CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

Cloudflare AI Security Suite

Garantiza la seguridad de las interacciones con la IA mediante el control de los datos y la gestión de los riesgos a lo largo de todo el ciclo de vida de la IA.

Escala la IA con confianza

Los riesgos de la IA exigen una seguridad moderna

Tus equipos están utilizando la IA para innovar más rápido, pero esta práctica conlleva riesgos críticos para la seguridad. La tradicional estrategia de bloquear la IA o añadir soluciones específicas complejas está fallando porque frena la innovación e ignora la realidad:

- **El 85 % de los empleados** utiliza herramientas de IA antes de que el departamento de informática pueda verificarlas.[1]
- **El 93 % admite** haber facilitado datos de la empresa a la IA sin aprobación.[2]
- **El 63 % de las organizaciones afectadas** no tiene políticas de gobernanza de la IA.[1]

Aprende a proporcionar a tus equipos las herramientas necesarias, y a aprovechar las ventajas de la IA en términos de productividad, al tiempo que mantienes la seguridad y el control que requiere tu empresa.

Una plataforma unificada para proteger la IA generativa y la IA agéntica

Cloudflare proporciona una plataforma única para que tu organización adopte la IA con confianza. Ayudamos a los responsables de seguridad a gestionar los riesgos, a los equipos tecnológicos a aumentar la productividad y a los ingenieros de plataformas a desarrollar con seguridad, para garantizar que todos puedan innovar juntos de forma segura.

Empieza a utilizar Cloudflare AI Security Suite

Cloudflare AI Security Suite se ofrece en una plataforma unificada para proteger el uso de herramientas de IA en el espacio de trabajo y las aplicaciones de acceso público. Detecta elementos de Shadow AI, protege los modelos contra el uso indebido, garantiza el acceso de los agentes y evita la exposición de datos en las instrucciones, para que tu empresa pueda innovar con total seguridad y de forma eficaz, con mejor visibilidad y con un mayor control.

Amplía la visibilidad

en aplicaciones de IA, puntos finales de las API y conexiones de agentes de IA.

Mitiga los riesgos

con medidas de protección, control de postura y mitigación de amenazas en tiempo real.

Protege los datos

con protección de instrucciones y controles de acceso para empleados y agentes de IA.

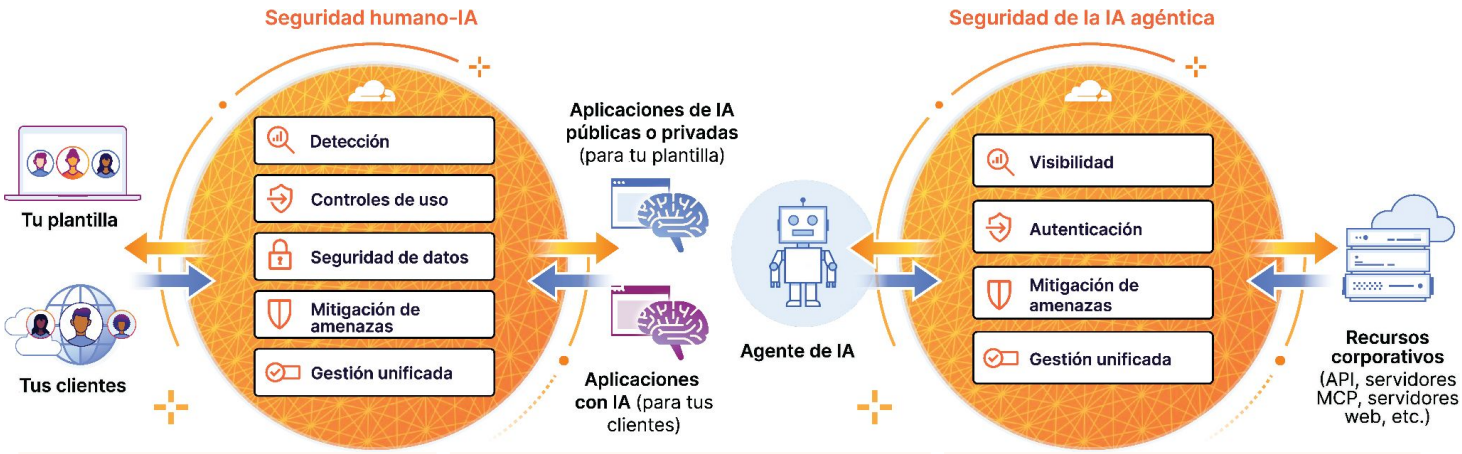
La seguridad está integrada
en el desarrollo de la IA en Cloudflare.

 | +34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:PMM-OCT2025

Protege la comunicación de la IA generativa y la IA agéntica con Cloudflare AI Security Suite

Protege todas las comunicaciones de IA mediante el control de los datos que tu equipo utiliza en la IA generativa y la gestión de los riesgos de seguridad que plantean los agentes autónomos.

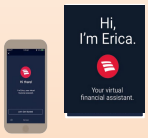


- **Tu plantilla:** empleados, contratistas, desarrolladores, etc.
- **Tus clientes:** visitantes de tus sitios web y aplicaciones

- **Aplicaciones de IA generativa:** independientes o integradas

Gemini · Claude · ChatGPT · Copilot

- **Aplicaciones habilitadas para IA** ej.: el bot de chat de IA de Bank of America, Erica



- **API** y **servidores MCP** para cualquier aplicación.

Google Workspace

- **Servidores web** para la inferencia y la generación aumentada por recuperación (RAG)

Acelera la adopción de la IA con el principio de la "seguridad por diseño" en todo el ciclo de vida de la IA

Protege el uso de la IA por parte de los empleados

Implementa controles de uso de la IA y la gestión de la postura de seguridad de la IA (AI-SPM) para mitigar los riesgos y proteger los datos.

Protege las aplicaciones basadas en IA

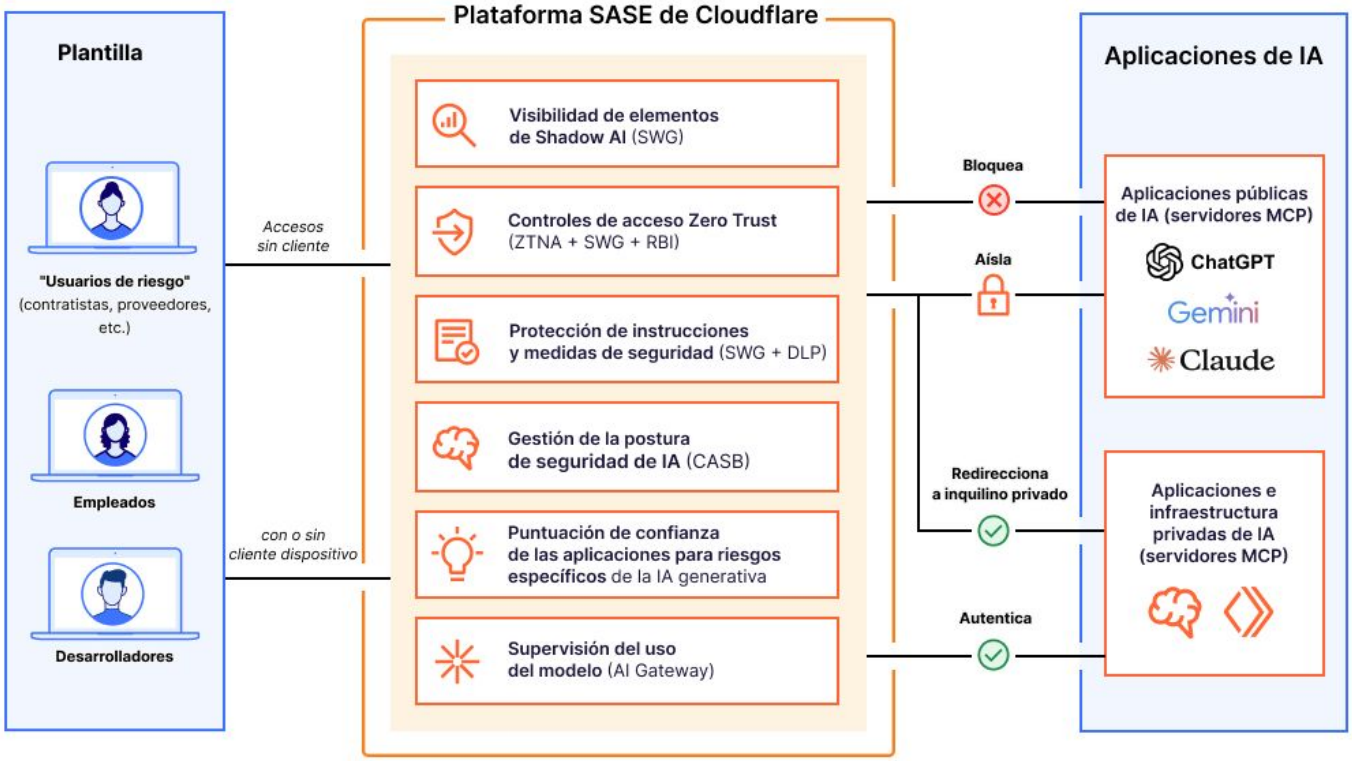
Protege tus API y aplicaciones de IA contra la inyección de instrucciones y las fugas de datos en tiempo real.

Desarrolla la IA con total seguridad

Proporciona a los desarrolladores las herramientas necesarias para proteger las aplicaciones de IA con observabilidad integrada, limitación de velocidad y medidas de protección de la IA en línea.

 | +34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

Protege el uso de las aplicaciones y las cargas de trabajo de IA por parte de los empleados con la plataforma SASE de Cloudflare



SSE para proteger la comunicación humano-IA

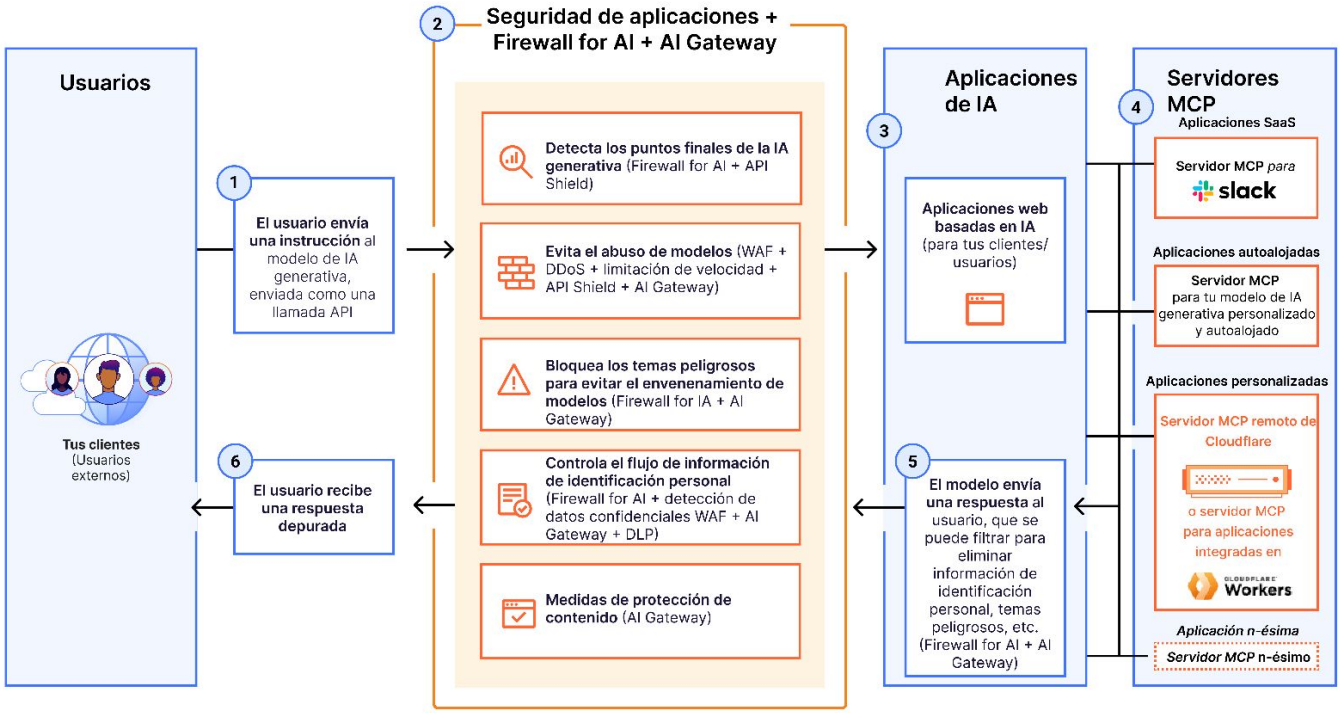
- **Visibilidad:** detecta y analiza el uso de elementos de Shadow AI mediante la inspección del tráfico en línea. Evalúa los riesgos que plantean esas aplicaciones de IA con una puntuación transparente.
- **Controles de acceso:** bloquea, aísla, redirige o permite las conexiones de los usuarios. Aplica reglas Zero Trust basadas en la identidad por aplicación.
- **Protección de instrucciones y medidas de seguridad:** detecta y bloquea las instrucciones de los usuarios en función de su intención (p. ej., intentos de jailbreak, abuso de código, solicitudes de información de identificación personal).
- **Seguridad de los datos:** evita la exposición de datos confidenciales con la detección de prevención de pérdida de datos (DLP) basada en IA de información de identificación personal, código fuente y mucho más.
- **Gestión de la postura de seguridad de la IA:** integra con herramientas de IA generativa a través de la API para buscar errores de configuración con nuestro agente de seguridad de acceso a la nube (CASB). Ya disponible para ChatGPT, Claude, y Google Gemini.

Portales de servidores MCP para proteger la comunicación IA-recursos

- **Visibilidad:** agrega todos los registros de solicitudes del protocolo de contexto del modelo (MCP) para fines de auditoría y análisis. Revisa y aprueba cada servidor MCP antes de agregarlo al portal.
- **Autenticación:** autentica el acceso de los usuarios al portal en función de su identidad. Limita el acceso a los servidores MCP según el principio de privilegio mínimo.
- **Conexiones:** conecta todos los servidores MCP accesibles con una sola URL, en lugar de configurar individualmente cada servidor MCP.
- **Gestión unificada:** aplica las mismas políticas de acceso granular para las conexiones de IA que para los usuarios humanos.

Nota: los portales de servidores MCP son compatibles con cualquier servidor MCP, incluidos, entre otros, los servidores MCP remotos desarrollados o implementados en Cloudflare. Esta capacidad está disponible como un control de acceso a la red de Zero Trust (ZTNA).

Protege las aplicaciones y las cargas de trabajo basadas en IA con la seguridad en línea, independiente de modelos, de Cloudflare



Protege la IA accesible al público con las soluciones de seguridad de aplicaciones y Firewall for AI

- **Descubre los puntos finales de la IA generativa:** detecta automáticamente todos los modelos de IA y las API en tus propiedades web.
- **Protege los modelos de IA del uso indebido:** utiliza nuestra solución Firewall for AI diseñada específicamente para bloquear la inyección de instrucciones, el envenenamiento de modelos, el uso excesivo y otras amenazas que pueden eludir las protecciones de seguridad tradicionales.
- **Controla el flujo de información de identificación personal:** analiza las instrucciones de los usuarios y las respuestas de los modelos para bloquear la exposición de datos confidenciales, lo que te ayudará a garantizar la conformidad normativa.
- **Medidas de protección de contenido:** bloquea las instrucciones no seguras o peligrosas utilizando modelos integrados como Llama Guard. Crea reglas WAF personalizadas para bloquear o registrar fácilmente interacciones sospechosas de la IA.

Protege la IA que desarrollas con la plataforma para desarrolladores y AI Gateway

- Panel de control de IA **unificado:** gestiona todas tus aplicaciones de IA desde un único panel de control. Enruta las solicitudes, almacena en caché las respuestas, controla los costes y supervisa el rendimiento.
- **Protege las credenciales en el perímetro:** almacena de forma segura las claves API y los secretos en el perímetro, para evitar la exposición del lado cliente y simplificar la rotación de claves entre proveedores.
- **Aplica medidas de seguridad del contenido:** identifica y bloquea o elimina automáticamente contenido dañino e información de identificación personal en las instrucciones y las respuestas.

 | +34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

Cloudflare es el único proveedor que protege tanto tus entornos de IA públicos como privados

Implementa las medidas de protección adecuadas para adoptar la IA con confianza, asegurándote de que la seguridad acelere tu innovación, en lugar de obstaculizarla.

- **Protección unificada del ecosistema de IA:** las pilas de seguridad complejas aumentan los riesgos. Utiliza una plataforma para proteger los datos y garantizar la conformidad normativa durante todo el ciclo de vida de la IA.
- **Arquitectura global preparada para el futuro:** evita hoy los desafíos del mañana con una red a prueba de la tecnología poscuántica y escalable a cualquier volumen de tráfico, que se adapta continuamente a las nuevas amenazas y que se puede programar para nuevos casos de uso.
- **Seguridad con tecnología de IA:** nuestras medidas de protección basadas en la IA inspeccionan las instrucciones y las respuestas para detectar las amenazas en tiempo real.
- **Liderazgo demostrado en IA:** innova con total confianza en una plataforma en la que confía el 80 % de las 50 principales empresas de IA generativa.
- **Implementación independiente de modelos:** los controles de seguridad funcionan para todos los modelos de IA de tu entorno, lo que proporciona un enfoque unificado para gestionar las implementaciones de IA.

Qué dicen nuestros clientes

indeed

Portal web de empleo n.º 1 del mundo
Leer caso práctico

Identifica y controla la Shadow AI

En paralelo con el proyecto de sustitución de la VPN

APPLIED

Tecnología de seguros
Leer caso práctico

Aísla las herramientas de IA generativa públicas como ChatGPT

para bloquear la función de copiar y pegar datos confidenciales

Empresa SaaS basada en IA

Protege la información de identificación personal

mediante la prevención del envío de información confidencial por parte de los clientes a los puntos finales de IA generativa de acceso público

Cyndx

Tecnología financiera impulsada por IA

Reducción del 95 % de los costes de inferencia

gracias a la adopción de Cloudflare para almacenar en caché y ejecutar las respuestas de los proveedores de modelos de IA

¿Quieres hablar de tus necesidades en materia de seguridad de la IA?

Te ayudamos

1. Estudio de Manage Engine de 2025: Fuente
2. 2025 IBM, Cost of a Data Breach report: Fuente

 | +34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/