Grupo ENERGO-PRO

Política sobre el uso de la inteligencia artificial

2025

ENERGO-PRO

Política sobre el uso de la inteligencia artificial

Versión: 1.0 | **En vigor desde:** 01 de octubre de 2025 | **Propietario:** Comité de Gobernanza de la IA (AI Governance Committee o AIGC en inglés)

1. Objetivo y ámbito de aplicación

1.1. La presente Política sobre el uso de la inteligencia artificial (la **«Política»**) establece las normas vinculantes para el uso seguro, eficaz y responsable de las herramientas de inteligencia artificial (la **«IA»**) dentro de ENERGO – PRO a.s. (la **«Empresa»**) y sus filiales (en conjunto, denominadas el **«Grupo»**). A los efectos de la presente Política, el Grupo está compuesto por DK Holding Investments, s.r.o., único accionista de la Empresa, y todas sus filiales directas e indirectas.

1.2. Nuestro objetivo es fomentar la innovación y la productividad mediante la incorporación de las últimas tecnologías, garantizando al mismo tiempo el máximo nivel de protección de nuestros datos, de la propiedad intelectual, de los clientes y de nuestra reputación. La incorporación de la IA debe estar basada no solo en la innovación, sino también en un firme compromiso con la seguridad operativa, la seguridad pública y la confianza que la sociedad ha depositado en nosotros.

1.3. Nos comprometemos a garantizar que todo uso de la IA se ajuste a nuestros principios éticos fundamentales de integridad, respeto, transparencia y conducta ética. Es fundamental que todo proceso basado en la IA siga estando sometido a la supervisión y la responsabilidad humanas.

1.4. Esta Política se aplica a todos los empleados y empleadas, contratistas externos, consultores y proveedores que acceden a los sistemas de información del Grupo o que procesan datos del mismo (en conjunto, denominados el **«Personal»**). Es aplicable a todos los sistemas de IA utilizados dentro del Grupo, independientemente de si han sido desarrollados internamente, adquiridos a terceros o accesibles como servicio público.

2. Definiciones

A los efectos de la presente Política, se utilizarán las siguientes definiciones:

2.1. **Sistema de IA:** Un sistema de IA es, según el artículo 3(1) de la Ley de IA, tal y como se define a continuación. «Un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales». Esta definición se aplica independientemente de si el sistema de IA es una aplicación independiente o una función integrada en un paquete de software más amplio.

IA empresarial: Un sistema de IA aprobado que se rige por un contrato (incluido un Anexo de procesamiento de datos, tal y como se define a continuación) que garantiza la protección de nuestros datos. Dichos contratos deben prohibir explícitamente al proveedor utilizar los datos del Grupo para entrenar sus propios modelos o los de terceros.

Ejemplos: Microsoft Copilot para M365, DeepL Pro.

IA pública: Un sistema de IA aprobado, normalmente accesible públicamente en Internet, que no ofrece garantías contractuales de protección de datos y que puede utilizar entradas (instrucciones o «*prompts*») y salidas (respuestas) para entrenar o mejorar sus propios modelos o los de terceros.

Ejemplos: Versiones estándar de ChatGPT, Google Gemini, Google Translate.

2.2. **Clasificación de datos:** Todos los datos se clasifican en cuatro niveles:

Públicos (Nivel 1): Cualquier información que sea de dominio público de forma legal. Esto incluye tanto la información publicada oficialmente por el Grupo como la información procedente de fuentes públicas externas.

Ejemplos: Comunicados de prensa publicados, artículos académicos, artículos periodísticos, bases de datos públicas gubernamentales, información en sitios web de acceso público.

Internos (Nivel 2): Información no pública cuya divulgación no autorizada supondría un riesgo bajo.

Ejemplos: Actas de reuniones de equipo de carácter general (que no contengan datos personales ni secretos comerciales), guías internas, borradores de proyectos no confidenciales.

Confidencial (Nivel 3): Datos sensibles, cuya divulgación podría causar un daño moderado a grave al Grupo, a sus socios o a sus clientes.

Ejemplos: Planes financieros, estrategias comerciales, resultados financieros no auditados, contratos anonimizados.

Estrictamente confidencial (Nivel 4): Los datos más sensibles, protegidos por leyes o contratos, cuya divulgación no autorizada podría ocasionar graves daños legales, financieros o para la reputación.

Ejemplos: Datos personales según la definición del RGPD (tal y como se define a continuación), por ejemplo, registros de empleados o clientes, secretos comerciales, información sensible sobre precios, información protegida por un acuerdo de confidencialidad (NDA), conocimientos técnicos, inicios de sesión y contraseñas del sistema, código fuente propietario, datos operativos de infraestructuras críticas (por ejemplo, sistemas SCADA), evaluaciones detalladas de la vulnerabilidad de la red o esquemas de unidades de generación de energía.

2.3. **Anexo de procesamiento de datos (DPA):** Contrato legalmente vinculante celebrado entre un responsable del tratamiento de datos y un encargado del tratamiento de datos, de conformidad con el artículo 28 del RGPD. Regula el tratamiento de datos personales por parte del encargado del tratamiento en nombre del responsable. Es un requisito obligatorio en virtud del RGPD siempre que un responsable del tratamiento contrate a un encargado del tratamiento para que gestione datos personales.

2.4. **Ultrasuplantación:** Un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos.

2.5. **Alucinación:** Fenómeno en el que un modelo de IA genera resultados sin sentido, incorrectos en cuanto a los hechos o totalmente inventados, a pesar de presentarlos con confianza y soltura.

2.6. **Instrucción (*prompt*):** Cualquier entrada, como una pregunta, una indicación o un conjunto de datos, proporcionada por un usuario a un sistema de IA para obtener una salida.

3. Funciones, responsabilidades y gobernanza

Comité de Gobernanza de la IA (AI Governance Committee o AIGC en inglés): Un equipo multidisciplinar compuesto por representantes de altos cargos, del departamento legal, de RR. HH. y otros departamentos clave. Se encarga de aprobar la estrategia de IA y la presente Política, así como de mantener el Registro.

Navegador de IA: El principal punto de contacto para obtener orientación y asesoramiento sobre cuestiones relacionadas con la IA. Esta función proporciona asesoramiento proactivo, presta apoyo al AIGC y ayuda al personal con las consultas relacionadas con la IA.

Propietario del Sistema de IA: A menos que el Comité de Gobernanza de IA (AIGC) determine lo contrario, el Navegador de IA actuará como propietario del sistema de IA para cada sistema de IA aprobado. El propietario del Sistema de IA es responsable de:

1. garantizar que el Sistema de IA se utilice únicamente para los fines aprobados y dentro de los parámetros autorizados;
2. actuar como contacto comercial principal para las auditorías y las valoraciones de rendimiento;
3. gestionar el acceso de los usuarios en coordinación con el departamento de TI; e
4. informar de cualquier problema o incidente significativo relacionado con el rendimiento al navegador de IA para que este lo eleve al AIGC.

Personal: Todos los miembros del Personal son responsables de comprender y cumplir esta Política.

4. Principios básicos del uso de la IA

Todo uso de la IA dentro del Grupo deberá cumplir los siguientes principios básicos:

4.1. ***Human in the Loop*** **(supervisión humana obligatoria):** La IA es una herramienta de apoyo, no un sistema autónomo de toma de decisiones. Un sistema de IA puede ayudar y servir de apoyo a las capacidades humanas, pero no sustituye el juicio y la responsabilidad del ser humano. Todos los resultados generados por la IA, especialmente aquellos con posibles consecuencias legales o financieras, deben someterse a una revisión crítica, verificarse y ser aprobados por una persona cualificada y responsable antes de su uso. El nivel de escrutinio deberá ser proporcional al riesgo de la decisión (por ejemplo, verificar un solo dato en un informe requiere menos escrutinio que aprobar un programa de mantenimiento de red generado por IA).

4.2. **Responsabilidad:** La responsabilidad última de cualquier decisión o acción basada en los resultados generados por la IA recae en la persona que la utiliza, no en el propio Sistema de IA. El Personal debe ser consciente de la posibilidad de que un Sistema de IA pueda producir «alucinaciones» y deberá verificar siempre la información importante a partir de una fuente independiente y fiable.

4.3. **Transparencia:** Cuando un Sistema de IA esté diseñado para interactuar directamente con personas físicas (por ejemplo, a través de un chatbot), se informará a dichas personas de que están interactuando con un Sistema de IA. El Personal que genere o manipule contenidos de imagen, audio o vídeo que aparenten ser auténticos (desde ilustraciones generadas por IA para materiales de marketing hasta ultrasuplantaciones o *deepfakes*) deberá indicar de forma clara y visible que

el contenido ha sido generado o manipulado artificialmente, tal y como se detalla en la Sección 6.3(iii).

4.4. **No discriminación y equidad:** Los Sistemas de IA se utilizarán de forma que se evite crear o reforzar prejuicios injustos o discriminación contra personas o grupos en función de características protegidas (por ejemplo, por su edad, género u origen étnico).

4.5. **Seguridad y privacidad desde el diseño:** La protección y la seguridad de los datos son fundamentales. Todos los proyectos de IA, desde la adquisición hasta la implementación y la posible eliminación, deberán en todo momento respetar los principios de privacidad y seguridad.

5. Legislación y políticas aplicables

5.1. Marco jurídico y normativo

5.2. El desarrollo, la adquisición y el uso de Sistemas de IA por parte del Grupo se rigen por un marco de leyes y normas internacionales aplicables. Todo el Personal está obligado a cumplir con las últimas versiones de los siguientes documentos, sin limitación:

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (**«Ley de IA»**).

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización (**«Reglamento de Datos»**).

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (**«Directiva SRI 2»**).

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital (**«Directiva sobre derechos de autor»**).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (**«Reglamento general de protección de datos»**).

ISO/IEC 42001:2023 – Tecnología de la información — Inteligencia artificial — Sistema de gestión.

Toda la legislación nacional aplicable en las jurisdicciones en las que opera el Grupo, incluyendo, entre otras, las leyes que regulan el derecho laboral, la propiedad intelectual y la responsabilidad civil.

5.3. Relación con otras políticas internas

5.4. Esta Política complementa y debe leerse junto con las demás políticas vinculantes del Grupo. El Personal también deberá asegurarse de que el uso que haga de los Sistemas de IA cumpla con todas las demás políticas internas pertinentes, entre las que se incluyen, entre otras:

- El Código de Conducta
- La Política de Derechos Humanos

- La Política de Recursos Humanos
- La Política de Seguridad
- Las Políticas de Protección de Datos (Internas y Externas)
- Plan de gestión de contratistas y subcontratistas

5.5. En caso de discrepancia entre esta Política y otra política interna, se aplicará la disposición más restrictiva. El caso deberá remitirse sin demora al Navegador de IA para que el AIGC lo esclarezca.

6. Uso aceptable y prohibido

6.1. La regla de oro: Vincular los datos al Sistema de IA adecuado.

El principio más importante es garantizar que los datos solo sean procesados por un sistema de IA con el nivel de seguridad correspondiente. El incumplimiento de este principio constituye una infracción grave de la presente Política.

Clasificación de datos	**IA pública**	**IA empresarial**
Nivel 1: Público	Permitido	Permitido
Nivel 2: Interno	Permitido	Permitido
Nivel 3: Confidencial	Permitido con restricciones	Permitido
Nivel 4: Estrictamente confidencial	Prohibido	Solo se permite con la aprobación del AIGC, sujeto a una Evaluación de impacto en la protección de datos (DPIA) obligatoria y una evaluación de riesgos de seguridad informática.

6.2. Sistemas de IA aprobados

Regla general

El Personal solo puede utilizar los Sistemas de IA que figuran en el «Registro de Sistemas de IA aprobados» oficial (el **«Registro»**). Queda estrictamente prohibido el uso de cualquier Sistema de IA que no figure en el Registro.

A efectos de referencia, se adjunta como Apéndice A una lista de los Sistemas de IA aprobados a la fecha de entrada en vigor de la presente Política. El AIGC mantiene y actualiza periódicamente la versión oficial y vigente del Registro, que está disponible en el SharePoint de M365 del Grupo.

Uso de Sistemas de IA de riesgo mínimo

Sin perjuicio de lo dispuesto en la cláusula anterior, el personal podrá utilizar un Sistema de IA que no figure en el Registro, siempre que dicho sistema reúna los requisitos para ser considerado un «Sistema de IA de riesgo mínimo» de conformidad con la clasificación establecida en la Sección 8 de la presente Política. La persona que tenga la intención de utilizar el sistema será la única responsable de su correcta evaluación y clasificación como Sistema de IA de riesgo mínimo.

La persona que haga uso de esta excepción deberá notificar al Navegador de IA el uso de dicho Sistema de IA sin demora injustificada por correo electrónico. El uso de cualquier sistema de este tipo deberá cumplir en todo momento con la presente Política y con todas las demás políticas del Grupo, incluidas, entre otras, las relativas a la protección de datos (RGPD), la seguridad de la información y la seguridad informática.

Uso de Sistemas Públicos de IA para Datos de Nivel 3 (Confidenciales)

El procesamiento de Datos de Nivel 3 (Confidenciales) utilizando Sistemas Públicos de IA está estrictamente prohibido, excepto cuando se cumplan todas las condiciones siguientes:

(i) El Sistema Público de IA utilizado debe estar aprobado para este fin en el Registro y utilizarse de acuerdo con las condiciones especificadas en el mismo. Según la última revisión de esta Política, los métodos requeridos son:

- **Para Adobe Acrobat AI Assistant:** Aprobado para su uso sin necesidad de configuraciones de privacidad adicionales. Su arquitectura de privacidad desde el diseño garantiza que los datos de los usuarios estén aislados y no se utilicen para el entrenamiento de modelos.
- **Para ChatGPT:** Se debe utilizar la función «Chat temporal».
- **Para Google Gemini:** Se debe desactivar la configuración «Actividad de las aplicaciones Gemini».
- **Para NotebookLM:** Aprobado para su uso sin necesidad de configuraciones de privacidad adicionales. Su arquitectura de privacidad desde el diseño garantiza que los datos de los usuarios estén aislados y no se utilicen para el entrenamiento de modelos.

(ii) Los términos de uso del Sistema de IA Público garantizan que las entradas de los usuarios (instrucciones o «*prompts*») y las salidas del sistema (respuestas) no se utilizarán con fines de entrenamiento o mejora de los modelos de IA del proveedor o de terceros.

(iii) Todas las entradas y salidas de la sesión no deberán conservarse en el historial de conversaciones permanente del usuario y deberán eliminarse automáticamente por parte del proveedor. Los usuarios deben aceptar el periodo de conservación del proveedor por motivos de seguridad y operativos, que actualmente es:

- Hasta 30 días para el «chat temporal» de ChatGPT.
- Hasta 72 horas (3 días) para Google Gemini con la «actividad» desactivada.

Es responsabilidad del usuario seleccionar la función correcta y comprender el período de retención de datos aplicable antes de enviar cualquier dato de Nivel 3 (Confidencial) al Sistema Público de IA.

6.3. **Actividades prohibidas**

Queda estrictamente prohibido el uso de la IA para los siguientes fines:

(i) Cualquier actividad que contravenga la legislación aplicable, en particular las prácticas prohibidas definidas en el artículo 5 de la Ley de IA, o que viole el Código de Conducta del Grupo o cualquier otra política interna aplicable.

(ii) Introducir datos de Nivel 4 en cualquier sistema público de IA o introducir datos de Nivel 3 en cualquier sistema público de IA sin cumplir las restricciones establecidas en la Sección 6.2.

(iii) Se prohíbe la creación o difusión de ultrasuplantaciones o *deepfakes* y otros medios sintéticos generados por IA con fines maliciosos, fraudulentos o engañosos, o que tengan la intención, o sea razonablemente probable, que hagan creer a cualquier persona que el contenido es auténtico.

Se permite la creación y el uso de imágenes, audio, vídeo o productos similares generados o manipulados por IA con fines ilustrativos, educativos, artísticos, formativos u otros fines comerciales legítimos, siempre que:

a. el contenido se revele claramente al público destinatario como generado o manipulado por IA (por ejemplo, mediante una etiqueta en el propio contenido, un pie de foto, una marca de agua, un aviso en los metadatos, una nota al pie de la diapositiva u otra información adjunta visible al utilizarlo); y

b. el contenido no se presente como un registro de hechos reales sobre personas, objetos, lugares, temas o acontecimientos del mundo real.

(iv) La creación y el uso de avatares realistas con apariencia humana con el fin de suplantar la identidad o interactuar de forma engañosa con empleados, clientes o el público.

(v) Tomar decisiones definitivas y automatizadas sobre personas (por ejemplo, en la contratación, las evaluaciones de rendimiento o el despido) sin que una persona real lleve a cabo una supervisión y revisión significativas.

(vi) Cualquier intento de eludir las medidas de seguridad o las limitaciones de uso de un sistema de IA aprobado.

6.4. **Actividades recomendadas**

Aceptamos y fomentamos el uso de Sistemas de IA aprobados. La siguiente lista es ilustrativa, no exhaustiva, y proporciona ejemplos de usos que pueden resultar útiles:

(i) Ayudar en la redacción de correos electrónicos, informes o presentaciones.

(ii) Traducir documentos (sujeto a las normas de clasificación de datos).

(iii) Resumir documentos y analizar datos para hallar nuevas ideas.

(iv) Hacer lluvias de ideas o elaborar borradores conceptuales.

(v) Automatización de tareas repetitivas (por ejemplo, obtención de fórmulas en hojas de cálculo).

(vi) Redacción inicial de informes técnicos sobre tendencias del mercado energético basados en datos públicos, con todos los datos y cifras verificados posteriormente por un experto en la materia.

Para cualquier posible caso de uso no especificado anteriormente, el Personal deberá actuar con la debida precaución y asegurarse de que el uso propuesto cumpla plenamente con los principios fundamentales de esta Política y con todas las demás normativas legales e internas aplicables. En todo momento deberá hacerse uso de un criterio profesional sensato. Si existe alguna incertidumbre sobre la permisibilidad o el cumplimiento de un uso propuesto, es obligatorio consultarlo con el Navegador de IA antes de proceder.

7. Adquisición y aprobación de Sistemas de IA

7.1. Todo nuevo Sistema de IA debe someterse al siguiente proceso de aprobación antes de poder utilizarse:

(i) **Presentación de la solicitud:** La persona deberá presentar una solicitud utilizando el formulario oficial (véase el Apéndice B).

(ii) **Evaluación inicial:** El Navegador de IA revisará la solicitud en función de los criterios básicos.

(iii) **Evaluación de riesgos:** El AIGC llevará a cabo una evaluación detallada de los riesgos (véase la Sección 8).

(iv) **Decisión:** El AIGC deberá aprobar o rechazar el Sistema de IA, o aprobarlo con limitaciones específicas.

(v) **Registro:** El Sistema de IA aprobado deberá inscribirse en el Registro.

8. Evaluación de riesgos y clasificación del Sistema

8.1. Cada Sistema de IA deberá clasificarse según el modelo de riesgo de cuatro niveles de la Ley de IA:

Riesgo inaceptable: Sistemas de IA prohibidos por la ley y por la presente Política (por ejemplo, puntuación social o «*social scoring*»).

Riesgo alto: Un Sistema de IA que cumple los criterios establecidos en el artículo 6 de la Ley de IA, incluidos, entre otros, los Sistemas de IA que podrían afectar significativamente a la salud, la seguridad o los derechos fundamentales de las personas (por ejemplo, un Sistema de IA utilizado en la gestión de infraestructuras fundamentales o un Sistema de IA utilizado para filtrar solicitudes de empleo). Estos sistemas están sujetos a normas más estrictas, como el registro obligatorio, la realización de rigurosas pruebas y la supervisión continua.

Riesgo limitado: Esta categoría abarca los Sistemas de IA que plantean riesgos específicos de manipulación o engaño y, por lo tanto, están sujetos a obligaciones específicas de transparencia. Estas obligaciones varían en función del tipo de Sistema de IA y su uso:

- **Sistemas de interacción directa (por ejemplo, chatbots):** Cuando se utilizan sistemas diseñados para la interacción directa con personas, como los chatbots para el soporte interno de RR. HH. o el servicio de atención al cliente externo, se debe informar claramente a los usuarios de que están comunicándose con una IA.

- **Medios sintéticos (imágenes, audio, vídeo):** Los Sistemas de IA utilizados para generar o manipular imágenes, audio o contenido de vídeo realistas (por ejemplo, *deepfakes*) deben etiquetar claramente sus resultados como «generados por IA» o «manipulados artificialmente», a menos que el contenido sea obviamente artístico o creativo y no pretenda representar la realidad.
- **IA de propósito general (GPAI) para la generación de texto:** Los modelos subyacentes de herramientas como ChatGPT, Gemini y Copilot se consideran IA de propósito general (GPAI) y están sujetos a los requisitos de transparencia de sus proveedores. Para nuestros fines como usuarios (implementadores), cuando estas herramientas se utilizan para funciones de asistencia, como resumir textos, redactar correos electrónicos o generar ideas, el texto generado no necesita etiquetarse como generado por IA, siempre que se someta a una revisión humana significativa y a un control editorial antes de su uso. En estos casos, la IA funciona como un asistente, y la responsabilidad final del contenido recae íntegramente en el Personal.

Riesgo mínimo: Esta categoría se aplica a los Sistemas de IA que presentan un riesgo insignificante para los derechos, las libertades o la seguridad de las personas. Un sistema se clasificará como de riesgo mínimo solo si cumple todas las condiciones siguientes:

- No toma decisiones ni determina cuestiones que afecten a los derechos legales de las personas físicas;
- No procesa datos personales sensibles; y
- Su posible fallo o resultado erróneo no tendría un impacto significativo en la seguridad.

Un Sistema de IA puede reclasificarse en una categoría de riesgo superior (Riesgo limitado o alto) si se modifica su finalidad prevista para incluir el tratamiento de datos personales, biométricos o críticos para la seguridad. Aunque no está específicamente regulado por la Ley de IA, el uso de cualquier Sistema de IA de riesgo mínimo debe ajustarse a los principios generales establecidos en esta Política.

Ejemplo de Sistemas de IA de riesgo mínimo: Filtros de spam basados en IA, modelos de predicción meteorológica, sistemas de gestión de inventario que utilizan IA simple para la predicción de la demanda, asistentes de revisión gramatical y ortográfica integrados en procesadores de texto o clientes de correo electrónico, herramientas de traducción automática (por ejemplo, traducción automática de sitios web) utilizadas para una comprensión rápida (la traducción de textos disponibles públicamente solo supone un riesgo insignificante cuando no hay datos sensibles involucrados).

9. Protección de datos, propiedad intelectual y seguridad

Privacidad desde el diseño: El principio de protección de datos desde el diseño y por defecto se integrará en todos los proyectos de IA desde el principio.

Evaluación de impacto en la protección de datos (DPIA): Es obligatorio realizar una evaluación de impacto en la protección de datos o DPIA (véase el Apéndice C) para cualquier Sistema de IA que pueda suponer un riesgo alto para los derechos y libertades de las personas físicas.

Propiedad intelectual del contenido generado por IA: El Personal debe ser consciente de que la situación jurídica del contenido generado por IA es compleja y está en constante evolución. A

menos que se indique explícitamente lo contrario en los términos de un Sistema de IA aprobado, los resultados generados por IA pueden no estar sujetos a la protección de los derechos de autor o pueden estar sujetos a derechos de terceros. Todo el contenido creado utilizando IA en el desempeño de las funciones laborales se considera producto del trabajo del Grupo, sin embargo, el Personal no debe asumir que el Grupo posee los derechos de autor exclusivos. El uso de contenido generado por IA en materiales destinados al público o productos comerciales requiere una consulta previa con el Navegador de IA.

Protección de la información confidencial y la propiedad intelectual: El Personal debe actuar con extrema precaución para proteger la información confidencial del Grupo. Esto incluye, entre otros, secretos comerciales, información sensible sobre precios, conocimientos técnicos, información protegida por acuerdos de confidencialidad, derechos de autor y derechos de propiedad industrial. Tal y como se estipula en la Sección 6, dicha información nunca debe introducirse en un Sistema de IA Público.

Seguridad: Todos los sistemas de IA deben cumplir con nuestras normas de ciberseguridad establecidas.

10. Supervisión, informes y métricas

Supervisaremos el rendimiento, la precisión y la seguridad de nuestros Sistemas de IA.

En el caso de los sistemas de IA de Riesgo alto, es obligatorio presentar informes periódicos de rendimiento al AIGC.

Mediremos no solo los parámetros técnicos, sino también el valor comercial generado (por ejemplo, el tiempo ahorrado, las mejoras en los procesos).

11. Respuesta a incidentes y gestión de cambios

Incidentes: Cualquier incidente relacionado con un Sistema de IA (por ejemplo, una violación de datos, un resultado erróneo con un impacto significativo, un caso sospechoso de discriminación) debe ser reportado inmediatamente al Navegador de IA.

Cambios: Cualquier cambio significativo en un Sistema de IA (por ejemplo, una nueva versión, un cambio en su uso previsto) requiere una nueva evaluación de riesgos por parte del AIGC. Entre los cambios significativos se incluyen, entre otros: un cambio en la finalidad prevista del sistema, la implementación de una nueva versión importante de su modelo subyacente o una alteración sustancial de sus entradas o salidas de datos.

12. Formación del Personal y conocimientos básicos sobre IA

Formación obligatoria: Todo el Personal está obligado a recibir una formación inicial sobre el uso de la IA, abarcando la presente política, la seguridad de los datos, la concienciación sobre los riesgos (incluidos la discriminación y las alucinaciones) y el uso adecuado de los Sistemas de IA aprobados. Se realizará formación adicional según sea necesario, por ejemplo, tras actualizaciones significativas en la legislación o en nuestros sistemas de IA.

Formación avanzada: Se impartirá al Personal que trabaje de forma intensiva con la IA, centrándose en las funciones avanzadas y de activación eficaz de los Sistemas de IA aprobados.

Portal de IA: Un sitio interno de SharePoint que sirve como centro de recursos para todos los asuntos relacionados con la IA. Contiene el registro, guías de usuario, materiales de formación, políticas e información de contacto.

13. Gestión de terceros y proveedores

Antes de la adquisición de cualquier Sistema de IA empresarial, el proveedor deberá someterse a un exhaustivo proceso de diligencia debida. Esta evaluación analizará la postura de seguridad del proveedor, sus certificaciones de cumplimiento, su reputación y la transparencia de sus modelos de IA.

Requisito no negociable: Debemos tener un Anexo de procesamiento de datos (DPA) firmado con cualquier proveedor cuyo Sistema de IA procese nuestros datos no públicos (Niveles 2-4). Este DPA deberá prohibir al proveedor utilizar nuestros datos para entrenar sus modelos.

14. Revisión y auditoría de la Política

La presente Política es un documento vivo. El AIGC la revisará y actualizará al menos una vez al año, o con mayor frecuencia en caso de cambios tecnológicos o legislativos significativos. La Auditoría Interna verificará periódicamente el cumplimiento de esta Política.

15. Sanciones por incumplimiento

El incumplimiento de esta Política se considerará una infracción grave de las obligaciones laborales y podrá ser objeto de medidas disciplinarias de conformidad con el reglamento interno y la legislación aplicable, entre las que se incluyen el despido o la rescisión del contrato.

16. Apéndices (disponibles en el portal de IA)

- **Apéndice A:** Registro de los Sistemas de IA aprobados
- **Apéndice B:** Formulario de solicitud para la aprobación de un nuevo Sistema de IA
- **Apéndice C:** Plantilla para la Evaluación de impacto sobre la protección de datos (DPIA)
- **Apéndice D:** Detalles de contacto

Apéndice A: Registro de los Sistemas de IA aprobados

Última actualización: 01 de octubre de 2025 | **A cargo de:** Navegador de IA

Este registro proporciona una lista definitiva de los Sistemas de IA que han sido evaluados y aprobados para su uso dentro del Grupo. Cualquier Sistema de IA que no figure en esta lista se considera prohibido, a menos que haya sido aprobado explícitamente por el Comité de Gobernanza de la IA (AIGC).

Nombre del Sistema de IA	**Categoría**	**Clasificación del riesgo**	**Ejemplos de casos de uso aprobados**	**Clasificación máxima de datos permitida**	**Estado**
Asistente de IA de Acrobat	IA pública	Riesgo limitado	El Asistente de IA analiza rápidamente sus documentos para extraer información clave, identificar patrones y responder preguntas complejas, con todas las respuestas directamente vinculadas a las fuentes dentro del texto.	Nivel 3 (Confidencial) con restricciones	**Aprobado**
Asistente de IA de Celsia	IA empresarial	Riesgo limitado	Filtrar información relevante de documentos internos del Grupo, elaborar resúmenes concisos y responder a preguntas relacionadas con ESG.	Nivel 4 (Estrictamente confidencial)	**Aprobado**
ChatGPT (versiones Free/Plus)	IA pública	Riesgo limitado	Redactar correos electrónicos, resumir documentos, aportar ideas o traducir textos.	Nivel 3 (Confidencial) con restricciones	**Aprobado**
DeepL Pro	IA empresarial	Riesgo limitado	Traducción de documentos, incluidos aquellos que contienen información estrictamente confidencial.	Nivel 4 (Estrictamente confidencial)	**Aprobado**
Google Gemini	IA pública	Riesgo limitado	Redactar correos electrónicos, resumir	Nivel 3 (Confidencial)	**Aprobado**

			documentos, aportar ideas o traducir textos.	con restricciones	
Tradutor de Google	IA pública	Riesgo limitado	Únicamente traducción de información pública no sensible.	Nivel 2 (Interno)	**Aprobado**
Microsoft Copilot para M365	IA empresarial	Riesgo limitado	Redacción de correos electrónicos, resumen de documentos y reuniones, análisis de datos en aplicaciones de Microsoft 365.	Nivel 4 (Estrictamente confidencial)	**Aprobado**
NotebookLM	IA pública	Riesgo limitado	Convertir documentos específicos de proyectos, investigaciones y notas de reuniones en un experto interactivo al que se le pueden solicitar resúmenes, respuestas objetivas y nuevas perspectivas basadas únicamente en fuentes privadas.	Nivel 3 (Confidencial)	**Aprobado**

Apéndice B: Formulario de solicitud para la aprobación de un nuevo Sistema de IA

Le rogamos que rellene este formulario íntegramente y lo envíe al Navegador de IA para cualquier nuevo sistema de IA que desee utilizar para fines del Grupo.

Sección 1: Información del solicitante

- **Nombre completo:**
- **Departamento:**
- **Cargo:**
- **Fecha de la solicitud:**

Sección 2: Detalles del Sistema de IA

- **Nombre del Sistema de IA:**
- **Proveedor:**
- **Enlace al sitio web del Sistema:**
- **Enlace a la Política de privacidad/Condiciones del servicio:**

Sección 3: Uso previsto:

- **Finalidad comercial:** (Por favor, describa el problema relacionado con la empresa que está tratando de resolver y cómo le ayudará este Sistema de IA. ¿Cuál es el objetivo principal?)
- **Tareas específicas:** (Enumere las tareas específicas que pretende realizar con este Sistema de IA, por ejemplo, «traducir contratos legales», «generar textos de marketing», «analizar los comentarios de los clientes»).

Sección 4: Uso de datos

- **¿Cuál es el nivel más alto de clasificación de datos que pretende procesar con este Sistema de IA?** (Consulte la Sección 2.2 de la Política de IA)
    - [ ] Nivel 1: Público
    - [ ] Nivel 2: Interno
    - [ ] Nivel 3: Confidencial
    - [ ] Nivel 4: Estrictamente confidencial
- **¿El Sistema de IA procesará algún Dato Personal tal y como lo define el RGPD?**
    - [ ] Sí

- [ ] No

- **¿Se utilizará el Sistema de IA para tomar decisiones que tengan un efecto significativo en las personas (por ejemplo, contratación, evaluación del rendimiento)?**
  - [ ] Sí
  - [ ] No

Sección 5: Evaluación inicial de riesgos

- **¿Proporciona el proveedor un Anexo de procesamiento de datos (DPA) que prohíba explícitamente el uso de nuestros datos para su propio entrenamiento de modelos o el de terceros?**
  - [ ] Sí
  - [ ] No
  - [ ] no lo sé
- **Según su conocimiento, ¿existe alguna vulnerabilidad de seguridad conocida o algún problema ético asociado a este Sistema de IA?** (Si la respuesta es afirmativa, por favor, especifique).

Para uso interno exclusivo del AIGC

- **ID de la solicitud:**
- **Fecha de recepción:**
- **Evaluación del Navegador de IA:** Completo/Incompleto
- **Decisión del AIGC:** Aprobado/ Rechazado/Aprobado con limitaciones
- **Fecha de la decisión:**
- **Justificación/Limitaciones:**

Apéndice C: Plantilla para la Evaluación de impacto sobre la protección de datos (DPIA) para un Sistema de IA

Esta plantilla debe completarse para cualquier Sistema de IA clasificado como de **Riesgo alto** o cualquier Sistema de IA que procese datos de **Nivel 4 (Estrictamente confidencial)**, especialmente cuando se procesan datos personales a gran escala o cuando es probable que el procesamiento suponga un riesgo alto para los derechos y libertades de las personas físicas.

Referencia DPIA: [Identificador único]

Nombre del Sistema de IA: [Nombre del Sistema de IA]

Propietario del Sistema de IA: [Nombre]

Fecha de la evaluación: [Fecha]

Parte 1: Descripción del tratamiento

- **Naturaleza y alcance del tratamiento:** Describa la funcionalidad del Sistema de IA, la naturaleza de los datos que tratará, el volumen de datos y las categorías de los sujetos de datos implicados.
- **Finalidad del tratamiento:** ¿Cuáles son los resultados y beneficios previstos para el Grupo, los clientes o los empleados?
- **Contexto del tratamiento:** Describa la relación con los sujetos de datos y sus expectativas razonables. Detalle las fuentes de datos y cualquier flujo de datos a terceros.

Parte 2: Evaluación de la necesidad y la proporcionalidad

- **Base jurídica:** ¿Cuál es la base jurídica para el tratamiento de datos personales en virtud del artículo 6 del RGPD?
- **Limitación de la finalidad:** ¿Se tratan los datos estrictamente para los fines especificados, explícitos y legítimos?
- **Minimización de datos:** ¿Son los datos tratados adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan?

Parte 3: Evaluación de riesgos

- **Riesgos para los derechos y libertades de los sujetos de datos:** Identifique los riesgos potenciales, tales como:
    - Acceso no autorizado o violación de datos.
    - Resultados poco exactos que conducen a decisiones incorrectas.

- Sesgo discriminatorio en los resultados (por ejemplo, en la contratación o en la calificación crediticia).
- Falta de transparencia o explicabilidad en las decisiones basadas en la IA.
- Reidentificación de datos anonimizados o seudonimizados.

- **Probabilidad y gravedad:** Para cada riesgo identificado, evalúe su probabilidad (baja/media/alta) y la gravedad potencial de su impacto.

Parte 4: Medidas previstas para mitigar los riesgos

- **Medidas técnicas:** Describa los controles de seguridad implantados (por ejemplo, cifrado, controles de acceso, seudonimización).
- **Medidas organizativas:** Describa los controles de procedimiento (por ejemplo, supervisión humana, auditorías periódicas, formación del personal, DPA de los proveedores).
- **Mitigación de sesgos:** Describa las medidas adoptadas para comprobar y mitigar los sesgos algorítmicos.
- **Medidas de transparencia:** ¿Cómo se informará a los interesados sobre el uso del sistema de IA y sus derechos?

Parte 5: Consulta y aprobación

- **Consulta con el delegado de protección de datos:** Registre el asesoramiento proporcionado por el Responsable de Protección de Datos.
- **Decisión del AIGC:**
  - [ ] Continuar con el procesamiento.
  - [ ] Continuar con el procesamiento sujeto a la implementación de medidas adicionales.
  - [ ] No continuar con el procesamiento.
  - [ ] Consultar con la Autoridad Supervisora.

Firma:

- **Propietario del Sistema de IA:** _____
- **Responsable de Protección de Datos:** _____
- **Presidente del AIGC:** _____

Apéndice D: Detalles de contacto

Para cualquier consulta relacionada con esta Política o con el uso de la IA dentro del Grupo, póngase en contacto con las personas pertinentes.

Principal persona de contacto

- **Navegador de IA**
  - **Nombre:** Tomáš Brandejský
  - **Correo electrónico:** t.brandejsky@energo-pro.com
  - **Responsabilidades:** Atención directa para el Personal, coordinación de la formación y gestión del proceso de aprobación del Sistema de IA.

Gobernanza y escalamiento

- **Comité de Gobernanza de la IA (AI Governance Committee o AIGC en inglés)**
  - **Presidente:** Jakub Fajfr
  - **Consejero general:** Christian Blatchford
  - **Responsable de Protección de Datos (DPO):** Marina Radeva
  - **Jefe de RR. HH.:** Nikola Šugra
  - **Correo electrónico:** AIGC@energo-pro.com
  - **Responsabilidades:** Supervisión estratégica, aprobación y actualización periódica del Registro de Sistemas de IA aprobados, aprobación de la Política de IA, gestión de riesgos y aprobación final de los Sistemas de IA de Riesgo Alto.