NEWSLETTER

Subcomité de Seguridad

17 de abril 2026| nº 29

Noticias de Ciberseguridad

Décalogo de Seguridad en la IA Agéntica

La IA agéntica, a diferencia de otros sistemas de inteligencia artificial, no solo genera respuestas o recomendaciones, sino que puede tomar decisiones, interactuar con herramientas y ejecutar acciones de forma autónoma. Esa capacidad amplía su utilidad, pero también eleva los riesgos.

Ante este escenario, el Decálogo de Seguridad en la IA Agéntica de ISMS Forum ofrece una guía práctica para ayudar a las organizaciones a abordar los retos de seguridad, control y gobernanza asociados a los agentes de IA, y a diseñar y desplegar estos sistemas de forma segura y responsable.

El documento plantea diez principios fundamentales que cubren todo el ciclo de vida del agente y su ecosistema: el inventario de agentes, la gestión de identidades y privilegios, la protección de datos, la aplicación de guardarraíles, la supervisión humana, la monitorización del comportamiento, la respuesta ante incidentes, la gobernanza de la IA, la gestión de riesgos y el control de la cadena de suministro.

El Decálogo ha sido contrastado y alineado con referentes internacionales clave en seguridad de la IA agéntica, como el OWASP Top 10 for Agentic Applications y el AI Agents Attack Matrix.



Más información
Ver noticia

El Consejo de la UE da luz verde a su posición para simplificar las reglas sobre inteligencia artificial

El Consejo de la Unión Europea ha acordado su posición negociadora sobre la propuesta para simplificar determinadas disposiciones del Reglamento de Inteligencia Artificial, en el marco del paquete legislativo "Omnibus VII" de simplificación normativa. El objetivo es aportar mayor seguridad jurídica, hacer las reglas más proporcionadas y favorecer una aplicación más homogénea en los Estados miembros.

Entre los principales cambios, el Consejo respalda aplazar la aplicación de algunas obligaciones para sistemas de IA de alto riesgo y fija nuevas fechas: el 2 de diciembre de 2027 para los sistemas autónomos de alto riesgo y el 2 de agosto de 2028 para los sistemas de alto riesgo integrados en productos. El mandato también incorpora una nueva prohibición sobre prácticas de IA relacionadas con la generación de contenido sexual o íntimo no consentido y de material de abuso sexual infantil.

La posición del Consejo también recupera la obligación de registrar en la base de datos de la UE ciertos sistemas considerados exentos de la categoría de alto riesgo, mantiene el criterio de estricta necesidad para tratar categorías especiales de datos personales con fines de detección y corrección de sesgos, y retrasa hasta el 2 de diciembre de 2027 el plazo para establecer entornos de pruebas regulatorios a nivel nacional.

Tras este acuerdo, la presidencia del Consejo iniciará las negociaciones con el Parlamento Europeo para cerrar el texto definitivo.



Ver noticia

El NIST alerta sobre los retos de monitorizar los sistemas de inteligencia artificial una vez desplegados

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha publicado un nuevo informe en el que examina las principales dificultades para monitorizar sistemas de inteligencia artificial ya desplegados en entornos reales. El documento subraya que la monitorización posterior al despliegue es fundamental para una adopción generalizada y segura de estas tecnologías.

El informe, elaborado a partir de talleres con profesionales y de una revisión de literatura especializada, identifica seis grandes áreas de seguimiento —funcionalidad, operación, factores humanos, seguridad, cumplimiento e impactos a gran escala— y señala desafíos como la degradación del rendimiento, la falta de estándares consolidados, la fragmentación de los mecanismos de intercambio de incidentes y la necesidad de equilibrar supervisión, innovación y capacidades técnicas.



Ver noticia