NEWSLETTER

Subcomité de Seguridad

9 de junio de 2026 | nº 31

CTEAJE
Comité Técnico Estatal de la Administración Judicial Electrónica

Noticias de Ciberseguridad

Nuevo impulso europeo a la soberanía tecnológica

La Comisión Europea ha presentado el nuevo Paquete de Soberanía Tecnológica Europea, una iniciativa destinada a reforzar la autonomía y la resiliencia digital de la Unión Europea en ámbitos estratégicos como los semiconductores, la inteligencia artificial, la computación en la nube y el software de código abierto.

El paquete incluye la propuesta de una nueva Ley de Chips 2.0, la Ley de Desarrollo de la Nube y la IA, una Estrategia Europea de Código Abierto y una hoja de ruta para la digitalización y el uso de la inteligencia artificial en el sector energético.

Con estas medidas, la Unión Europea busca reducir su dependencia de proveedores tecnológicos externos para tecnologías digitales esenciales. La iniciativa responde, además, al creciente aumento de la demanda de capacidad informática derivada de la expansión de la inteligencia artificial y pretende asegurar que Europa pueda desarrollar, desplegar y asegurar las tecnologías de las que dependen los europeos.



Ver más

Noticias en Ciberseguridad

La Comisión Europea impulsa nuevas directrices sobre transparencia y clasificación de sistemas de IA de alto riesgo

La Comisión Europea ha abierto durante el mes de mayo dos procesos de consulta pública vinculados a la aplicación de la Ley de Inteligencia Artificial (AI Act), centrados en las obligaciones de transparencia y en la clasificación de los sistemas de IA de alto riesgo.

Por un lado, la Comisión ha publicado un borrador de directrices sobre las obligaciones de transparencia que serán aplicables a partir del 2 de agosto de 2026. Estas medidas prevén que los ciudadanos sean informados cuando interactúen con sistemas de inteligencia artificial o cuando estén expuestos a determinados contenidos generados o manipulados mediante IA. Asimismo, se establecen requisitos de identificación para contenidos sintéticos, deepfakes, sistemas de reconocimiento de emociones y determinadas aplicaciones de categorización biométrica.

De forma paralela, la Comisión ha sometido a consulta un borrador de directrices destinado a aclarar los criterios de clasificación de los sistemas de IA de alto riesgo. El documento incorpora ejemplos prácticos para ayudar a proveedores e implementadores a determinar si una aplicación concreta entra dentro de las categorías consideradas de alto riesgo por la normativa europea, entre los que se encuentran ejemplos de sistemas de IA utilizados en el ámbito de la Administración de Justicia. Para facilitar esta tarea, la Comisión ha habilitado una web de acceso rápido a resúmenes y ejemplos del borrador de las Directrices sobre la clasificación de los sistemas de IA de alto riesgo en virtud de la Ley de IA.



Directrices Sistemas de IA de alto riesgo

Directrices de transparencia

Noticias en Ciberseguridad

ENISA publica su informe anual NIS360 que evalúa la madurez de la ciberseguridad de los sectores críticos de la UE

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha publicado la edición 2026 de su informe NIS360, una herramienta que ayuda a evaluar el nivel de madurez de la ciberseguridad de los sectores críticos incluidos en el ámbito de la Directiva NIS2.

Entre sus principales conclusiones, el informe sitúa a las Administraciones Públicas dentro de la denominada "zona de riesgo", junto a sectores como salud, ferrocarriles, transporte marítimo, servicios de gestión TIC, espacio, agua potable y aguas residuales.



El sector de las Administraciones Públicas aún se encuentra en una etapa temprana de madurez en ciberseguridad, con una gestión de riesgos reactiva y desigual, y una colaboración limitada entre entidades. El sector se caracteriza por la presencia de administraciones centrales, regionales y locales, así como municipios de diversos tamaños, que enfrentan diferentes limitaciones de recursos y experiencia, lo que se traduce en variaciones en los niveles de madurez.

ENISA destaca que, aunque la madurez general de la ciberseguridad en Europa continúa mejorando, gracias a la implantación de la NIS2 y a la inversión en ciberseguridad, persisten importantes desafíos relacionados con la falta de experiencia, conocimientos y recursos en ciberseguridad, así como la escasez de personal cualificado.

Ver más