

La Comisión presenta el Plan de Acción de la UE sobre Ciberseguridad e Inteligencia Artificial

La Comisión Europea ha presentado un Plan de Acción para dar una respuesta estructurada a fin de abordar los riesgos y aprovechar las oportunidades que ofrecen los modelos avanzados de inteligencia artificial (IA) para la ciberseguridad.

Los nuevos modelos avanzados de IA están redefiniendo la ciberseguridad. La IA puede utilizarse indebidamente para detectar vulnerabilidades, automatizar ataques y aumentar la magnitud y la velocidad de los ciberincidentes a un ritmo sin precedentes.

Sobre la base del marco jurídico único de la UE en materia de IA y ciberseguridad, el Plan de Acción reunirá a los Estados miembros, la industria y las organizaciones de la UE para reforzar la ciberseguridad de nuestro entorno digital frente a las vulnerabilidades que plantea la IA avanzada.

Evaluación de los modelos de IA

Una seguridad eficaz requiere un conocimiento profundo de cómo las nuevas tecnologías pueden utilizarse correctamente, utilizarse indebidamente o explotarse. En virtud del Reglamento de Inteligencia Artificial, los modelos avanzados de IA deben evaluarse, y las medidas de mitigación deben sopesarse cuidadosamente antes de que dichos modelos se introduzcan en el mercado de la UE.

Con el fin de fomentar los conocimientos especializados en nuestro territorio, la Comisión pondrá en marcha una convocatoria específica para crear una capacidad de evaluación de la UE que abarque la ciberseguridad, y que se espera que esté operativa en 2027. Esta nueva capacidad contribuirá a la función reguladora de la Oficina de IA al reforzar la evaluación independiente de las capacidades y los riesgos de la IA a escala mundial.

Acceso a modelos avanzados de IA

Europa también necesita condiciones claras y transparentes para acceder a los sistemas de IA más avanzados.

La Comisión trabajará con la Agencia de la Unión Europea para la Ciberseguridad (ENISA) para definir unplan europeo para el acceso estructurado a capacidades avanzadas de IA para la ciberseguridad. Estas orientaciones servirán para que las organizaciones europeas pertinentes, tanto públicas como privadas, puedan acceder a modelos avanzados de IA.

Probar la IA aplicada a la ciberseguridad

ENISA y el Centro Común de Investigación de la Comisión crearán una plataforma segura para probar la IA aplicada a la ciberseguridad, lo que incluirá el uso de entornos simulados. Esto proporcionará conocimientos técnicos sobre el uso seguro de la IA a los operadores de sectores críticos, como el financiero, el energético, el sanitario, el del transporte y la administración pública.

Reforzar la ciberseguridad de la UE y subsanar las vulnerabilidades

La UE debe proteger sus infraestructuras críticas frente a las vulnerabilidades derivadas del posible uso indebido de estas tecnologías.

Tal como prevén las normas de ciberseguridad de la UE, las organizaciones deben reforzar las prácticas de ciberhigiene, las medidas de gestión de riesgos y los principios de «seguridad desde el diseño».

Las organizaciones deberían empezar a utilizar las capacidades de IA ya disponibles, también a través de modelos de código abierto, para identificar y subsanar las vulnerabilidades con mayor rapidez, así como para prevenir y responder a los ciberataques.

Para ayudar a las organizaciones en esta transición, la ENISA respaldará y facilitará las asociaciones entre las autoridades públicas, las empresas y las comunidades de código abierto en el ecosistema cibernético. Esto incluirá orientaciones, recomendaciones y buenas prácticas, así como una campaña para proteger el software de código abierto crítico.

Ampliar las capacidades europeas de IA para la ciberseguridad

Para estimular el crecimiento del mercado europeo, la Comisión pondrá en marcha el «Gran reto de la UE sobre IA para la ciberseguridad». Este concurso reunirá a empresas, investigadores y organizaciones con el objetivo de desarrollar soluciones de inteligencia artificial para la ciberseguridad.

La UE debe seguir invirtiendo en el desarrollo de sus propias capacidades soberanas avanzadas de IA, aprovechando la infraestructura proporcionada por las factorías de IA y las futuras gigafactorías. En este contexto, el futuro fondo de capital para el sector tecnológico europeo, anunciado en el Paquete de medidas de soberanía tecnológica, podría atraer inversión privada para ampliar las capacidades de IA autóctonas.

Contexto

La UE cuenta con un marco jurídico adecuado para abordar la ciberseguridad en la era de las tecnologías emergentes, como la inteligencia artificial. El Reglamento de IA exige evaluar y mitigar los riesgos derivados de los modelos de IA, mientras que el Código de buenas prácticas para la IA de uso general especifica con mayor detalle estos requisitos y facilita el cumplimiento por parte de los proveedores de modelos avanzados. Estas disposiciones empezarán a aplicarse el 2 de agosto de 2026.

El Reglamento de Ciberresiliencia (aplicable a finales de 2027) exige que los productos de hardware y software incorporen la seguridad desde el diseño. Además, la Directiva sobre redes y sistemas de información (SRI 2) tiene por objeto impulsar la seguridad de los sectores críticos como el transporte y la energía, junto con el Reglamento sobre la resiliencia operativa digital del sector financiero. El Reglamento de Cibersolidaridad refuerza las capacidades de la UE para detectar, prepararse y responder ante amenazas y ataques de ciberseguridad graves y a gran escala.

Fuente: La Comisión presenta el Plan de Acción de la UE sobre Ciberseguridad e Inteligencia Artificial - Representación en España