



Inspiring Technology
for People

GUÍA COMPLETA DE GOBIERNO DE IA

De la adopción acelerada de Inteligencia Artificial a una **gestión controlada, ética y estratégica empresarial.**

Área de Inteligencia Artificial

Fecha 17/09/2026

Versión 1.0

Clasificación: Público

ÍNDICE

01**El reto del gobierno IA****02****Qué implica gobernar la IA****03****Regulación y Estándares de Referencia****04****Inventario y Gestión del Riesgo****05****Datos, Privacidad y Trazabilidad****06****Seguridad de la IA****07****Gobierno de la IA Generativa****08****Responsabilidades y Ciclo de Vida****09****Roadmap de Implantación en 4 Fases**

El reto del gobierno IA

La Inteligencia Artificial se está incorporando a ritmo vertiginoso en desarrollo, análisis de datos, automatización, atención al cliente y gestión documental. No obstante, este despliegue masivo genera un ecosistema altamente distribuido que resulta complejo de controlar.

Además de los proyectos específicos de IA, las organizaciones consumen diariamente funcionalidades inteligentes empaquetadas en soluciones SaaS, plataformas cloud y herramientas de productividad diaria.

El desafío de las 5 preguntas clave

Una organización con un modelo de gobernanza maduro debe responder con absoluta precisión a:

- ¿Qué sistemas de IA utilizamos exactamente?
- ¿Para qué procesos de negocio concretos?
- ¿Qué datos procesan y dónde se alojan?
- ¿Qué riesgos operativos/legales presentan?
- ¿Quién es la persona u órgano responsable del sistema?

Gobierno de IA: Una capacidad transversal

El gobierno eficiente de la Inteligencia Artificial exige conectar de forma fluida cinco dimensiones clave:

Seguridad y datos

Protección de amenazas, calidad, privacidad y trazabilidad.

Compliance

Cumplimiento regulatorio, ético y normativo.

Negocio & IT

Qué tan grave sería la exposición de información sensible si se accede sin autorización.

Qué implica gobernar la IA

Un modelo de Gobierno de IA establece las estructuras, políticas y metodologías necesarias para desarrollar, adquirir y operar sistemas de IA respetando el apetito de riesgo de la organización.

Los Pilares del modelo

Política

Define usos permitidos, restringidos y prohibidos

Inventario

Registro centralizado de activos de IA

Riesgo

Evaluación del impacto operativo, ético y legal.

Control

Medidas de seguridad, supervisión e imparcialidad.

Responsabilidad

Evaluación del impacto operativo, ético y legal.

Evidencia

Trazabilidad y auditoría continua.

Qué implica gobernar la IA

El principio de proporcionalidad

El nivel de control debe adaptarse rigurosamente al riesgo del contexto. Una herramienta interna para redactar borradores no exige el mismo nivel de pruebas, gobernanza y validación que un algoritmo que automatiza decisiones de crédito o de selección de personal.

Mayor impacto



Mayor nivel de control

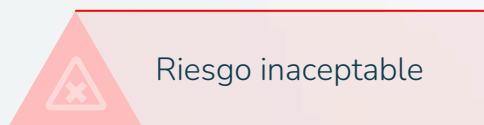
Regulación y Estándares de Referencia

El ecosistema de gobernanza exige combinar exigencias legales vinculantes con marcos técnicos y normativos internacionales para garantizar la resistencia y legalidad de los sistemas.

REGLAMENTO (UE) 2024/1689 (AI ACT)

Primer marco legal integral sobre IA a nivel mundial. Basado en un enfoque de gestión de riesgos con obligaciones escalonadas y fechas de aplicación progresiva (agosto 2026 para el grueso de requisitos de Alto Riesgo).

Categorías



Sistemas **prohibidos por su impacto** sobre derechos fundamentales o seguridad.



IA utilizada en:

- Educación
- Sanidad
- Fianzas
- Recusos humanos
- Infraestructura crítica
- Servicios esenciales



Requisitos de **transparencia** para asistentes virtuales o IA generativa.



Sistemas con **menor nivel de obligaciones** regulatorias.

Regulación y Estándares de Referencia

ISO/IEC 42001:2023 (SGIA)



Estándar internacional certificable para implantar un Sistema de Gestión de Inteligencia Artificial (SGIA) estructurado y de mejora continua.

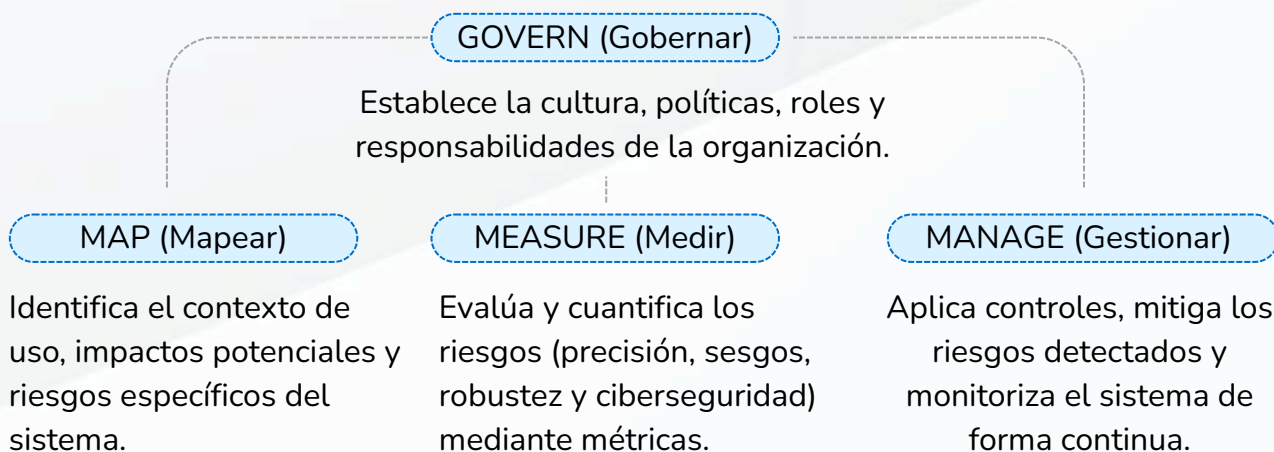
Aporta: Estructura organizativa, evaluación periódica, políticas corporativas y responsabilidad en todo el ciclo de vida del software.

ISO/IEC 23894

Proporciona orientaciones específicas para integrar la gestión de riesgos en IA en los procesos existentes de la organización (alineado con ISO 31000).

NIST AI RMF 1.0

Estructura la gestión del riesgo operacional mediante cuatro funciones clave continuas:



Regulación y Estándares de Referencia

Comparativa Visual de Marcos y Estándares

Vulnerabilidad	Criticidad	Enfoque principal	Acción Recomendada
EU AI Act	Reglamento obligatorio	Cumplimiento legal, protección de derechos fundamentales y seguridad	Mercado europeo / Sistemas que impacten a residentes en la UE.
ISO/IEC 42001	Estandar certificable	Sistema de gestión organizacional e integración de procesos (SGIA).	Organizaciones que desarrollan o utilizan soluciones de IA.
ISO/IEC 23894	Guía de buenas prácticas	Evaluación del riesgo y principios de la gestión de incertidumbres.	Equipos de Gestión de Riesgo, Auditoría Interna y CISO.
NIST AI RMF	Framework operativo	Gestión operacional continua del ciclo de vida del software.	Desarrolladores, arquitectos de software e ingenieros de datos.

La aplicación de cada marco debe analizarse evaluando la finalidad concreta del sistema, el rol de la organización (proveedor vs. desplegador) y los marcos territoriales aplicables.

Inventario y Gestión del Riesgo

"No se puede gobernar aquello que se desconoce". La base imprescindible para el control es construir un registro unificado que abarque soluciones propias, de terceros y capacidades embebidas en SaaS

Atributos Mínimos de un AI Inventory Corporativo

Campo del Inventario	Descripción y Evidencia Requerida
Sistema & Versión	Nombre comercial o técnico, identificador de versión y release actual.
Propietario (Owner)	Área de negocio o departamento responsable de la operación y costes.
Origen & Proveedor	Desarrollo interno, proveedor externo de software o componente SaaS
Finalidad & Impacto	Proceso de negocio soportado, nivel de autonomía y grado de criticidad.
Datos e Integraciones	Tipología de datos (confidencial, PII) y sistemas corporativos conectados
Clasificación Riesgo	Nivel resultante de la evaluación de impacto (Bajo, Medio, Alto, Prohibido).

Evaluación Contextual del Riesgo

El riesgo de la IA no es intrínseco al modelo, sino a su contexto de aplicación. Los factores determinantes incluyen el nivel de autonomía delegada, la exposición de datos y la reversibilidad de los impactos.

Inventario y Gestión del Riesgo

Riesgo Limitado / Bajo

Generación de resúmenes internos, ayuda a redacción de borradores o filtros de spam básico.

Riesgo Limitado / Bajo

Análisis automatizado de documentación corporativa para soporte a analistas.

Alto Riesgo / Crítico

Sistemas de soporte a decisiones de contratación, Scoring crediticio o salud



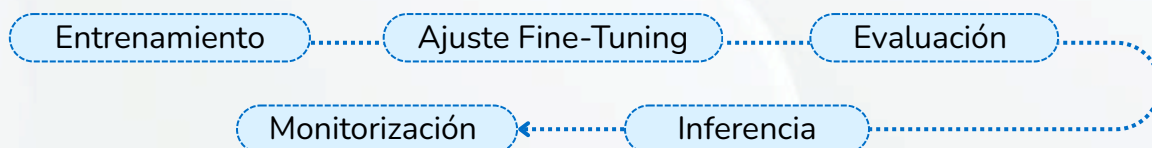
El Desafío del Shadow AI

El uso no autorizado de herramientas de IA externas por parte de empleados genera filtraciones masivas de información confidencial, violaciones del RGPD y dependencia opaca de proveedores. El gobierno debe combatirlo mediante una sólida combinación de políticas claras, formación continua, herramientas corporativas aprobadas y mecanismos técnicos de detección en red (CASB/DLP)

Datos, Privacidad y Trazabilidad

La calidad y legalidad de las decisiones generadas por una Inteligencia Artificial dependen de la calidad y gobierno de los datos que la alimentan en cada etapa de su ciclo de vida.

El Ciclo del Dato en Sistemas de IA



Preguntas Fundamentales de Privacidad

Origen

- ¿De dónde proceden los datos?
- ¿Existen bases legítimas, licencias y derechos suficientes para su tratamiento?

Contenido

- ¿Contienen datos de carácter personal (PII), secretos comerciales o información altamente sensible?

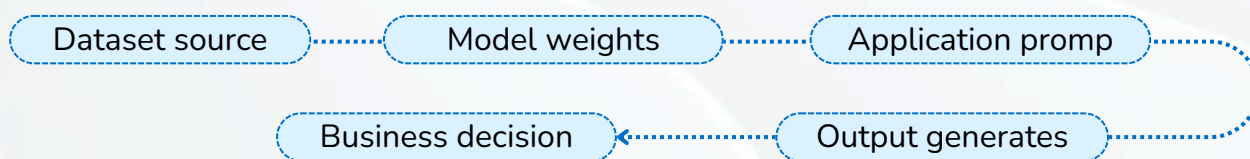
Destino

- ¿Cómo se conservan, protegen o transfieren?
- ¿El proveedor reutiliza los datos para entrenar sus modelos?

Datos, Privacidad y Trazabilidad

Trazabilidad de Extremo a Extremo

Un modelo maduro de gobernanza exige reconstruir el linaje completo de cualquier decisión automatizada o resultado generado por IA



Beneficios operativos:

- Respuesta ágil ante incidentes y fallos.
- Facilidad para superar auditorías externas.
- Gestión eficaz del cambio y versiones.

Requisitos garantizados:

- Explicabilidad de algoritmos a terceros.
- Asignación clara de responsabilidad.
- Cumplimiento estricto de normativas

Seguridad de la IA

La Inteligencia Artificial no solo requiere ciberseguridad tradicional; introduce vectores de ataque completamente nuevos dirigidos a prompts, modelos, pipelines de datos e integraciones.

Prompt Injection

Manipulación de entradas para saltarse restricciones éticas o ejecutar comandos no autorizados.

Data Poisoning

Corrupción deliberada de los datos de entrenamiento para sesgar el comportamiento del modelo.

Supply Chain Risks

Vulnerabilidades en modelos open-source, librerías, conectores y APIs de terceros.

Model Inversion / Theft

Extracción de datos de entrenamiento confidenciales o réplica del modelo mediante consultas

Security by Design

Mínimo privilegio, saneamiento riguroso de inputs/outputs, protección de APIs y monitorización continua en producción

 **Test****Deploy****Monitor****Detect****Respond**

Gobierno de la IA Generativa

La democratización masiva de la GenAI permite que cualquier área adopte capacidades avanzadas al instante. Sin embargo, su uso descentralizado genera riesgos críticos de alucinaciones y vulneración de PI.

Uso permitido

Herramientas corporativas bajo Enterprise SLA con datos protegidos y no reentrenados.

Uso restringido

Uso de código o documentos públicos sujeto a aprobación previa y validación humana.

Uso prohibido

Introducción de datos PII, secretos industriales o código core en herramientas públicas.

Idea clave: el factor humano

La gobernanza eficiente de GenAI exige capacitación: los empleados deben saber qué herramientas usar, cómo validar outputs, detectar alucinaciones y reportar posibles brechas de seguridad.

Responsabilidades y Ciclo de Vida

El Gobierno de IA requiere una asignación clara de funciones entre las diferentes áreas organizativas, acompañando al sistema desde su concepción hasta su retirada.

Matriz de Responsabilidades Organizativas

Alta Dirección

Aprobación de la estrategia, presupuesto y definición del apetito de riesgo corporativo.

Comité de Gobierno de IA

Supervisión transversal, aprobación de políticas y resolución de excepciones de uso.

CISO / CTO / CIO

Garantía de robustez técnica, ciberseguridad, arquitectura e integraciones de IT.

DPO & Legal / Compliance

Privacidad de datos, impacto RGPD, cumplimiento de AI Act y supervisión contractual.

Business Owners

Responsables del valor de negocio del sistema, supervisión operativa y uso correcto.

AI / Data Engineering

Team Desarrollo, alineación de modelos, pruebas de robustez, monitoreo y documentación.

Responsabilidades y Ciclo de Vida

Integración del Gobierno en el Ciclo de Vida (Lifecycle Governance)

En alineación con NIST AI RMF y la norma ISO 42001, la gestión del riesgo debe aplicarse de forma continua en cada fase de desarrollo e implantación:

Idea

Definición del caso de uso, alineación con estrategia y validación preliminar de viabilidad.

Diseño

Arquitectura, evaluación de impacto en privacidad (EIPD), análisis de riesgo y datos.

Desarrollo

Construcción del modelo, pruebas de mitigación de bias, documentación y seguridad.

Validación

Auditoría pre-despliegue, pruebas de penetración y aprobación formal del Owner.

Producción

Despliegue controlado, supervisión humana en bucle (HITL) y monitoreo de deriva.

Retirada

Gestión de cambios mayores o desactivación del sistema y archivado seguro de evidencias.

Roadmap de Implantación en 4 Fases

1

Visibilidad

Creación del inventario inicial, detección de Shadow AI, identificación de proveedores y asignación de propietarios.

Entregable: AI Inventory Corporativo.

2

Evaluación

Clasificación de sistemas según riesgo, análisis de impacto en privacidad y auditoría de ciberseguridad.

Entregable: AI Risk Register.

3

Control

Publicación de políticas de uso, establecimiento del Comité de IA e integración de controles en CI/CD.

Entregable: AI Governance Framework.

4

Monitorización

Medición de KPIs, auditorías periódicas, formación continua a la plantilla y actualización de reglas.

Entregable: Continuous AI Governance.

Integra IA de forma segura y efectiva

CONTACTA CON NOSOTROS



www.qualoom.es



contacto@qualoom.es



(+34) 91 236 4808

