El consenso de Beijín sobre el uso de la IA en la educación. Aspectos fundamentales del acuerdo

Beijing consensu son artificial intelligence and education

UNESCO. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

CONTEXTO Y PLAZOS

El Diario Oficial de la Unión Europea (DOUE) del 12 de julio recoge la publicación del **Reglamento UE 2024/1689** del Parlamento Europeo y del Consejo, de 13 de junio de 2024, en el que se establece el **marco europeo de responsabilidades para empresas proveedoras y empresas usuarias de tecnologías de inteligencia artificial,** en función de sus riesgos potenciales en diferentes ámbitos, entre ellos el laboral, y su nivel de impacto.

Los **valores de la UE** de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho, así como de los derechos fundamentales de no discriminación, la protección de datos e intimidad y los derechos del niño, inspiran la letra de esta nueva norma, cuyo **objetivo es garantizar un uso ético y responsable de la inteligencia articificial**. **Ambos conceptos se traducen en obligaciones y responsabilidades** concretas para todos los actores implicados en la producción, comercialización, representación, uso y vigilancia de los sistemas de IA.

Los modelos de IA que operen en el ámbito del empleo, la gestión de trabajadores en las empresas y el acceso al autoempleo se definen dentro del grupo de los de alto riesgo, por lo que quedan sometidos a las obligaciones que en dicho Reglamento se contemplan.

El Reglamento entra vigor a los 20 días de su publicación en el DOUE y será aplicable (salvo determinadas disposiciones) a partir del 2 de agosto de 2026, con las siguientes excepciones:

- Prácticas prohibidas: a partir del 2 de febrero de 2025.
- Seguridad de los productos: a partir del 2 de agosto de 2025.
- Sistemas de alto riesgo: a partir del 2 de agosto de 2027.

ENFOQUE DE RIESGO BASADO EN VALORES

El texto de la norma es muy clara sobre cuál es su objetivo y cómo quiere conseguirlo:

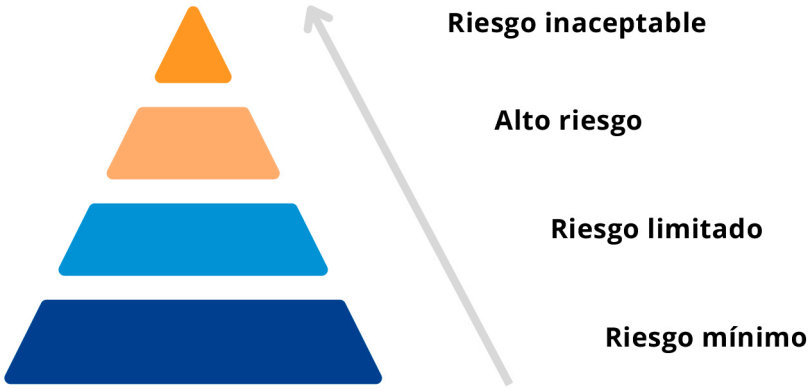
- **Objetivo:** Aumentar la confianza en la IA y garantizar que esta tecnología respete los derechos fundamentales, los valores y la seguridad de los ciudadanos de la UE.
- **Procedimiento:** Estableciendo, para ello, un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA basado en niveles de riesgos claramente definidos, con sus correspondientes obligaciones -incluidas las de transparencia- para los operadores pertinentes.

El **enfoque de riesgo que refleja el Reglamento está inspirado por las Directrices éticas para una IA fiable, de 2019,** elaboradas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisión, que concluyeron formulando siete principos éticos a los que el RIA ahora añade una definición explícita:

1. ACCIÓN Y SUPERVISIÓN HUMANA.Se entiende que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por eres humanos.
2. SOLIDEZ TÉCNICA Y SEGURIDAD. Los sistemas de IA se desarrollan y utilizan de manera que sean sólidos en caso de problemas y resilientes frente a los intentos de alterar el uso o el funcionamiento del sistema de IA para permitir su uso ilícito por terceros y reducir al mínimo los daños no deseados.
3. GESTIÓN DE LA PRIVACIDAD Y DE LOS DATOS. Los sistemas de IA se desarrollan y utilizan de conformidad con normas en materia de protección de la intimidad y de los datos, al tiempo que tratan datos que cumplen normas estrictas en términos de calidad e integridad.
4. TRANSPARENCIA. Los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos.
5. DIVERSIDAD, NO DISCRIMINACIÓN Y EQUIDAD. Los sistemas de IA se desarrollan y utilizan de un modo que incluya a diversos agentes y promueve la igualdad de acceso, la igualdad de género y la diversidad cultural, al tiempo que se evitan los efectos discriminatorios y los sesgos injustos prohibidos por el Derecho nacional o de la Unión.
6. BIENESTAR SOCIAL Y AMBIENTAL. Los sistemas de IA se desarrollan y utilizan de manera sostenible y respetuosa con el medio ambiente, así como en beneficio de todos los seres humanos.
7. RENDICIÓN DE CUENTAS. Supervisión y evaluación de los efectos a largo plazo en las personas, la sociedad y la democracia.

El enfoque de la UE con respecto a la inteligencia artificial se centra en la excelencia y la confianza, con el objetivo de impulsar la investigación y la capacidad industrial, garantizando al mismo tiempo la seguridad y los derechos

El logro de estos objetivos de confianza y excelencia, junto con los principios éticos antes mencionados, inspiran **cuatro niveles de riesgo en función del impacto que el uso de la inteligencia artificial puede tener en los derechos antes referidos**:



La pirámide de riesgo de la IA

Fuente: Estrategia Digital de la UE, 2024.

RIESGO INACEPTABLE

Los que suponen una amenaza para las personas.

- **Manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos:** por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños.
- **Puntuación o "scoring" social:** clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales;
- **Sistemas de identificación biométrica** en tiempo real y a distancia, como el reconocimiento facial.

ALTO RIESGO

Los que afectan negativamente a la seguridad o a los derechos fundamentales. Todos serán evaluados antes de su comercialización y a lo largo de su ciclo de vida. Se dividirán en dos categorías:

- **Los que se utilicen en productos sujetos a la legislación de la UE sobre seguridad de los productos,** p. ej.: juguetes, aviación, automóviles, dispositivos médicos y ascensores.
- **Los pertenecientes a ocho ámbitos específicos** que deberán registrarse en una base de datos de la UE:
- Identificación biométrica y categorización de personas físicas, gestión y explotación de infraestructuras crítica, educación y formación profesional, empleo, gestión de trabajadores y acceso al autoempleo, acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas, aplicación de la ley, gestión de la migración, el asilo y el control de fronteras, asistencia en la interpretación jurídica y aplicación de la ley.

RIESGO LIMITADO

Deben cumplir unos requisitos mínimos de transparencia que permitan a los usuarios tomar decisiones con conocimiento de causa. Ello significa que:

- **Los usuarios deben ser conscientes de cuándo están interactuando con la IA,** incluídos los chatbots y los sistemas de IA que generan o manipulan contenidos de imagen, audio o vídeo.
- tras interactuar con las aplicaciones y habiendo reconocido su naturaleza artificial, **el usuario puede decidir si desea seguir utilizándolas.**

RIESGO MÍNIMO

Todos los demás sistemas de IA pueden desarrollarse y utilizarse conforme a la normativa vigente sin otro tipo de obligaciones adicionales, pudiendo los proveedores adoptar optar voluntariamente las directrices para una IA digna de confianza y adherirse a códigos de conducta voluntarios.

IMPACTO EN LA GESTIÓN RH

El legislador europeo ha tenido especial celo en salvaguardar los valores de la UE de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho, así como de los derechos fundamentales de no discriminación, la protección de datos e intimidad y los derechos del niño. Y pone especial foco en el ámbito del empleo, un derecho fundamental que no puede verse perjudicado por una aplicación de la IA que no garantice la igualdad de trato y la equidad en la toma de decisiones relacionadas con el acceso al empleo y el desarrollo profesional, y que socave la protección de los datos personales y la intimidad.

A este respecto, el Reglamento es explícito al afirmar que "deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores y el acceso al autoempleo" y más concretamente en:

- **La contratación y la selección de personal** en lo que atañe a los anuncios de empleo y en análisis, filtrado y evaluación de los candidatos, así como a la toma de decisiones de incorporación.
- **La toma de decisiones que afecten a las condiciones de las relaciones de índole laboral:**
  - condiciones de trabajo.
  - promoción y desarrollo profesional.
  - asignación de tareas basadas en el comportamiento o las características de la persona.
  - supervisión o evaluación de las personas en el marco de las relaciones contractuales de índole laboral,
- **La rescisión de relaciones contractuales.**

Para todos ellos es importante señalar que las responsabilidades adquiridas lo son tanto para los objetivos (explícitos) del sistema de IA utilizado como para los que se pudieran derivar de su aplicación a un contexto específico (implícitos) sin ser intencional su hallazgo.

Además, y en base a los niveles de riesgo anteriormente explicitados, se prohíbe usar sistemas de IA en el ámbito laboral para inferir emociones o categorizar de manera biométrica a los trabajadores para obtener determinados datos sensibles.

1. OBLIGACIONES

De los responsables del despliegue de sistemas de IA de alto riesgo

Aunque los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño, también pueden derivarse riesgos del uso que se hace de ellos. Por ello, los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, como complemento de las obligaciones del proveedor al desarrollar el sistema de IA.

Además, se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que

no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los colectivos de personas que probablemente se vean afectados, entre los que se incluyen colectivos vulnerables.

- **Han de adoptar las medidas técnicas y organizativas adecuadas** para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen. **Encomendarán la supervisión humana a personas físicas** que tengan la competencia, la formación y la autoridad necesarias.
- **Las obligaciones anteriores no afectan a otras obligaciones** que el Derecho nacional o de la Unión imponga a los responsables del despliegue ni a su libertad para organizar sus propios recursos y actividades con el fin de poner en práctica las medidas de supervisión humana que indique el proveedor.
- **Se asegurarán de que los datos de entrada sean pertinentes y suficientemente representativos** en vista de la finalidad prevista del sistema, en la medida en que ejerza el control sobre dichos datos.
- **Vigilarán el funcionamiento del sistema** basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores.
  - **Cuando tengan motivos para considerar que utilizar el sistema conforme a sus instrucciones puede dar lugar a que ese sistema presente un riesgo informarán**, sin demora indebida, al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso de ese sistema.
  - **Cuando detecten un incidente grave** informarán inmediatamente, en primer lugar, al proveedor y, a continuación, al importador o distribuidor y a la autoridad de vigilancia del mercado pertinente.
- **Conservarán los archivos de registro** que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.
- Antes de poner en servicio o utilizar el un sistema en el lugar de trabajo, **los responsables del despliegue que sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados** de que estarán expuestos a la utilización del sistema de IA de alto riesgo. A este respecto, el Reglamento explicita que "los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas".
- Cuando proceda, **utilizarán la información facilitada para cumplir la obligación de llevar a cabo una evaluación de impacto** relativa a la protección de datos.
- **Cooperarán con las autoridades competentes** pertinentes en cualquier medida que éstas adopten.

Además, están obligados a realizar una evaluación de impacto para identificar los riesgos específicos para los derechos fundamentales de las personas o grupos de personas que puedan verse afectados, y para identificar las medidas que deben adoptarse en caso de que se materialicen estos

riesgos. Dicha evaluación se tendrá que realizar antes de desplegar el o los sistemas de IA de alto riesgo. A tal fin, la norma establece el siguiente contenido para dicha evaluación:

- **una descripción de los procesos del responsable del despliegu**e en los que se utilizará el sistema en consonancia con su finalidad prevista;
- **una descripción del período de tiempo** durante el cual se prevé utilizar cada sistema de y la frecuencia con la que está previsto utilizarlo;
- **las categorías de personas físicas y colectivos que puedan verse afectados** por su utilización en el contexto específico;
- **los riesgos de perjuicio** que puedan afectar a las categorías de personas físicas y colectivos determinados por su uso en el contexto específico;
- **una descripción de la aplicación de medidas de supervisión humana,** de acuerdo con las instrucciones de uso;
- **las medidas que deben adoptarse en caso de que dichos riesgos se materialicen**, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación;

La obligación se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si durante el uso del sistema de IA de alto riesgo el responsable del despliegue considera que alguno de los elementos enumerados ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.

Una vez realizada la evaluación, **el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado,** presentando el modelo cumplimentado que elaborará la Oficina de IA y que contendrá información detallada sobre los seis puntos anteriores. Dicho modelo de cuestionario será diseñado mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada.

Si ya se cumple cualquiera de las obligaciones establecidas mediante la evaluación de impacto relativa a la protección de datos realizada con arreglo al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos:

2. OBLIGACIONES

De los proveedores de sistemas de IA de alto riesgo

- Velarán por que sus sistemas de IA de alto riesgo cumplan los requisitos relativos al sistema de control de riesgos que han de dfinir de acuerdo al contenido explciitado en el Reglamento.
- Serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables en virtud de los actos legislativos de armonización de la Unión.
- Indicarán en el sistema de IA de alto riesgo o, cuando no sea posible, en el embalaje del sistema o en la documentación que lo acompañe, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.
- Contarán con un sistema de gestión de la calidad que cumpla con lo dispuesto en el artículo 17 del Reglamento.

- Conservarán toda la documentación relacionada con el sistema durante un periodo de 10 años.
- Cuando estén bajo su control, conservarán los archivos de registro generados automáticamente por sus sistemas.
- Se asegurarán de que los sistemas sean sometidos al procedimiento pertinente de evaluación de conformidad antes de su puesta en el mercado o en servicio.
- Elaborarán una declaración UE de conformidad y colocarán el marcado CE en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar la conformidad con el Reglamento.
- Cumplirán las obligaciones de registro consignadas en el Reglamento.
- Adoptarán las medidas correctoras necesarias y facilitarán la información exigida.
- Demostrarán, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema con los requisitos establecidos en la sección 2.
- Velarán por que el sistema cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

De una manera más específica, la lectura del RIA aporta información detallada sobre estas responsabilidades de la figura del proveedor de IA de alto riesgo, que en su debe tiene:

- **Definir y aplicar un sistema de gestión de riesgos pre y post comercialización:**
  - Que sea iterativo, continuo, planificado y ejecutado durante todo el ciclo de vida del sistema.
  - Que tenga por objeto detectar y mitigar los riesgos pertinentes de los sistemas de IA para la salud, la seguridad y los derechos fundamentales.
  - Que permita documentar las medidas de gestión de riesgos más adecuadas. Que permita tener en cuenta los usos de los sistemas de IA que, aunque no estén directamente cubiertos por la finalidad prevista ni establecidos en las instrucciones de uso, cabe esperar razonablemente que se deriven de un comportamiento humano fácilmente previsible en el contexto de las características específicas y del uso de un sistema de IA concreto.
- **Proporcionar la documentación necesaria para que el responsable de la implantación tenga:**
  - **Información clara sobre sobre el funcionamiento del sistema, sus fortalezas y limitaciones,** así como de cualquier circunstancia, conocida o previsible, asociada a la utilización del sistema conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales. Con ello se pretende garantizar que el responsable del despliegue sea consciente de estos riesgos y los tenga en cuenta al utilizar el sistema de IA de alto riesgo.
  - **Información para facilitar la interpretación de los resultados de salida del sistema de IA**. La transparencia, incluidas las instrucciones de uso que acompañan a los sistemas de IA, debe ayudar a los responsables del despliegue a utilizar el sistema y tomar decisiones con conocimiento de causa. A fin de mejorar la legibilidad y la accesibilidad de la información incluida en las instrucciones de uso, cuando proceda, deben incluirse ejemplos ilustrativos, por ejemplo, sobre las limitaciones y sobre los usos previstos y excluidos del sistema de IA. Los proveedores deben garantizar que toda la documentación, incluidas las instrucciones de uso, contenga información significativa, exhaustiva, accesible y comprensible, que tenga en cuenta las necesidades y los conocimientos previsibles de los responsables del despliegue destinatarios. Las instrucciones de uso deben estar disponibles en una lengua fácilmente comprensible paralos responsables del despliegue destinatarios.

- **Definir las medidas adecuadas de supervisión humana** antes de su introducción en el mercado o puesta en servicio.
- Cuando proceda, dichas medidas deben garantizar, en concreto, **que el sistema esté sujeto a limitaciones operativas incorporadas en el propio sistema que éste no pueda desactivar,** que responda al operador humano y que las personas físicas a quienes se haya encomendado la supervisión humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función.
- También es esencial, según proceda, **garantizar que los sistemas incluyan mecanismos destinados a orientar e informar a las personas físicas** a las que se haya asignado la supervisión humana para que tomen decisiones con conocimiento de causa acerca de si intervenir, cuándo hacerlo y de qué manera, a fin de evitar consecuencias negativas o riesgos, o de detener el sistema si no funciona según lo previsto.
- **Garantizar un nivel de ciberseguridad adecuado a los riesgos**, adoptando medidas adecuadas y teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente.
- **Garantizar el pleno cumplimiento de los requisitos de accesibilidad,** incluidas la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo (38) y la Directiva (UE) 2019/882, para asegurar que las personas con discapacidad tengan acceso, en igualdad de condiciones con las demás, a las tecnologías y sistemas de la información y las comunicaciones, así como para garantizar el respeto a la intimidad de las personas con discapacidad;
- **Llevar registros y disponer de documentación técnica** que contenga la información necesaria para evaluar si el sistema de IA de que se trate cumple los requisitos pertinentes. Dicha información ha de estar actualizada a lo largo de toda la vida útil del sistema y debe incluir las características generales, las capacidades y las limitaciones del sistema y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos pertinente, elaborada de manera clara y completa.
- **Facilitar a las autoridades toda la información necesaria sobre la conformidad** del sistema y registrar éste en la base de datos de la UE de alto riesgo.
- Y finalmente, con carácter excepcional, y en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, deben ser capaces de tratar categorías especiales de datos personales, como cuestión de interés público esencial.

DEBERES DE TRANSPARENCIA E INSTRUCCIONES DE USO

Transparencia y comunicación de información a los responsables del despliegue por parte de los proveedores

Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de 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.

Para ello, irán acompañados de las instrucciones de uso correspondientes con las siguientes características y contenidos mínimos:

- En un formato digital o de otro tipo adecuado.
- Con información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible, y que, al menos, contenga:

- **la identidad y los datos de contacto del proveedor** y, en su caso, de su representante autorizado;
- **las características, capacidades y limitaciones del funcionamiento del sistema**, con inclusión de:
  - su **finalidad** prevista,
  - el **nivel de precisión** (incluidos los parámetros para medirla), solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse, así como cualquier circunstancia conocida y previsible que pueda afectar al nivel de precisión, solidez y ciberseguridad esperado,
  - **cualquier circunstancia conocida o previsible,** asociada a la utilización del sistema conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales,
  - en su caso, las **capacidades y características técnicas** del sistema para proporcionar información pertinente **para explicar sus resultados de salida**, cuando proceda, **su funcionamiento con respecto a determinadas personas o colectivos** de personas en relación con los que esté previsto utilizar el sistema, cuando proceda, **especificaciones relativas a 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 de alto riesgo,
  - en su caso, **información que permita interpretar los resultados de salida** del sistema y utilizarla adecuadamente;
- Los **cambios en el sistema de IA de alto riesgo** y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;
- Las medidas de supervisión humana, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue;
- Los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema y las medidas de mantenimiento y cuidado necesarias (incluida su frecuencia) para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a las actualizaciones del software;
- Cuando proceda, una **descripción de los mecanismos incluidos en el sistema que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro.**

DATOS DE CALIDAD

Hacia un modelo de gobernanza de los datos

El RIA incluye la obligación de instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad:

- Todos ellos, **incluidas las etiquetas, deben ser pertinentes, lo suficientemente representativos,**
- En la mayor medida posible, **estar libres de errores y ser completos** en vista de la finalidad prevista del sistema.
- En materia de **protección de datos,** las prácticas de gestión y gobernanza de datos deben incluir,

en el caso de los datos personales, la transparencia sobre el fin original de la recopilación de datos.

- Los conjuntos de datos deben tener las **propiedades estadísticas adecuadas,** también en lo que respecta a las personas o los colectivos de personas en relación con los que esté previsto utilizar el sistema de IA de alto riesgo.
- Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las **características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico** en el que está previsto que se utilice el sistema de IA de alto riesgo.

Los sesgos pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos o generados cuando los sistemas se despliegan en entornos del mundo real. Los resultados de los sistemas de IA dependen de dichos sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados colectivos vulnerables, incluidos colectivos raciales o étnicos.

El requisito de que los conjuntos de datos, en la mayor medida posible, sean completos y estén libres de errores no debe afectar al uso de técnicas de protección de la intimidad en el contexto del desarrollo y la prueba de sistemas de IA. En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto que se utilice el sistema de IA.

Los requisitos relacionados con la gobernanza de datos pueden cumplirse recurriendo a terceros:

- que ofrezcan servicios certificados de cumplimiento,
- incluida la verificación de la gobernanza de datos, la integridad del conjunto de datos y las prácticas de entrenamiento, validación y prueba de datos,

Todo ello en la medida en que se garantice el cumplimiento de los requisitos en materia de datos del presente Reglamento.

El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. **Las medidas adoptadas por los proveedores para garantizar el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados.**

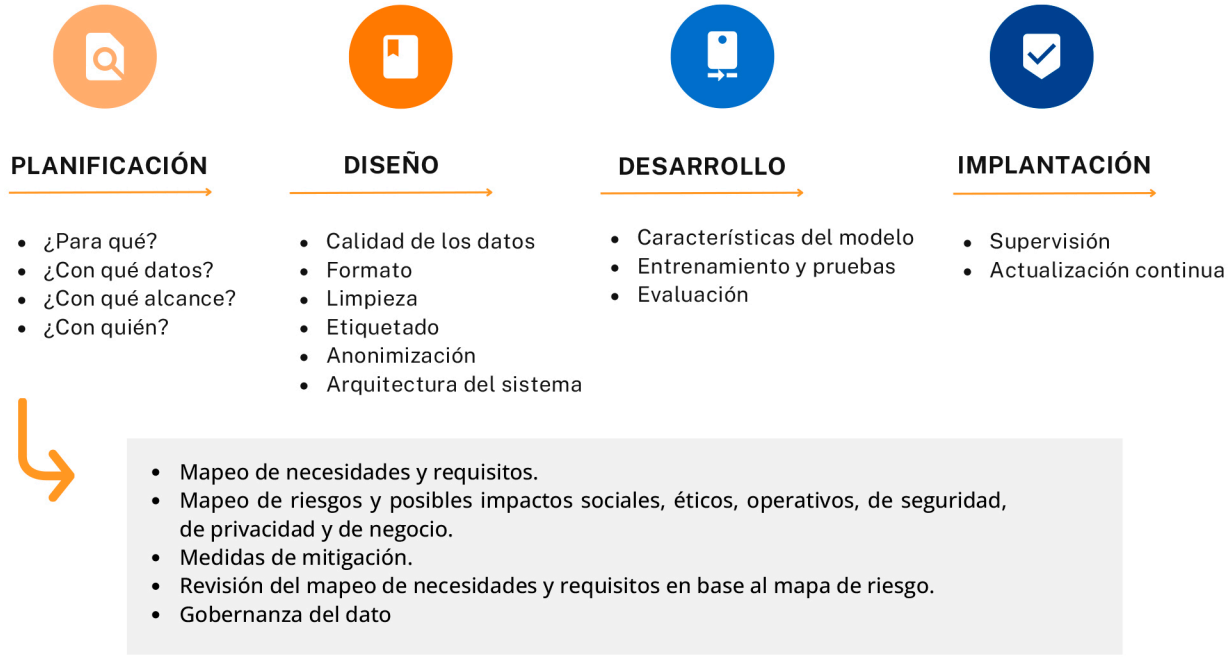
MAPA DE RUTA

El modelo de gobernanza de la IA más allá de la gobernanza de los datos

La inteligencia artificial es un **reto de gobernanza en el que todos los colectivos de una organización han de estar involucrados.** Y ello es así porque los desafíos que trae consigo no son tanto tecnológicos sino profundamente humanos. Ante un potencial de negocio que se antoja infinito es más necesario que nunca comprometerse con la idea de que el fin no justifica los medios, y en lo que

respecta a la IA, marcar los límites de los cómo y los para qué no es sólo una cuestión de regulación normativa sino mucho más de valores y de ética corporativa.

Dado que sus posibilidades crecen exponencialmente y los plazos que impone el RIA, el posicionamiento de las empresas no se puede dilatar: la reflexión debe iniciarse ahora y desde arriba, y ha de expresarse en un modelo de gobernanza que recoja la estrategia corporativa, tanto dentro como fuera de ella.



El cumplimiento normativo y el cumplimiento ético son, en el marco de la inteligencia artificial, obligaciones críticas, interdependientes y al mismo nivel de prioridad, ya que ambos resultan esenciales para garantizar un uso responsable y beneficioso de esta tecnología. Y no sólo porque la velocidad de crecimiento exponencial de ésta choque con los tiempos jurídicos, sino porque los grises que pueda generar su aplicación en muchos casos habrán de quedar cubiertos por los principios y los valores organizacionales, profesionales pero también personales.

La distinción entre estas tres esferas no es baladí, porque **si ponemos a la persona en el centro del algoritmo y las personas queremos estar en el centro del él, más allá del compromiso de las organizaciones y de sus profesionales, cada individuo tiene su propia responsabilidad para conducirse con ella y en ella.** Las empresas tienen un rol referente a la hora de crear cultura de compliance pero el cumplimiento no sólo se agota en ella; de la misma manera de compliance somos todos, la cultura de IA también ha de ser de todos.

LA RESPONSABILIDAD EMPRESARIAL EN LA CONSTRUCCIÓN DE UNA CULTURA DE USO DE IA

El Reglamento Europeo de IA será de obligado cumplimiento en 2026, o antes si los procedimientos se aceleran, y las obligaciones que impone, con sus consiguientes sanciones en caso de incumplimiento, llaman a poner orden en cada casa con antelación y en detalle. A los principios tradicionales de respeto a los derechos humanos y no discriminación que inspiran el RIA, el legislador suma los de transparencia y explicabilidad, con los que quiere exponer la razonabilidad de las decisiones basadas en IA al entendimiento de todas las partes implicadas.

Precisamente esta claridad de conceptos, usos y fines de la IA es la que le dota de un objetivo adicional a un modelo de gobernanza, más allá del mero cumplimiento normativoEtiquetado y para hacer de éste una misión común: el de contribuir a generar una cultura de uso éticoAAnonimizaciónrquitectura del sistema y responsable de la misma. Del modelo se derivarán políticas y procedimientos de obligado cumplimiento que, para ello, habrán de ser interiorizados a través de hábitos en los procesos y en las actitudes de toda la jerarquía de la organización. La visión holística y multidisciplinar, es el primer mandato de un modelo de gobernanza que debería incluir:

Si ponemos a la persona en el centro del algoritmo y las personas queremos estar en el centro del él, más allá del compromiso de las organizaciones y de sus profesionales, cada individuo tiene su propia responsabilidad para conducirse con ella y en ella.