

En virtud de la autoridad que me confiere la Constitución y las leyes de los Estados Unidos de América como Presidente, por la presente se ordena:

Sección 1. Propósito . Estados Unidos continúa liderando el mundo en Inteligencia Artificial (IA) gracias al enorme talento e innovación de nuestra industria de IA, y porque nos negamos a frenar esta innovación con regulaciones excesivamente onerosas. Mi administración ha impulsado un crecimiento tecnológico y una inversión económica extraordinarios en IA al eliminar las trabas burocráticas que la administración anterior imponía a los desarrolladores e investigadores de IA estadounidenses, y al fomentar la innovación en IA y acelerar su adopción responsable en el gobierno y la industria.

Las capacidades avanzadas de IA fortalecen a nuestra nación, pero también plantean nuevas consideraciones de seguridad nacional que requieren una acción coordinada entre los distintos departamentos y agencias del poder ejecutivo. A medida que estas capacidades evolucionen, mi administración seguirá colaborando estrechamente con la industria para garantizar que la mejor y más segura tecnología se implemente con rapidez para hacer frente a todas las amenazas a nuestro país. Continuaremos liderando una iniciativa de ciberseguridad que priorice a Estados Unidos y que fortalezca tanto nuestra seguridad nacional como nuestro liderazgo global en IA.

La política de Estados Unidos consiste en promover la innovación y la seguridad en inteligencia artificial mediante la colaboración con el sector privado para modernizar los sistemas de información gubernamentales y privados y fortalecerlos contra las amenazas externas; proteger el ingenio y la propiedad intelectual estadounidenses de la explotación y el robo por parte de adversarios; y cultivar las capacidades avanzadas de Estados Unidos basadas en inteligencia artificial.

Sec . 2. Actualización de los sistemas estadounidenses para IA avanzada . (a) Dentro de los 30 días siguientes a la fecha de esta orden, el Comité de Sistemas de Seguridad Nacional priorizará la ciberdefensa de los Sistemas de Seguridad Nacional, según se definen en 44 USC 3552(b)(6)(A), tomando medidas apropiadas y expeditas de conformidad con el propósito de esta orden.

(b) Dentro de los 30 días siguientes a la fecha de esta orden, el Secretario de Guerra deberá priorizar la ciberdefensa de los sistemas de información del Departamento de Guerra mediante la adopción de medidas apropiadas y expeditas de conformidad con el propósito de esta orden.

(c) Dentro de los 30 días siguientes a la fecha de esta orden, el Secretario de Seguridad Nacional, a través del Director de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), en consulta con el Director de la Oficina de Administración y Presupuesto (OMB), el Asistente del Presidente para Asuntos de Seguridad Nacional y el Director Nacional de Ciberseguridad, publicará Directivas Operativas Vinculantes y otras directrices según corresponda para:

(i) acelerar y priorizar la ciberdefensa de los sistemas de información civiles del Gobierno Federal con el fin de proteger las funciones vitales de nuestra Nación;

(ii) establecer o ampliar programas federales y servicios de ciberseguridad que mejoren las herramientas defensivas habilitadas por IA; y

(iii) facilitar el acceso a herramientas y servicios de ciberseguridad, incluidos, cuando corresponda, modelos de frontera cubierta para agencias, autoridades estatales y locales, y operadores de infraestructura crítica como hospitales rurales, bancos comunitarios y servicios públicos locales.

(d) Dentro de los 30 días siguientes a la fecha de esta orden, el Secretario del Tesoro, en consulta con el Director Nacional de Ciberseguridad, el Secretario de Guerra, a través del Director de la Agencia de Seguridad Nacional (NSA), y el Secretario de Seguridad Nacional, a través del Director de CISA, formará un centro de intercambio de información sobre ciberseguridad de IA, en colaboración voluntaria con la industria de IA y los operadores de infraestructura crítica, que coordine y resuelva los conflictos en el escaneo de vulnerabilidades de software, descubra y valide dichas vulnerabilidades, y coordine y priorice la remediación y distribución de parches de vulnerabilidad.

(e) Dentro de los 30 días siguientes a la fecha de esta orden, el Director de la OMB, en coordinación con el Director Nacional de Ciberseguridad y el Director de CISA, determinará si algún programa de subvenciones federales dispone de fondos pertinentes que puedan dirigirse a los solicitantes que desarrollen sistemas avanzados de detección de vulnerabilidades de IA.

(f) Dentro de los 60 días siguientes a la fecha de esta orden, el Director de la Oficina de Gestión de Personal deberá ampliar las vías de contratación y colocación de especialistas en ciberseguridad de la información de la Fuerza Tecnológica de los Estados Unidos.

Sección 3. Despliegue del Modelo de Frontera Segura . Dentro de los 60 días siguientes a la fecha de esta orden, el Secretario del Tesoro, el Secretario de Guerra, a través del Director de la NSA, y el Secretario de Seguridad Nacional, a través del Director de la CISA, en consulta con el Jefe de Gabinete de la Casa Blanca, a través del Director Nacional de Ciberseguridad, el Asistente del Presidente para Ciencia y Tecnología (APST), y el Secretario de Comercio, a través del Director del Instituto Nacional de Estándares y Tecnología, y en coordinación con otros organismos, según corresponda, deberán:

(a) desarrollar y mantener un proceso de evaluación comparativa clasificado para valorar las capacidades cibernéticas avanzadas de los modelos de IA y determinar el umbral a partir del cual un modelo de IA debe ser designado como un “modelo de frontera cubierta” para los fines de esta orden, compartiendo dichas evaluaciones con los desarrolladores e investigadores de IA según corresponda. Dicha determinación la realizará el Director de la NSA, en consulta con el Director Nacional de Ciberseguridad, el APST, el Director de CISA y otros representantes del Departamento de Guerra, según corresponda.

b) diseñar un marco voluntario con desarrolladores de IA a través del cual los desarrolladores puedan:

(i) involucrar al Gobierno Federal para determinar si el/los modelo(s) en desarrollo cumplen con la designación de “modelo de frontera cubierta”;

(ii) proporcionar al Gobierno Federal acceso a modelos fronterizos cubiertos, sujetos a los requisitos apropiados de confidencialidad, ciberseguridad, riesgo interno y protección de la propiedad intelectual, uso y no divulgación, por un período de hasta 30 días antes de que planeen divulgar dichos modelos a otros socios de confianza; y

(iii) colaborar con el Gobierno Federal para seleccionar socios de confianza que tendrán acceso temprano a modelos fronterizos cubiertos para promover la innovación segura y fortalecer la ciberseguridad de la infraestructura crítica.

(c) Nada de lo dispuesto en esta sección se interpretará como una autorización para la creación de un requisito obligatorio de licencia, autorización previa o permiso gubernamental para el desarrollo, publicación, lanzamiento o distribución de nuevos modelos de IA, incluidos los modelos de vanguardia.

Sección 4. Protección contra los delincuentes . El Fiscal General priorizará la aplicación de los artículos 1028, 1030 y 1343 del Título 18 del Código de los Estados Unidos, así como de todas las demás leyes penales federales aplicables, contra cualquier persona que utilice inteligencia artificial para acceder ilegalmente a un ordenador o dañarlo sin autorización, o que utilice inteligencia artificial durante dicho acceso ilegal para cometer cualquier otro delito. Esto incluye la violación de cualquier sistema de tecnología de la información público o privado, o el empleo de agentes de inteligencia artificial para acceder ilegalmente a datos o información que posteriormente se utilicen con fines delictivos o ilícitos.

Sección 5. Disposiciones generales . (a) Nada de lo dispuesto en esta orden se interpretará en el sentido de menoscabar o afectar de otro modo:

(i) la autoridad otorgada por ley a un departamento u organismo ejecutivo, o a su titular; o

(ii) las funciones del Director de la Oficina de Administración y Presupuesto relacionadas con propuestas presupuestarias, administrativas o legislativas.

(b) Esta orden se implementará de conformidad con la ley aplicable y con sujeción a la disponibilidad de asignaciones presupuestarias.

(c) Esta orden no tiene la intención de crear, ni crea, ningún derecho o beneficio, sustantivo o procesal, exigible por ley o por equidad por ninguna parte contra los Estados Unidos, sus departamentos, agencias o entidades, sus funcionarios, empleados o agentes, o cualquier otra persona.

(d) Los costos de publicación de esta orden correrán a cargo del Departamento de Guerra.

DONALD J. TRUMP

LA CASA BLANCA,

2 de junio de 2026.