NEWSLETTER

Subcomité de Seguridad

11 de septiembre | nº 33

1 Noticias de Ciberseguridad

La Comisión comienza a hacer cumplir las normas de la Ley de IA y los nuevos requisitos de transparencia

Desde el **2 de agosto de 2026**, la Oficina de IA de la Comisión Europea y las autoridades nacionales comienzan a hacer cumplir nuevas disposiciones de la Ley de IA. Los chatbots deberán informar cuando el usuario interactúe con una IA, mientras que los deepfakes y otros contenidos generados o modificados mediante inteligencia artificial tendrán que estar identificados, también mediante marcas legibles por máquina.

Las nuevas normas establecen además obligaciones para los proveedores de modelos de IA de uso general, especialmente para aquellos considerados de riesgo sistémico, que deberán adoptar medidas adicionales frente a amenazas como la ciberdelincuencia, la manipulación o la pérdida de control de los sistemas. La Comisión también ha puesto en marcha herramientas para denunciar posibles infracciones y ha anunciado que más de 180 organizaciones han firmado el Código de buenas prácticas sobre transparencia.

La aplicación de las normas para sistemas de IA de alto riesgo, conforme al Reglamento Ómnibus, queda aplazada hasta diciembre de 2027, mientras que algunas disposiciones específicas para productos regulados entrarán en vigor en agosto de 2028.

La Comisión comienza a hacer cumplir las normas de la Ley de IA y los nuevos requisitos de transparencia.



2 Noticias en Ciberseguridad

El Centro Criptológico Nacional advierte de los graves riesgos que supone la amenaza cuántica para la seguridad de la información

El Centro Criptológico Nacional (CCN) ha publicado el **Informe CCN-TEC 009 BP/37 Recomendaciones para una transición postcuántica segura**, que orienta a las organizaciones en la migración ordenada hacia sistemas resistentes a la computación cuántica. El documento advierte de que un ordenador cuántico con capacidad para romper la criptografía actual podría aparecer alrededor de 2035, poniendo en riesgo sistemas de cifrado y firma electrónica basados en criptografía asimétrica.

El CCN establece estos plazos de migración según el nivel de riesgo:

- **Riesgo alto**: migración completa antes del **31 de diciembre de 2030**.
- **Riesgo medio**: migración antes del **31 de diciembre de 2035**.
- **Riesgo bajo:** migración en la medida de lo posible.

El informe recomienda comenzar cuanto antes la identificación de sistemas criptográficos, la adquisición de soluciones, su despliegue y puesta en marcha. Entre los principales riesgos destaca el modelo "almacena ahora y descifra después", por el que información interceptada actualmente podría ser descifrada en el futuro, así como los largos plazos que puede requerir una migración completa.
Además, el documento aborda la gobernanza de la transición, la elaboración de un plan de migración, el uso de soluciones híbridas, encapsulados de claves y firmas digitales, e incluye un decálogo de buenas prácticas para facilitar una transición ordenada.
https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/13174-el-centro-criptologico-naciona…

3 Noticias en Ciberseguridad

La CNIL actualiza su herramienta de trazabilidad para modelos publicados en código abierto

La **CNIL** (autoridad francesa de protección de datos) ha actualizado **Genmod**, su herramienta para rastrear la genealogía de los modelos de IA de código abierto. Esta aplicación permite identificar tanto los **modelos de origen (antecesores)** como los **modelos derivados (descendientes)** de sistemas como LLaMA, Mistral Medium o Kimi K3.

La finalidad principal es mejorar la trazabilidad de los modelos de IA, especialmente para analizar cómo la posible memorización de datos personales puede propagarse entre modelos relacionados. Esto resulta relevante para evaluar el ejercicio de los derechos contemplados en el RGPD. La nueva versión de Genmod es más rápida, más fácil de usar y se mantiene actualizada automáticamente, facilitando el análisis de la genealogía y trazabilidad de los modelos de IA de código abierto.
IA: la CNIL actualiza su herramienta de trazabilidad para modelos publicados en código abierto | CN…

