

Documento de Gobierno y Uso de la IA

Logística Levante S.L. (empresa ficticia de ejemplo)

Versión	v0.1
Estado	Borrador pendiente de aprobación
Generado	13/10/2026 22:17 por Marta (ejemplo) · Legal / Compliance
Expediente	AUD-EJEMPLO-USO-1NLU · instantánea SNP-A3C74AC4
Motor y corte normativo	RULESET-LALEYIA-2026.10 · 06/10/2026
Secciones pendientes de validar	3 de 28

Índice

- Objeto
- Alcance
- Principios
- Definiciones
- Estructura de gobierno y responsabilidades
- Inventario de sistemas de IA
- Herramientas autorizadas y uso aceptable
- Uso no autorizado (Shadow AI) · pendiente de validar
- Alta y aprobación de nuevas herramientas
- Clasificación de riesgos
- Proveedores y contratos · pendiente de validar
- Protección de datos · pendiente de validar
- Seguridad
- Supervisión humana
- Transparencia
- Agentes y automatizaciones
- Personas trabajadoras
- Casos de uso de posible alto riesgo
- Formación y alfabetización en IA
- Incidentes
- Registros y evidencias
- Gestión de cambios
- Revisión y auditoría
- Excepciones
- Retirada de sistemas
- Incumplimiento
- Aprobación y control de versiones
- Anexo A. Puntos pendientes del expediente

1. Objeto

Este documento establece cómo Logística Levante S.L. (empresa ficticia de ejemplo) gobierna el uso de los sistemas de inteligencia artificial (IA): quién decide, qué herramientas y usos están permitidos, qué información no puede introducirse en ellas, cómo se supervisan sus resultados y cómo se demuestra todo ello.

Se ha redactado con las respuestas que la empresa ha dado en el cuestionario del expediente AUD-EJEMPLO-USO-1NLU de La Ley IA (motor RULESET-LALEYIA-2026.10, marco normativo comprobado hasta 06/10/2026, instantánea SNP-A3C74AC4). Cuando falta una respuesta o un dato, el apartado se marca como «[Sección pendiente de validar por la empresa]» e indica qué falta: el documento no completa por su cuenta información que la empresa no ha facilitado.

Junto a cada regla se indica si responde a una obligación normativa o a una buena práctica de gobernanza adoptada por la empresa.

2. Alcance

Se aplica a todas las personas que trabajan para Logística Levante S.L. (empresa ficticia de ejemplo) o en su nombre, incluidas las personas colaboradoras externas con acceso a sus sistemas, y a todos los sistemas de IA que la empresa usa o contrata.

Departamentos incluidos: IA global de la empresa, Atención al cliente, Marketing y comunicación. A la fecha de este documento hay 3 sistemas inventariados (4 casos de uso analizados).

3. Principios

- Solo se usan herramientas autorizadas y para los usos aprobados (apartado «Herramientas autorizadas y uso aceptable»).
- La información de la lista de información protegida no se introduce en herramientas no autorizadas ni en cuentas personales.
- La supervisión humana es proporcional al riesgo de cada caso de uso (apartado «Supervisión humana»).
- Las personas afectadas reciben la información que exige la ley (apartados «Protección de datos» y «Transparencia»).
- Cada decisión relevante sobre IA queda registrada y se puede demostrar (apartado «Registros y evidencias»).

4. Definiciones

- Sistema de IA: sistema basado en máquinas que, a partir de la información que recibe, genera resultados como contenidos, predicciones, recomendaciones o decisiones (art. 3.1 AI Act).
- Caso de uso: uso concreto de una herramienta para una finalidad. Una misma herramienta puede tener varios casos de uso con riesgos distintos.
- Responsable del despliegue: quien usa un sistema de IA bajo su autoridad en su actividad profesional. Es el papel de Logística Levante S.L. (empresa ficticia de ejemplo) respecto a la IA de terceros que utiliza.
- Proveedor: quien desarrolla un sistema de IA y lo comercializa o pone en servicio con su nombre o marca.
- Uso no autorizado (Shadow AI): uso de herramientas de IA no aprobadas o de cuentas personales para trabajar.
- Incidente de IA: resultado erróneo, fuga de información, decisión incorrecta o comportamiento inesperado de un sistema de IA con efectos relevantes.

5. Estructura de gobierno y responsabilidades

Según el cuestionario, hasta ahora nadie tenía asignada la responsabilidad sobre la IA; este documento la asigna.

Responsable de IA: Albert rod. Mantiene el inventario, aprueba o rechaza herramientas y usos nuevos, coordina la evaluación de riesgos y de proveedores, custodia las evidencias, gestiona los incidentes y propone la revisión de este documento (buena práctica de gobernanza).

Comité de IA: Dirección, IT, Seguridad de la información, Privacidad (DPO), Legal y RR. HH. Se reúne de forma periódica y siempre que se proponga un caso de uso de posible alto riesgo o se produzca un incidente relevante.

Propietarios de las herramientas

Herramienta	Propietario	Departamento
AI-SYS-001 · Microsoft 365 Copilot	Director de IT	IA global de la empresa
AI-SYS-002 · Asistente de atención al cliente	Responsable de Customer Service	Atención al cliente
AI-SYS-003 · ChatGPT	Responsable de marketing	Marketing y comunicación

Matriz de responsabilidades (RACI)

Actividad	Responsable de IA	Propietario de la herramienta	IT y Seguridad	Privacidad (DPO)	Legal	RR. HH.	Dirección
Alta de una herramienta nueva	A/R	R	C	C	C	—	I
Mantener el inventario	A/R	R	C	I	—	—	I
Evaluar proveedores y contratos	A	C	C	C	R	—	I
Protección de datos (registro, EIPD, información)	C	C	C	A/R	C	C	I
Supervisión de resultados	I	A/R	—	C	—	C	—
Formación del personal	A	C	C	C	C	R	I
Gestión de incidentes de IA	A/R	R	R	C	C	—	I
Revisión de este documento	R	C	C	C	C	C	A

R: realiza · A: rinde cuentas · C: consultado · I: informado.

6. Inventario de sistemas de IA

Según el cuestionario, el registro de sistemas de IA estaba incompleto; el inventario siguiente lo sustituye.

ID	Herramienta	Proveedor	Departamento	Estado	Casos de uso y clasificación
AI-SYS-001	Microsoft 365 Copilot	Microsoft	IA global de la empresa	Producción	USE-001 Resumir correos y redactar documentos internos (riesgo mínimo); USE-002 Preselección de currículums para puestos de almacén (potencial alto riesgo)
AI-SYS-002	Asistente de atención al cliente	Proveedor de chatbot (ejemplo)	Atención al cliente	Producción	USE-003 Responder consultas de seguimiento de envíos (obligaciones de transparencia)
AI-SYS-003	ChatGPT	OpenAI	Marketing y comunicación	Piloto	USE-004 Textos e imágenes para redes sociales (riesgo mínimo)

El Responsable de IA actualiza el inventario con cada alta, cambio o retirada y lo revisa al menos cada tres meses. El expediente AUD-EJEMPLO-USO-1NLU de La Ley IA es su versión de referencia (buena práctica de gobernanza; es la base para acreditar las obligaciones aplicables).

7. Herramientas autorizadas y uso aceptable

Según el cuestionario, ya existían normas internas escritas sobre el uso de la IA; este apartado las sustituye o integra.

Herramientas autorizadas

Según el cuestionario, no existía una lista de herramientas autorizadas; la tabla siguiente es la primera.

Herramienta	Usos permitidos	Cuentas
AI-SYS-001 · Microsoft 365 Copilot	Resumir correos y redactar documentos internos; Preselección de currículums para puestos de almacén	Corporativas
AI-SYS-002 · Asistente de atención al cliente	Responder consultas de seguimiento de envíos	Corporativas
AI-SYS-003 · ChatGPT	Textos e imágenes para redes sociales	Corporativas y personales (acción: eliminar el uso de cuentas personales)

Reglas de uso

- Para trabajar solo se usan cuentas corporativas de las herramientas autorizadas.
- Los resultados de la IA se revisan siempre antes de usarlos: pueden contener errores o datos inventados.
- La IA no se usa para decidir sobre personas fuera de los casos de uso aprobados.
- Ninguna herramienta se conecta a correo, documentos, CRM, ERP u otros sistemas sin aprobación del Responsable de IA y de IT.

Información protegida

Nunca se introduce en herramientas no autorizadas ni en cuentas personales:

- Datos personales de clientes
- Datos personales de la plantilla o de candidatos
- Datos de salud y otras categorías especiales
- Información confidencial y secretos empresariales
- Contraseñas, claves y credenciales

8. Uso no autorizado (Shadow AI)

[Sección pendiente de validar por la empresa] Falta: responder en el cuestionario «¿Hay medidas que impidan introducir información de la empresa en...» (consta «No lo sé»).

Está prohibido usar herramientas de IA que no figuren en la lista de autorizadas para tratar información de la empresa. Quien necesite una herramienta nueva la solicita por el procedimiento de alta (buena práctica; conecta con la seguridad del art. 32 RGPD y la protección de secretos empresariales).

Pendiente: responder en el cuestionario «¿Hay medidas que impidan introducir información de la empresa en...» (consta «No lo sé»)

IT publica la lista de herramientas autorizadas y aplica medidas técnicas para restringir las no aprobadas.

9. Alta y aprobación de nuevas herramientas

Según el cuestionario, no existía un procedimiento para aprobar una herramienta nueva antes de usarla; este apartado lo establece.

Según el cuestionario, el contrato y las condiciones de las herramientas nuevas se revisan solo en algunos casos.

- Solicitud por escrito al Responsable de IA, indicando la finalidad, las personas afectadas, los datos que se usarán y lo que podrá hacer la herramienta.
- Revisión del proveedor y del contrato: contrato y condiciones, contrato de encargo de tratamiento (DPA), uso de los datos para entrenamiento, subencargados, ubicación de los datos, conservación, compromisos de servicio, aviso de incidentes, auditoría y salida.
- Clasificación del caso de uso con La Ley IA y, si trata datos personales con indicadores de alto riesgo, evaluación de impacto en protección de datos.
- Aprobación documentada por el Responsable de IA o por el comité si el caso es de posible alto riesgo o trata categorías especiales de datos.
- Alta en el inventario, asignación de propietario y formación de las personas usuarias antes del primer uso.

Buena práctica de gobernanza y de compras: el control empieza antes de contratar.

10. Clasificación de riesgos

Cada caso de uso se clasifica según el AI Act por su finalidad y su contexto, no por la tecnología: práctica prohibida, posible alto riesgo, obligaciones de transparencia o riesgo mínimo. Además se estima el riesgo inherente y el residual tras los controles.

Caso de uso	Herramienta	Clasificación	Riesgo inherente	Riesgo residual
USE-001 · Resumir correos y redactar documentos internos	Microsoft 365 Copilot	Riesgo mínimo	Bajo	Bajo
USE-002 · Preselección de currículums para puestos de almacén	Microsoft 365 Copilot	Potencial alto riesgo	Muy alto	Muy alto
USE-003 · Responder consultas de seguimiento de envíos	Asistente de atención al cliente	Obligaciones de transparencia	Medio	Medio
USE-004 · Textos e imágenes para redes sociales	ChatGPT	Riesgo mínimo	Bajo	Bajo

11. Proveedores y contratos

[Sección pendiente de validar por la empresa] Falta: comprobar si el proveedor entrena con vuestros datos (AI-SYS-002); preguntar al proveedor dónde trata los datos (AI-SYS-002).

Antes de contratar y en cada renovación se revisa el contrato con la lista del procedimiento de alta. No se da por cumplido un requisito por el tamaño o la reputación del proveedor.

Herramienta	Contrato	DPA	¿Entrena con nuestros datos?	Ubicación de los datos
AI-SYS-001 · Microsoft 365 Copilot	Sí	Sí	No (contrato)	Dentro de la UE / EEE
AI-SYS-002 · Asistente de atención al cliente	Sí	No	Pendiente: comprobar si el proveedor entrena con vuestros datos (AI-SYS-002)	Pendiente: preguntar al proveedor dónde trata los datos (AI-SYS-002)
AI-SYS-003 · ChatGPT	Sí	No trata datos personales	No (desactivado)	Fuera del EEE (o con subencargados fuera)

12. Protección de datos

[Sección pendiente de validar por la empresa] Falta: completar en el cuestionario «Transferencias internacionales de datos»; completar en el cuestionario «Evaluación de impacto en protección de datos (EIPD)» (Preselección de currículums para puestos de almacén · Microsoft 365 Copilot).

Cuando una herramienta de IA trata datos personales, el DPO o la persona responsable de privacidad comprueba antes de su uso los siguientes requisitos (obligaciones normativas). Estado a la fecha de este documento:

Requisito	Estado
Registro de actividades de tratamiento (art. 30 RGPD)	no cumple
Contrato de encargo con cada proveedor que trata datos (art. 28 RGPD)	no cumple
Garantías de las transferencias fuera del EEE (arts. 44 a 49 RGPD)	pendiente de verificación
Información a las personas afectadas (arts. 13 y 14 RGPD)	no cumple
Medidas de seguridad (art. 32 RGPD)	con observaciones
Evaluación de impacto (art. 35 RGPD) · Preselección de currículums para puestos de almacén	pendiente de verificación

La IA en materia de protección de datos y el cumplimiento del AI Act son ámbitos relacionados pero distintos: cumplir uno no acredita el otro.

13. Seguridad

Según el cuestionario, las medidas de seguridad de las herramientas de IA están configuradas solo en parte.

IT configura cada herramienta autorizada con acceso mediante la cuenta corporativa (inicio de sesión único cuando sea posible), permisos por perfil, plazo de conservación definido y, cuando el contrato lo permita, el uso de los datos para entrenamiento desactivado. La configuración se documenta y se revisa cada seis meses.

Asistentes conectados al correo, a documentos o a bases de datos (Resumir correos y redactar documentos internos): antes de ampliar su uso se revisan los permisos de las carpetas, sitios y buzones conectados, porque el asistente muestra todo lo que la

persona puede ver (buena práctica; conecta con el art. 32 RGPD).

14. Supervisión humana

La supervisión no se acredita con «siempre lo revisa alguien»: para cada caso de uso se define quién revisa, cuándo, con qué autoridad para detener o corregir el resultado y cómo queda registrada la revisión.

Caso de uso	Quién revisa y cómo	Naturaleza
USE-002 · Preselección de currículums para puestos de almacén	La técnica de RR. HH. revisa solo los descartados cuando hay tiempo	Buena práctica hoy; obligación (art. 26.2 AI Act) desde el 02/12/2027

Chatbots (Responder consultas de seguimiento de envíos): la conversación pasa a una persona cuando el chatbot no sabe responder o el cliente lo pide; cada mes se revisa una muestra de conversaciones y el chatbot no da asesoramiento legal, médico o financiero ni compromete precios o condiciones (buenas prácticas).

15. Transparencia

Sistemas que interactúan con personas ajenas a la empresa (Responder consultas de seguimiento de envíos): el propietario comprueba en cada canal que el sistema avisa de que es una IA al inicio de la interacción y lo exige por contrato al proveedor (art. 50.1 AI Act, obligación de diseño del proveedor desde el 02/08/2026; diligencia de la empresa).

El contenido comercial generado con IA sigue el criterio de etiquetado que aprueba Marketing con Legal, y no se genera la imagen ni la voz de personas reales identificables sin su consentimiento escrito (buenas prácticas).

16. Agentes y automatizaciones

Sistemas que pueden ejecutar acciones en otros sistemas: USE-003 Responder consultas de seguimiento de envíos (Asistente de atención al cliente); USE-004 Textos e imágenes para redes sociales (ChatGPT).

- Tienen solo los permisos imprescindibles para su tarea, revisados cada trimestre.
- Enviar comunicaciones, publicar, pagar o borrar requiere aprobación humana previa.
- Todas sus acciones quedan registradas.
- IT dispone de un mecanismo probado para detenerlos de inmediato.

Buenas prácticas de gobernanza de agentes; conectan con el art. 32 RGPD cuando hay datos personales.

17. Personas trabajadoras

Cuando un sistema de IA influye en decisiones sobre la plantilla o sobre candidatos:

- RR. HH. informa a la representación legal de las personas trabajadoras de los parámetros, reglas e instrucciones de los algoritmos que afectan a sus condiciones de trabajo o al acceso al empleo (art. 64.4.d del Estatuto de los Trabajadores). Estado: no cumple.
- Se revisa periódicamente que los resultados no perjudican de forma injustificada a ningún colectivo (Ley 15/2022, de igualdad de trato y no discriminación).

18. Casos de uso de posible alto riesgo

Los siguientes casos de uso tienen una finalidad incluida en los anexos del AI Act. Sus obligaciones como responsable del despliegue se aplican desde la fecha indicada y se preparan con antelación; la supervisión humana ya se aplica hoy como buena práctica.

Caso de uso	Finalidad	Desde	A preparar
USE-002 · Preselección de currículums para puestos de almacén	RR. HH.: selección o filtrado de candidatos (Anexo III, punto 4.a)	02/12/2027	Supervisión humana por personas competentes (alto riesgo); Uso conforme a las instrucciones del proveedor; Conservación de registros del sistema; Información a las personas sometidas a decisiones

Antes de su uso, el propietario debe valorar con un experto si el caso podría quedar fuera del alto riesgo por no influir de forma sustancial en la decisión (art. 6.3 AI Act). Esa conclusión se documenta; no se presume.

19. Formación y alfabetización en IA

Según el cuestionario, las medidas de formación en IA cubren solo a una parte del personal o de los contenidos.

Según el cuestionario, no se conserva registro de la formación; a partir de este documento debe conservarse.

RR. HH. mantiene un plan de formación por perfiles (personas usuarias, propietarios de herramientas, RR. HH., IT) sobre el uso de cada herramienta, sus límites, los errores e invenciones de la IA, la información protegida y la supervisión. Se conserva el registro de asistencia y los materiales.

El art. 4 AI Act, en la redacción del Reglamento (UE) 2026/1744, exige adoptar medidas que apoyen la alfabetización del personal; no exige un certificado. Estado a la fecha: con observaciones.

20. Incidentes

Según el cuestionario, no existía un procedimiento para registrar y gestionar los incidentes de IA; este apartado lo establece.

Cualquier persona comunica un incidente de IA por este canal: Aviso inmediato al Responsable de IA y a Seguridad de la información. El Responsable de IA lo registra con fecha, sistema, impacto, personas y datos afectados, medidas y cierre.

- Si hay datos personales afectados, el DPO valora la notificación a la autoridad de protección de datos sin dilación indebida y, a más tardar, en 72 horas (art. 33 RGPD) y la comunicación a las personas afectadas (art. 34 RGPD).
- Se informa al proveedor de la herramienta y se conserva su respuesta.
- En sistemas de alto riesgo, desde su fecha de aplicación, los incidentes graves se comunican al proveedor y a las autoridades (art. 26.5 AI Act).

21. Registros y evidencias

Cada requisito aplicable tiene una evidencia identificada (EVD-...). El Responsable de IA custodia las evidencias, su versión, fecha y responsable, y las revisa con la periodicidad indicada en el expediente. A la fecha de este documento hay 3 evidencias por registrar.

Las evidencias se conservan mientras el sistema esté en uso y, como mínimo, hasta la siguiente revisión completa (criterio interno), sin perjuicio de los plazos que exija la normativa aplicable.

22. Gestión de cambios

Antes de aplicarlos, el propietario comunica al Responsable de IA los cambios que pueden alterar las conclusiones del expediente:

- Herramienta, proveedor o integración nuevos.
- Cambio de finalidad, de datos tratados, de personas afectadas o de departamento.
- Aumento de permisos o de autonomía, o cambio importante del modelo.
- Cambio contractual o normativo.
- Incidente, fallo relevante o reclamación.

23. Revisión y auditoría

Este documento y el expediente de La Ley IA se revisan cada 6 meses y, de forma extraordinaria, ante cualquiera de los cambios del apartado anterior. Próxima revisión recomendada: 11/04/2027.

Cada revisión compara el expediente anterior con el actual: riesgos solucionados y nuevos, acciones cerradas, sistemas nuevos, cambios normativos y evidencias vencidas.

24. Excepciones

Solo el Responsable de IA o el comité puede autorizar por escrito una excepción a este documento, con un plazo máximo, un motivo y las medidas que la compensan. Las excepciones se registran y se revisan al vencer su plazo.

25. Retirada de sistemas

Cuando una herramienta deja de usarse se marca como «Retirado» en el inventario (sin borrarla del histórico), se revocan los accesos, se recuperan o eliminan los datos según el contrato y se conservan las evidencias.

26. Incumplimiento

El incumplimiento podrá dar lugar a las medidas previstas en la normativa laboral y en el convenio colectivo aplicables.

27. Aprobación y control de versiones

Órgano que aprueba: Dirección General. La fecha de aprobación, la persona que la registra y cada versión constan en el historial del expediente AUD-EJEMPLO-USO-1NLU.

Anexo A. Puntos pendientes del expediente

Este documento no resuelve por sí solo las deficiencias del expediente. A la fecha de su generación quedan abiertos estos puntos:

- HAL-001 · No discriminación en decisiones apoyadas en IA — Preselección de currículums para puestos de almacén (no cumple)
- HAL-002 · Contrato de encargo de tratamiento con proveedores (no cumple)
- HAL-003 · Información a la representación de los trabajadores sobre algoritmos (no cumple)
- HAL-004 · Información a las personas afectadas (no cumple)
- HAL-005 · Registro de actividades de tratamiento con IA (no cumple)
- Transferencias internacionales de datos · Organización: información pendiente
- Evaluación de impacto en protección de datos (EIPD) · Preselección de currículums para puestos de almacén · Microsoft 365 Copilot: información pendiente
- Permisos mínimos y aprobación de acciones irreversibles · Responder consultas de seguimiento de envíos · Asistente de atención al cliente: información pendiente
- Revisión de derechos de terceros en lo publicado · Textos e imágenes para redes sociales · ChatGPT: información pendiente

La aprobación de este documento acredita la política de uso aceptable de IA (OB-GOV-03). Los demás controles (inventario, responsable, alta de herramientas, Shadow AI, incidentes, formación...) necesitan evidencia de que se aplican: la gobernanza no es solo un documento.

La Ley IA ayuda a ordenar, documentar y priorizar el cumplimiento del uso de IA. No es una certificación ni sustituye el asesoramiento jurídico: contrasta las conclusiones relevantes con un abogado o tu DPO. Motor RULESET-LALEYIA-2026.10 · Marco normativo comprobado hasta 06/10/2026.