las referencias a dicha materia contenidas en la propia Normativa sobre Inteligencia artificial. Obviamente, no siempre (aunque sí muchas veces) va a ser así.

Ahora bien, el hecho de que no siempre que hablemos de IA van a estar implicados datos personales no debería evitar que siempre que hablemos de la articulación contractual de la IA tengamos en cuenta las necesarias previsiones en materia de Protección de datos personales. Es por ello que en el anterior apartado sobre "Identificación de riesgos en el uso de Sistemas de IA y Gestión de proveedores" haya un subapartado sobre "Riesgos de Privacidad", relativo, como se indica al inicio del mismo, a "La identificación de riesgos de privacidad asociado al uso de sistemas de inteligencia artificial…".

Ahora bien, conviene que la Protección de datos personales sea objeto de un análisis independiente, desvinculado de que el objeto del contrato puedan ser determinados sistemas de Inteligencia Artificial, puesto que hay que valorar si los tratamientos de datos personales relevantes se producen con relación no tanto a los sistemas de IA, sino con relación a otros elementos relacionados pero diferentes (servicio IT, servicios externalizados, formación, etc.).

En consecuencia, la primera precaución contractual será, precisamente, analizar si para la ejecución del contrato van a ser necesario realizar, en mayor o medida, un tratamiento de datos personales. Inclusive, por precaución y para evitar sorpresas, puede incluirse una regulación sobre el tratamiento de datos personales, porque concurra o porque pueda concurrir.

Esto nos llevará necesariamente a la necesidad de reflejar en el contrato los acuerdos para dar cumplimiento al Reglamento europeo de Protección de datos [Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)], en materias tales como Encargo de tratamiento, Registro de Actividades, Seguridad, Privacidad desde el diseño, Transferencia internacional, ect.

Asimismo, se debería valorar la oportunidad de incorporar a la regulación contractual aspectos derivados de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, como los que

pudieran ser relativos a consentimiento de los menores de edad, bloqueo de datos u operaciones mercantiles (supuesto este último que puede ser oportuno prever a futuro, dado el constante movimiento de los operadores del sector de la IA).

Propiedad intelectual e industrial

Desde el punto de vista de Propiedad intelectual, lo primero a tener en cuenta es que el contrato debe regular su licenciamiento como software, condición atribuible en muchos casos. Es decir, se debe articular adecuadamente la cesión de los derechos de Propiedad intelectual para que la adquisición de la herramienta tecnológica basada, de manera más o menos intensa, en IA, nos permita su uso del modo, con las capacidades y con la extensión (temporal y geográfica) que teníamos prevista.

Lógicamente, particularmente en el caso de la IA Generativa, puede haber importantes cuestiones a tener en cuenta con relación a la Propiedad intelectual aplicable a datos de entrenamiento, inputs (no solo prompts, sino más aun materiales o contenidos gráficos, videográficos, etc., sobre los que le pedimos a la IA que trabaje) y los outputs. En muchos casos, la respuesta a la pregunta sobre por qué y para qué queremos una IA se convierte, en su vertiente contractual, en una pregunta sobré como articulamos la Propiedad Intelectual en la relación entre las partes contratantes, para que se puedan lograr los objetivos esperados y no se generen limitaciones y, en último término, frustraciones, cuando hagamos uso de esa IA.

Cuando la IA contratada está incorporada a un dispositivo, producto o procedimiento, hay que valorar la necesidad de incorporar al contrato aspectos sobre existencia de patentes o patentabilidad de ese elemento cuando puede ser el resultado del contrato. Por otro lado, y al igual que ocurre con la Propiedad Intelectual, dentro de la Propiedad Industrial y en el caso concreto de las patentes, si bien la Normativa se orienta a que el inventor debe ser una persona física, puede resultar de interés incorporar al contrato una regulación explícita sobre quién se considera inventor en caso de la generación de un resultado patentable mediante un procedimiento que otorgue un protagonismo principal o tendencialmente único a la IA contratada.

Ciberseguridad y Seguridad de la información

En el contexto de un contrato con un proveedor de inteligencia artificial debe incorporar compromisos en cuanto a Confidencialidad, estableciendo cláusulas que obliguen al proveedor a mantener la confidencialidad de toda la información y datos a los que tenga acceso, y Protección de Datos, en el sentido ya expresado de asegurar que el proveedor cumpla con el Reglamento General de Protección de Datos (RGPD), incluyendo la implementación de medidas técnicas y organizativas adecuadas.

Ahora bien, este apartado específico se centra de manera específica en Ciberseguridad y Seguridad de la Información, referido a definir las medidas de seguridad que el proveedor debe implementar para proteger la integridad, disponibilidad y confidencialidad de los datos. En este mismo sentido, pueden incluirse cláusulas sobre:

- Seguridad de la Información: El contrato debe especificar las medidas de seguridad, como cifrado de datos, control de acceso y autenticación multifactor. También debe incluir políticas de gestión de riesgos y formación continua para el personal.
- Brechas de Seguridad: Definir un procedimiento para la detección y notificación de brechas, incluyendo un plazo máximo de notificación (por ejemplo, 24 horas). Detallar las responsabilidades del proveedor en la investigación y mitigación de la brecha.
- Respuesta a Incidentes: Establecer un plan de respuesta que incluya la identificación, contención, erradicación y recuperación del incidente. Incluir la obligación de realizar un análisis post-incidente para identificar causas y mejorar las medidas de seguridad.

Además, puede ser especialmente interesante introducir cláusulas relativas a la realización de auditorías de seguridad, como instrumento fundamental para garantizar el cumplimiento de las medidas de ciberseguridad acordadas. Estas cláusulas deberán detallar los aspectos clave como (i) Periodicidad: Establecer la frecuencia de las auditorías, que pueden ser anuales o semestrales, dependiendo del nivel de riesgo; (ii) Alcance: Definir qué sistemas, procesos y datos serán auditados para asegurar una cobertura completa; (iii) Acceso a Información: Asegurar que el auditor tenga acceso a toda la información necesaria para realizar una evaluación exhaustiva; (iv) Informes de Auditoría: El proveedor debe proporcionar informes detallados de los resultados, incluyendo hallazgos, recomendaciones y acciones correctivas; (v) Derecho a Auditorías Externas: Permitir la contratación

de auditores externos independientes para garantizar imparcialidad; o (vi) Seguimiento: Establecer un proceso para el seguimiento y verificación de la implementación de las recomendaciones de auditoría. Estos elementos ayudan a mantener la integridad y seguridad del sistema.

Adicionalmente y en función de circunstancias concretas de la relación entre el proveedor del sistemas de inteligencia artificial y la entidad que lo contrata, puede ser necesario introducir cláusulas específicas en materia de ciberseguridad y seguridad de la información derivadas del Reglamento DORA [Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011 (Texto pertinente a efectos del EEE)], del Reglamento de Ciberresiliencia [Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828] cuando sea exigible o la Normativa de transposición de la Directiva NIS 2 [Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)].

Laboral

Desde el punto de vista Laboral, podríamos distinguir dos ámbitos materiales que pueden conllevar la incorporación de contenidos específicos en el instrumento contractual cuyo objeto verse sobre Inteligencia artificial.

Por un lado, tenemos las cuestiones relativas a:

- **Impacto en el Empleo:** Es crucial evaluar cómo el sistema puede modificar las funciones laborales, potencialmente reduciendo o transformando puestos de trabajo. El contrato debe incluir un análisis de impacto laboral y medidas para mitigar efectos negativos.

- **Formación y Capacitación:** El proveedor debe comprometerse a ofrecer formación adecuada a los empleados para el uso eficiente y seguro del sistema, asegurando que el personal esté preparado para adaptarse al uso de la Inteligencia Artificial.

- **Seguridad y Salud Laboral:** El sistema no debe comprometer la seguridad y salud de los trabajadores. El contrato debe incluir evaluaciones de riesgos y medidas preventivas.

Por otro lado, están aquellos contenidos contractuales vinculados al impacto que pueda tener en la intimidad del empleado la implementación de un determinado sistema de Inteligencia Artificial y el aseguramiento de que ese impacto no entra en conflicto con lo dispuesto sobre "Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral" en el Artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En este sentido, la aplicación de la Inteligencia Artificial a fines de control del empleado, mejora de la productividad, supervisión de actividades, etc., debe incorporarse al contrato de modo que se respeten los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente, inclusive con la participación de los representantes de los trabajadores.

Secretos empresariales

En España, la normativa sobre secretos empresariales está regulada por la Ley 1/2019, de 20 de febrero, de Secretos Empresariales. Esta ley protege la información empresarial que no es generalmente conocida y que tiene valor comercial por ser secreta. Establece medidas para proteger dicha información contra la obtención, utilización y divulgación ilícitas, y define qué constituye un secreto empresarial y las acciones legales disponibles en caso de infracción.

Por tanto, es importante que las empresas implementen medidas de protección adecuadas para salvaguardar sus secretos empresariales, lo cual puede ser especialmente importante en la contratación de sistemas de Inteligencia Artificial que pueden incidir, accede, procesar, etc., información corporativa de máxima sensibilidad y que va a encajar de manera plena en el concepto de secreto empresarial.

Por ello, en el contrato se deben incorporar aquellas previsiones y compromisos dirigidos a implementar medidas razonables para proteger los secretos empresariales implicados en el uso de secretos empresariales. Estas medidas pueden incluir:

1. Restricción de acceso a la información confidencial solo a personal autorizado.
2. Uso de acuerdos de confidencialidad con empleados y socios comerciales.
3. Implementación de medidas de seguridad física y digital, como contraseñas y cifrado.
4. Capacitación a los empleados sobre la importancia de la confidencialidad.
5. Monitoreo y auditoría regular de las prácticas de seguridad.

Competencia

La normativa sobre competencia en España se centra en garantizar la libre competencia y evitar prácticas anticompetitivas. La Ley de Defensa de la Competencia (Ley 15/2007) es la principal regulación, prohibiendo acuerdos colusorios, abuso de posición dominante y concentraciones que puedan restringir la competencia. La Comisión Nacional de los Mercados y la Competencia (CNMC) es el organismo encargado de supervisar y aplicar estas normas. Además, las normativas de la Unión Europea también son aplicables en España, complementando la legislación nacional para asegurar un mercado competitivo.

Por tanto, en un contrato de inteligencia artificial, las cláusulas sobre competencia deben incluir, entre otras cuestiones:

- No Competencia: Restringir el uso de la tecnología para desarrollar productos o servicios que compitan directamente con los del proveedor.
- Confidencialidad: Proteger la información sensible y evitar su uso para fines competitivos.
- Propiedad Intelectual: Definir claramente los derechos sobre las innovaciones y desarrollos derivados.
- Exclusividad: Establecer si el uso de la tecnología es exclusivo para el cliente o si el proveedor puede ofrecerla a otros.
- Cumplimiento Normativo: Asegurar que ambas partes cumplan con las leyes de competencia aplicables.

Responsabilidad civil

La retirada por la Comisión Europea de la Directiva sobre responsabilidad civil extracontractual de la IA [Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability)] no debería distraer la necesaria atención que se debería prestar a la regulación sobre responsabilidad civil con relación al sistema de Inteligencia Artificial provisionado en el contrato que lo regule.

El proveedor del sistema de Inteligencia Artificial debe asumir contractualmente que lo provisiona bajo su única y exclusiva responsabilidad, y responderá frente a su cliente de su correcta provisión.

Por ello, se recogerá que el proveedor será responsable de cuantos daños y perjuicios puedan irrogarse directa o indirectamente al cliente, a sus empleados, administradores, directivos o representantes, o a cualquier tercero. Asimismo, el proveedor asumirá, exclusivamente y por entero, las responsabilidades que se puedan derivar en caso de insuficiencia o imperfección de los materiales, equipos, útiles, sistemas, métodos y medios auxiliares utilizados para la prestación de su servicio.

El proveedor se deberá comprometer a realizar sus mayores esfuerzos a fin de evitar o, en su caso, mitigar los efectos dañosos y perjudiciales que pudieran derivarse para su cliente de la provisión de la Inteligencia Artificial con arreglo al Contrato, así como a colaborar con él en la defensa de sus intereses en el caso de que se presente cualquier reclamación o se inicie o incoe cualquier procedimiento judicial o administrativo por esta causa.

Y a tal efecto, el proveedor deberá disponer de una póliza de responsabilidad civil con suficientes coberturas, que podrá ser anexada al contrato o aportada posteriormente a petición del cliente.

Consideraciones sectoriales, el ejemplo del sector salud.

A los efectos del presente documento y ya por una mera cuestión de extensión, no es posible recoger las múltiples cuestiones que podrían tenerse en cuenta en la contratación de un sistema de Inteligencia Artificial teniendo en cuanto determinados sectores a los que pueden pertenecer las entidades que los contraten.

Por ello, se recoge, a modo de muestra, algunas cuestiones a tener en cuenta y que pueden conllevar contenidos contractuales concretos cuando quien adquiere el sistema de Inteligencia Artificial pertenece al Sector de Salud. En este caso, podríamos hablar, por ejemplo, de lo siguiente:

- Ante todo, está el impacto del tratamiento de salud a efectos de la clasificación de los sistemas de Inteligencia Artificial según su nivel de riesgo para garantizar una supervisión proporcional. En este sentido, cualquier sistema de Inteligencia Artificial que conlleve el procesamiento de datos de salud va a ser, al menos, un Sistema de Riesgo alto, con lo que ello conlleva en cuanto a:
  - » Supervisión humana constante.
  - » Datos de calidad y representativos.
  - » Mecanismos de transparencia.

  Así, por ejemplo, un sistema de detección de tumores en imágenes médicas debe permitir a los médicos auditar y validar sus resultados antes de tomar decisiones clínicas.

- Por otro lado, el despliegue de un sistema de Inteligencia Artificial que vaya a procesar datos de salud se debe articular mediante compromisos contractuales claros en cuanto a quiénes van a acceder a tales datos. Se ha de tener en cuenta que la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, establece que el acceso a la historia clínica está limitado a los profesionales sanitarios que participan en el diagnóstico o tratamiento del paciente. También se establece que el personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones

- Obviamente, el paciente tiene derecho a acceder a su propia historia clínica, salvo excepciones legales. También se permite el acceso a terceros con autorización expresa del paciente o por mandato legal. En definitiva, la Ley garantiza la confidencialidad de la información contenida en la historia clínica, estableciendo medidas para protegerla contra accesos no autorizados y asegurando que solo se utilice para los fines previstos.

- Como último ejemplo, hay que tener en cuenta que el Reglamento de Productos Sanitarios [Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo] regula los dispositivos médicos, inclusive los que incorporan IA, exigiendo validaciones exhaustivas para su aprobación. Sus principales disposiciones incluyen:

  - » Validación clínica: Demostrar que los dispositivos funcionan correctamente en condiciones reales. Un ejemplo sería un sistema que monitoriza a pacientes con enfermedades cardiovasculares, que debe detectar anomalías con alta precisión.
  - » Supervisión del ciclo de vida: Garantizar que las actualizaciones de software no afecten negativamente al rendimiento del dispositivo.
  - » Cumplimiento de estándares internacionales: En concreto, aquellos que certifican la calidad y seguridad de los sistemas.

Cláusula de cierre

Como señalábamos al inicio de este apartado, la relación de Normativas que se ha expuesto no es exhaustiva, en tanto que puede haber otras Normativas a considerar en base a variables como sector de actividad o ubicación geográfica de alguna de las Partes contratantes, circunstancias del caso concreto, etc.

En este sentido, conviene incorporar al contrato sobre Inteligencia Artificial una cláusula, específica a tal fin o no, que indique que habrán de tenerse en cuenta y serán de obligatorio cumplimiento para todas las Partes todas aquellas Normativas, de cualquier tipo, que resulten aplicables al objeto del Contrato mientras se mantenga la duración prevista para el mismo. Esto incluirá, obviamente, tanto normativas en vigor en el momento de la firma del contrato, como aquellas otras que se aprueben y/o entren en vigor con posterioridad a dicho momento y mientras mantenga su vigencia.

CONTACTA CON NOSOTROS

Si estás interesado/a en colaborar con nosotros o necesitas más información sobre nuestros proyectos, escríbenos a: proyectos@ismsforum.es

ISMS Forum Spain
C. del Segre, 29, 1ºB
28002 Madrid

T. +34 915 63 50 62
E. proyectos@ismsforum.es
www.ismsforum.es