DISEÑO DEL MODELO DE GOBERNANZA DE DATOS EN SISTEMAS DE IA

1. Objeto y enfoque del Plan de Gobernanza de Datos

Objetivo: implantar un conjunto de políticas, procedimientos, procesos y normas para garantizar que los datos utilizados en entrenamiento, validación y prueba de los sistemas de IA sean adecuados, pertinentes, suficientemente representativos y cumplan requisitos de calidad y completitud.

Enfoque: El Plan se debe articular conforme a las fases del modelo de gestión de datos:

Fuente: Guía AESIA – "Datos y Gobernanza del Dato"

Ámbito de aplicación:

Los requisitos descritos en el artículo 10 "Datos y gobernanza de datos" del Reglamento IA están orientados fundamentalmente al desarrollo del sistema, realizado por el proveedor.

En dicho artículo, no se especifican requisitos para aquel que hace uso del sistema, es decir, el responsable del despliegue. En caso de que el responsable del despliegue, en una situación determinada, participase en el desarrollo del sistema, o fuera responsable de los datos de entrenamiento o prueba, éste debería aplicar las medidas desarrolladas para el proveedor.

2. Modelo operativo por fases en el modelo de gestión:

Fase 1 — Requisitos de información

Proceso para establecer con qué información debemos alimentar el sistema de IA para lograr el objetivo para el que fue diseñado.

Cómo se implementa:

- Definir objetivo/finalidad del sistema y la necesidad que cubre.
- Identificar la información necesaria para cubrir esa necesidad o resolver el problema (lista de variables/información requerida).

Fase 2 — Recopilación de datos

Proceso para obtener los datos que contienen la información necesaria.

Cómo se implementa:

- Para cada requisito de información, seleccionar fuentes y método de recopilación en función de la necesidad y el contexto de implementación, teniendo en cuenta las cautelas necesarias para garantizar la precisión del sistema.
- Tener en especial consideración la normativa aplicable en materia de protección de datos personales.

Fase 3 — Preparación de datos

Fase de procesado y acondicionamiento de los datos recopilados; se compone de operaciones que se realizan según la naturaleza/estado de los datos.

3.1. Medición y mejora de la calidad del dato

La calidad es el grado de adecuación de los datos al propósito para el que han sido definidos o recabados. Medir calidad es analizar esa adecuación y mejorar es ajustar para aumentarla.

Medición y mejora de la calidad es un proceso imprescindible en un adecuado gobierno del dato.

Cómo se implementa:

- Seleccionar dimensiones de calidad adecuadas por dato/dataset (completitud, representatividad, auditabilidad, consistencia, relevancia, diversidad, credibilidad, etc.).
- Definir y aplicar controles de calidad para dichas dimensiones (deben establecerse catálogos de controles por dimensión y su definición).

3.2. Transformación, agregación, muestreo, creación/selección de características, enriquecimiento, etiquetado

Se deben contemplar estas operaciones como posibles tratamientos dentro de la preparación.

- Transformación: conversión de los datos a un formato homogeneizado para su uso en el sistema de IA.

- Agregación de datos: agrupar datos con el fin de poder analizarlos y facilitar observaciones para extraer conclusiones sobre la información que éstos representan.
- Muestreo: se extrae un subconjunto de datos desde un conjunto de datos más grande para hacer pruebas de manera ágil.

- Creación y selección de características: permiten aumentar o reducir la dimensionalidad de nuestro conjunto de datos. Aumentaremos la dimensionalidad mediante la creación de nuevas características y la reduciremos mediante la selección de un subconjunto de las características disponibles.

- Enriquecimiento: Implica incorporar datos de nuevas fuentes; se interpreta como un proceso posterior a la recopilación inicial, cuando se identifican necesidades adicionales de datos o características.

- Etiquetado: se aborda si se requieren datos etiquetados y no se dispone de etiquetas en las fuentes; se trata de un proceso de asignación de etiquetas identificativas a los datos.

3.3. Análisis de sesgos en los datos

Podemos definir el sesgo como la tendencia o potencial error sistemático por desequilibrio, al sobreponderar o sobrerrepresentar elementos del conjunto de datos.

Cómo se implementa:

- Incluir un proceso de análisis de sesgos dentro de la preparación y apoyarse en listados de:
    - fuentes comunes de sesgo,
    - técnicas de evaluación,
    - medidas de tratamiento/mitigación

Fase 4 — Disposición de los datos

Proceso de proporcionar los datos, tras la preparación, para su uso en el sistema de IA.

Cómo se implementa (como mínimo):

- Especificar el proceso de disposición, dónde se almacenan los datos y cómo acceder.
- Implementar autenticación y acceso a datos.
- Documentar y mantener control de versiones de procesos de disposición y registro de actualizaciones.
- Informar sobre los procesos previos (requisitos de información, recopilación, preparación incluyendo calidad/sesgos).
- Informar de posible presencia de datos personales/categorías especiales y de medidas de seguridad y privacidad implementadas (p. ej., seudonimización/anonimización), y de posibles usos indebidos razonablemente previsibles.
- Documentar detalles y metadatos necesarios (distribución/propiedades estadísticas, tipos, formato, fechas de adquisición/actualización).

Fase 5 — Eliminación de datos

Última fase del ciclo de vida: retirada de los datos dispuestos y utilizados para el desarrollo del sistema.

Cómo se implementa:

- Ejecutar la retirada mediante eliminación o transferencia, según el caso.
- Para transferencia, identificar un destinatario con garantías adecuadas para custodiar los datos y asumir obligaciones legales y contractuales asociadas.

3. Política de documentación

Debe documentarse el sistema para demostrar el cumplimiento de los requisitos en materia de gobernanza del dato, incluyendo fichas técnicas con metodologías/técnicas y datasets de entrenamiento, descripción general,

procedencia, alcance, características, y cómo se obtuvieron y seleccionaron los datos.

Repositorio documental mínimo:

- Fichas técnicas/datasheets de datasets (procedencia, alcance, características, obtención y selección).
- Resultados de calidad (dimensiones, controles y mejoras).
- Evidencia de análisis y tratamiento de sesgos.
- Proceso de disposición: accesos, autenticación, versionado y registro de actualizaciones.
- Registros de eliminación/transferencia.

4. Catálogo inicial (mínimo) de dimensiones a considerar

El proveedor/responsable debe operar con un catálogo de dimensiones de calidad, entre otras: accesibilidad, auditabilidad e identificabilidad (incluyendo la relevancia de desidentificación/anonimización para reducir posibilidad de identificación).

5. Gobernanza de la implantación (mecanismo interno de control)

Para que el sistema de gobernanza sea aplicable operativamente, se recomienda que el proveedor/responsable establezca un mecanismo interno de control que asegure, antes de usar datos en IA, que:

- se han definido requisitos de información,
- se han recopilado datos conforme al contexto,
- se ha completado la preparación (incluida calidad y sesgos),
- se dispone el dataset con controles de acceso, versionado, metadatos e información de usos indebidos previsibles,
- y existe procedimiento de eliminación/transferencia.

BLOQUE SOBRE RGPD:

Recopilación de datos: "especial consideración" de la normativa de protección de datos

En la fase de recopilación, al seleccionar fuentes y métodos de obtención, se debe tener especial consideración hacia la normativa aplicable en materia de protección de datos personales.

Al poner a disposición los datos, debe informarse de:

- la posible presencia de datos personales y categorías especiales,
- las medidas de seguridad y privacidad aplicadas (incluida seudonimización/anonimización),
- y los usos indebidos razonablemente previsibles.

Los datos seudonimizados y la información adicional vinculada permanecen dentro del ámbito de aplicación del RGPD, porque la identificación directa se reduce, pero no se elimina totalmente.

Se deben establecer garantías aplicables, incluyendo:

- que el proceso impida reidentificar sin la información adicional,
- aplicación de principios de protección de datos a los datos seudonimizados (p. ej., conservación, comunicación),
- y medidas de seguridad para evitar brechas tanto del conjunto seudonimizado como de la información adicional.

Debe hacerse especial mención a datos de categoría especial y enlazarlo expresamente con:

- registros de actividades de tratamiento conforme a Reglamento (UE) 2016/679 y otras normas citadas, incluyendo la exigencia de que dichos registros incorporen las razones por las que el tratamiento de categorías especiales era estrictamente necesario para detectar/corregir sesgos y por qué no se lograba con otros datos (obligación del RIA).
- referencia al art. 9.1 del RGPD como marco general de categorías especiales, indicando que el tratamiento puede permitirse cuando una norma de la UE o del Estado miembro lo contemple por razones de interés público esencial, y conectando este razonamiento con el tratamiento de categorías especiales para detectar/corregir sesgos.
- necesidad de aplicar medidas y garantías de privacidad y seguridad; y se describen, entre otras, anonimización y seudonimización, indicando

que los datos anonimizados quedan fuera del ámbito de la normativa de protección de datos si puede demostrarse objetivamente que no existe capacidad material de asociación a una persona identificable.

Para el "tratamiento de categorías especiales para sesgos" deberán tenerse en cuenta los siguientes aspectos:

1. Justificación de necesidad (por qué es estrictamente necesario para detectar/corregir sesgo y por qué no sirven datos sintéticos/anonimizados).
2. Limitaciones técnicas de reutilización y "medidas punteras" de seguridad y privacidad, incluida seudonimización.
3. Eliminación de categorías especiales una vez corregido el sesgo o al final del periodo de conservación (si antes).
4. Registro de actividades de tratamiento: incorporar la motivación de necesidad y la imposibilidad de alcanzar el objetivo con otros datos.

Nota importante sobre "decisiones automatizadas".

En función de las finalidades previstas en el uso de sistemas de IA, se deberá prestar especial atención a la toma de decisiones automatizadas del art. 22 RGPD y a lo dispuesto en el art. 86 del Reglamento de IA (RIA) si se trata de sistemas de IA de alto riesgo, por ejemplo, los previstos en el punto 5 del anexo III del RIA:

5. Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones:

   a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución

   b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros

   c) Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud

   d) Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia

BETA LEGAL ASSESSORS, S.L.