Kiteworks

SOLUTION BRIEF

Kiteworks Compliant AI

Gobernanza en la capa de datos para agentes de IA Acceso a datos regulados

Los agentes de IA son los nuevos empleados digitales: acceden a registros financieros, datos de pacientes, CUI y secretos comerciales a velocidad de máquina. A diferencia de los empleados humanos, los agentes no ejercen juicio y accederán a cualquier dato o ejecutarán cualquier función que no se les impida explícitamente.

Regulaciones como HIPAA, CMMC/ITAR, PCI DSS, SEC y SOX exigen controles estrictos para el acceso a datos, registros de auditoría y cifrado. Estas obligaciones aplican igualmente a los agentes de IA que acceden a datos regulados.

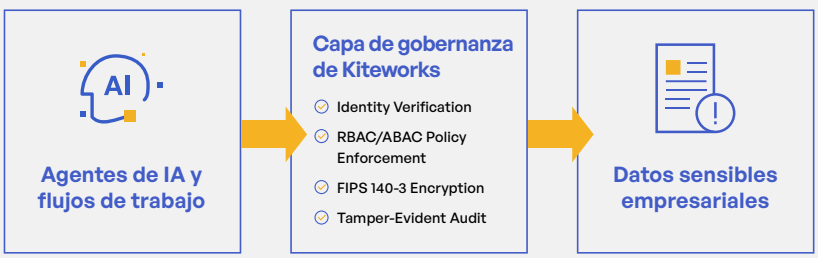
Gobernanza en la capa de datos: la única capa que los agentes de IA no pueden eludir

Kiteworks Compliant AI controla las interacciones de los agentes en la capa de datos, no en la del modelo. Los prompts y filtros de seguridad del modelo pueden ser eludidos; la aplicación en la capa de datos no.

Cada interacción de agente pasa por cuatro puntos de control de gobernanza:

- **Identidad autenticada:** Los agentes se verifican mediante OAuth 2.0 y se vinculan al autorizador humano que delegó el flujo de trabajo.
- **Acceso controlado por políticas (ABAC):** Las solicitudes se evalúan en tiempo real según la identidad del agente, la clasificación de los datos y el contexto. Se aplica el acceso mínimo necesario a nivel de operación.
- **Cifrado validado FIPS 140-3:** Todos los datos a los que accede el agente se cifran en tránsito y en reposo con módulos criptográficos validados.
- **Registro de auditoría a prueba de manipulaciones:** Cada interacción se registra con atribución completa y se transmite en tiempo real a SIEM.

Donde la IA cumple con los requisitos



Cumplimiento integrado en la arquitectura, no añadido después de la implementación

Solución Aspectos destacados

Controla el acceso de agentes de IA a datos sensibles en la capa de datos, independientemente del modelo, prompt o framework del agente

Cifrado validado FIPS 140-3 para todos los datos accedidos por agentes en tránsito y en reposo

Autorizado por FedRAMP Moderate; FedRAMP High en proceso

Tres Governed Assists disponibles para compra a través de MCP para flujos de trabajo regulados

Funciona con Claude, Copilot y cualquier LLM compatible con MCP

Tres Governed Assists: flujos de trabajo de IA listos para cumplimiento

Kiteworks Compliant AI incluye tres Governed Assists: capacidades discretas y adquiribles impulsadas por el Model Context Protocol (MCP) y gobernadas de extremo a extremo por el motor de políticas de datos de Kiteworks. Cada operación se verifica por identidad, se evalúa por ABAC, se cifra con FIPS 140-3 y se registra de forma a prueba de manipulaciones.

Governed Folder Operations Assist: Los agentes de IA navegan, crean, renombran, mueven y eliminan jerarquías de carpetas usando lenguaje natural, con cada operación gobernada por el motor de políticas de datos. Las estructuras de carpetas heredan controles RBAC/ABAC automáticamente, cumpliendo con la segregación de CUI (CMMC), segregación de registros (HIPAA) y requisitos de provisión de espacios de trabajo de auditoría.

Casos de uso: Estructuración de portafolios de clientes · Segregación de carpetas CUI · Provisión de espacios de trabajo de auditoría · Espacios de trabajo para retención legal · Documentación de ensayos clínicos

Governed File Management Assist: Los agentes de IA controlan todo el ciclo de vida de los datos: subir, descargar, leer, crear, mover, renombrar y eliminar archivos, con cada operación aplicada por el motor de políticas de datos. Cumple con los calendarios de retención (NARA, SOX), acceso mínimo necesario (HIPAA) y requisitos de eliminación (PCI).

Casos de uso: Barridos de retención SOX · Verificación de marcado CUI · Empaquetado de informes de eventos adversos · Generación de logs de privilegios · Cumplimiento de calendarios de registros

Governed Forms Creation Assist: Los agentes de IA generan formularios de recolección de datos gobernados a partir de descripciones en lenguaje natural, eliminando la carga manual de crear formularios y asegurando que todas las presentaciones se dirijan a almacenamiento gobernado por políticas con controles RBAC/ABAC heredados.

Casos de uso: Ingreso KYC/CDD · Reporte de incidentes FISMA · Formularios de autorización HIPAA · Cuestionarios de calificación de proveedores · Recepción de reportes de denunciantes

Cumple con confianza los requisitos de auditoría y gobernanza

- Demuestra control sobre los flujos de datos regulados (CUI, PCI, PHI, PII, contenido regulado por SEC)
- Mapea la actividad de los agentes de IA a marcos de cumplimiento como HIPAA, CMMC, PCI DSS, SEC/SOX, GDPR, NIST CSF e ISO 27001
- Exporta registros de auditoría unificados y reportes de cumplimiento de IA dedicados para auditorías y respuesta a incidentes
- Produce paquetes de evidencia de IA listos para la junta directiva rápidamente

Integración fluida con cualquier plataforma de IA

Kiteworks Compliant AI funciona con cualquier plataforma de IA compatible con MCP: Claude, Copilot y cualquier LLM futuro que soporte el Model Context Protocol. La puerta de enlace de datos IA proporciona APIs REST para pipelines RAG y flujos de trabajo de IA programáticos. Implementa en cualquier entorno—nube, en las instalaciones de la empresa o híbrido—con soporte multiplataforma para Windows, macOS y Linux. Gobernanza basada en estándares y neutralidad de proveedor que protege tu inversión sin importar qué plataformas de IA adopte tu organización.