



GUÍA DE BUENAS PRÁCTICAS PARA UTILIZAR LA IA DE FORMA SEGURA EN TU EMPRESA

Cómo aprovechar la Inteligencia Artificial para analizar información, crear contenidos y mejorar la productividad

La Inteligencia Artificial está transformando la manera en que las empresas trabajan, se comunican y toman decisiones, ofreciendo nuevas oportunidades para mejorar su productividad y competitividad. Sin embargo, su incorporación también plantea desafíos relacionados con la seguridad, la privacidad y el uso responsable de la información.

Desde la **Oficina Acelera Pyme ADEME**, hemos elaborado esta guía de buenas prácticas con el objetivo de ayudar a pymes, personas autónomas y profesionales a aprovechar las ventajas de la Inteligencia Artificial de forma **segura, responsable y eficaz**.

A través de recomendaciones prácticas, ejemplos y herramientas de aplicación sencilla, esta guía ofrece las claves para integrar la IA en la actividad diaria de cualquier negocio, minimizando riesgos y fomentando una transformación digital basada en la confianza y la protección de los datos.

1. Por qué importa utilizar la IA con seguridad

Los asistentes de inteligencia artificial pueden apoyar la redacción, la búsqueda de ideas, la atención al cliente, la traducción y el análisis de información. Su utilidad no elimina la necesidad de controlar qué datos se comparten, qué decisiones se delegan y cómo se comprueban los resultados.

Cinco principios para cualquier pyme

Finalidad definida: utilizar la herramienta para una tarea concreta y legítima.

Minimización: compartir solo la información imprescindible.

Verificación: comprobar hechos, cálculos, enlaces y referencias antes de usarlos.

Supervisión: una persona responsable valida resultados y decisiones relevantes.

Trazabilidad: documentar herramientas, usos permitidos e incidencias.



Una distinción esencial

Una respuesta fluida no garantiza que sea correcta. La IA puede producir afirmaciones inexactas, referencias inexistentes o recomendaciones desactualizadas. También puede reproducir sesgos o divulgar información si se utiliza sin controles.

Ejemplo de uso apropiado

Una tienda quiere redactar una descripción genérica de un producto. Puede pedir un borrador con características públicas y revisar el resultado. No necesita compartir pedidos reales ni datos de sus compradores.

2. Identificar los riesgos antes de empezar

Antes de activar una herramienta, conviene clasificar cada tarea según la información implicada, el posible daño y el nivel de supervisión necesario.

Nivel	Ejemplos	Tratamiento recomendado
Bajo	Ideas de campañas, títulos, textos genéricos	Uso permitido con revisión básica
Medio	Resúmenes de documentación interna no sensible	Revisar condiciones, acceso y contenido
Alto	Datos de clientes, nóminas, expedientes, salud	No introducir sin evaluación específica y garantías adecuadas

Preguntas de evaluación previa

- ¿Qué problema concreto queremos resolver?
- ¿Qué datos se introducirán y quién es su titular?
- ¿La herramienta conserva entradas o las usa para entrenar modelos?
- ¿Se puede trabajar con información anonimizada o ficticia?
- ¿Qué sucede si la respuesta es incorrecta?
- ¿Quién aprueba el resultado antes de enviarlo o publicarlo?

Regla operativa: cuando una tarea afecte a derechos, obligaciones, decisiones económicas importantes o personas identificables, aumenta el nivel de control y solicita asesoramiento especializado cuando corresponda.



3. Datos personales y confidenciales

La protección de datos comienza antes de escribir el primer prompt. El hecho de que una herramienta sea fácil de utilizar no significa que sea adecuada para recibir cualquier información de la empresa.

Información que requiere especial precaución

- Datos de clientes y empleados: nombres, teléfonos, correos, identificadores, contratos y expedientes.
- Información sensible: datos de salud, datos biométricos y otras categorías especialmente protegidas.
- Secretos empresariales: precios negociados, estrategias, contraseñas, información financiera no pública.
- Documentos de terceros sujetos a compromisos de confidencialidad.

Alternativas más seguras

En lugar de...	Utiliza...
Pegar una reclamación con nombre y teléfono	Describir el caso sin identificadores personales
Subir un contrato completo	Plantear una consulta genérica o usar entorno autorizado
Compartir una base de datos de clientes	Trabajar con datos sintéticos o agregados
Pegar credenciales de acceso	Nunca compartir contraseñas, claves API o tokens

RGPD: qué revisar

Si se tratan datos personales, hay que determinar la base jurídica, la finalidad, los roles de responsable y encargado, las garantías contractuales, la conservación, las transferencias internacionales cuando existan y las medidas de seguridad apropiadas. La anonimización efectiva no equivale a sustituir únicamente el nombre por iniciales.



4. Uso responsable de herramientas y cuentas

La empresa debe saber qué herramientas utilizan sus trabajadores y bajo qué condiciones. El uso de cuentas personales para tareas profesionales puede dificultar el control de accesos y de la información compartida.

Controles mínimos

- Crear un inventario de herramientas autorizadas y finalidad de uso.
- Revisar políticas de privacidad, retención, configuración y condiciones del proveedor.
- Activar autenticación multifactor cuando esté disponible.
- Asignar permisos por función y retirar accesos al cambiar de puesto.
- Evitar extensiones, conectores y automatizaciones sin revisión previa.
- Establecer un canal para comunicar incidentes o respuestas problemáticas.

Configuración de privacidad

No debe asumirse que todos los planes o productos gestionan los datos del mismo modo. Antes de usar una herramienta, revisa la configuración concreta de la cuenta y la documentación contractual vigente; las opciones pueden cambiar con el tiempo.

Ejemplo

Una asesoría autoriza un asistente para redactar comunicaciones genéricas, pero prohíbe introducir documentación fiscal identificable en cuentas no evaluadas. La plantilla interna identifica qué tareas están permitidas y quién puede aprobar excepciones.

5. Verificación y supervisión humana

Una de las buenas prácticas más importantes es separar la generación de contenido de su aprobación. La IA puede proponer; la empresa debe decidir y verificar.

Protocolo de comprobación en cuatro pasos

1. Identificar qué afirmaciones del borrador son comprobables.
2. Contrastar cifras, normativa, fechas y enlaces con fuentes fiables y actuales.



- 3. Revisar el tono, la exactitud y la adecuación al destinatario.
- 4. Registrar la aprobación humana cuando el contenido tenga consecuencias relevantes.

Usos que exigen especial vigilancia

Uso	Control adicional
Información legal, fiscal o laboral	Revisión por profesional competente
Cálculos y presupuestos	Recalcular con herramienta fiable
Atención al cliente	Verificar condiciones y evitar promesas no autorizadas
Selección o evaluación de personas	Evaluación de impacto y normativa aplicable
Publicaciones públicas	Comprobar hechos, derechos de imagen y marca

No utilices una respuesta de IA como única base para tomar decisiones de alto impacto. Documenta el criterio de revisión y conserva los materiales necesarios para justificar la decisión.

6. Auditoría, imagen y transparencia

La generación de textos, imágenes, audios y vídeos plantea cuestiones sobre derechos de autor, uso de marcas, derechos de imagen y posibles confusiones para la audiencia.

Buenas prácticas de publicación

- No solicitar imitaciones que infrinjan derechos de terceros ni incorporar obras protegidas sin autorización.
- Comprobar las condiciones de uso comercial del proveedor y de los materiales de origen.
- No crear testimonios, reseñas o fotografías de clientes inexistentes para presentarlos como reales.
- Evitar suplantaciones de voz o imagen de personas sin base legítima y autorización cuando proceda.
- Indicar el uso de contenido sintético cuando sea necesario para evitar engaños o cuando la normativa aplicable lo exija.

Ejemplo en redes sociales

Una cafetería puede usar IA para preparar propuestas de textos y un calendario editorial. Si publica una



imagen generada, debe evitar presentarla como fotografía real de un plato que no existe o que no se sirve en el local.

Marco normativo

Además del RGPD y la normativa sobre propiedad intelectual, la regulación europea de IA establece obligaciones que dependen del sistema, del papel de la organización y del uso concreto. Conviene verificar los calendarios de aplicación y las orientaciones oficiales actualizadas antes de tomar decisiones de cumplimiento.

7. Ciberseguridad y amenazas específicas

La IA también introduce riesgos de seguridad propios. Uno de ellos es la inyección de instrucciones: un texto recibido de una web, correo o documento intenta manipular el comportamiento del asistente y hacer que ignore las instrucciones legítimas.

Situaciones que deben generar alerta

- Un documento externo pide al asistente revelar información privada o cambiar su función.
- Una automatización intenta enviar datos a una dirección desconocida.
- Una respuesta recomienda instalar programas o ejecutar comandos sin validación.
- Un mensaje aparenta proceder del proveedor y solicita claves o pagos urgentes.

Medidas preventivas

- Separar instrucciones confiables de contenidos aportados por terceros.
- Limitar permisos de conectores y revisar acciones antes de ejecutarlas.
- Mantener copias de seguridad, actualizaciones y protección de cuentas.
- Probar las automatizaciones con datos ficticios antes de operar con datos reales.
- Establecer autorización humana para envíos, borrados, compras o cambios irreversibles.

La IA no sustituye los controles de ciberseguridad tradicionales; debe integrarse en ellos.



8. Política interna de uso de IA para una pyme

Una política eficaz no tiene que ser extensa. Debe definir de forma clara quién puede utilizar IA, para qué tareas, con qué información y cómo se supervisa.

Contenido mínimo recomendado

Elemento	Decisión que debe documentarse
Responsable	Persona o función que autoriza herramientas
Herramientas	Listado de servicios permitidos
Datos	Información prohibida o condicionada
Usos	Tareas autorizadas y no autorizadas
Revisión	Quién valida resultados relevantes
Incidencias	Cómo comunicar errores o filtraciones
Formación	Instrucciones básicas para el equipo

Ejemplo de norma sencilla

“El personal podrá utilizar las herramientas de IA autorizadas para generar borradores y apoyar tareas no sensibles. No se introducirán datos personales, credenciales ni información confidencial sin evaluación y autorización. Toda comunicación externa deberá ser revisada por una persona responsable antes de su difusión”.

Esta redacción es una plantilla orientativa y debe adaptarse a la actividad y a los tratamientos de información de cada empresa.

9. Casos prácticos por sectores

Comercio minorista

Uso: preparar fichas de productos a partir de características públicas. Riesgo: inventar prestaciones o condiciones de garantía. Control: contraste con catálogo y aprobación de la persona responsable.

Hostelería y restauración

Uso: planificar publicaciones y traducir descripciones genéricas de platos. Riesgo: introducir información errónea sobre alérgenos. Control: validar toda información alimentaria con la documentación real del establecimiento.



Servicios profesionales

Uso: resumir documentación pública o redactar correos tipo. Riesgo: compartir expedientes identificables o confiar en citas normativas inventadas. Control: anonimización adecuada, entorno autorizado y revisión especializada.

Industria y talleres

Uso: crear listas de comprobación de mantenimiento no crítico. Riesgo: instrucciones técnicas inseguras. Control: validar con manuales del fabricante y personal cualificado; no delegar decisiones de seguridad.

Asociaciones y entidades locales

Uso: elaborar borradores de convocatorias, agendas y materiales informativos. Riesgo: publicar fechas o requisitos incorrectos. Control: cotejo con bases y documentos oficiales.

10. Recursos y conclusiones

Fuentes oficiales para profundizar

- Agencia Española de Protección de Datos (AEPD): <https://www.aepd.es/>
- Instituto Nacional de Ciberseguridad (INCIBE): <https://www.incibe.es/>
- Comisión Europea, enfoque europeo de IA: <https://digital-strategy.ec.europa.eu/>
- EUR-Lex, normativa europea: <https://eur-lex.europa.eu/>
- Agencia Española de Supervisión de Inteligencia Artificial (AESIA): <https://aesia.digital.gob.es/>

Consulta las versiones vigentes de guías, recomendaciones y normativa. Las obligaciones pueden variar según el tipo de sistema y la actividad de la organización.

Diez ideas para recordar

- No compartir información por inercia.
- Usar únicamente herramientas evaluadas.
- Configurar cuentas y permisos con cuidado.
- Comprobar antes de publicar o decidir.
- Mantener siempre supervisión humana.
- No confundir contenido generado con hechos verificados.
- Respetar datos personales, autoría e imagen.
- Proteger integraciones y automatizaciones.



- Formar al equipo y registrar incidencias.
- Revisar periódicamente normas y herramientas.

Edición: Septiembre 2026