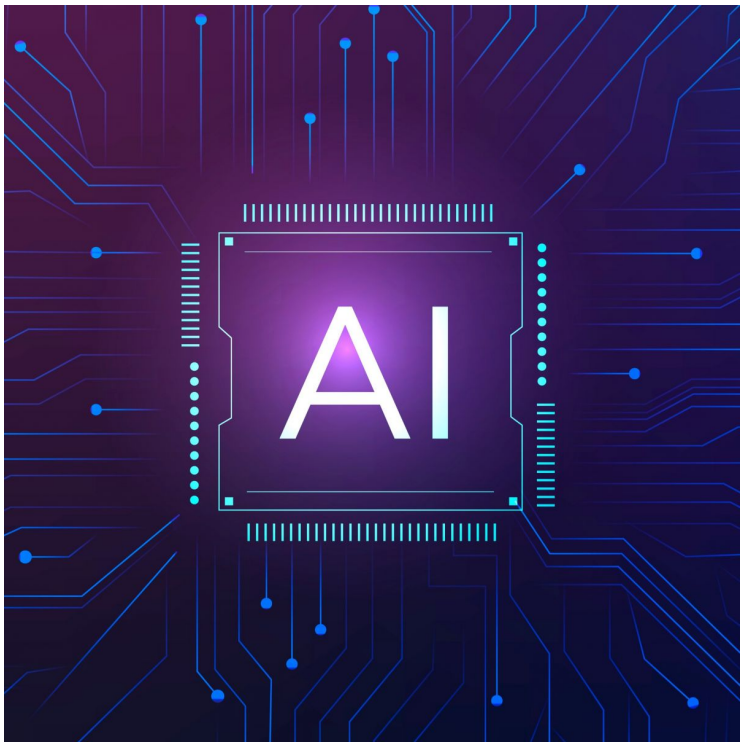
17/05/2024

Cómo adecuar tu empresa al Reglamento de inteligencia artificial: primeros pasos

Llegar tarde a su adecuación no debería ser una opción para las empresas si nos fijamos en su régimen sancionador, que fija sanciones de hasta 35 millones de euros o hasta un 7 % de la facturación anual



Tras la aprobación del Reglamento Europeo de Inteligencia Artificial (RIA), han comenzado a correr los plazos de entrada en vigor, **y casi todas las obligaciones del RIA que aplican con carácter general a la mayoría de las empresas** y organismos públicos serán exigibles en 24 meses desde su aprobación.

Dos años no es tanto tiempo. Ya aprendimos lo que significa enfrentarse a un proceso de adecuación normativa como el RGPD hace unos años. En el caso del RIA **hablamos también de una norma con enorme calado en gran parte de los procesos de muchas organizaciones.** Llegar tarde a su adecuación no debería ser una opción para las empresas si nos fijamos en su régimen sancionador, que fija sanciones de hasta 35 millones de euros o hasta un 7% de la facturación anual.

Algunas entidades pioneras ya han comenzado esa andadura, estableciendo un adecuado marco de gobierno interno **y un marco de control para acompañar la explotación de las posibilidades de la inteligencia artificial con un uso responsable de la misma** y alineado a los requisitos regulatorios del RIA.

Últimamente me preguntan mucho: “¿Por dónde debemos empezar a adecuar la empresa al RIA?”. A continuación, indico algunas claves que considero nucleares en ese proyecto de adecuación al nuevo Reglamento:

Levantamiento e inventario de IAs: realizar un inventario de qué IAs se están utilizando, dónde y para qué en una gran organización es todo un reto en sí mismo. Para ello, conviene definir una metodología de identificación y descubrimiento, una ficha-registro mínima que permita tener una primera información sobre dicha IA, así como un sistema de actualización del inventario. Además, es necesario considerar que habrá IAs desarrolladas internamente, IAs compradas a proveedores y que corren en infraestructura de la empresa, IAs contratadas a proveedores y que corren en su infraestructura, así como proveedores que nos prestan diversos servicios utilizando a su vez IAs propias o de terceros y que ni siquiera sabemos.

Modelo de Gobierno de IA: el RIA no establece obligaciones concretas sobre cómo organizarse en una empresa para cumplir sus requerimientos, ni tampoco regula una figura del tipo **Chief IA Compliance Officer**. Por ello, son las organizaciones las que tienen que establecer sus propios mecanismos internos de Gobierno, definiendo los roles y competencias de las funciones que más afectadas se verán en el impulso y supervisión del cumplimiento de las obligaciones del RIA, tales como DPO, Compliance, Jurídico, CISO, IT, Riesgos, Auditoría, RRHH, etc.

Identificación de las palancas existentes en la entidad: el objetivo es establecer una política de adecuación eficaz al RIA sin partir de cero. **Se podrán aprovechar los mecanismos y procesos que ya existen en sus sistemas de cumplimiento, de privacidad y de ciberseguridad** (Políticas, Privacy by design, Gestión de incidentes de seguridad, Diligencia debida con terceros y proveedores, programas de formación anuales, etc). Todos ellos deberán ser revisados para alinearlos a los nuevos requisitos del RIA, pero su función primigenia será una buena base sobre la que construir el modelo de cumplimiento del RIA.

Modelos de "triaje" y metodología de riesgos: comprender el RIA no es fácil, y las compañías tendrán diversas obligaciones dependiendo del rol que desempeñen ante una IA (si desarrollan el modelo, si lo entrenan, si la compran, si la explotan, etc.). Por ello es fundamental trabajar ya metodologías de "triaje" para comprender el rol de la organización ante cada proyecto IA al que se enfrenten, y por supuesto, **definir una metodología de riesgos para aplicarla de manera constante a cada IA y determinar el impacto que pudiera tener en los derechos de las personas afectadas por su operativa.**

> "Hay muchos más aspectos en los que habrá que trabajar y que iremos desarrollando a lo largo de los próximos meses. Empecemos por estos para dar los primeros pasos de adecuación al RIA"

Concienciación: aunque alcanzar procesos maduros de cumplimiento del RIA llevarán tiempo, es fundamental realizar una labor de concienciación sobre**el impacto que una norma** así va a tener, al menos en 3 escalas: a) a la Dirección de la compañía para que tenga una visión general de este nuevo marco regulatorio, b) **a las áreas que van a tener una función esencial en el cumplimiento del RIA (Compliance, Privacidad, Seguridad, IT, Compras, etc.)** y c) al resto de usuarios de la organización para comenzar a cultivar una cultura colectiva de uso responsable de la IA.

Descartar usos prohibidos: algo inmediato que debería hacerse es comprobar que ninguno de los casos de uso que ya se estén desarrollando en la organización están incluidos en el listado de usos prohibidos que la norma establece.
Hay muchos más aspectos en los que habrá que trabajar y que iremos desarrollando a lo largo de los próximos meses, pero empecemos por estos para dar los primeros pasos de adecuación al RIA con garantías.

Y será mejor empezar ya.

Fuente: www.elconfidencial.com

LINK DE LA NOTICIA