CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

Cloudflare AI Security Suite

Protege 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.

Amplía la IA con confianza

Los riesgos de la IA exigen una seguridad moderna

Tus equipos están utilizando la IA para innovar con más velocidad, pero esto genera riesgos de seguridad críticos. La estrategia tradicional para bloquear la IA o añadir soluciones puntuales complejas está fallando porque frena la innovación e ignora la realidad:

- El **85 % de los empleados** utilizan herramientas de IA antes de que el departamento de informática pueda examinarlas.[1]
- El **93 % admite** haber introducido datos de la empresa en la IA sin aprobación.[2]
- El **63% de las organizaciones vulneradas** no tienen políticas de gobernanza de la IA.[1]

Conoce cómo empoderar a tus equipos y aprovechar los beneficios de la productividad de la IA, mientras mantienes la seguridad y el control que tu empresa necesita.

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

Cloudflare ofrece una plataforma única para que tu organización adopte la IA con confianza. Empoderamos a los líderes de seguridad para gestionar el riesgo, a los equipos de tecnología para impulsar la productividad, y a los ingenieros de plataforma para desarrollar con seguridad, y garantizamos que todos puedan innovar juntos de forma segura.

Primeros pasos para iniciar con Cloudflare AI Security Suite

Cloudflare AI Security Suite se ofrece en una plataforma unificada para proteger el uso del espacio de trabajo de las herramientas de IA y las aplicaciones de acceso público. Identifica la Shadow AI, protege los modelos contra el uso indebido, asegura el acceso de los agentes y evita la exposición de datos en los prompts, para que tu empresa pueda innovar de forma segura y eficiente, con mayor visibilidad y un control más estricto.

Ampliación de la visibilidad

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

Mitigación del riesgo

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

Protección de los datos

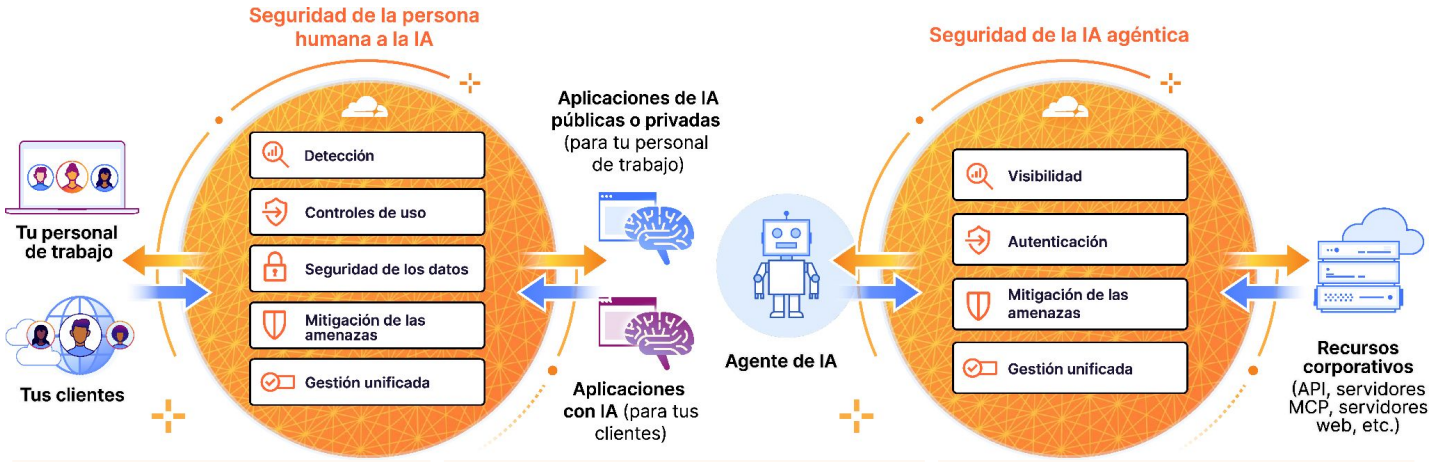
con protección de prompts y controles de acceso para empleados y agentes de IA.

La seguridad está integrada
al desarrollar la IA en Cloudflare.

© 2025 Cloudflare, Inc. Todos los derechos reservados. +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

Comunicación segura 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 personal utiliza en la IA generativa y la gestión de los riesgos de seguridad que plantean los agentes autónomos.

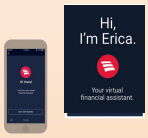


- **Tu personal de trabajo:** empleados, contratistas, desarrolladores, etc.
- **Tus clientes:** visitantes de tus sitios web y aplicaciones.

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

Gemini · Claude · ChatGPT · Copilot

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



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

Google Workspace

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

Adopción de la IA agilizada con el principio de la "seguridad por diseño" en todo el ciclo de vida de la IA

Uso seguro de la IA por parte de los usuarios

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

Protección de las aplicaciones con tecnología de IA

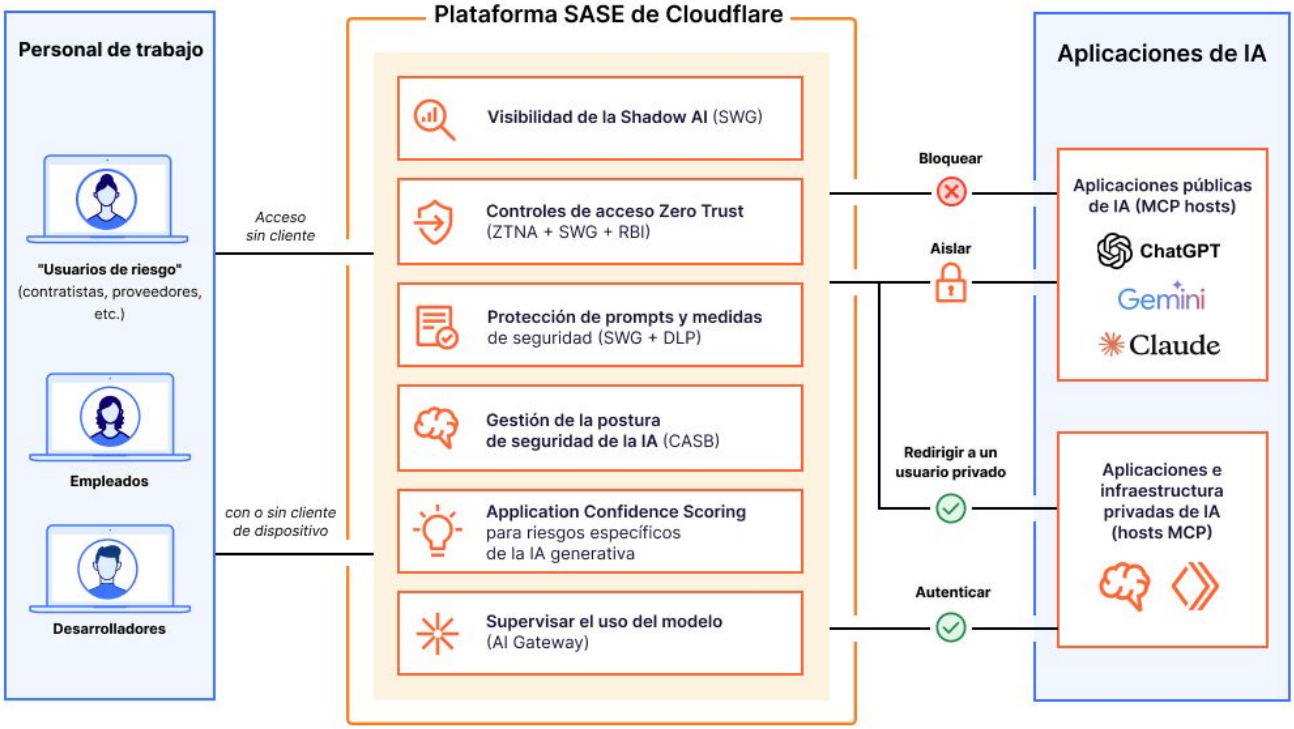
Protege tus aplicaciones de IA y API de la inyección de prompts y las fugas de datos en tiempo real.

Desarrollo seguro de la IA

Brinda a los desarrolladores una protección de las aplicaciones de IA mediante funciones integradas de observabilidad, limitación de velocidad y protecciones de IA en línea.

© 2025 Cloudflare, Inc. Todos los derechos reservados. +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

Protección del uso de aplicaciones y las cargas de trabajo de IA por parte de los usuarios con la plataforma SASE de Cloudflare



SSE para proteger la comunicación entre los humanos y la IA

- **Visibilidad:** identifica y analiza el uso de la 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:** bloquear, aislar, redirigir o permitir conexiones de usuario. Aplica reglas Zero Trust basadas en la identidad por cada aplicación.
- **Protección de prompts y medidas de seguridad**: detecta y bloquea los prompts de usuario según la 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 detecciones de prevención de pérdida de datos (DLP) impulsadas por IA para información de identificación personal, código fuente y más.
- **Gestión de la postura de seguridad de la IA:** integra con herramientas de IA generativa a través de la API para escanear en busca de errores de configuración con nuestro agente de seguridad de acceso a la nube (CASB). Ya está disponible para ChatGPT, Claude, y Google Gemini.

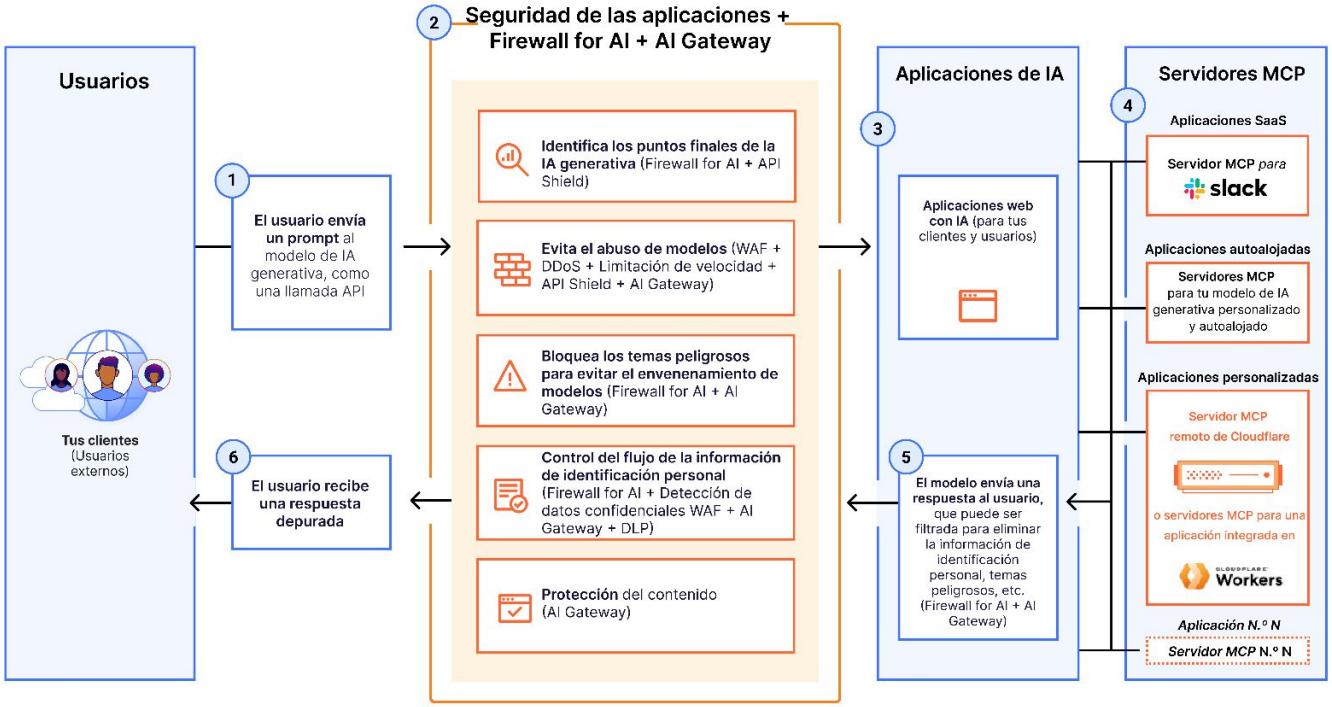
Portales de servidores MCP para proteger la comunicación de la IA a los recursos

- **Visibilidad:** añade todos los registros de solicitudes del Protocolo de Contexto de Modelo (MCP) para auditorías y análisis. Revisa y aprueba cada servidor MCP antes de añadirlo al portal.
- **Autenticación:** autentica el acceso del usuario al portal en función de la identidad. Limitar 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.
- **Administración unificada:** aplica las mismas políticas de acceso específicos 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 función está disponible como un control de acceso a la red Zero Trust (ZTNA).

© 2025 Cloudflare, Inc. Todos los derechos reservados.

Protección de las aplicaciones y cargas de trabajo habilitadas para la IA con la seguridad en línea de Cloudflare, independiente del modelo



Protección de la IA de acceso público con seguridad de aplicaciones y Firewall for AI para:

- **Descubrir los puntos finales de la IA generativa:** detecta de forma automática todos los modelos de IA y las API en tus propiedades web.
- **Proteger los modelos de IA contra las amenazas:** utiliza nuestro Firewall for AI, diseñado específicamente para bloquear la inyección de prompts, el envenenamiento de modelos, el uso excesivo y otras amenazas que pueden evitar las protecciones de seguridad tradicionales.
- **Controlar el flujo de información de identificación personal:** analiza los prompts del usuario y las respuestas del modelo para bloquear la exposición de los datos confidenciales, lo que ayuda a mantener el cumplimiento normativo.
- **Proteger el contenido:** bloquear los prompts no seguros o peligrosos mediante el uso de modelos integrados como Llama Guard. Implementa reglas WAF personalizadas para bloquear o registrar interacciones sospechosas de IA de forma sencilla.

Protección de la IA que desarrollas con la plataforma para desarrolladores y AI Gateway:

- **Plano de control de IA unificado:** gestiona todas tus aplicaciones de IA desde un único panel de control. Dirige las solicitudes, guarda en caché las respuestas, controla los costos y supervisa el rendimiento.
- **Protección de las credenciales en el perímetro:** almacena de forma segura las clave API y la información confidencial en el perímetro, lo que evita la exposición del lado del cliente y simplifica la rotación de claves entre proveedores.
- **Implementación de medidas de seguridad del contenido:** identifica y bloquea, y elimina automáticamente contenido dañino e información de identificación personal en las solicitudes y las respuestas.

© 2025 Cloudflare, Inc. Todos los derechos reservados. +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA

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

Implementa las protecciones adecuadas para adoptar la IA con confianza, garantizando que la seguridad acelere tu innovación y no la obstaculice.

- **Protección unificada del ecosistema de IA:** las infraestructuras de seguridad complejas aumentan el riesgo. Utiliza una plataforma para proteger los datos y garantizar el cumplimiento normativo en todo el ciclo de vida de la IA.
- **Arquitectura global preparada para el futuro:** evita hoy los desafíos del mañana con una red segura post-cuántica escalable a cualquier volumen de tráfico, que se adapta constantemente a las nuevas amenazas y es programable para nuevos casos de uso.
- **Seguridad con tecnología de IA:** nuestras defensas con tecnología de IA inspeccionan los prompts y las respuestas para la detección de amenazas en tiempo real.
- **Liderazgo comprobado en IA:** innova con confianza en una plataforma en la que confía el 80 % de las 50 principales empresas de IA generativa.
- **Implementación independiente del modelo:** los controles de seguridad funcionan para todos los modelos de IA en su entorno, y proporcionan un enfoque unificado para gestionar las implementaciones de IA.

Qué dicen nuestros clientes

indeed

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

Identificación y control de la Shadow AI

en paralelo con el proyecto de sustitución de la VPN.

APPLIED

Tecnología de seguros
Leer el caso práctico

Aislamiento de las herramientas públicas de IA generativa como ChatGPT

para bloquear la función de copiar y pegar datos confidenciales.

Empresa SaaS con IA

Protección de la información de identificación personal

al evitar que los clientes envíen información confidencial a los puntos finales públicos de la IA generativa.

Cyndx

Fintech impulsada por la IA

Costos de inferencia reducidos en un 95 %

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

¿Quieres hablar de tus necesidades de seguridad de IA?

Te ayudamos

1. Investigación de Manage Engine de 2025: Fuente
2. Informe de IBM sobre el costo de una filtración de datos de 2025: Fuente

© 2025 Cloudflare, Inc. Todos los derechos reservados. +55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-LA