

REGLAMENTO DE INTELIGENCIA ARTIFICIAL ("RIA")

Capítulo III; Secciones 1 y 2 (arts. 6 a 15)

píldora #2

RESUMEN EJECUTIVO (I)

ARTÍCULO	RESUMEN
6	Un sistema de IA se considera de alto riesgo si es componente de seguridad de un producto regulado por legislación de la Unión Europea o si es uno de dichos productos y debe ser evaluado antes de su mercado o uso. Además, los sistemas en el anexo III también son de alto riesgo, a menos que no presenten un riesgo significativo para la salud o derechos fundamentales bajo ciertas condiciones especificadas.
7	La Comisión puede modificar el anexo III agregando o eliminando casos de uso de sistemas de IA de alto riesgo, siguiendo criterios específicos que evalúan la intención, uso, naturaleza de datos, autonomía, y riesgos potenciales para la salud, seguridad, o derechos fundamentales.
8	Los sistemas de IA de alto riesgo deben cumplir con determinados requisitos y considerar su gestión de riesgos. Los proveedores deben garantizar que sus productos cumplen con todos los requisitos aplicables y pueden integrar procesos y documentación necesarios en los ya requeridos por la legislación de la UE.
9	Se debe establecer y mantener un sistema de gestión de riesgos para los sistemas de IA de alto riesgo, requiriendo la identificación, análisis, estimación y mitigación de riesgos conocidos y previsibles para la salud, seguridad y derechos fundamentales.
10	Los sistemas de IA de alto riesgo que entrenan modelos con datos deben desarrollarse con conjuntos de datos que cumplan criterios de calidad específicos y se sometan a prácticas de gobernanza y gestión. Se deben tomar medidas para detectar, prevenir y mitigar sesgos potenciales.

RESUMEN EJECUTIVO (II)

ARTÍCULO	RESUMEN
11	Antes de la introducción en el mercado o uso, los sistemas de IA de alto riesgo deben contar con documentación técnica actualizada que demuestre su conformidad con los requisitos establecidos y provea información clara a las autoridades competentes.
12	Los sistemas de IA de alto riesgo deben permitir el registro técnico de eventos para facilitar la trazabilidad, la detección de riesgos, y la vigilancia posventa. Deben incluir registros mínimos como uso del sistema y verificación de resultados.
13	Los sistemas de IA de alto riesgo deben facilitar transparencia y ser acompañados de instrucciones de uso que incluyan información clara y pertinente para permitir a los usuarios interpretar y utilizar correctamente sus resultados.
14	Los sistemas de IA de alto riesgo deben ser diseñados para una supervisión efectiva, con medidas proporcionales y herramientas adecuadas para permitir la intervención humana y garantizar la verificación y confirmación de resultados.
15	Los sistemas de IA de alto riesgo deben alcanzar niveles adecuados de precisión, solidez y ciberseguridad, y se deben tomar medidas para resistir errores, fallos y vulnerabilidades, con una resistencia específica a ataques externos y manipulaciones.

ARTÍCULO 6: REGLAS DE CLASIFICACIÓN DE LOS SISTEMAS DE IA ALTO RIESGO (I)

- Un sistema de IA se considerará de alto riesgo cuando:
 - Esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I.
- Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.
- Un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas.

ARTÍCULO 6: REGLAS DE CLASIFICACIÓN DE LOS SISTEMAS DE IA ALTO RIESGO (II)

- Tareas de procedimiento limitada
- Mejora de actividad humana previa
- Detección de patrones de toma de decisiones
- Tarea preparatoria para evaluación
- Elaboración de perfiles de personas físicas
- Documentación de evaluación por proveedor

ARTÍCULO 6: REGLAS DE CLASIFICACIÓN DE LOS SISTEMAS DE IA ALTO RIESGO (III)

- La Comisión proporcionará directrices sobre la aplicación práctica del artículo
 - Esto se hará en consulta con el Consejo de IA
 - Se proporcionará una lista de ejemplos prácticos de casos de uso de sistemas de IA de alto y no alto riesgo
- La Comisión puede modificar el apartado 3, párrafo segundo, mediante actos delegados
 - Esto se hace para añadir o modificar condiciones cuando existan pruebas concretas y fiables
 - Esto no reducirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales

ARTÍCULO 7: MODIFICACIONES DEL ANEXO III (I)

- La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97
 - Objetivo: modificar el anexo III
 - Adición o modificación de casos de uso de sistemas de IA de alto riesgo
- Condiciones para modificar el anexo III:
 - Los sistemas de IA deben ser utilizados en los ámbitos que figuran en el anexo III
 - Los sistemas de IA deben plantear un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales
 - El riesgo debe ser equivalente o mayor que el riesgo de los sistemas de IA de alto riesgo ya mencionados en el anexo III

ARTÍCULO 7: MODIFICACIONES DEL ANEXO III (II)

- Finalidad prevista del sistema de IA
 - Medida en que se haya utilizado o sea probable que se utilice un sistema de IA
 - Naturaleza y cantidad de los datos tratados y utilizados por el sistema de IA
 - Grado de autonomía con el que actúa el sistema de IA
 - Posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio
- Medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad
- Posible alcance de dicho perjuicio o dichas repercusiones negativas
- Medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan del resultado generado por un sistema de IA

ARTÍCULO 8: CUMPLIMIENTO DE LOS REQUISITOS

- Cumplimiento de los requisitos
 - Los sistemas de IA de alto riesgo deben cumplir con los requisitos establecidos en la presente sección.
 - Se tendrá en cuenta el estado actual de la técnica en materia de IA y tecnologías relacionadas.
 - Se tendrá en cuenta el sistema de gestión de riesgos a que se refiere el artículo 9.
- Responsabilidad de los proveedores
 - Los proveedores son responsables de garantizar que su producto cumpla con todos los requisitos aplicables.
 - Los proveedores pueden optar por integrar los procesos de prueba y presentación de información necesarios.

ARTÍCULO 9: SISTEMA DE GESTIÓN DE RIESGOS (I)

- Establecimiento, implementación, documentación y mantenimiento de un sistema de gestión de riesgos para sistemas de IA de alto riesgo.
- Etapa de determinación y análisis de riesgos conocidos y previsibles para la salud, seguridad y derechos fundamentales.
- Etapa de estimación y evaluación de riesgos en uso previsto y uso indebido razonablemente previsible.
- Evaluación de otros riesgos a partir del análisis de datos recogidos con el sistema de vigilancia post comercialización.
- Adopción de medidas adecuadas y específicas de gestión de riesgos para hacer frente a los riesgos detectados.

ARTÍCULO 9: SISTEMA DE GESTIÓN DE RIESGOS (I)

- Las medidas de gestión de riesgos deben tener en cuenta los efectos y la posible interacción derivados de la aplicación combinada de los requisitos
 - Esto se hace para reducir al mínimo los riesgos de manera más eficaz y lograr un equilibrio adecuado en la aplicación de las medidas
- Las medidas de gestión de riesgos considerarán aceptables los riesgos residuales pertinentes asociados a cada peligro
 - Así como el riesgo residual general de los sistemas de IA de alto riesgo
- Para determinar las medidas de gestión de riesgos más adecuadas, se procurará eliminar o reducir los riesgos detectados y evaluados
- Los sistemas de IA de alto riesgo serán sometidos a pruebas para determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas

ARTÍCULO 10: DATOS Y GOBERNANZA DE DATOS

- Los sistemas de IA de alto riesgo se desarrollarán a partir de conjuntos de datos que cumplan los criterios de calidad
 - Estos conjuntos de datos se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo
 - Las prácticas se centrarán en decisiones de diseño, procesos de recogida de datos, operaciones de tratamiento, formulación de supuestos, evaluación de disponibilidad, examen de sesgos, medidas para detectar sesgos y detección de lagunas o deficiencias
- Los conjuntos de datos serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y estarán completos en vista de su finalidad prevista

ARTÍCULO 11: DOCUMENTACIÓN TÉCNICA

- La documentación técnica se elaborará antes de la introducción en el mercado o puesta en servicio y se mantendrá actualizada
 - Debe demostrar que el sistema cumple los requisitos establecidos y proporcionar información necesaria para evaluar la conformidad del sistema
 - Contendrá los elementos contemplados en el anexo IV
- Se elaborará un único conjunto de documentos técnicos para sistemas de IA de alto riesgo asociados a un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión
- La Comisión estará facultada para modificar el anexo IV para garantizar que la documentación técnica proporcione toda la información necesaria

ARTÍCULO 12: CONSERVACIÓN DE REGISTROS

- Registro automático de acontecimientos a lo largo de todo el ciclo de vida del sistema.
 - Garantizar un nivel de trazabilidad del funcionamiento del sistema de IA de alto riesgo.
- Capacidades de registro para registrar acontecimientos pertinentes para:
 - La detección de situaciones que puedan dar lugar a riesgos.
 - Facilitación de la vigilancia post comercialización.
 - Vigilancia del funcionamiento de los sistemas de IA de alto riesgo.
- En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las capacidades de registro incluirán, como mínimo:

ARTÍCULO 13: TRANSPARENCIA Y COMUNICACIÓN DE INFORMACIÓN A LOS RESPONSABLES DEL DESPLIEGUE

- Los sistemas de IA de alto riesgo deben ser diseñados para garantizar transparencia
 - Los responsables del despliegue deben poder interpretar y usar correctamente los resultados
- Los sistemas de IA de alto riesgo deben ir acompañados de instrucciones de uso
 - Las instrucciones deben ser concisas, completas, correctas y claras
 - Las instrucciones deben ser pertinentes, accesibles y comprensibles para los responsables del despliegue
- Las instrucciones de uso deben contener información específica
 - Identidad y datos de contacto del proveedor
 - Características, capacidades y limitaciones del sistema de IA de alto riesgo
 - Información sobre la precisión, solidez y ciberseguridad del sistema
 - Información sobre riesgos para la salud, seguridad y derechos fundamentales

ARTÍCULO 14: SUPERVISIÓN HUMANA

- Los sistemas de IA de alto riesgo deben ser vigilados por personas físicas
 - El objetivo es prevenir o minimizar riesgos para la salud, seguridad o derechos fundamentales
 - Las medidas de supervisión deben ser proporcionales a los riesgos y al nivel de autonomía del sistema
 - Las medidas pueden ser definidas por el proveedor o por el responsable del despliegue
 - Las personas encargadas de la supervisión deben entender las capacidades y limitaciones del sistema
 - Deben ser conscientes del sesgo de automatización y poder interpretar correctamente los resultados
 - Deben poder decidir no utilizar el sistema o intervenir en su funcionamiento

ARTÍCULO 15: PRECISIÓN, SOLIDEZ Y CIBERSEGURIDAD

- Los sistemas de IA de alto riesgo deben alcanzar un nivel adecuado de precisión, solidez y ciberseguridad
 - La Comisión fomentará el desarrollo de parámetros de referencia y metodologías de medición
- Los niveles de precisión se indicarán en las instrucciones de uso
- Los sistemas de IA de alto riesgo serán resistentes a errores, fallos o incoherencias
 - Se adoptarán medidas técnicas y organizativas
- Los sistemas de IA de alto riesgo serán resistentes a intentos de alteración por parte de terceros no autorizados
 - Se utilizarán soluciones técnicas adecuadas para garantizar la ciberseguridad

www.croma.legal

sergio.dejuancreix@croma.legal | +34 693 296 432

carlos.garcia@croma.legal | +34 665 933 743

El contenido ha sido creado con el soporte de una herramienta de IA, pero revisado por nosotros. La información contenida en este documento es de carácter general y no constituye asesoramiento jurídico. Croma Legal no asume compromiso alguno de actualización o revisión de su contenido.