NEWSLETTER

Subcomité de Seguridad

13 de enero 2026 | nº 26

1 Noticias de Ciberseguridad

La AEPD publica su Política interna de uso de Inteligencia Artificial

La Agencia Española de Protección de Datos (AEPD) ha publicado su **Política general interna para el uso de IA generativa,** que, formando parte de su Política de Información, define las directrices de implementación, gobernanza y uso responsable de estos sistemas en sus procesos administrativos.

Es la primera política interna de este tipo en el sector público y posiciona a la AEPD como referente en un uso seguro y responsable de la IA. La iniciativa se integra en su Plan Estratégico 2025–2030, con una apuesta por un enfoque de IA first donde estos sistemas deben integrarse como un proceso normal en el funcionamiento de las administraciones públicas, al igual que en otros sectores. El documento incluye casos de uso, análisis de riesgos y un marco operativo que establece criterios sobre tratamiento de datos, transparencia, explicabilidad, protección de derechos y supervisión humana, además de procedimientos de revisión y gestión de incidentes.

La AEPD precisa que la Política se limita al uso interno y no supone evaluación ni certificación vinculada al Reglamento de Inteligencia Artificial, previendo una mejora continua para adaptarse a avances tecnológicos y cambios normativos. Además, como complemento a esta política la AEPD ha publicado un **anexo práctico** para su aplicación con casos de uso concretos, análisis de riesgos en función del sistema implementado, medidas de mitigación, así como un plan de despliegue estructurado para alcanzar los objetivos del modelo de gobernanza.



https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/agencia-publica-politica-interna-uso-inteligencia-artificial
https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/desarrollo-practico-politica-general-interna-para-uso-ia-generativa-en-aepd

La AESIA difunde guías para el uso de Inteligencia Artificial

La Agencia Española de Supervisión de Inteligencia Artificial (AESIA) ha publicado una serie de **recursos y guías de apoyo orientados a facilitar la implementación y el cumplimiento de la normativa europea de Inteligencia Artificial.** Estos materiales se difunden sin perjuicio de las guías técnicas que está elaborando la Comisión Europea, cuyo objetivo es asegurar una aplicación consistente de la regulación en todos los Estados miembros.

Los documentos se han desarrollado en el marco del piloto español de sandbox regulatorio de IA, mediante un trabajo colaborativo entre los participantes del piloto, asistencias técnicas, potenciales autoridades nacionales competentes y el grupo asesor de expertos del sandbox. El resultado es un conjunto de recomendaciones prácticas diseñadas para ayudar a organizaciones públicas y privadas a aterrizar obligaciones y requisitos regulatorios en medidas operativas.



La AESIA subraya que estas guías no tienen carácter vinculante y no sustituyen ni desarrollan la normativa aplicable. No obstante, ofrecen orientaciones alineadas con el marco regulatorio europeo, especialmente relevantes mientras se completan las normas armonizadas y directrices de aplicación comunes. Se prevé un proceso permanente de evaluación y revisión, con actualizaciones periódicas en función de la evolución de estándares y de las directrices de la Comisión Europea, y una revisión adicional cuando se apruebe el denominado Ómnibus digital que modifica el Reglamento de Inteligencia Artificial. https://aesia.digital.gob.es/es/guias

Enfoque de protección de datos desde el diseño y por defecto para los monederos de identidad digital

El Supervisor Europeo de Protección de Datos (SEPD) ha publicado el TechDispatch n.º 3/2025 sobre monederos de identidad digital, una tecnología que permite almacenar credenciales e identidad en un repositorio digital para acceder a servicios físicos y online.

El documento identifica riesgos clave con impacto directo en ciberseguridad y privacidad: accesos no autorizados (exposición de datos, incluso sensibles), sobredivulgación de información a los verificadores y vinculación de transacciones, que puede facilitar seguimiento y perfilado. Para mitigarlos, se proponen medidas como el uso de entornos seguros físicamente separados, así como entornos de ejecución confiables, que se utilizan para aislar las operaciones criptográficas y almacenar datos confidenciales, y las credenciales anónimas, que permiten autenticación sin identificación cuando no es necesaria. Finalmente, se analiza el Reglamento eIDAS 2 y la Cartera Europea de Identidad Digital, evaluando su capacidad para integrarse en este marco y reducir los riesgos de protección de datos antes de su despliegue previsto para 2026.

https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-12-15-techdispatch-32025-digital-identity-wallets_en