JEFEDEPROYECTOS.COM

# CHECKLIST DE AUDITORÍA AI ACT PARA PROJECT MANAGERS (2026)

### 1. CLASIFICACIÓN DEL NIVEL DE RIESGO

Antes de auditar, identifica en qué categoría cae tu proyecto:

- [ ] **Riesgo Inaceptable:** (Sistemas de puntuación social, manipulación de comportamiento). *Acción: Cancelación inmediata del proyecto.*
- [ ] **Alto Riesgo:** (Infraestructuras críticas, educación, empleo, salud, biometría). *Acción: Cumplimiento estricto de toda esta lista.*
- [ ] **Riesgo Limitado/Mínimo:** (Chatbots generales, filtros de spam). *Acción: Obligación de transparencia (hay que informar que es una IA).*

---

## 2. GOBERNANZA Y CALIDAD DE DATOS

- [ ] **Procedencia:** ¿Está documentada la fuente de todos los datasets de entrenamiento, validación y test?
- [ ] **Sesgos:** ¿Se han realizado pruebas estadísticas para detectar sesgos discriminatorios (género, raza, edad) en los datos de entrada?
- [ ] **Gobernanza:** ¿Existe un protocolo de limpieza y etiquetado de datos que minimice errores sistemáticos?

---

## 3. DOCUMENTACIÓN TÉCNICA Y TRANSPARENCIA

- [ ] **Ficha Técnica (Model Card):** ¿Existe un documento que detalle las capacidades, limitaciones y métricas de rendimiento del modelo?
- [ ] **Instrucciones de Uso:** ¿Están claros los escenarios en los que la IA NO debe ser utilizada?
- [ ] **Explicabilidad:** ¿Contamos con herramientas (p.e.: SHAP, LIME) para explicar la lógica detrás de las decisiones de alto impacto?

---

## 4. SUPERVISIÓN HUMANA Y ROBUSTEZ

- [ ] **Human-in-the-loop:** ¿Existe un mecanismo para que un humano pueda intervenir, anular o corregir una decisión de la IA en tiempo real?
- [ ] **Ciberseguridad:** ¿Se han realizado pruebas de estrés contra ataques adversarios (data poisoning, prompt injection)?
- [ ] **Tasa de Error:** ¿Están definidos los umbrales de error aceptables antes de que el sistema se detenga automáticamente?

---

## 5. REGISTRO DE ACTIVOS (LOGGING)

- [ ] **Trazabilidad:** ¿El sistema genera logs automáticos de todos los eventos durante su ciclo de vida para permitir auditorías post-despliegue?
- [ ] **Control de Versiones:** ¿Podemos reproducir una decisión tomada por una versión específica del modelo y de los datos (Versionado de Modelos/DVC)?

---

## BLOQUE DE ACCIÓN PARA EL JEFE DE PROYECTOS

**Certificación:** Una vez completado este checklist, el proyecto debe contar con una **Declaración UE de Conformidad** y, si es de alto riesgo, el marcado **CE** antes de su puesta en servicio.