Módulo 6

IA segura: riesgos, datos, verificación y supervisión



Una respuesta rápida no garantiza que sea correcta

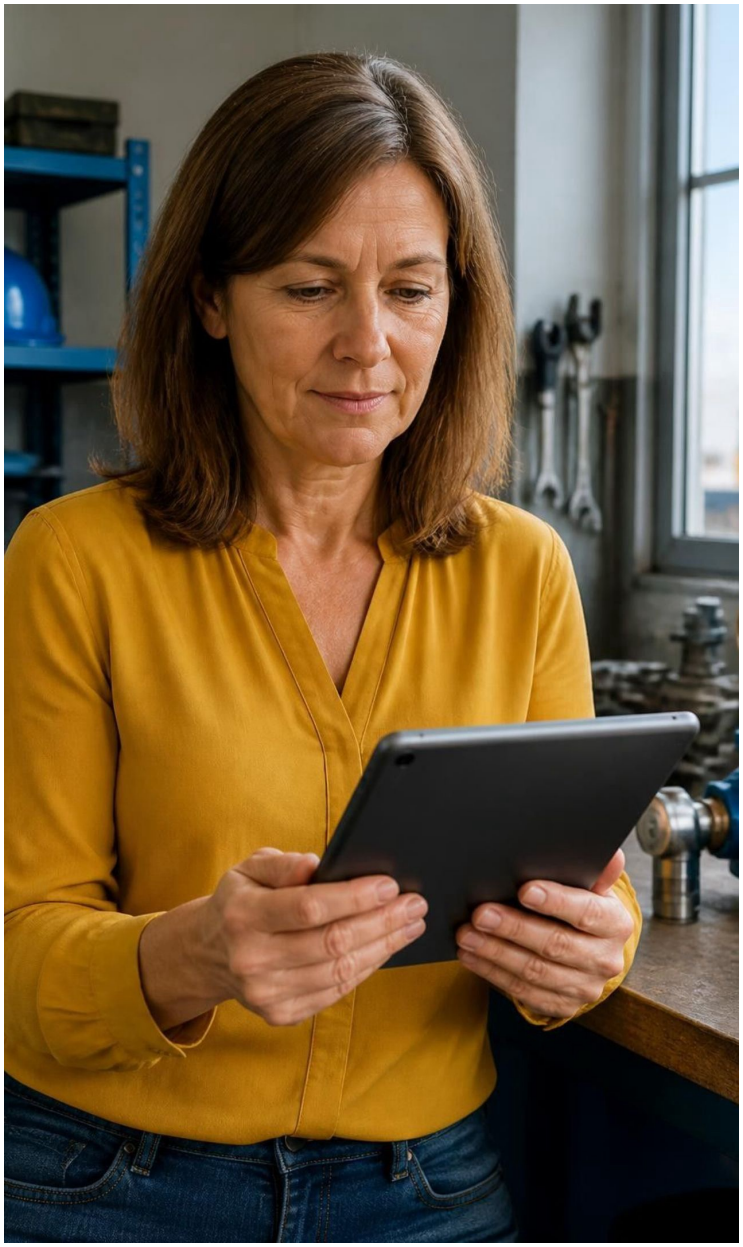
Usar IA con responsabilidad es aprovechar sus beneficios sin delegar decisiones, datos ni compromisos.

ANTES DE USARLA

Qué información necesita

Qué pasa si falla

Quién revisa



Riesgos frecuentes y cómo controlarlos

Riesgo	Qué puede ocurrir	Control
Información incorrecta	La IA genera un precio, fecha o dato no confirmado	Verificar con la fuente original antes de usarlo
Uso inadecuado	Se delega una decisión que requiere criterio humano	Definir límites y aprobación obligatoria

La IA apoya el trabajo, no sustituye la responsabilidad.



Comparte solo lo estrictamente necesario

Antes de copiar un documento, tabla o conversación, revisa si contiene datos personales, financieros, contraseñas o secretos comerciales.

SI HAY DUDA, NO LO COMPARTAS HASTA TENER AUTORIZACIÓN

Siete tipos de información, siete preguntas antes de usar IA

Personal

¿Identifica a una persona?

Financiera

¿Expone dinero o medios de pago?

Acceso

¿Permite entrar a un sistema?

Clientes

¿Incluye datos privados de terceros?

Comercial

Costos, márgenes, estrategia no pública.

Laboral

Evaluaciones, nómina.

Pública

¿Ya está autorizada para divulgarse?

Anonimiza: Cliente 01 en lugar de nombres y documentos

EN LUGAR DE

Nombres y documentos

ANONIMIZA

Cliente 01

Si la tarea puede resolverse con datos resumidos o anonimizados, el riesgo baja y el uso es más responsable.

Respeta las políticas internas y la normativa de privacidad.

La IA puede sonar convincente y estar equivocada

Puede inventar datos o sacar conclusiones que no se desprenden de lo que le diste.

Verificar es parte normal del proceso, no un paso opcional.



Verificar en seis pasos antes de usar el resultado

1. **Identificar**

   Qué datos son comprobables.

2. **Comparar**

   Con la fuente original.

3. **Separar**

   Hechos, inferencias y recomendaciones.

4. **Detectar**

   Supuestos no suministrados.

5. **Corregir**

   O pedir nueva versión.

6. **Autorizar**

   El uso tras la revisión.

Señales de alerta y plantilla de verificación

Señales de alerta

- Cifras, nombres o fuentes que no diste ni puedes comprobar.
- Certeza pese a información incompleta.
- Recomendaciones sin explicar en qué datos se apoyan.
- Contradice tus registros.

PLANTILLA

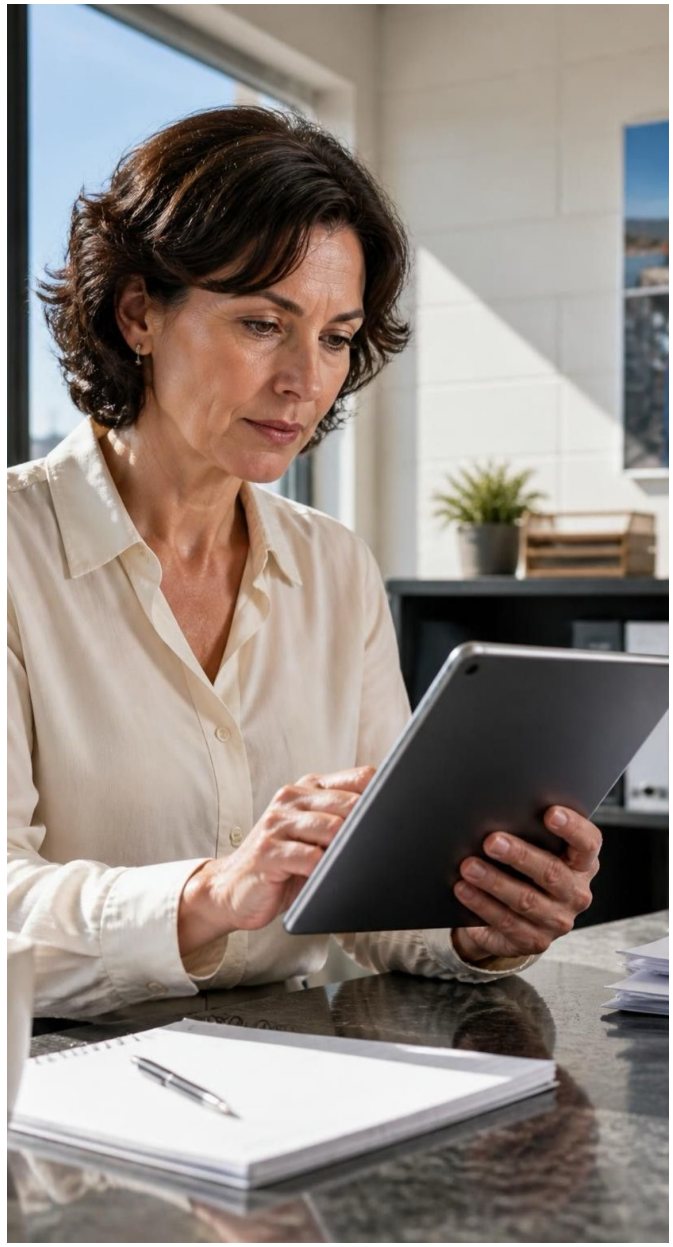
Pide separar

- Datos confirmados
- Información por verificar
- Supuestos

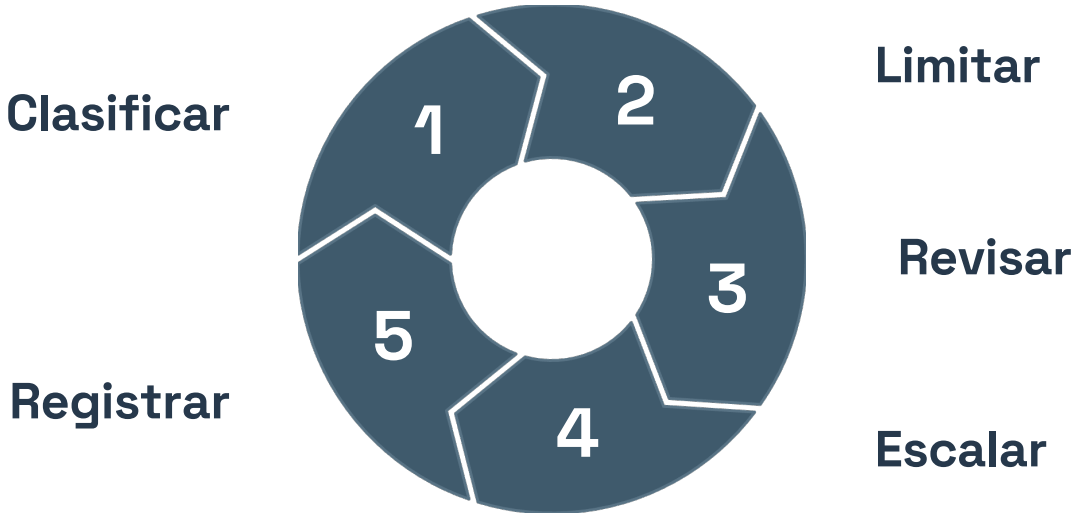
Sin agregar información nueva.

A mayor impacto, mayor supervisión

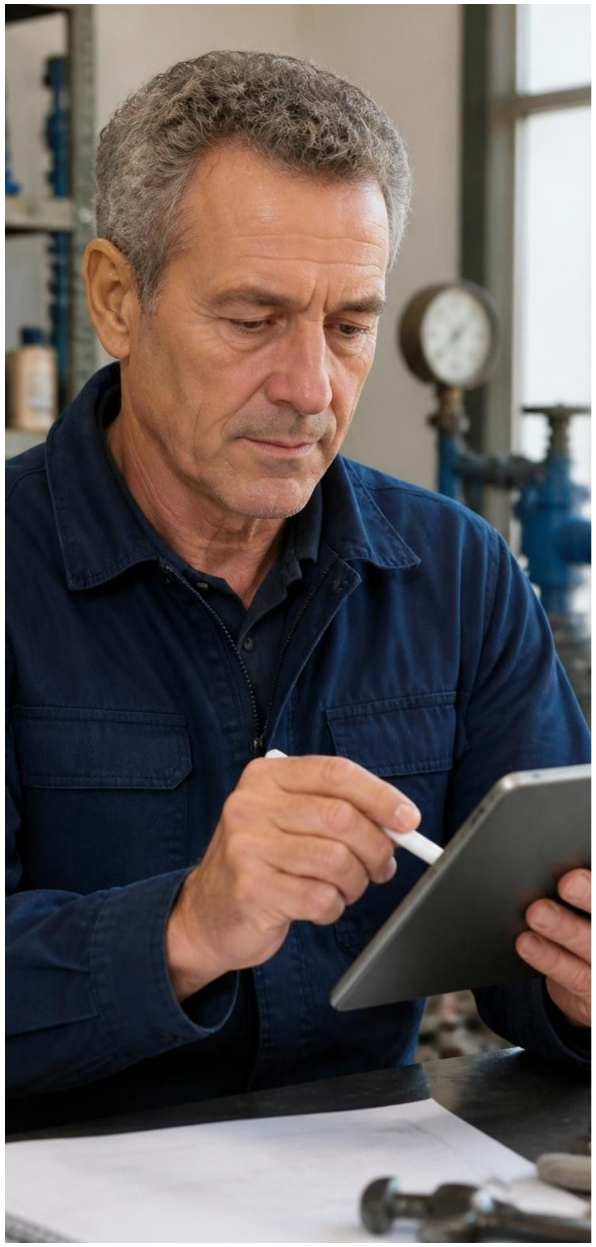
Impacto	Uso	Supervisión
Bajo	Borradores e ideas sin datos sensibles	Revisión habitual
Medio	Mensajes a clientes, análisis internos	Revisión obligatoria
Alto	Decisiones financieras, legales, laborales o de seguridad	Decisión humana y revisión especializada



Ciclo de supervisión: clasificar, limitar, revisar, escalar, registrar



Define qué puede hacer la IA, asigna a una persona responsable, consulta cuando haga falta y documenta datos, instrucciones, correcciones y versión usada.



Cierre: la responsabilidad final permanece en las personas

Lista de comprobación antes de usar IA:

1. Datos mínimos: solo la información necesaria.
2. Privacidad protegida: sin datos sensibles sin razón y autorización.
3. Exactitud verificada: cifras, nombres, fechas y condiciones.
4. Sesgos revisados: sin trato injusto ni conclusiones engañosas.
5. Supervisión definida: una persona responsable autoriza el uso.
6. Decisión documentada: aprobado, corregido o descartado, con razón.

La IA puede equivocarse. La información importante se verifica y la responsabilidad final sigue siendo de las personas.

PROMIPYME | Consejo Nacional de Promoción y Apoyo a la Micro, Pequeña y Mediana Empresa

ESPACIO DE REFLEXIÓN Y OPINIÓN

Tu experiencia cuenta

Compartamos lo aprendido en este encuentro académico.

01 ¿Qué conocimiento o herramienta de IA te resultó más útil?

02 ¿Cómo aplicarías lo aprendido en tu negocio o emprendimiento?

03 ¿Qué te pareció el encuentro académico y qué mejorarías?

