POLÍTICA REGIONAL PARA EL TERRITORIO DE IBERIA Y AMÉRICA LATINA SOBRE EL DESARROLLO Y USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL

Revisión 01

DICIEMBRE 2025

YOU MATTER TO US

Contenido

CONTROL DEL DOCUMENTO

Elaborado por	Revisado por	Aprobado por	Fecha de Aplicación:
Écija Abogados	CISO Fdo: Javier Rincón	CEO Fdo: Sandra Gibert	1 de diciembre de 2025 **Copia Nº:** **Destinatario:**

HISTÓRICO DE MODIFICACIONES

Cuando se modifique la norma ésta avanzará secuencialmente el estado de edición del documento, actualizándose también la fecha del mismo. Dichos cambios se detallarán en la siguiente tabla:

FECHA	MOTIVO DE MODIFICACIÓN	APARTADO MODIFICADO	EDICIÓN
18/11/2025	Revisión inicial	Todos	1.0

1. Introducción

El presente documento establece la Política Regional aplicable a las empresas pertenecientes al Grupo Intelcia Holding ("**Intelcia**" o el "**Grupo**") en Iberia y Latinoamérica en relación con el desarrollo y uso responsable de la Inteligencia Artificial ("**Política Regional**").

Esta Política Regional ha sido aprobada por el Comité Global de IA, el órgano designado por el Consejo de Administración del Grupo con el objetivo de garantizar que la implementación de los Sistemas de Inteligencia Artificial ("**Sistemas de IA**") en Iberia y Latinoamérica ("**Territorio de Aplicación**"), donde están presentes las empresas, divisiones y filiales que conforman Intelcia, esté alineada con los valores, políticas y normativas de Intelcia, maximizando a su vez su potencial innovador de forma ética y responsable.

Asimismo, esta Política Regional será también aplicable, cuando proceda, a alianzas empresariales temporales, *joint ventures* y otras asociaciones equivalentes, nacionales o extranjeras, siempre que cualquiera de las empresas, divisiones o filiales de Intelcia situadas en el Territorio de Aplicación tenga el control de su gestión, y siempre dentro de los límites legalmente establecidos.

Esta Política es esencial para garantizar que el uso de los Sistemas de IA en Intelcia y en sus empresas, filiales y divisiones en el Territorio de Aplicación siga alineado con los altos estándares de seguridad, privacidad y ética exigidos por Intelcia. Dada la naturaleza de sus operaciones y su papel clave en la prestación de servicios de *outsourcing* y soluciones digitales para sectores estratégicos, asegurar un uso responsable de la IA resulta fundamental para proteger la confianza de clientes, empleados y socios de negocio.

Por ello, esta Política Regional, que sigue un enfoque de análisis y control de riesgos, tiene como finalidad establecer un marco claro y detallado que permita implementar dichos sistemas conforme a la normativa de IA aplicable a las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación.

1.1. Ámbito de aplicación

Esta Política Regional se aplica a todas las personas empleadas en las empresas, divisiones y filiales de Intelcia, incluido el personal directivo y los becarios, que desempeñen sus funciones dentro del Territorio de Aplicación, con independencia de su rol o responsabilidad. Se extiende también a los proveedores que desarrollen soluciones de IA para las empresas, divisiones y filiales de Intelcia en dicho territorio, así como a los profesionales independientes que presten servicios mediante una relación contractual con estas empresas.

En todos los niveles, áreas y departamentos de dichas empresas, el Comité Global de IA velará por la implementación real y efectiva de esta Política Regional. Es responsabilidad de todos los empleados, profesionales, proveedores y colaboradores de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación (los "**Usuarios**") leer y comprender el contenido de esta Política Regional, así como seguir y cumplir sus directrices, principios y procedimientos en su labor profesional.

Asimismo, es responsabilidad de los directores y responsables de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación evaluar la necesidad real de

que los miembros de sus equipos dispongan y utilicen Herramientas de Inteligencia Artificial ("**HIA**") para el desempeño de sus funciones profesionales.

Comprender y adherirse a lo dispuesto en esta Política Regional es fundamental para garantizar el uso efectivo y ético de las HIA.

1.2. Aprobación y Vigencia

La presente Política Regional entra en vigor en la fecha de su publicación y permanecerá vigente hasta la emisión de una nueva versión que la revoque o modifique.

2. Director Regional de IA: Nombramiento y Responsabilidades

La Política Regional será sometida a aprobación por el Comité Global de IA ("**Comité**"), que garantizará su alineación con la estrategia corporativa del Grupo y con los principios éticos sobre inteligencia artificial establecidos en la Política Global de Desarrollo y Uso Responsable de la Inteligencia Artificial, cuyas directrices estratégicas y de gestión han sido aprobadas por el Consejo de Administración.

Asimismo, el Comité designará un Director de IA para la región de Iberia y Latinoamérica, que será responsable de garantizar la eficacia de los sistemas de gestión y control de riesgos de IA, velando por el cumplimiento de la legislación aplicable, de las directrices éticas y de los marcos internos de gobernanza, así como por su plena adecuación al entorno regulatorio y tecnológico.

Sus responsabilidades incluyen:

- Implementar la política de IA adaptándose a los requisitos regulatorios locales sin comprometer la coherencia global.
- Supervisar el uso de la IA en la región, identificando riesgos, proponiendo mejoras y garantizando el cumplimiento ético y legal.
- Asegurar evaluaciones éticas y legales de impacto de las soluciones de IA antes de su implantación, en colaboración con expertos multidisciplinares.
- Informar periódicamente al Comité, proporcionando análisis sobre el estado de cumplimiento, riesgos emergentes y oportunidades de mejora en la gestión de la IA.
- Impulsar la formación y concienciación en IA, garantizando que los equipos implicados comprendan sus implicaciones regulatorias y éticas.

3. Herramientas Corporativas de IA

3.1. Concepto

Se considerarán "**Herramientas Corporativas de IA**" aquellas herramientas de inteligencia artificial validadas y aprobadas por el Comité.

Las Herramientas Corporativas de IA serán proporcionadas por el Comité para su uso profesional, de acuerdo con lo establecido en esta Política Regional y en cumplimiento de los procedimientos aprobados por el propio Comité.

Queda prohibido cualquier uso personal o particular de las Herramientas Corporativas de IA, y los empleados no pueden esperar privacidad respecto al contenido generado mediante estas herramientas ni sobre su utilización.

Las Herramientas Corporativas de IA deberán utilizarse únicamente en dispositivos corporativos facilitados y aprobados por Intelcia.

Las suscripciones o pagos derivados del uso de Herramientas Corporativas de IA serán asumidos por el Comité y formarán parte de los recursos tecnológicos que Intelcia pone a disposición de los empleados para el desempeño de sus funciones.

Los usuarios de estas Herramientas Corporativas de IA deben conocer y leer los correspondientes términos de uso y entender el funcionamiento de la HIA pertinente. Si fuera necesario, deberán solicitar información y formación para garantizar un uso adecuado de la herramienta.

3.2. Metodología de trabajo

3.2.1. Análisis y Aprobación

Las empresas, divisiones y filiales de Intelcia dentro del Territorio de Aplicación desempeñan un papel fundamental en la identificación de Sistemas de IA que, por su funcionalidad, calidad y resultados, puedan aportar beneficios a Intelcia.

Cualquier herramienta o sistema que pueda resultar útil deberá ser comunicado, con carácter previo a su uso, al director, responsable o superior jerárquico correspondiente, quien deberá evaluar y justificar su necesidad ante el Director Regional de IA o el Comité.

El Comité, en el ejercicio de sus funciones y a propuesta del Director Regional de IA, evaluará la viabilidad de la propuesta y definirá las condiciones específicas para su posible implementación.
El Comité no aprobará la incorporación de un Sistema de IA al conjunto de herramientas corporativas sin un análisis exhaustivo del sistema en cuestión, realizado por el Director Regional de IA. Dicho análisis incluirá, en todo caso, las siguientes fases o etapas:

a) Evaluación de necesidades

Serán considerados los siguientes aspectos:

- *Definición del propósito*: identificación del problema o necesidad específica que el Sistema de IA pretende abordar.

- *Impacto potencial*: estimación de cómo el sistema mejorará la eficiencia, reducirá costes o aportará valor en términos de calidad, seguridad o innovación.

- *Coherencia:* verificación de que el sistema está alineado con los objetivos estratégicos de Intelcia.

b) Análisis de riesgos

Con base en la definición del artículo 3.2 del Reglamento de Inteligencia Artificial que define “riesgo” como la combinación de la probabilidad de que se produzca un daño y su gravedad, el Director Regional de IA procederá a:

- Identificar los riesgos potenciales asociados al uso del sistema (operativos, regulatorios, éticos, de ciberseguridad, etc.).

- Analizar en qué medida los riesgos identificados podrían afectar a las operaciones, reputación o cumplimiento normativo de la empresa.

- Asignar un nivel de riesgo (bajo, medio, alto o sistémico) según los criterios establecidos en la Política Global de Intelcia para el Desarrollo y Uso Responsable de la Inteligencia Artificial.

En el Anexo I, se identifican los principales niveles de riesgo identificados.

c) Verificación técnica

La verificación consistirá en comprobar los siguientes puntos:

- Realizar pruebas de funcionalidad para asegurar que el sistema cumple las especificaciones técnicas requeridas

- Evaluar la calidad, origen y legalidad de los datos que el sistema utilizará para su entrenamiento y ejecución.

- Analizar los algoritmos utilizados con el fin de garantizar su integridad ética y seguridad.

- Verificar la compatibilidad del sistema con las infraestructuras tecnológicas existentes en las empresas, divisiones y filiales de Intelcia dentro del Territorio de Aplicación.

d) Cumplimiento normativo

En materia de cumplimiento normativo, deberán ser verificados los siguientes aspectos:

- *Auditoría regulatoria*: garantizar que el sistema cumple la normativa nacional e internacional aplicable (incluido el Reglamento de Inteligencia Artificial y otras normativas relevantes).

- *Aspectos éticos*: evaluar el impacto del sistema en términos de privacidad, equidad y transparencia.

- *Protección de datos: asegurar que el sistema cumple con la normativa de protección de datos personales, como el RGPD.*

e) Evaluación económica

- Realizar un análisis financiero para determinar si los beneficios justifican el coste de implementación y mantenimiento.

- Identificar los costes asociados, incluidas actualizaciones, formación del personal y posibles riesgos económicos derivados de su uso.

f) Procedimiento de Validación Preliminar

- Implementar el sistema en un entorno controlado para validar su eficacia y detectar posibles problemas antes de su despliegue completo.
- Recoger comentarios y experiencias previas de empleados y proveedores durante la fase piloto.
- Identificar ajustes o mejoras necesarios antes de su implantación definitiva.

g) Medidas de Detección y Mitigación

- Establecer planes de contingencia y procedimientos para gestionar incidentes o fallos de los Sistemas de IA.
- Diseñar un plan de seguimiento y auditoría para evaluar regularmente el desempeño del sistema
- Garantizar que los empleados reciben formación suficiente, adecuada y actualizada de forma periódica sobre el uso y supervisión del Sistema de IA.

h) Aprobación final

Si tras completar las fases descritas en los apartados A–G, el Comité aprueba la incorporación del Sistema de IA al conjunto de herramientas corporativas, deberá documentar todos los resultados del análisis, incluidos los riesgos identificados, pruebas realizadas y medidas de mitigación. Esta documentación deberá incorporarse a los registros corporativos, especificando el nivel de riesgo del sistema, su propósito y las condiciones de uso.

3.2.2. Implementación y uso

Las fases para la implementación y el uso continuo serán las siguientes:

a) Formación y Educación Continua

Todos los Usuarios de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación que interactúen con Sistemas de IA deberán recibir formación específica sobre su uso adecuado, así como sobre los riesgos asociados y las medidas de protección que deben aplicarse durante su funcionamiento.

Para ello, el Director Regional de IA proporcionará materiales formativos actualizados y organizará los seminarios y talleres necesarios para garantizar una formación continua y actualizada sobre los avances tecnológicos, la normativa aplicable y las mejores prácticas para el uso de Sistemas de IA por parte de los empleados.

b) Interacción y Supervisión

El Director Regional de IA garantizará que la integración de los Sistemas de IA sea coherente y no afecte negativamente a la funcionalidad o eficiencia de los procesos operativos existentes.

Para lograrlo, los procedimientos operativos serán revisados periódicamente a fin de garantizar que los Sistemas de IA no interfieran con los estándares de calidad, seguridad y sostenibilidad de Intelcia. Estas revisiones se documentarán y se presentarán regularmente al Comité.

Asimismo, el Comité podrá establecer un sistema de supervisión continua para detectar desviaciones en el comportamiento de la IA y evaluar su impacto a largo plazo, garantizando el cumplimiento de los estándares de rendimiento, seguridad y ética establecidos en la Política Global de Desarrollo y Uso Responsable de la Inteligencia Artificial.

Los Usuarios de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación deberán informar de cualquier anomalía o desviación del sistema para su análisis por parte del Comité, tras la correspondiente comunicación del Director Regional de IA.

c) Actualizaciones

El Comité, a solicitud del Director Regional de IA, será responsable de actualizar adecuadamente los Sistemas de IA, teniendo en cuenta los avances tecnológicos, los cambios regulatorios y las lecciones aprendidas de su uso. Estas actualizaciones estarán siempre orientadas a mejorar el rendimiento de la IA o garantizar el cumplimiento de nuevas normativas.

d) Retirada del Sistema de IA

Si durante la fase de supervisión o en una revisión posterior, el Director Regional de IA identifica que un Sistema de IA presenta un riesgo inaceptable, el Comité decidirá su retirada.

La retirada se llevará a cabo de forma que no se interrumpan los procesos críticos de negocio en las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación. Se adoptarán las medidas necesarias para evitar consecuencias negativas para los usuarios o sus actividades.

Los Usuarios del Sistema de IA afectado serán informados de su retirada y, si fuera necesario, el Director Regional de IA será responsable de proporcionar soluciones alternativas o sustituciones.

3.2.3. Riesgos asociados

Los Usuarios de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación deben utilizar los Sistemas Corporativos de IA en pleno cumplimiento de esta Política Regional y de la Política Global de Intelcia, prestando especial atención a la legislación aplicable y a los riesgos específicos que se detallan a continuación.

a) Reglamento de Inteligencia Artificial

El uso de Sistemas de IA dentro de INTELCIA implica su clasificación, según el Reglamento de Inteligencia Artificial, como Usuario o, cuando proceda, como Responsable de Despliegue. En consecuencia, será obligatorio cumplir con las obligaciones establecidas en el Reglamento de Inteligencia Artificial, así como en cualquier otra normativa aplicable relacionada con la IA.

En cuanto a los Sistemas Corporativos de IA que interactúen con personas físicas, deberá garantizarse que dichas personas sean informadas de que están interactuando con un Sistema de IA, salvo que ello resulte evidente por el contexto de uso.

Respecto a los Sistemas Corporativos de IA que realicen reconocimiento de emociones o categorización biométrica para acceder a servicios o aplicaciones, las personas afectadas deberán ser debidamente informadas.

Asimismo, cuando un Sistema Corporativo de IA genere o manipule contenido en forma de imagen, sonido o vídeo que se asemeje significativamente a personas, objetos, lugares, entidades o eventos reales de manera que pueda inducir a error sobre su autenticidad o veracidad, deberá indicarse claramente que dicho contenido ha sido generado por IA.

Todo lo anterior se entiende sin perjuicio de las obligaciones específicas que Intelcia deba asumir cuando sea considerada Proveedor de IA conforme al artículo 16 del Reglamento de Inteligencia Artificial. En este sentido, Intelcia será clasificada como Proveedor de IA cuando *(i)* comercialice un Sistema de IA bajo su nombre o marca, *(ii)* modifique la finalidad prevista de un Sistema de IA existente o *(iii)* realice una modificación sustancial en un Sistema de IA suministrado por un tercero.

b) Propiedad Intelectual e Industrial

En relación con los derechos de propiedad intelectual e industrial, el principal riesgo se refiere a la autoría y titularidad de los derechos asociados a los Resultados generados por los Sistemas de IA.

Por lo general, los términos de uso de la IA transfieren la titularidad del Resultado al Usuario. Sin embargo, en la mayoría de los casos no existe garantía de que el contenido generado sea único o diferenciable de otros Resultados. Puede ser idéntico o muy similar a Resultados previos generados por el Sistema de IA o a los que este pueda generar para terceros.

Por ello, los Usuarios deben llevar a cabo un análisis exhaustivo para asegurarse de que cualquier Resultado generado por un Sistema Corporativo de IA no infringe derechos de propiedad intelectual de terceros.

c) Privacidad y Protección de Datos

Los Sistemas de IA, especialmente aquellos basados en *machine learning* y procesamiento del lenguaje natural, funcionan analizando y procesando grandes volúmenes de datos. Estos conjuntos de datos pueden incluir con frecuencia Datos Personales respecto de los cuales las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación actúan como Responsables o Encargados del Tratamiento, lo que implica un riesgo inherente para la privacidad de las personas.

En consecuencia, queda estrictamente prohibida la inclusión de Datos Personales en los Prompts generados por los Usuarios, salvo en el caso de Sistemas de IA que garanticen expresamente la exclusión de dichos Datos en los Inputs.

Asimismo, los Interesados deberán ser adecuadamente informados del Tratamiento de sus Datos, asegurando la existencia de una Base Jurídica adecuada.

Las decisiones automatizadas que afecten a los Interesados solo se adoptarán bajo condiciones específicas y con el consentimiento correspondiente. El tratamiento de categorías especiales de Datos Personales se limitará a casos excepcionales que cumplan estrictamente con la normativa aplicable.

Sin perjuicio de lo anterior, cualquier uso de Sistemas Corporativos de IA que implique Tratamiento de Datos deberá ajustarse estrictamente a los principios y compromisos establecidos en la Política General de Protección de Datos de Intelcia.

d) Confidencialidad de la información

El principal riesgo relacionado con la Información Confidencial reside en que, por regla general, la mayoría de los términos de uso de los modelos de IA incluyen una licencia de uso a favor del proveedor de IA respecto del contenido, textos e imágenes introducidos en los *Prompts*, pasando así a formar parte de los *Inputs* del modelo de IA.

Esto implica que, si los Usuarios emplean Información Confidencial al generar un *Prompt*, el modelo de IA podría conservar dicha información para su entrenamiento, pudiendo llegar a incorporarla en sus *Inputs* y/o en un *Output* generado para un tercero, con el correspondiente impacto sobre la confidencialidad de la información de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación.

Por lo tanto, los Usuarios deberán abstenerse de utilizar Información Confidencial en el contexto de modelos de IA, garantizando el cumplimiento efectivo de sus obligaciones en materia de confidencialidad y seguridad de la información.

e) Cyberseguridad

El Director General de IA realizará un análisis de riesgos de ciberseguridad antes de implementar un modelo corporativo de IA, con el fin de prevenir accesos y/o usos fraudulentos de Información Confidencial y garantizar el uso adecuado de los medios técnicos e informáticos.

Estos análisis de riesgo se llevarán a cabo de forma regular y podrán realizarse, cuando sea viable, mediante declaraciones periódicas de cumplimiento. En cualquier caso, deberán realizarse con una periodicidad mínima anual, salvo decisión motivada del Comité, que deberá estar individualizada para el caso concreto.

f) Derecho de la competencia

El principal riesgo en el ámbito del derecho de la competencia son las elevadas sanciones que las autoridades competentes podrían imponer a Intelcia en caso de infracción.

En particular, la utilización de modelos de IA para el seguimiento de precios o la fijación dinámica de precios podría ser considerada por las autoridades de competencia como una herramienta de coordinación con competidores o como un medio para controlar los precios finales aplicados por los clientes de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación.

En este sentido, si se emplean modelos de IA para el seguimiento de precios o la fijación dinámica de precios, deberán respetarse los siguientes principios:

• No se utilizarán modelos de IA que permitan la coordinación con competidores.

• El seguimiento y monitorización de precios mediante modelos de IA solo podrá utilizarse para la determinación interna de los precios y promociones que las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación ofrezcan a sus clientes.

• La información recibida del modelo de IA no podrá compartirse con terceros (proveedores, clientes o competidores).

• La información recibida del modelo de IA no podrá utilizarse para monitorizar la adherencia de los clientes a los precios recomendados por las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación.

• La información recibida no podrá utilizarse, ni directa ni indirectamente, en conversaciones con clientes.

4. Herramientas de IA de Uso Personal

4.1. Concepto y ámbito

Las Herramientas de IA de Uso Personal son aquellas que no han pasado por un proceso de validación ni han sido aprobadas por el Comité, y que pueden ser utilizadas eventualmente por los Usuarios de las empresas, divisiones y filiales de Intelcia en el Territorio de Aplicación para fines personales, pero con un posible impacto en su actividad profesional.

El Comité no es responsable, en ningún caso, del uso que se haga de las Herramientas de IA de Uso Personal ni del contenido generado a través de dichas herramientas que no haya sido previamente validado o aprobado por él.

Estas herramientas pueden ofrecer soluciones útiles y eficientes, pero también pueden comportar riesgos en materia de Propiedad Intelectual, privacidad o Información Confidencial. Aunque su uso pueda autorizarse en determinadas circunstancias, será necesaria la autorización expresa y por escrito del Director Regional de IA, y es importante que los Usuarios comprendan las implicaciones y responsabilidades asociadas.

El Usuario que utilice Herramientas de IA de Uso Personal deberá dejar claro que el contenido generado y, en su caso, publicado, es personal y no deberá identificarse, bajo ninguna circunstancia, como Empleado/Proveedor de la empresa, división o filial de Intelcia en el Territorio de Aplicación en dicho contexto.

Además, el Usuario no podrá manifestar, comentar hechos, usar y/o publicar contenido generado por Herramientas de IA de Uso Personal que directa o indirectamente

comprometa el nombre, la reputación, la imagen o el prestigio de la empresa, división, filial de Intelcia y/o del Grupo.

4.2. Obligaciones Relacionadas con las Herramientas de IA de Uso Personal

a) Deber de Información

Si un Usuario utiliza una herramienta de IA no aprobada, tiene la responsabilidad de informar a su director o responsable de departamento para que éste remita la información al Director Regional de IA.

Esto permite al Director Regional de IA supervisar y controlar las herramientas utilizadas, evaluar riesgos potenciales y, si procede, iniciar el proceso de validación y aprobación de la herramienta ante el Comité. Este deber de información es esencial para mantener la transparencia, la seguridad y el cumplimiento normativo en el uso de herramientas de IA dentro de las empresas del Territorio de Aplicación y del Grupo.

En caso de que la herramienta de IA de uso personal no haya sido validada y aprobada por el Comité, o no exista autorización expresa, el Usuario deberá abstenerse de utilizarla.

En consecuencia, cuando un Usuario genere contenido o utilice Herramientas de IA de Uso Personal con fines laborales sin aprobación previa o autorización expresa del Comité, asumirá la responsabilidad por cualquier consecuencia que pueda derivarse de tales acciones y podrá enfrentarse a las medidas legales y/o disciplinarias que correspondan.

b) Deber de Cumplimiento

Independientemente de que una herramienta haya sido aprobada o no, todos los Usuarios están obligados a respetar y cumplir las disposiciones de esta Política Regional. Esto incluye, entre otros aspectos, el uso ético y responsable de las herramientas de IA, el respeto por la privacidad y la seguridad de los datos, y el cumplimiento de la normativa aplicable.

En resumen, aunque el uso de herramientas no aprobadas pueda ser autorizado en determinados casos, los Empleados deben ser plenamente conscientes de sus responsabilidades y obligaciones, y el Director Regional de IA establecerá mecanismos de control y supervisión para garantizar la seguridad, la privacidad y el cumplimiento normativo.

4.3. Riesgos Asociados al Uso de Herramientas de IA de Uso Personal

Los riesgos asociados a las Herramientas de IA de Uso Personal son los mismos que los relacionados con las Herramientas Corporativas de IA. A este respecto, véase el apartado 3.3.

5. Consideraciones éticas

a) Uso ético de Herramientas de Inteligencia Artificial para la creación de contenido

El Comité es responsable de garantizar que cualquier contenido generado mediante Herramientas de Inteligencia Artificial cumpla con lo establecido en esta Política, asegurando su carácter ético y su respeto a la normativa vigente.

En este sentido, el Comité prohibirá el uso de este tipo de herramientas para crear contenidos que puedan resultar engañosos, manipuladores o que provoquen perjuicios a personas o a la reputación de Intelcia, sus empresas, divisiones y filiales dentro del Territorio de Aplicación y/o del Grupo.

La transparencia será un principio prioritario para asegurar que los consumidores puedan distinguir entre contenido generado por personas y contenido generado mediante Herramientas de Inteligencia Artificial.

Este enfoque ético será esencial para fomentar la confianza y el respeto entre el Grupo Intelcia, sus Usuarios y Profesionales, colaboradores, clientes y el público en general.

b) Transparencia

El Comité se compromete a proporcionar, en la medida de lo posible y de forma razonable, información detallada sobre el uso de Herramientas de Inteligencia Artificial dentro del Grupo Intelcia y de sus empresas, divisiones y filiales en el Territorio de Aplicación. Este compromiso incluye explicar qué tipos de datos se recopilan, cómo se procesan y cómo intervienen estas herramientas en la toma de decisiones y en la generación de contenidos.

Asimismo, el Comité hará todo lo posible para garantizar que los proveedores de estas Herramientas de Inteligencia Artificial cumplan con el principio de transparencia, promoviendo así una cultura ética y responsable dentro del ecosistema de inteligencia artificial del Grupo Intelcia.

c) Supervisión humana y rendición de cuentas

El Comité velará para que los contenidos o resultados producidos mediante Herramientas de Inteligencia Artificial estén, en todo momento, bajo la responsabilidad del Usuario o Profesional que las utilice, manteniendo un adecuado grado de supervisión humana.

El Comité garantizará que los Usuarios y Profesionales revisen de manera adecuada los resultados generados por estas herramientas, verificando que cumplen con los requisitos establecidos en la Política.

d) Control de sesgos y discriminación

El Comité asegurará que no se genere ni utilice contenido que sea discriminatorio, amenazante o perjudicial para los derechos de las personas. Asimismo, identificará y mitigará cualquier sesgo presente en los datos o algoritmos utilizados por las Herramientas de Inteligencia Artificial dentro de Intelcia, sus empresas, divisiones y filiales en el Territorio de Aplicación.

e) Responsabilidad social corporativa

En el marco de la responsabilidad social corporativa del Grupo Intelcia, el Comité garantizará que el uso de Herramientas de Inteligencia Artificial aporte beneficios a la sociedad en su conjunto.

Para ello, se compromete a formar y apoyar a los Usuarios y Profesionales, conforme a lo previsto en este Procedimiento, para asegurar el cumplimiento de los principios éticos aplicables al uso de estas herramientas.

6. Supervisión, interpretación y revisión

6.1. Supervisión

El cumplimiento de esta Política será supervisado por el Comité. Se realizarán auditorías y revisiones periódicas para garantizar que todas las Herramientas de Inteligencia Artificial cumplen con los estándares establecidos.

Cualquier incidencia o problema que pueda afectar al funcionamiento o a la seguridad de los sistemas de información de Intelcia deberá ser comunicado de inmediato al Comité a través de los canales designados en los Procedimientos.

Como métrica de rendimiento, el proceso de gestión de vulnerabilidades se documentará mensualmente, incluyendo la relación de vulnerabilidades gestionadas y el estado de su resolución.

El incumplimiento de esta Política podrá derivar en responsabilidades legales de diversa índole, según la legislación aplicable. Intelcia se reserva el derecho de emprender las acciones legales que considere oportunas.

6.2. Interpretación

El Comité será el punto de contacto principal para cualquier consulta o duda relacionada con la interpretación o aplicación de esta Política. El Comité Global de IA podrá ser contactado mediante los canales oficiales habilitados para este fin.

6.3. Revisión y actualización

Esta Política será revisada y actualizada periódicamente con el fin de alinearla con los avances tecnológicos, los cambios regulatorios o las novedades organizativas, técnicas o procedimentales dentro de Intelcia. Asimismo, se incorporarán las mejores prácticas identificadas en el uso de inteligencia artificial.

Toda modificación o actualización deberá contar con la aprobación del Consejo de Administración de Intelcia, tras el informe correspondiente del Comité Global de IA. La versión revisada será comunicada a los Profesionales y Usuarios a través de los canales establecidos.

7. Difusión de la Política

Esta Política Regional será publicada en la página web corporativa de Intelcia, garantizando que todos los Profesionales y Usuarios puedan conocer su contenido íntegro y sus disposiciones.

Además, Intelcia llevará a cabo acciones de comunicación, formación y sensibilización para facilitar la comprensión y correcta aplicación de esta Política y de sus futuras actualizaciones.

Se recomienda a los Usuarios revisar periódicamente esta Política en los canales disponibles, a fin de asegurar su pleno conocimiento. La falta de conocimiento total o parcial de esta Política no exime del cumplimiento de sus disposiciones.

8. Entrada en vigor

Esta Política Regional fue aprobada por el Comité Global de IA el [] de [] de [2025] y entrará en vigor en el momento de su publicación en la página web corporativa de Intelcia.

APÉNDICE 1: Niveles de Riesgo

RIESGO INACEPTABLE

Se entienden como sistemas IA de riesgo inaceptable aquellos que se catalogan como prácticas prohibidas por el RIA en el sentido de su artículo 5.

- En el caso de los **proveedores**, en ningún caso podrá contratarse con proveedores que ofrezcan, comercialicen o implementen este tipo de sistemas.

  En este sentido, los proveedores que incumplan esta directriz estarán sujetos a la terminación inmediata de su relación contractual y, en su caso, a las sanciones legales pertinentes.

- En el caso de los **empleados, contratistas, y proveedores y colaboradores** de Intelcia deben abstenerse de proponer, recomendar o utilizar Sistemas de IA que puedan clasificarse como de riesgo inaceptable.

  Asimismo, en caso de identificar un sistema sospechoso, deben informar de inmediato al Comité.

A efectos ejemplificativos, a continuación, se presenta una relación de las principales prácticas prohibidas:

a) **Técnicas manipulativas**:
   - El uso de IA para influir de manera subliminal o engañosa en el comportamiento de las personas, afectando su capacidad de decisión.

b) **Explotación de vulnerabilidades**:
   - Sistemas IA que se aprovechan de personas vulnerables por su edad, discapacidad o situación económica, afectando su comportamiento de manera perjudicial.

c) **Evaluaciones perjudiciales**:
   - Los que clasifican o evalúan a personas, mediante puntuaciones injustas o en contextos no relacionados.

d) **Evaluación de riesgos criminales**:
   - El uso de IA para predecir el riesgo de delito basado únicamente en perfiles o rasgos de personalidad, sin hechos objetivos.

e) **Reconocimiento facial indiscriminado**:
   - La creación de bases de datos de reconocimiento facial a partir de imágenes obtenidas sin consentimiento.

f) **Inferencia de emociones**:
   - Uso de IA para deducir emociones en lugares de trabajo o educativos, excepto en casos médicos o de seguridad.

g) **Categorización biométrica**:
   - Clasificación basada en datos biométricos para inferir características sensibles.

h) **Identificación biométrica en tiempo real**:
   - Uso de identificación biométrica remota en espacios públicos para el cumplimiento de la ley, solo en situaciones excepcionales.

Así mismo tendrá carácter de riesgo inaceptable el uso de sistemas IA que no puedan garantizar que la información proporcionada no será utilizada para entrenar el sistema ni que la información no será ofrecida como resultado para otros usuarios, con independencia de su pertenencia o no a Intelcia.

RIESGO ALTO

En aquellos casos en los que el sistema de IA no se considere de riesgo inaceptable, deberá estarse a la posibilidad de que se trate de un sistema de alto riesgo.

Estos sistemas deben cumplir con una serie de requisitos, que, a título enunciativo consisten en: contar con un sistema de gestión de riesgos, prácticas de gobernanza y gestión de datos, redacción de la documentación técnica, conservación de registros, transparencia, supervisión humana y precisión, solidez y ciberseguridad.

A modo ejemplificativo, se presenta un listado de los principales casos de riesgo alto identificados por Intelcia de conformidad con el RIA:

a) Biometría:
- Identificación remota de personas mediante características biométricas.
- Categorización de personas por atributos sensibles (como raza o género).
- Sistemas que reconocen emociones.

b) Infraestructuras críticas:
- Sistemas de IA que controlan la seguridad de infraestructuras esenciales como el tráfico, agua, gas o electricidad.

c) Educación:
- IA que decide quién puede acceder a centros educativos.
- IA que evalúa el desempeño académico de estudiantes.
- IA que determina el nivel educativo de una persona.
- IA que detecta comportamientos inadecuados durante exámenes.

d) Empleo y gestión laboral:
- IA utilizada en procesos de selección de personal o promoción.
- IA que evalúa el desempeño de los empleados o asigna tareas según su comportamiento.

e) Servicios esenciales:
- IA que decide si una persona puede acceder a servicios públicos, como la asistencia sanitaria.
- IA que evalúa la solvencia o calificación crediticia de una persona.
- IA que clasifica la urgencia de llamadas de emergencia (policía, bomberos, ambulancias).

f) Aplicación de la ley:
- IA que ayuda a las autoridades a evaluar el riesgo de que alguien sea víctima de delitos o cometa un delito.
- IA que evalúa la fiabilidad de pruebas en investigaciones criminales.
- IA que utiliza perfiles de personas para detectar o investigar delitos.

g) Migración y control de fronteras:
- IA que ayuda a evaluar riesgos (como migración irregular) en personas que quieren entrar a un país.
- IA que ayuda a decidir sobre solicitudes de asilo o visado.

h) Justicia y procesos democráticos:
- IA utilizada por jueces para interpretar leyes o hechos en investigaciones.
- IA que influye en elecciones o en el comportamiento de los votantes.

Así mismo tendrá carácter de riesgo alto el uso de Sistemas IA que no puedan garantizar que la información proporcionada no será ofrecida como resultado para otros usuarios pertenecientes a Intelcia o vinculados a este.

RIESGO LIMITADO

Este nivel comprende los riesgos asociados con la falta de transparencia en el uso de los sistemas de IA e incluye el contenido generado por IA que debe ser etiquetado como generado artificialmente.

Estos sistemas deben garantizar un nivel básico de cumplimiento con los principios de transparencia, responsabilidad y no discriminación, informando a los usuarios de que están interactuando con un sistema de IA, garantizando la supervisión humana cuando sea necesario y asegurando que el sistema de IA no sea empleando en influir en los usuarios de forma engañosa.

A modo ejemplificativo, a continuación, se presenta un listado de los principales casos de riesgo limitado identificados por Intelcia de conformidad con el RIA:

a) Interacción con usuarios:
- Chatbots y asistentes virtuales para atención al cliente.
- Sistemas de recomendación en plataformas de entretenimiento o comercio electrónico.

b) Marketing y publicidad:
- Sistemas de IA utilizados para personalizar anuncios basados en preferencias del usuario.
- Herramientas para segmentación de audiencias en campañas publicitarias.

c) Productividad:
- Procesadores de texto con capacidades de corrección automática.
- Aplicaciones que sugieren mejoras en la redacción o estructura de documentos.

RIESGO MÍNIMO

Los sistemas de IA clasificados como de **riesgo mínimo o nulo** presentan un impacto insignificante sobre los derechos fundamentales y la seguridad. Estos sistemas no requieren medidas regulatorias específicas, aunque deben respetar los principios generales de ética y responsabilidad corporativa.

Estos sistemas deben garantizar un uso responsable que evite toda discriminación o parcialidad e implementar códigos de buenas prácticas conforme a los estándares de la industria.

A modo ejemplificativo, a continuación, se presenta un listado de los principales casos de riesgo limitado identificados por Intelcia de conformidad con el RIA:

a) Filtros y clasificaciones:
- Filtros de spam en correos electrónicos.
- Sistemas que clasifican contenido según categorías (p. ej., etiquetado en bibliotecas digitales).

b) Automatización sencilla:
- Herramientas para automatizar tares en aplicaciones de oficina.
- Sistemas de recomendación en plataformas de entretenimiento o comercio electrónico.

d) Corrección y ayuda técnica:
- Correctores ortográficos y gramaticales en aplicaciones de escritura.
- Calculadoras avanzadas que sugieren métodos para resolver problemas matemáticos.