Política de uso de la IA

[Empresa] · Documento interno

Redacta	Revisan	Aprueba
[Nombre y cargo]	[Protección de datos] · [Seguridad]	[Dirección]

Versión	Fecha	Qué cambia	Quién
1.0	[dd/mm/aaaa]	Primera versión	[Nombre]

Cómo usar esta plantilla. Borrad este recuadro antes de firmar.

- Pasad a limpio lo que decidisteis en el lienzo. La letra entre paréntesis, (A), (D)..., dice de qué casilla sale cada apartado.
- Sustituid lo que va entre corchetes, [así], por lo vuestro.
- Los apartados que empiezan por «Rellenad esto si...» solo hacen falta si la respuesta es sí. Si es no, borradlos.
- Donde aparezca ⚖, consultad a un abogado. Esta plantilla no es asesoría jurídica.
- Es una política para empezar: recoge lo que pide la ley a cualquier empresa que usa IA y lo que coinciden en pedir las guías. Para ir más allá, mirad el final.

Plantilla de Venturalítica, versión del 19 de octubre de 2026 · venturalitica.ai/politica-de-uso · CC BY-NC-SA 4.0

Parte 1 · Normas de uso de la IA

Para todas las personas que trabajan para [Empresa], también con contrato temporal, en prácticas o desde otra empresa. Son instrucciones de la empresa y son cortas para que se puedan leer enteras.

1.1 · Herramientas que podéis usar (B)

Herramienta	Con qué cuenta	Para qué
[Herramienta]	[Cuenta de empresa]	[Usos aprobados]
[Herramienta]	[Cuenta de empresa]	[Usos aprobados]

Para el trabajo, solo estas herramientas y solo con cuenta de empresa. Ninguna otra herramienta ni cuenta personal, aunque sea gratuita y la información sea pública: las cuentas personales pueden usar lo que se escribe para entrenar sus modelos y no tienen contrato con [Empresa]. Si necesitáis otra, pedid el alta (2.5). Las funciones de IA que traen los programas que ya usamos se activan después de una revisión rápida (2.5).

1.2 · ¿Puedo pegar esto? (D)

Información	[Herramienta 1]	[Herramienta 2]	[Herramienta 3]
Pública	[sí / no]	[sí / no]	[sí / no]
Interna	[sí / no]	[sí / no]	[sí / no]
Confidencial: clientes, contratos, finanzas, código propio	[sí / no]	[sí / no]	[sí / no]
Datos personales: de clientes, del personal, de candidatos	[sí / no]	[sí / no]	[sí / no]
Credenciales: claves, contraseñas, tokens	Nunca	Nunca	Nunca

Las clases de información son las de [nuestra política de seguridad / esta tabla]. Si dudáis de qué clase es algo, tratadlo como confidencial y preguntad. Marcar «sí» en datos personales exige lo del apartado 2.8.

1.3 · Lo que no entra nunca (E)

Ni siquiera en una herramienta aprobada: claves, contraseñas y tokens; esquemas y volcados de bases de datos; configuraciones de seguridad y resultados de pruebas de intrusión; [lo que añadáis vosotros].

1.4 · Antes de usar lo que devuelve (F)

- La IA se equivoca, y a veces se inventa datos o citas. Revisad lo que devuelve antes de usarlo. Quien lo usa responde de ello igual que si lo hubiera hecho a mano.
- Comprobad que no copia textos, imágenes, marcas o código de otros. Si dudáis, no lo uséis y preguntad.
- [Quién revisa qué: por ejemplo, el código generado pasa la revisión de código de siempre].
- Decid que habéis usado IA cuando [lo entreguéis a un cliente / lo publiquéis / ...].

1.5 · Lo que no hacemos (G)

- Decidir sobre personas (contratar, evaluar, despedir, conceder un crédito) con lo que diga la IA, sin una persona que revise y decida.
- Lo que prohíbe la ley de IA (el Reglamento de IA, art. 5). Por ejemplo, reconocer las emociones de los empleados.
- Generar material de abuso sexual infantil o imágenes íntimas de personas reales sin su consentimiento.

- Usarla para engañar o hacer daño: vídeos, audios o imágenes falsos que desinformen, código malicioso o información para actividades ilegales.
- [Lo que añadáis vosotros].

1.6 · Confidencialidad

Lo que sabéis de [Empresa], de sus clientes y de su personal es confidencial, también cuando usáis IA y también después de dejar la empresa.

1.7 · Dudas y avisos (H)

Si tenéis dudas, preguntad a [persona o canal]. Si pegáis algo que no debíais, o la IA hace algo raro o dañino, avisad enseguida a [persona o canal]. Avisar a tiempo es lo que permite arreglarlo.

1.8 · Si no se cumplen ⚖

Estas normas son instrucciones de [Empresa] en el ejercicio de su poder de dirección. Los incumplimientos se gradúan según su gravedad y se sancionan por escrito según [el convenio colectivo / el régimen disciplinario]. ⚖ Encajarlo en vuestro convenio (faltas, sanciones y lo que hay que comunicar al comité) es trabajo de un laboralista.

Estas normas se revisan con la política (2.16) y cuando cambia una herramienta o lo que no entra nunca (J).

Parte 2 · Política de gobierno de la IA

La aprueba la dirección. Dice quién decide sobre la IA en [Empresa], cómo entra una herramienta o un uso nuevo y qué se hace cuando algo sale mal.

2.1 · Objeto y alcance

Esta política se aplica a toda IA que [Empresa] usa: herramientas generales (asistentes y chats), funciones de IA dentro de otros programas, automatizaciones y lo que construyamos sobre un modelo. Llamamos IA a los programas que generan textos, imágenes, predicciones, recomendaciones o decisiones a partir de lo que reciben. Se aplica al personal, a quien trabaja para nosotros desde otra empresa y a los proveedores que usan IA con nuestra información. [Empresa] usa IA de otros; para la ley es «responsable del despliegue», no proveedora. ⚖ Pasaría a ser proveedora de un sistema de alto riesgo si le pone su marca, lo modifica a fondo o le cambia la finalidad hasta hacerlo de alto riesgo (art. 25 del Reglamento de IA).

2.2 · Principios

- Usamos la IA solo cuando es adecuada para la tarea.
- Cada uso de IA tiene una finalidad escrita y una persona que responde de él.
- Las medidas son proporcionales al riesgo: más revisión cuanto más afecta a personas o al negocio.
- Ninguna decisión sobre personas sale solo de la máquina.
- Usamos la información imprescindible y respetamos los derechos de autor de otros.
- Explicamos a clientes y empleados dónde usamos la IA, y quien habla con un asistente de IA nuestro sabe que es una IA.

2.3 · Responsables (C)

Quién	Qué hace
Dirección	Aprueba esta política, da los medios y decide si se acepta un riesgo alto.
Responsable de IA: [cargo, por ejemplo CTO o CIO]	Mantiene el inventario y las normas de uso, revisa las altas, hace el repaso anual y propone cambios.
Protección de datos: [delegado o responsable]	Revisa esta política antes de aprobarla y todo uso con datos personales. ⚖
Seguridad: [responsable]	Revisa esta política antes de aprobarla, las altas con información confidencial y los incidentes.
Personas: [RR. HH.]	Formación, comunicación de las normas y relación con la representación de los trabajadores.
Cada área y cada persona	El área es dueña de sus usos; cada persona sigue las normas y avisa de lo que sale mal.

2.4 · Aprobación y puesta en marcha (J)

1. Protección de datos y seguridad revisan el borrador.
2. Si hay comité de empresa o delegados de personal, se les informa y consulta antes de aprobarla, y se les da el plazo para su informe (hasta quince días). ⚖
3. La dirección la aprueba y la firma.
4. Se comunica a todo el personal y se deja en [intranet], junto a las guías de uso. Cada persona confirma que la ha recibido (acuse de recibo, en el anexo C).

5. Quien empieza a usar una herramienta de IA recibe antes la formación del apartado 2.11. Quien ya usaba una herramienta aprobada la recibe en [un mes]. Las herramientas no aprobadas se dejan de usar desde la firma.

2.5 · Inventario, alta y riesgo de cada uso

El responsable de IA mantiene el inventario de IA, con cada uso que ya se hace, y lo repasa cada [6] meses. Las herramientas aprobadas van en el anexo A. Toda herramienta nueva, también las gratuitas, pasa por el alta y, si se aprueba, se usa con cuenta de empresa: quien la necesita la pide a [persona o canal] con la finalidad y la información que va a usar; el responsable de IA hace al proveedor las preguntas del anexo B; protección de datos y seguridad la revisan si hay datos personales o información confidencial; decide [quién aprueba] y se anota en el inventario y, si se aprueba, en el anexo A. Las funciones de IA que llegan dentro de un programa ya aprobado tienen un alta rápida: se apuntan en el inventario y el responsable de IA las revisa con el anexo B antes de activarlas.

Antes de aprobar un uso se mira cuánto está metida la IA (en el navegador, en la ofimática, en todo el entorno, en un proceso o en el producto) y a quién afecta. Cuanto más metida, más revisión. Aquí «riesgo alto» es riesgo para la empresa o para las personas; el «alto riesgo» del Reglamento de IA es otra cosa: el inventario señala qué usos pueden serlo (anexo D).

> **Rellenad esto si habéis metido IA en un proceso o en vuestro producto, o montado un asistente propio sobre un modelo.**

2.6 · Validar antes de producción

- Antes de usarlo en serio se escriben los criterios de aceptación: qué tiene que hacer bien y cuánto error se tolera.
- Se prueba contra esos criterios: exactitud y respuestas inventadas, sesgo con las personas afectadas, prompt injection y fuga de información.
- [Quién] firma que pasa las pruebas. Se vuelve a probar cuando cambia el modelo, el proveedor, los datos o la finalidad.
- Se puede parar, y alguien sabe cómo.

2.7 · Usos prohibidos

Los que prohíbe el art. 5 del Reglamento de IA, como reconocer emociones en el trabajo, manipular a las personas o puntuarlas por su conducta social. Tampoco se genera material de abuso sexual infantil ni imágenes íntimas de personas reales sin su consentimiento: la ley de IA lo prohíbe expresamente desde el 2 de diciembre de 2026. Además: [lo que añada Empresa].

2.8 · Datos personales y decisiones sobre personas ⚖

Ningún uso con datos personales empieza sin base jurídica, sin contrato de encargo con el proveedor y sin comprobar dónde se tratan los datos; si el uso es de alto riesgo para las personas, se hace antes una evaluación de impacto. Cuando los datos de clientes, personal o candidatos pasan por una herramienta de IA, se actualiza la información que se les da, y sus peticiones de acceso, rectificación o supresión siguen el procedimiento de siempre, con ayuda del proveedor. Lo revisa [protección de datos].

> **Rellenad esto si la IA decide, o ayuda a decidir, algo sobre personas: selección, turnos, rendimiento, crédito.**
>
> Una persona con conocimiento y autoridad revisa y decide, y puede corregir o descartar lo que propone la IA. Ninguna persona queda sujeta a una decisión tomada solo por la máquina que la afecte de forma importante (art. 22 del RGPD). Si el sistema es de alto riesgo, se aplica además el anexo D.

2.9 · Proveedores y seguridad

- Se contrata en modalidad de empresa, con la cláusula de que no se entrena con nuestros datos, y se sabe dónde se guardan y procesan, cuánto tiempo y cómo se recuperan al dejar el servicio.
- Los términos de cada proveedor se repasan cada [6] meses; cambian a menudo.
- Si una herramienta es crítica para un proceso, hay un plan B para seguir trabajando si falla: [otra herramienta / volver al trabajo manual].
- Las normas de uso se apoyan en medios técnicos, en proporción al riesgo y siguiendo buenas prácticas de seguridad reconocidas para la IA: [bloquear las herramientas no aprobadas / avisar al pegar información marcada como confidencial].

> **Rellenad esto si sois entidad financiera, dais servicio a la administración o estáis en un sector esencial, o si ya tenéis una política de seguridad.**
>
> Los proveedores de IA entran en [el registro de proveedores TIC (DORA) / las medidas del ENS / la gestión de la cadena de suministro (NIS2)]. Esta política cuelga de [nombre de la política de seguridad] y usa sus clases de información, sus accesos y su procedimiento de incidentes.

2.10 · Qué revisa la empresa del uso de la IA ⚖

[Empresa] puede revisar el uso de las herramientas de IA que pone a disposición del personal, solo para comprobar que se siguen estas normas y para proteger su información, con respeto a la dignidad y la intimidad de las personas, y lo informa antes (art. 20.3 del Estatuto de los Trabajadores y art. 87 de la LOPDGDD). [Si se permite usar estas herramientas para fines personales: qué usos se admiten y qué no se revisa de ellos.]

2.11 · Formación

[Empresa] forma a cada persona según lo que hace con la IA antes de darle acceso (en [un mes] si ya la usaba), y guarda registro (anexo C). La formación explica qué herramientas usamos y qué no hacen bien, estas normas, los derechos de autor y los datos personales, y los engaños que se hacen con IA (voces y correos falsos). Se repite cada [12] meses y cuando cambia una herramienta, y entra en el plan de formación de la empresa.

> **Rellenad esto si publicáis contenido generado con IA: textos, imágenes, voces o vídeos.**
>
> ### 2.12 · Transparencia
>
> Se indica que es artificial toda imagen, audio o vídeo generado o manipulado que parezca auténtico. Los textos generados que se publican para informar sobre asuntos de interés público también se marcan, salvo que una persona los revise y responda de ellos (art. 50 del Reglamento de IA, desde el 2 de agosto de 2026). Lo lleva [comunicación].

> **Rellenad esto si tenéis comité de empresa o delegados de personal. ⚖**
>
> ### 2.13 · Representación de los trabajadores
>
> Además de la consulta del apartado 2.4, [Empresa] informa a la representación de los parámetros, reglas e instrucciones de los algoritmos que afectan a las condiciones de trabajo, al acceso al empleo o a su mantenimiento (art. 64.4.d del Estatuto de los Trabajadores), y le pide informe sobre los planes de formación.

2.14 · Incidentes

Es un incidente de IA: meter información donde no debía ir, una salida dañina o discriminatoria, una respuesta inventada que llega a un cliente, un ataque de prompt injection o un agente que actúa fuera de lo previsto. Se avisa a [persona o canal] y se trata con [el procedimiento de incidentes de seguridad]. Cada incidente se clasifica como

leve o grave. Si es grave, [quién] avisa a la dirección, puede parar el sistema y decide cómo y cuándo se informa a los afectados. Si hay datos personales, se valora avisar a la AEPD en 72 horas.

2.15 · Excepciones

Las excepciones a esta política se piden, se justifican y se aprueban por escrito. Los incumplimientos se tratan según el apartado 1.8.

2.16 · Seguimiento y revisión

Cada [12] meses el responsable de IA compara el inventario con lo que se usa de verdad (también las herramientas sin aprobar que aparezcan), pregunta a quien usa la IA qué le sirve y qué no, y lleva el resultado a la dirección. Con eso se revisa la política, y también antes si hay un incidente grave, un uso nuevo de riesgo, un cambio en los términos de un proveedor o una norma nueva (por ejemplo, la ley española de IA, cuyo proyecto decayó al disolverse las Cortes en octubre de 2026). Al aprobarla se revisan las demás políticas que afecta la IA: [privacidad, seguridad, contratación, condiciones de servicio].

Cuando queráis ir más allá. Esta política es una base. Lo siguiente es un sistema de gestión de la IA según la ISO/IEC 42001, que añade:

- un inventario completo, con la documentación de cada herramienta y el origen de los datos que usa;
- la evaluación de riesgos de cada uso con un método y criterios escritos;
- contratos con proveedores que fijen niveles de servicio, avisos de incidentes y derechos sobre lo generado;
- pruebas y seguimiento de los sistemas en producción;
- la auditoría interna, que nace del repaso anual del 2.16, y la revisión por la dirección.

Referencias

- Reglamento (UE) 2024/1689 de inteligencia artificial, modificado por el Reglamento (UE) 2026/1744 (Ómnibus digital sobre IA).
- Reglamento General de Protección de Datos y Ley Orgánica 3/2018 (LOPDGDD).
- Estatuto de los Trabajadores, arts. 20, 58 y 64. Ley 1/2019 de secretos empresariales.
- Siguiente paso, si queréis certificaros: ISO/IEC 42001:2023, sistema de gestión de la IA.

Anexo A · Herramientas aprobadas

Los usos de cada herramienta y su calificación ante el Reglamento de IA van en el inventario de IA (plantilla en venturalitica.ai/inventario). Aquí, solo las herramientas aprobadas y sus condiciones.

Herramienta y plan	Dueño	Usos aprobados	Información que admite	¿Afecta a personas?	Términos repasados

Anexo B · Doce preguntas al proveedor

Pregunta	Respuesta
1. ¿Entrena con nuestros datos? ¿Por defecto o solo si lo aceptamos? ¿Lo dice el contrato?	
2. ¿Cuánto tiempo guarda lo que escribimos y lo que devuelve? ¿Se puede pedir que no guarde nada?	
3. ¿Leen personas las conversaciones? ¿Cuándo?	
4. ¿Qué subcontratistas y modelos de terceros intervienen? ¿Hay contrato de encargo del tratamiento? ⚖	
5. ¿Dónde se guardan y dónde se procesan los datos? ¿Con qué plan se queda en la UE?	
6. ¿Hay inicio de sesión de empresa, roles y registros que podamos exportar?	
7. ¿Qué certificaciones tiene, y qué cubren de verdad?	
8. ¿Qué conectores o agentes trae, qué permisos piden y puede limitarlos el administrador?	
9. Si lo dejamos: ¿cómo nos llevamos los datos, cómo se borran y con qué preaviso cambia el modelo o los términos?	
10. ¿Nos cubre si lo que genera infringe derechos de otros?	
11. ¿Nos avisa de los incidentes graves y nos ayuda con auditorías y con las peticiones de acceso o supresión de datos?	
12. ¿A qué niveles de servicio se compromete (disponibilidad, soporte, tiempo de respuesta)?	

Anexo C · Registro de formación

Persona o grupo	Qué hace con la IA	Formación	Fecha	Recibió la política

Rellenad esto si usáis un sistema de IA de alto riesgo: por ejemplo, para seleccionar o evaluar personal, o para decidir sobre crédito o seguros. ⚖

Anexo D · Si usáis un sistema de alto riesgo

Desde el 2 de diciembre de 2027 (y desde el 2 de agosto de 2028 para los que van dentro de productos regulados, del anexo I), quien usa un sistema de alto riesgo tiene que (art. 26):

- usarlo según las instrucciones del proveedor y encargar la supervisión a personas competentes, con formación y autoridad;
- darle datos de entrada pertinentes para su finalidad;
- vigilar cómo funciona, avisar al proveedor de los problemas y suspender el uso si hay riesgo;
- guardar al menos seis meses los registros que genere;
- informar antes a la representación de los trabajadores y a las personas afectadas, e informar a las personas sobre las que se decide;
- cooperar con las autoridades.

Quien presta servicios públicos o usa la IA para solvencia o seguros de vida y salud hace además una evaluación de impacto en los derechos fundamentales antes de usarlo, la actualiza si cambia algo y notifica el resultado a la autoridad (art. 27). Hasta 2027, [Empresa] [anota cómo se prepara]. Parte de esto ya se pide hoy por otras leyes: informar a la representación (2.13) y las garantías de los datos personales (2.8).