



MANUAL OPERATIVO **SHADOW AI**

Política lista para adoptar, matrices de decisión, formularios de aprobación, controles técnicos, checklists de auditoría y plantillas de respuesta a incidentes.

APFerrer

INDICE

1	Qué es y por qué te debe importar
2	Dónde aparece: señales y vectores
3	Mapa de riesgos
4	Qué ha pasado ya: incidentes y multas
5	Qué te obliga la ley: UE y España
6	Consecuencias y sanciones
7	Clasificación de usos (verde / amarillo / naranja / rojo)
8	Política interna de uso aceptable (texto para adoptar)
9	Reglas por departamento
10	Procedimiento de aprobación y formulario
11	Controles técnicos por capas
12	Gobierno y roles
13	Plan de implantación
14	Checklist de auditoría
15	Respuesta ante incidentes y plantilla
16	Pautas para empleados (cartel y reglas)
17	Glosario

1.

Qué es y por qué te debe importar

El **Shadow AI** es el uso de herramientas, modelos, agentes, extensiones o servicios de inteligencia artificial sin que la empresa lo apruebe, lo conozca o lo pueda rastrear. Ocurre cuando alguien pega un contrato en una IA pública, conecta una extensión a Gmail o Drive, sube datos de clientes a una herramienta SaaS o usa un copiloto de código no autorizado.

No depende de si la herramienta es buena o mala. Una herramienta excelente es Shadow AI si se usa con cuenta personal, sin contrato, sin control de datos y sin saber qué información se introduce en ella. El criterio es uno solo: **si la empresa no lo conoce y no lo gobierna, es Shadow AI.**

La cifra que ordena la conversación

El 81 % de los empleados y el 88 % de los responsables de seguridad usan herramientas de IA no aprobadas. El Shadow AI aparece en el 20 % de las brechas de datos y añade de media 670.000 \$ al coste de cada una. El 97 % de las organizaciones que sufrieron un incidente con IA no tenía controles de acceso adecuados. No es un riesgo de minorías: es el estado por defecto.

El principio de gestión

No se controla prohibiendo todo. Si todo necesita permiso, nadie pide permiso, y el uso se va al móvil personal, donde ya no lo ves. Se controla dando una alternativa aprobada, útil y rápida, con reglas claras por tipo de dato, revisión de proveedores, control técnico y formación breve. Prohibir sin alternativa no reduce la exposición: reduce tu visibilidad sobre ella.

2.

Dónde aparece: señales y vectores

SEÑAL	QUÉ INDICA	QUÉ HACER
Cuentas personales	La empresa no controla el acceso ni la baja del usuario.	Migrar a cuenta corporativa o bloquear el uso con datos internos.
OAuth sin revisar	La herramienta puede leer Drive, Gmail, CRM o Slack.	Revisar permisos, revocar lo que sobre y aprobar por IT.
Datos pegados en chats públicos	Exposición de datos personales, confidenciales o contractuales.	DLP, formación y alternativa aprobada.
Extensiones de navegador	Pueden leer páginas, formularios y contenido sensible.	Inventario, lista blanca y bloqueo por defecto.
Automatizaciones con agentes	Capacidad de actuar sin supervisión.	Permisos mínimos, logs y confirmación humana.
IA embebida en SaaS	Funciones activadas por defecto por el proveedor.	Inventario periódico de funciones y cambios.

La diferencia con el Shadow IT de siempre

El Shadow IT clásico almacenaba datos fuera. El Shadow AI los procesa: lee, transforma, infiere, genera, clasifica y puede ejecutar acciones. Por eso el control no basta con cubrir la aplicación: tiene que cubrir el proveedor, el dato de entrada, el prompt, el modelo, los conectores, la salida y la revisión humana.

3.

Mapa de riesgos

El riesgo no lo marca la herramienta sola. Lo marcan el dato que se introduce, la finalidad, la conexión con sistemas internos, la capacidad de actuar, el proveedor, dónde se trata el dato y si hay revisión humana.

RIESGO	EJEMPLO CONCRETO	CONTROL MÍNIMO
Privacidad	Subir un Excel de clientes a una IA pública.	Base jurídica, contrato de encargado, minimización y registro.
Confidencialidad	Pegar una propuesta, un presupuesto o un contrato.	Clasificación de datos y DLP.
Ciberseguridad	Extensión con acceso completo a correo y Drive.	Control de identidad, revisión OAuth, mínimo privilegio y logs.
Propiedad intelectual	Generar código o textos sin verificar origen ni licencia.	Revisión de derechos y trazabilidad de la salida.
Calidad	Resumen legal o financiero con errores o invenciones.	Revisión humana y verificación de fuentes.
Cumplimiento	IA que evalúa candidatos sin evaluación previa.	Evaluación de riesgo y revisión legal.

4.

Qué ha pasado ya: incidentes y multas

Samsung (abril de 2023)

En menos de veinte días desde que permitió ChatGPT a sus ingenieros, Samsung tuvo tres fugas: un empleado pegó código fuente propietario para depurarlo, otro subió código de detección de defectos para optimizarlo y un tercero metió la grabación de una reunión interna para que le redactaran el acta. Samsung limitó los prompts a 1.024 bytes y después prohibió la IA generativa en equipos corporativos. Lo que entra en el modelo no se recupera.

La banca y las tecnológicas cerraron el grifo (2023)

JPMorgan, Bank of America, Citigroup, Goldman Sachs, Deutsche Bank, Wells Fargo, Apple y Verizon restringieron o prohibieron ChatGPT. Varias no sabían, antes de bloquearlo, cuántos empleados lo usaban ni para qué: ese es el punto ciego que define el Shadow AI.

Transcriptores de reuniones (Otter.ai, 2024-2025)

Un inversor recibió de Otter.ai la transcripción de una reunión que incluía la conversación privada posterior a su desconexión. En 2025 se acumularon demandas colectivas en California por grabar sin consentimiento de todos los participantes y por capturar la huella de voz biométrica. En la UE el consentimiento debe darlo cada interviniente, no solo quien organiza la llamada.

Extensiones de navegador maliciosas (2024-2025)

En diciembre de 2024, una extensión legítima con más de 400.000 usuarios fue comprometida y reemplazada por una versión que robaba sesiones; la campaña afectó a unos 2,6 millones de usuarios en 35 extensiones. En diciembre de 2025 se detectaron dos extensiones con más de 900.000 usuarios que exfiltraban conversaciones de ChatGPT y DeepSeek cada media hora. El canal de extensiones es una puerta trasera que casi nadie vigila.

4.

Qué ha pasado ya: incidentes y multas

La primera gran multa, y su matiz

En diciembre de 2024 la autoridad italiana multó a OpenAI con 15 millones de euros por tratar datos para entrenar ChatGPT sin base jurídica adecuada, por fallos de transparencia, por no verificar la edad y por no notificar a tiempo una brecha. En marzo de 2026 un tribunal de Roma anuló la multa, pero por un motivo de competencia (el caso debía llevarlo la autoridad irlandesa), no porque ChatGPT cumpliera el RGPD. El fondo del asunto sigue abierto.

5.

Qué te obliga la ley: UE y España

El Reglamento de IA de la UE: cuándo aplica cada cosa

FECHA	QUÉ ENTRA EN VIGOR
2 feb 2025	Prácticas prohibidas (art. 5) y obligación de formar a la plantilla en IA (art. 4).
2 ago 2025	Modelos de propósito general, gobernanza y régimen de sanciones.
2 ago 2026	Obligaciones de transparencia (art. 50) y sistemas de alto riesgo del Anexo III.
2 ago 2027	Alto riesgo integrado en productos ya regulados.

Aviso: en 2026 se tramita el llamado paquete de simplificación que podría retrasar parte del alto riesgo a diciembre de 2027. No retrasa las prohibiciones, ni las sanciones, ni la transparencia, ni la formación. Hasta que se publique oficialmente, las fechas de arriba son las que obligan.

Las cuatro categorías de riesgo

Riesgo inaceptable (prohibido). Alto riesgo (Anexo III: biometría, infraestructuras críticas, educación, empleo y recursos humanos, servicios esenciales como banca o seguros, aplicación de la ley, migración y justicia), con obligaciones de gestión de riesgos, gobernanza de datos, documentación, registros, supervisión humana, exactitud y ciberseguridad. Riesgo limitado (obligación de transparencia: avisar de que hay una IA detrás y etiquetar deepfakes). Riesgo mínimo (sin obligaciones específicas).

España: AESIA y la ley de gobernanza

España fue el primer país de la UE con una agencia dedicada a vigilar la IA: la AESIA, con sede en A Coruña. Empezó a inspeccionar prácticas prohibidas en febrero de 2025 y asumió potestad sancionadora en agosto de 2025. La ley nacional reparte competencias: AESIA en general, la Agencia de Protección de Datos en biometría y fronteras, y el Banco de España, la CNMV, el Consejo General del Poder Judicial y la Junta Electoral Central en sus ámbitos. No etiquetar un contenido generado con IA, incluidos los deepfakes, es infracción grave.

6.

Consecuencias y sanciones

Sanciones del Reglamento de IA (la mayor de las dos cifras)

INFRACCIÓN	MULTA MÁXIMA
Usar una práctica prohibida (art. 5)	35 millones € o el 7 % de la facturación mundial.
Incumplir obligaciones de alto riesgo u otras	15 millones € o el 3 %.
Dar información incorrecta a la autoridad	7,5 millones € o el 1,5 %.

Sanciones de la ley española (tramos)

GRAVEDAD	IMPORTE	EJEMPLO
Muy grave	7.500.001 a 35.000.000 € (o 2-7 %)	Usar IA prohibida; no comunicar un incidente grave.
Grave	500.001 a 7.500.000 € (o 1-2 %)	No etiquetar un deepfake; falta de supervisión humana en biometría laboral.
Leve	Desde 6.000 €	No incorporar el marcado CE en un sistema de alto riesgo.

Las pymes y empresas emergentes se acogen a la cuantía menor, y en infracciones leves puede bastar el apercibimiento si se corrige a tiempo. Pero ojo: la multa no es el único coste. Hay que sumar la fuga irreversible de datos o secretos, la pérdida de confianza de clientes, la posible obligación de notificar una brecha en 72 horas y, en propiedad intelectual, el riesgo de usar salidas de IA sin verificar su origen.

6.

Consecuencias y sanciones

Y el RGPD, en paralelo

Pegar datos personales en una IA con cuenta personal infringe el RGPD por tres vías a la vez: no hay base jurídica para esa cesión, no hay contrato de encargado con el proveedor, y hay una transferencia internacional de datos sin garantías. La empresa sigue siendo responsable aunque el empleado lo haya hecho por su cuenta. Las multas del RGPD llegan al 4 % de la facturación mundial, y se acumulan a las anteriores.

7.

Clasificación de usos

Una política útil separa lo permitido, lo condicionado y lo prohibido. Esta es la regla general; ajústala por sector.

NIVEL	USO	CONDICIÓN
VERDE: libre	Redactar texto general, resumir contenido público, generar ideas sin datos internos.	No incluir datos personales, secretos, contratos, clientes ni documentos internos.
AMARILLO: con herramienta aprobada	Resumir documentos internos, preparar informes, traducir documentación corporativa.	Cuenta corporativa, proveedor revisado, logs y reglas de conservación.
NARANJA: requiere evaluación	IA conectada a CRM, correo, Drive, ERP, RRHH o sistemas de clientes.	Revisión previa de IT, seguridad, legal y protección de datos.
ROJO: prohibido salvo autorización	Pegar credenciales, secretos, datos de salud, datos de menores, expedientes sensibles, código con secretos.	No permitido en herramientas no aprobadas. Puede requerir evaluación de impacto.

8.

Política interna de uso aceptable

Este es el texto para adoptar como política interna. Revísalo con tu mapa de tratamientos, tus contratos y tu infraestructura, y publícalo.

TEXTO BASE DE LA POLÍTICA

La organización permite el uso de herramientas de inteligencia artificial cuando ese uso esté alineado con la finalidad profesional, no comprometa información confidencial, no implique tratamiento no autorizado de datos personales, no eluda controles de seguridad y no sustituya la validación humana en decisiones con impacto relevante.

Reglas mínimas

1. No introducir datos personales, datos de clientes, contratos reales, expedientes, credenciales, secretos, código propietario ni documentación interna en herramientas de IA no aprobadas.
2. Usar solo cuentas corporativas cuando la herramienta se emplee para trabajo de la empresa.
3. No conectar herramientas de IA a correo, repositorios, Drive, CRM, ERP, Slack o Teams sin aprobación de IT.
4. No usar IA para decidir automáticamente sobre personas sin revisión legal, de privacidad y de impacto.
5. Validar toda salida de IA antes de usarla en documentos, código, informes, comunicaciones externas o decisiones.
6. Avisar a IT o seguridad al detectar una herramienta de IA no inventariada o un posible envío de información sensible.
7. Conservar evidencia de uso cuando el resultado afecte a clientes, empleados, decisiones contractuales, soporte, seguridad o cumplimiento.

8.

Política interna de uso aceptable

Permitido por defecto

- *Lluvia de ideas sin datos reales de la empresa.*
- *Mejorar la redacción de textos no confidenciales.*
- *Resumir información pública y traducir textos genéricos.*
- *Crear plantillas, estructuras y ejemplos ficticios.*

No permitido en herramientas no aprobadas

- *Subir bases de datos, hojas con clientes, nóminas, CV o incidencias.*
- *Contratos reales, expedientes, propuestas económicas o planes estratégicos.*
- *Código propietario, claves API, tokens, logs con identificadores o volcados de base de datos.*
- *Automatizaciones que envíen correos, cambien registros o aprueben operaciones sin supervisión.*
- *Evaluar personas, seleccionar candidatos o puntuar clientes sin evaluación previa.*

9.

Reglas por departamento

ÁREA	USO HABITUAL	DECISIÓN
Marketing	Generar campañas con datos de clientes reales.	Solo con herramienta aprobada y datos minimizados.
Ventas	Resumir llamadas, propuestas y CRM.	Proveedor aprobado y control de acceso.
RRHH	Filtrar CV, evaluar entrevistas, redactar informes.	Revisión legal previa y evaluación específica de impacto.
Legal	Resumir contratos o expedientes.	Solo entorno aprobado, sin entrenamiento, con contrato y logs.
Finanzas	Analizar balances, deuda, nóminas o previsiones.	Uso supervisado y datos agregados cuando sea posible.
IT y desarrollo	Copilotos de código, análisis de logs, scripts.	Herramienta aprobada, escaneo de secretos y revisión de licencias.
Atención al cliente	Responder tickets con IA.	Base de conocimiento aprobada y revisión humana.
Dirección	Preparar estrategia con documentación interna.	Herramienta corporativa y documentos clasificados.

10.

Procedimiento de aprobación y formulario

Breve para usos sencillos, exigente para herramientas conectadas a datos internos. Se revisa la herramienta y el caso de uso, no solo el nombre del proveedor.

PASO	RESPONSABLE	EVIDENCIA MÍNIMA
1. Solicitud	Área usuaria	Herramienta, proveedor, finalidad, usuarios, datos, frecuencia.
2. Clasificación de datos	Área + protección de datos	Tipo de dato: público, interno, confidencial, personal, sensible, secreto.
3. Revisión técnica	IT y seguridad	Autenticación, permisos, conectores, logs, cifrado y residencia de datos.
4. Revisión legal	Legal y protección de datos	Contrato, encargado, subencargados, transferencias y conservación.
5. Evaluación de IA	Gobierno de IA	Finalidad, riesgo, revisión humana, exactitud, sesgos y trazabilidad.
6. Decisión	Comité o responsable	Aprobada, con condiciones, piloto, rechazada o pendiente.
7. Registro	IT / Gobierno de IA	Inventario actualizado, propietario, usuarios y fecha de revisión.

10.

Procedimiento de aprobación y formulario

Formulario de solicitud

CAMPO	RESPUESTA
Herramienta y URL	
Proveedor y país de la entidad contratante	
Departamento y responsable	
Finalidad concreta	
Datos que se introducen	
Datos que genera	
Conexiones solicitadas (Drive, CRM, correo...)	
¿Entrena con tus datos?	
¿Conserva prompts o ficheros? ¿Se puede desactivar?	
¿Hay contrato, encargo de tratamiento o plan enterprise?	
Decisión y fecha de revisión	

11.

Controles técnicos por capas

Los controles técnicos no sustituyen la política, pero evitan que todo dependa de la memoria del empleado. Se implantan por capas y cada una deja evidencia.

CAPA	CONTROL	PARA QUÉ
Identidad	Inicio de sesión único, doble factor, altas y bajas automáticas.	Que solo acceda a la IA aprobada quien debe.
Permisos	Mínimo privilegio y revisión de consentimientos OAuth.	Evitar conectores con acceso excesivo.
Datos	Prevención de fuga de datos (DLP) en correo, navegador y SaaS.	Detectar o bloquear el envío de datos sensibles.
Red	Control de aplicaciones cloud y del tráfico hacia servicios de IA.	Ver qué IA se usa y cuánto.
Dispositivo	Control de extensiones y lista blanca de navegador.	Frenar plugins y software no autorizado.
Aplicación	Logs de prompts, salidas, ficheros y acciones.	Trazabilidad y auditoría.
Secretos	Escaneo de claves y tokens en repositorios y prompts.	Evitar exponer credenciales.
Proveedor	Contrato de encargado, subprocesadores, residencia y retención.	Controlar las condiciones del tratamiento.

11.

Controles técnicos por capas

Agentes y conectores

- Permisos mínimos por tarea, no acceso completo por comodidad.
- Separar lectura, escritura, envío, borrado y aprobación.
- Confirmación humana antes de enviar correos, modificar el CRM o aprobar pagos.
- Registrar cada acción: quién, cuándo, qué dato, qué instrucción y qué resultado.
- Probar en entorno aislado antes de conectar a producción, y caducar los permisos.

Sobre bloquear sin más

Bloquear todas las herramientas de IA reduce la exposición inmediata, pero empuja el uso a móviles personales y redes externas. Lo estable es combinar herramienta aprobada, bloqueo selectivo, monitorización, formación y aprobación rápida.

12.

Gobierno y roles

ROL	RESPONSABILIDAD
Dirección	Aprobar el apetito de riesgo, el presupuesto y las consecuencias del incumplimiento.
IT	Inventario, identidad, permisos, integraciones y ciclo de vida de las herramientas.
Seguridad	DLP, control de red, alertas, incidentes y análisis de exposición.
Protección de datos	Mapa de tratamientos, evaluaciones de impacto, contratos y transferencias.
Legal	Condiciones de proveedor, propiedad intelectual, confidencialidad y responsabilidad.
Responsables de área	Justificar usos, validar salidas, formar al equipo y detectar necesidades.
Personas usuarias	Cumplir las reglas, no subir datos no permitidos, revisar resultados y reportar.
Compras	Verificar expediente y condiciones antes de pagar; evitar contrataciones dispersas.

En una pyme no hace falta una estructura pesada: basta un grupo con IT o responsable técnico, legal o asesoría, protección de datos cuando exista y un responsable de negocio. Regla clara: los usos verdes se documentan, los amarillos se aprueban por vía rápida, los naranjas y rojos pasan por revisión formal.

13.

Plan de implantación

FASE	PLAZO	ACCIONES
0. Decisión	Semana 1	Nombrar responsables, fijar el criterio de riesgo y comunicar que no se busca castigar el uso pasado.
1. Descubrimiento	Semanas 1-3	Inventariar herramientas de IA, extensiones, tráfico, cuentas, pagos y conexiones OAuth.
2. Política	Semanas 2-4	Publicar la política, la matriz de usos y un canal de consulta.
3. Alternativa aprobada	Semanas 3-6	Activar la herramienta corporativa con identidad única, logs, retención y reglas de datos.
4. Controles	Semanas 4-8	DLP, revisión OAuth, bloqueo selectivo, control de extensiones y alertas.
5. Formación	Semanas 4-10	Sesiones por rol, ejemplos reales, checklist de uso y preguntas frecuentes.
6. Auditoría	Mensual / trimestral	Revisar uso, incidentes, proveedores, permisos y cambios de normativa.

14.

Checklist de auditoría

La auditoría debe probar dos cosas: que la empresa sabe qué IA se usa y que tiene criterios para permitir, limitar o bloquear cada uso. Marca cada punto y guarda la evidencia.

- ☐ Existe inventario de herramientas de IA aprobadas.
- ☐ Existe inventario de herramientas de IA detectadas y no aprobadas.
- ☐ Las herramientas aprobadas usan cuenta corporativa e inicio de sesión único.
- ☐ Se revisan los permisos OAuth y los conectores.
- ☐ Hay política sobre qué datos pueden y no pueden introducirse.
- ☐ Hay contrato de encargado de tratamiento cuando aplica.
- ☐ Se revisan las transferencias internacionales y los subencargados.
- ☐ Existe procedimiento para aprobar nuevos casos de uso.
- ☐ Hay DLP o control equivalente para datos sensibles.
- ☐ Se controlan las extensiones de navegador.
- ☐ Hay logs suficientes para los usos con impacto relevante.
- ☐ El personal ha recibido pautas de uso y formación.
- ☐ Existe canal para reportar uso no aprobado o incidentes.
- ☐ Se ha probado el plan de respuesta ante incidentes.
- ☐ Se revisan herramientas y permisos de forma periódica.

15.

Respuesta ante incidentes

Un incidente puede ser una subida accidental de información sensible, una conexión no autorizada a un repositorio, una extensión con permisos excesivos, una salida errónea enviada a un cliente o una automatización que actúa sin permiso.

PASO	QUÉ HACER
1. Contener	Suspender el uso, cerrar sesión, revocar OAuth, bloquear la herramienta y detener la automatización.
2. Identificar datos	Determinar qué se introdujo o conectó: datos personales, secretos, código, clientes afectados, volumen y fechas.
3. Revisar proveedor	Ver retención y borrado, pedir eliminación si es posible, revisar logs y subencargados.
4. Valorar impacto	Confidencialidad, integridad, disponibilidad, derechos de personas y obligaciones contractuales.
5. Notificar	Activar avisos internos: protección de datos, seguridad, dirección, y cliente o autoridad si corresponde (72 h).
6. Corregir	Eliminar la causa raíz: DLP, bloqueo, formación, alternativa aprobada o cambio de permisos.
7. Documentar	Guardar cronología, evidencias, decisiones, comunicaciones y medidas.

15.

Respuesta ante incidentes

Plantilla de registro del incidente

CAMPO	CONTENIDO
Fecha y hora de detección	
Quién o qué lo detecta	
Herramienta de IA implicada	
Cuenta utilizada (personal / corporativa)	
Datos introducidos o conectados	
Clientes, empleados o terceros afectados	
Proveedor y condiciones de retención	
Medidas de contención	
Evaluación de impacto	
Notificaciones realizadas	
Medidas correctivas	
Cierre y fecha de revisión	

16.

Pautas para empleados

REGLA DE BOLSILLO

Si no lo enviarías por correo a un proveedor externo desconocido, no lo pegues en una IA no aprobada.

Antes de usar una IA, comprueba

- ¿Uso cuenta corporativa o personal?
- ¿La herramienta está aprobada por la empresa?
- ¿El texto o fichero contiene datos personales o información interna?
- ¿Estoy conectando la herramienta a una cuenta o sistema corporativo?
- ¿El resultado se usará para una decisión, un cliente o publicación?
- ¿Puedo verificar la salida con fuentes o revisión humana?

Qué no hacer, y por qué

NO HAGAS	POR QUÉ
Pegar datos de clientes para que la IA los ordene.	Puede ser tratamiento no autorizado y fuga de datos.
Instalar extensiones de IA sin revisar permisos.	Pueden leer páginas, formularios, documentos y correos.
Dar acceso completo a Drive a un agente.	El permiso excede la finalidad y expone documentos no relacionados.
Usar IA para decidir sobre una persona.	Exige transparencia, evaluación de impacto y revisión humana.
Copiar resultados sin revisión.	La salida puede tener errores, invenciones o sesgos.

16.

Pautas para empleados

Cartel para imprimir

CARTEL INTERNO

ANTES DE PEGAR ALGO EN UNA IA

Pausa. Limpia. Revisa.



No pegues información sensible en herramientas no aprobadas.
La comodidad no compensa una fuga de datos, un incumplimiento o una exposición innecesaria.

- 1** | Quita datos personales y de cliente.
- 2** | No pegues contratos reales, secretos, credenciales ni código propietario.
- 3** | No conectes apps a Drive, Gmail, CRM o repositorios sin aprobación.
- 4** | Usa la herramienta corporativa cuando exista.
- 5** | Revisa siempre la respuesta antes de usarla.

SI TIENES DUDAS, NO LO PEGUES.
Pregunta antes o usa el canal interno aprobado.

Uso interno | Protección de datos, confidencialidad y seguridad de la información

17.

Glosario

TÉRMINO	QUÉ SIGNIFICA
Shadow AI	Uso de IA no aprobado, no inventariado o no supervisado por la empresa.
Shadow IT	Uso de tecnología no aprobada por IT.
LLM	Modelo de lenguaje que genera, resume, transforma o clasifica texto.
Prompt	La instrucción o contenido que se entrega a la IA. Puede contener datos sensibles.
Salida (output)	El resultado que genera la IA. Debe revisarse antes de usarse.
DLP	Tecnología o proceso para prevenir la fuga de datos.
OAuth	Mecanismo para dar a una app permisos sobre tus cuentas o servicios.
Agente	IA que puede planificar o ejecutar acciones con herramientas externas.
Revisión humana	Comprobación por una persona antes de usar o ejecutar la salida de la IA.
Evaluación de impacto	Análisis previo cuando un tratamiento puede suponer alto riesgo para las personas.



Si tienes dudas o quieres asesoramiento
personalizado para tu empresa, no dudes en
escribirme:
info@apferrer.com