AcreditaPRO

MANUAL DE ESTUDIO

Ética y Riesgos de la IA en el Entorno Laboral

Material de apoyo para la preparación del examen

Formación impartida conforme al artículo 4 del Reglamento (UE) 2024/1689 (AI Act), al Reglamento (UE) 2016/679 (RGPD) y a la Ley Orgánica 3/2018 (LOPDGDD), en materia de uso ético y responsable de sistemas de inteligencia artificial.

Generado el 12/11/2026

© AcreditaPro

Índice

1. 1. Introducción y objetivos del curso
2. 2. ¿Por qué importa la ética en la IA?
3. 3. El AI Act y la clasificación de riesgo ético
4. 4. Riesgos técnicos: alucinaciones y errores
5. 5. Sesgos algorítmicos: qué son y cómo afectan
6. 6. Privacidad y protección de datos en el uso de IA
7. 7. Transparencia: saber cuándo se usa IA
8. 8. Derechos laborales y IA en el trabajo
9. 9. IA en contratación y evaluación de empleados
0. 10. Vigilancia y monitorización con IA
11. 11. Deepfakes y desinformación
12. 12. Propiedad intelectual y contenido generado por IA
13. 13. Responsabilidad: ¿quién responde cuando la IA se equivoca?
4. 14. La IA y las decisiones de alto impacto
5. 15. Dependencia tecnológica y resiliencia
6. 16. IA y desigualdad: brechas digitales
17. 17. El papel del empleado en el uso responsable de la IA
8. 18. Cómo denunciar usos indebidos de IA en la empresa
9. 19. Buenas prácticas de uso ético de IA
0. 20. Resumen de puntos clave
21. 21. Anexo normativo: marco de referencia
22. 22. Glosario de términos

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

Este curso acredita competencias en el uso ético y responsable de la inteligencia artificial en el trabajo, conforme al artículo 4 del Reglamento (UE) 2024/1689 (AI Act) y al Marco Europeo de Competencias Digitales DigComp 3.0. Es una acreditación de competencias profesionales con base normativa específica.

1. Introducción y objetivos del curso

La IA es una herramienta poderosa — y como toda herramienta poderosa, puede usarse bien o mal. La diferencia está en las personas que la usan y en las organizaciones que la despliegan. Entender los riesgos éticos de la IA no es alarmismo — es la base para usarla de forma responsable y para saber cuándo hay que decir no o pedir explicaciones.

Al finalizar este curso, serás capaz de:

- Identificar los principales riesgos éticos de la IA en el entorno laboral.
- Conocer tus derechos como empleado cuando la empresa usa IA.
- Aplicar principios de uso responsable de herramientas de IA.
- Saber cuándo y cómo denunciar usos indebidos de IA en la empresa.

2. ¿Por qué importa la ética en la IA?

La IA no es neutral — los sistemas de IA toman decisiones que afectan a personas: quién recibe una oferta de empleo, quién obtiene un crédito, qué noticias ve cada usuario. Y esas decisiones pueden estar sesgadas, ser opacas o ser difíciles de impugnar.

La ética en la IA no es un tema abstracto para filósofos — es una cuestión práctica para cualquier empleado que usa o es afectado por sistemas de IA. La diferencia entre una empresa que usa IA éticamente y una que no es la diferencia entre una herramienta que amplifica el talento humano y una que perpetúa discriminaciones o elimina garantías laborales.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

3. El AI Act y la clasificación de riesgo ético



El Reglamento (UE) 2024/1689 (AI Act) clasifica los sistemas de IA por su nivel de riesgo:

- **Riesgo inaceptable (PROHIBIDO)**: manipulación subliminal, puntuación social, reconocimiento de emociones en el trabajo. Prohibidos en la UE.
- **Alto riesgo (REGULADO)**: IA en contratación, crédito, justicia, infraestructuras críticas. Obligatoria supervisión humana, registro, auditoría y derecho del afectado a explicación.
- **Riesgo limitado (TRANSPARENCIA)**: chatbots y deepfakes — obligación de informar al usuario de que interactúa con IA.
- **Riesgo mínimo (LIBRE)**: filtros de spam, juegos, herramientas de productividad.

El AI Act (art. 86) también reconoce el derecho del trabajador afectado por una decisión de IA de alto riesgo a obtener una explicación comprensible de esa decisión.

4. Riesgos técnicos: alucinaciones y errores

El riesgo técnico más conocido de la IA generativa son las alucinaciones: el sistema genera información falsa (fechas, cifras, citas, nombres) con total apariencia de veracidad.

Ejemplos reales de errores graves por alucinaciones de IA:

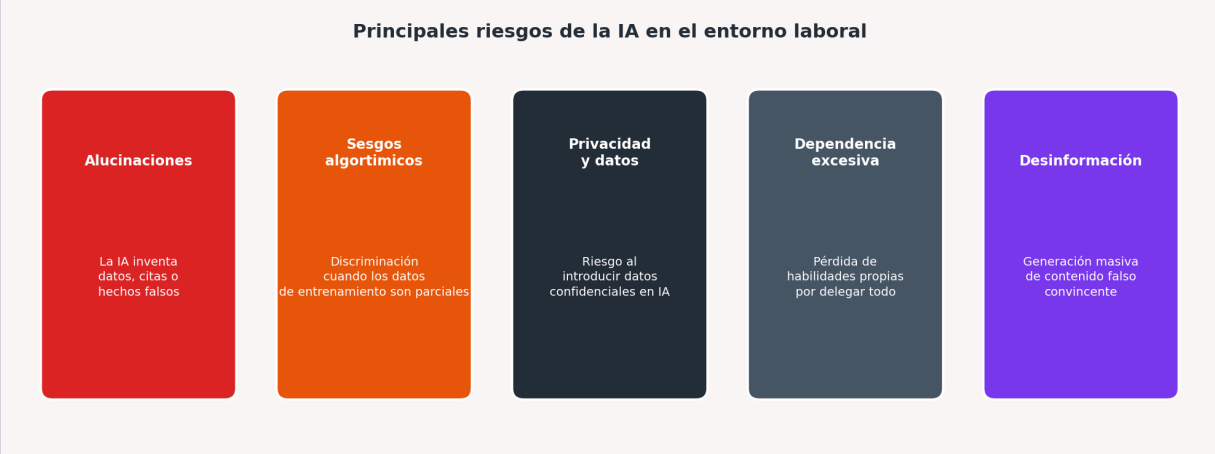
- Abogados que presentaron citas de sentencias inexistentes generadas por ChatGPT.
- Informes médicos con dosis incorrectas calculadas por IA.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

- Artículos periodísticos que citaban estudios que nunca existieron.

La solución no es no usar IA — es verificar siempre los datos factuales críticos antes de usarlos en documentos oficiales o decisiones importantes.

5. Sesgos algorítmicos: qué son y cómo afectan



Los sesgos algorítmicos son tendencias de los sistemas de IA a producir resultados discriminatorios o injustos, originadas en los datos con los que fueron entrenados.

Ejemplos documentados:

- Sistemas de selección de CV que penalizaban a candidatas mujeres porque el modelo aprendió de datos históricos de contratación donde predominaban los hombres.
- Herramientas de reconocimiento facial con tasas de error significativamente más altas en personas de piel oscura.
- Algoritmos de concesión de crédito que penalizaban a personas de ciertos códigos postales históricamente marginados.

Los sesgos no son inevitables — pero requieren detección activa y corrección deliberada. Un sistema de IA no es objetivo por el hecho de ser automático.

6. Privacidad y protección de datos en el uso de IA

El uso de IA en el trabajo genera riesgos específicos para la privacidad:

Riesgo 1 — Datos de empleados: muchos sistemas de IA de RRHH (análisis de productividad, evaluación de desempeño, predicción de abandono) recopilan datos de los empleados que pueden afectar a sus condiciones laborales sin que sean plenamente conscientes.

Riesgo 2 — Datos de clientes: introducir datos de clientes en herramientas de IA públicas puede violar el RGPD si esos datos se usan para entrenar el modelo o se almacenan en servidores de terceros sin el consentimiento adecuado.

Riesgo 3 — Datos confidenciales de la empresa: información estratégica, patentes, datos financieros o planes de negocio introducidos en herramientas de IA públicas pueden quedar expuestos.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

7. Transparencia: saber cuándo se usa IA

La transparencia es uno de los principios fundamentales del uso ético de la IA. En la práctica, significa:

- **Para empresas**: informar a los clientes cuando se usa IA en la atención al cliente, en la generación de contenido o en la toma de decisiones que les afecten.
- **Para empleados**: saber cuándo la empresa usa IA para evaluar su trabajo, monitorizar su actividad o tomar decisiones sobre su carrera.
- **Para todos**: el AI Act obliga a los sistemas de chatbots y deepfakes a identificarse como IA.

La falta de transparencia sobre el uso de IA no es solo un problema ético — puede ser una infracción legal según el AI Act y el RGPD.

8. Derechos laborales y IA en el trabajo

Como empleado, tienes derechos específicos cuando tu empresa usa IA:

- **Derecho a la información**: saber si la empresa usa sistemas de IA que te afectan y para qué.
- **Derecho a no ser evaluado solo por IA**: el AI Act exige supervisión humana en sistemas de alto riesgo como los de evaluación de empleados.
- **Derecho a una explicación**: para decisiones de alto impacto tomadas con IA (no contratación, despido, evaluación), tienes derecho a una explicación comprensible.
- **Derecho a impugnar**: puedes solicitar revisión humana de decisiones automatizadas que te afecten significativamente (derecho del RGPD, art. 22.3, y de la LOPDGDD, art. 22; no del AI Act, que exige supervisión humana como obligación de diseño, art. 14).

El Estatuto de los Trabajadores y la normativa de protección de datos también limitan cómo las empresas pueden usar IA para monitorizar a los empleados.

9. IA en contratación y evaluación de empleados

Los sistemas de IA en RRHH son uno de los ámbitos de mayor riesgo ético. Usos comunes:

- **Cribado de CVs**: herramientas que filtran candidaturas automáticamente. Riesgo: sesgo en los criterios de filtrado.
- **Análisis de entrevistas en vídeo**: sistemas que analizan expresiones faciales, tono de voz y palabras usadas. Bajo el AI Act, el reconocimiento de emociones en el trabajo es de alto riesgo o incluso prohibido.
- **Evaluación de desempeño**: algoritmos que calculan puntuaciones de productividad. Riesgo: no capturan el valor real del trabajo, especialmente el trabajo colaborativo o de soporte.

Si eres candidato o empleado afectado por estos sistemas, tienes derecho a saber que se usan y a solicitar revisión humana.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

10. Vigilancia y monitorización con IA

La expansión del trabajo remoto ha impulsado el uso de software de vigilancia laboral: herramientas que capturan pantallas periódicamente, analizan el tiempo activo en el teclado, o monitorizan el uso de aplicaciones.

El uso de estas herramientas en España tiene límites legales claros:

- Los trabajadores deben ser informados del uso de herramientas de monitorización.
- La vigilancia debe ser proporcional — no se puede monitorizar todo sin justificación.
- El Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos han limitado la vigilancia excesiva en el trabajo.

11. Deepfakes y desinformación

Los deepfakes son contenidos multimedia (vídeo, audio, imagen) generados o manipulados por IA para hacer parecer que alguien dijo o hizo algo que no hizo. Los riesgos en el entorno laboral:

- **Fraude empresarial**: casos reales de directivos suplantados en videollamadas para autorizar transferencias.
- **Daño reputacional**: vídeos falsos de personas en situaciones comprometidas.
- **Desinformación interna**: documentos o audios falsos que generan conflictos en el equipo.

El AI Act obliga a los deepfakes a identificarse como tal. Si recibes un video o audio sorprendente de alguien, verifica su autenticidad por otra vía antes de actuar.

12. Propiedad intelectual y contenido generado por IA

La propiedad intelectual del contenido generado por IA es un área legal en evolución. Algunas consideraciones prácticas:

- **¿Puedo usar contenido generado por IA en mi trabajo?** Depende de la política de tu empresa y de los términos de la herramienta.
- **¿El contenido de IA es original?** No en el sentido legal clásico — los modelos aprenden de millones de obras con derechos de autor, lo que genera debates legales en curso.
- **Riesgo de plagio involuntario**: la IA puede generar texto muy similar a obras existentes sin que el usuario lo sepa.

Buena práctica: no uses contenido de IA para publicaciones externas, propuestas comerciales o documentos legales sin verificar que no reproduce contenido protegido.

13. Responsabilidad: ¿quién responde cuando la IA se equivoca?

Una pregunta central en la ética de la IA: si un sistema de IA toma una decisión errónea que perjudica a una persona, ¿quién es responsable?

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

La respuesta actual es clara: **la responsabilidad recae en las personas y organizaciones que despliegan y usan la IA**, no en la IA misma. Esto tiene implicaciones directas para los empleados:

- Si usas IA para generar un informe con datos erróneos y ese informe causa un perjuicio, la responsabilidad es tuya.
- Si tu empresa usa IA para tomar decisiones de contratación discriminatorias, la empresa es responsable.
- La IA no es una excusa legal — "lo dijo la IA" no exime de responsabilidad.

14. La IA y las decisiones de alto impacto

Las decisiones de alto impacto son aquellas que afectan significativamente a la vida de las personas: contratación, despido, crédito, diagnóstico médico, sentencia judicial. Para estas decisiones, la ética y la ley (AI Act) exigen:

- **Supervisión humana**: una persona debe revisar y poder anular la decisión de la IA.
- **Explicabilidad**: el afectado tiene derecho a entender por qué la IA tomó esa decisión.
- **Auditabilidad**: el sistema debe dejar registro que permita revisarlo.
- **Derecho de recurso**: el afectado puede solicitar revisión humana.

15. Dependencia tecnológica y resiliencia

Un riesgo menos visible pero real es la dependencia excesiva de la IA: cuando los sistemas de IA dejan de funcionar (por fallos técnicos, problemas de conexión o desaparición del proveedor), los empleados que dependían de ellos se quedan sin herramientas.

Buenas prácticas para la resiliencia:

- Mantener las habilidades básicas aunque la IA las pueda hacer — si la IA falla, tú puedes continuar.
- No delegar en IA ningún proceso crítico sin un plan de respaldo manual.
- Conocer las alternativas a las herramientas de IA que usas habitualmente.

16. IA y desigualdad: brechas digitales

La IA puede ampliar las brechas existentes entre quienes tienen acceso a buenas herramientas y conocimientos digitales y quienes no. En el entorno laboral:

- Los empleados con mejor acceso a herramientas de IA y formación para usarlas tendrán más ventajas.
- Los sectores con mayor proporción de trabajo manual o con menor acceso a tecnología son más vulnerables a la automatización sin acceso a las oportunidades que crea la IA.
- La formación en IA no puede ser solo para los perfiles más cualificados — debe llegar a todos los empleados.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

17. El papel del empleado en el uso responsable de la IA

Cada empleado que usa IA tiene responsabilidades concretas:

- **Verificar antes de confiar**: no publicar ni actuar sobre datos de IA sin verificarlos.
- **No compartir confidencial**: nunca datos de clientes o información estratégica en herramientas públicas.
- **Reportar anomalías**: si un sistema de IA produce resultados que parecen sesgados o incorrectos, reportarlo al equipo responsable.
- **Mantener el juicio propio**: la IA asiste, no decide. La responsabilidad final es siempre humana.
- **Informarse**: conocer las políticas de uso de IA de la empresa y mantenerse actualizado.

18. Cómo denunciar usos indebidos de IA en la empresa

Si detectas que tu empresa usa IA de forma que puede ser ilegal o contraria a los derechos de los trabajadores:

1. **Documenta**: guarda evidencias de lo que observas.
2. **Canal interno**: primero, usa el canal de denuncias interno de la empresa (obligatorio para empresas de 50 o más trabajadores desde la Ley 2/2023: desde el 13 de junio de 2023 las de 250 o más, y desde el 1 de diciembre de 2023 las de 50 a 249).
3. **Autoridad de control**: la Agencia Española de Protección de Datos (AEPD) recibe denuncias sobre usos de IA que violen el RGPD. La Inspección de Trabajo recibe denuncias sobre vigilancia laboral indebida.
4. **Representación sindical**: los representantes de los trabajadores tienen derecho a ser informados sobre el uso de IA que afecte a las condiciones laborales.

19. Buenas prácticas de uso ético de IA

- **Verifica siempre** los datos factuales antes de usarlos en documentos oficiales.
- **No compartas datos confidenciales** de clientes, empleados o estrategia en herramientas de IA públicas.
- **Cuestiona las decisiones de IA** que te afecten — tienes derecho a una explicación.
- **Informa si detectas sesgos**: si un sistema de IA produce resultados que parecen injustos o discriminatorios, repórtalo.
- **Mantén tus habilidades**: no dependas completamente de la IA para tareas críticas.
- **Sé transparente**: cuando uses IA para generar contenido que otros van a leer como tuyo, asegúrate de que cumple los estándares que aplicarías a tu trabajo propio.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

20. Resumen de puntos clave

- La IA no es neutral — los sesgos en los datos de entrenamiento producen resultados sesgados.
- El AI Act prohíbe el reconocimiento de emociones en el trabajo y exige supervisión humana en sistemas de alto riesgo.
- Como empleado, tienes derecho a saber cuándo la IA te afecta y a solicitar revisión humana de decisiones automatizadas.
- La responsabilidad por los errores de la IA recae en las personas y organizaciones que la usan, no en la IA.
- Verificar datos, no compartir información confidencial y mantener el juicio propio son las tres responsabilidades básicas de todo empleado que usa IA.

21. Anexo normativo: marco de referencia

- **Reglamento (UE) 2024/1689 (AI Act)**: clasificación de riesgo de sistemas de IA, prohibiciones, obligaciones de transparencia, supervisión humana y derechos de los afectados.
- **Reglamento (UE) 2016/679 (RGPD)**: protección de datos personales en el uso de sistemas de IA.
- **Ley Orgánica 3/2018 (LOPDGDD)**: derechos digitales en el trabajo, incluyendo limitaciones a la vigilancia laboral con tecnología.
- **Ley 2/2023**: canal de denuncias obligatorio para empresas de 50 o más trabajadores (250 o más desde el 13 de junio de 2023; de 50 a 249 desde el 1 de diciembre de 2023).

22. Glosario de términos

- **AI Act**: Reglamento (UE) 2024/1689, primera regulación mundial sobre inteligencia artificial, que clasifica los sistemas de IA por riesgo y establece obligaciones para empresas y empleados.
- **Alucinación**: fenómeno por el que una IA genera información falsa con apariencia de veracidad.
- **Sesgo algorítmico**: tendencia de un sistema de IA a producir resultados discriminatorios por sesgos en sus datos de entrenamiento.
- **Deepfake**: contenido multimedia (vídeo, audio, imagen) generado o manipulado por IA para hacer parecer que alguien dijo o hizo algo que no hizo.
- **Supervisión humana**: principio del AI Act que exige que una persona pueda revisar y anular las decisiones de sistemas de IA de alto riesgo.
- **Explicabilidad**: derecho del afectado por una decisión de IA a recibir una explicación comprensible de cómo se tomó esa decisión.
- **Auditabilidad**: capacidad de revisar y supervisar externamente cómo funciona un sistema de IA y qué decisiones ha tomado.
- **Propiedad intelectual**: conjunto de derechos sobre obras creadas, cuya aplicación al contenido generado por IA es un área legal en evolución.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.

- **Resiliencia digital**: capacidad de mantener el funcionamiento cuando las herramientas digitales (incluyendo IA) fallan o no están disponibles.
- **Canal de denuncias (whistleblowing)**: mecanismo interno de las empresas para reportar irregularidades, obligatorio desde la Ley 2/2023 para empresas de 50 o más trabajadores.

© AcreditaPro — Bimedio. Material gratuito, prohibida su reventa.