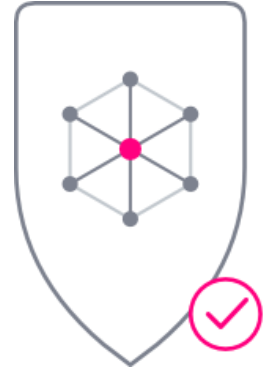


GOBIERNO Y SEGURIDAD DE IA

Escala tu IA con confianza y seguridad.

La IA generativa incorpora más de 60 riesgos potenciales a lo largo de su ciclo de vida. Gestiona, monitorea y gobierna toda tu IA desde una única plataforma para garantizar seguridad, cumplimiento y trazabilidad de extremo a extremo.



■ EL RETO

Las organizaciones quieren acelerar la adopción de IA, pero cada modelo en producción trae riesgos: sesgo, deriva (drift), falta de explicabilidad, fuga de datos personales y exposición regulatoria. Sin un marco de gobierno, esos riesgos quedan invisibles hasta que generan un problema de cumplimiento, de reputación o de confianza.

■ LA SOLUCIÓN

Una plataforma de gobierno y seguridad de IA que dirige, monitorea y gestiona toda la actividad de IA de la organización mediante automatización.

Centraliza el inventario de modelos, automatiza la documentación, evalúa riesgos y aplica guardrails de observabilidad sobre cada modelo —sin importar dónde se construyó (IBM, AWS, Azure, GenAI apps u otros). Un buen gobierno no frena la IA: impulsa su adopción.

■ CÓMO FUNCIONA

01 Documenta e inventaría

Captura automáticamente los hechos de cada modelo (AI Factsheet) a lo largo de su ciclo de vida y construye un inventario centralizado de activos de IA.

02 Evalúa y mitiga riesgos

Identifica y evalúa riesgos por modelo, con aceleradores de cumplimiento y flujos de aprobación desde la concepción hasta el retiro del servicio.

03 Observa y aplica guardrails

Monitorea salud del modelo, precisión, drift, sesgo, explicabilidad y detección de contenido perjudicial o datos personales (PII) en entradas y salidas.

04 Reporta y cumple

Tableros centralizados con visibilidad y transparencia para auditoría, gestión de riesgos y preparación normativa.

■ RESULTADOS

-40%

Tiempo de validación de modelos

-30%

Riesgo de no cumplimiento

+25%

Confianza en los sistemas de IA

■ CASOS DE USO

→ Gestión del ciclo de vida de IA: documentación automática e inventario de modelos

→ Recursos Humanos: detectar y mitigar sesgo en modelos de contratación

→ Bots RAG: evaluar calidad de respuestas y atribución a la fuente

→ Auditoría: captura de metadatos y monitoreo de toxicidad, PII y temas fuera de alcance

■ INTEGRACIONES

WATSONX.GOVERNANCE

IBM

AWS

MS AZURE

GENAI APPS

SAAS

MCP

Agenda una sesión de diagnóstico

45 min para mapear tu portafolio de modelos y ver dónde el gobierno de IA reduce más riesgo en tu operación.



Escanea el código →

ESCANEAR