

EIOPA publica una Consulta sobre la gobernanza y la gestión de riesgos en el uso de la Inteligencia Artificial

Legal Alert

Febrero 2025

kpmgabogados.es
kpmg.es



EIOPA publica una Consulta sobre la gobernanza y la gestión de riesgos en el uso de la Inteligencia Artificial

La Inteligencia Artificial se ha convertido en un elemento fundamental dentro de la cadena de valor de las entidades aseguradoras, desempeñando un papel clave en diversos aspectos de la comercialización de seguros. Esta transformación ha generado la necesidad de actualizar el marco regulatorio del sector, con el objetivo de establecer requisitos que garanticen un uso seguro y coherente de esta tecnología, al tiempo que se mitigan posibles sesgos que puedan surgir. En este contexto, y con el propósito de adecuarse al Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, el “Reglamento de IA”) la Autoridad Europea de Seguros y Pensiones de Jubilación (“EIOPA”) ha iniciado trabajos de consulta y la publicación de opiniones destinadas a asegurar el cumplimiento de las disposiciones establecidas en dicha normativa.

El objetivo de este a opinión sobre la que EIOPA solicita comentarios a través de un documento de Consulta Pública es proporcionar claridad sobre los principios y requerimientos de la legislación sectorial relativa a aquellos sistemas de Inteligencia Artificial (“IA”) que no estén prohibidos o considerados de alto riesgo por el Reglamento de IA.

La Consulta Pública sigue un enfoque basado en los principios y se encuentra en línea con aquellos establecidos por el Reglamento de IA y por otras iniciativas internacionales en el mismo ámbito. Del mismo modo, EIOPA aclara que no pretende instaurar nuevos principios ni extender lo que establece el propio Reglamento.

Contexto normativo

La Consulta Pública se sitúa en el marco del Reglamento de IA, la Directiva (UE) 2016/97 de distribución de seguros (en adelante, “**IDD**”), la Directiva 2009/138/CE (en adelante, “**Solvencia II**”), y el Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (en adelante, “**DORA**”).

¿Qué establece EIOPA?

EIOPA, siguiendo las previsiones de Solvencia II, IDD y DORA, y en aras de garantizar un uso responsable

de la IA que maximice sus beneficios y disminuya al mínimo sus riesgos, considera que las entidades deberán instaurar sistemas de gobernanza y gestión del riesgo considerando seis principios, que son:

1. Actuar conforme a principios éticos y justos, priorizando el interés del consumidor.

El art. 17 de IDD establece que los Estados Miembros garantizarán que los intermediarios de seguros o los distribuidores de seguros, cuando desarrollen actividades de distribución de seguros, “*actúen siempre con honestidad, equidad y profesionalidad, en beneficio de los intereses de sus clientes*”.

Sobre la base de este artículo, las entidades deberán adoptar un enfoque basado en el consumidor a la hora de utilizar sistemas de inteligencia artificial a lo largo de toda la cadena de valor del producto. Esto se realizará para asegurar que se está tratando a los consumidores de una forma ética y siempre en interés de estos.

La información utilizada para el “entrenamiento” de la IA deberá ser adecuada, completa, representativa del público objetivo al que se quiere dirigir el producto y libre de sesgos. Además, en caso de existir dichos sesgos en los outputs de los sistemas de IA, estos deberán ser fácilmente identificables y poder mitigarse.

2. Implementar Políticas sólidas de gobernanza de datos

De acuerdo con el art. 260.1.a). iii de Reglamento Delegado 2015/35, las entidades deberán implementar una política de gobernanza de datos que se encuentre alineada con los potenciales impactos que pueda tener el uso de la IA, y que cumpla con la legislación en materia de protección de datos.

Una política sólida de gobernanza de datos debe asegurar que los datos utilizados para entrenar y evaluar los sistemas de IA son

- Completos (representativos de la población y con un histórico suficiente).
- Adecuados (sin errores significativos y libres de sesgos).
- Apropiados (coherentes con el propósito para el que se van a utilizar).

En caso de que se utilicen datos provenientes de un tercero externo, deberán aplicarse exactamente los mismos estándares.

3. Mantener una documentación adecuada y ordenada

Las entidades deberán mantener la información relativa a los sistemas de IA guardada y ordenada de forma adecuada.

Para ello, en el Anexo I del documento, EIOPA establece un modelo de cómo debe hacerse este trámite.

4. Transparencia y explicabilidad

En cumplimiento del artículo 20.1 de IDD, las entidades deberán adoptar las medidas necesarias para asegurar que los resultados de los sistemas de IA puedan ser explicados en su mayoría. Para ello podrán utilizarse diferentes métodos, como utilizar algoritmos más claros y transparentes en detrimento de otros más opacos.

Asimismo, las explicaciones deberán adaptarse para cada caso específico de uso de la IA. En caso de tratarse de un sistema de IA muy complejo, las entidades deberán contemplar utilizar medidas complementarias para mitigar el riesgo que esto pueda occasionar, entre las que se pueden destacar mayores barreras y una supervisión humana más fuerte.

5. Definir claramente los roles y responsabilidades del personal involucrado

El artículo 46 de Solvencia II establece que las entidades deberán tener controles internos de los sistemas, a todos sus niveles.

Estos roles deberán estar definidos en la política interna de cada entidad, en la que, como mínimo, se deberán contemplar:

- Responsabilidad de los miembros del órgano de dirección del uso de la IA, asegurando que cuenten con el suficiente conocimiento y que estos conocen cuáles son los potenciales riesgos en su entidad.
- Funciones de cumplimiento normativo y auditoría deberán asegurar que el uso de la IA cumple con lo previsto en la regulación.
- El DPO deberá, también, confirmar que la información y datos utilizados por los sistemas de IA son procesados correctamente y conforme a la legislación.

6. Adecuación, robustez y ciberseguridad

Los niveles de adecuación, robustez y ciberseguridad deberán adecuarse siempre a la magnitud, naturaleza y complejidad del sistema de IA que se esté utilizando en cada momento.

Por último, EIOPA afirma que el uso responsable de IA será una combinación de diferentes medidas de gestión del riesgo. Todas las medidas anteriores son complementarias una de la otra e interdependientes entre ellas.

Próximos pasos

La Consulta se encontrará abierta hasta el 12 de mayo de 2025. Posteriormente, EIOPA considerará los comentarios recibidos, y, tras evaluar el impacto de la evaluación recibida, revisará su opinión acorde con la misma.

Documentos

Por si resulta de interés, les dejamos el link a la Consulta:

- [Link](#)

Contactos

Francisco Uría
Socio
KPMG Abogados
Tel. 91 451 30 67
furia@kpmg.es

María Pilar Galán
Socia
KPMG Abogados
Tel. 91 451 31 70
mariapilargalan@kpmg.es

Pablo Alonso Montes
Director
KPMG Abogados
Tel. 91 456 34 00
pabloalonso@kpmg.es

Oficinas de KPMG en España

A Coruña

Calle de la Fama, 1
15001 A Coruña
T: 981 21 8241
Fax: 981 20 02 03

Alicante

Muelle de Levante, 8
Planta Alta
03001 Alicante
T: 965 92 07 22
Fax: 965 22 75 00

Barcelona

Torre Realia
Plaça de Europa, 41
08098 L'Hospitalet de Llobregat
Barcelona
T: 932 53 2900
Fax: 932 80 49 16

Bilbao

Torre Iberdrola
Plaza Euskadi, 5
48009 Bilbao
T: 944 79 73 00
Fax: 944 15 29 67

Girona

Edifici Sèquia
Sèquia, 11
17001 Girona
T: 972 22 0120
Fax: 972 22 22 45

Las Palmas de Gran Canaria

C/Bravo Murillo, 22
35003 Las Palmas de Gran Canaria
T: 928 32 32 38
Fax: 928 32 45 55

Madrid

Torre de Cristal
Paseo de la Castellana, 259 C
28046 Madrid
T: 91 456 34 00
Fax: 91 456 59 39

Málaga

Marqués de Larios, 3
29005 Málaga
T: 952 61 14 00
Fax: 952 30 53 42

Oviedo

Ventura Rodríguez, 2
33004 Oviedo
T: 985 27 69 28
Fax: 985 27 49 54

Palma de Mallorca

Edificio Reina Constanza
Calle de Porto Pi, 8
07015 Palma de Mallorca
T: 971 72 1601
Fax: 971 72 58 09

Pamplona

Edificio Iruña Park
Arcadio M. Larraona, 1
31008 Pamplona
T: 948 17 1408
Fax: 948 17 35 31

San Sebastián

Avenida de la Libertad, 17-19
20004 San Sebastián
T: 943 42 2250
Fax: 943 42 42 62

Sevilla

Avda. de la Palmera, 28
41012 Sevilla
T: 954 93 4646
Fax: 954 64 70 78

Valencia

Edificio Mapfre
Paseo de la Almeda, 35, planta 2
46023 Valencia
T: 963 53 4092
Fax: 963 51 27 29

Vigo

Plaza Compostela, 20
36201, Vigo
T: 986 22 8505
Fax: 986 43 85 65

Zaragoza

Centro Empresarial de Aragón
Avda. Gómez Laguna, 25
50009 Zaragoza
T: 976 45 8133
Fax: 976 75 48 96

© 2025 KPMG Abogados S.L.P., sociedad española de responsabilidad limitada profesional y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Limited, sociedad inglesa limitada por garantía.

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.