NEWSLETTER

Subcomité de Seguridad

22 de julio| nº 32

CTEAJE
Comité Técnico Estatal de la Administración Judicial Electrónica

1 Noticias de Ciberseguridad

El CEPD publica nuevas directrices sobre anonimización, raspado web e IA generativa y culmina su guía sobre blockchain

El Comité Europeo de Protección de Datos (CEPD) ha publicado nuevas directrices sobre anonimización de datos, para determinar cuándo unos datos pueden considerarse realmente anónimos y, por tanto, quedar fuera del ámbito de aplicación del RGPD, y sobre raspado web (*web scra*ping) en el contexto de la IA generativa, con el objetivo de aclarar cómo deben aplicarse los requisitos del RGPD cuando se recopilan datos de internet para entrenar modelos de IA.

Las **directrices sobre anonimización** recuerdan que un dato es anónimo cuando no permite identificar, directa o indirectamente, a una persona física, teniendo en cuenta los medios razonablemente disponibles para quien acceda a la información y propone utilizar tres criterios para comprobar si los datos son anónimos: ningún aislamiento de registros, ninguna vinculación y ninguna inferencia.



La guía sobre el raspado web para el entrenamiento de **modelos de IA** aclara diversos aspectos de cumplimiento, incluida la base jurídica de dichas actividades y las condiciones en las que pueden tratarse categorías especiales de datos en este contexto, y destaca la importancia de la **transparencia, la minimización de datos y la aplicación de las medidas técnicas y organizativas** adecuadas para evitar la recogida y difusión de los datos personales.

1 Noticias en Ciberseguridad

Las directrices sobre anonimización y raspado web permanecerán en consulta pública hasta el 30 de octubre de 2026.

Asimismo, el CEPD ha adoptado la versión final de sus directrices sobre tecnologías *blockchain*, para ayudar a las organizaciones que utilizan tecnologías blockchain a cumplir con las exigencias del RGPD.

https://www.edpb.europa.eu/news/edpb-sheds-light-on-anonymisation-and-web-scraping-for-generative-ai-and-adopts-final-version_es

2 Noticias en Ciberseguridad

Ciberseguridad en la era de la IA de Frontera

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha publicado un **informe sobre la ciberseguridad en la era de la inteligencia artificial (IA) de frontera**, para apoyar a los proveedores de servicios y autoridades nacionales a desarrollar las capacidades operativas necesarias para hacer frente a amenazas que pueden ejecutarse a "velocidad de máquina", con ciclos de descubrimiento, explotación, movimiento lateral y exfiltración cada vez más automatizados y reducidos.

La Agencia advierte de que los modelos avanzados de inteligencia artificial están modificando el ritmo operativo de la ciberseguridad y obligan a revisar las capacidades de detección, gestión de vulnerabilidades, respuesta a incidentes y seguridad por diseño.

La publicación de **ENISA** conecta con el nuevo **Plan de Acción sobre Ciberseguridad e Inteligencia Artificial**, presentado por la Comisión Europea recientemente. Este plan busca promover el uso seguro y responsable de la IA avanzada, reforzar la ciberseguridad y la resiliencia europea y ampliar las capacidades de IA de Europa para la ciberseguridad.

En España, **INCIBE** ha publicado también recientemente un informe de **Medidas de ciberseguridad y ciberresiliencia ante modelos de IA de frontera**, que identifica y expone medidas como reducir el tiempo de respuesta, reforzar la identidad digital y el control de accesos, aprovechar la IA como herramienta defensiva, defensa perimetral más inteligente o automatizar la respuesta ante incidentes.

https://www.enisa.europa.eu/publications/enisas-view-on-cybersecurity-in-the-frontier-ai-era

https://www.incibe.es/incibe-cert/blog/medidas-de-ciberseguridad-y-ciberresiliencia-ante-modelos-de-ia-de-frontera

3 Noticias en Ciberseguridad

Nueva herramienta del CCN para medir el grado de madurez frente a la IA ofensiva

El **Centro Criptológico Nacional** (CCN) ha incorporado a su Portal de Gobernanza un nuevo cuestionario de autoevaluación para que los organismos del sector público y sus proveedores puedan medir su nivel de preparación frente a la IA ofensiva y priorizar acciones de mejora.

El cuestionario convierte las recomendaciones de la **guía de Buenas Prácticas frente al modelo de IA ofensiva**, publicada recientemente, en una evaluación práctica, medible y accionable. En la guía se advierte del cambio de paradigma que supone la inteligencia artificial para la ciberseguridad al reducir la complejidad técnica y permitir campañas muchísimo más rápidas, automatizadas y a gran escala. En este contexto, el CCN plantea una adaptación basada en cuatro fundamentos: volver a reforzar los controles básicos, como la gestión de identidades, la segmentación, la monitorización continua o el control de accesos; transformar los procesos IT para integrar la seguridad desde el diseño; construir sistemas resilientes y seguros por defecto; y utilizar la IA como una capacidad defensiva gobernada, con supervisión humana, trazabilidad y límites claros de actuación.

https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/13170-el-sector-publico-espanol-ya-puede-medir-su-grado-de-madurez-frente-a-la-ia-ofensiva-con-una-herramienta-del-centro-criptologico-nacional.html

