

Índice

1 Objeto	2
2. Marco normativo de referencia	2
3. Ámbito de aplicación	2
4. Principio general de uso	3
5. Principios rectores	3
6. Responsabilidades	5
7. Sistemas de IA autorizados	6
8. Usos permitidos de IA	6
9. Usos sujetos a autorización previa reforzada	7
10. Usos prohibidos	7
11. Reglas específicas para ChatGPT, NotebookLM, Claude, Perplexity y agentes de IA	8
12. Revisión humana obligatoria	10
13. Prohibición de dependencia automática del output	11
14. Protección de datos personales	11
15. Confidencialidad y secreto empresarial	11
16. Propiedad intelectual	12
17. Clasificación de riesgos de usos de IA	12
18. Procedimiento de aprobación de nuevos sistemas o usos de IA	13
19. Uso de IA en proyectos de consultoría normativa	14
20. Uso de IA en proyectos de ingeniería, seguridad industrial, instalaciones industriales y máquinas	14
21. Uso de IA en relaciones con clientes	15
22. Transparencia sobre contenidos generados por IA	15
23. Alfabetización y formación en IA	15
24. Gestión de incidentes relacionados con IA	16
25. Conservación de evidencias y trazabilidad	17
26. Proveedores de IA	17
27. Integración con el sistema de gestión de riesgos	17
28. Control de freelancers y colaboradores externos	18
29. Control documental	18
30. Medidas específicas para evitar errores técnicos y normativos	18
31. Evaluación periódica	19
32. Medidas disciplinarias y consecuencias del incumplimiento	19
33. Declaración corporativa de uso responsable de IA	19

1 Objeto

La presente Política Corporativa de Gobernanza y Uso Responsable de Inteligencia Artificial tiene por objeto establecer los principios, responsabilidades, controles y procedimientos internos aplicables al uso de sistemas de inteligencia artificial por parte de SOLINGESA.

La entidad utiliza sistemas de IA, entre ellos ChatGPT, NotebookLM y agentes internos o externos basados en IA, como herramientas de apoyo para la elaboración de borradores, análisis preliminares, estructuración de información, generación de propuestas, preparación de documentación de consultoría normativa, apoyo a proyectos de ingeniería, seguridad industrial, instalaciones industriales, máquinas y actividades auxiliares de gestión.

La presente política establece que ningún resultado generado por IA tendrá valor definitivo, vinculante, técnico, jurídico, contractual o entregable sin revisión, validación y aprobación por una persona competente.

Esta política tiene como finalidad asegurar que el uso de IA se realiza de forma lícita, segura, transparente, trazable, proporcionada, supervisada y alineada con el Reglamento (UE) 2024/1689, conocido como Reglamento Europeo de Inteligencia Artificial o AI Act.

2. Marco normativo de referencia

Esta política se interpreta conforme a la normativa aplicable, en particular:

- Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial.
- Reglamento (UE) 2016/679, Reglamento General de Protección de Datos.
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- Normativa sobre seguridad industrial, instalaciones industriales, máquinas, prevención de riesgos laborales, metrología, productos, marcado CE y demás legislación técnica aplicable a los proyectos en los que intervenga la entidad.
- Normativa sobre propiedad intelectual, secretos empresariales, confidencialidad contractual y competencia desleal.
- Normativa interna de seguridad de la información, protección de datos, calidad, compliance, gestión documental y contratación.

A efectos del RIA, la entidad actúa ordinariamente como responsable del despliegue de sistemas de IA, en la medida en que utiliza sistemas de IA bajo su propia autoridad y en el marco de su actividad profesional. El Reglamento define al responsable del despliegue como la persona física o jurídica que utiliza un sistema de IA bajo su propia autoridad, salvo usos personales no profesionales .

3. Ámbito de aplicación

Esta política se aplica a:

- A todo el personal de SOLINGESA, incluida su dirección y responsables.
- Profesionales freelance, colaboradores externos y subcontratistas integrados en proyectos de la entidad.
- Proveedores tecnológicos que operen sistemas de IA por cuenta de la entidad.
- Cualquier persona que utilice herramientas de IA en nombre de la entidad o para preparar trabajos, entregables, informes, propuestas, cálculos, revisiones, análisis, documentación técnica, documentación legal, documentación normativa o documentación de ingeniería.

Esta política se aplica al uso de cualquier sistema de IA, incluyendo, sin carácter limitativo:

- ChatGPT
- NotebookLM
- Claude
- Perplexity

- e. Agentes de IA configurados por la entidad.
- f. Herramientas de IA generativa de texto, imagen, audio, vídeo, código o documentos.
- g. Asistentes integrados en suites ofimáticas, navegadores, buscadores, repositorios documentales, herramientas de gestión de proyectos o plataformas de productividad.
- h. Sistemas de IA utilizados para clasificación documental, resúmenes, extracción de requisitos, generación de checklists, preparación de ofertas, análisis normativo, análisis de riesgos, elaboración de borradores o soporte técnico.
- i. Cualquier sistema de IA incorporado en software de terceros utilizado en proyectos.

4. Principio general de uso

SOLINGESA solo utilizará IA como herramienta de apoyo a profesionales humanos.

La IA podrá utilizarse para acelerar tareas, mejorar la estructura de documentos, generar borradores, identificar cuestiones preliminares, comparar requisitos, preparar listas de verificación o apoyar tareas de análisis. Sin embargo, la IA no sustituirá el juicio profesional, técnico, jurídico o de compliance de la entidad.

Toda salida generada por IA deberá ser revisada antes de su uso profesional, especialmente cuando pueda afectar a:

- a. Cumplimiento legal o regulatorio.
- b. Seguridad industrial.
- c. Seguridad de máquinas.
- d. Instalaciones industriales.
- e. Evaluaciones de riesgos.
- f. Conformidad normativa.
- g. Recomendaciones a clientes.
- h. Informes técnicos.
- i. Documentación contractual.
- j. Derechos, intereses o expectativas legítimas de terceros.
- k. Seguridad de personas, bienes, procesos o instalaciones.

La revisión humana deberá ser realizada por una persona con competencia suficiente en la materia objeto del documento o análisis.

5. Principios rectores

El uso de IA por SOLINGESA se regirá por los siguientes principios:

5.1. Legalidad

La IA solo podrá utilizarse para finalidades lícitas, legítimas y compatibles con la normativa aplicable, los compromisos contractuales con clientes y las políticas internas.

5.2. Supervisión humana

Todo uso profesional de IA estará sometido a supervisión humana. En ningún caso se aceptarán outputs de IA de forma automática para emitir conclusiones técnicas, jurídicas, regulatorias o de ingeniería.

5.3. Responsabilidad profesional

La responsabilidad sobre el contenido final de los entregables corresponderá siempre a la persona o equipo que los revise, valide y apruebe. La IA no será considerada autora, responsable técnica, responsable jurídica ni responsable del proyecto. La responsabilidad profesional incluye un deber de prudencia, discernimiento y cuidado. Ninguna presión de plazo, coste, productividad o automatización

justificará aceptar outputs de IA sin revisión suficiente cuando puedan afectar a clientes, seguridad industrial, cumplimiento normativo, derechos de personas, confianza pública o integridad documental

5.4. Solidaridad profesional

El uso de IA deberá favorecer la colaboración, el aprendizaje compartido, la mejora de capacidades y la calidad del trabajo común, evitando que la automatización genere aislamiento, precarización del juicio profesional, dependencia acrítica o transferencia injusta de riesgos a freelancers, clientes o usuarios finales.

5.5. Transparencia interna

SOLINGESA mantendrá un registro de los sistemas de IA autorizados y de sus usos principales. Los colaboradores externos deberán informar del uso de IA cuando esta haya contribuido de forma sustancial a la elaboración de un entregable.

5.6. Confidencialidad

No se introducirán en herramientas de IA datos confidenciales, secretos empresariales, información sensible de clientes, documentación contractual, datos personales, planos, esquemas, informes, expedientes técnicos o documentación protegida, salvo que la herramienta esté expresamente autorizada para ello y existan garantías contractuales, técnicas y organizativas suficientes.

5.7. Verdad, integridad y no simulación

SOLINGESA no utilizará IA para aparentar conocimientos, evidencias, verificaciones, inspecciones, revisiones o certezas que no existan. Todo documento deberá distinguir entre análisis preliminar, hipótesis, borrador, evidencia verificada y conclusión profesional validada..

5.8. Protección de datos

Todo tratamiento de datos personales mediante sistemas de IA deberá contar con base jurídica, finalidad determinada, minimización, limitación de conservación y medidas de seguridad adecuadas.

5.9. Seguridad técnica

El uso de IA deberá respetar los requisitos internos de seguridad de la información, control de accesos, gestión de credenciales, protección de documentación de clientes y prevención de fugas de información.

5.10. Calidad técnica

Los resultados generados por IA deberán ser verificados frente a fuentes fiables, normativa vigente, documentación técnica aplicable, instrucciones de fabricantes, especificaciones del cliente, normas armonizadas y criterios profesionales.

5.11. Subsidiariedad tecnológica

La IA deberá apoyar el trabajo humano, no sustituir indebidamente el juicio experto ni desplazar responsabilidades que corresponden a personas competentes. Las decisiones relevantes deberán permanecer en el nivel humano y profesional adecuado.

5.12. No discriminación y derechos fundamentales

SOLINGESA no utilizará IA para generar, justificar o automatizar decisiones discriminatorias, arbitrarias o contrarias a los derechos fundamentales.

5.13. Primacía de la dignidad humana

SOLINGESA utilizará la inteligencia artificial como herramienta al servicio de las personas, evitando todo uso que reduzca a clientes, trabajadores, colaboradores, usuarios, proveedores o personas afectadas a meros datos, perfiles, recursos productivos o variables de eficiencia. La IA deberá emplearse de forma compatible con la dignidad, la libertad, la responsabilidad y el valor intrínseco de toda persona.

5.14. Bien común y utilidad social del uso de IA

Antes de incorporar o ampliar un uso de IA, SOLINGESA valorará no solo su eficiencia interna, sino también su contribución real a la calidad del servicio, la seguridad, la fiabilidad técnica, la protección de clientes y la mejora responsable de los procesos. No se aprobarán usos de IA cuya única finalidad sea acelerar tareas si ello deteriora la calidad, la seguridad, la verdad documental o la responsabilidad profesional.

5.15. Cuidado de los vulnerables y partes afectadas

Cuando un uso de IA pueda afectar directa o indirectamente a trabajadores, autónomos, clientes pequeños, usuarios finales, comunidades, personas con discapacidad, personas en situación de dependencia o terceros expuestos a riesgos de seguridad, se aplicará un criterio reforzado de prudencia, revisión humana y proporcionalidad.

5.16. Trazabilidad

Cuando el uso de IA sea relevante para un entregable, deberá conservarse evidencia razonable del uso realizado, de la revisión humana aplicada y de la versión final aprobada.

6. Responsabilidades

Personal propio

El personal propio de SOLINGESA deberá cumplir esta política. Sus obligaciones son:

- a. Utilizar IA únicamente cuando esté permitido por SOLINGESA o por el responsable del proyecto.
- b. No introducir información de clientes en herramientas de IA no autorizadas.
- c. No entregar contenidos generados por IA como si fueran definitivos o verificados.
- d. Informar internamente cuando hayan utilizado IA de forma sustancial en un documento, análisis o entregable.
- e. Revisar profesionalmente cualquier resultado de IA antes de remitirlo.
- f. Respetar la confidencialidad, propiedad intelectual y protección de datos.
- g. Comunicar errores, sesgos, resultados anómalos o riesgos detectados.

Freelancers y colaboradores externos

Los freelancers y colaboradores externos que participen en proyectos de la entidad deberán cumplir esta política como condición de colaboración.

Sus obligaciones son:

- h. Utilizar IA únicamente cuando esté permitido por SOLINGESA o por el responsable del proyecto.
- i. No introducir información de clientes en herramientas de IA no autorizadas.
- j. No entregar a SOLINGESA contenidos generados por IA como si fueran definitivos o verificados.
- k. Informar a SOLINGESA cuando hayan utilizado IA de forma sustancial en un documento, análisis o entregable.
- l. Revisar profesionalmente cualquier resultado de IA antes de remitirlo.
- m. Respetar la confidencialidad, propiedad intelectual y protección de datos.
- n. Comunicar errores, sesgos, resultados anómalos o riesgos detectados.

o. Aceptar la supervisión de SOLINGESA sobre los trabajos realizados con apoyo de IA. SOLINGESA podrá exigir a los freelancers una declaración específica de cumplimiento de esta política para cada proyecto.

Responsables de proyecto

Para cada proyecto concreto, el responsable asignado deberá:

- Determinar si puede utilizarse IA en el proyecto.
- Definir qué información puede introducirse en herramientas de IA.
- Verificar que los outputs se revisan antes de incorporarse a entregables.
- Mantener evidencia de revisión cuando el uso sea relevante.
- Consultar al Responsable de Cumplimiento de IA ante dudas.

7. Sistemas de IA autorizados

SOLINGESA mantendrá un Inventario de Sistemas de IA Autorizados.

Inicialmente, se consideran sujetos a esta política los siguientes sistemas:

- ChatGPT
- NotebookLM
- Claude
- Perplexity (solo búsquedas, no generación)
- Agentes de IA desplegados por la entidad para apoyo documental, análisis preliminar, preparación de borradores, clasificación de información, generación de checklists o asistencia en proyectos.

El uso de cualquier nueva herramienta de IA requerirá una revisión previa mínima por el Responsable de Cumplimiento IA, salvo herramientas de bajo riesgo integradas en software corporativo ya aprobado, siempre que no traten información confidencial, datos personales o documentación de clientes.

El inventario deberá indicar, al menos:

- Nombre del sistema.
- Proveedor.
- Finalidad autorizada.
- Áreas que pueden usarlo.
- Tipo de información permitida.
- Restricciones.
- Fecha de autorización.
- Responsable interno.
- Necesidad de revisión periódica.
- Riesgos principales.
- Medidas de control.

8. Usos permitidos de IA

Los usos permitidos solo lo serán cuando no comprometan la verdad, la calidad profesional, la seguridad, la confidencialidad, la dignidad de las personas ni la responsabilidad humana final.

Con carácter general, se permiten los siguientes usos, siempre que se respeten las restricciones de confidencialidad, protección de datos y revisión humana:

- Preparación de primeras versiones de políticas, procedimientos, informes, checklists, matrices y documentos normativos.
- Preparación de borradores de documentación técnica o de ingeniería, sujetos a revisión técnica.

- c. Resumen de documentos no confidenciales o previamente autorizados.
- d. Comparación preliminar de requisitos normativos.
- e. Identificación de posibles apartados faltantes en documentos.
- f. Generación de esquemas, índices y estructuras documentales.
- g. Revisión lingüística, claridad, estilo y formato.
- h. Elaboración de actas o notas internas a partir de información no confidencial o debidamente autorizada.
- i. Generación de preguntas de auditoría o listas de comprobación.
- j. Apoyo a formación interna.
- k. Generación de ejemplos genéricos.
- l. Apoyo al análisis de riesgos, siempre que la valoración final sea humana.
- m. Creación de plantillas reutilizables.

9. Usos sujetos a autorización previa reforzada

Requerirán autorización previa de la Dirección o del Responsable de Cumplimiento de IA los siguientes usos:

- a. Uso de IA con documentación confidencial de clientes.
- b. Uso de IA con datos personales.
- c. Uso de IA con documentación técnica sensible, planos, expedientes, fotografías de instalaciones, esquemas eléctricos, layouts industriales o información de seguridad.
- d. Uso de IA para apoyar evaluaciones de conformidad de máquinas, instalaciones o equipos.
- e. Uso de IA para análisis que puedan afectar a la seguridad de personas, bienes, instalaciones o procesos industriales.
- f. Uso de IA para preparar informes que puedan ser aportados a autoridades, organismos de control, juzgados, aseguradoras o terceros con efectos relevantes.
- g. Uso de IA para decisiones sobre selección, evaluación o contratación de freelancers o personal.
- h. Uso de IA para scoring, priorización o evaluación de clientes, proveedores o personas.
- i. Uso de IA conectada a repositorios internos de clientes.
- j. Uso de agentes autónomos que ejecuten acciones, envíen comunicaciones, modifiquen documentos o tomen decisiones sin validación humana previa.
- k. Uso de IA para generar contenido público sobre asuntos de interés público.
- l. Uso de IA para generar imágenes, audio o vídeo sintético.
- m. Uso de IA que pueda afectar a la reputación profesional de personas, empresas cliente o colaboradores.
- n. Uso de IA para resumir, reinterpretar o reformular declaraciones de personas en auditorías, entrevistas o investigaciones internas.
- o. Uso de IA para generar conclusiones sobre cultura ética, clima organizativo, madurez de compliance o comportamiento humano.
- p. Uso de IA en proyectos donde el cliente sea una pyme, entidad vulnerable o con baja capacidad técnica para revisar outputs.
- q. Uso de IA para elaborar materiales de comunicación pública del cliente.

10. Usos prohibidos

Queda prohibido:

- a. Utilizar IA para manipular, engañar o alterar sustancialmente el comportamiento de personas de forma perjudicial.
- b. Utilizar IA para explotar vulnerabilidades por edad, discapacidad, situación social o económica.
- c. Utilizar IA para realizar puntuación social de personas físicas.

- d. Utilizar IA para inferir opiniones políticas, afiliación sindical, religión, orientación sexual, raza u otros atributos sensibles a partir de datos biométricos.
- e. Utilizar IA para reconocimiento de emociones en el entorno laboral o en procesos de selección, salvo que una norma aplicable lo permita expresamente y exista autorización previa de Dirección.
- f. Utilizar IA para vigilancia laboral encubierta.
- g. Utilizar IA para tomar decisiones finales automatizadas sobre personas.
- h. Utilizar IA para sustituir la firma, criterio o validación de un técnico competente.
- i. Utilizar IA para emitir conclusiones definitivas sobre seguridad industrial, conformidad de máquinas, cumplimiento normativo o riesgos graves sin revisión humana cualificada.
- j. Introducir información confidencial de clientes en herramientas públicas de IA no autorizadas.
- k. Introducir datos personales en herramientas de IA sin base jurídica, información previa y garantías adecuadas.
- l. Introducir secretos empresariales, know-how, ofertas, contratos, expedientes técnicos o documentación protegida sin autorización.
- m. Utilizar cuentas personales para trabajos profesionales con IA cuando ello implique pérdida de control sobre la información.
- n. Presentar contenido generado por IA como si fuera íntegramente elaborado, contrastado o verificado por una persona.
- o. Usar IA para generar documentación falsa, evidencias ficticias, certificados inexistentes, firmas, sellos, actas, inspecciones o registros no reales.
- p. Usar IA para eludir obligaciones legales, contractuales o profesionales.
- q. Usar IA para producir documentos que oculten incertidumbre técnica, jurídica o factual relevante.
- r. Usar IA para sustituir la escucha directa del cliente, trabajadores o personas afectadas cuando esa escucha sea necesaria para comprender el caso.
- s. Usar IA para imponer decisiones por pura eficiencia cuando existan impactos relevantes sobre personas o seguridad.
- t. Usar IA para diluir la responsabilidad profesional, contractual o técnica.

Estas prohibiciones se alinean con el artículo 5 del AI Act, que prohíbe prácticas como sistemas de IA manipuladores, explotación de vulnerabilidades o sistemas de puntuación social que provoquen tratos perjudiciales o desfavorables .

11. Reglas específicas para ChatGPT, NotebookLM, Claude, Perplexity y agentes de IA

11.1. ChatGPT

ChatGPT podrá utilizarse para:

- a. Generar borradores.
- b. Reestructurar textos.
- c. Preparar checklists.
- d. Revisar claridad y coherencia.
- e. Proponer enfoques preliminares.
- f. Ayudar en análisis normativos no definitivos.
- g. Crear ejemplos y plantillas.

No podrá utilizarse para:

- a. Introducir información confidencial de clientes salvo autorización expresa y configuración adecuada.
- b. Delegar conclusiones técnicas finales.
- c. Sustituir revisión normativa actualizada.

- d. Sustituir el criterio del Director Técnico o del consultor responsable.
- e. Generar entregables finales sin revisión.

11.2. NotebookLM

NotebookLM podrá utilizarse para:

- a. Trabajar sobre documentación autorizada.
- b. Resumir materiales internos permitidos.
- c. Comparar documentos cargados.
- d. Preparar mapas de contenidos.
- e. Extraer cuestiones pendientes de revisión.

Antes de cargar documentación en NotebookLM deberá verificarse:

- a. Que se permite cargar dicha documentación.
- b. Que no contiene datos personales innecesarios.
- c. Que no contiene información de cliente no autorizada.
- d. Que el uso respeta compromisos de confidencialidad.
- e. Que se aplican las condiciones de seguridad aprobadas.

11.3. Claude

ChatGPT podrá utilizarse para:

- a. Generar borradores.
- b. Reestructurar textos.
- c. Preparar checklists.
- d. Revisar claridad y coherencia.
- e. Proponer enfoques preliminares.
- f. Ayudar en análisis normativos no definitivos.
- g. Crear ejemplos y plantillas.

No podrá utilizarse para:

- a. Introducir información confidencial de clientes salvo autorización expresa y configuración adecuada.
- b. Delegar conclusiones técnicas finales.
- c. Sustituir revisión normativa actualizada.
- d. Sustituir el criterio del Director Técnico o del consultor responsable.
- e. Generar entregables finales sin revisión.

11.4. Perplexity

ChatGPT podrá utilizarse para:

- a. Realizar búsquedas en internet asistida por IA.
- b. Refinar búsquedas en internet.
- c. Obtener fuentes de referencia en internet para una temática.

No podrá utilizarse para:

- a. Introducir información confidencial de clientes salvo autorización expresa y configuración adecuada.
- b. Delegar conclusiones técnicas finales.
- c. Sustituir revisión normativa actualizada.
- d. Sustituir el criterio del Director Técnico o del consultor responsable.

- e. Generar entregables finales sin revisión.
- f. Generar borradores.
- g. Reestructurar textos.
- h. Preparar checklists.
- i. Revisar claridad y coherencia.
- j. Proponer enfoques preliminares.
- k. Ayudar en análisis normativos no definitivos.
- l. Crear ejemplos y plantillas.

11.5. Agentes de IA

Los agentes de IA desplegados por la entidad se utilizarán únicamente para las finalidades aprobadas.

Todo agente deberá tener:

- a. Finalidad definida.
- b. Responsable interno.
- c. Instrucciones de uso.
- d. Límites funcionales.
- e. Prohibición de actuación autónoma no autorizada.
- f. Registro mínimo de uso cuando sea relevante.
- g. Revisión periódica.
- h. Control de acceso.
- i. Prueba previa antes de uso en proyectos reales.

Los agentes no podrán enviar comunicaciones a clientes, modificar entregables finales, emitir informes, aprobar documentos, tomar decisiones o ejecutar acciones externas sin validación humana previa.

12. Revisión humana obligatoria

Todo contenido generado por IA que vaya a utilizarse profesionalmente deberá ser revisado por una persona competente.

La revisión humana incluirá, según proceda:

- a. Comprobación de exactitud.
- b. Comprobación normativa.
- c. Comprobación técnica.
- d. Verificación de fuentes.
- e. Adecuación al contexto del cliente.
- f. Detección de errores, omisiones o invenciones.
- g. Revisión de sesgos.
- h. Revisión de confidencialidad.
- i. Revisión de protección de datos.
- j. Revisión de coherencia con el alcance contratado.
- k. Revisión de responsabilidad profesional.
- l. Revisión de humanidad y contexto: Usar IA para diluir la responsabilidad profesional, contractual o técnica.
- m. Revisión de justicia y proporcionalidad: En entregables que afecten a personas, organización del trabajo, cumplimiento, seguridad o medidas correctoras, se revisará que las recomendaciones sean proporcionadas, justas, aplicables y no trasladen cargas indebidas a colectivos con menor capacidad de respuesta.
- n. Aprobación final.

En proyectos de ingeniería, seguridad industrial, instalaciones industriales o máquinas, la revisión deberá realizarse por profesional competente designado.

El AI Act exige que, en sistemas de IA de alto riesgo, la supervisión humana se encomiende a personas físicas con competencia, formación y autoridad necesarias. Aunque los usos actuales de SOLINGESA se configuran principalmente como apoyo documental, la entidad adopta este criterio como estándar interno general.

13. Prohibición de dependencia automática del output

Los usuarios deberán evitar el sesgo de automatización, entendido como la tendencia a aceptar como correcto un resultado generado por IA por el mero hecho de haber sido producido por un sistema avanzado.

Queda prohibido:

- Copiar y pegar outputs de IA en entregables sin revisión.
- Aceptar referencias normativas sin comprobación.
- Aceptar cálculos, criterios técnicos o conclusiones sin verificación.
- Confiar en que la IA conoce la normativa vigente sin contraste.
- Utilizar IA como única fuente para interpretar obligaciones legales o técnicas.
- Incorporar citas, normas, artículos o jurisprudencia sin validación.

14. Protección de datos personales

La introducción de datos personales en sistemas de IA solo estará permitida cuando:

- Exista una finalidad legítima.
- Exista base jurídica aplicable.
- Se haya informado a los interesados cuando proceda.
- Se respete el principio de minimización.
- Se hayan evaluado los riesgos.
- Exista contrato de encargo del tratamiento o garantías equivalentes cuando corresponda.
- La herramienta haya sido autorizada para tratar dichos datos.
- Se respeten las políticas internas de protección de datos.

Como regla general, antes de introducir información en una herramienta de IA se aplicará un criterio de minimización: anonimizar, seudonimizar, resumir o eliminar datos identificativos siempre que sea posible.

Cuando el uso de IA pueda implicar alto riesgo para los derechos y libertades de personas físicas, se valorará la necesidad de realizar una evaluación de impacto en protección de datos.

15. Confidencialidad y secreto empresarial

La información de clientes, proyectos, instalaciones, procesos, máquinas, ofertas, contratos, auditorías, informes, planos, esquemas, fotografías, expedientes, bases de datos, registros, estrategias y know-how de la entidad tendrá la consideración de información protegida.

No podrá introducirse dicha información en sistemas de IA salvo autorización expresa y verificación de garantías.

La confidencialidad no se concibe solo como obligación contractual, sino como deber de respeto hacia clientes, trabajadores, colaboradores y terceros cuya información puede revelar aspectos técnicos, económicos, personales o estratégicos relevantes.

SOLINGESA no realizará extracción oportunista de conocimiento: No se utilizará IA para apropiarse, reutilizar o transformar conocimiento de clientes, freelancers o terceros de forma incompatible con la confianza recibida, la finalidad del encargo o los derechos de propiedad intelectual e industrial.

Los freelancers y colaboradores externos deberán:

- Mantener la confidencialidad de la información recibida.

- b. No usar herramientas de IA no autorizadas con información de SOLINGESA o de clientes.
- c. No reutilizar prompts, documentos, datasets o outputs de proyectos para otros clientes.
- d. No entrenar sistemas propios con información de SOLINGESA o de sus clientes.
- e. Eliminar o devolver la información al finalizar el proyecto, según instrucciones de la entidad.

16. Propiedad intelectual

Los usuarios deberán respetar los derechos de propiedad intelectual e industrial de terceros.

Antes de utilizar outputs de IA en documentos profesionales se verificará que:

- a. No incorporan texto protegido reproducido de forma indebida.
- b. No contienen imágenes, diagramas, marcas, logotipos o materiales sujetos a derechos no autorizados.
- c. No se atribuyen fuentes inexistentes.
- d. No se vulneran derechos de terceros.
- e. El contenido final puede ser utilizado contractualmente por la entidad y por el cliente.

Cuando se utilicen sistemas de IA para generar plantillas, diagramas, gráficos o documentación, la persona responsable deberá revisar su originalidad, adecuación y licitud.

17. Clasificación de riesgos de usos de IA

SOLINGESA clasificará los usos de IA en las siguientes categorías internas:

17.1. Riesgo bajo

Usos administrativos o de productividad sin datos personales, sin información confidencial y sin impacto en personas o seguridad, como por ejemplo:

- Reformulación de textos genéricos.
- Creación de índices.
- Preparación de plantillas internas.
- Corrección de estilo.
- Resúmenes de contenido público.

17.2. Riesgo medio

Usos que apoyan tareas profesionales internas o de proyecto, pero siempre con revisión humana y sin decisión automatizada, como por ejemplo:

- Borradores de informes de cumplimiento normativo
- Borradores de procedimientos.
- Comparativas normativas preliminares.
- Checklists de auditoría.
- Apoyo a documentación técnica no final.

17.3. Riesgo alto interno

Usos que pueden afectar a clientes, seguridad, cumplimiento, derechos de personas, documentación técnica sensible o decisiones relevantes, como por ejemplo:

- Informes de seguridad industrial.
- Documentación de máquinas o instalaciones.
- Evaluaciones de cumplimiento normativo.
- Informes para autoridades u organismos de control.
- Evaluación de riesgos laborales, industriales o regulatorios.
- Tratamiento de datos personales o confidenciales.

- Análisis contractual o jurídico sensible.
- Estos usos requerirán revisión reforzada.

17.4. Uso potencialmente alto riesgo AI Act

Si se pretendiera utilizar IA en ámbitos incluidos en el AI Act como alto riesgo, por ejemplo empleo, acceso a servicios esenciales, educación, crédito, seguros, biometría, infraestructuras críticas, cumplimiento de la ley, migración, justicia o procesos democráticos, se requerirá evaluación específica antes de cualquier uso.

Actualmente, SOLINGESA **no autoriza** el uso de IA para decisiones automatizadas en dichos ámbitos.

18. Procedimiento de aprobación de nuevos sistemas o usos de IA

Antes de utilizar una nueva herramienta de IA o un nuevo uso relevante, el Responsable de Cumplimiento IA deberá completar una revisión interna proporcionada.

En todo caso Solingesa establece un criterio previo de rechazo ético: Se rechazará o suspenderá cualquier uso de IA que, aunque sea técnicamente posible o productivo, pueda comprometer la dignidad de las personas, la verdad documental, la seguridad técnica, la justicia en la relación con clientes o colaboradores, o la responsabilidad profesional de SOLINGESA.

La revisión incluirá:

- a. Descripción de la herramienta.
- b. Proveedor.
- c. Finalidad prevista.
- d. Tipo de información tratada.
- e. Usuarios previstos.
- f. Proyectos afectados.
- g. Riesgos de confidencialidad.
- h. Riesgos de protección de datos.
- i. Riesgos técnicos.
- j. Riesgos de derechos fundamentales.
- k. Posibilidad de outputs incorrectos.
- l. Necesidad de supervisión humana.
- m. Condiciones contractuales del proveedor.
- n. Medidas de seguridad.
- o. Criterios de discernimiento ético:
 1. ¿Este uso mejora realmente la calidad, seguridad o fiabilidad del servicio?
 2. ¿Puede desplazar indebidamente el criterio de una persona competente?
 3. ¿Puede perjudicar a personas vulnerables o con menor capacidad de defensa?
 4. ¿Puede crear apariencia de verdad, evidencia o revisión que no existe?
 5. ¿Puede aumentar dependencia acrítica de herramientas tecnológicas?
 6. ¿Quién asume la responsabilidad humana final?
- p. Impacto humano y profesional:
 1. ¿El uso de IA afecta a personas, clientes, trabajadores, freelancers o terceros?
 2. ¿Puede generar dependencia excesiva de outputs automáticos?
 3. ¿Puede reducir la calidad del juicio profesional?
 4. ¿Puede crear una apariencia de revisión o evidencia inexistente?
 5. ¿Puede afectar a seguridad, dignidad, derechos o confianza del cliente?
 6. ¿Qué beneficio humano concreto aporta?
 7. ¿Qué riesgo humano o profesional introduce?
 8. ¿Qué medida de revisión humana se aplicará?
- q. Decisión de aprobación, rechazo o aprobación condicionada.

La aprobación podrá documentarse de forma simplificada mediante ficha interna, correo de aprobación o registro en el inventario de IA.

19. Uso de IA en proyectos de consultoría normativa

En proyectos de cumplimiento normativo, la IA podrá apoyar:

- a. Estructuración de políticas.
- b. Preparación de matrices de cumplimiento.
- c. Elaboración de checklists.
- d. Resumen de requisitos normativos.
- e. Preparación de borradores de informes.
- f. Identificación preliminar de brechas.
- g. Redacción de planes de acción.
- h. Preparación de materiales formativos.

No obstante:

- a. La interpretación normativa final será humana.
- b. Las obligaciones legales deberán verificarse contra fuentes oficiales.
- c. Las conclusiones de auditoría deberán basarse en evidencias reales.
- d. No se inventarán evidencias, controles, entrevistas o registros.
- e. Toda recomendación al cliente deberá ser revisada por el consultor responsable.

20. Uso de IA en proyectos de ingeniería, seguridad industrial, instalaciones industriales y máquinas

En proyectos técnicos, la IA podrá apoyar:

- a. Preparación de borradores de documentación.
- b. Estructuración de informes.
- c. Elaboración de checklists preliminares.
- d. Identificación inicial de normativa potencialmente aplicable.
- e. Redacción de textos explicativos.
- f. Preparación de tablas de requisitos.
- g. Revisión de coherencia documental.
- h. Preparación de listas de verificación para revisión humana.

Queda expresamente prohibido utilizar IA como fuente única o definitiva para:

- a. Cálculos de ingeniería.
- b. Dimensionamientos.
- c. Declaraciones de conformidad.
- d. Evaluaciones finales de seguridad de máquinas.
- e. Determinación definitiva de requisitos legales o técnicos.
- f. Validación de cumplimiento reglamentario.
- g. Diseño de medidas de seguridad sin revisión técnica.
- h. Selección definitiva de componentes críticos.
- i. Evaluación de riesgos que pueda afectar a la seguridad de personas.
- j. Informes finales destinados a organismos de control o autoridades.

Toda conclusión técnica deberá ser revisada por un profesional competente participante en el proyecto.

21. Uso de IA en relaciones con clientes

SOLINGESA podrá utilizar IA para preparar borradores de comunicaciones, propuestas, informes o documentos para clientes, siempre con revisión previa.

Cuando el uso de IA sea meramente auxiliar y el documento sea revisado y asumido por SOLINGESA, no será necesario informar al cliente en cada caso, salvo que:

- El contrato lo exija.
- Se utilicen datos del cliente en sistemas de IA.
- Se generen contenidos sintéticos que puedan inducir a error.
- Se publique contenido generado por IA sobre asuntos de interés público.
- El cliente haya prohibido expresamente el uso de IA.
- La naturaleza del encargo exija transparencia reforzada.

SOLINGESA incluye una cláusula de transparencia en ofertas y/o contratos indicando que SOLINGESA puede utilizar herramientas de IA como apoyo interno, siempre bajo revisión humana y sin cesión no autorizada de información confidencial.

22. Transparencia sobre contenidos generados por IA

Cuando SOLINGESA utilice IA para generar o manipular imágenes, audio o vídeo que puedan inducir razonablemente a pensar que son auténticos, informará de forma clara de su origen artificial.

Cuando se utilice IA para generar o manipular texto destinado a publicarse con el fin de informar al público sobre asuntos de interés público, se divulgará que el texto ha sido generado o manipulado artificialmente, salvo que haya sido sometido a revisión humana o control editorial y una persona física o jurídica asuma la responsabilidad editorial de la publicación. Esta regla se basa en las obligaciones de transparencia previstas en el artículo 50 del AI Act .

En la actividad ordinaria de SOLINGESA, los documentos de consultoría e ingeniería generados inicialmente con apoyo de IA y posteriormente revisados, corregidos y aprobados por profesionales humanos serán considerados documentos profesionales de la entidad, sin perjuicio de las obligaciones de transparencia que puedan derivarse del contrato, del contexto o de la normativa aplicable.

23. Alfabetización y formación en IA

SOLINGESA garantiza que las personas que utilicen IA en su nombre tengan un nivel suficiente de alfabetización en IA, teniendo en cuenta sus conocimientos técnicos, experiencia, formación, contexto de uso y personas o colectivos afectados. Esta obligación deriva del artículo 4 del AI Act .

La formación mínima incluirá:

- Qué es y qué no es un sistema de IA.
- Riesgos de errores, alucinaciones y sesgos.
- Confidencialidad y protección de datos.
- Uso permitido y prohibido.
- Revisión humana obligatoria.
- Uso correcto de ChatGPT, NotebookLM y agentes.
- Limitaciones en proyectos GRC.
- Limitaciones en proyectos de ingeniería y seguridad industrial.
- Reporte de incidentes.
- Responsabilidad profesional.

Los freelancers deberán recibir esta política o una versión resumida antes de participar en proyectos donde puedan utilizar IA.

SOLINGESA conservará evidencias razonables de formación, comunicación o aceptación de esta política.

24. Gestión de incidentes relacionados con IA

Se considerará incidente relacionado con IA cualquier evento que pueda afectar a la seguridad, confidencialidad, calidad, legalidad, derechos de terceros o fiabilidad profesional del trabajo realizado, como por ejemplo:

- a. Introducción indebida de información confidencial en una herramienta de IA.
- b. Uso de datos personales sin autorización.
- c. Output incorrecto incorporado a un borrador avanzado.
- d. Referencias legales o técnicas inexistentes.
- e. Fuga de información.
- f. Uso no autorizado por un freelancer.
- g. Generación de contenido discriminatorio, ofensivo o sesgado.
- h. Error técnico relevante en un agente de IA.
- i. Uso de IA fuera de la finalidad aprobada.
- j. Dependencia excesiva de outputs no verificados.
- k. Incidentes éticos:
 - 1. Output que presenta como cierta una evidencia no verificada.
 - 2. Output que contiene lenguaje deshumanizante, discriminatorio o que reduce personas a etiquetas.
 - 3. Uso de IA que elimina indebidamente la escucha directa al cliente o a personas afectadas.
 - 4. Output que recomienda medidas desproporcionadas para trabajadores, freelancers, pymes o terceros vulnerables.
 - 5. Uso de IA que genera apariencia de revisión profesional inexistente.
 - 6. Uso de IA que dificulta atribuir responsabilidad humana por una decisión o entregable.

Todo incidente deberá comunicarse al Responsable de Cumplimiento de IA o a Dirección.

La gestión del incidente se registrará en la Lista de Incidencias del Sistema de Gestión de SOLINGESA e incluirá:

- a. Registro del incidente.
- b. Evaluación del impacto.
- c. Evaluación del impacto ético: En incidentes de IA de impacto medio o alto se evaluará no solo el daño técnico, legal o contractual, sino también el impacto sobre confianza, verdad, dignidad, justicia, reputación y personas afectadas.
- d. Medidas inmediatas de contención.
- e. Revisión del trabajo afectado.
- f. Comunicación al cliente si procede.
- g. Comunicación al proveedor si procede.
- h. Comunicación al DPO o responsable de privacidad si hay datos personales.
- i. Suspensión del sistema si existe riesgo relevante.
- j. Acción correctiva.
- k. Cierre documentado.

Aunque actualmente no están autorizados en SOLINGESA, en caso de uso de sistemas de IA de alto riesgo, el AI Act exige que el responsable del despliegue vigile su funcionamiento, informe al proveedor y, en su caso, a la autoridad competente cuando detecte riesgos o incidentes graves, y suspenda el uso si procede .

25. Conservación de evidencias y trazabilidad

SOLINGESA conservará evidencias proporcionales al riesgo del uso de IA, aunque para usos de bajo riesgo bastará con el documento final revisado.

Para usos medios o altos, se conservará, cuando sea razonable:

- Versión inicial generada con apoyo de IA.
- Prompt o descripción de la tarea (siendo válido el historial de la propia plataforma IA).
- Fuentes utilizadas.
- Revisión humana realizada.
- Persona revisora.
- Fecha de revisión.
- Cambios relevantes.
- Versión final aprobada.

Para agentes de IA, se conservarán registros de configuración, finalidad, versiones relevantes, responsables, pruebas y cambios sustanciales.

El AI Act prevé la importancia de los registros para permitir trazabilidad, vigilancia del funcionamiento y detección de situaciones de riesgo en sistemas de alto riesgo. SOLINGESA adopta este enfoque como buena práctica proporcional incluso en usos que no sean de alto riesgo.

26. Proveedores de IA

Antes de utilizar herramientas de IA relevantes, la entidad evaluará de forma proporcional al riesgo:

- Identidad del proveedor.
- Condiciones de uso.
- Tratamiento de datos.
- Uso de datos para entrenamiento.
- Ubicación de datos.
- Medidas de seguridad.
- Posibilidad de control empresarial.
- Configuración de privacidad.
- Derechos de auditoría o información.
- Gestión de incidentes.
- Cambios de modelo o servicio.
- Garantías de confidencialidad.
- Posibilidad de eliminación de datos.

Cuando el proveedor ofrezca configuraciones empresariales, controles de privacidad, exclusión de entrenamiento o garantías reforzadas, SOLINGESA priorizará dichas opciones frente a cuentas personales o gratuitas.

27. Integración con el sistema de gestión de riesgos

La IA se integrará en el sistema de gestión de riesgos de la entidad.

Los riesgos de IA se evaluarán considerando:

- Probabilidad de error.
- Impacto técnico.
- Impacto jurídico.
- Impacto en seguridad industrial.
- Impacto en derechos de personas.
- Impacto en confidencialidad.

- g. Impacto reputacional.
- h. Impacto contractual.
- i. Dependencia del proveedor.
- j. Nivel de autonomía del sistema.
- k. Capacidad de revisión humana.
- l. Complejidad del proyecto.

El Responsable de Cumplimiento de IA informará a Dirección de los riesgos relevantes, incidentes y necesidades de mejora.

28. Control de freelancers y colaboradores externos

Antes de incorporarse a un proyecto, los freelancers y colaboradores externos deberán recibir instrucciones sobre el uso permitido de IA.

De forma general SOLINGESA requerirá a los freelancers y colaboradores externos:

- a. Declaración de uso o no uso de IA.
- b. Identificación de herramientas utilizadas.
- c. Compromiso de no introducir información confidencial en herramientas no autorizadas.
- d. Compromiso de revisión humana.
- e. Compromiso de eliminación de información al finalizar el proyecto.
- f. Aceptación expresa de esta política.

En proyectos sensibles, SOLINGESA podrá exigir además el registro de prompts o outputs relevantes del proyecto.

La infracción de esta política podrá dar lugar a la suspensión de la colaboración, rechazo de entregables, exigencia de correcciones, reclamación de daños o resolución contractual.

29. Control documental

Los documentos generados con apoyo de IA seguirán el mismo circuito de control documental que el resto de documentos profesionales en SOLINGESA.

El hecho de que un documento haya sido inicialmente asistido por IA no reduce los requisitos de calidad, revisión, responsabilidad ni control documental.

30. Medidas específicas para evitar errores técnicos y normativos

Dado que SOLINGESA presta servicios de cumplimiento normativo y de ingeniería, se aplicarán las siguientes medidas reforzadas:

- a. Toda referencia legal deberá verificarse en fuente oficial o base normativa fiable.
- b. Toda referencia a normas técnicas deberá comprobarse respecto a versión vigente, ámbito y aplicabilidad.
- c. Toda conclusión sobre seguridad industrial deberá revisarse por persona competente.
- d. Todo cálculo deberá realizarse o verificarse con herramienta adecuada y criterio técnico humano.
- e. Toda recomendación a cliente deberá adaptarse al caso concreto.
- f. La IA no se utilizará como sustituto de inspecciones, mediciones, verificaciones in situ, ensayos, cálculos reglamentarios o juicio técnico.
- g. No se generarán evidencias ficticias.
- h. No se asumirán hechos no verificados del cliente.
- i. No se utilizarán respuestas de IA como prueba de cumplimiento.

31. Evaluación periódica

Esta política se revisará:

- a. Al menos una vez al año.
- b. Cuando se incorporen nuevas herramientas de IA relevantes.
- c. Cuando se despliegan nuevos agentes.
- d. Cuando se produzca un incidente significativo.
- e. Cuando cambie la normativa aplicable.
- f. Cuando un cliente o contrato imponga requisitos específicos.
- g. Cuando se detecten desviaciones en el uso de IA.

La revisión será aprobada por Dirección.

32. Medidas disciplinarias y consecuencias del incumplimiento

El incumplimiento de esta política podrá dar lugar, según la gravedad y la relación existente, a:

- a. Advertencia interna.
- b. Retirada de acceso a herramientas de IA.
- c. Revisión obligatoria de trabajos.
- d. Formación adicional.
- e. Rechazo de entregables.
- f. Suspensión de colaboración.
- g. Resolución contractual.
- h. Comunicación al cliente si procede.
- i. Acciones legales en caso de daño, fuga de información o incumplimiento contractual.

33. Declaración corporativa de uso responsable de IA

SOLINGESA declara que utiliza la inteligencia artificial como herramienta de apoyo profesional, no como sustituto del conocimiento experto, la responsabilidad técnica, la revisión jurídica ni la validación humana.

SOLINGESA se compromete a:

- a. Usar IA de forma proporcionada y segura.
- b. Mantener control humano sobre los resultados.
- c. Proteger la información de clientes.
- d. Respetar la protección de datos personales.
- e. Evitar usos prohibidos o abusivos.
- f. Formar a las personas que utilicen IA en su nombre.
- g. Revisar los outputs antes de su uso profesional.
- h. Documentar los usos relevantes.
- i. Gestionar incidentes.
- j. Mejorar progresivamente su gobernanza de IA.

Mayo 2026

La Dirección