Secuoya
content group

POLÍTICA DE USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

Secuoya, Grupo de Comunicación, S.A. y las Sociedades de su Grupo

SEDE CENTRAL:
Avenida de España, 4
28760, Tres Cantos, Madrid
+34 913 717 569

SEDE SOCIAL:
Gran Vía de Colón, 12
18010, Granada,
+34 958 216 898

Índice

1. INTRODUCCIÓN

Secuoya Grupo de Comunicación, S.A. ("Secuoya", "Secuoya Content Group" o "el Grupo") junto con las sociedades que lo integran, así como todos los Profesionales y Colaboradores que desarrollan su actividad en el Grupo, actúan conforme a la normativa vigente y a los más altos estándares éticos y profesionales.

En línea con estos principios y con el Reglamento (UE) 2024/1689 de Inteligencia Artificial (*AI Act*), esta Política de Uso Responsable de la Inteligencia Artificial (la "Política") establece el marco de actuación para el desarrollo, adopción y utilización de herramientas de inteligencia artificial ("IA") dentro del Grupo.

Esta Política forma parte del marco normativo interno de Secuoya, complementa el Código Ético, el Manual de Compliance y las demás políticas corporativas en materia de seguridad, privacidad y buen gobierno, y es de obligado cumplimiento para todas las personas y entidades a las que resulte aplicable.

Su finalidad es promover el uso responsable, ético, seguro y transparente de la IA, proporcionando a los Profesionales y Colaboradores de Secuoya directrices claras que les permitan:

- Mejorar la eficiencia y la calidad de su trabajo mediante la utilización adecuada de herramientas de IA aprobadas.
- Proteger la información y la privacidad de los datos personales y corporativos, aplicando los principios de confidencialidad, minimización y seguridad desde el diseño.
- Actuar de manera ética, responsable y transparente en todas las interacciones con sistemas de IA, garantizando la supervisión humana y el respeto a los derechos fundamentales.
- Impulsar la creatividad, la innovación y el desarrollo profesional, favoreciendo un entorno de trabajo seguro, confiable y sostenible que promueva la igualdad de oportunidades y el respeto a la dignidad de las personas.

Esta política se adapta progresivamente al marco regulatorio europeo establecido por el Reglamento (UE) de Inteligencia Artificial (AI Act), aplicable desde 2024, y será revisada conforme avancen sus fases de implementación.

Cualquier uso de herramientas de inteligencia artificial (IA) o sistemas híbridos de inteligencia artificial (HIA) por parte de Profesionales, Colaboradores o terceros que no se realice conforme a las directrices establecidas en la presente Política, en el Código Ético o en las normas internas del Grupo, será de su exclusiva responsabilidad. En ningún caso Secuoya Content Group ni las sociedades del Grupo serán responsables de los daños, perjuicios o consecuencias derivados de un uso inadecuado, no autorizado o negligente de dichas herramientas.

2. DEFINICIONES

A efectos de la presente Política, se entenderá por los siguientes términos:

- Inteligencia Artificial (IA)/Herramienta de Inteligencia Artificial (HIA): Sistema, programa o aplicación diseñado para funcionar con distintos niveles de autonomía y capaz de generar resultados automatizados (predicciones, recomendaciones, decisiones o contenidos) mediante algoritmos de aprendizaje automático u otras técnicas de IA.

- HIA Corporativa: Herramienta de IA proporcionada o previamente validada y aprobada por Secuoya para su uso profesional, tras las evaluaciones de CISO/IT (seguridad), DPO (privacidad) y Compliance (ética y uso permitido) cuando corresponda.

- HIA de Uso Personal: Herramienta de IA externa no proporcionada ni validada por Secuoya. Su utilización para fines profesionales requiere autorización previa del CISO/IT y revisión de DPO y Compliance para verificar riesgos de privacidad, propiedad intelectual y cumplimiento normativo.

- Profesional / Colaborador: Toda persona que trabaje o colabore directamente con cualquier sociedad del Grupo, y que acceda a sistemas o información del Grupo.

- Reglamento de Inteligencia Artificial (RIA): 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, así como cualquier norma que lo sustituya o desarrolle.

- Datos personales: Toda información sobre una persona física identificada o identificable, en los términos del Reglamento (UE) 2016/679 (RGPD) y de la Ley Orgánica 3/2018, incluyendo cualquier dato que permita identificar directa o indirectamente a una persona (nombre, imagen, voz, datos de contacto, identificadores en línea, etc.).

- Órgano de Supervisión y Control: Órgano interno de Secuoya regulado en el Manual de Compliance, con autonomía e independencia, encargado de vigilar el cumplimiento de las políticas corporativas, incluida la presente, y de proponer medidas correctoras o disciplinarias.

- Inputs/Outputs: *Inputs*: Datos, contenidos o información introducidos en una HIA para su procesamiento (textos, imágenes, vídeos, sonidos u otros). *Outputs*: Resultados generados por una HIA (informes, textos, imágenes, decisiones, recomendaciones u otros).

- Sesgo en IA: Tendencia o inclinación sistemática que puede producir resultados injustos, inexactos o discriminatorios en una HIA, derivada de datos de entrenamiento sesgados, supuestos incorrectos o algoritmos inadecuados.

- Tratamiento de Datos: Cualquier operación realizada sobre datos personales (recogida, registro, conservación, modificación, consulta, comunicación, supresión, etc.), de acuerdo con el RGPD y la normativa española de protección de datos.

- Trazabilidad: Capacidad de rastrear y documentar los datos, procesos, parámetros y decisiones que conducen a un determinado resultado de una HIA, incluyendo los *inputs*, algoritmos, modelos, versiones y revisiones. En el caso de herramientas o servicios en la nube, Secuoya deberá asegurarse, a través de la Dirección de IT/CISO de que la información necesaria para verificar dicha trazabilidad sea accesible y pueda conservarse como evidencia a efectos de auditoría y cumplimiento.

- Usuario: Cualquier persona que utilice, custodie o acceda a una HIA Corporativa, incluyendo Profesionales, Colaboradores o terceros expresamente autorizados por Secuoya.

- Contenido Sintético o Generado por IA: Contenido (texto, imagen, audio, vídeo u otros) producido total o parcialmente por una HIA, susceptible de ser confundido con material creado por una persona, incluidas las denominadas *deepfakes*.

- Riesgo de Alto Impacto / Alto Riesgo: Categoría definida en el Reglamento (UE) 2024/1689 para los sistemas de IA que, por su finalidad o efectos, pueden afectar a derechos fundamentales o a la seguridad (por ejemplo, IA para selección de personal, evaluación crediticia o reconocimiento biométrico).

3. ALCANCE

La presente Política es de aplicación a Secuoya Grupo de Comunicación, S.A. (“Secuoya”), a todas las sociedades que integran Secuoya Content Group en territorio español, y a todos los profesionales y colaboradores que desarrollen su actividad para el Grupo en España, con independencia de su relación jurídica, modalidad contractual o función.

Asimismo, la Política tendrá carácter orientativo para las sociedades participadas, filiales, *joint ventures*, uniones temporales de empresas (UTE) y otras entidades en las que Secuoya ejerza control o gestión fuera de España, en la medida en que la normativa local lo permita y resulte compatible con sus marcos legales y contractuales.

La Política será igualmente de obligado cumplimiento para los proveedores, contratistas, consultores, *freelancers* y demás terceros que, por razón de su actividad, accedan a sistemas, datos, contenidos o recursos del Grupo o desarrollen para el Grupo proyectos que impliquen el uso de herramientas de IA.

En estos casos, Secuoya podrá incorporar una cláusula de adhesión o de obligaciones equivalentes en los contratos, acuerdos de prestación de servicios o condiciones de colaboración que se formalicen, incluyendo compromisos en materia de seguridad de la información, protección de datos, uso ético de la IA y la facultad de auditoría o verificación por parte de Secuoya cuando resulte necesario, todo ello sin perjuicio de la normativa local aplicable.

Esta proyección pretende que cualquier persona o entidad que utilice o tenga acceso a herramientas de IA en nombre de Secuoya respete los principios de seguridad, privacidad, ética y cumplimiento normativo definidos en el presente documento.

4. PRINCIPIOS GENERALES DE ACTUACIÓN

Secuoya se compromete a poner los medios a su alcance para el uso ético, responsable y seguro de la inteligencia artificial, alineado con sus valores corporativos y con su vocación de liderazgo en el sector audiovisual y de contenidos.

Los principios que se detallan a continuación deben interpretarse y aplicarse conjuntamente con el Código Ético, el Manual de Compliance y las demás políticas corporativas del Grupo, de obligado cumplimiento para todos los Profesionales, Colaboradores y terceros vinculados a Secuoya. El incumplimiento de la presente Política podrá ser tratado como infracción de las obligaciones derivadas del Código Ético y de la normativa laboral o contractual aplicable.

Los siguientes principios deben guiar el uso de las herramientas de IA por parte de los Profesionales y Colaboradores del Grupo, tanto en el uso directo de herramientas accesibles como en la contratación o desarrollo de soluciones de IA corporativas:

I. Privacidad y protección de datos: Los Profesionales deberán abstenerse de introducir en las herramientas de IA datos personales o información confidencial del Grupo o de terceros, salvo que la herramienta haya sido previamente aprobada como HIA corporativa y cuente con las garantías establecidas por el Delegado de Protección de Datos (DPO). Se aplicarán en todo caso el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 y las políticas internas de protección de datos.

II. Seguridad y revisión de contenidos: Los resultados generados por IA deberán revisarse antes de ser utilizados, para asegurar que no contienen errores, información sensible o material que pueda afectar a terceros o a la reputación del Grupo, siguiendo las directrices de la Política de Seguridad de la Información y de la Política de Clasificación de Datos.

III. Ética y respeto a la dignidad: El uso de IA debe realizarse de forma ética, evitando daños psicológicos, reputacionales, engaños o perjuicios a terceros y respetando los valores de Secuoya, así como los derechos humanos reconocidos en el Código Ético.

IV. Propiedad intelectual: Queda prohibido introducir o utilizar en las herramientas de IA contenidos de terceros que puedan infringir derechos de autor o propiedad intelectual, salvo que se cuente con los derechos o licencias correspondientes.

V. Transparencia y comunicación: Cuando se utilice IA para generar contenidos o tomar decisiones relevantes, los Profesionales deberán dejar constancia de que se ha utilizado un sistema automatizado y, en la medida de lo posible, proporcionar explicaciones comprensibles sobre su funcionamiento y limitaciones.

VI. Seguridad y fiabilidad *(aplicable a las HIA corporativas)*: Las HIA corporativas deberán ser seguras y confiables, funcionar según su propósito y contar con mecanismos de control que eviten resultados inesperados o perjudiciales. Los sistemas deberán ser sólidos, resilientes y diseñados aplicando el principio de seguridad y cumplimiento desde el diseño.

VII. Prevención de sesgos y discriminación: Los resultados obtenidos mediante IA deben revisarse para garantizar que no reproducen estereotipos, prejuicios o discriminación de ningún tipo. Las HIA corporativas deberán ser entrenadas con datos diversos para minimizar sesgos y promover la igualdad de oportunidades, en línea con los compromisos de igualdad y no discriminación del Código Ético.

VIII. Formación y actualización continua: Los Profesionales deberán familiarizarse con las herramientas de IA y, en su caso, con las herramientas híbridas de inteligencia artificial (HIA) que utilicen, y participar en las acciones de formación que establezca el Grupo en materia de buenas prácticas, riesgos y principios éticos.

IX. Uso aceptable *(aplicable a HIA corporativas)*: Las HIA corporativas deben emplearse exclusivamente para fines profesionales, relacionados con las funciones encomendadas, y nunca para uso personal o ajeno a las actividades del Grupo.

X. Innovación y sostenibilidad: La estrategia de IA en Secuoya debe impulsar la innovación y apoyar el desarrollo sostenible, generando valor a largo plazo para la compañía y para la sociedad, siempre dentro de los límites legales y éticos.

XI. Respeto a la autonomía humana: El uso de IA debe respetar la libertad y autonomía de las personas, garantizando la supervisión y control humano sobre los procesos de trabajo y evitando que las decisiones se tomen de forma totalmente automatizada sin intervención o revisión.

XII. Evaluación y monitorización *(aplicable a HIA corporativas)*: Las HIA corporativas estarán sujetas a procedimientos continuos de evaluación y monitoreo para asegurar su correcto funcionamiento y el cumplimiento de la presente Política, garantizando, en la medida en que las capacidades técnicas de la herramienta lo permitan, la trazabilidad de sus resultados.

5. DIRECTRICES DE USO ESPECÍFICAS

Diferencias de uso entre Herramientas de IA Corporativa y Herramientas de IA de Uso Personal	
HIA Corporativa	**HIA de Uso Personal**
❖ Son herramientas de IA **identificadas, evaluadas y aprobadas** de forma previa por la **Dirección de IT/CISO**, con informe de **DPO** y validación de **Compliance**, y facilitadas por Secuoya para su uso profesional por los trabajadores autorizados. ❖ Su utilización se limita exclusivamente a fines profesionales vinculados con la actividad del Grupo. **No pueden emplearse con fines personales o ajenos a Secuoya**. ❖ No puede esperarse **ninguna expectativa de privacidad** sobre los contenidos generados por dichas herramientas, al tratarse de entornos corporativos sujetos a monitorización y trazabilidad. ❖ Es fundamental que todos los usuarios de las HIA Corporativas conozcan y respeten sus **condiciones de uso**, siendo plenamente conscientes de los posibles riesgos, de esta Política y de las **recomendaciones y advertencias** preparadas por IT/DPO/Compliance.	❖ El uso de los resultados obtenidos por una HIA de Uso Personal para fines profesionales **requiere la aprobación previa del CISO/IT**, tras la revisión de **DPO** y **Compliance** cuando se trate de datos personales o contenidos corporativos. ❖ El uso personal de herramientas de IA está permitido de forma individual y privada, siempre que **no se introduzcan datos confidenciales, personales o corporativos**, ni se utilicen resultados en el entorno profesional sin la autorización correspondiente. ❖ Secuoya **no se responsabiliza** en ningún caso del uso que se haga de las HIA de Uso Personal ni del contenido obtenido de las mismas, mientras no hayan sido aprobadas previamente por la sociedad. ❖ Si se desea incorporar resultados de herramientas personales en el trabajo, el profesional deberá asegurarse de que **cumplen los principios de esta Política**, incluyendo privacidad, propiedad intelectual, seguridad y ética ❖ Ante cualquier duda sobre la fiabilidad o adecuación de una HIA de Uso Personal, los

	Profesionales deberán **consultar con su responsable o con el área de Compliance** antes de emplear los resultados en tareas corporativas.

Procedimiento de identificación y aprobación de HIA Corporativas

Ninguna herramienta de IA podrá ser utilizada como HIA Corporativa sin que previamente:

- Dirección de IT/CISO haya realizado la evaluación técnica de seguridad y registrado la herramienta en el Inventario de HIA.
- DPO haya valorado los riesgos de privacidad y, en su caso, emitido informe o DPIA.
- Compliance haya validado el uso previsto y las cláusulas de contratación con el proveedor.

Solo tras estas validaciones la herramienta quedará autorizada para uso profesional y se comunicará a los empleados junto con las instrucciones y advertencias de uso.

La comunicación se llevará a cabo a través de la herramienta de Gestión de Incidencias o Ticketing (https://helpdesk.secuoyacontentgroup.com/) desde la cual ya se gestionan las solicitudes de nuevo software y/o servicios. En el caso de sistemas instalados localmente en los equipos de los usuarios, deberá tenerse especial precaución, dado que las políticas de seguridad internas y las herramientas implantadas en dichos equipos impiden la instalación de software no autorizado. En el caso de sistemas en la nube o sitios web, podrán establecerse límites de acceso dentro de las redes corporativas de la organización.

6. REGLAS GENERALES APLICABLES AL USO INDIVIDUAL DE LAS HIA

Para garantizar un uso responsable y seguro de la inteligencia artificial, Secuoya establece las siguientes directrices aplicables a todos los Profesionales y Colaboradores, con independencia de que utilicen herramientas de IA corporativas o de uso personal:

I. Riesgo de filtración de información sensible → No introducir en ninguna HIA datos personales, información confidencial o clasificada de las sociedades del Grupo, de sus trabajadores o de terceros, salvo que se trate de una HIA Corporativa autorizada y se cumplan las garantías establecidas por la Política de Clasificación de Datos y el Delegado de Protección de Datos (DPO).

II. Riesgo de errores, información incompleta o sesgada → Revisar siempre los resultados generados antes de compartirlos o utilizarlos, asegurando que no contengan errores, información sensible o contenidos inapropiados que puedan afectar a terceros o a la reputación del Grupo.

III. Riesgo de infringir derechos de terceros → Respetar en todo momento los derechos de autor, marcas, patentes y demás derechos de propiedad intelectual o industrial de terceros.

IV. Riesgo de generar contenidos ofensivos o discriminatorios → Actuar de manera ética y responsable, evitando generar resultados que puedan ser discriminatorios, ofensivos o perjudiciales para personas o para el Grupo, en línea con los compromisos de igualdad y no discriminación del Código Ético.

V. Riesgos de exposición de datos o vulneración de sistemas → Al utilizar plataformas externas, seguir las buenas prácticas de seguridad definidas por la Dirección de IT/CISO y mantenerse actualizado sobre los riesgos, principios éticos y recomendaciones de uso seguro de la IA.

VI. Riesgo de sesgos discriminatorios → Revisar críticamente los resultados para identificar sesgos y proporcionar retroalimentación regular a los responsables internos (IT/CISO, DPO o área de Compliance) sobre la funcionalidad y eficacia de las herramientas, con el fin de mejorar su precisión y utilidad.

El uso de la inteligencia artificial conlleva, además, una serie de derechos y responsabilidades que deben ser observados por cada profesional:

- Derecho a la explicación: Los Profesionales tienen derecho a solicitar y recibir una explicación acerca de las decisiones o resultados generados por sistemas de IA que tengan un impacto directo sobre su actividad o condiciones de trabajo. Este derecho garantiza la transparencia y la confianza en la interacción con dichas herramientas.

- Responsabilidad personal: Cada profesional es responsable de utilizar la IA de manera ética y segura, actuando con la debida diligencia en la revisión y aplicación de los resultados obtenidos y cumpliendo todos los riesgos, principios y directrices establecidos en esta Política.

- Responsabilidad de reporte de incidentes: Cada profesional debe notificar de manera inmediata cualquier brecha de seguridad, uso indebido o sospecha de mal manejo de datos a los responsables de seguridad de la información (Dirección de IT/CISO), al Delegado de Protección de Datos (DPO) o a través de los canales habilitados en el Portal del Empleado y en el Canal Ético de Secuoya, siguiendo los procedimientos establecidos en la Política de Brechas de Seguridad. Para realizar dicho reporte, deberá utilizar la herramienta de Gestión de Incidencias o Helpdesk (https://helpdesk.secuoyacontentgroup.com/), a través de la cual se gestionan las incidencias relacionadas con el área de IT y Seguridad de la Información.

7. FORMACIÓN

Para garantizar un uso responsable y seguro de la inteligencia artificial, Secuoya proporcionará la formación necesaria únicamente a los Profesionales y Colaboradores que utilicen herramientas de IA facilitadas o aprobadas por el Grupo, integrándola en los planes formativos anuales de las unidades afectadas.

En particular, cada profesional con acceso a herramientas de IA corporativas deberá:

- Recibir formación inicial, impartida o coordinada por Secuoya, sobre el uso de las herramientas que emplee, los riesgos asociados, los principios éticos y las normas de seguridad aplicables.

- Mantenerse actualizado respecto a cambios normativos o técnicos cuando así lo determine la Dirección de IT o el área de Compliance.

- Aplicar en su trabajo diario lo aprendido, revisando los resultados generados por IA y actuando conforme a los principios y directrices de Secuoya.

- Consultar ante cualquier duda al área de Compliance, al DPO o a la Dirección de IT, de acuerdo con los canales internos establecidos.

8. SUPERVISIÓN, CONTROL Y REVISIÓN

Secuoya establecerá mecanismos de supervisión y control para asegurar que el uso de la inteligencia artificial por parte de sus Profesionales se realice de manera responsable, ética y conforme a la presente Política. Estos mecanismos incluirán, como mínimo, los siguientes elementos:

- Directrices de gestión: Se definirán criterios claros para la identificación y gestión de riesgos asociados a la IA, mediante políticas específicas, formaciones y píldoras informativas. Estas directrices asegurarán que todos los Profesionales conozcan los estándares de seguridad, privacidad y ética aplicables.

- Revisión periódica: Se realizarán evaluaciones periódicas del uso de herramientas de IA, incluyendo revisión de riesgos, incidencias y buenas prácticas, con el fin de mejorar continuamente la presente Política y su aplicación. El uso de herramientas de IA deberá documentarse, indicando la finalidad y versión utilizada, a efectos de trazabilidad y rendición de cuentas.

- Actualización de la Política: La Política será revisada y actualizada de manera regular para adaptarse a cambios normativos, tecnológicos o estratégicos, garantizando que siga siendo útil y eficaz para todos los Profesionales del Grupo.

- Gestión de incidencias: Cualquier incidente, brecha de seguridad o uso indebido de la IA deberá ser reportado de manera inmediata a la Dirección de IT/CISO o, en su caso, al Delegado de Protección de Datos (DPO), utilizando los canales internos

habilitados (Portal del Empleado y Canal Ético). El Órgano de Supervisión y Control (OSC) recibirá información periódica de las incidencias relevantes para ejercer sus funciones de vigilancia.

- Funciones de CISO: El Chief Information Security Officer (CISO) es responsable de coordinar la evaluación técnica de seguridad de las HIA, mantener actualizado el Inventario de HIA corporativas, gestionar los incidentes reportados y trasladar al Órgano de Supervisión y Control (OSC) los informes necesarios para el seguimiento y control.

9. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Uso Responsable de la Inteligencia Artificial ha sido aprobada por el Consejo de Administración de Secuoya en fecha 19 de diciembre de 2025, constando en el acta correspondiente.

El Órgano de Supervisión y Control (OSC), como órgano de vigilancia del sistema de cumplimiento, podrá proponer al Consejo de Administración las modificaciones que considere necesarias para mantener un control adecuado de las actividades del Grupo, asegurar el cumplimiento de la normativa vigente y de los procedimientos internos, y minimizar el riesgo de incumplimientos.

Asimismo, la Política se adaptará progresivamente al marco regulatorio europeo establecido por el Reglamento (UE) de Inteligencia Artificial (AI Act) y a la normativa sectorial aplicable, incluyendo la futura regulación del uso de la IA en el ámbito audiovisual y artístico, y será revisada conforme avancen sus fases de implementación o se aprueben nuevas disposiciones específicas.

Cualquier actualización o modificación de la presente Política deberá ser igualmente aprobada por el Consejo de Administración y entrará en vigor en la fecha indicada en el acuerdo de aprobación, manteniéndose vigente hasta que sea expresamente sustituida, modificada o derogada.