Protección de tus datos confidenciales

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

Protección unificada para los datos, en todas partes

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

- **El 93 % de los empleados** admite haber introducido información en las herramientas de IA sin aprobación.[1]
- **El 79 % de los países** tienen leyes de privacidad de datos.[2]

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

- **Protección en todas partes:** aplica controles consistentes en todo el tráfico web, SaaS, correo electrónico y en la nube.
- **Bloqueo de la exfiltración de IA:** analiza los prompts de la IA generativa para bloquear datos confidenciales y controlar el uso de la IA.
- **Control de los riesgos de los datos:** detecta y gestiona la presencia de Shadow IT y Shadow AI, y analiza las aplicaciones SaaS y en la nube con CASB.

"El aumento de todas estas herramientas de IA no autorizadas nos obliga a reconsiderar nuestro enfoque de seguridad. Ahora estamos analizando SASE". - *Director de seguridad de la información,* ***AllSaints***

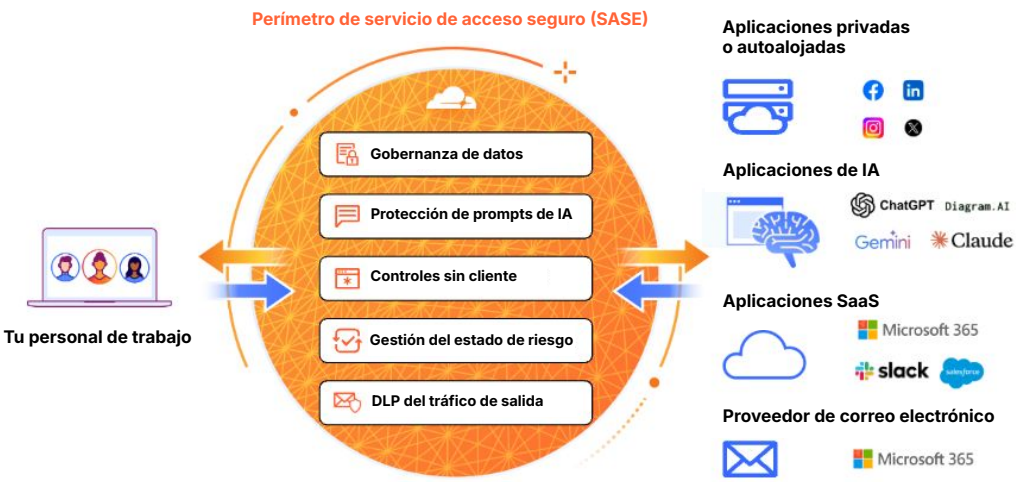
¿Por qué es mejor SASE que la protección de pérdida de datos (DLP) empresarial?

La plataforma de perímetro de servicio de acceso seguro (SASE) de Cloudflare está diseñada para situarse entre tu personal de trabajo y todas las aplicaciones y fuentes de datos. Esto convierte a SASE en un punto de partida ideal para que muchos comiencen a proteger los datos de forma segura.

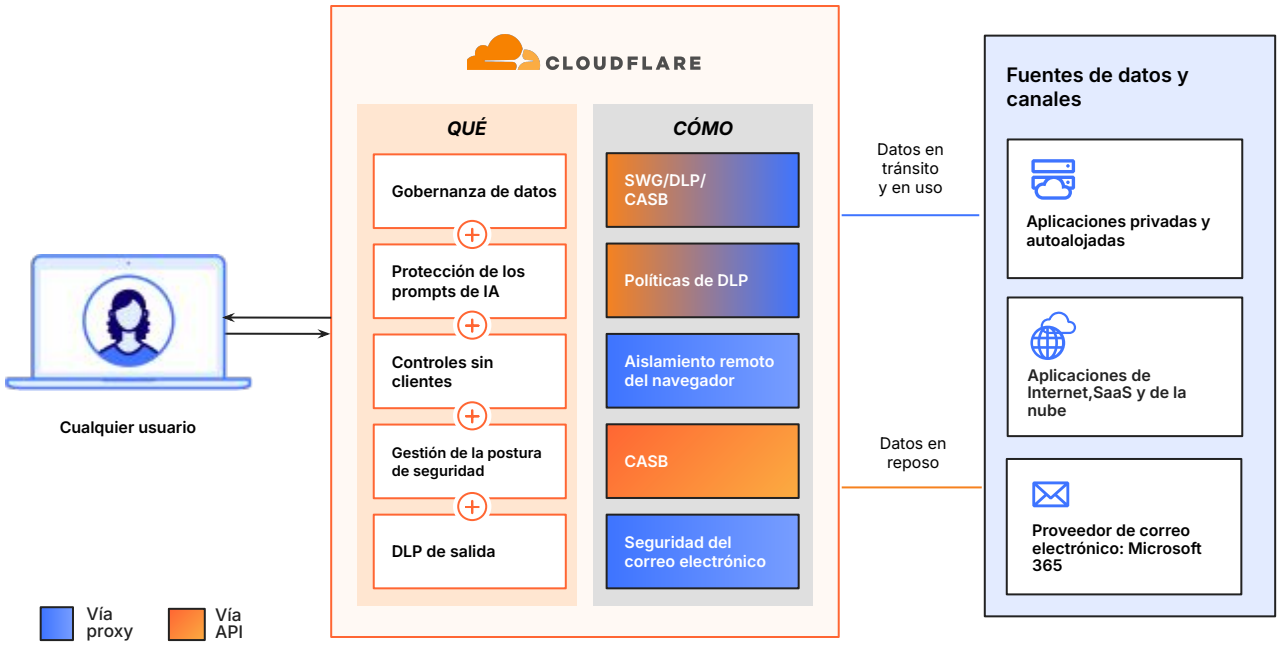
Ya sea que los empleados accedan a datos en aplicaciones SaaS, descarguen archivos confidenciales o interactúen con herramientas de IA generativa, la plataforma SASE de Cloudflare aplica controles de seguridad consistentes en todas las interacciones de los datos.

Cómo funciona

La plataforma SASE de Cloudflare se ubica entre tu personal de trabajo y tus recursos para unificar la visibilidad y los controles.



Protección de los datos potenciada por la IA con la plataforma SASE de Cloudflare
en el tráfico web, SaaS, de correo electrónico y de la nube



Protección de datos en línea y en tiempo real

- **DLP especifica:** evita la exposición de los datos confidenciales con las detecciones contextuales para la información de identificación personal, el código fuente, los datos de clientes y más.
- **DLP de correo electrónico de salida:** marca automáticamente los datos confidenciales en los correos electrónicos de salida, y evita las fugas accidentales de los datos.
- **Protección de prompts:** detecta y bloquea los prompts y las respuestas de IA peligrosos según la intención (p. ej., intentos de jailbreak, abuso de código, solicitudes de información de identificación personal).

Acceso seguro y controles de clientes

- **Acceso seguro a las aplicaciones:** aplica reglas de acceso a la red Zero Trust (ZTNA), como el análisis DLP especifico para conexiones de IA mediante agentes, en todas las aplicaciones corporativas.
- **Control del estado del dispositivo:** controla el acceso con controles específicos del estado, como el cifrado de disco y la DLP de punto final habilitada.
- **Control sin cliente:** aplica controles de datos basados en el navegador para proteger el acceso de terceros y las políticas BYOD de los empleados.

Riesgos de la Shadow IT y de la postura de seguridad

- **Detección de Shadow IT y Shadow AI:** detecta y gestiona el uso de Shadow IT y Shadow AI en todo tu entorno. Mide el riesgo con puntuaciones de confianza de las aplicaciones y métricas de transferencia de datos para mitigar rápidamente la exposición.
- **Gestión de la postura de seguridad:** analiza las aplicaciones SaaS y los entornos en la nube para detectar riesgos de configuración. Adopta medidas específicas para resolver los problemas de seguridad detectados.
- **Control de las licencias:** bloquea las licencias personales de aplicaciones SaaS para evitar la filtración de datos.

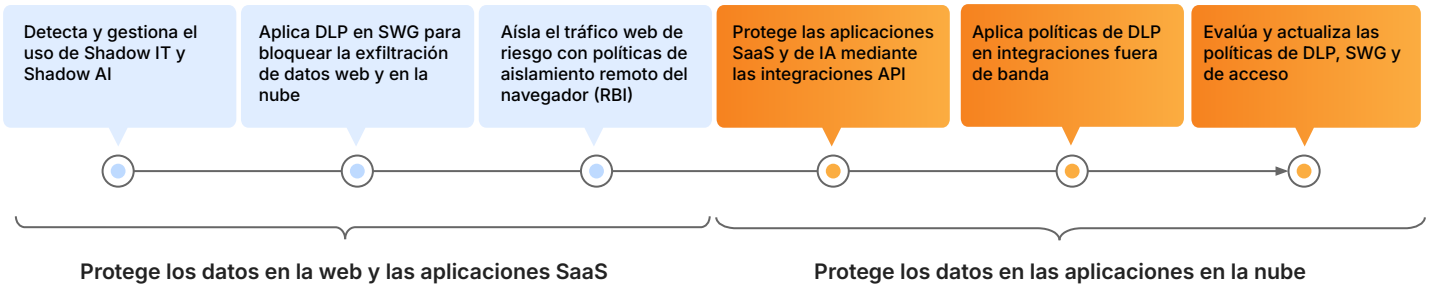
Integraciones e informes

- **Integraciones CASB:** logra integraciones eficientes con las principales plataformas SaaS e IA (incluyendo Microsoft 365, Google Workspace y ChatGPT) para los análisis CASB basados en API.
- **Integración de Microsoft MIP:** sincroniza de forma continua con las etiquetas de protección de la información de Microsoft (MIP) para políticas DLP consistentes.
- **Observabilidad y análisis forense**: registra de forma segura los datos en tu SIEM de preferencia para la verificación, o analiza los registros al instante a través del panel de control o la API.

Ejemplo del recorrido de la protección de los datos

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

Luego, implementa CASB para proteger las aplicaciones SaaS y de IA autorizadas mediante la corrección de configuraciones erróneas y la aplicación de políticas internas de uso compartido. Mejora e integra políticas DLP especificas y de acceso en SWG, correo electrónico y CASB para lograr una prevención automatizada y unificada en todos los principales vectores de datos.



Ejemplos de casos de uso para empezar

- **Bloquea la exfiltración de la información de identificación personal y de la información médica protegida en tiempo real** en todos los canales de comunicación y almacenamiento no aprobados.
- **Protege el código fuente y la propiedad intelectual (IP)** contra el robo interno y la distribución no autorizada.
- **Aplica políticas de protección de prompts para las aplicaciones de IA generativa** con el fin de evitar la exposición de los datos confidenciales y la contaminación del modelo.
- **Evita las configuraciones erróneas** y aplica controles de acceso específico en todas las aplicaciones SaaS y de IA.

Resultados de los clientes

EESTI RAUDTEE

Proveedor de infraestructura
Leer el caso práctico

Mitigación de la pérdida de datos y las vulnerabilidades de SaaS

mediante la identificación de fugas de datos y configuraciones erróneas.

APPLIED

Tecnología de seguros
Leer el caso práctico

Aislamiento de las herramientas públicas de la IA generativa 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 logro del cumplimiento normativo con la seguridad del correo electrónico y Zero Trust.

CREDIT SAISON INDIA

Prestamista de NBFC
Leer el caso práctico

Protección de la información de identificación personal y logro del cumplimiento normativo

para prevenir la salida de datos no deseada.

¿Te interesa hablar de tus necesidades para la protección de datos?

Solicitar seminario

1. Investigación de Manage Engine de 2025: Fuente
2. Conferencia de las Naciones Unidas sobre el comercio y desarrollo 2025: Fuente

