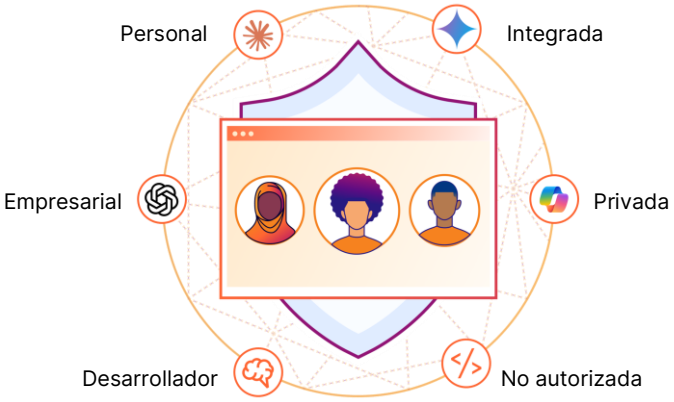
# Protege el uso de la IA generativa y agéntica por parte de los empleados

Permite a tus equipos de trabajo utilizar cualquier herramienta de IA de forma segura con las protecciones que ofrece la plataforma SASE de Cloudflare.




## Recupera el control, aumenta la productividad

La carrera por incorporar la IA está dejando una estela de riesgos cada vez mayores, entre los que se incluyen las fugas de datos, los incumplimientos normativos y una superficie de ataque en expansión. Si se bloquea la IA por completo, solo se conseguirá eliminar la ventaja competitiva, y si se experimenta con soluciones específicas, solo se añadirá complejidad.

Cloudflare protege el uso de la IA por parte de tu organización mediante la ampliación de la visibilidad, la mitigación de riesgos y la protección integral de los datos en todos los entornos de IA:

- **Detecta elementos de Shadow AI** y gestiona las políticas para todas las herramientas de IA autorizadas y no autorizadas.
- **Mejora la gobernanza de la IA** con controles de acceso basados en la identidad y la gestión de la postura.
- **Evita la pérdida de datos** mediante el bloqueo de información confidencial en las instrucciones de los usuarios, la aplicación de medidas de protección avanzadas y la búsqueda de configuraciones incorrectas en las herramientas de IA.

Amplía Cloudflare para adoptar la IA de forma segura, tanto si tu estrategia de IA consiste en limitar su uso a aplicaciones específicas como en experimentar con una gama más amplia de herramientas diversas.

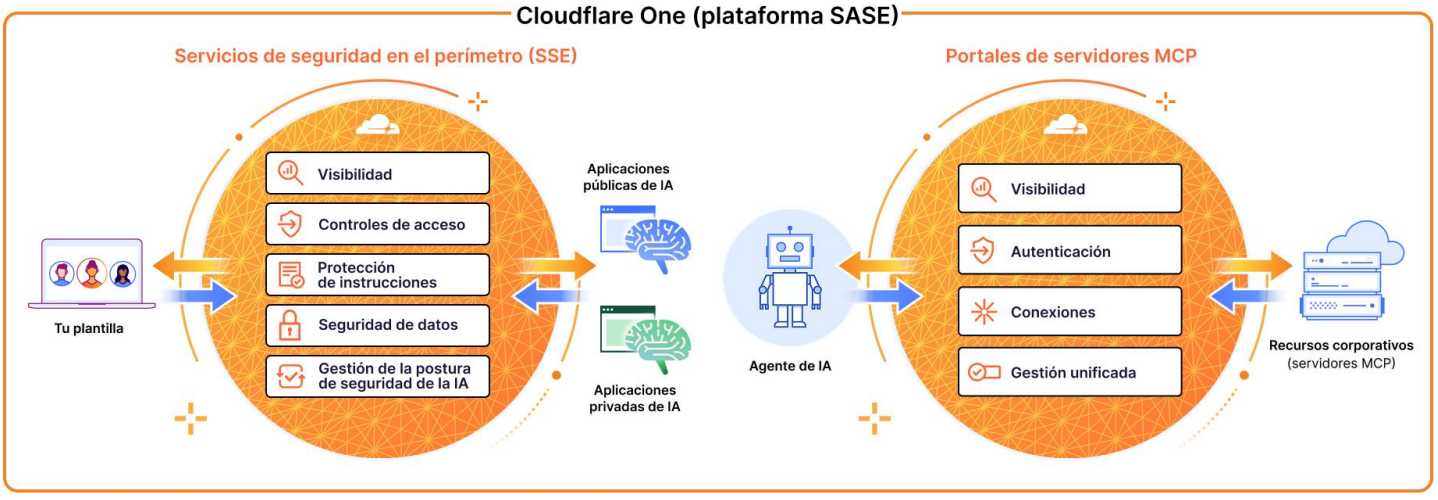
### Por qué utilizar SASE para garantizar el uso seguro de la IA por parte de los empleados

La plataforma de perímetro de servicio de acceso seguro (SASE) de Cloudflare se sitúa entre tu equipo y las herramientas de IA. Por eso, SASE es un punto de partida ideal para que muchos empiecen a utilizar la IA de forma segura.

Tanto si los empleados chatean con ChatGPT como si los agentes de IA recopilan información de los recursos corporativos, la plataforma SASE de Cloudflare aplica controles de seguridad coherentes.

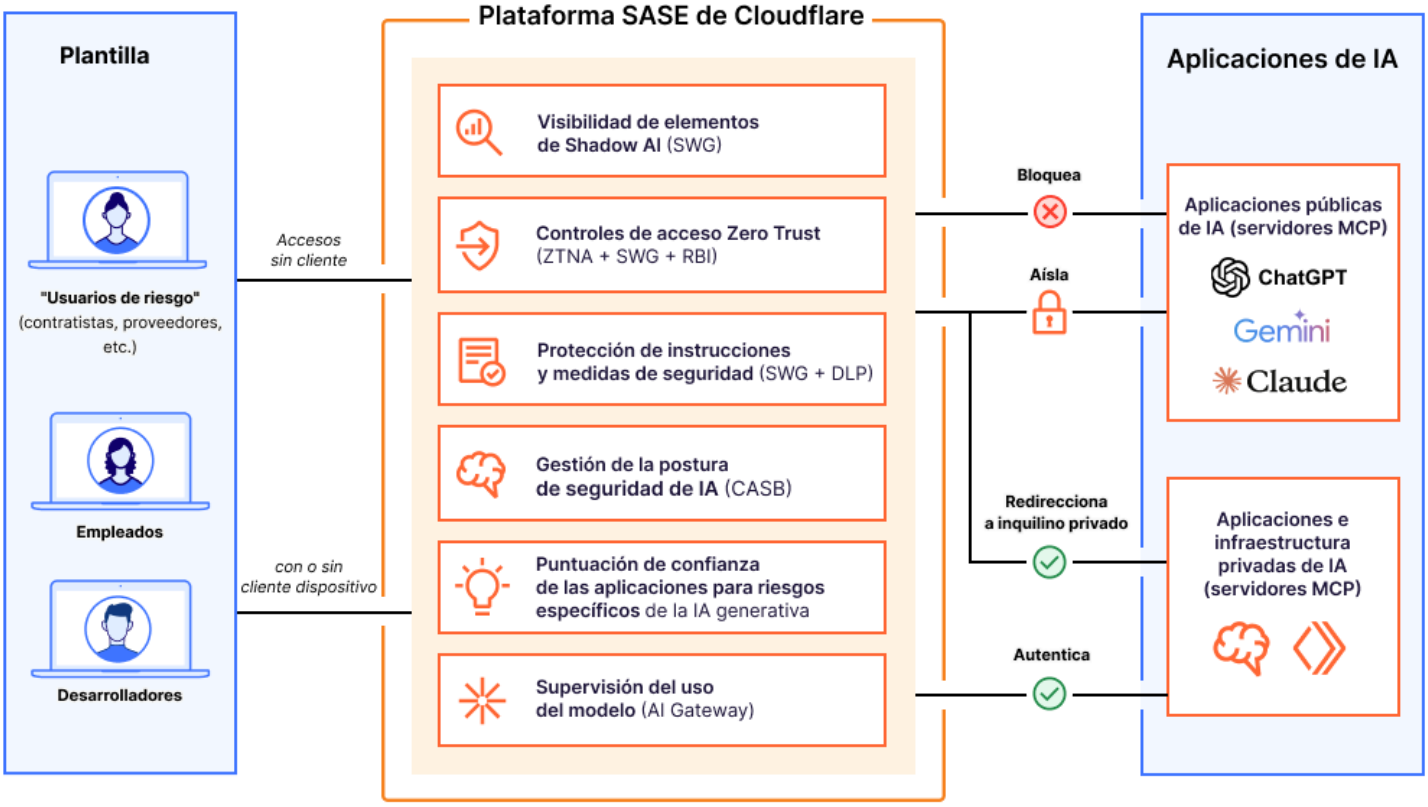
## Protege la comunicación de la IA generativa y la IA agéntica

La plataforma SASE de Cloudflare proporciona un panel de control unificado para gestionar tanto las interacciones humano-IA como entre dispositivos en toda la organización.




A diferencia de otros proveedores de SASE, Cloudflare también ayuda a conectar y proteger las aplicaciones y cargas de trabajo habilitadas para la IA accesibles al público (como el bot de chat de IA de tu sitio web o los motores de recomendación).

# **Protege la comunicación de los usuarios con aplicaciones de IA generativa** mediante controles de uso de la IA en la plataforma SASE de Cloudflare




- **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 de 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 (disponible ahora para ChatGPT, Claude y Google Gemini) para buscar errores de configuración mediante nuestro agente de seguridad de acceso a la nube (CASB).

## Resultados para los clientes

indeed

Sitio web de empleo n.º 1 del mundo

**Identifica y controla los elementos de Shadow AI**

en paralelo con el proyecto de sustitución de la VPN

APPLIED

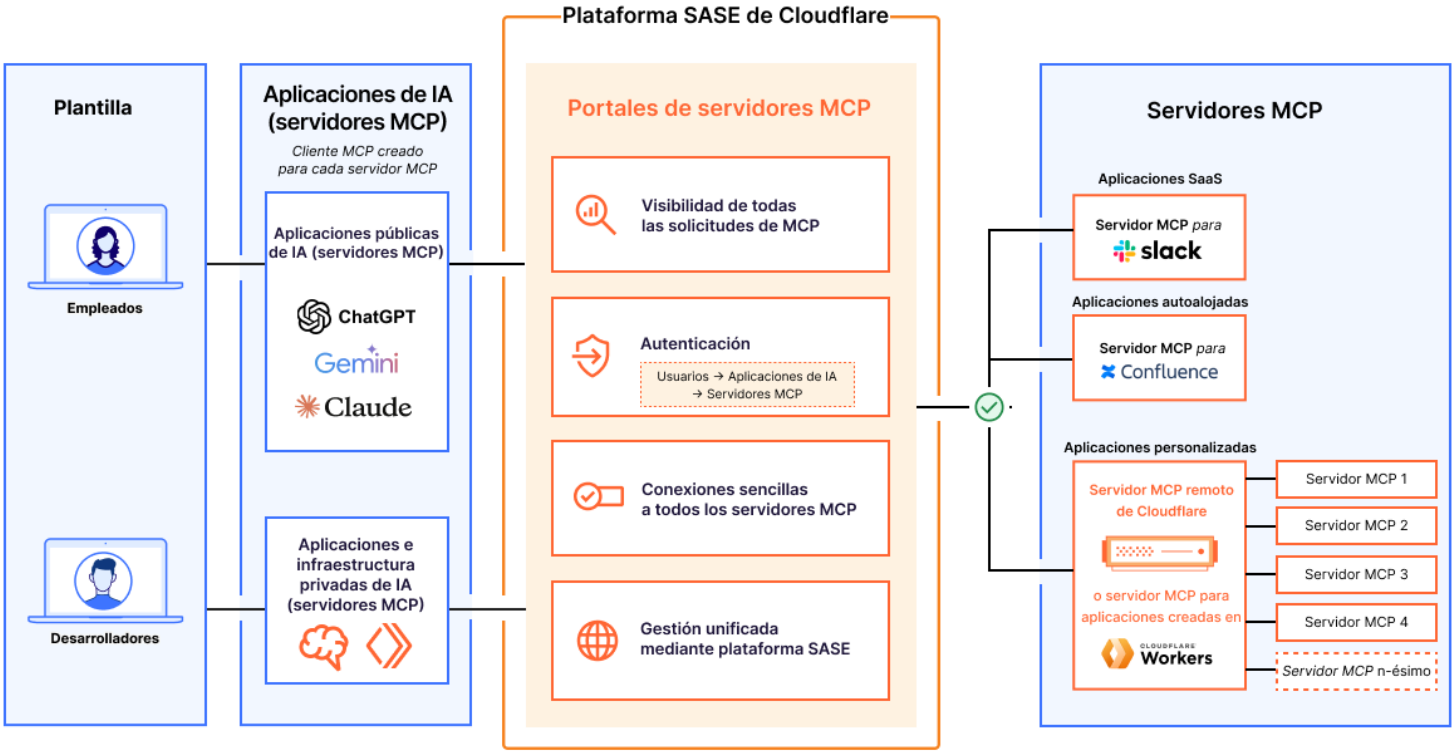
Tecnología de seguros

**Aísla las herramientas públicas de la IA generativa como ChatGPT,**

para bloquear las operaciones de copiar y pegar datos confidenciales

# Protege la comunicación de la IA agéntica (IA-recurso)
con los portales de servidores MCP en la plataforma SASE de Cloudflare




- **Visibilidad:** agrega todos los registros de solicitudes 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.
- **Personaliza las herramientas por portal:** elige las herramientas específicas y las plantillas de mensajes disponibles para cada usuario.

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

**Más información sobre nuestra filosofía en este blog.**

## ¿Te interesa descubrir cómo Cloudflare puede ayudarte a proteger el uso de la IA?

Solicitar seminario