23/07/2026

La Comisión Europea publica su Plan de Acción sobre Ciberseguridad e Inteligencia Artificial



La publicación del Plan de Acción sobre Ciberseguridad e Inteligencia Artificial de la Comisión Europea llega cuando la conversación sobre IA empieza a abandonar la comodidad del debate regulatorio para entrar en el terreno de la seguridad real. Europa ha construido un marco normativo ambicioso: Reglamento de IA, NIS2, DORA, Ley de Ciberresiliencia, Ley de Solidaridad Cibernética. El diagnóstico, sin embargo, es claro: tener buenas reglas no garantiza estar preparado si las capacidades críticas se desarrollan fuera, si los atacantes avanzan más rápido y si las organizaciones siguen gestionando la ciberseguridad con procesos pensados para otra época.

Inteligencia artificial y ciberseguridad

La IA de frontera cambia la escala del problema. Permite detectar amenazas, analizar vulnerabilidades, priorizar riesgos y responder con una velocidad imposible para los equipos humanos trabajando solos. Pero esas mismas capacidades también pueden automatizar ataques, abaratar operaciones criminales, mejorar campañas de phishing, acelerar la explotación de vulnerabilidades y reducir la barrera técnica de entrada para actores menos sofisticados. La cuestión ya no es si la IA tendrá impacto en la ciberseguridad. La cuestión es quién va a usarla antes y con qué controles.

El plan de la Comisión acierta al situar el problema en tres planos. El primero es la evaluación de los modelos avanzados antes de que lleguen al mercado o se desplieguen en entornos sensibles. No basta con confiar en declaraciones de proveedores. Si un modelo puede ayudar a explotar sistemas, descubrir vulnerabilidades o generar capacidades ofensivas, Europa necesita capacidad propia para medir ese riesgo y entender qué está poniendo en circulación. Esta es una discusión de cumplimiento, pero también de soberanía técnica. Una autoridad que no puede evaluar lo que supervisa acaba dependiendo de quien fabrica la tecnología.

El segundo plano es el acceso. Muchas capacidades avanzadas están en manos de proveedores no europeos y sujetas a decisiones poco transparentes: quién accede, con qué límites, bajo qué criterios y durante cuánto tiempo. Puede ser razonable restringir el acceso por motivos de seguridad, pero no que operadores críticos, autoridades públicas o proveedores europeos de ciberseguridad dependan de procesos opacos para proteger infraestructuras esenciales. El Blueprint europeo que se anuncia junto con ENISA puede ser relevante si ordena ese acceso sin burocratizarlo.

El tercer plano es operativo: probar antes de desplegar. La idea de plataformas seguras y cyber ranges para testar IA en casos reales de ciberseguridad es acertada porque no todo modelo útil en laboratorio funciona en una organización crítica. Hay que saber cómo se comporta ante falsos positivos, incidentes complejos, sistemas heredados, restricciones regulatorias y datos sensibles. La IA aplicada a ciberseguridad no puede entrar en producción como una promesa comercial.

Descubrir vulnerabilidades

Pero el mensaje más importante del documento está en algo más básico: la velocidad. La Comisión insiste en que la IA está cambiando la economía del descubrimiento de vulnerabilidades. Los atacantes podrán encontrar más fallos, antes y con menos coste. Si el cuello de botella sigue siendo la remediación, el parcheo y la coordinación interna, el desequilibrio se ampliará. Muchas empresas no pierden la batalla por falta de herramientas, sino por procesos lentos, inventarios incompletos, dependencias no controladas y decisiones tardías.

Por eso el plan conecta IA con NIS2, DORA y la Ley de Ciberresiliencia. No se trata de añadir otra capa regulatoria, sino de hacer funcionar los fundamentos: gestión de riesgos, gobierno de proveedores, seguridad por diseño, gestión de vulnerabilidades, continuidad, respuesta a incidentes y responsabilidad de los órganos de dirección. En la era de la IA, esos fundamentos dejan de ser una lista de cumplimiento y se convierten en capacidad competitiva. La empresa que no pueda parchear rápido, priorizar bien y entender su exposición real será más vulnerable, aunque tenga políticas formalmente correctas.

También es acertado que la Comisión mire al software de código abierto. Buena parte de la economía digital se apoya en componentes mantenidos por comunidades pequeñas, a veces sin recursos suficientes, pero presentes en infraestructuras críticas. Si la IA acelera el descubrimiento de vulnerabilidades en esos componentes, Europa debe ayudar a acelerar también su mantenimiento, patrocinio y remediación.

La gran pregunta es si Europa será capaz de ejecutar al ritmo que exige el riesgo. El documento habla de evaluación, acceso, pruebas, formación, inversión, AI Factories, capacidades soberanas y cooperación internacional. Pero el éxito dependerá de que las organizaciones entiendan que la IA en ciberseguridad no es una herramienta más, sino un cambio de modelo. Obliga a revisar la arquitectura de defensa, la relación con proveedores, la gestión de vulnerabilidades, el papel del consejo y la preparación de los equipos.

Europa ha demostrado capacidad para regular. Ahora tiene que demostrar capacidad para desplegar. En ciberseguridad, llegar tarde rara vez sale gratis. Y en la era de la IA, la distancia entre llegar tarde y no llegar puede medirse en días, no en años.

Fuente: La Comisión Europea publica su Plan de Acción sobre Ciberseguridad e Inteligencia Artificial - El Derecho - Compliance