

Buen gobierno de la Inteligencia Artificial

Guía práctica para organizaciones que ya usan
o están adoptando sistemas de IA

CONTEXTO

La IA ya está dentro de tu organización

En la mayoría de las empresas, la IA ya se utiliza en el día a día: generación de contenido, análisis de datos, atención al cliente, selección de personal o soporte a decisiones. El reto ya no es si adoptarla, sino cómo hacerlo con control, trazabilidad y cumplimiento normativo.



Adopción silenciosa

Equipos y áreas incorporan IA sin pasar por procesos formales de aprobación.



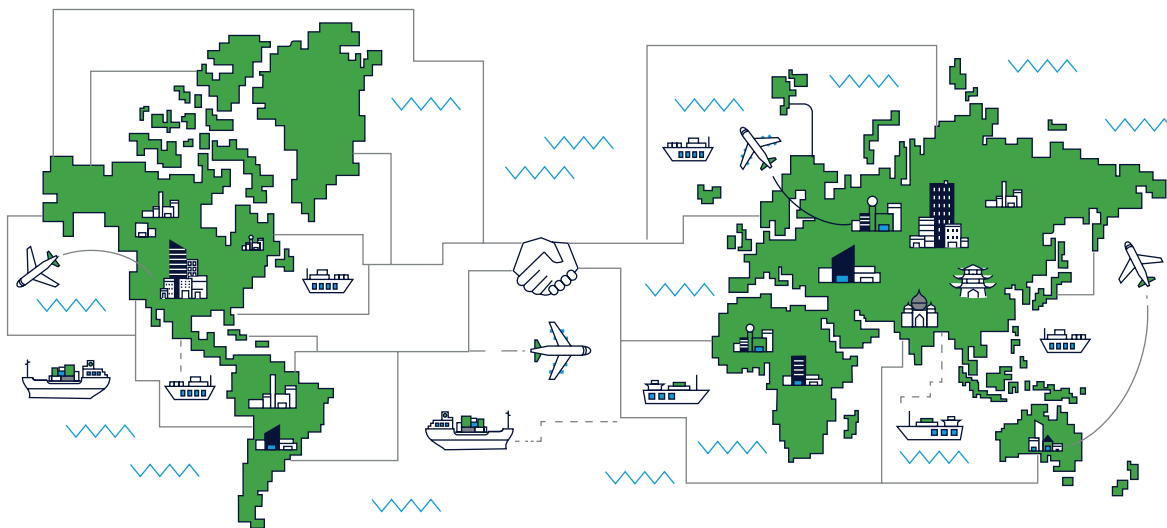
Visibilidad limitada

Pocas organizaciones tienen un inventario completo de sus sistemas de IA.



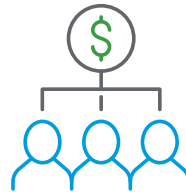
Marco regulatorio nuevo

El AI Act se suma al RGPD y exige un enfoque de cumplimiento conjunto.



RETOS HABITUALES · 1 DE 2**Lo que más cuesta gobernar en la práctica****Shadow AI**

Herramientas de IA usadas por equipos sin conocimiento ni aprobación de la organización.

**Responsabilidad difusa**

Nadie tiene asignada de forma clara la supervisión de los sistemas de IA en uso.

**Cumplimiento fragmentado**

RGPD, AI Act y normativa sectorial se gestionan por separado, sin visión conjunta.



RETOS HABITUALES · 2 DE 2

Y los que más exposición generan

**Decisiones poco explicables**

Sesgos, opacidad o falta de trazabilidad en resultados generados o soportados por IA.

**Terceros no controlados**

Proveedores que integran IA en sus servicios sin cláusulas ni garantías específicas.

Una causa común

Todos estos retos comparten el mismo origen: **la falta de un gobierno estructurado de la IA dentro de la organización.**

MARCO DE REFERENCIA RSM

6 pilares del buen gobierno de la IA

01



**Inventario &
clasificación**

02



**Roles &
responsabilidad**

03



**Evaluación
de impacto**

04



**Supervisión
humana**

05



**Terceros &
proveedores**

06



**Alfabetización
en IA**



PILAR 01 DE 6**Inventario & clasificación RESUELVE Shadow AI y falta de visibilidad**

Antes de escribir cualquier política, hay que saber qué sistemas de IA existen realmente en la organización: comprados, desarrollados internamente o embebidos en otras herramientas.

**ACCIONES PRÁCTICAS**

- ✓ Levanta un inventario por departamento, no solo por IT.
- ✓ Clasifica cada sistema según su nivel de Riesgo.
- ✓ Mantén el inventario como un registro vivo, no un ejercicio puntual.

PILAR 02 DE 6**Roles & responsabilidad** **RESUELVE** **Responsabilidad difusa**

Un sistema de IA sin un responsable claro es un riesgo. La gobernanza empieza por asignar quién decide, quién supervisa y quién responde.

**ACCIONES PRÁCTICAS**

- ✓ Nombra un responsable de IA o comité.
- ✓ Define quién aprueba nuevos usos antes de su despliegue.
- ✓ Integra la IA en los comités de riesgo y cumplimiento ya existentes.

PILAR 03 DE 6**Evaluación de impacto** **RESUELVE** **Cumplimiento fragmentado**

RGPD y AI Act comparten lógica:
identificar el riesgo antes de actuar.
Evaluar el impacto de forma conjunta
evita duplicar esfuerzos y huecos de
cumplimiento.

**ACCIONES PRÁCTICAS**

- ✓ Integra la evaluación de riesgo de IA en el proceso de DPIA/EIPD existente.
- ✓ Documenta las decisiones y las medidas de mitigación adoptadas.
- ✓ Revisa la evaluación antes de escalar cualquier sistema a producción.

PILAR 04 DE 6**Supervisión humana** **RESUELVE** Decisiones poco explicables

Cuando una decisión automatizada afecta a personas, debe poder explicarse, revisarse y corregirse. La supervisión humana es la garantía frente al sesgo y la opacidad.

**ACCIONES PRÁCTICAS**

- ✓ Registra el uso y los resultados relevantes de los sistemas de IA (logs).
- ✓ Revisa periódicamente los resultados, no solo en el momento del despliegue.
- ✓ Habilita un mecanismo de reclamación o corrección para las personas afectadas.

PILAR 05 DE 6**Terceros & proveedores** **RESUELVE** Terceros no controlados

Es habitual usar IA de terceros sin saberlo: proveedores que la incorporan a sus propios servicios. El control contractual es la única forma de gestionar ese riesgo.

**ACCIONES PRÁCTICAS**

- ✓ Incluye un cuestionario de debida diligencia específico de IA para proveedores.
- ✓ Incorpora cláusulas contractuales sobre uso, datos y responsabilidad en IA.
- ✓ Revisa también los contratos ya vigentes, no solo los nuevos.

PILAR 06 DE 6**Alfabetización en IA RESUELVE Falta de formación en el uso de la IA**

El AI Act (art. 4) exige que quien use o supervise IA tenga los conocimientos para hacerlo con seguridad y sentido crítico. Sin ella, el resto de pilares pierde eficacia.

**ACCIONES PRÁCTICAS**

- ✓ Diseña un plan de formación diferenciado por rol: usuarios, supervisores y responsables.
- ✓ Adapta el contenido formativo al nivel de riesgo de los sistemas usados.
- ✓ Documenta la formación impartida como evidencia de cumplimiento.

ACOMPANIAMIENTO RSM

Cómo te ayudamos a implementarlo



Diagnóstico inicial

Mapa de sistemas de IA en uso y nivel de madurez de gobierno actual.



Diseño del marco

Políticas, roles y procesos de gobierno de IA a medida de la organización.



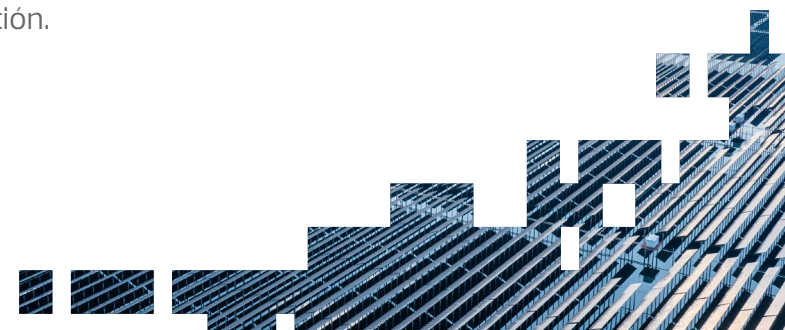
ISO/IEC 42001

Implantación del sistema de gestión de IA y preparación para certificación.



Formación

Capacitación práctica para equipos técnicos, legales y dirección.



El AI Act ya convive en la mayoría de organizaciones.



RSM Spain
Óscar López
Partner | Risk Advisory Services

HABLEMOS