

Seguridad para la innovación en IA a escala

Seguridad para IA con Cisco AI Defense

La adopción de la IA se está acelerando, pero también los riesgos. Las empresas se enfrentan a un nuevo repertorio de amenazas que incluye desde IA en la sombra hasta ataques antagónicos. Conscientes de ello, en NTT DATA hemos llegado a un acuerdo estratégico con Cisco y, conjuntamente, hemos desarrollado un enfoque integrado para la seguridad de la IA. Nuestros servicios integrales de seguridad, unidos a la plataforma AI Defense de Cisco, ofrecen visibilidad, protección y garantías en todo el ciclo de vida de la IA.

Nuestra colaboración ayuda a las empresas a innovar en IA con seguridad y confianza.

Puede que estés en pleno proceso de adopción de la IA, pero que los sesgos, las fugas de datos y los ataques te frenen en el proceso. Garantizar el cumplimiento y ganarte la confianza de las partes interesadas sigue siendo algo difícil. Por eso, te ofrecemos las defensas nativas de IA de Cisco, que se combinan con nuestros marcos de riesgo y cumplimiento de IA para

reducir los riesgos normativos y de reputación. Te ayudamos a generar confianza en tus sistemas de IA desde el principio, integrando medidas de gobernanza, garantía y protección durante la ejecución para que puedas innovar de forma segura y a escala.

Cobertura integral

NTT DATA protege todo el ciclo de vida de la IA (diseño, desarrollo, despliegue y monitorización) y Cisco AI Defense protege las aplicaciones con IA integrada y los usos de IA en la sombra en tiempo real.

Garantía completa

Con las medidas de protección técnicas integradas de Cisco —que incluyen protección contra la inyección de prompts, cortafuegos de IA y prevención de fugas de datos— y los servicios expertos de gobernanza de NTT DATA, podrás cumplir con los requisitos de la ISO/IEC 42001, del National Institute of Standards and Technology (NIST) AI RMF y del Reglamento de IA de la UE.

“Nuestras herramientas te ayudan a actuar con rapidez, escalar la innovación de IA con seguridad y evitar riesgos reputacionales, financieros y legales.

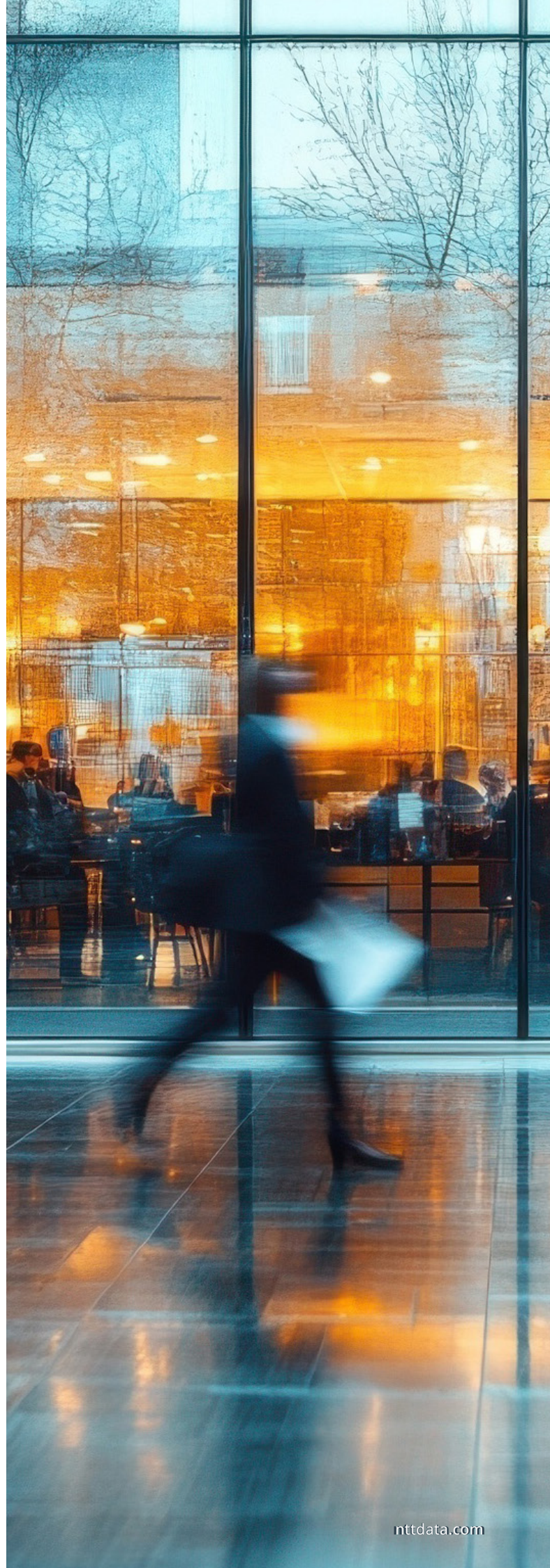
Nuestro enfoque integrado

Servicios de seguridad de NTT DATA para IA

- **Servicio de riesgo y cumplimiento de IA**
Evaluaciones y gobernanza del ciclo de vida de la IA alineadas con los estándares de la ISO/IEC 42001, el NIST AI RMF y otras normativas globales.
- **Servicio de protección de IA**
Defensa de modelos de IA, datos, aplicaciones, API y entornos de IA generativa.
- **Servicio de garantía de IA**
Pruebas continuas de penetración (red teaming), pruebas estructuradas de modelos de lenguaje a gran escala (LLM) y simulación de ataques antagónicos.
- **Laboratorio de IA seguro**
Un entorno de innovación y pruebas listo para usar, con integraciones de partners incorporadas.
- **Modelos de contratación**
Evaluaciones de preparación, adopción, servicios gestionados y pruebas de penetración bajo demanda.

Capacidades de defensa de IA de Cisco

- **Visibilidad de la IA en la nube**
Descubrimiento e inventario de cargas de trabajo, modelos y flujos de datos de IA en todos los entornos de nube.
- **Acceso a la IA**
Control del uso de los empleados para evitar fugas de datos.
- **Validación de modelos y aplicaciones de IA**
Identificación de vulnerabilidades en los modelos y aplicaciones de IA durante las primeras etapas de desarrollo.
- **Gestión de riesgos en la cadena de suministro de IA**
Protección de los modelos, los conjuntos de datos y las dependencias de fuentes externas frente a posibles vulneraciones.
- **Protección durante la ejecución**
Bloqueo de amenazas en tiempo real para cargas de trabajo de IA





Protege tu IA y tu negocio

Seguridad para la innovación a escala

Evalúa los casos de uso de IA y ejecuta pruebas de concepto (POC) seguras más rápido en el Secure AI Lab de NTT DATA, preconfigurado con capacidades de Cisco AI Defense. Así, reducirás el plazo de implementación de meses a semanas y acelerarás la creación de valor.

Campo de pruebas de IA experimental

El centro de excelencia (CoE) Secure AI Lab de NTT DATA ofrece un entorno experimental de seguridad para la IA listo para usar. En él, tu equipo podrá aprender, experimentar y definir rápidamente medidas de seguridad para los casos de uso de la IA en la empresa.

Cumplimiento y gobernanza de confianza

Los servicios de garantía de NTT DATA te ayudan a alinear tus programas de IA con estándares globales como el ISO/IEC 42001 y el NIST AI RMF. Gracias al modelo de amenazas de Cisco, que se actualiza continuamente, podrás reducir tus riesgos legales y evitar costosas penalizaciones o daños a tu reputación.

Descubre los riesgos ocultos de la IA

El servicio de pruebas de penetración de IA de NTT DATA combina herramientas líderes con un marco propio y una amplia biblioteca de casos de uso antagónicos prevalidados para el descubrimiento proactivo de riesgos ocultos y la garantía continuada.

Gestión de riesgos de IA en la sombra

Detectamos de forma proactiva el uso no autorizado de herramientas de IA y aplicamos políticas para prevenir las fugas de datos. Estas medidas reducen los riesgos ocultos al tiempo que facilitan la adopción segura de nuevas herramientas de IA.

Defensa en tiempo real para IA de producción

Protegemos tus cargas de trabajo de producción con IA aplicando medidas de seguridad multicapa, cortafuegos de IA y control inteligente del cumplimiento de las políticas.

[Ponte en contacto con nosotros](#) para obtener más información.

“Juntos, te ayudamos a adoptar la IA con seguridad, escalabilidad y resiliencia para impulsar la innovación y el crecimiento”.

Visita nttdata.com para saber más.

Somos un líder global en servicios digitales, tecnológicos y empresariales. Ayudamos a nuestros clientes a innovar, optimizar y transformarse para alcanzar el éxito. Somos Global Top Employer y contamos con expertos en más de 70 países, además de un sólido ecosistema de partners. NTT DATA forma parte del Grupo NTT.

