Kiteworks

FICHA DE SOLUCIÓN

PARA CISO, EQUIPOS DE CUMPLIMIENTO Y SEGURIDAD

Gobierne cada intercambio de datos sensibles con el Data Policy Engine

Defina la política una vez. Aplíquela en cada intercambio de datos sensibles, para personas y agentes de IA.

CMMC 2.0 | HIPAA / HITECH | RGPD / NIS 2 | ITAR / EAR | SOC 2 Type II | ISO 27001, 27017, 27018

FedRAMP Class D Agency Auth In Process (antes High In Process) | FedRAMP Class C Certified (antes Moderate Authorized)

El desafío

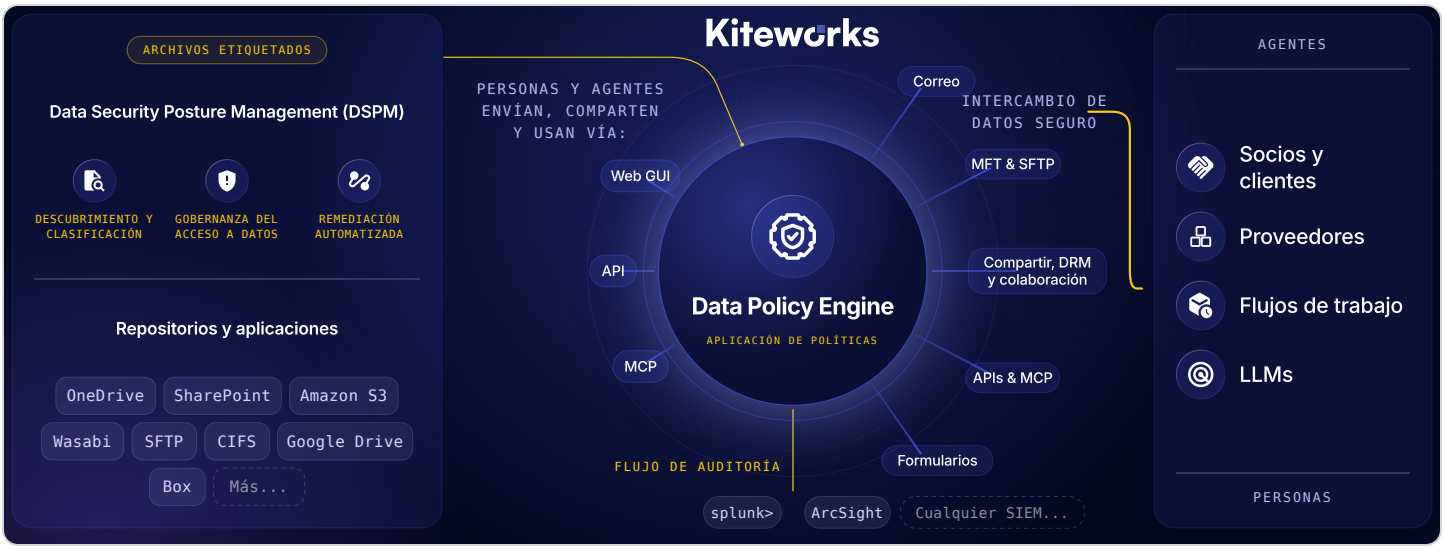
Agentes de IA, empleados y partes externas solicitan datos sensibles por los mismos canales: MCP, API, correo, formularios, SFTP, uso compartido de archivos y MFT. Las herramientas tradicionales tienen cada una sus propias políticas y registros. La aplicación varía según el canal, se abren brechas y demostrar el cumplimiento exige reunir pruebas de cada sistema antes de auditar.

La solución

Con el Data Policy Engine (DPE) de Kiteworks, los administradores definen las políticas de datos una vez y se aplican en tiempo de ejecución en cada canal. Cada decisión pondera datos, actor (persona o agente de IA) y acción: permitir, bloquear, exigir aprobación o limitar a ver o editar de forma protegida. Toda acción de agentes y usuarios va a un único registro.

Un único plano de control para cada intercambio de datos sensibles

Tanto si la solicitud procede de un empleado, un socio o un agente de IA, el Data Policy Engine evalúa los mismos atributos de datos, actor y acción, y aplica las mismas políticas en API, agentes de IA, correo electrónico, uso compartido de archivos y otros canales.



Cómo decide el Data Policy Engine

1 DATOS

Evaluar los datos

Atributos como las etiquetas de clasificación, la carpeta y las palabras clave del correo describen qué se intercambia.

2 ACTOR

Identificar al actor

El contexto, como dirección de correo, dominio, perfil y geolocalización, define al usuario o agente solicitante.

3 ACCIÓN

Valorar la acción

Acceder, enviar, compartir o cargar activa en cada caso sus propias respuestas.

4 APLICAR

Aplicar la directiva

La regla correspondiente se aplica de forma automática y en tiempo real, sin pasos manuales.

Control de políticas sin complejidad

Reglas SI-ENTONCES basadas en datos, usuario o agente y acción. Parta de una plantilla o cree las reglas desde cero.

Reglas Y/O unificadas
Una única lógica de reglas para usuarios, datos y acciones, aplicada a MCP, API, la web y el resto de los canales de intercambio de datos.

Plantillas predefinidas
Plantillas, por ejemplo, para impedir que los datos salgan de la organización o exigir aprobación antes de compartir.

Basadas en clasificación
Controle el acceso de personas y agentes de IA con etiquetas de Kiteworks, de IA de Cyera o de Microsoft Purview. Las políticas también etiquetan al cargar.

Sovereign Edit
Una política puede obligar a ciertos usuarios y socios a editar en el navegador; el archivo queda en Kiteworks y nunca se descarga, extrae ni envía a la nube de Microsoft.

Flujos de aprobación y justificación
Exija aprobación antes de compartir, o un formulario de justificación antes de acceder o cargar.

RBAC granular y caducidad
Roles de mínimo privilegio, acceso por carpeta y caducidad por tiempo para archivos y enlaces compartidos.

Gobernar en tiempo real cada solicitud de datos de agentes y personas

Acceso
Bloquear, SafeVIEW, Sovereign Edit, justificación o permitir.

Compartir o enviar
Bloquear, exigir la aprobación de un responsable o permitir.

Carga
Bloquear, etiqueta de Kiteworks, justificación o permitir.

Aplicar automáticamente el cumplimiento de agentes y personas y demostrarlo

Un registro de auditoría inmutable
Toda acción de agentes y personas se registra de forma centralizada y alimenta los informes de cumplimiento y las integraciones con SIEM.

Informes y paneles de políticas
Evalúe una política antes de activarla y mida su impacto en producción.

Marcos normativos
Las reglas de DPE ofrecen soporte amplio y granular para normativas como CMMC 2.0, HIPAA, RGPD, FedRAMP, ITAR, NIS 2, PCI DSS y PIPEDA.

¿Listo para gobernar cada intercambio de datos sensibles?

www.kiteworks.com sales@kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

Copyright © 2026 Kiteworks.