CLOUDFLARE

RESUMEN DE LA SOLUCIÓN

Protege tus datos confidenciales

Mejora tu arquitectura de red para una protección de datos más eficaz, más productiva y más ágil.

Protección unificada para los datos, en todas partes

La protección de datos no es un nuevo requisito, pero el cambio a las arquitecturas de nube híbrida, junto con la rápida adopción de la IA, plantea nuevos desafíos:

- El **93 % de los usuarios** admite introducir información en herramientas de IA sin una autorización previa.[1]
- El **79 % de todos los países** tienen legislaciones sobre la privacidad de los datos.[2]

Cloudflare aplica controles coherentes en todo el ciclo de vida de tus datos:

- **Protección en todas partes:** aplica controles coherentes en todo el tráfico (web, SaaS, correo electrónico y en la nube).
- **Bloqueo de la exfiltración a la IA:** analiza las instrucciones de la IA generativa para bloquear los datos confidenciales y regular el uso de la IA.
- **Control de riesgos de los datos:** identifica y gestiona el shadow IT y shadow IA y analiza las aplicaciones SaaS o en la nube con CASB.

"El auge de todas estas herramientas de IA no autorizadas nos hace reconsiderar nuestro enfoque de seguridad. Ahora estamos analizando SASE". - *Responsable de seguridad de la información,* ***AllSaints***

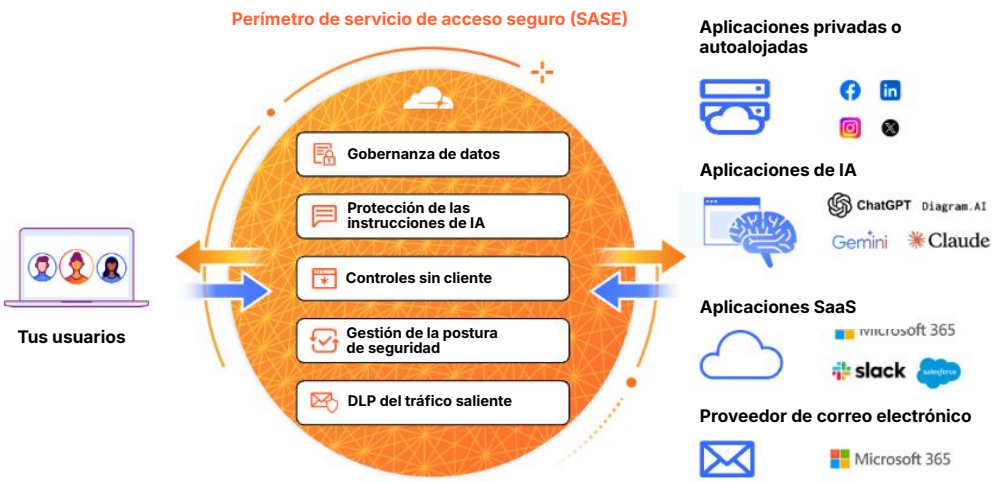
¿Por qué SASE es mejor que la protección de pérdida de datos (DLP) empresarial?

La plataforma de perímetro de servicio de acceso seguro (SASE) de Cloudflare está diseñada para situarse entre tus usuarios y todas las aplicaciones y fuentes de datos. Por este motivo, SASE es un punto de partida ideal para que muchos empiecen a proteger los datos con total seguridad.

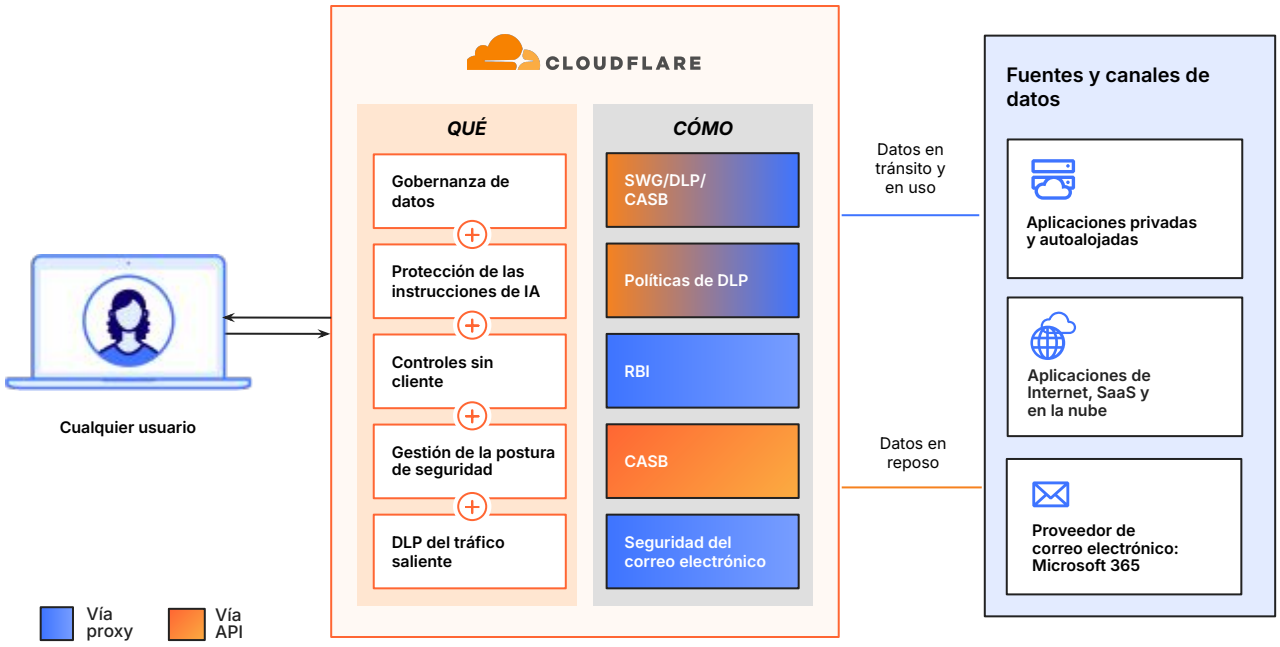
Tanto si los empleados acceden a los datos en aplicaciones SaaS, descargan archivos confidenciales o chatean con herramientas de IA generativa, la plataforma SASE de Cloudflare aplica controles de seguridad coherentes en todas las interacciones de datos.

Funcionamiento

La plataforma SASE de Cloudflare se sitúa entre tus usuarios y tus recursos para unificar la visibilidad y los controles.



Protección de datos basada en IA con la plataforma SASE de Cloudflare
en todo el tráfico (web, SaaS, correo electrónico y en la nube)



Protección de datos, en línea y en tiempo real

- **DLP granular:** evita la exposición de los datos confidenciales con detecciones basadas en el contexto para la información de identificación personal, el código fuente, los datos de los clientes y otros.
- **DLP del correo electrónico saliente:** identifica automáticamente los datos confidenciales en los correos electrónicos salientes y evita las fugas accidentales de datos.
- **Protección de las instrucciones:** detecta y bloquea las instrucciones y las respuestas de IA peligrosas en función de la intención (p. ej., los intentos de jailbreak, el abuso del código, las solicitudes de información de identificación personal).

Acceso seguro y controles de los clientes

- **Acceso seguro a las aplicaciones:** aplica reglas de acceso a la red Zero Trust (ZTNA), como el análisis DLP granular para las conexiones con la IA agéntica, en todas las aplicaciones corporativas.
- **Comprobaciones de la postura del dispositivo:** controla el acceso en función de comprobaciones granulares de la postura de seguridad, como la encriptación de discos y la activación de DLP en los puntos finales.
- **Controles sin cliente:** aplica controles de datos basados en el navegador para proteger el acceso de terceros y las políticas BYOD (trae tu propio dispositivo) de los empleados.

Shadow IT y riesgos de la postura de seguridad

- **Detección de shadow IT y shadow IA:** detecta y gestiona el shadow IT y el shadow IA en todo tu entorno. Cuantifica el riesgo mediante las puntuaciones de confianza de las aplicaciones y las métricas de transferencia de datos para mitigar rápidamente la exposición.
- **Gestión de la postura:** analiza las aplicaciones SaaS y los entornos de nube para identificar los riesgos de la postura de seguridad. Adopta medidas prescriptivas para corregir los problemas de seguridad detectados.
- **Control de inquilinos:** bloquea a los inquilinos personales de aplicaciones SaaS para evitar la exfiltración de datos.

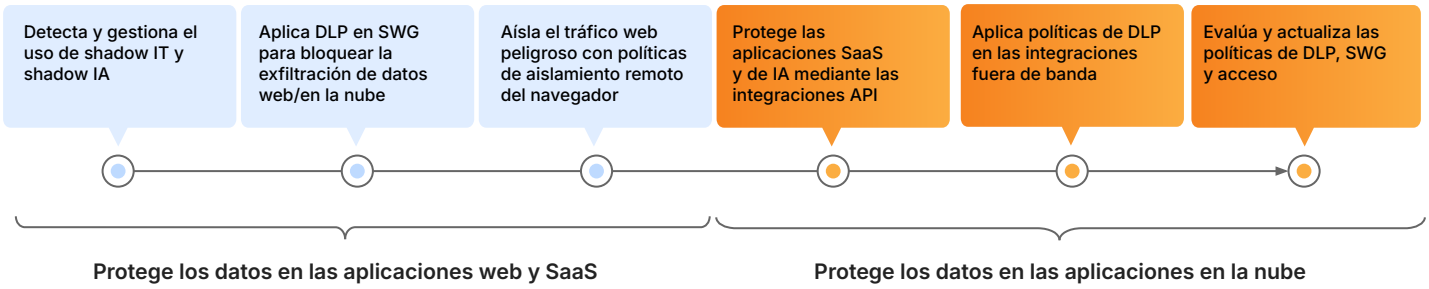
Integraciones e informes

- **Integraciones de CASB:** integra fácilmente con las principales plataformas SaaS y de IA (como Microsoft 365, Google Workspace y ChatGPT) para análisis CASB basados en API.
- **Integración de Microsoft MIP:** garantiza una sincronización continua con las etiquetas de Microsoft Information Protection (MIP) para beneficiarte de políticas DLP coherentes.
- **Observabilidad y análisis forense**: registra de forma segura los datos en tu SIEM preferido para fines de auditoría, o bien analiza los registros al instante a través del panel de control o la API.

Ejemplo de recorrido para la protección de los datos

Empieza por detectar el shadow IT y el shadow IA para tener visibilidad de tu superficie de ataque. Configura políticas básicas de DLP en SWG para bloquear la fuga de datos de riesgo de las aplicaciones en la nube no gestionadas, e implementa el aislamiento remoto del navegador (RBI) para el tráfico web no aprobado.

A continuación, implementa CASB para proteger tus aplicaciones SaaS y de IA autorizadas mediante la corrección de los errores de configuración y la aplicación de políticas sobre el uso compartido interno. Mejora e integra políticas granulares de DLP y de acceso en SWG, el correo electrónico y CASB para beneficiarte de una prevención automatizada y unificada en todos los principales vectores de datos.



Ejemplos de casos de uso para empezar

- **Bloquea la exfiltración en tiempo real de la información de identificación personal y la información sanitaria protegida** en todos los canales de comunicación y de almacenamiento no aprobados.
- **Protege el código fuente y la propiedad intelectual** contra el robo interno y la distribución no autorizada.
- **Aplica políticas de protección de las instrucciones** para las aplicaciones de IA generativa a fin de evitar la exposición de datos confidenciales y la contaminación de los modelos.
- **Evita los errores de configuración** y aplica controles de acceso granulares en todas las aplicaciones SaaS y de IA.

Resultados para los clientes

EESTI RAUDTEE

Proveedor de infraestructura
Leer caso práctico

Mitigación de la pérdida de datos y de las vulnerabilidades de SaaS

gracias a la identificación de las fugas de datos y de los errores de configuración

APPLIED

Tecnología de seguros
Leer caso práctico

Aislamiento de las herramientas de IA generativa públicas como ChatGPT

para bloquear la función de copiar y pegar datos confidenciales

Flo

Aplicación de salud líder
Leer caso práctico.

Protección de los datos de los pacientes

y conformidad gracias a la seguridad del correo electrónico y Zero Trust.

CREDIT SAISON INDIA

Entidad crediticia NBFC
Leer caso práctico

Protección de la información de identificación personal y conformidad

para evitar la salida no deseada de datos

¿Quieres que hablemos de tus necesidades de protección de datos?

Solicitar seminario

1. Estudio de Manage Engine de 2025: Fuente
2. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2025: Fuente

 | +34 518 880 290 | enterprise@cloudflare.com | cloudflare.com/es-es/ BDES-8612-03DIC2025