NEWSLETTER

Subcomité de Seguridad

07 de abril de 2025| nº 19

Noticias de Ciberseguridad

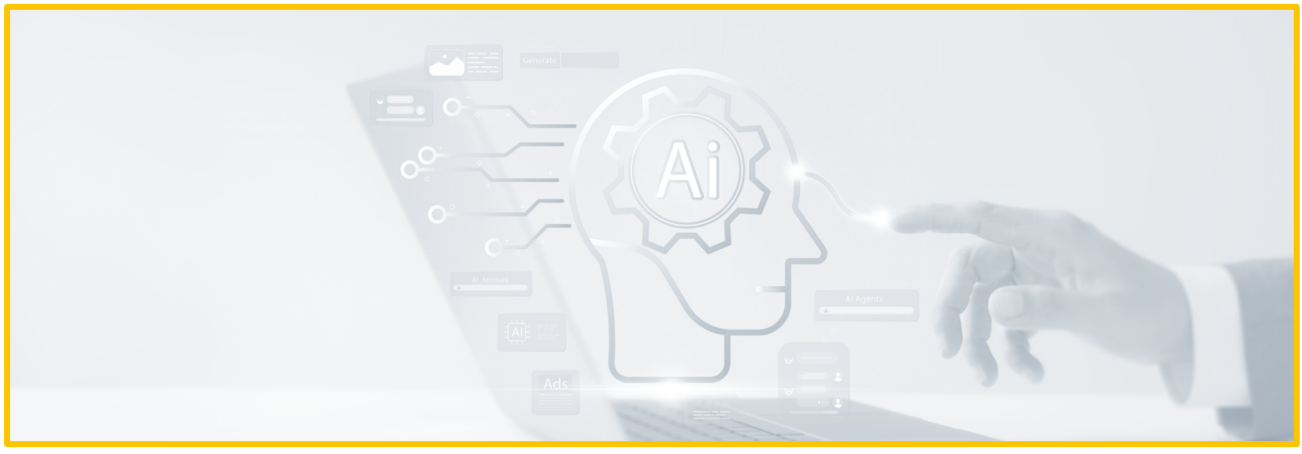
España impulsa una nueva legislación para la gobernanza ética de la Inteligencia Artificial

El Gobierno de España ha aprobado el anteproyecto de ley de gobernanza de la Inteligencia Artificial (IA), una medida para adaptar la legislación española al Reglamento (UE) 2024/1689.
Esta legislación pretende asegurar un uso de la IA que sea ético, inclusivo y beneficioso, alineando las normativas nacionales con el citado reglamento.

El texto introduce mecanismos de supervisión y sanción frente a prácticas prohibidas —como la manipulación subliminal, la clasificación biométrica discriminatoria o la puntuación social— y establece obligaciones estrictas para los sistemas de alto riesgo, en ámbitos como la justicia, la salud, la educación o los servicios esenciales.

Las autoridades encargadas de vigilar los sistemas de alto riesgo serán las que por defecto ya estén supervisando al sector afectado cuando se trate de productos sujetos a legislación armonizada. Adicionalmente, serán competentes la Agencia Española de Protección de Datos (para sistemas de gestión de migraciones y asilo asociados a las Fuerzas y Cuerpos de Seguridad del Estado); el CGPJ para sistemas de IA en administración de justicia y la Junta Electoral Central (para sistemas de procesos electorales), entre otras.

Asimismo, se reconoce un nuevo derecho digital a la retirada provisional del mercado de sistemas de IA que hayan causado incidentes graves.



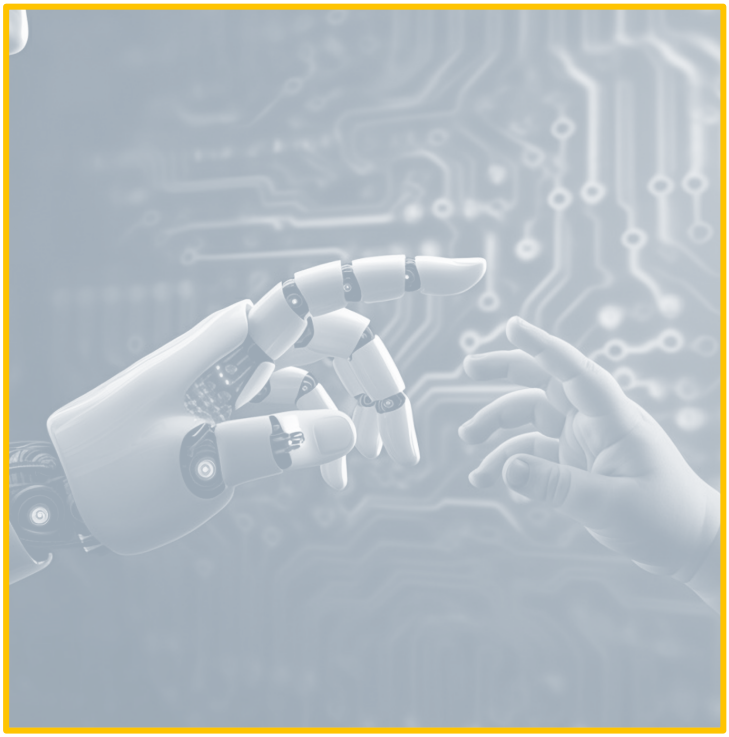
Ver noticia

Publicación del tercer borrador del Código de buenas prácticas de modelos IA de uso general

La adhesión a este futuro código va a permitir a los proveedores de modelos IA de propósito general, y a los proveedores de modelos IA de propósito general con riesgo sistémico, la presunción del cumplimiento de sus obligaciones establecidas en el Reglamento de Inteligencia Artificial.

Este tercer borrador se presentó el pasado 11 de marzo partiendo de las observaciones efectuadas sobre el segundo proyecto. Tras la finalización de las alegaciones al tercer borrador el 30 de marzo, se espera que el Código definitivo esté listo en mayo, siguiendo con lo previsto en el Reglamento de Inteligencia Artificial.

Las dos primeras secciones del Código detallan las obligaciones de transparencia y derechos de autor para todos los proveedores de modelos de IA de uso general, con notables exenciones de las obligaciones de transparencia para los proveedores de determinados modelos de código abierto en consonancia con la Ley de IA.
La tercera sección del Código destinada a los proveedores de los modelos de IA de uso general con riesgos sistémicos describe las medidas para la evaluación y mitigación del riesgo sistémico, incluidas las evaluaciones de modelos, la notificación de incidentes y las obligaciones de ciberseguridad.



Ver más

Informe ENISA NIS360 para evaluar la madurez de la ciberseguridad de los sectores NIS2

En marzo, la Agencia Europea para la Ciberseguridad (ENISA) presentó el NIS360, una nueva herramienta para evaluar la madurez y criticidad de los sectores clave bajo la Directiva NIS2. Este recurso permite realizar análisis comparativos y detallados, apoyando a las autoridades y agencias nacionales en la implementación efectiva de la Directiva para mejorar la ciberresiliencia en toda la Unión Europea.

El NIS360 busca proporcionar una perspectiva integral del estado de la ciberseguridad, facilitando así la elaboración de políticas y estrategias nacionales y comunitarias. Destaca, además, la importancia de incrementar la colaboración entre distintos sectores y alinear los requisitos transfronterizos, junto con el desarrollo de directrices sectoriales durante la adaptación de la NIS2.

Uno de los seis sectores del NIS que se encuentran dentro de la zona de riesgo son las Administraciones Públicas, al ser un objetivo principal para el hacktivismo y las operaciones de nexo entre estados, el sector debe apuntar a fortalecer sus capacidades de ciberseguridad aprovechando el conocido como Reglamento de Cibersolidaridad de la UE y explorando modelos de servicios compartidos entre entidades del sector en áreas comunes, como las billeteras digitales. Otros sectores como la electricidad, las telecomunicaciones y la banca muestran altos niveles de madurez y cooperación público-privada, y otros, como las infraestructuras digitales y la gestión de servicios TIC, enfrentan desafíos significativos por su diversidad y carácter transfronterizo.

Ver noticia