



AI Act Compliance Checklist para CTOs

Guía práctica de gobernanza, auditoría y
seguridad para cumplir con la regulación de IA
en la Unión Europea.

1. Clasificación y análisis de riesgo

- ¿El sistema usa IA generativa, predictiva o de decisión?
- ¿Has clasificado cada sistema según el AI Act (riesgo mínimo, limitado, alto riesgo)?
- ¿Tienes inventariados los modelos, datasets y APIs externas involucradas?

2. Documentación técnica y trazabilidad

- ¿Existe documentación técnica actualizada del modelo y su arquitectura?
- ¿Utilizas un sistema de versionado de modelos (model registry)?
- ¿Registras decisiones automatizadas y sus resultados para auditoría?

3. Supervisión humana

- ¿Existe un flujo claro de intervención humana para casos críticos?
- ¿Hay roles definidos responsables de supervisar, revisar y aprobar el modelo?
- ¿Informas al usuario cuando está interactuando con un sistema de IA?

4. Datos, seguridad y privacidad

- ¿Los datos utilizados cumplen con el RGPD y otras normativas aplicables?
- ¿Tienes controles para detectar y mitigar sesgos o impactos no deseados?
- ¿El sistema está protegido frente a ataques adversarios y fugas de información?

5. Ciclo de vida del modelo

- ¿Monitorizas el rendimiento del modelo en producción de forma continua?
- ¿Reentrenas el modelo cuando cambian los datos o el contexto de negocio?
- ¿Dispones de un proceso para corregir, desactivar o retirar modelos en caso de riesgo?

6. Infraestructura y auditoría cloud

- ¿Tu arquitectura cloud cumple requisitos de seguridad, trazabilidad y segregación de entornos?
- ¿Controlas el uso de recursos para evitar configuraciones inseguras o sobrecostes inesperados?
- ¿Utilizas herramientas compatibles con el marco europeo, como Cloud-Trim, para optimizar y auditar tu entorno?

7. Preparación para auditoría

- ¿Cuentas con toda la documentación necesaria para demostrar cumplimiento ante una auditoría?
- ¿Puedes aportar evidencia de supervisión humana, mitigación de riesgos y trazabilidad del modelo?
- ¿Existe un responsable o equipo asignado al cumplimiento del AI Act dentro de la organización?