PROTOCOLO DE USO DE HERRAMIENTAS DE IA

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**RESPONSABLE**	**OBSERVACIONES**
1.0	19/06/2025	Compliance penal	Delimitación y contenido de la política.
	24/06/2025	Consejo de Administración	Aprobación
	19/12/2025	Compliance penal	Modificación del ámbito de aplicación
	27/03/2026	Compliance Penal	Modificación cuestiones Protección de Datos

ÍNDICE

I.- OBJETO

Este protocolo establece las directrices para el uso responsable, legal y ético de los sistemas de Inteligencia Artificial (IA) dentro de Grupo Fedola, en cumplimiento con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, con el fin de asegurar su utilización de forma ética, legal, segura, transparente y alineada con los valores y objetivos corporativos.

II.- ÁMBITO DE APLICACIÓN

Esta política es de aplicación en todas las sociedades autónomas e independientes entre sí (existentes o que pudieran existir en el futuro) que forman parte del grupo mercantil "Grupo Fedola".

A efectos de esta política, se entenderá por Grupo Fedola o Grupo, todas las sociedades independientes que lo integran a las que le será de aplicación: GRUPO FEDOLA, S.L.; PREFABRICADOS TEIDE, S.L.; FERRETERIA HERMANOS LÓPEZ ARVELO, S.L.U.; OFISABEL, S.L.U.; MASQUECARPAS, S.L.U.; FEDOLA, S.LU.; BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.; PRICEMESA, S.L.U.; AGRO INNOVACIÓN FEDOLA, S.L.U; GF-TIC, S.L.U; CAMULSE, S.L.U.; EXPLOTACIONES SANTONEL, S.L.; FELAHOTEL, S.L; COSTA ADEJE GRAN HOTEL, S.L.; ISABEL FAMILY HOTEL, S.L.U.; NOELIA PLAYA, S.L.U.

Se aplica, por tanto, a todas las personas trabajadoras, personas que ostentan puestos directivos, personas colaboradoras externas y proveedores que utilicen, desarrollen o gestionen sistemas de IA en el marco de sus actividades profesionales.

III.- DEFINICIONES

Inteligencia artificial (IA): Sistema basado en algoritmos que realiza tareas que normalmente requieren inteligencia humana, como reconocimiento de patrones, predicciones, generación de texto, automatización de decisiones, etc.

Herramientas de IA: Aplicaciones o plataformas que integran IA, tales como asistentes virtuales, modelos de lenguaje, sistemas de recomendación, etc.

Datos personales: Información que permite identificar directa o indirectamente a una persona física.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos manuales o automatizados, incluyendo la recogida, registro, almacenamiento, uso, transmisión, difusión o supresión de dicha información. Abarca desde el uso de formularios en webs hasta videovigilancia.

Alfabetización en materia de IA: las capacidades, los conocimientos y la comprensión que permiten llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

IV.- PRINCIPIOS DE USO RESPONSABLE DE LAS HERRAMIENTAS BASADAS EN IA

1. Confidencialidad: Las personas trabajadoras que utilicen las herramientas basadas en IA autorizadas por la empresa no deberán introducir en la misma información confidencial tal como datos económicos, datos personales, contratos, documentación corporativa restringida o información sensible.
2. Supervisión humana: El contenido generado por IA debe ser revisado, validado y en su caso, corregido por una persona profesional.
3. Instrucciones básicas (prompts): Se recomienda el uso de prompts para lograr mejores resultados. Asimismo, se desaconseja utilizar la IA para cuestiones avanzadas, sino que se recomienda para consultas de primera orientación. PJ. Si se trata de una consulta jurídica, el ámbito es el derecho español, que no invente nada y que indique la fuente que deberá ser comprobada por un profesional.
4. Transparencia: En todo momento se deberá identificar qué documentos han sido generados por IA. Esto NO será necesario en el caso que se haya utilizado como consulta o inspiración y haya sido elaborado finalmente por una persona profesional. Asimismo, las decisiones relevantes tomadas con asistencia de IA deberán documentarse. Para garantizar la transparencia del uso de herramientas con IA, las personas trabajadoras deberán ser informados si interactúan con un sistema de IA.
5. Equidad: Las personas trabajadoras que utilicen las herramientas de IA autorizadas por la dirección de la empresa, deberán asegurarse que las decisiones y resultados del sistema no discriminen. Para ello, se limitará el uso de procesos automatizados, siendo éstos últimos supervisados por una persona.
6. Desarrollo sostenible: Se debe tener en cuenta el alto coste ecológico que puede representar el uso de ciertas herramientas de IA.
7. Legalidad: Todo uso de IA deberá cumplir con la legislación vigente, en especial la normativa de protección de datos, normativa laboral, normativa de propiedad intelectual e industrial y normativa en materia de IA. En ningún caso, podrá utilizarse las herramientas de IA para fines ilícitos y/o para facilitar la comisión de delitos.
8. Calidad y fiabilidad: Los sistemas de IA utilizados deberán ser técnicamente sólidos y tener sus límites bien definidos, cuya fiabilidad y procedencia serán verificadas.

V.- HERRAMIENTAS DE IA

1. Herramientas de IA corporativas: La dirección evaluará, identificará y aprobará las herramientas de IA para su uso profesional. Éstas serán comunicadas junto con su protocolo de uso y los responsables asignados a cada una. Su uso se regirá por los principios de este protocolo (revisión humana y confidencialidad) excepto que la herramienta haya sido diseñada para ello. Las herramientas IA corporativas, son las que se exponen en el ANEXO I "HERRAMIENTAS IA AUTORIZADAS POR GRUPO FEDOLA".

2. Herramientas de IA pública: El empleo de las herramientas de IA públicas de uso general, está prohibido excepto con autorización previa de la dirección de la empresa y, en todo caso, con lo dispuesto en este protocolo. Su uso se deberá limitar a consultas de conocimiento general, información pública y redacción de textos no confidenciales. Tras cada uso, se deberán eliminar los chats generados para que no queden almacenados en los sistemas de la IA (fuera de la Unión Europea). Si a pesar de la negativa de la dirección para su utilización, la persona trabajadora hace uso de la misma, asumirá toda la responsabilidad de las consecuencias de su uso.

VI.- USOS PERMITIDOS Y PROHIBIDOS

a) Usos permitidos

- Automatización de tareas administrativas o repetitivas.
- Generación de contenido preliminar para uso interno (textos, resúmenes, informes).
- Asistencia en análisis de datos y predicción de tendencias.
- Mejora de la experiencia del cliente mediante chatbots o recomendaciones.
- Traducir texto de una fuente secundaria disponible públicamente.
- Realizar una investigación sobre un tema no sensible.
- Lluvia de ideas sobre un tema no confidencial.
- Generación de contenido creativo, ya sea texto, vídeo o imágenes bajo supervisión humana.

b) Usos prohibidos

Queda expresamente prohibido el uso de cualquier sistema de IA que se encuentre dentro de las categorías de riesgo inaceptable, incluyendo:

- Cualquier uso que implique la mención, tratamiento o utilización de datos personales sin el consentimiento expreso, libre e informado del interesado, de conformidad con la normativa vigente en materia de protección de datos.

- Manipulación subliminal o explotación de vulnerabilidades.
- Puntuación social automatizada de personas físicas.
- Reconocimiento emocional en el entorno laboral.
- Creación de bases de datos de reconocimiento facial mediante recolección no autorizada de imágenes.
- Uso de IA para vigilar personas trabajadoras sin su consentimiento.
- Generación o difusión de contenido falso o manipulado (deepfakes, fake news).
- Tomar decisiones automatizadas que afecten a personas sin revisión humana.
- Uso de IA sin autorización o evaluación previa por parte del responsable de cumplimiento tecnológico.

VII.- EVALUACIÓN, SUPERVISIÓN Y REVISIÓN DE SISTEMAS DE IA

El uso de herramientas de IA deberá ser evaluado antes de su implantación mediante un análisis de impacto ético y legal, antes de que éste sea aprobado por la dirección de la empresa.

A tal fin, se nombra como persona responsable de IA a GF-TIC, que será la empresa encargada de la evaluación preliminar, la supervisión de su uso y la revisión periódica de los sistemas de IA utilizados.

Asimismo, GF-TIC es el único administrador, y por tanto gestor, de las herramientas IA utilizadas, por lo que tiene facultades de limitación y/o bloqueo en caso de incumplimiento.

VIII.- FORMACIÓN Y ALFABETIZACIÓN DIGITAL

Las empresas de Grupo Fedola impartirán formación periódica y obligatoria sobre los principios éticos y legales del uso de la IA, los riesgos y limitaciones de los sistemas empleados y los procedimientos de uso responsable y supervisión, tal y como se recogen en este protocolo.

IX.- CANAL DE CONSULTA

Grupo Fedola habilita un canal interno para consultas sobre el uso de IA soporte@gf-tic.com , en cuyas comunicaciones debe ir la persona jerárquicamente superior directa, debidamente copiada en el email.

X.- PROTECCIÓN DE DATOS PERSONALES

Grupo Fedola establece la prohibición expresa del uso de herramientas de IA que conlleven el tratamiento de datos de carácter personal, especialmente

aquellos de naturaleza sensible o confidencial. Esta limitación responde a la obligación de salvaguardar la seguridad de la información, la confidencialidad de los datos y el estricto cumplimiento del marco normativo vigente en materia de protección de datos.

Ante cualquier duda o intención de uso de herramientas de IA deberá ser previamente comunicada y contar con la correspondiente autorización por parte de la Dirección y del delegado de Protección de Datos (DPD).

Para ello, se remitirá un email a la persona que ostente el puesto jerárquicamente superior, para que ésta sea la que recabe la autorización correspondiente.

Sin perjuicio de lo anterior, cualquier sistema de IA que trate datos personales deberá contar mínimo con los siguientes requisitos:

- Base jurídica adecuada.
- Medidas de seguridad técnicas y organizativas implementadas para tal fin.
- Evaluación de impacto si es necesario.

XI.- ENTRADA EN VIGOR Y REVISIÓN

Este protocolo entra en vigor a partir de su implantación, previa información a la representación legal de las personas trabajadoras.

El Compliance Penal y GF-TIC revisarán semestralmente el contenido de este protocolo, asegurándose de que recoge las recomendaciones y mejores prácticas en vigor en cada momento, y propondrá al Consejo de Administración las modificaciones y actualizaciones que contribuyan a su desarrollo y mejora continua, atendiendo, en su caso, a las sugerencias y propuestas que realicen los/as profesionales de las sociedades del Grupo. No obstante, se modificará este protocolo siempre que haya un cambio normativo o cambio de criterio significativo.

XII.- COMUNICACIÓN DE INCUMPLIMIENTOS Y RÉGIMEN SANCIONADOR

Si cualquiera de las personas trabajadoras de las sociedades del Grupo, tuviera constancia o sospechas fundadas respecto de cualquier forma de incumplimiento deberá comunicarlo inmediatamente a través del canal habilitado en el sistema interno de información de Grupo Fedola. Este canal está gestionado de forma privada y confidencial.

El Grupo Fedola no tolerará ninguna represalia contra quien, de buena fe, comunique hechos que pudieran constituir un incumplimiento de este protocolo o de cualquier otro que esté vigente en el seno de la empresa.

El incumplimiento de este protocolo tendrá la consideración de infracción de las normas internas del Grupo y podrá ser objeto de medidas disciplinarias. Igualmente, las sociedades del Grupo, se reservarán el derecho de adoptar las medidas que consideren oportunas contra los socios comerciales que las incumplan.

Grupo Fedola, considera que cumplir con este protocolo es responsabilidad de todo el personal.

XIII.- COMUNICACIÓN DE LA POLÍTICA Y DIFUSIÓN

Se informa a las personas trabajadoras de la existencia del presente protocolo por medios de los instrumentos de comunicación interna.

El protocolo se encuentra a disposición de todas las partes interesadas en la App corporativa.

ANEXO I.- HERRAMIENTAS IA AUTORIZADAS POR GRUPO FEDOLA

Las herramientas IA autorizadas para su uso laboral en las empresas que componen Grupo Fedola y, por tanto, se ostenta licencia de uso, en orden de uso preferente son:

1º.- Gemini. Asistente de IA para Google Workspace

2º.- Chat GPT Pro. Herramienta IA de OpenAI.

ANEXO II.- PRÁCTICAS DE IA PROHIBIDAS

1. Quedan prohibidas las siguientes prácticas de IA:

a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los

lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias