



POLÍTICA CORPORATIVA SOBRE USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

1. OBJETIVO

Establecer los lineamientos corporativos para la adquisición, desarrollo, implementación, utilización y supervisión responsable de soluciones de inteligencia artificial (IA), promoviendo una gestión basada en principios de ética, seguridad, transparencia, privacidad, supervisión humana, cumplimiento normativo y gestión de riesgos.

2. ALCANCE

La presente Política aplica a Grupo Aval Acciones y Valores S.A (Grupo Aval) y sus entidades subordinadas. Su cumplimiento es obligatorio para colaboradores, administradores y terceros que participen en la adquisición, desarrollo, implementación, operación o utilización de soluciones de IA.

Aplica para las diferentes tecnologías y modalidades de IA, incluyendo IA generativa, modelos de lenguaje, Machine Learning, analítica avanzada, automatización inteligente, asistentes virtuales, sistemas de recomendación y predicción, agentes de IA y soluciones de IA provistas como servicio, tanto desarrolladas internamente como suministradas por terceros.

3. LINEAMIENTOS DE USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL

Esta Política:

- Define e implementa un Programa de IA Responsable que establezca los procesos, roles, controles y herramientas necesarios para asegurar que el desarrollo, adquisición, implementación y uso de sistemas de inteligencia artificial se realicen de manera ética, segura, transparente y alineada con los principios definidos en esta Política.
- Orienta la adquisición, desarrollo, implementación, uso y supervisión de soluciones de IA. Su aplicación deberá ser proporcional al nivel de riesgo, criticidad e impacto de cada caso de uso, tomando como referencia la normativa colombiana aplicable, la Política Nacional de Inteligencia Artificial, los principios de IA confiable de la OCDE, el Marco de Gestión de Riesgos de IA del NIST, la ISO/IEC 42001 y las restricciones de la Ley de Inteligencia Artificial de la Unión Europea frente a usos prohibidos.
- Promueve la incorporación de criterios ambientales, sociales y de gobernanza (ASG) en el uso de soluciones de IA propias y de terceros, considerando la medición de impactos en sostenibilidad, derechos humanos, inclusión, equidad, accesibilidad, eficiencia energética, uso responsable de recursos y reducción de la huella ambiental. Para ello, podrán realizarse evaluaciones de riesgos e impactos, procesos de debida diligencia, validaciones de diseño y mecanismos de monitoreo periódico.

3.1. Gobierno y responsabilidad

La utilización de sistemas de inteligencia artificial constituye una herramienta de apoyo para la gestión y la toma de decisiones, pero no reemplaza el juicio profesional, la responsabilidad ni las funciones asignadas a las personas o instancias de gobierno definidas por Grupo Aval y sus entidades. Las decisiones apoyadas por IA continuarán siendo responsabilidad de las áreas.

Toda herramienta, sistema, modelo o aplicación que incorpore funcionalidades de inteligencia artificial, ya sea desarrollada internamente o adquirida a terceros, deberá contar como mínimo con la siguiente estructura de gobierno, la cual no podrá delegarse exclusivamente al proveedor:

✓ Responsable funcional

Área:	Código:	Versión:	Fecha Última Actualización:
-------	---------	----------	-----------------------------

- ✓ Responsable técnico.
- ✓ Áreas de control participantes.
- ✓ Nivel de aprobación requerido.
- ✓ Responsables del monitoreo.

3.2. Privacidad, protección de datos y propiedad intelectual

- La utilización de IA deberá cumplir las disposiciones internas sobre protección de datos personales, confidencialidad de la información, propiedad intelectual y demás obligaciones legales y regulatorias aplicables como la Ley 1581 de 2012 (régimen general de protección de datos personales), el Decreto 1377 de 2013 y la doctrina de la Superintendencia de Industria y Comercio (SIC).
- El uso de sistemas de inteligencia artificial deberá realizarse de manera consistente con las políticas de confidencialidad y protección de datos de la Organización. En consecuencia, no podrá compartirse información confidencial, reservada, privilegiada o datos personales en herramientas de IA que no cuenten con los controles y autorizaciones correspondientes.
- Deberá respetarse la titularidad de los derechos de autor tanto sobre la información utilizada como sobre los contenidos generados mediante herramientas de IA, conforme a la normativa aplicable y las políticas corporativas.

3.3. Seguridad de la información y ciberseguridad

- Las soluciones de inteligencia artificial deberán cumplir con los lineamientos de seguridad de la información y ciberseguridad definidos por la Grupo Aval, incorporando medidas de control acordes con su nivel de riesgo y con la naturaleza de la información que procesan.
- Durante el ciclo de vida de los sistemas de inteligencia artificial, entendiendo este como las etapas de diseño, desarrollo, adquisición, implementación, operación, monitoreo y retiro de la solución, se deberán implementar medidas de seguridad acordes con su nivel de riesgo, tales como filtrado de contenido, monitoreo de vulnerabilidades, validación de instrucciones, protección frente a manipulaciones de modelos y otros mecanismos que resulten aplicables.

3.4. Transparencia, trazabilidad y capacidad razonable de explicación

- Los desarrollos efectuados por terceros o las decisiones o recomendaciones generadas internamente mediante IA deberán ser trazables, tener claridad del por qué y para qué son usadas, cuáles son sus limitaciones, quién responde por el resultado y deberá ser susceptible de revisión cuando su naturaleza o impacto así lo requieran.
- En los casos en que una solución de IA pueda incidir en cualquier decisión (derechos, condiciones económicas, acceso a productos o servicios, empleo u otros), deberá existir supervisión humana efectiva.

3.5. Uso ético, equidad y no discriminación

- En el desarrollo, adquisición y utilización de soluciones de inteligencia artificial se deberán observar y aplicar los principios, compromisos y lineamientos corporativos de Grupo Aval y sus entidades en materia de ética, derechos humanos, diversidad, inclusión y respeto por la dignidad de las personas. En consecuencia, las soluciones de IA no deberán utilizarse de manera que generen discriminación, exclusión, sesgos indebidos o tratos injustificados que puedan afectar a las personas o grupos de interés. Los casos de uso de IA que puedan afectar de manera significativa los derechos, oportunidades, condiciones o decisiones que involucren a las personas deberán ser identificados y evaluados previamente, antes de su implementación o puesta en producción. La evaluación deberá considerar el nivel de riesgo asociado al uso de la IA y permitir identificar, prevenir y mitigar posibles sesgos, discriminación, errores o cualquier otro impacto adverso que pueda afectar a las personas.

Área:	Código:	Versión:	Fecha Última Actualización:
-------	---------	----------	-----------------------------

3.6. Usos permitidos, restringidos y prohibidos

La IA podrá utilizarse para fortalecer la innovación, la eficiencia operativa, la gestión de riesgos, la analítica, la automatización y el apoyo a la toma de decisiones, siempre que se respeten los lineamientos establecidos en esta Política.

Se consideran usos prohibidos, entre otros:

- Sustituir completamente el juicio humano en cualquier decisión.
- Utilizar herramientas de IA no autorizadas para procesar información confidencial o datos personales.
- Generar información falsa, engañosa o discriminatoria.
- Desarrollar soluciones destinadas a vulnerar derechos, la privacidad, la seguridad o la normativa aplicable.
- Implementar sistemas catalogados como prohibidos por la legislación vigente o por las políticas corporativas.

3.7. Gestión del ciclo de vida de la IA

- Toda solución de IA deberá gestionarse durante su ciclo de vida, desde su evaluación, adquisición o desarrollo hasta su retiro, garantizando la implementación de controles de riesgo, seguridad, calidad, monitoreo y mejora continua.
- Las modificaciones significativas realizadas a una solución de IA deberán ser evaluadas antes de su entrada en operación.

3.8. Gestión de terceros

La contratación de proveedores de soluciones de IA deberá incluir una evaluación de riesgos que considere, seguridad de la información, protección de datos, privacidad, continuidad del servicio, cumplimiento normativo, propiedad intelectual, atención de incidentes, gestión de vulnerabilidades y niveles de transparencia ofrecidos por el proveedor. Los contratos deberán incorporar las obligaciones necesarias para garantizar el cumplimiento de esta Política.

3.9. Monitoreo, incidentes y mejora continua

Las soluciones implementadas deberán monitorearse periódicamente para verificar:

- ✓ Exactitud de los resultados.
- ✓ Permanencia de los controles.
- ✓ Cambios relevantes en el desempeño.
- ✓ Riesgos emergentes.
- ✓ Incidentes asociados.
- ✓ Cumplimiento de esta Política.

Cuando se identifiquen desviaciones relevantes deberán establecerse planes de tratamiento y seguimiento.

3.10. Indicadores y reporte

Se deben definir y monitorear indicadores que permitan medir la efectividad del Programa de IA Responsable, incluyendo, cuando resulte aplicable, métricas relacionadas con la adopción, riesgos identificados, indicadores de sostenibilidad asociados a la IA, incidentes, sesgos detectados, cumplimiento de controles, desempeño de los modelos, capacitación, acciones de mejora y reportes periódicos a las instancias correspondientes.

Área:	Código:	Versión:	Fecha Última Actualización:
-------	---------	----------	-----------------------------

3.11. Sostenibilidad

En el desarrollo de soluciones de inteligencia artificial y en los procesos de adquisición, selección y evaluación de proveedores asociados a estas tecnologías, se consideren criterios de eficiencia energética, reducción de huella ecológica y gestión ambiental, cuando ello resulte viable y proporcional al caso de uso, mediante la incorporación de dichos aspectos en las evaluaciones de proveedores, procesos de contratación o requerimientos de diseño de las soluciones.

3.12. Formación y cultura organizacional

Esta política busca que se promuevan programas de capacitación para fortalecer el uso responsable de la IA a colaboradores y terceros autorizados desde Grupo Aval y sus entidades. Las actividades de formación deberán abordar, según corresponda:

- ✓ Lineamientos de esta Política.
- ✓ Ética en IA.
- ✓ Protección de datos.
- ✓ Seguridad de la información.
- ✓ Riesgos asociados.
- ✓ Buenas prácticas.
- ✓ Herramientas autorizadas.
- ✓ Responsabilidades de los usuarios.

3.13. Inventario de soluciones de IA

Se debe mantener un inventario actualizado de los sistemas, modelos, herramientas y casos de uso de inteligencia artificial, identificando como mínimo:

- ✓ Responsable del negocio.
- ✓ Responsable técnico.
- ✓ Finalidad del sistema.
- ✓ Datos utilizados.
- ✓ Estado del ciclo de vida.
- ✓ Controles implementados.

Para tal fin, las áreas responsables de seguridad de la información y tecnología, en coordinación con las áreas de negocio o áreas usuarias que desarrollen, adquieran o utilicen soluciones de IA, deberán colaborar en la identificación, registro, actualización y seguimiento de dicho inventario.

3.14. Evaluación de riesgos

Antes de implementar una solución de IA, deberá realizarse una evaluación de riesgos acorde con su criticidad. Como mínimo deberán analizarse aspectos relacionados con:

- ✓ Privacidad y protección de datos.
- ✓ Seguridad de la información.
- ✓ Riesgos de ciberseguridad.
- ✓ Cumplimiento regulatorio.
- ✓ Derechos humanos.
- ✓ Riesgo operacional y reputacional.
- ✓ Dependencia de terceros.
- ✓ Impactos ambientales cuando sean relevantes.
- ✓ Continuidad del negocio

La evaluación deberá actualizarse cuando existan cambios significativos en el modelo o en su utilización.

Área:	Código:	Versión:	Fecha Última Actualización:
-------	---------	----------	-----------------------------

3.15. Gestión documental y trazabilidad

Se debe conservar como mínimo la siguiente documentación para demostrar la gestión del ciclo de vida de las soluciones de IA:

- ✓ Evaluaciones realizadas.
- ✓ Aprobaciones.
- ✓ Riesgos identificados.
- ✓ Controles implementados.
- ✓ Cambios relevantes.
- ✓ Incidentes.
- ✓ Monitoreos efectuados.
- ✓ Decisiones adoptadas.

La información deberá mantenerse conforme a las políticas o procedimientos de gestión documental.

4. GLOSARIO

- **Inteligencia artificial —IA—:** sistema basado en máquinas que, con distintos niveles de autonomía, puede generar resultados como predicciones, contenidos, recomendaciones, clasificaciones o decisiones a partir de datos de entrada.
- **Sistema de IA:** conjunto de modelos, algoritmos, datos, infraestructura, reglas, interfaces, procesos y controles que permiten desarrollar, operar o utilizar capacidades de inteligencia artificial.
- **IA generativa:** tipo de IA capaz de generar texto, imágenes, audio, video, código, simulaciones u otros contenidos nuevos a partir de instrucciones, datos o patrones aprendidos.
- **Sesgo:** desviación sistemática en datos, modelos, procesos o resultados que puede producir errores, exclusión, discriminación o trato inequitativo.
- **Explicabilidad:** es la capacidad de un sistema de inteligencia artificial para explicar de manera clara y comprensible cómo llegó a un resultado, una recomendación o una decisión.
- **Transparencia:** obligación de informar de manera clara y suficiente el uso, propósito, alcance, limitaciones y responsables de un sistema de IA, según el contexto.
- **Supervisión humana:** capacidad real de una persona competente para revisar, validar, modificar, suspender, revertir o intervenir una decisión o resultado generado por IA.
- **Huella ecológica de IA:** impacto ambiental asociado al desarrollo, entrenamiento, operación, almacenamiento, procesamiento y uso de sistemas de IA, incluyendo consumo energético, emisiones, agua, infraestructura y ciclo de vida tecnológico.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	RAZÓN DEL CAMBIO
2026	1	Emisión del documento

Área:	Código:	Versión:	Fecha Última Actualización:
-------	---------	----------	-----------------------------