IMPACTO DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL EN LAS EMPRESAS ASEGURADORAS Y NECESARIA VALORACIÓN DE SUS ASESORÍAS JURÍDICAS

1) Introducción.

El Reglamento (UE) 2024/1689 de Inteligencia Artificial ("**AI Act**") establece un marco regulatorio basado en el riesgo, para el desarrollo, la comercialización y el uso de sistemas de inteligencia artificial en la Unión Europea. Su objetivo se articula en torno a un "**doble eje**" regulatorio: (i) salvaguarda de la salud, la seguridad y los derechos fundamentales; y (ii) preservación de la innovación y del mercado interior, mediante un esquema de obligaciones graduadas según el riesgo y roles en la cadena de valor (proveedor, *deployer*, etc.).

Los Reglamentos europeos son directamente aplicables a todos los Estados miembros de la UE, sin necesidad de transposición al Derecho nacional y así lo establece el art. 113 del AI Act (publicado en el Diario Oficial de la UE el 12 de julio de 2024):

Artículo 113 - Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

Será aplicable a partir del 2 de agosto de 2026.

No obstante:

a) *los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;*
b) *el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;*
c) *el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.*

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Esta aplicación escalonada no es meramente formal: impone a las entidades aseguradoras un calendario de adecuación progresiva que exige planificación anticipada, particularmente en lo relativo a sistemas potencialmente calificables como de alto riesgo y a modelos de IA de uso general (GPAI) integrados en procesos críticos.

En el sector asegurador, el Reglamento incide de forma directa en **procesos clave del negocio** que afectan a personas físicas, como la suscripción, la tarificación, el *scoring* o la atención al cliente, entre otros. Determinados usos pueden calificarse, en supuestos concretos, como **sistemas de IA de alto riesgo**, lo que activa obligaciones técnicas, organizativas y de gobernanza especialmente exigentes.

La aseguradora puede asumir, según el caso, la condición de **proveedor** o de **responsable del despliegue (*deployer*)**, con responsabilidades diferenciadas. El incumplimiento del AI Act conlleva **riesgos regulatorios, sancionadores y reputacionales relevantes**, por lo que la IA debe abordarse como una **cuestión estratégica y no meramente tecnológica**.

2) Conceptos y categorías clave del AI Act.

El AI Act adopta un **enfoque escalonado por niveles de riesgo**, en función del tipo de sistema y del impacto potencial sobre los derechos fundamentales.

- **Definiciones esenciales**. El AI Act define ll concepto de "**sistema de IA**", el cual debe interpretarse de forma amplia, e incluye sistemas basados en técnicas de aprendizaje automático, lógica basada en reglas o aproximaciones estadísticas avanzadas, siempre que generen resultados como predicciones, recomendaciones o decisiones que influyan en entornos físicos o virtuales. En el sector asegurador, muchos modelos y motores de decisión automatizados pueden quedar subsumidos en esta definición.

  Por otro lado, distingue entre los distintos roles: "**proveedor**" (quien desarrolla o pone en el mercado un sistema bajo su nombre o marca) y "**responsable del despliegue" -*deployer*-** (quien utiliza el sistema bajo su autoridad). Estas calificaciones determinan obligaciones legales específicas.

  Asimismo, el AI Act introduce un deber transversal de "**alfabetización en materia de IA**" para proveedores y *deployers*, con impacto directo en formación, procedimientos

operativos y modelo de control interno en aseguradoras que desplieguen IA en procesos relevantes.

- **Sistemas prohibidos**. El AI Act prohíbe determinadas prácticas de IA, como aquellas que emplean técnicas subliminales o manipulativas, explotan vulnerabilidades de colectivos protegidos o realizan *social scoring* generalizado.

  En general, **los usos habituales del sector asegurador no suelen encajar en esta categoría**, si bien deben analizarse, rigurosamente, sistemas de perfilado extremo o explotación de vulnerabilidades.

  Debe prestarse especial atención a sistemas que, a través de técnicas de inferencia conductual o análisis psicométrico, puedan **influir de forma indebida en decisiones económicas de consumidores vulnerables** (por ejemplo, en seguros vinculados a financiación o productos complejos), así como a prácticas de segmentación que, en la práctica, generen exclusiones sistemáticas basadas en categorías sensibles.

  El incumplimiento de estas prohibiciones puede dar lugar a multas **de hasta 35 millones de euros, o de hasta el 7 % de su volumen de negocios mundial** total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

- **Sistemas de alto riesgo**. El principal impacto del AI Act para las aseguradoras se concentra en esta categoría. El Reglamento califica, expresamente, como **sistemas de alto riesgo** aquellos destinados a la **evaluación de riesgos y fijación de precios en seguros de vida y salud** respecto de personas físicas.

  Asimismo, el AI Act, también clasifica como alto riesgo los sistemas destinados a la **gestión de recursos humanos**, lo cual afecta transversalmente a la aseguradora en su condición de empleadora. Esto incluye sistemas para la selección de personal y para la toma de decisiones sobre promociones, asignación de tareas o rescisión de relaciones laborales basadas en el comportamiento o rendimiento.

El incumplimiento de estas obligaciones puede conllevar multas de hasta **15 millones de euros o de hasta el 3 % de su volumen de negocios mundial total** correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

- **Sistemas de riesgo limitado (obligaciones de transparencia).** Son aquellos que están sujetos a deberes específicos de información hacia el usuario final **para evitar la manipulación o confusión**. Incluyen, entre otros, sistemas destinados a interactuar directamente con personas físicas (por ejemplo, chatbots o asistentes virtuales); o a generar contenido sintético. Su obligación principal es **garantizar que el usuario esté informado de que se trata de un sistema de IA**.

  En caso de incumplimiento, las sanciones serían las mismas que en el apartado anterior.

- **Otros sistemas de IA no clasificados (sistemas de riesgo mínimo)**. Son aquellos que no encajan en las categorías anteriores (no están prohibidos, no son de alto riesgo, ni están sujetos a obligaciones de transparencia específica). Esta categoría abarca la gran mayoría de **herramientas de uso corporativo, como los filtros de spam, la gestión documental interna o la optimización de procesos logísticos**.

  Estos sistemas no están sujetos a obligaciones específicas ni a un régimen sancionador propio ligado a una categoría de riesgo, por lo que quedan sometidos al marco general del AI Act, en particular a su finalidad de protección de derechos fundamentales y a sujeción a otros marcos regulatorios.

3) Ejemplos de principales usos de la IA en el sector asegurador y clasificación probable.

- **Suscripción y tarificación de pólizas**: modelos predictivos para evaluar riesgos, fijar primas y condiciones. → **Sistema de alto riesgo**, cuando son destinados a la **evaluación de riesgos y la tarificación** en relación con personas físicas pero, **únicamente, en el caso de seguros de vida y salud**. Si estos sistemas se usan para, por ejemplo, **seguros de hogar**, sin evaluar solvencia o sin establecer clasificación crediticia, en principio no sería de alto riesgo, sin perjuicio de exigir estándares elevados de prudencia.

- **Scoring y segmentación de clientes**: análisis automatizado de perfiles de riesgo. → **Sistema de alto riesgo**, cuando implique evaluación de solvencia o clasificación crediticia, con excepción de sistemas destinados a la detección de fraude financiero.

- **Gestión y tramitación de siniestros**: → **No se regulan como sistemas de alto riesgo,** cuando estén específicamente destinados a esta finalidad, salvo que concurran otros factores (biometría, denegación de servicios esenciales).

- **Atención al cliente**: *chatbots* y asistentes virtuales → **Sistema de riesgo limitado**, sujeto a obligaciones de transparencia. En caso de integración con modelos de IA de propósito general (GPAI), la aseguradora deberá verificar contractualmente el cumplimiento de las obligaciones específicas impuestas a los proveedores de dichos modelos (Capítulo V).

- **Prevención del fraude**: identificación de patrones anómalos o comportamientos sospechosos → **Sistema excluido expresamente** de la categoría de alto riesgo cuando se limite a la detección del fraude financiero.

4) Obligaciones clave según el rol de la aseguradora de sistemas de alto riesgo.

4.1. La aseguradora como responsable del despliegue (deployer).

En la mayoría de los casos, la aseguradora actuará como **deployer**, asumiendo, entre otras, las siguientes obligaciones:

- **Uso conforme:** Utilizar el sistema de acuerdo con las instrucciones de uso facilitadas por el proveedor.

- **Supervisión humana efectiva**: Garantizar que las personas físicas encargadas de la supervisión cuenten con la competencia, formación y autoridad necesarias para vigilar el sistema.

- **Calidad del dato**: Asegurar que los datos de entrada sean pertinentes y representativos para la finalidad prevista del Sistema, en la medida en que ejerza el control sobre dichos datos.

- **Monitorización**: Realizar un seguimiento continuo del funcionamiento y suspender su uso si se detectan riesgos para la salud, la seguridad o los derechos fundamentales, junto con los correspondientes deberes de informar al respecto, así como en el caso de incidentes graves y disfunciones relevantes.

- **Registros (logs)**: Conservar los registros generados automáticamente por el sistema, en la medida en que losa archivos estén bajo su control, durante un periodo de al menos seis meses.

- **Información laboral**: Informar a los representantes de los trabajadores y a los empleados afectados antes de poner en servicio un sistema de alto riesgo en el lugar de trabajo.

- **Evaluación de Impacto en Derechos Fundamentales**: Antes de desplegar sistemas de alto Riesgo, realizar una evaluación detallada sobre el impacto en los derechos de las personas. Obligación exigible únicamente cuando se desplieguen sistemas para evaluar la solvencia/crédito o para la suscripción de seguros de vida y salud.

- **Deber de transparencia con afectados**: Informar a las personas físicas cuando estén sujetas a decisiones tomadas por sistemas de alto Riesgo.

Estas obligaciones se conectan, además, con el Reglamento General de Protección de Datos (decisiones automatizadas, transparencia, no discriminación).

4.2. La aseguradora como proveedor de IA (en su caso, menos frecuente).

Aunque es menos frecuente, la aseguradora adquiere la condición legal de proveedor, cuando **desarrolle el sistema internamente**, cuando **pone su marca** a un producto de terceros, o cuando lo **modifica sustancialmente**, con el consiguiente traslado íntegro del régimen de obligaciones del Capítulo III. En estos casos, asumiría, entre otras, las siguientes obligaciones:

- **Sistema de Gestión de Riesgos**: Implementar un proceso iterativo y continuo de identificación y mitigación de riesgos durante todo el ciclo de vida del sistema.

- **Gobernanza de Datos**: Asegurar la calidad de los conjuntos de datos, separando estrictamente los datos de entrenamiento, validación y prueba, y mitigando sesgos.

- **Documentación Técnica y Trazabilidad**: Elaborar y mantener actualizada una documentación exhaustiva que demuestre el cumplimiento normativo ante las autoridades, así como asegurar que el sistema genere registros automáticos que permitan trazar su funcionamiento durante todo su ciclo de vida.

- **Transparencia e Información**: Asegurar que el sistema sea interpretable y acompañarlo de instrucciones de uso claras, entre otras, detallando sus capacidades, finalidades de uso, limitaciones y margen de error.

- **Herramientas de Supervisión Humana**: Incorporar interfaces que permitan a las personas físicas vigilar el sistema, interpretar sus resultados e intervenir o detenerlo si fuera necesario.

- **Precisión, solidez y ciberseguridad**: Garantizar niveles adecuados de precisión, resistencia ante errores o ataques adversarios y ciberseguridad desde el diseño.

- **Sistema de calidad**: Implantar un sistema de gestión de calidad interno (procedimientos, políticas y controles) específico para la IA.

- **Evaluación de Conformidad:** Según proceda, realizar un procedimiento de control interno o un procedimiento fundamentado en la evaluación del sistema de gestión de la calidad y de la documentación técnica (con intervención de organismo notificado).

- **Marcado CE y Registro**: Colocar el marcado CE, emitir la declaración UE de conformidad y registrar el sistema en la base de datos de la UE.

5) Conclusiones y recomendaciones estratégicas.

5.1. Conclusiones clave.

- El AI Act **afecta de lleno al core del negocio asegurador**.
- Determinados sistemas utilizados por las aseguradoras **pueden calificarse como sistemas de IA de alto riesgo**, en particular en los ámbitos de **suscripción y tarificación en seguros de vida y salud**.
- Con independencia de que la aseguradora desarrolle o no los sistemas de IA, **asume responsabilidades relevantes como responsable del despliegue (deployer)** en relación con su uso efectivo.
- El enfoque regulatorio exige **anticipación, gobernanza y control**, y no se limita a un cumplimiento formal o meramente tecnológico.

5.2. Recomendaciones estratégicas.

1. **Inventariar todos los sistemas de IA** utilizados en la compañía, incluyendo aquellos basados en modelos de IA de uso general (GPAI) y **clasificarlos por nivel de riesgo.**
2. **Analizar de forma específica** los sistemas de **suscripción y tarificación,** especialmente en seguros de vida y salud.
3. **Documentar la finalidad prevista del correspondiente sistema de IA**, inputs/outputs, incidencia material en decisiones y medidas de mitigación (sesgos, calidad del dato, supervisión humana).
4. Implantar un **modelo de gobernanza de IA**, integrado con las funciones de cumplimiento normativo, gestión de riesgos y principios éticos, que establezca un inventario, criterios de riesgo y responsabilidades claras sobre todos los usos de IA en la entidad mediante una política corporativa que sea vinculante y un protocolo de control: que nadie pueda desarrollar, contratar o desplegar IA sin pasar previamente por los debidos controles (revisión y clasificación de riesgos, DPIA -*Data Protection Impact Assessment*- / FRIA -*Fundamental Rights Impact Assessment*- cuando proceda,

cumplimiento, protección de datos, ética, y, en su caso, validación técnica independiente).

5. **Reforzar la supervisión humana efectiva** y la **trazabilidad de las decisiones asistidas o automatizadas**, especialmente en procesos con impacto económico relevante para clientes o terceros.

6. Revisar **contratos con proveedores de IA** (roles, responsabilidades, acceso a documentación).

7. Coordinar el cumplimiento del Reglamento de IA con otros marcos regulatorios aplicables (**Reglamento General de Protección de Datos, Reglamento DORA y normativa sectorial)**.

8. Desarrollar **políticas internas de explicabilidad, gestión de sesgos y controles de calidad del dato**, especialmente en ramos de vida y salud.

9. Preparar el frente de **transparencia con cliente**: plantillas y guías de comunicación para (i) interacciones con chatbots/IA; (ii) explicaciones comprensibles de decisiones relevantes (sin revelar secretos industriales); y (iii) canales efectivos de reclamación/impugnación con intervención humana real.

10. **Asegurar la alfabetización en materia de IA** mediante planes de formación segmentados por perfiles (negocio, TI, riesgos, legal, mediadores, etc.), con carácter periódico y obligatorio, y mantener evidencia documental suficiente (registros, materiales, evaluaciones) para su verificación por auditoría interna y por el supervisor.

11. **Sensibilizar a la alta dirección**: la IA debe gestionarse como un **riesgo regulatorio y estratégico transversal**, y no únicamente como una cuestión tecnológica.

En síntesis, el AI Act no constituye únicamente una norma tecnológica, sino un nuevo eje regulatorio estructural para el sector asegurador que redefine la forma en que las entidades diseñan, implementan y controlan los procesos nucleares del negocio cuando la inteligencia artificial interviene en decisiones con impacto relevante para personas físicas. No se trata de un ajuste operativo puntual, sino de **una exigencia de transformación organizativa que afecta a la gobernanza, a la gestión del riesgo, a la trazabilidad de las decisiones y a la rendición de cuentas**.

La anticipación en la adaptación, la delimitación clara de roles y responsabilidades dentro de la organización y frente a terceros, y la integración del cumplimiento en la estrategia corporativa serán factores decisivos para **reducir exposición sancionadora, litigiosa y reputacional**. La IA deja de ser un proyecto tecnológico para convertirse en una cuestión de dirección estratégica y de control interno.

Desde una **perspectiva de negocio**, las entidades que integren de manera temprana (i) una gobernanza sólida basada en evidencia documentada; (ii) una disciplina rigurosa en el diseño, validación y monitorización de modelos y datos; y (iii) una experiencia de cliente transparente, comprensible y jurídicamente defendible, estarán en mejor posición para escalar soluciones de IA con seguridad y eficiencia, evitando acumulación de riesgos regulatorios latentes y conflictos futuros.

Asimismo, **el uso correcto, gobernado y jurídicamente seguro de la IA puede actuar como un verdadero multiplicador de ingresos para las entidades aseguradoras**. La mejora en la precisión del *pricing*, la optimización de la selección de riesgos, la reducción de fraude, la personalización de productos y la eficiencia en la gestión de siniestros permiten aumentar márgenes técnicos, mejorar ratios combinados y ampliar cuota de mercado. Cuando estos beneficios se articulan dentro de un marco de control robusto, **la IA no solo reduce costes, sino que puede impulsar de forma significativa y sostenida el crecimiento de ingresos y la rentabilidad del negocio asegurador**.

En este contexto, **un cumplimiento avanzado y estructurado del AI Act puede convertirse en un elemento diferenciador en el mercado**. No solo refuerza la confianza de clientes y supervisores, sino que proyecta una imagen de solidez, responsabilidad y madurez organizativa, alineada con los estándares europeos de buen gobierno y protección de los

derechos fundamentales. **La gestión responsable de la inteligencia artificial pasa así a formar parte del capital reputacional y estratégico de la entidad aseguradora**.